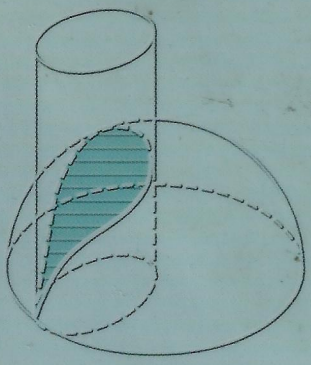
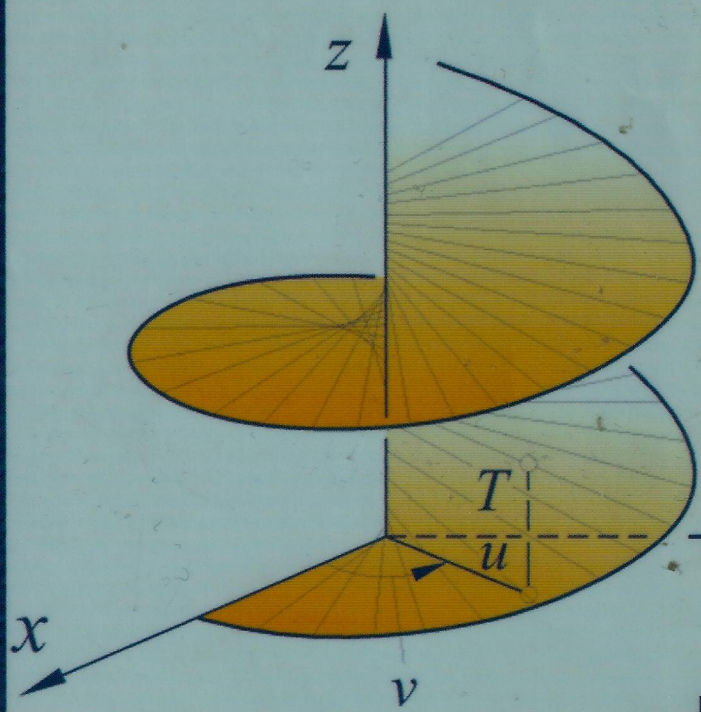
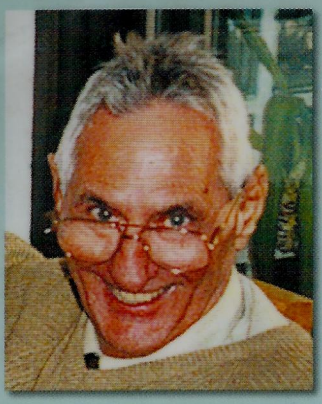
HORVATIC



LINEARNA ALGEBRA



GOLDEN MARKETING
TEHNIČKA KNJIGA



KREŠIMIR HORVATIĆ rođen je 193
škole te na PMF-u 1954. diplomira
ku. Godine 1966.–1968. provodi n
gdje je na University of Georgia, A
geometrijske topologije *Embeddin*
Kao gostujući profesor, boravio je š
sity of Utah, Salt Lake City. U nek
kraće je vrijeme proveo u Varšavi, I
i onda 1988. na Ludwig Maximilian
to sudjeluje na periodičkim sastanc
Graz, kao i tradicionalnom *Topolo*

Cijeli radni vijek proveo je pr
PMF-a u Zagrebu. Član je Hrvatskoga matematičkog društva i American Mathematical Society.

IZ RECENZIJA

Za razliku od postojećih tekstova, autor uvodi čitatelja postupno u pojedine teme, uz odgovarajuću motivaciju, objašnjavajući geometrijsku pozadinu obrađivanih ideja ... .

Potpuno je nestandardno posljednje poglavlje, od interesa za sve one koji žele dobiti prvu informaciju o teoriji kategorija, teoriji o teorijama ... .

akademik S. Mardešić

Tekst je ... pisan jednostavnim i jasnim jezikom i u potpunosti pokriva gradu predviđenu programima za linearnu algebru na raznim studijskim usmjerenjima. Pojedini dijelovi dobro će poslužiti i studentima završnih godina.

Posebnu važnost imaju brojni ilustrativni primjeri i pomno odabrani zadaci, kojima se objašnjava dokazano, upućuje na korisne primjene, ali i produbljuje teorijsku pozadinu.

prof. dr. H. Kraljević

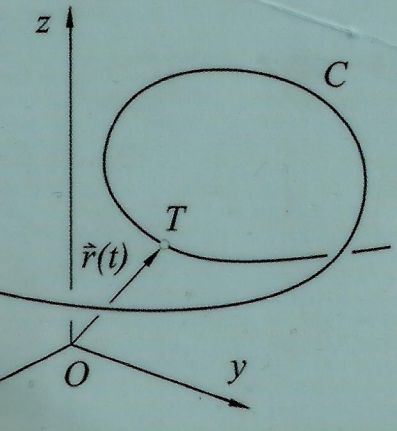
Autor je poznati matematičar i cijenjeni sveučilišni nastavnik, čija se zapažena i uspješna predavačka karijera izvrsno oslikava u kvaliteti ovog udžbenika.

Izvrsno je obavio zadatak, napisavši udžbenik koji je matematički dosljedan, ispravan, čist i strog, ali istodobno vrlo čitljiv, sadržajan, metodički odlično komponiran, ...

Uspješno je riješio stručne i metodičke probleme i dileme, koje postavlja vrlo obuhvatan i zahtjevan program linearne algebre.

Knjiga je napisana na temelju dugogodišnjeg iskustva i iznimnoga predavačkog talenta autora, s dubokim razumijevanjem za predmet poučavanja, ali i one, koje se poučava ... .

prof. dr. M. Polonijo



ISBN 953-212-182-X
9 789532 121827



UDŽBENICI SVEUČILIŠTA U ZAGREBU
MANUALIA UNIVERSITATIS STUDIORUM ZAGRABIENSIS

Krešimir Horvatić

LINEARNA ALGEBRA



1991 MATHEMATICS SUBJECT CLASSIFICATION
15-01

Copyright © 2004., Golden marketing – Tehnička knjiga, Zagreb
Sva prava pridržana

Nakladnik
Golden marketing – Tehnička knjiga
Jurišićeva 10, Zagreb

Za nakladnika
Ana Maletić

Urednik
prof. dr. sc. Boris Pavković

Recenzenti
akademik Sibe Mardešić
prof. dr. sc. Hrvoje Kraljević
prof. dr. sc. Mirko Polonijo

Objavljivanje i uporabu ovog sveučilišnog udžbenika
odobrio je
Senat Sveučilišta u Zagrebu
odlukom broj 02-1616/3-2004
od 15. srpnja 2004.

ISBN 953-212-182-X

Dr. sc. Krešimir Horvatić
redoviti profesor
Prirodno-matematički fakultet – Matematički odjel
Sveučilište u Zagrebu

LINEARNA ALGEBRA

1. (9.) izdanje

Golden marketing – Tehnička knjiga
Zagreb, 2004.

Mojoj unučadi

PREDGOVOR

Linearna algebra jedna je od tradicionalnih matematičkih disciplina, a izvorište joj je u nalaženju rješenja linearnih jednadžbi. Problem rješavanja sustava takvih jednadžbi je izuzetno važan zbog svekolikih primjena u ostalim granama matematike pa i u drugim znanostima, danas posebno u numeričkoj matematici i računarstvu. Za rješavanje tog i drugih srodnih problema razvijene su razne metode (npr. matrične, operatorske itd.), a dobiveni rezultati dopuštaju i algebarsku i geometrijsku interpretaciju. Ne zalazeći daleko u povijest, navest ćemo imena nekoliko značajnih matematičara koji su odigrali ključnu ulogu u oblikovanju linearne algebre u suvremenu matematičku granu. To su, među ostalima, G. Cramer, H. Grassmann, W.R. Hamilton, A. Cayley, J.J. Sylvester, M.E.C. Jordan, L. Kronecker i C. Hermite. O njihovim pojedinačnim prilozima i zaslugama bit će govora na odgovarajućim mjestima u knjizi.

Na studiju matematike, zatim fizike, elektrotehnike pa i drugdje, Linearna algebra važan je uvodni kolegij, na neki način komplementaran Matematičkoj analizi. U ta se dva kolegija obrađuje velik broj pojmova i činjenica, bitnih i korisnih kao temelj za druge kolegije, predviđene planovima i programima studija mnogih, napose egzaktnih znanosti.

Ovaj je udžbenik, u njegovoj današnjoj formi, napisan na temelju dugog, gotovo četrdesetgodišnjeg iskustva autora u predavanju Linearne algebre i njoj srodnih kolegija studentima matematike, studentima fizike te politehničkog odgoja na PMF-u u Zagrebu. A povremeno i drugdje (Osijek, Zadar, ...).

Tijekom godina (koje su dolazile i prolazile), knjiga je doživjela mnoga izdanja, objavljivana je u raznim formama i tehnikama, od raznih izdavača. Njezin je sadržaj neprekidno dotjerivan, prateći suvremena stremljenja u matematici, kao i odgovarajuće modifikacije u nastavnim planovima i programima. Dakako, uvažavane su i uvijek dobrodošle kritičke primjedbe znalaca.

Nekoliko riječi o sadržaju udžbenika. Moglo bi se reći, da je njegovih petnaest poglavlja podijeljeno u tri cjeline.

Prvi je dio (poglavlja 1–6) uvodnog karaktera i u njemu je prikupljen i sistematiziran raznorodni materijal više-manje poznat iz ranijeg školovanja. Osim rudimenata matematičke logike, tu je riječ o skupovima, funkcijama i relacijama, pa zatim o osnovnim algebarskim strukturama (grupa, prsten, tijelo, polje). Konačno, dosta je detaljno obrađena klasična algebra vektora u trodimenzionalnom prostoru, uključujući i elemente analitičke geometrije. Bolje pripremljeni čitatelj mogao bi veliki dio tog dijela udžbenika i izostaviti.

Drugi dio (poglavlja 7–11) obuhvaća standardne naslove koji se susreću u uvodnim tečajevima linearne algebre. Na temelju prethodne motivacije, ovdje se aksiomatski uvodi pojam linearnog prostora (nad bilo kojim poljem), te definira njegova baza i dimenzija. Zatim se govori o linearnim operatorima i fukcionalima, svojstvenim vrijednostima i problemu dijagonalizacije operatora. S tim u vezi je, dakako, obrađena i algebra matrica, zajedno s teorijom determinanata. Taj dio udžbenika završava općom teorijom sustava linearnih jednadžbi.

U trećem, posljednjem dijelu (poglavlja 12–15) preko skalarnog množenja uvodimo na linearnom prostoru dodatnu strukturu, i tako dolazimo do unitarnog prostora. Tu se susrećemo s normom vektora, pa onda i metrikom, linearnom i angularnom, te s raznim pojmovima i rezultatima vezanim uz ortogonalnost vektora. Nadalje, izučavaju se operatori na unitarnom prostoru, napose unitarni, hermitski i normalni operatori. Zatim su, kao generalizacija prethodnih ideja, obrađeni bilinearni i kvadratni funkcionali i pripadne forme, Lagrangeov algoritam te zakon inercije. U posljednjem poglavlju dan je kratki pregled osnovnih ideja teorije kategorija. Tu su, dakako, najvažniji primjeri, uzeti uglavnom iz same knjige, koji ukazuju na širinu i domete te "teorije o teorijama". Na kraju knjige dodan je popis literature te kazalo imena i kazalo pojmova, koji se spominju u tekstu.

Kako smo već rekli, knjiga je podijeljena na poglavlja, a ova dalje na točke. Unutar pojedine točke provodimo jedinstvenu numeraciju izreka, neovisno o tome, radi li se o propoziciji, teoremu, korolaru, napomeni i sl. Na primjer, kad negdje citiramo Tm. 3 iz 7.2., imamo na umu izreku navedenu pod brojem 3 (koja je slučajno teorem) u drugoj točki sedmog poglavlja. Simbolom ■ označen je završetak dokaza neke izreke (ili se ukazuje na kraj izreke, ako je dokaz ispušten).

Spomenimo još, da gotovo svaka točka završava zadacima, koji su pretežno teorijskog karaktera, i često proširuju osnovni tekst. Svakako, za vježbu je uputno koristiti specijalizirane zbirke zadataka iz linearne algebre. Dostupno je nekoliko izuzetno dobrih takvih zbirki, raznih autora i izdavača (Čaklović, Bakić-Milas, Aglić-Elezović...).

Malo o historijatu. U svojoj (pra)iskonskoj formi, ovaj se tekst prvi puta

pojavio još davne 1978. godine. Tada je naime ondašnja studentska organizacija na PMF-u pokrenula inicijativu, da se predavanja iz linearne algebre objave u obliku skripata. Tekst tih predavanja najprije je pažljivo pretipkan na matrice i zatim umnožen (ondašnja tehnika!). Posebne zasluge u raznim fazama tog mukotrpnog posla pripadaju Josipu Pataročiću, Mariji Galeković, Vladimiri Zlatić, te dr. Miroslavu Lovriću. Sljedeća izdanja doživjela su samo neznatne promjene, zbog nemogućnosti izvođenja većih zahvata na matricama.

Kako su se s vremenom skripta počela koristiti u nastavi i na drugim fakultetima u Zagrebu i ostalim sveučilištima u Hrvatskoj, na zahtjev ondašnjeg Ministarstva prosvjete su pored prvotnih recenzija prof. H. Kraljevića i prof. S. Mardešića s PMF-a u Zagrebu, za četvrto izdanje pribavljene i dodatne recenzije profesora L. Krnića (FSB, Zagreb), Ž. Paušea (FGZ, Zagreb), D. Ugrin Šparca (ETF, Zagreb), J. Reša (PF, Rijeka) i A. Vukovića (FESB, Split). Na temelju tih recenzija, tekstu je odlukom Odbora za nastavu i izdavačku djelatnost Sveučilišta u Zagrebu, odobren status sveučilišnog udžbenika. Kao takvog, 1986. godine objavila ga je Sveučilišna naklada Liber, u dva sveska, u novoj formi i formatu, te suvremenijoj opremi.

Ukorak s vremenom, za peto izdanje korištena je računalna tehnika. Cijeli je tekst najprije prenesen s računala na diskete i zatim tiskan, što je knjizi dalo sasvim nov izgled. Sljedeća dva izdanja, tiskana u teškim uvjetima Domovinskog rata, nisu doživjela znatnije promjene.

Zato je osmo izdanje, tiskano 1995. godine, temeljito prerađeno, dopunjeno i dotjerano. To se izdanje pojavljuje u tri sveska, koji se podudaraju s tri cijeline knjige, koja je pred vama. Brigu oko izdavanja udžbenika preuzelo je poduzeće LPC iz Zagreba.

Kako je već ranije spomenuto, tekst udžbenika je od izdanja do izdanja dotjerivan i dopunjavan, uklanjane su greške i uvažavane primjedbe recenzenata, kolega, prijatelja i drugih čitatelja. Tu prije svega imam na umu važne ispravke prof. P. Papića (već nakon prvog izdanja), pa onda velik broj raznih sugestija i korisnih savjeta poteklih redom od profesorā S. Mardešića, R. Mangera, zatim M. Polonija i Z. Šikića, te D. Bakića, koji su pridonijeli, da se tekst na nekoliko važnih mjesta znatno poboljša. Svima njima toplo zahvaljujem. Zahvala ide i dr. Aleksandri Čižmešiji, koja je, uz korekturu teksta, strpljivo i s puno truda sastavila kazalo imena i pojmova. Konačno, mnogo dugujem i prof. Alki Zdjelar-Paunović, koja je s mnogo volje i strpljenja dotjerala ovaj tekst s jezične strane. Kao i Boženi Grdović, za intervencije tehničke prirode i konačnu redakturu, čime je ovaj obimni posao priveden kraju.

Da završim. Kad je poznata zagrebačka izdavačka kuća "Golden marketing" preuzela poduzeće "Tehnička knjiga" (u stečaju), preuzela je, rekao

bih, i tešku obvezu izdavanja, često nekomercijalnih, ali izuzetno važnih publikacija znanstvenog i stručnog karaktera (monografija, sveučilišnih udžbenika, priručnika, ...), posebno iz egzaktnih disciplina i tehnike, bitnih za opći napredak društva i ove naše države. U tu kategoriju, vjerujem, spada i ovaj udžbenik, *Linearna algebra*, koji eto izlazi u novom, devetom izdanju. Uz manje promjene u tekstu, to se izdanje sada tiska kao jedna, jedinstvena knjiga, i to u nadasve lijepoj i bogatoj opremi. Istaknimo da je za to posebno zaslužan g. Franjo Maletić, dipl. iur., direktor i glavni urednik Golden marketing-Tehničke knjige, izdavača knjige. Tehničku stranu tog zahtjevnog posla vrlo je stručno i savjesno obavio ing. Željko Prodanović, izvršni urednik.

Na kraju, jedna molba. Volio bih da čitatelji, kao i dosada, skrenu pažnju meni osobno ili pak izdavaču, na uočene greške, bile one stručne ili tehničke naravi. Dobrodošla je i svaka sugestija za poboljšanje teksta. Sve će one biti pažljivo razmotrene, te će se o njima voditi računa u sljedećem izdanju knjige, do kojeg će, vjerujem, jednom doći.

Krešimir Horvatić

Zagreb, veljača 2004.

SADRŽAJ

PREDGOVOR vii

1 **SKUPOVI I PRESLIKAVANJA**
1.1. O simbolima i terminima 1
1.2. Skupovi 5
1.3. Preslikavanja 11
1.4. Kardinalni broj skupa 19
1.5. Kartezijev produkt skupova 22
1.6. Relacije 28

2 **GRUPE**
2.1. Binarna operacija. Grupoid 39
2.2. Asocijativnost. Polugrupa 43
2.3. Neutralni element. Monoid 45
2.4. Invertibilni elementi 49
2.5. Grupa 52
2.6. Alternativne definicije grupe 56
2.7. Podgrupa 59
2.8. Primjeri grupa 65
2.9. Grupe permutacija. Simetrična grupa 75

3 **PRESLIKAVANJA GRUPA. KVOCIJENT I PRODUKT GRUPA**
3.1. Homomorfizam grupa 85
3.2. Izomorfizam grupa 90
3.3. Primjeri izomorfizama 93
3.4. Cayleyjev teorem 96
3.5. Normalne podgrupe 99
3.6. Susjedne klase. Lagrangeov teorem 103
3.7. Kvocijentna grupa 106
3.8. Teorem o izomorfizmu 110
3.9. Direktni produkt grupa 114

4 PRSTENOVI I TIJELA

4.1. Definicija prstena 119
4.2. Djelitelji nule. Integralna domena 125
4.3. Potprstenovi i ideali 126
4.4. Homomorfizam prstenova 130
4.5. Karakteristika 135
4.6. Tijelo i polje 137

5 KLASIČNA ALGEBRA VEKTORA

5.1. Uvodne napomene 145
5.2. Orijentirane dužine 146
5.3. Vektori 148
5.4. Modul, smjer i orijentacija vektora 150
5.5. Zbrajanje vektora 153
5.6. Množenje vektora skalarom 156
5.7. Kolinearni i komplanarni vektori 161
5.8. Baza prostora V^3. Koordinatizacija 166
5.9. Skalarni produkt 169
5.10. Ortonormirana baza. Koordinatni prikaz skalarnog produkta . 174
5.11. Vektorski produkt 177
5.12. Koordinatni prikaz vektorskog produkta 184
5.13. Mješoviti produkt 187
5.14. Operatori na V^3 193

6 ELEMENTI ANALITIČKE GEOMETRIJE U E^3

6.1. Kartezijev koordinatni sustav 207
6.2. Udaljenost točke od ravnine 211
6.3. Razni oblici jednadžbe ravnine 212
6.4. Kut dviju ravnina 218
6.5. Analitička predočenja pravca 220
6.6. Kut dvaju pravaca. Kut pravca i ravnine 223
6.7. Udaljenost točke od pravca 225
6.8. Zajednička normala i najkraća udaljenost dvaju pravaca . . . 227
6.9. Analitičko predočenje ploha. Plohe 2. reda 231
6.10. Analitičko predočenje krivulja 238
6.11. Neki drugi koordinatni sustavi u prostoru 240

7 LINEARNI PROSTOR

7.1. Definicija i osnovna svojstva 247
7.2. Primjeri linearnih prostora 251
7.3. Linearna zavisnost i nezavisnost 255
7.4. Skup izvodnica linearnog prostora. Baza i dimenzija 260
7.5. Konačnodimenzionalni prostori 262
7.6. Potprostori 268
7.7. Presjek i suma potprostora 273
7.8. Kvocijentni prostor. Direktni produkt prostora 282

8 LINEARNI OPERATORI

8.1. Definicija i osnovna svojstva 289
8.2. Primjeri linearnih operatora 292
8.3. Egzistencija i način zadavanja linearnih operatora 297
8.4. Izomorfizam linearnih prostora 299
8.5. Rang i defekt 304
8.6. Prostor $\mathrm{Hom}(U, V)$ 310
8.7. Linearni funkcionali. Dualni prostor 319

9 MATRICE I DETERMINANTE

9.1. Uvodne napomene 331
9.2. Definicija matrice 332
9.3. Linearni prostor M_{mn} 336
9.4. Množenje matrica. Algebra M_n 340
9.5. Regularne matrice. Opća linearna grupa 347
9.6. Rang matrice 354
9.7. Pojam determinante. Osnovna svojstva 363
9.8. Binet-Cauchyjev teorem 370
9.9. Laplaceov razvoj determinante 375
9.10. Još o rangu i inverzu matrice 381

10 INVARIJANTE LINEARNOG OPERATORA

10.1. Koordinatizacija 385
10.2. Transformacija koordinata 387
10.3. Matrični zapis linearnog operatora 391
10.4. Izomorfizam prostora $\mathrm{Hom}\,(U, V)$ i M_{mn} 393
10.5. Odnos matričnih zapisa istog operatora 397
10.6. Karakteristični polinom. Hamilton-Cayleyjev teorem 398

10.7. Minimalni polinom 404
10.8. Invarijantni potprostori 412
10.9. Svojstvene vrijednosti linearnog operatora 417
10.10. Dijagonalizacija. Jordanova forma matrice 425

11 SUSTAVI LINEARNIH JEDNADŽBI

11.1. Notacija i formulacija problema 435
11.2. Geometrijska interpretacija 438
11.3. Egzistencija rješenja 441
11.4. Cramerov sustav 443
11.5. Homogeni sustav 447
11.6. Nehomogeni sustav 449
11.7. Gauss–Jordanova metoda eliminacije 452
11.8. Metoda redukcije na Cramerov sustav 459
11.9. Matrične jednadžbe 462

12 UNITARNI PROSTOR

12.1. Uvodne napomene 465
12.2. Definicija i osnovna svojstva 467
12.3. Primjeri unitarnih prostora 470
12.4. Nejednakost Schwarz-Cauchy-Bunjakovskog 472
12.5. Norma vektora. Kut 474
12.6. Metrika 479
12.7. Gramova matrica 482
12.8. Ortonormirani skupovi vektora 486
12.9. Gram-Schmidtov postupak ortogonalizacije 492
12.10. Ortogonalni komplement. Projektor 497

13 OPERATORI NA UNITARNOM PROSTORU

13.1. Unitarni operator 505
13.2. Karakterizacije unitarnog operatora 512
13.3. Matrica unitarnog operatora. Unitarna grupa 515
13.4. Adjungirani operator 525
13.5. Hermitski i antihermitski operatori 530
13.6. Normalni operatori 539
13.7. Dekompozicije linearnog operatora 548
13.8. Funkcionali na unitarnom prostoru 564

14 BILINEARNI I KVADRATNI FUNKCIONALI. FORME
14.1. Bilinearni funkcionali 571
14.2. Kvadratni funkcionali 580
14.3. Kvadratne forme. Lagrangeov algoritam 583
14.4. Zakon inercije. Definitnost forme 592
14.5. Hermitski funkcionali i pripadne forme 601
14.6. Pseudounitarni prostori 613
14.7. Geometrija linearnog prostora 622

15 KATEGORIJE I FUNKTORI
15.1. Definicija kategorije 633
15.2. Primjeri kategorija 641
15.3. Funktori 644
15.4. Prirodne transformacije 652

LITERATURA 663

KAZALO IMENA 669

KAZALO POJMOVA 673

BILJEŠKA O AUTORU 695

1

SKUPOVI I PRESLIKAVANJA

Svrha je ovog poglavlja uvesti uobičajenu terminologiju i notaciju koja će se dosljedno rabiti u ovom udžbeniku. Osim kratkog opisa nekih logičkih simbola, u poglavlju se daje pregled pojmova i činjenica elementarne teorije skupova. Pretpostavljajući da čitalac tu građu u većoj ili manjoj mjeri već poznaje, većina standardnih dokaza je ispuštena.

1.1. O simbolima i terminima

Nekoliko uvodnih riječi o znakovima, nazivima i nekim pojmovima, uobičajenim u matematici, kojima ćemo se služiti kako bismo tekst učinili jasnijim, preglednijim i sažetijim. Strogi pristup tom gradivu je predmet posebnih matematičkih disciplina, kao što su matematička logika, osnove matematike i sl. Najprije nešto o izjavama u matematici i pripadnim simbolima. Kao što znamo, **izjava** je smislena rečenica koja može biti samo istinita ili lažna. Na primjer upitna rečenica ne može biti izjava. Pojedine izjave možemo povezati veznicima; tako dolazimo do **složenih izjava**.

Konjunkcija izjava A i B je složena izjava koju označujemo s

$$A \wedge B\,,$$

a nastaje povezivanjem izjava A i B veznikom i. Tu izjavu zato čitamo "A *i* B" ili također "A *et* B". Istinita je jedino u slučaju kad su i izjava A i izjava B istinite; inače je lažna. Za konjunkciju je uobičajena oznaka i $A\&B$.

Disjunkcija izjava A i B je složena izjava, koju označujemo s

$$A \vee B\,,$$

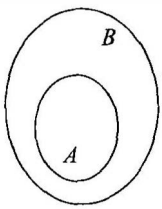
a dobivamo je povezivanjem izjava A i B veznikom *ili*. Čitamo "A *ili* B" odnosno "A *vel* B". Ta je izjava istinita ako je istinita izjava A ili je is-

tinita izjava B ili su istinite obje te izjave (inkluzivna disjunkcija!). Drugim riječima, $A \vee B$ je lažna jedino onda kad su obje izjave, A i B, lažne.

Implikacija je složena izjava, označena kao

$$A \Rightarrow B\,,$$

koju čitamo "*A povlači B*" ili "*A implicira B*". Ta je izjava istinita uvijek kad je B istinita izjava ili kad su obje izjave A i B lažne. Lažna je dakle jedino u slučaju kad je izjava A istinita, a izjava B lažna. Posebno, ako su izjave A i $A \Rightarrow B$ istinite, zaključujemo da je i izjava B istinita; to će biti naša standardna primjena implikacije. Kažemo (posebno u tom slučaju),



da je A **dovoljan uvjet** za B, odnosno da je B **nuždan uvjet** za A.

Ekvivalencija izjava A i B je složena izjava, koju zapisujemo

$$A \Leftrightarrow B\,,$$

i čitamo "*A je jednakovrijedna kao B*" ili češće "*A je ekvivalentna s B*". Ta je izjava istinita kad su obje polazne izjave A i B istinite, ili su obje lažne; inače je lažna. Iz prethodno rečenog, možemo "izračunati" da će to biti jedino u slučaju kad

$$A \Rightarrow B \quad \wedge \quad B \Rightarrow A\,.$$

Zato se i govori "*A je nuždan i dovoljan uvjet za B*", odnosno "*A je ako i samo ako je B*" ili "*A je onda i samo onda, kada je B*". To su termini kojima ćemo u pojedinim konkretnim slučajevima opisivati ekvivalenciju.

Ilustrirajmo navedene pojmove s nekoliko primjera. Promatrajmo izjave:
A: 3 *je mjera za* 9;
B: 9 *je višekratnik od* 3;
C: 3 *je paran broj* .
Onda su konjunkcije $A \wedge C$ i $B \wedge C$ lažne, dok je $A \wedge B$, dakako, istinita. U drugu ruku, sve su tri disjunkcije $A \vee C$, $B \vee C$ i $A \vee B$ istinite. Nadalje, istinita je implikacija $B \Rightarrow A$, ali, prema našoj definiciji, i $C \Rightarrow A$, dok je $A \Rightarrow C$ lažna. Konačno, kako je uz $B \Rightarrow A$ istinita i obrnuta implikacija $A \Rightarrow B$, imamo zaključak da je $A \Leftrightarrow B$, tj. da su izjave A i B ekvivalentne.

Promotrimo sada rečenicu "*x je mjera za y*". To očito nije izjava jer se ne može utvrditi niti da je istinita, niti da je lažna. Takvu rečenicu nazivamo **izjavna funkcija**, u ovom slučaju u dvije **varijable**; pišemo

$$I = I(x, y) \ .$$

Specifikacijom varijabli izjavna funkcija postaje izjava. U našem je primjeru $I(3, 9)$ istinita izjava, a $I(9, 3)$ lažna. Općenito, imat ćemo izjavne funkcije i s više varijabli. U drugu ruku, od interesa su i funkcije sa samo jednom varijablom; njima se opisuje neko **svojstvo** promatranih objekata. Na primjer, izjavna funkcija

$$I = I(x),$$

opisana rečenicom "*x je paran*", utvrđuje određeno svojstvo prirodnih brojeva.

Posebno je važan slučaj kad izjavna funkcija prelazi u izjavu pomoću neodređenih zamjenica **svaki** odnosno **neki**, tzv. kvantifikatora.

Univerzalni kvantifikator, u oznaci $\forall$, kazuje da je izjavna funkcija istinita za **sve** vrijednosti neke od varijabli. Tako u našem primjeru pišemo

$$(\forall y) \qquad I(1, y),$$

i čitamo "*svaki broj y je takav, da je* 1 *mjera od y* ". Nasuprot tome, **egzistencijalni kvantifikator**, u oznaci $\exists$, tvrdi da je izjavna funkcija istinita za **neki** izbor varijable. Na primjer pišemo

$$(\exists x) \qquad I(x, 9),$$

i čitamo "*postoji (bar jedan) broj x takav da je x mjera za* 9". To će, dakako, biti brojevi $x = 1, 3$ i 9. Katkada je taj izbor jedinstven; tada egzistencijalni kvantifikator označujemo s $\exists!$ ili $\exists_1$. U našem primjeru

$$(\exists!\ x) \qquad I(x, 1),$$

što znači i čita se "*postoji točno jedan broj x takav da je x mjera za* 1", i to je broj $x = 1$. Izjavne funkcije možemo prevesti u izjave i kombiniranjem kvantifikatora. Imamo na primjer

$$(\forall\, x)(\exists\, y) \qquad I(x, y)\ ,$$

što čitamo "*za svaki x postoji y takav da je x mjera za y*".

U pravilu su vrijednosti varijabli u izjavnoj funkciji (pa onda i kod kvantifikatora) ograničene na neki određeni skup (vidi točku 1.2.). U našim primjerima to je bio skup prirodnih brojeva.

Na kraju, nešto o simbolu $=$, koji čitamo "*biti jednak*". Govoreći općenito, s $a = b$, odnosno $a \neq b$, označivat ćemo da a i b predstavljaju jedan te isti objekt, odnosno da se radi o različitim objektima. Međutim, u nekim teorijama simbol $=$ može imati i neko drugo, posebno definirano značenje.

Još nekoliko napomena. Tradicionalno, počevši još od Euklida i geometrije, većina se matematičkih disciplina, u višoj fazi izgradnje, nastoji strogo utemeljiti. To znači da se, prihvaćajući neke jednostavne pojmove kao poznate, svi ostali pojmovi opisuju pomoću njih, tj. definiraju. I nadalje, polazeći od određenog broja činjenica, koje se prihvaćaju kao istinite, sve se ostale tvrdnje izvode iz njih, tj. dokazuju. To je **aksiomatski pristup** nekoj matematičkoj disciplini.

Suvremene matematičke teorije, od kojih ćemo neke upoznati i u ovoj knjizi, slijede više-manje upravo tu shemu. Nabrojit ćemo nekoliko termina koji su u vezi s takvim pristupom, a s kojima ćemo se u daljnjem tekstu neprekidno susretati.

Osnovni pojam neke teorije (u pravilu) jednostavan je pojam, koji se smatra poznatim pa se ne opisuje pomoću drugih pojmova te teorije.

Definirani pojam neke teorije je pojam koji se u toj teoriji opisuje (definira!) pomoću osnovnih pojmova i prethodno definiranih pojmova.

Aksiom za neku teoriju je polazna, obično vrlo jednostavna tvrdnja u nekoj teoriji koja se bez dokaza prihvaća kao istinita.

Teorem u okviru neke teorije je izjava, tvrdnja, čija se istinitost dokazuje, tj. izvodi logičkim zaključivanjem iz aksioma i već dokazanih teorema te teorije. Neki važni (i obično teški) teoremi imaju i ime, često po matematičaru koji ih je prvi dokazao (npr. teorem o dimenziji, Cayleyjev teorem, Binet–Cauchyjev teorem). U drugu ruku, teoreme za koje postoje jednostavni i kratki dokazi obično nazivamo **propozicije**. Teorem koji sam za sebe nije od posebnog interesa nego služi kao etapa u dokazu nekog važnijeg i složenijeg teorema, naziva se **lema**. Konačno, **korolar** je teorem koji je neposredna i jednostavna posljedica drugog, prethodno dokazanog teorema, i njegov je dokaz toliko očigledan, da ga obično ispuštamo.

ZADACI

1. **Negacija** izjave A je izjava koja se obično označuje s $\neg A$ i čita "*nije* A" ili "*non* A", a istinita je ako i samo ako je izjava A lažna. Što možeš reći o složenoj izjavi $A \wedge (\neg A)$ i složenoj izjavi $A \vee (\neg A)$? Dokaži da su složene izjave

$$\neg(A \wedge B) \quad i \quad (\neg A) \vee (\neg B)$$

ekvivalentne, za bilo koje izjave A i B.

2. Kažemo da je složena izjava **tautologija** ako je istinita bez obzira na istinitost polaznih izjava. Pokaži da su izjave $(A \vee B) \Leftrightarrow (B \vee A)$ i $(A \wedge B) \Rightarrow B$ tautologije, dok $A \vee B$ to nije.

3. Neka je izjavi A pridružen broj 0 ako je ta izjava lažna, odnosno broj 1 ako je istinita. Onda se istinitost, odnosno lažnost, složene izjave može prikazati u zavisnosti od vrijednosti polaznih izjava pomoću tzv. **tablice istinitosti**. Na primjer, za izjavu $A \vee B$ imamo tablicu

A	0	0	1	1
B	0	1	0	1
A ∨ B	0	1	1	1

.

Odredi tablice istinitosti za $A \wedge B$, $A \Rightarrow B$ i $A \Leftrightarrow B$. Nadalje, prikaži tablicama složene izjave $\neg(A \Rightarrow B)$ i $A \wedge (\neg B)$. Što zapažaš?

4. Neka je izjava $A \Rightarrow B$ istinita, a $B \Rightarrow A$ lažna. Tada često kažemo da je A **samo** dovoljan uvjet za B, odnosno da je B **samo** nuždan uvjet za A. Ilustriraj to s nekoliko primjera iz svakidašnjeg života i matematike.

5. Implikaciju "*ako je broj pozitivan, onda je i njegov kvadrat pozitivan*", izrazi pomoću termina nuždan i dovoljan.

6. Kakav god bio prirodni broj x, uvijek se može naći prirodni broj y sa svojstvom da je razlika $x - y$ mjera za bilo koji broj z. Zapiši tu nezgrapnu rečenicu kratko, pomoću kvantifikatora. [Uputa: $(\forall x)\ (\exists y)\ (\forall z)\ (x - y \mid z)$, gdje smo s $(x - y \mid z)$, kako je uobičajeno, označili da $x - y$ dijeli z.]

1.2. Skupovi

Intuitivno je jasno što se podrazumijeva pod pojmom **skup**. To je svaka kolekcija objekata, bilo nabrojenih pojedinačno, bilo karakteriziranih nekim zajedničkim svojstvom. Dakako, to nije definicija skupa jer je kolekcija samo sinonim za skup. Mi ćemo prigodno upotrebljavati i neke druge nazive za skup, kao što su **množina**, **familija** itd. Daljnja analiza pokazuje kako je pojam skupa toliko jednostavan da ga i nije moguće definirati, tj. opisati uz pomoć još jednostavnijih pojmova. Prema tome, skup se smatra osnovnim, nedifiniranim pojmom u matematici.

Govorimo npr. o skupu svih građana jednoga grada, o skupu svih slova nekog alfabeta, o skupu svih točaka na pravcu ili u ravnini, o skupu svih koncentričnih kugala u prostoru i onda, naravno, o raznim skupovima brojeva:

o skupu prirodnih brojeva, cijelih, racionalnih itd. Za te skupove imamo standardne oznake:

$\mathbb{N}$ = skup prirodnih brojeva,
$\mathbb{Z}$ = skup cijelih brojeva,
$\mathbb{Q}$ = skup racionalnih brojeva,
$\mathbb{R}$ = skup realnih brojeva,
$\mathbb{C}$ = skup kompleksnih brojeva.

Tu ćemo notaciju upotrebljavati dosljedno. Uopće, skupove ćemo označivati velikim tiskanim slovima, kao $A, B, C, \ldots, X, Y$.

Objekte koji tvore dani skup nazivamo **elementima** toga skupa ili njegovim **članovima** ili, također, **točkama** skupa, i to bez obzira na to radi li se zaista o točkama ili o nekim drugim, možda i apstraktnim objektima. Shematski, skup obično prikazujemo kao

gdje točke predstavljaju elemente skupa (tzv. Vennov dijagram). Činjenicu da neki objekt x pripada skupu X zapisujemo

$$x \in X$$

i čitamo "*x je element skupa X*". U drugu ruku, simbol

$$x \notin X$$

označivat će, da objekt x ne pripada skupu X. Na primjer,

$$7 \in \mathbb{N}, \qquad 0 \notin \mathbb{N}, \qquad \sqrt{2} \in \mathbb{R}, \qquad \sqrt{2} \notin \mathbb{Q}.$$

Zadati skup znači propisati njegove elemente, tj. skup X je zadan ako za svaki objekt možemo reći pripada li skupu X ili mu ne pripada. Ako skup ne sadrži previše elemenata, možemo ga zapisati eksplicitno, kao npr.

$$\begin{aligned} A &= \{-1, 1\}, \\ B &= \{a, b, c, d\}, \\ C &= \{x\}. \end{aligned}$$

Posljednji se skup sastoji iz jednog jedinog elementa x. S logičkog bi stajališta trebalo razlikovati skup $\{x\}$ od njegova elementa $x \in \{x\}$, iako ćemo ih često (nekorektno) poistovjećivati. Iz praktičnih razloga uvodimo i pojam **praznog skupa**, tj. skupa bez ijednog elementa, za koji ćemo upotrebljavati simbol $\emptyset$.

Ako skup ima mnogo elemenata, praktično je nemoguće popisati sve elemente, kako je učinjeno u prethodnim primjerima. Ako elemenata ima beskonačno mnogo, to nije moguće ni teoretski. Često je u takvom slučaju pogodan zapis skupa pomoću tzv. **karakterističnog svojstva**. Neka je p izvjesno svojstvo, a $p(x)$ neka označava, da to svojstvo ima objekt x; onda je s

$$X = \{x \mid p(x)\}$$

opisan skup, čiji svi elementi, i samo oni, posjeduju svojstvo p. Na primjer,

$$\begin{aligned} A &= \{x \mid x^2 + 1 = 0\} = \{-i, i\}\,, \\ B &= \{x \mid x = \frac{m}{n},\ m, n \in \mathbb{Z},\ n \neq 0\} = \mathbb{Q}\,, \\ C &= \{x \mid x = 2n,\ n \in \mathbb{Z}\} = \{\ldots, -2, 0, 2, 4, \ldots\} = 2\mathbb{Z}\,, \\ D &= \{x \mid x = n^2,\ n \in \mathbb{Z}\} = \{0, 1, 4, 9, \ldots\}\,. \end{aligned}$$

Neka su A i B skupovi sa svojstvom da je svaki element skupa A ujedno element skupa B. U tom slučaju kažemo da je A **podskup** od B ili da je A **sadržan** u B, odnosno da je B **nadskup** skupa A, ili da B **sadrži** A, i pišemo

$$A \subset B\,.$$

Pritom relaciju $\subset$ nazivamo **inkluzija**. Naravno,

$$A \not\subset B$$

označivat će da A nije podskup od B. Na primjer, imamo ovaj niz inkluzija

$$\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}\,.$$

Podskup se može zadati i dodatnim svojstvom, koje moraju zadovoljavati elementi skupa. Na primjer,

$$I = \{x \in \mathbb{R} \mid 0 \leq x \leq 1\} = [0, 1] \subset \mathbb{R}\,.$$

Očito je da za svaki skup A vrijedi

$$\emptyset \subset A \quad \text{i} \quad A \subset A\,.$$

Za skupove A i B kažemo da su **jednaki** i pišemo

$$A = B\,,$$

ako se oni sastoje iz istih elemenata, tj. ako vrijedi

$$A \subset B \quad \text{i} \quad B \subset A\,.$$

Ako to nije slučaj, pišemo $A \neq B$. Ako vrijedi

$$A \subset B \quad \text{i} \quad A \neq B\,,$$

kažemo da je A **pravi** podskup od B.

Skup svih podskupova nekog skupa X označavamo s $\mathcal{P}(X)$ i nazivamo **partitivni skup** skupa X. Na primjer, za $X = \{a, b\}$ je

$$\mathcal{P}(X) = \{\{a, b\}, \{a\}, \{b\}, \emptyset\}.$$

Za partitivni skup od X još je uobičajena oznaka 2^X, iz razloga koji će biti objašnjen kasnije (vidi Zad. 9. u 1.5.).

Sada ćemo definirati niz operacija sa skupovima koje omogućuju da se od zadanih skupova formiraju novi skupovi.

Pod **unijom** skupova A i B razumijevamo novi skup $A \cup B$, čiji elementi imaju svojstvo da pripadaju bar jednom od skupova A i B. Prema tome,

$$A \cup B = \{x \mid x \in A \vee x \in B\}\,.$$

Primijetimo da je uvijek

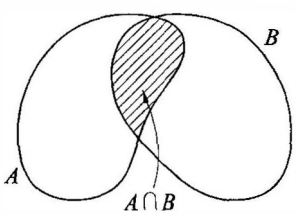
$$A \cup \emptyset = A \quad \text{i} \quad A \cup A = A$$

i, uopće, $B \subset A$ povlači

$$A \cup B = A\,.$$

Presjek skupova A i B definiramo kao skup $A \cap B$, čiji elementi imaju svojstvo da pripadaju i skupu A i skupu B, tj.

$$A \cap B = \{x \mid x \in A \wedge x \in B\}\,.$$



Očito je

$$A \cap \emptyset = \emptyset \quad \text{i} \quad A \cap A = A$$

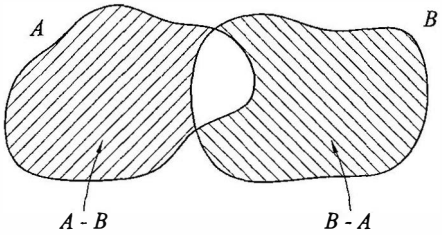
i, općenito, iz $B \subset A$ slijedi

$$A \cap B = B\,.$$

Ako je $A \cap B = \emptyset$, kažemo da su A i B **disjunktni** skupovi.

Diferencija ili **razlika** skupova A i B je skup $A - B$, koji se sastoji iz svih onih elemenata skupa A koji ne pripadaju skupu B; drugim riječima,

$$A - B = \{x \mid x \in A \wedge x \notin B\}\,.$$



Lako se provjeri (koristeći Tm. 1 koji slijedi), da uvijek vrijedi

$$(A - B) \cup (A \cap B) \cup (B - A) = A \cup B \, .$$

Ako je $A \subset X$, onda diferenciju $X - A$ nazivamo **komplement** od A u skupu X i pišemo

$$C_X A = X - A \, ,$$

ili često samo CA, ako je jasno u odnosu na koji skup se uzima komplement. Očito vrijedi

$$A \cup CA = X, \qquad A \cap CA = \emptyset$$

i nadalje je

$$CX = \emptyset, \qquad C\emptyset = X, \qquad C(CA) = A.$$

Sljedećim teoremom su obuhvaćena osnovna svojstva definiranih operacija.

TEOREM 1

Ako su A, B, C i X bilo koji skupovi, onda vrijede

(1) *zakoni asocijacije, tj.*

$$(A \cup B) \cup C = A \cup (B \cup C) \, ,$$
$$(A \cap B) \cap C = A \cap (B \cap C) \, ;$$

(2) *zakoni komutacije, tj.*

$$A \cup B = B \cup A \, ,$$
$$A \cap B = B \cap A \, ;$$

(3) *zakoni distribucije, tj.*

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C) \, ,$$
$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C) \, ;$$

(4) *De Morganove formule, tj.*

$$X - (A \cup B) = (X - A) \cap (X - B) \, ,$$
$$X - (A \cap B) = (X - A) \cup (X - B) \, .$$

Dokaz

Jednostavan, slijedi neposredno iz definicija operacija. Dokažimo radi ilustracije prvu od formula (4). Kako dokazujemo jednakost dvaju skupova, prema definiciji treba provjeriti obje inkluzije. Najprije dokazujemo inkluziju $X-(A\cup B)\subset(X-A)\cap(X-B)$. Neka je $x\in X-(A\cup B)$. To znači da je $x\in X$ i $x\notin A\cup B$. Prema tome, $x\notin A$ i $x\notin B$, dakle je $x\in X-A$ i $x\in X-B$, što znači da je $x\in(X-A)\cap(X-B)$. Ostaje pokazati inkluziju $(X-A)\cap(X-B)\subset X-(A\cup B)$. Ako je $x\in(X-A)\cap(X-B)$, onda je $x\in X-A$ i $x\in X-B$. Prema tome, $x\notin A$ i $x\notin B$, dakle $x\notin A\cup B$. Odatle slijedi da je $x\in X-(A\cup B)$ i tvrdnja je dokazana. ■

ZADACI

1. U kakvom su odnosu skupovi $\emptyset$, $\{\emptyset\}$ i $\{\{\emptyset\}\}$? Je li $\emptyset=\{\emptyset\}$ i $\emptyset\in\{\{\emptyset\}\}$?

2. Pokaži da za bilo koje skupove vrijedi

$$A\cap B\subset A\subset A\cup B.$$

3. Uvjeri se da je uvijek istina

   (a) $A\subset B$ i $B\subset C$ povlači $A\subset C$;

   (b) $A\subset C$ i $B\subset C$ povlači $A\cup B\subset C$;

   (c) $C\subset A$ i $C\subset B$ povlači $C\subset A\cap B$.

4. Dokaži da podskupovi danog skupa X imaju i ova svojstva:

   (a) $C(A-B)=CA\cup B$;

   (b) $A\subset B$ povlači $CB\subset CA$.

5. Dokaži da za bilo koje skupove A,B,C vrijede sljedeće skupovne jednakosti:

   (a) $A-(A-B)=A\cap B$;

   (b) $A\cap(B-C)=(A\cap B)-(A\cap C)$;

   (c) $(A-C)\cup(B-C)=(A\cup B)-C$.

6. Poopći pojam unije i presjeka skupova za bilo koji broj skupova. Uvjeri se da i u toj situaciji vrijede zakoni iz Tm. 1.

7. Poopći De Morganove formule.

1.3. Preslikavanja

Neka su X i Y neprazni skupovi, a f neka je zakon koji svakom elementu skupa X pridružuje (jedan jedini) element skupa Y. Onda uređenu trojku

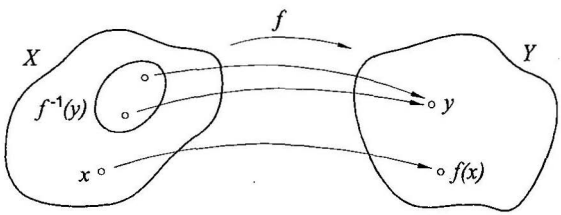
$$(X, Y, f)$$

nazivamo **preslikavanje** skupa X u skup Y ili **funkcija** sa skupa X u skup Y, i obično pišemo

$$f : X \to Y .$$

Skup X nazivamo **područje definicije** ili **domena**, skup Y **područje vrijednosti** ili **kodomena**, a f **zakon** danog preslikavanja. Kad je iz konteksta jasno što su domena i kodomena preslikavanja, često poistovjećujemo preslikavanje s njegovim zakonom, i govorimo jednostavno o funkciji f.

Neka je s $f(x) \in Y$ označen onaj element skupa Y koji je prema zakonu f pridružen elementu $x \in X$. Kažemo da je $f(x)$ **slika od** x u odnosu na preslikavanje f. Kaže se još da je $f(x)$ **vrijednost funkcije** f za vrijednost **varijable** (argumenta) x, ili u "*točki*" $x \in X$.



U drugu ruku, neka je $y \in Y$ bilo koji element, a

$$f^{-1}(y) = \{x \in X \mid f(x) = y\} \subset X$$

neka je skup svih elemenata iz X, čija je slika dani element y. Onda kažemo da je $f^{-1}(y)$ **praslika od** y, u odnosu na preslikavanje f. Primijetimo da praslika nekog elementa iz Y može biti i prazan skup.

Ako su $A \subset X$, odnosno $B \subset Y$ dani podskupovi, onda skupove

$$f(A) = \{f(x) \in Y \mid x \in A\} \subset Y$$

i

$$f^{-1}(B) = \{x \in X \mid f(x) \in B\} \subset X$$

nazivamo **slikom podskupa** A, odnosno **praslikom podskupa** B u odnosu na preslikavanje f. Praslika od B je očito unija praslika elemenata iz B. Primijetimo da je uvijek

$$f^{-1}(Y) = X .$$

dok je, općenito,

$$f(X) \subset Y ,$$

i taj skup nazivamo **slikom domene** X s obzirom na preslikavanje f, i označavamo katkada sa $S(f)$.

PRIMJERI

1. Neka je $A \subset X$ podskup od X, a $i : A \to X$ preslikavanje dano zakonom $i(x) = x$, za svaki x iz A. Onda kažemo da je funkcija i **inkluzija** od A u X. Specijalno, ako je $A = X$, inkluziju i nazivamo **identiteta** na X (i označujemo obično s e).

2. Neka je $a \in Y$ bilo koji element, a $f_a : X \to Y$ preslikavanje definirano s $f_a(x) = a$, za svaki $x \in X$. Onda f_a nazivamo konstantnim preslikavanjem ili **konstantom** (određenom s $a \in Y$).

3. Neka je $f : X \to Y$ preslikavanje čija je kodomena Y skup realnih brojeva ili neki njegov podskup. Onda kažemo da je f **realna funkcija na skupu** X. Ako je npr. X skup svih kružnica u ravnini, a $f : X \to \mathbb{R}$ preslikavanje koje svakoj kružnici pridružuje njezin polumjer, onda je f jedna realna funkcija na X.

4. Preslikavanje $f : X \to Y$ čije su i domena i kodomena skup $\mathbb{R}$ ili njegovi podskupovi, zove se **realna funkcija realne varijable**. Takve su npr. funkcija $f : \mathbb{R} \to \mathbb{R}$ dana zakonom $f(x) = 2x$, odnosno funkcija $g : \mathbb{R} \to \mathbb{R}$ definirana s $g(x) = x^2$.

5. Neka je $f : \mathbb{N} \to X$ preslikavanje skupa prirodnih brojeva u skup X. Takvo se preslikavanje zove **niz u skupu** X. Ako za svaki $k \in \mathbb{N}$ označimo sliku $f(k) = x_k$, onda niz možemo pisati i u tradicionalnoj formi

$$f = (x_1, x_2, \ldots, x_k, \ldots) ,$$

popisujući redom vrijednosti funkcije f. Za element $x_k \in X$ kažemo da je k-ti član danog niza.

Sljedeće propozicije govore o ponašanju danog preslikavanja prema podskupovima domene, odnosno kodomene.

PROPOZICIJA 1

Neka je $f : X \to Y$ dano preslikavanje, a $A, B \subset X$ bilo koji podskupovi domene. Onda vrijedi

(1) $f(A \cup B) = f(A) \cup f(B)$;

(2) $f(A \cap B) \subset f(A) \cap f(B)$. ■

Tvrdnje je lako dokazati i generalizirati na bilo koji broj podskupova od X. Primijetimo da u (2) neće općenito vrijediti znak jednakosti. Neka je npr. $X = \{a, b\}$, $A = \{a\}$, $B = \{b\}$, $Y = \{y\}$, a $f : X \to Y$ jedina moguća, konstantna funkcija. Očito je $f(\emptyset) = \emptyset$, dakle $f(A \cap B) = \emptyset$, a u drugu ruku je $f(A) \cap f(B) = Y$, što pokazuje da u tom slučaju

$$f(A) \cap f(B) \not\subset f(A \cap B).$$

Tako smo **protuprimjerom** pokazali da u (2) općenito ne može stajati znak jednakosti.

PROPOZICIJA 2

Neka je $f : X \to Y$ dano preslikavanje, a $C, D \subset Y$ bilo koji podskupovi. Onda vrijedi

(1) $f^{-1}(C \cup D) = f^{-1}(C) \cup f^{-1}(D)$;

(2) $f^{-1}(C \cap D) = f^{-1}(C) \cap f^{-1}(D)$;

(3) $f^{-1}(A - B) = f^{-1}(A) - f^{-1}(B)$. ■

Tvrdnje (1) i (2) se lako generaliziraju na bilo koji broj podskupova od Y. Uočimo da se, s obzirom na osnovne operacije sa skupovima, praslike bolje ponašaju od slika. Na primjer iz $C \cap D = \emptyset$, prema (2), slijedi da su i praslike tih skupova disjunktne, što ne mora biti točno za slike.

Neka su sada $f : X \to Y$ i $g : Y \to Z$ dva preslikavanja sa svojstvom da se kodomena prvog preslikavanja podudara s domenom drugog. Onda je njima jednoznačno određeno preslikavanje

$$h : X \to Z$$

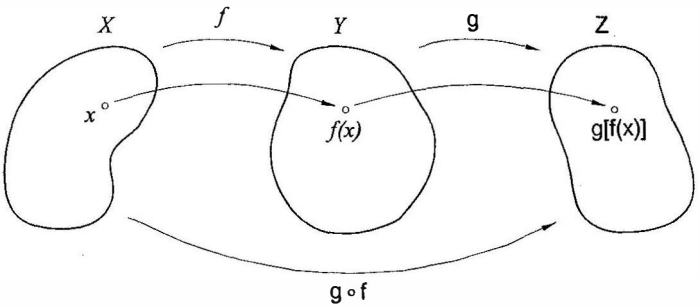
definirano zakonom

$$h(x) = g[f(x)],$$

za svaki $x \in X$. Preslikavanje h označavamo kao

$$g \circ f$$

i nazivamo **kompozicijom preslikavanja** f i g.



Ako su npr. $f, g : \mathbb{R} \to \mathbb{R}$ funkcije dane s $f(x) = 2x$ odnosno $g(x) = \sin x$, onda je kompozicija $g \circ f$ definirana s

$$(g \circ f)(x) = g[f(x)] = g(2x) = \sin 2x.$$

U ovom je slučaju određena i kompozicija $f \circ g$, i ona je dana s

$$(f \circ g)(x) = f[g(x)] = f(\sin x) = 2 \sin x.$$

Primjer pokazuje da **komponiranje preslikavanja nije komutativno.**

Operacija komponiranja preslikavanja je, međutim, **asocijativna.** Vrijedi naime

PROPOZICIJA 3

Neka su $f : X \to Y$, $g : Y \to Z$ i $h : Z \to V$ bilo koja preslikavanja. Onda su definirane kompozicije $(h \circ g) \circ f$ i $h \circ (g \circ f)$ i za svaki $x \in X$ vrijedi

$$[(h \circ g) \circ f](x) = [h \circ (g \circ f)](x) \ .$$

Dokaz

Na osnovi definicije komponiranja vrijedi redom

$$\begin{aligned} [(h \circ g) \circ f](x) &= (h \circ g)[f(x)] = h\{g[f(x)]\} \ , \\ [h \circ (g \circ f)](x) &= h[(g \circ f)(x)] = h\{g[f(x)]\} \end{aligned}$$

pa je asocijativnost dokazana. ■

Zapamtimo to važno svojstvo komponiranja na koje ćemo se često pozivati.

Za dva preslikavanja $f : X \to Y$ i $g : X' \to Y'$ kažemo da su **jednaka**, i pišemo (pojednostavnjeno)

$$f = g \ ,$$

ako se ta preslikavanja podudaraju u domeni, kodomeni i u zakonu pridruživanja, tj. ako vrijedi

$$X' = X \quad \text{i} \quad Y' = Y \ ,$$

kao i

$$g(x) = f(x)$$

za svaki $x \in X$. Ako su npr. f, g i h tri preslikavanja, koja se mogu komponirati (u tom poretku), onda tvrdnju iz Prop. 3 možemo pisati kao jednakost preslikavanja

$$(h \circ g) \circ f = h \circ (g \circ f).$$

Uočimo da u definiciju jednakosti bitno ulazi domena i kodomena. Ako je

$$X = \{(4k+1)\pi/2 \mid k \in \mathbb{Z}\},$$

a $f, g : X \to \mathbb{R}$ realne funkcije dane s $f(x) = \sin x$, $g(x) = 1$, onda je u smislu naše definicije $f = g$.

Neka je $f : X \to Y$ dano preslikavanje, a $A \subset X$ podskup od X. Onda definiramo preslikavanje

$$g : A \to Y$$

stavljajući

$$g(x) = f(x)$$

za svaki $x \in A$, i to preslikavanje zovemo **restrikcija** ili **ograničenje** od f na skup A i pišemo

$$g = f/_A .$$

U drugu ruku, ako je dano preslikavanje $g : A \to Y$, ako je $A \subset X$, a $f : X \to Y$ je bilo koje preslikavanje sa svojstvom da je $f/_A = g$, onda kažemo da je f **ekstenzija** ili **proširenje** od g preko cijelog skupa X.

Dok je restrikcija preslikavanja očito jednoznačno određena, proširenja preslikavanja će općenito biti mnogo. Na primjer, funkcije $f, g : \mathbb{R} \to \mathbb{R}$ dane s $f(x) = \sin x$, $g(x) = 1$ su različita proširenja funkcije

$$X \to \mathbb{R}$$

opisane u prošlom primjeru, preko skupa $\mathbb{R}$. Naravno, ima mnogo drugih proširenja te funkcije.

Na preslikavanja možemo postaviti neke dodatne zahtjeve. Za preslikavanje $f : X \to Y$ kažemo da je **surjektivno** (ili surjekcija), ako je slika domene cijela kodomena, tj. ako vrijedi

$$f(X) = Y.$$

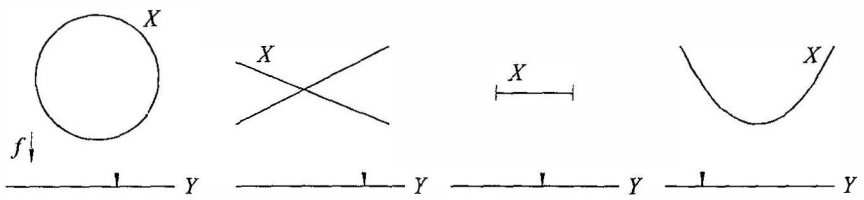
To će očito biti ako i samo ako je za svaki $y \in Y$ praslika $f^{-1}(y) \neq \emptyset$.

Preslikavanje $f : X \to Y$ je **injektivno** (ili injekcija) ako različiti elementi iz domene imaju različite slike, tj. ako iz $x_1, x_2 \in X$ i $x_1 \neq x_2$ slijedi

$f(x_1) \neq f(x_2)$. To će dakako biti ako i samo ako se za svaki $y \in Y$ praslika $f^{-1}(y)$ sastoji od najviše jednog elementa.

Konačno, za preslikavanje $f : X \to Y$ kažemo da je **bijektivno** (ili bijekcija), ako je i surjektivno i injektivno.

Na primjer, identiteta je uvijek bijekcija. Ako su realne funkcije f, g, $h : \mathbb{R} \to \mathbb{R}$ dane s $f(x) = 2x$, $g(x) = x^2$, $h(x) = x^3$, onda su prva i treća funkcija bijekcije, dok druga to nije (zapravo, ta funkcija nije niti surjekcija niti injekcija). Ili geometrijski primjer: Neka je Y pravac u ravnini, a za X uzmimo u toj istoj ravnini redom kružnicu, par pravaca, segment odnosno parabolu (vidi sliku).



Ako je sada preslikavanje $f : X \to Y$ definirano kao ortogonalna projekcija, onda vidimo da prvo preslikavanje nije ni surjektivno ni injektivno, drugo je surjektivno (ali nije injektivno), treće je injektivno (ali nije surjektivno) i konačno, četvrto je preslikavanje i surjektivno i injektivno, dakle bijektivno.

Primijetimo da svaka injekcija zamjenom kodomene sa slikom domene postaje bijekcija. Slično, svaka surjekcija dopušta restrikciju (ograničenje domene), koja je bijekcija.

Neka su $f : X \to Y$ i $g : Y \to Z$ preslikavanja koja se mogu komponirati. Ako su oba preslikavanja f i g bilo surjektivna, bilo injektivna ili pak bijektivna, onda i njihova kompozicija $h = g \circ f$ ima to isto svojstvo. Interesantno je, međutim, da vrijedi neka vrsta obrata te očigledne činjenice.

PROPOZICIJA 4

Neka je $h = g \circ f$ kompozicija preslikavanja f i g. Ako je

(1) *h surjekcija, onda je i g surjekcija,*

(2) *h injekcija, onda je i f injekcija.*

Dokaz

Dokažimo npr. (2). Neka su $a, b \in X$ i $a \neq b$. Kako je h injekcija po pretpostavci, to je $h(a) \neq h(b)$. Dakle je $g[f(a)] \neq g[f(b)]$, odakle zaključujemo da mora biti $f(a) \neq f(b)$ i, prema tome, f je injekcija. ■

Neka je $f : X \to Y$ bijektivno preslikavanje. Onda se za svaki $y \in Y$ praslika $f^{-1}(y)$ očito sastoji iz jednog jedinog elementa. Ako skup $f^{-1}(y)$

identificiramo s tim elementom iz X, dolazimo prirodno do preslikavanja

$$g : Y \to X$$

danog zakonom

$$g(y) = f^{-1}(y)$$

za svaki $y \in Y$. Preslikavanje g nazivamo **inverznim preslikavanjem** ili **inverzom** preslikavanja f i iz očiglednih razloga označavamo standardno s f^{-1}.

Odmah se vidi da je inverzno preslikavanje f^{-1} također bijekcija i da vrijedi

$$f^{-1} \circ f = e_X, \qquad f \circ f^{-1} = e_Y ,$$

gdje su s e_X i e_Y označene identitete na skupu X odnosno Y.

Kažimo na kraju i ovo: Ako su X i Y dani skupovi, onda skup svih preslikavanja $X \to Y$ standardno označavamo kao

$$Y^X$$

i zovemo **funkcijski skup** za (uređeni) par skupova X i Y. Naravno, u općem će slučaju Y^X i X^Y biti različiti skupovi. Na primjer, $\mathbb{R}^X$ je oznaka za skup svih realnih funkcija na skupu X, a $\mathbb{R}^{\mathbb{R}}$ za skup svih realnih funkcija realne varijable (vidi i Zad. 8. u 1.5.).

ZADACI

1. Kad je iz konteksta jasno što je domena, a što kodomena, često se dano preslikavanje zapisuje kraće kao $y = f(x)$ ili $f : x \mapsto y$ ili $x \overset{f}{\mapsto} y$. Uzimajući za domenu maksimalni skup realnih brojeva za koji zakon pridruživanja ima smisla, opiši preslikavanja dana s $x \mapsto x^2$, $x \mapsto \dfrac{1}{x}$, $x \mapsto \mathrm{tg}x$, $x \mapsto |x|$.

2. Definiraj pojam kompleksne funkcije kao i kompleksne funkcije kompleksne varijable i daj primjere takvih funkcija.

3. Dokaži Prop. 1 i Prop. 2. Dokaži da za $f : X \to Y$ i $A, B \subset X$ vrijedi

   $$f(A) - f(B) \subset f(A - B).$$

   Uvjeri se protuprimjerom da u gornoj relaciji općenito ne vrijedi znak jednakosti.

4. Neka je $f : X \to Y$ bilo koje preslikavanje, i $A \subset X$, $B \subset Y$. Dokaži da vrijedi

(a) $A \subset f^{-1}[f(A)]$;

(b) $f[f^{-1}(B)] \subset B$;

(c) $f[A \cap f^{-1}(B)] = f(A) \cap B$.

5. Neka je $A \subset X$ podskup od X. Onda definiramo funkciju

$$\chi_A : X \to \mathbb{R}$$

stavljajući

$$\chi_A(x) = \begin{cases} 1, & x \in A \\ 0, & x \in X - A \end{cases} .$$

Ta se funkcija zove **karakteristična funkcija** od A u X. Verificiraj ove jednakosti:

(a) $\chi_{A\cap B}(x) = \chi_A(x) \cdot \chi_B(x)$;

(b) $\chi_{A\cup B}(x) = \chi_A(x) + \chi_B(x) - \chi_A(x) \cdot \chi_B(x)$;

(c) $\chi_{A-B}(x) = \chi_A(x)\,[1 - \chi_B(x)]$;

(d) $\chi_{CA}(x) = 1 - \chi_A(x)$;

za svaki $x \in X$.

6. Neka je $\mathcal{P}(X)$ partitivni skup skupa X i $A \in \mathcal{P}(X)$. Definiramo

$$\Psi_A : \mathcal{P}(X) \to \mathbb{R}$$

stavljajući

$$\Psi_A(B) = \begin{cases} 1, & \text{ako je } B \cap A \neq \emptyset \\ 0, & \text{ako je } B \cap A = \emptyset \end{cases} .$$

Analiziraj tu funkciju.

7. Kompozicija preslikavanja se može definirati i u slučaju kad je kodomena prvog preslikavanja **sadržana** u domeni drugog. Je li ta definicija bitno općenitija od one u tekstu?

8. Neka je $A \subset X$, $i : A \to X$ inkluzija, $f : X \to Y$ i $g : A \to Y$ bilo koja preslikavanja. Promatraj **dijagram**

$$\begin{array}{ccc} A & \xrightarrow{\ i\ } & X \\ & {\scriptstyle g}\searrow \quad \swarrow{\scriptstyle f} & \\ & Y & \end{array} .$$

Uvjeri se da je $g = f/_A$ ako i samo ako je taj dijagram **komutativan**, tj. vrijedi $f \circ i = g$.

9. Neka su $A, B \subset X$ podskupovi, koji **fiksiraju** X, tj. takvi da je $A \cup B = X$. Neka su $f : A \to Y$ i $g : B \to Y$ preslikavanja sa svojstvom da je
$$f/_{A\cap B} = g/_{A\cap B} .$$
Onda postoji jedinstveno preslikavanje
$$h : X \to Y$$
takvo da je $h/_A = f$ i $h/_B = g$. Dokaži i generaliziraj.

10. Dokaži ovaj važan **kriterij** za prepoznavanje injektivnog preslikavanja: Preslikavanje $f : X \to Y$ je injektivno onda i samo onda ako iz $f(a) = f(b)$ slijedi $a = b$.

11. Dokaži: Ako je $h = g \circ f$ kompozicija preslikavanja $f : X \to Y$ i $g : Y \to Z$, onda je
    (a) $h(A) = g[f(A)]$, za svaki $A \subset X$;
    (b) $h^{-1}(C) = f^{-1}[g^{-1}(C)]$, za svaki $C \subset Z$.

    Primijeni taj teorem za dokaz tvrdnje (1) u Prop. 4.

12. Iz Prop. 4 slijedi: Ako je $h = g \circ f$ bijekcija, onda je f injekcija i g surjekcija. Je li istinit obrat te tvrdnje?

13. Koristeći Prop. 4 dokaži: Preslikavanje $f : X \to Y$ je bijektivno ako i samo ako postoji $g : Y \to X$ tako da su kompozicije $g \circ f$ i $f \circ g$ identitete. Pritom je $g = f^{-1}$.

1.4. Kardinalni broj skupa

Nekoliko osnovnih činjenica o pojmu kardinalnog broja. Kažemo da je skup X **ekvipotentan** (jednakobrojan) skupu Y ako postoji bar jedna bijekcija
$$f : X \to Y.$$
Skup X je **konačan** ako je ekvipotentan s jednim od skupova S_i, $i = 0, 1, 2, \ldots$, gdje je
$$\begin{aligned} S_0 &= \emptyset \\ S_1 &= \{1\} \\ S_2 &= \{1, 2\} \\ \ldots &\quad \ldots \\ S_n &= \{1, 2, \ldots, n\} \\ \ldots &\quad \ldots \end{aligned}$$

U protivnom kažemo da je X **beskonačan** skup. Primijetimo da za $i \neq j$ skup S_i nije ekvipotentan sa skupom S_j.

Kardinalni broj skupa broji njegove elemente. Točnije, konačni skup X je **kardinalnog broja** n,

$$\operatorname{card}(X) = n \,,$$

ako je ekvipotentan sa skupom S_n. Posebno, dakle, $\operatorname{card}(X) = 0$ ako i samo ako je $X = \emptyset$.

Teškoće nastupaju kad je skup beskonačan. G. Cantor (konac 19. st.) prvi je primijetio da beskonačni skupovi ne moraju biti ekvipotentni, da ih ima koji su "više beskonačni" od drugih beskonačnih skupova. Konkretno, pokazalo se da skup $\mathbb{R}$ realnih brojeva i skup $\mathbb{N}$ prirodnih brojeva nisu ekvipotentni; prvi ima bitno više elemenata od drugog.

Za skup X koji je ekvipotentan sa skupom $\mathbb{N}$ kažemo da je **prebrojivo beskonačan**, i za njegov kardinalni broj tradicionalno pišemo

$$\operatorname{card}(X) = \aleph_0 \,,$$

što čitamo alef nula ($\aleph$ je hebrejsko slovo alef). Na primjer, lako se pokazuje da su skupovi $\mathbb{Z}$ i $\mathbb{Q}$ prebrojivo beskonačni.

Za skup koji je ili konačan ili prebrojivo beskonačan, kažemo da je **prebrojiv**. Skup koji nije prebrojiv je **neprebrojivo beskonačan** ili **neprebrojiv**. U smislu naše primjedbe, takav je npr. skup $\mathbb{R}$.

Ako je X ekvipotentan sa skupom $\mathbb{R}$, pišemo

$$\operatorname{card} X = c$$

i kažemo da X ima kontinuum elemenata (c dolazi od latinske riječi continuum – neprekidnost).

Mogu se konstruirati neprebrojivi skupovi koji nisu ekvipotentni s $\mathbb{R}$, ali oni za naše praktične potrebe nisu od interesa.

Strogim fundiranjem kardinalnih brojeva i detaljnim izučavanjem njihovih svojstava bavi se teorija skupova.

ZADACI

1. Uoči da je $\operatorname{card}\{1, \ldots, n\} = n$, $\operatorname{card} \mathbb{N} = \aleph_0$, $\operatorname{card} \mathbb{R} = c$.

2. Pokušaj dokazati da $\mathbb{N}$ i $\mathbb{C}$ nisu ekvipotentni.

3. Dokaži da je $\operatorname{card} \mathbb{Z} = \aleph_0$ i $\operatorname{card} \mathbb{Q} = \aleph_0$. Dokaži, nadalje, da je

$$\operatorname{card} \mathbb{C} = c \,.$$

4. Za realni broj x kažemo da je **algebarski** prebrojivo beskonačan ako je nultočka polinoma u jednoj varijabli s cjelobrojnim koeficijentima. Pokaži da je skup svih algebarskih brojeva prebrojiv.

5. Dokaži: Unija od prebrojivo mnogo prebrojivih skupova je prebrojiv skup.

6. Ako su X i Y konačni skupovi, dokaži da vrijedi

$$\operatorname{card}(X \cup Y) = \operatorname{card} X + \operatorname{card} Y - \operatorname{card}(X \cap Y) .$$

7. Dokaži: Skup je beskonačan ako i samo ako je ekvipotentan s jednim svojim pravim podskupom. Ilustriraj to primjerima.

8. Neka je X konačan skup, a $\mathcal{P}(X)$ partitivni skup od X. Dokaži da onda vrijedi

$$\operatorname{card} \mathcal{P}(X) = 2^{\operatorname{card}(X)} .$$

9. Uvjeri se da je u slučaju kad je skup X prebrojivo beskonačan, skup $\mathcal{P}(X)$ neprebrojivo beskonačan. I više, $\operatorname{card} \mathcal{P}(X) = c$.

10. Neka su X i Y konačni skupovi, a Y^X neka je skup svih preslikavanja iz X u Y. Onda je i Y^X konačan i vrijedi

$$\operatorname{card}(Y^X) = (\operatorname{card} Y)^{\operatorname{card} X} .$$

Diskutiraj i slučaj kad je jedan od danih skupova prebrojivo beskonačan.

1.5. Kartezijev produkt skupova

Opisat ćemo još jedan način kako se iz danih skupova mogu proizvesti novi.

Za dane skupove X i Y definiramo njihov **Kartezijev produkt** $X \times Y$ kao skup

$$X \times Y = \{(x, y) \mid x \in X,\ y \in Y\} ,$$

tj. kao skup svih **uređenih** parova, u kojima je prvi element iz skupa X, a drugi iz skupa Y. Kažemo da su X i Y **faktori** Kartezijeva produkta. Osim naziva Kartezijev produkt, još su u upotrebi nazivi kombinirani ili, također, direktni produkt skupova. Na primjer, ako je

$$X = \{a, b\}, \qquad Y = \{1, 2, 3\} ,$$

Kartezijev produkt tih skupova jest skup

$$X \times Y = \{(a, 1), (a, 2), (a, 3), (b, 1), (b, 2), (b, 3)\} .$$

U drugu ruku, imamo

$$Y \times X = \{(1,a),(1,b),(2,a),(2,b),(3,a),(3,b)\}$$

i prema tome

$$X \times Y \neq Y \times X\,.$$

Kartezijevo množenje skupova nije, dakle, općenito komutativno. To će biti slučaj ako i samo ako je $Y = X$; tada govorimo o **Kartezijevu kvadratu**

$$X^2 = X \times X = \{(a,b) \mid a,b \in X\}$$

skupa X. Za Kartezijev kvadrat definiramo **dijagonalu**

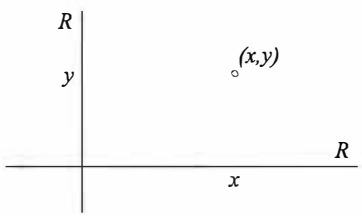
$$D = \{(a,a) \mid a \in X\} \subset X^2\,.$$

PRIMJERI

1. Neka je $X = Y = \mathbb{R}$. Onda je Kartezijev kvadrat

$$\mathbb{R}^2 = \{(x,y) \mid x,y \in \mathbb{R}\}\ ,$$

dakle, kako se to kaže u srednjoj školi, ravnina Kartezijeva koordi-

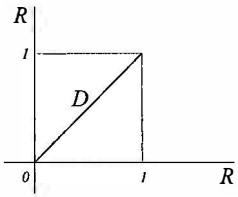


natnog sustava, koordinatna ravnina. Odatle i potječe naziv za Kartezijev produkt. Prema tome, Kartezijev produkt dvaju neparalelnih pravaca možemo geometrijski interpretirati kao ravninu.

2. Slično, uz $X = Y = I = [0,1]$ imamo

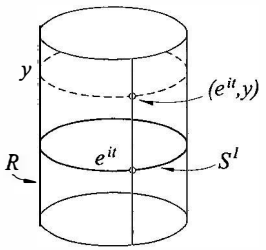
$$I^2 = \{(x,y) \in \mathbb{R}^2 \mid 0 \leq x, y \leq 1\},$$

a to je u koordinatnoj ravnini pravi kvadrat, u kojem se dijagonala

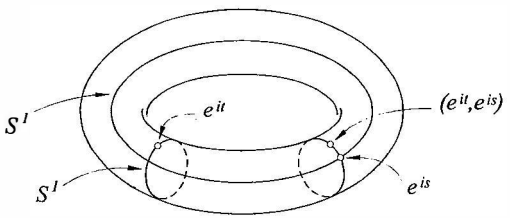


produkta D podudara s njegovom geometrijskom dijagonalom.

3. Neka je $X = S^1 = \{e^{it} \mid t \in \mathbb{R},\ 0 \leq t < 2\pi\}$, dakle kružnica u kompleksnoj ravnini, a $Y = \mathbb{R}$, tj. pravac. Uređenim parom (e^{it}, y) jednoznačno je određena točka na cilindru, kojem je S^1 baza (vidi sliku) pa u tom smislu shvaćamo $X \times Y$ kao (beskonačni) **cilindar**.



4. Posve analogno, $S^1 \times S^1$ možemo geometrijski interpretirati kao **torus**,



plohu koja odgovara zračnici automobilske gume.

Primijetimo da će biti

$$X \times Y = \emptyset$$

onda i samo onda, ako je bar jedan od skupova X i Y prazan. Daljnja svojstva Kartezijeva produkta popisana su ovim teoremom:

TEOREM 1

Neka su X, Y i Z bilo koji skupovi. Onda je

(1) $(X \cup Y) \times Z = (X \times Z) \cup (Y \times Z)$;

(2) $(X \cap Y) \times Z = (X \times Z) \cap (Y \times Z)$;

(3) $(X - Y) \times Z = (X \times Z) - (Y \times Z)$;

tj. Kartezijevo je množenje distributivno prema uniji, presjeku i razlici skupova.

Dokaz

Pokažimo npr. (3). Neka je $(x, z) \in (X - Y) \times Z$. To znači da je $x \in X - Y$, a $z \in Z$. No, $x \in X - Y$ povlači da je $x \in X$ i $x \notin Y$. Prema tome je $(x, z) \in X \times Z$ i $(x, z) \notin Y \times Z$, dakle $(x, z) \in (X \times Z) - (Y \times Z)$, pa je inkluzija $(X - Y) \times Z \subset (X \times Z) - (Y \times Z)$ dokazana. Slično se vidi i obratna inkluzija. ■

Navedimo još kako se Kartezijev produkt ponaša prema podskupovima faktora.

TEOREM 2

Ako je $A \subset X$ i $B \subset Y$, onda je

(1) $A \times B \subset X \times Y$;

(2) $(X \times Y) - (A \times B) = [(X - A) \times Y] \cup [X \times (Y - B)]$. ■

Uz produkt $X \times Y$ prirodno su vezana neka preslikavanja. Imamo tako preslikavanja

$$p_1 : X \times Y \to X, \qquad p_2 : X \times Y \to Y$$

definirana s

$$p_1(x, y) = x, \qquad p_2(x, y) = y,$$

koja nazivamo **projekcije** na prvi, odnosno drugi faktor. U drugu ruku, za bilo koji fiksni $x_0 \in X$, odnosno $y_0 \in Y$, preslikavanja

$$j_1 : X \to X \times Y, \qquad j_2 : Y \to X \times Y\ ,$$

zadana s

$$j_1(x) = (x, y_0), \qquad j_2(y) = (x_0, y)\ ,$$

nazivamo **inkluzije**, određene s $y = y_0$, odnosno $x = x_0$. Jasno je da su projekcije surjektivna preslikavanja, a inkluzije injektivna.

Konačno, ako su

$$f : S \to X \quad \text{i} \quad g : S \to Y$$

bilo koja preslikavanja, definiramo preslikavanje

$$h : S \to X \times Y$$

stavljajući

$$h(s) = (f(s), g(s))$$

za svaki $s \in S$. To preslikavanje obično označavamo s

$$h = f \times g$$

i nazivamo **Kartezijev produkt preslikavanja** f i g.

Pojam Kartezijeva produkta se generalizira na slučaj kad imamo više faktora. Ako su $X_1, X_2, \ldots, X_n$ bilo koji skupovi, definiramo

$$X_1 \times X_2 \times \cdots \times X_n = \{(x_1, x_2, \ldots, x_n) \mid x_i \in X_i\} \ .$$

Produkt se slično definira i kad imamo prebrojivo mnogo faktora (nizovi umjesto uređenih n-torki), pa i neprebrojivo (vidi Zad. 8.). Nije teško definirati projekcije i inkluzije i u toj općenitijoj situaciji.

ZADACI

1. Dokaži Tm. 1 i Tm. 2.

2. Neka su $A, C \subset X$, a $B, D \subset Y$. Dokaži da je onda

   (a) $(A \times B) \cap (C \times D) = (A \cap C) \times (B \cap D)$;

   (b) $(A \times B) \cup (C \times D) \subset (A \cup C) \times (B \cup D)$.

   Uvjeri se protuprimjerom da u (2) općenito ne vrijedi znak jednakosti.

3. Neka je

   $$s : X \times Y \to Y \times X$$

   preslikavanje dano sa

   $$s(x, y) = (y, x) \ .$$

   Pokaži da je s bijekcija i prema tome je skup $X \times Y$ ekvipotentan sa skupom $Y \times X$.

4. Uvjeri se da je $(X \times Y) \times Z \neq X \times (Y \times Z)$, tj. Kartezijevo množenje nije asocijativno. Konstruiraj prirodnu bijekciju

$$(X \times Y) \times Z \to X \times (Y \times Z)$$

koja pokazuje da su ti skupovi ekvipotentni.

5. Ako su X i Y konačni skupovi, onda je

$$\text{card}\,(X \times Y) = \text{card}\,X \cdot \text{card}\,Y\ .$$

Dokaži!

6. Dokaži da je Kartezijev produkt prebrojivih skupova prebrojiv.

7. Neka je

$$d : X \to X^2$$

dijagonalna inkluzija, tj. preslikavanje dano s

$$d(x) = (x, x)\ .$$

Pokaži da je d injekcija i da je $d(X) = D =$ dijagonala u X^2. Nadalje, ako je $s : X^2 \to X^2$ preslikavanje iz Zad. 2., onda je

$$s \circ d = d\ .$$

Konačno, ako su $p_i : X^2 \to X$, $i = 1, 2$, projekcije, onda vrijedi

$$p_i \circ d = e\ ,$$

gdje je e identiteta na X.

8. Neka je M bilo koji skup, a $\{X_\mu | \mu \in M\}$ familija skupova, indeksirana elementima iz M. Neka je s X označena unija skupova iz te familije. Onda pod **Kartezijevim produktom dane familije skupova** razumijevamo skup F svih preslikavanja

$$f : M \to X$$

sa svojstvom da je

$$f(\mu) \in X_\mu \subset X$$

za svaki $\mu \in M$. Kartezijev produkt označavamo obično kao

$$F = \prod_{\mu \in M} X_\mu\ .$$

Uvjeri se da se u slučaju kad je $M = \{1, 2\}$, odnosno $M = \{1, 2, \ldots, n\}$, ta definicija svodi na definicije Kartezijeva produkta iz teksta. Razmotri slučaj kad je $M = \mathbb{N}$. Ako su svi faktori u produktu jednaki, $X_\mu = X$ za svaki $\mu \in M$, onda F nazivamo M-ta **Kartezijeva potencija** skupa X i pišemo

$$F = X^M .$$

To je, dakle, skup svih preslikavanja $M \to X$. Uoči da je to generalizacija Kartezijeva kvadrata X^2 i n-te potencije X^n. Kako ćeš opisati skup $X^{\mathbb{N}}$?

9. Kako smo spomenuli u točki 1.2., za partitivni skup od M se upotrebljava i oznaka 2^M. Uzmimo sada da je $X = \{0, 1\}$ pa definirajmo preslikavanje

$$f : 2^M \to X^M$$

stavljajući za svaki $A \in 2^M$, dakle $A \subset M$,

$$f(A) = \chi_A ,$$

gdje je $\chi_A : M \to X$ karakteristična funkcija od A u M (vidi Zad. 5. u 1.3.). Pokaži da je f bijekcija. Time se objašnjava klasična oznaka 2^M za partitivni skup od M.

10. Generaliziraj pojam projekcija, inkluzija kao i pojam Kartezijeva produkta preslikavanja za opći slučaj Kartezijeva produkta skupova.

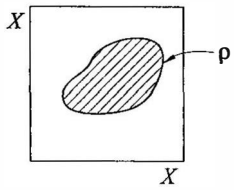
1.6. Relacije

U mnogim konkretno zadanim skupovima primjećujemo da su neki od elemenata u izvjesnom međusobnom odnosu. Tako npr. u skupovima brojeva će neki od brojeva biti manji od danog broja ili možda jednaki tom broju, ili veći od njega. U skupovima pravaca govorimo o parovima paralelnih pravaca, o parovima okomitih pravaca i slično. Generalizirajući te ideje, dolazimo do apstraktnog pojma relacije.

Neka je X neprazni skup, a X^2 njegov Kartezijev kvadrat. Svaki podskup

$$\varrho \subset X^2$$

tog kvadrata nazivamo **relacija** na skupu X. Ako je ϱ bilo koja relacija

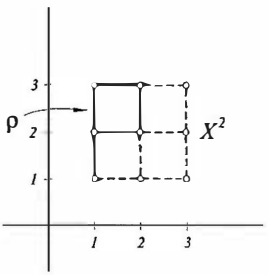


na skupu X, a $a, b \in X$ elementi sa svojstvom da je $(a, b) \in \varrho \subset X^2$, onda kažemo da je element a u **relaciji** ϱ s b i pišemo

$$a \varrho b .$$

Ako je npr. $X = \{1, 2, 3\}$, jedna relacija na X je

$$\varrho = \{(1,1), (1,2), (1,3), (2,2), (2,3)\} \subset X^2 ,$$



što znači da je

$$1 \varrho 1, \quad 1 \varrho 2, \quad 1 \varrho 3, \quad 2 \varrho 2, \quad 2 \varrho 3 .$$

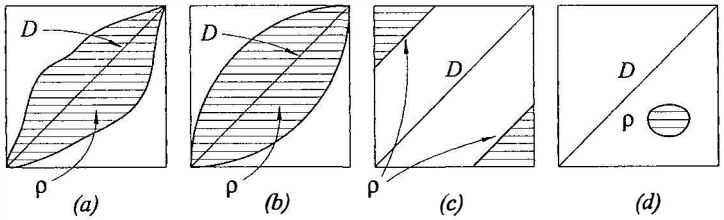
Za nas će biti od interesa relacije koje imaju neka dobra dodatna svojstva.

Relacija ϱ je **refleksivna** ako je $a \varrho a$ za svaki $a \in X$. Drugim riječima, ϱ je refleksivna ako i samo ako je $(a, a) \in \varrho$, za svaki $a \in X$, tj. ako je dijagonala $D \subset X^2$ sadržana u ϱ.

Relacija ϱ je **simetrična** ako iz $a \varrho b$ slijedi da je i $b \varrho a$, tj. ako $(a, b) \in \varrho$ povlači $(b, a) \in \varrho$. Geometrijski gledano, simetrična relacija je podskup u X^2 koji je simetričan s obzirom na dijagonalu D. Pritom ϱ može, ali ne mora, sadržavati dijagonalu; simetrična relacija nije nužno refleksivna.

Relacija ϱ je **antisimetrična** ako iz $a \varrho b$ i $b \varrho a$ slijedi da je nužno $a = b$. Prema tome, uz $a \neq b$ je kod antisimetrične relacije od odnosa $a \varrho b$ i $b \varrho a$ istinit najviše jedan; $(a, b) \in \varrho$ povlači $(b, a) \notin \varrho$.

Relacija je **tranzitivna**, ako iz $a \varrho b$ i $b \varrho c$ slijedi da je i $a \varrho c$, odnosno ako $(a, b) \in \varrho$ i $(b, c) \in \varrho$ povlači $(a, c) \in \varrho$.



Na slici je (a) refleksivna relacija, (b) i (c) su simetrične relacije, a (d) je antisimetrična. Svojstvo tranzitivnosti je teško predočiti grafički.

Konačno, za relaciju ϱ na skupu X kažemo da je **relacija ekvivalencije,** ako je ta relacija i refleksivna i simetrična i tranzitivna, tj. ako istovremeno vrijedi

(1) $a \varrho a$, za svaki $a \in X$,

(2) $a \varrho b$ povlači $b \varrho a$, i

(3) $a \varrho b$ i $b \varrho c$ povlači $a \varrho c$.

Za takvu je relaciju još uobičajen naziv **relacija klasifikacije**, zbog njezina svojstva, koje ćemo uskoro upoznati (vidi Tm. 1).

Relaciju ekvivalencije standardno označavamo s $\sim$. Ako je $a \sim b$, onda kažemo da je element a **ekvivalentan** s elementom b.

Neka je $\sim$ relacija ekvivalencije definirana na skupu X, a $a \in X$ bilo koji element. Neka je sa $C(a) \subset X$ označen podskup od X, koji se sastoji od svih elemenata iz X koji su ekvivalentni s a, tj.

$$C(a) = \{x \in X \mid x \sim a\} \ .$$

Kažemo da je $C(a)$ **klasa ekvivalencije** određena elementom $a \in X$. Primijetimo da je, zbog refleksivnosti, $a \in C(a)$ za svaki $a \in X$ i, prema tome, je uvijek $C(a) \neq \emptyset$.

TEOREM 1

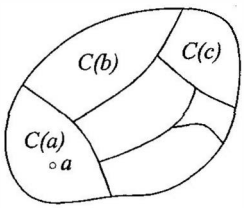
Neka su $a, b \in X$ bilo koji elementi. Onda je $C(a) \cap C(b) = \emptyset$ ili je $C(a) = C(b)$.

Dokaz

Pretpostavimo da je $C(a) \cap C(b) \neq \emptyset$. Treba dokazati da je u tom slučaju $C(a) = C(b)$. Neka je $c \in C(a) \cap C(b)$ bilo koja točka. Pokažimo inkluziju $C(a) \subset C(b)$. Neka je $x \in C(a)$. Po definiciji to znači da je $x \sim a$. Kako je i $c \in C(a)$, dakle $c \sim a$, odnosno zbog simetrije $a \sim c$, imamo iz tranzitivnosti da je $x \sim c$. U drugu ruku, jer je također $c \in C(b)$, vrijedi $c \sim b$. Ponovo, zbog tranzitivnosti, iz $x \sim c$ i $c \sim b$ zaključujemo da je $x \sim b$,

dakle $x \in C(b)$, pa je inkluzija $C(a) \subset C(b)$ dokazana. Posve analogno se dokazuje inkluzija $C(b) \subset C(a)$. Prema tome je $C(a) = C(b)$ i teorem je dokazan. ■

Iz teorema slijedi da svaki element skupa X pripada jednoj i samo jednoj klasi ekvivalencije, određenoj pomoću relacije $\sim$ na skupu X. Na taj smo



način proveli dakle izvjesnu klasifikaciju elemenata iz skupa X, pa zato $\sim$ nazivamo i relacijom klasifikacije.

Neka je s Q označen skup svih međusobno **različitih** klasa ekvivalencije određenih s relacijom $\sim$ na skupu X. Elementi od Q su neprazni podskupovi od X, koji su u parovima disjunktni i imaju svojstvo da je njihova unija jednaka čitavom X (pa prema tome predstavljaju jednu dekompoziciju skupa X, vidi Zad. 12.). Skup Q obično označavamo s

$$Q = X/_\sim$$

i nazivamo ga **kvocijentnim skupom** skupa X u odnosu na relaciju $\sim$, ili po relaciji $\sim$.

Uz kvocijentni skup je prirodno vezano preslikavanje

$$q : X \to X/_\sim$$

definirano s

$$q(a) = C(a) \ ,$$

koje svakom elementu skupa X pridružuje klasu ekvivalencije kojoj taj element pripada. Preslikavanje q se naziva **kvocijentno preslikavanje** skupa na pripadni kvocijent.

PRIMJERI

1. Neka je $X = \mathbb{Z}$, a $m \in \mathbb{N}$ dani prirodni broj. Na X definiramo relaciju $\sim$ stavljajući $a \sim b$ ako i samo ako je $a - b$ djeljivo s m. Lako se provjeri da je $\sim$ jedna relacija ekvivalencije i da se pripadni kvocijentni skup sastoji od točno m različitih klasa,

$$\mathbb{Z}/_\sim = \{C(0), C(1), \ldots, C(m-1)\} \ .$$

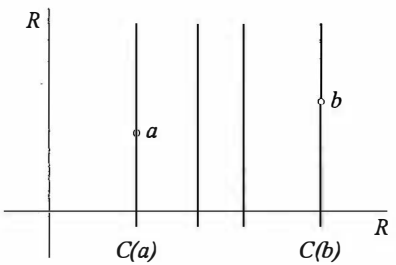
Pritom će klasa $C(k)$, $k = 0, 1, \ldots, m-1$ sadržavati one i samo one cijele brojeve koji pri dijeljenju s m daju ostatak k (oprez pri dijeljenju negativnih brojeva!). Na primjer, za $m = 3$ imamo

$$\begin{aligned} C(0) &= \{\ldots -3, 0, 3, 6, \ldots\}\ , \\ C(1) &= \{\ldots -2, 1, 4, 7, \ldots\}\ , \\ C(2) &= \{\ldots -1, 2, 5, 8, \ldots\}\ , \end{aligned}$$

tj. proveli smo klasifikaciju cijelih brojeva na one koji su djeljivi s 3, na one koji pri dijeljenju s 3 daju ostatak 1, te one koji pri dijeljenju s 3 daju ostatak 2.

2. Neka je $\mathcal{P}$ skup svih pravaca ravnine. Za pravce $a, b \in \mathcal{P}$ kažemo da su paralelni, i pišemo $a \parallel b$, ako ti pravci nemaju ni jedne točke zajedničke ili su im sve točke zajedničke. Onda je $\parallel$ jedna relacija ekvivalencije na $\mathcal{P}$. Klase ekvivalencije, tj. elemente kvocijentnog skupa $\mathcal{P}/_{\parallel}$, nazivamo **smjerovima u ravnini** (vidi i Zad. 1. u 5.4.). Je li relacija $a \perp b$, tj. "*biti okomit*" relacija ekvivalencije na skupu $\mathcal{P}$?

3. Neka je $X = \mathbb{R}^2$ koordinatna ravnina, na kojoj je relacija $\sim$ definirana s $(x, y) \sim (x', y')$ ako i samo ako je $x = x'$.



To je onda relacija ekvivalencije na $\mathbb{R}^2$, čije klase čine, geometrijski govoreći, pravci paralelni s osi y. Odmah se vidi da je kvocijentni skup $\mathbb{R}^2/_{\sim}$ prirodno ekvipotentan sa skupom $\mathbb{R}$ realnih brojeva.

4. Neka je s $\mathcal{T}$ označen skup svih trokuta u ravnini. Onda je svaki od odnosa "*biti kongruentan (sukladan) sa*", "*biti sličan sa*" i "*imati istu površinu kao*" među trokutima jedna dobro definirana relacija ekvivalencije na skupu $\mathcal{T}$. Na primjer, kvocijentni skup po zadnjoj od tih relacija će biti ekvipotentan sa skupom pozitivnih realnih brojeva.

Spomenimo još jedan važan tip relacija. To su tzv. **relacije uređaja**. Neka je ϱ relacija na skupu X, koja je refleksivna, antisimetrična i tranzitivna, tj. relacija za koju vrijedi

(1) $a \varrho a$, za svaki $a \in X$;

(2) $a \varrho b$ i $b \varrho a$ povlači $a = b$;

(3) $a \varrho b$ i $b \varrho c$ povlači $a \varrho c$.

Onda kažemo da je ϱ jedna **relacija parcijalnog** (djelomičnog) **uređaja** na skupu X. Ako je još ispunjeno i

(4) za svaki $a, b \in X$ je ili $a \varrho b$ ili $b \varrho a$ ili oboje,

onda takvu relaciju nazivamo **relacija totalnog** (potpunog, linearnog) **uređaja** na skupu X.

Relaciju parcijalnog, odnosno totalnog uređaja na skupu X označavamo standardno s $\leq$. Ako je $a \leq b$, kažemo da je element a manji ili jednak od elementa b.

Uređeni par $(X, \leq)$ koji se sastoji od skupa X i uređajne relacije $\leq$ na tom skupu nazivamo **parcijalno**, odnosno **totalno uređenim** skupom.

PRIMJERI

1. Neka je $X = \mathcal{P}(S)$ partitivni skup od S. Na njemu definiramo relaciju $\leq$ stavljajući $A \leq B$ za $A, B \in \mathcal{P}(S)$ ako i samo ako je $A \subset B$. Odmah se vidi da je to jedna relacija parcijalnog uređaja na $\mathcal{P}(S)$, pa je $(\mathcal{P}(S), \leq)$ parcijalno uređen skup (ne i totalno uređen, ako S ima više od jednog elementa).

2. Na skupu $X = \mathbb{N}$ definiramo relaciju $\leq$ stavljajući $a \leq b$ ako i samo ako je a mjera od b, tj. b je djeljiv s a. Onda se lako provjeri da je $\leq$ uređajna relacija, s obzirom na koju je skup $\mathbb{N}$ parcijalno uređen.

3. Neka je $X = \mathbb{R}$, a relaciju $\leq$ definiramo stavljajući $a \leq b$ ako i samo ako je razlika $b - a$ nenegativan realni broj. Lako se provjeri da je $\leq$ jedna relacija totalnog uređaja, koju nazivamo **prirodnim uređajem** na $\mathbb{R}$. Analogno definiramo prirodne uređaje na skupovima $\mathbb{N}, \mathbb{Z}$ i $\mathbb{Q}$.

4. Neka je $X = \mathbb{R}^{\mathbb{R}}$ skup svih realnih funkcija realne varijable. Za $f, g \in \mathbb{R}^{\mathbb{R}}$ stavljamo $f \leq g$ ako i samo ako je $f(x) \leq g(x)$ za svaki $x \in \mathbb{R}$, gdje druga relacija predstavlja prirodni uređaj za realne brojeve. Onda je $(\mathbb{R}^{\mathbb{R}}, \leq)$ parcijalno uređen skup.

Neka je $(X, \leq)$ totalno uređen skup. Kažemo da je taj skup **dobro uređen** ako za svaki neprazni podskup $A \subset X$ postoji **minimalni** (najmanji) element, tj. element $a \in A$ sa svojstvom da je $a \leq x$ za svako $x \in A$.

Svaki totalno uređen skup ne mora biti i dobro uređen. Na primjer, skup $\mathbb{N}$ je uz prirodni uređaj dobro uređen, ali skupovi $\mathbb{Z}, \mathbb{Q}$ i $\mathbb{R}$ to nisu. Mogućnost dobrog uređenja skupa pomoću neke uređajne relacije regulirana je u teoriji skupova aksiomatski.

ZADACI

1. Na skupu $\mathbb{N}$ prirodnih brojeva definiramo relaciju ϱ, stavljajući $a \varrho b$ ako i samo ako

   (a) $a = b$;

   (b) $a \neq b$;

   (c) a se razlikuje od b za manje od 2;

   (d) svaki prirodni broj koji dijeli a dijeli i b;

   (e) a je višekratnik od b.

   Ispitaj koja svojstva ima svaka od navedenih relacija ϱ.

2. Neka je s X označen skup svih ljudi na svijetu. Utvrdi koja svojstva imaju sljedeće relacije na skupu X:

   (a) " je rođak od";

   (b) " je potomak od";

   (c) " je vjenčan sa";

   (d) " je stariji nego";

   (e) " je istog spola kao".

3. Neka je ϱ bilo koja relacija na skupu X. Onda definiramo **inverznu relaciju** ϱ^{-1} od ϱ kao

   $$\varrho^{-1} = \left\{(a, b) \in X^2 \mid (b, a) \in \varrho\right\} .$$

   Dokaži ove tvrdnje:

   (a) za svaku relaciju ϱ je $(\varrho^{-1})^{-1} = \varrho$;

   (b) relacija ϱ je simetrična ako i samo ako je $\varrho^{-1} = \varrho$.

4. Neka su ϱ i σ relacije na skupu X. Onda definiramo njihovu **kompoziciju** $\varrho \circ \sigma$, kao relaciju na X sa svojstvom da je $(a, b) \in \varrho \circ \sigma$ ako i samo ako postoji $x \in X$ tako da je $(a, x) \in \varrho$ i $(x, b) \in \sigma$. Pokaži da je uvijek

   (a) $(\varrho \circ \sigma)^{-1} = \sigma^{-1} \circ \varrho^{-1}$;

(b) $(\varrho \circ \sigma) \circ \tau = \varrho \circ (\sigma \circ \tau)$.

Nadalje, pokaži primjerom da komponiranje relacija nije komutativno. Je li općenito istina da je $\varrho \circ \varrho^{-1} = \varrho^{-1} \circ \varrho = e$, gdje je

$$e = D = \{(x, x) \mid x \in X\}$$

tzv. **identična** relacija?

5. Pojam relacije možemo generalizirati na ovaj prirodan način: **Relacija na uređenom paru skupova** (X, Y) ili **relacija između** X i Y je svaki podskup $\varrho \subset X \times Y$ njihova Kartezijeva produkta. Kao i prije, reći ćemo da je $x \in X$ u relaciji ϱ s $y \in Y$ i pisati $x \varrho y$, ako i samo ako je $(x, y) \in \varrho$. U novije se vrijeme uobičava pisati relaciju i kao

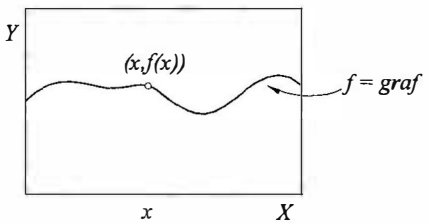
$$\varrho : X \to Y$$

stavljajući

$$\varrho(x) = \{y \in Y \mid x \varrho y\} \ .$$

Podskup $\{x \in X \mid \varrho(x) \neq \emptyset\}$ od X je onda domena za ϱ, a Y njezina kodomena. Definiraj u tim terminima pojmove inverzne relacije i kompozicije relacija, i utvrdi njihova svojstva. Kako bi se prirodno definirao pojam injektivne odnosno surjektivne relacije?

6. Preslikavanje $f : X \to Y$ možemo shvatiti kao specijalnu relaciju definiranu na paru (X, Y). Naime, relacija f će biti preslikavanje onda i samo onda, ako za svaki $x \in X$ postoji jedan i samo jedan element $y \in Y$ takav da je $(x, y) \in f$, tj. $x f y$. U tom slučaju pišemo $y = f(x)$. Drugim riječima, (u notaciji iz Zad. 5.) relacija $f : X \to Y$ je funkcija ako i samo ako se za svaki $x \in X$ skup $f(x)$ sastoji od točno jedne točke. Odatle odmah vidimo da je ovako definiran pojam preslikavanja identičan s onim u točki 1.3. Kažimo još da podskup $f \subset X \times Y$ nazivamo **graf** preslikavanja $f : X \to Y$.



Pokaži da je podskup $\varrho \subset X \times Y$ graf neke funkcije ako i samo ako iz pretpostavki $(x, y), (x', y') \in \varrho$ i $x' = x$ slijedi $y' = y$.

7. Neka je ϱ refleksivna relacija na skupu X. Ta relacija je relacija ekvivalencije ako i samo ako ima svojstvo da $a \varrho b$ i $a \varrho c$ povlači $b \varrho c$. Dokaži!

8. Neka je $f : X \to Y$ bilo koje preslikavanje. Onda na X definiramo relaciju $\overset{f}{\sim}$, stavljajući $a \overset{f}{\sim} b$, ako i samo ako je $f(a) = f(b)$. Pokaži da je $\overset{f}{\sim}$ relacija ekvivalencije.

9. Na skupu $\mathbb{R}$ realnih brojeva definiramo relaciju $\sim$ stavljajući $a \sim b$ onda i samo onda ako je $a - b$ cijeli broj. Pokaži da je $\sim$ jedna relacija ekvivalencije na $\mathbb{R}$. Kvocijentni skup $X/_\sim$ nazivamo **skup realnih brojeva modulo 1**.

10. Kako smo rekli (točka 1.4.), skup X je ekvipotentan sa skupom Y ako postoji bar jedna bijekcija $X \to Y$. Pokaži da je "*biti ekvipotentan*" jedna relacija ekvivalencije*). **Kardinalni broj** ili **potenciju** skupa X definiramo kao klasu ekvivalencije kojoj taj skup pripada, tj. kao zajedničko svojstvo svih ekvipotentnih skupova, i samo njih.

11. Neka je ϱ bilo koja relacija na skupu X. Na tom skupu definiramo onda novu relaciju $\sim$, stavljajući $a \sim b$ ako i samo ako postoji konačan broj točaka

$$a = x_1, x_2, \ldots, x_{k-1}, x_k = b$$

iz X, sa svojstvom da je za svaki i ispunjeno:

(a) $x_{i+1} = x_i$, ili

(b) $x_{i+1} \varrho x_i$, ili

(c) $x_i \varrho x_{i+1}$.

Dokaži da je $\sim$ jedna relacija ekvivalencije na X i da je to najmanja relacija ekvivalencije (podskup od X^2!) koja sadrži ϱ. Za $\sim$ kažemo da je **relacija ekvivalencije generirana s** ϱ.

12. Pod **particijom** (rastavom, dekompozicijom) nepraznog skupa X razumijevamo svaku familiju $\mathcal{D}$ podskupova od X, tj. svaki podskup $\mathcal{D} \subset \mathcal{P}(X)$ njegova partitivnog skupa koji ima ova svojstva:

(a) članovi od $\mathcal{D}$ nisu prazni;

(b) presjek bilo koja dva člana iz $\mathcal{D}$ je prazan; i

*) Izbjegli smo reći na skupu svih skupova jer takav ne postoji; to je čuveni paradoks u teoriji skupova. Zato se obično govori o **klasi** svih skupova.

(c) članovi od $\mathcal{D}$ prekrivaju X, tj. unija svih članova od $\mathcal{D}$ se podudara sa skupom X.

Ako je $\sim$ bilo koja relacija ekvivalencije na X, onda smo vidjeli da klase ekvivalencije određene tom relacijom imaju svojstva (a) – (c), dakle predstavljaju jednu dekompoziciju skupa X. Pokaži da vrijedi i obrnuto: Svaka particija skupa X prirodno definira jednu relaciju ekvivalencije na tom skupu. [Uputa: Stavi $a \sim b$ ako i samo ako a i b pripadaju istom članu dekompozicije.]

13. Pokaži: ϱ je relacija ekvivalencije na skupu X onda i samo onda ako postoji particija $\mathcal{D}$ od X takva da vrijedi

$$\varrho = \bigcup \{A^2 \subset X^2 \mid A \in \mathcal{D}\}.$$

14. Neka je S neprazan skup. Na skupu $X = \mathcal{P}(S)$ definiramo relaciju $\leq$ stavljajući $A \leq B$ ako i samo ako $A \supset B$. Pokaži da je to relacija uređaja, pa je i $(\mathcal{P}(S), \supset)$ parcijalno uređen skup. Uvjeri se, nadalje, da je relacija $\supset$ inverzna relaciji $\subset$.

15. Na skupu $X = \mathbb{R}$ definiramo relaciju $\geq$ stavljajući $a \geq b$ ako i samo ako je $a - b$ nenegativan realni broj. Onda je $(\mathbb{R}, \geq)$ totalno uređen skup, a relacija $\geq$ je inverzna relaciji $\leq$ definiranoj u tekstu. Nadalje, uz istu definiciju je i skup $(\mathbb{N}, \geq)$ totalno uređen. Je li taj skup i dobro uređen?

16. Pokaži da vrijedi i općenito: Ako je $\leq$ relacija uređaja na skupu X, onda je njoj inverzna relacija (vidi Zad. 3.) također relacija uređaja na tom skupu. Tu relaciju obično označavamo s $\geq$ i zovemo **suprotnim uređajem** od $\leq$.

17. Neka su $(X, \leq_1)$ i $(Y, \leq_2)$ totalno uređeni skupovi. Onda na $X \times Y$ definiramo relaciju $\leq$, stavljajući $(x, y) \leq (x', y')$ ako i samo ako je $x' \leq_1 x$ ili $x = x'$ i $y \leq_2 y'$. Pokaži da je $\leq$ relacija totalnog uređaja na $X \times Y$. Ta se relacija obično zove **leksikografski uređaj**.

18. Neka je $(S, \leq)$ totalno uređen skup i $X = S \times S$. Na X definiramo relaciju $\leq'$ stavljajući $(a, b) \leq' (a', b')$ ako i samo ako je $a \leq a'$ i $b \leq b'$. Pokaži da je $\leq'$ jedno parcijalno uređenje na skupu X.

19. Dokaži da je svaki podskup parcijalno (totalno) uređenog skupa također parcijalno (totalno) uređen skup, s obzirom na istu relaciju uređaja. Je li to istina i za dobro uređenje?

20. Neka je $(X, \leq)$ parcijalno (totalno) uređen skup, a $f : X \to Y$ bijekcija. Na skupu Y definiramo relaciju $\leq'$, stavljajući $a \leq' b$ ako i samo ako je $f^{-1}(a) \leq f^{-1}(b)$ u skupu X. Pokaži da je onda $(Y, \leq')$ također parcijalno (totalno) uređen skup. Primjenom te činjenice, može se na skupu $\mathbb{C}$ kompleksnih brojeva definirati jedno totalno uređenje (vidi Zad. 3. u 1.4). Bi li znao definirati direktno neki uređaj na skupu $\mathbb{C}$?

21. Neka je $(X, \leq)$ parcijalno (totalno) uređen skup. Na X definiramo novu relaciju $<$, stavljajući $a < b$ onda i samo onda ako je $a \leq b$ i $a \neq b$. Ta relacija očito nije refleksivna i, štoviše, $a < a$ nije istinito ni za jedan $a \in X$. Uvjeri se da je relacija $<$ tranzitivna. Katkad se i za tu relaciju kaže da je relacija parcijalnog (totalnog) uređaja na X. Na primjer, ako su s $\leq$ i $\geq$ označeni prirodni uređaj na $\mathbb{R}$ i njegov inverz, onda su inducirane relacije $<$ i $>$ ("*biti manji od*" i "*biti veći od*") totalni uređaji na $\mathbb{R}$ u tom novom smislu.

22. Analogno definiciji minimalnog elementa, za podskupove od $(X, \leq)$ definiraj pojam **maksimalnog** (najvećeg) elementa. Na primjer, skup $\mathbb{R}$ nema ni minimalni ni maksimalni element, a isto vrijedi za njegove podskupove $\mathbb{Z}$ i $\mathbb{Q}$. Naprotiv, $\mathbb{N}$ očito ima minimalni element, ali nema maksimalni.

23. Neka je $(X, \leq)$ totalno uređen skup, a $A \subset X$ njegov podskup. Ako A ima minimalni (maksimalni) element, on je određen jednoznačno.

24. Pojam relacije možemo generalizirati i tako da promatramo podskupove od X^n ili, još općenitije, od $X_1 \times \ldots \times X_n$. Svaki takav podskup nazivamo **n-arna relacija**. U toj terminologiji su relacije koje smo promatrali **binarne relacije**. Te su i najvažnije. Nađi primjere **ternarnih** i, općenito, n-arnih relacija.

2

GRUPE

U ovom poglavlju počinjemo s definiranjem algebarskih struktura na danom skupu određenih samo jednom binarnom operacijom. Takve su npr. grupoidi, polugrupe, monoidi i grupe.

2.1. Binarna operacija. Grupoid

Naučili smo obavljati razne računske operacije s brojevima. Pri kvadriranju $a \mapsto a^2$ npr. jednom danom broju pridružujemo novi broj, njegov kvadrat, pa takvu operaciju zovemo **unarna operacija**. Pri zbrajanju $(a, b) \mapsto a + b$ i množenju $(a, b) \mapsto ab$, uređenom paru brojeva pridružujemo novi broj, sumu, odnosno produkt, pa su to primjeri tzv. **binarnih operacija**. Slično, operaciju $(a, b, c) \mapsto a \log_b c$ zvati ćemo **ternarna**, itd.

Posve analogno mogu se definirati operacije s elementima bilo kakvih skupova. Za nas će biti od posebnog interesa binarne operacije, tj. one koje uređenom paru elemenata skupa pridružuju opet neki element tog skupa.

Točnije, neka je S dani neprazni skup. Pod **binarnom operacijom** na skupu S razumijevamo svako preslikavanje

$$\Theta : S \times S \to S$$

Kartezijeva kvadrata skupa S u skup S. Prema tome, binarna operacija svakom uređenom paru $(a, b) \in S \times S$ pridružuje neki element

$$c = \Theta(a, b) \in S$$

skupa S, koji nazivamo **rezultat** binarne operacije na paru (a, b). Kaže se, također, da je skup S zatvoren s obzirom na operaciju Θ. Uređeni par (S, Θ), koji se sastoji iz skupa S i binarne operacije Θ definirane na tom skupu, nazivamo **grupoid**.

Općenito, skup zajedno s nekim operacijama na njemu, koje mogu biti i u određenim vezama, naziva se **algebarska struktura**. Grupoid je, dakle, primjer jedne, vrlo jednostavne, algebarske strukture.

PRIMJERI

1. Neka je $S = \mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$, a binarna operacija definirana s

$$\Theta(a, b) = a + b\,,$$

koju zovemo **standardno zbrajanje**. Prema tome su ti skupovi uz tu operaciju grupoidi.

2. Neka je S kao u Prim. 1., a binarna operacija definirana s

$$\Theta(a, b) = ab\,,$$

koju zovemo **standardno množenje**. To je dobro definirana binarna operacija pa su gornji skupovi i uz tu operaciju grupoidi.

Primjećujemo da na istom skupu mogu biti definirane razne binarne operacije, čime dobivamo razne algebarske strukture. Tako su npr. $(\mathbb{N}, +)$ i $(\mathbb{N}, \cdot)$ različiti grupoidi, aditivni, odnosno multiplikativni grupoid prirodnih brojeva.

3. Skup $\mathbb{N}$ uz

$$\Theta(a, b) = a - b$$

nije grupoid, jer oduzimanje nije (dobro definirana) binarna operacija na $\mathbb{N}$. Međutim, skupovi $S = \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ u odnosu na oduzimanje jesu grupoidi.

4. Neka je S bilo koji skup, a $\mathcal{P}(S)$ njegov partitivni skup. Na $\mathcal{P}(S)$ definiramo

$$\begin{aligned}
\Theta(A, B) &= A \cup B\,, \quad \text{odnosno} \\
\Theta(A, B) &= A \cap B\,, \quad \text{odnosno} \\
\Theta(A, B) &= A - B\,, \quad \text{odnosno} \\
\Theta(A, B) &= A \,\Delta\, B = (A - B) \cup (B - A).
\end{aligned}$$

Posljednju operaciju Δ zovemo obično **simetrična diferencija** ili **simetrična razlika**. Uz svaku od tih operacija $\mathcal{P}(S)$ je grupoid.

5. Neka je S bilo koji neprazni skup, a

$$\mathcal{F}(S) = \{f \mid f : S \to S\} = S^S$$

funkcijski skup, tj. skup svih preslikavanja skupa S u sebe. Na skupu S^S promatramo binarnu operaciju

$$\Theta(f, g) = g \circ f \ ,$$

koju zovemo **standardna kompozicija**, a definirana je, kako smo već rekli, s

$$(g \circ f)(x) = g[f(x)]$$

za svaki $x \in S$. Onda je $(S^S, \circ)$ grupoid.

Spomenimo još da se u slučaju kad je skup S konačan, i nema previše elemenata, binarna operacija može zadati **tablično**, tj. pomoću **tablice množenja**:

	a_1	a_2	$\cdots$	a_n
a_1	a_1a_1	a_1a_2	$\cdots$	a_1a_n
$\vdots$	$\vdots$	$\vdots$		$\vdots$
a_n	a_na_1	a_na_2	$\cdots$	a_na_n

.

Takva se tablica zove još i **Cayleyjeva tablica** za strukturu na skupu S. Neka je npr. $S = \{a, b\}$. Onda S^S ima četiri elementa, $S^S = \{e, f, g, h\}$, gdje je

$$\begin{aligned} e(a) &= a, \quad & e(b) &= b \ , \\ f(a) &= a, \quad & f(b) &= a \ , \\ g(a) &= b, \quad & g(b) &= b \ \text{ i} \\ h(a) &= b, \quad & h(b) &= a \ . \end{aligned}$$

Grupoid $(S^S, \circ)$ možemo tada predočiti tablično ovako:

$\circ$	e	f	g	h
e	e	f	g	h
f	f	f	f	f
g	g	g	g	g
h	h	g	f	e

.

Primjećujemo da je u gornjem primjeru $e \circ e = e$, $f \circ f = f$, $g \circ g = g$. Za takve elemente grupoida kažemo da su **idempotentni**.

Umjesto funkcijske oznake $\Theta(a,b)$, rezultat binarne operacije je uobičajeno pisati kao

$$a+b\,, \quad a\cdot b\,, \quad a\circ b\,, \quad a*b\,,$$

bez obzira na to imaju li te operacije u primjerima opisano standardno značenje ili ne. U općim, apstraktnim razmatranjima se obično piše

$$\Theta(a,b)=a\cdot b=ab$$

i rezultat binarne operacije zovemo **produktom**.

Grupoid je, općenito, vrlo siromašna struktura, jer binarna operacija ne mora imati neka lijepa dodatna svojstva. Postulirajući daljnja svojstva binarne operacije, dolazimo do boljih struktura.

Neka je $(S,\cdot)$ grupoid i $a,b\in S$ bilo koji elementi. Onda će općenito biti

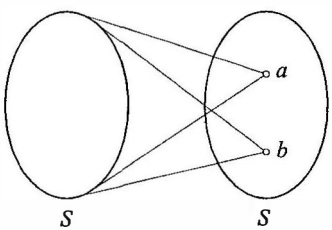
$$ab\neq ba\ .$$

Ako je iznimno $ab=ba$, onda kažemo da elementi a i b **komutiraju**. Ako je, međutim, to pravilo, tj. ako je

$$ab=ba$$

za svaki izbor $a,b\in S$, onda kažemo da je binarna operacija **komutativna**, odnosno da je grupoid $(S,\cdot)$ **komutativan ili Abelov**.

Na primjer standardno zbrajanje i množenje brojeva su komutativne operacije, dok oduzimanje to nije (ali jest $|a-b|$). Nadalje, partitivni skup je u odnosu na operaciju unije, presjeka i simetrične razlike komutativni grupoid, ali to nije s obzirom na razliku skupova. Konačno, standardno komponiranje nije komutativna operacija. To pokazuje ovaj jednostavan protuprimjer:



Neka su $f,g\in S^S$ dvije konstantne funkcije, $f(x)=a$ i $g(x)=b$, za svaki $x\in S$, te neka je $a\neq b$. Onda je za bilo koji $x\in S$

$$\left.\begin{array}{l}(g\circ f)(x)=g[f(x)]=g(a)=b\\(f\circ g)(x)=f[g(x)]=f(b)=a\end{array}\right\}\neq\ ,$$

dakle,

$$g \circ f \neq f \circ g \, .$$

ZADACI

1. U grupoidu $(S, \cdot)$ definiraj produkt od tri elementa i onda induktivno od n elemenata, za bilo koji $n \in \mathbb{N}$. [Uputa: Stavi $abc = (ab)c$.]

2. Definiraj nekoliko egzotičnih binarnih operacija na skupu $\mathbb{N}$.

2.2. Asocijativnost. Polugrupa

Neka je $(S, \cdot)$ grupoid. Za binarnu operaciju na skupu S kažemo da je **asocijativna**, ako je ispunjeno

$$a(bc) = (ab)c$$

za **svaki** izbor $a, b, c \in S$.

Grupoid s asocijativnom binarnom operacijom zovemo **asocijativni grupoid** ili **polugrupa**.

Standardno zbrajanje i množenje brojeva su asocijativne binarne operacije. Isto tako asocijativne operacije su unija i presjek u $\mathcal{P}(S)$. Oduzimanje, naprotiv, nije asocijativno,

$$(a - b) - c \neq a - (b - c) \, ,$$

pa grupoidi $(\mathbb{Z}, -)$, $(\mathcal{P}(S), -)$ nisu polugrupe. Međutim, $(S^S, \circ)$ je polugrupa jer je komponiranje preslikavanja uvijek asocijativno (Prop. 3 u 1.3.).

Zakon asocijacije omogućuje da se na jednoznačan način govori o produktu triju faktora; definiramo

$$a(bc) = (ab)c = abc$$

za bilo koje $a, b, c \in S$. Lako se vidi da je to svojstvo istinito i za više faktora. Vrijedi

PROPOZICIJA 1

Neka je $(S, \cdot)$ polugrupa, i $a, b, c, d \in S$ njezini elementi. Onda je uvijek

$$(ab)cd = a(bc)d = ab(cd) \, .$$

Dokaz

Iz prethodnog imamo redom

$$(ab)cd = [(ab)c]d = [a(bc)]d = a(bc)d\ .$$

Analogno se dokazuje druga jednakost. ■

U polugrupi ima smisla operacija **potenciranja** nekog elementa, koja ima standardna svojstva potencije. Definiramo

$$a^1 = a$$

i onda induktivno

$$a^{n+1} = a^n \cdot a, \quad \text{za } n \in \mathbb{N}\ .$$

Onda vrijedi

PROPOZICIJA 2

Neka je $(S, \cdot)$ *polugrupa i* $a \in S$. *Onda je*

(1) $a^m \cdot a^n = a^{m+n}$, *i*

(2) $(a^m)^n = a^{mn}$

za sve $m, n \in \mathbb{N}$.

Dokaz

Dokažimo (1) indukcijom. Za $n = 1$ imamo $a^m \cdot a^1 = a^m \cdot a = a^{m+1}$ po definiciji pa je tvrdnja istinita. Pretpostavimo da je (1) istinito za $n-1$, tj. da vrijedi

$$a^m \cdot a^{n-1} = a^{m+(n-1)}\ .$$

Onda imamo redom, zbog asocijativnosti i induktivne pretpostavke:

$$\begin{aligned} a^m \cdot a^n &= a^m(a^{n-1} \cdot a) = (a^m \cdot a^{n-1})a = \\ &= a^{m+(n-1)} \cdot a = a^{(m+(n-1))+1} = a^{m+n} \end{aligned}$$

i tvrdnja je dokazana. Analogno se dokazuje (2). ■

Ako je u polugrupi $(S, \cdot)$ binarna operacija još i komutativna, govorimo o **komutativnoj polugrupi**. Koje su od polugrupa u našim primjerima komutativne, a koje nisu?

ZADACI

1. Služeći se totalnom indukcijom, generaliziraj Prop. 2 na produkt od bilo kojega konačnog broja elemenata iz S, tj. dokaži da je u polugrupi produkt svake uređene n-torke elemenata jednoznačno određen, tj. neovisan o polaznom rasporedu zagrada.

2. Neka su $a, b \in \mathbb{N}$ dani brojevi, a $(\mathbb{N}, *)$ grupoid u kojem je binarna operacija definirana s
$$x * y = ax + by.$$
Odredi sve parove brojeva (a, b) za koje je $(\mathbb{N}, *)$ polugrupa. Kad je ta polugrupa komutativna?

3. Ispitaj sve moguće grupoide $(G, \cdot)$, ako je G skup koji sadrži tri elementa, tj. $G = \{a, b, c\}$. Odredi koliko je među njima komutativnih grupoida, a koliko polugrupa.

4. Definiramo binarnu operaciju $*$ na $\mathbb{R}$ s:
$$a * b = \min\{a, b\} .$$
Dokaži da je $(\mathbb{R}, *)$ komutativna polugrupa.

5. Dokaži: Ako su u komutativnoj polugrupi elementi a i b idempotentni, onda je i element $a \cdot b$ idempotentan.

2.3. Neutralni element. Monoid

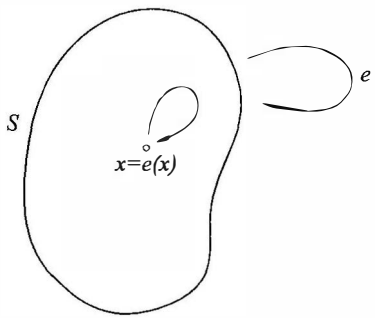
Moguće dobro svojstvo binarne operacije je posjedovanje neutralnog elementa. Neka je $(S, \cdot)$ grupoid. Ako postoji element $l \in S$ takav da vrijedi
$$la = a ,$$
za svaki $a \in S$, onda kažemo da je l **jedinica** za danu binarnu operaciju na skupu S. Analogno, ako postoji $d \in S$ sa svojstvom da je
$$ad = a ,$$
za svaki $a \in S$, onda je d **desna jedinica** za binarnu operaciju na S. Konačno, ako postoji element $e \in S$ takav da je
$$ea = ae = a ,$$
za svaki $a \in S$, tj. da je e i lijeva i desna jedinica, onda kažemo da je e **obostrana jedinica** ili samo **jedinica**, ili još **neutralni element** za danu

binarnu operaciju na S. Kaže se također da je e neutralni element grupoida $(S, \cdot)$.

U grupoidu $(\mathbb{N}, +)$ očito nema neutralnog elementa, dok je u $(\mathbb{N}, \cdot)$ to broj 1. Očito, u ostalim skupovima brojeva je 0 neutralni element s obzirom na zbrajanje, a 1 s obzirom na množenje. U partitivnom skupu $\mathcal{P}(S)$ je $\emptyset$ neutralni element za uniju, a čitav S za presjek. Konačno, u grupoidu $(S^S, \circ)$ postoji neutralni element, i to je preslikavanje

$$e : S \to S$$

definirano s $e(x) = x$, za svaki $x \in S$, koje, kako smo već spominjali, zovemo



identično preslikavanje ili **identiteta**. Zaista, za bilo koji $f \in S^S$ imamo

$$\begin{aligned} (e \circ f)(x) &= e[f(x)] = f(x)\,, \\ (f \circ e)(x) &= f[e(x)] = f(x) \end{aligned}$$

za svaki $x \in S$, dakle

$$e \circ f = f \circ e = f\,.$$

To su standardni primjeri, a evo sada i nekoliko egzotičnih. U grupoidu $(\mathcal{P}(S), -)$ je $\emptyset$ desna jedinica (jedina!), dok lijevih jedinica nema. Nadalje, neka je $(\mathbb{N}, *)$ grupoid, u kojem je binarna operacija dana zakonom

$$a * b = b^a.$$

Onda je $1 * b = b^1 = b$, tj. 1 je lijeva jedinica za tu binarnu operaciju, i to jedina, dok desnih jedinica očito nema. Konačno je $(\mathbb{N}, \circ)$ grupoid, gdje binarna operacija $\circ$ ima značenje "zaboravi drugi faktor", tj.

$$a \circ b = a.$$

Ovdje je **svaki** element od $\mathbb{N}$ desna jedinica, dok lijevih jedinica nema.

Vidimo da u grupoidu može biti i samo lijevih ili samo desnih jedinica i to jedna ili više njih. Ipak, neki red unose ove propozicije.

PROPOZICIJA 1

Neka u grupoidu $(S, \cdot)$ binarna operacija ima lijevu i desnu jedinicu. Onda su one jednake, tj. binarna operacija dopušta neutralni element.

Dokaz

Neka su $l, d \in S$ lijeva, odnosno desna jedinica. Onda je za bilo koji $a \in S$

$$la = a \quad \text{i} \quad ad = a\,,$$

dakle specijalno

$$ld = d \quad \text{i} \quad ld = l\,,$$

tj.

$$d = l\,,$$

što se i tvrdilo. ■

Odatle specijalno slijedi: Ako postoji bar jedna desna jedinica, ne može biti više od jedne lijeve jedinice, i obratno.

PROPOZICIJA 2

Ako u grupoidu $(S, \cdot)$ binarna operacija ima neutralni element, on je jedinstven.

Dokaz

Neka su $e, \overline{e} \in S$ neutralni elementi. Onda je za svaki $a \in S$

$$ea = ae = a \quad \text{i} \quad \overline{e}a = a\overline{e} = a\,,$$

dakle specijalno

$$e\overline{e} = \overline{e} \quad \text{i} \quad e\overline{e} = e\,,$$

tj.

$$e = \overline{e}.$$

■

Grupoid, u kojem je binarna operacija asocijativna i dopušta jedinicu naziva se **kvazigrupa** ili **monoid**. Drugim riječima, monoid je polugrupa s neutralnim elementom. Ako je binarna operacija i komutativna, govorimo o **komutativnomu monoidu**.

PRIMJERI

1. $(\mathbb{N}, +)$ nije monoid, ali $(\mathbb{N}_0, +)$, gdje je $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$, jest, i to komutativni. Isto tako je $(\mathbb{N}, \cdot)$ komutativni monoid.

2. $S = \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ su komutativni monoidi u odnosu na zbrajanje i u odnosu na množenje.

3. $(\mathcal{P}(S), \cup)$ i $(\mathcal{P}(S), \cap)$ su komutativni monoidi.

4. $(S^S, \circ)$ je nekomutativan monoid.

5. Neka je za dani $m \in \mathbb{N}$ sa $\mathbb{Z}_m$ označen skup

$$\mathbb{Z}_m = \{k \in \mathbb{Z} \mid 0 \leq k < m\} = \{0, 1, \ldots, m-1\} ,$$

tj. skup mogućih ostataka pri dijeljenju brojem m. Na njemu definiramo binarnu operaciju $\overset{+}{m}$ s

$$a \overset{+}{m} b = \text{ ostatak pri dijeljenju } a+b \text{ s } m .$$

To je dobro definirana binarna operacija, koja je asocijativna i ima $0 \in \mathbb{Z}_m$ za neutralni element. Operacija se zove **zbrajanje mod** m. Par $(\mathbb{Z}_m, \overset{+}{m})$ je komutativni monoid, koji se zove **aditivni monoid cijelih brojeva mod** m. Na primjer, za $m = 4$ imamo

$\overset{+}{4}$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

.

6. Na $\mathbb{Z}_m$ definiramo binarnu operaciju s

$$a \overset{\cdot}{m} b = \text{ostatak pri dijeljenju } ab \text{ s } m ,$$

koja se zove **množenje mod** m. Onda je $(\mathbb{Z}_m, \overset{\cdot}{m})$ komutativni monoid, koji se zove **multiplikativni monoid cijelih brojeva mod** m. Na primjer, za $m = 4$ imamo

$\overset{\cdot}{4}$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

.

ZADACI

1. Neka je $S = \{a, b\}$. Na tom skupu definiramo tzv. **Booleovo zbrajanje** $\oplus$ i **množenje** $\otimes$ tablicama

$\oplus$	a	b
a	a	a
b	a	b

$\otimes$	a	b
a	a	b
b	b	b

Pokaži da su $(S, \oplus)$ i $(S, \otimes)$ komutativni monoidi.

2. Neka je $(\mathbb{N}, *)$ grupoid s binarnom operacijom

$$a * b = a + b^2 .$$

Pokaži da ta binarna operacija nije ni asocijativna ni komutativna, niti ima neutralni element.

2.4. Invertibilni elementi

Neka je $(S, \cdot)$ grupoid sa svojstvom da binarna operacija ima neutralni element, kažimo e. Neka je $a \in S$ bilo koji njegov element.

Ako postoji $u \in S$ takav da vrijedi

$$u \cdot a = e ,$$

onda kažemo da je u **lijevi inverz** elementa a u grupoidu $(S, \cdot)$. Slično, ako postoji $v \in S$ takav da je

$$a \cdot v = e ,$$

onda v zovemo **desni inverz** za element a. Konačno, ako postoji element $y \in S$ takav da je

$$y \cdot a = a \cdot y = e ,$$

tj. koji je istodobno i lijevi i desni inverz, onda kažemo da je y **obostrani inverz** ili, kraće, **inverz** elementa a u strukturi $(S, \cdot)$. Ako za $a \in S$ postoji inverz, kažemo da je a **invertibilan** element u $(S, \cdot)$.

U svakom grupoidu s jedinicom ima invertibilnih elemenata. Takav je npr. sama jedinica grupoida. $(\mathbb{N}, \cdot)$ je primjer grupoida, u kojem je jedino neutralni element 1 invertibilan. U skupovima $S = \mathbb{Q}, \mathbb{R}, \mathbb{C}$ su, s obzirom na operaciju zbrajanja, invertibilni svi elementi: za $a \in S$ je inverz $-a \in S$. Međutim, u odnosu na množenje nije invertibilan $a = 0$, jer $1/a$ tada nije definiran. Što je s inverzima u skupu $\mathbb{Z}$, s obzirom na zbrajanje i množenje?

U grupoidu $(S^S, \circ)$ su invertibilna ona i samo ona preslikavanja $S \to S$, koja su bijekcije. Naime, jedino za bijekciju

$$f : S \to S$$

postoji inverzno preslikavanje

$$f^{-1} : S \to S$$

za koje vrijedi

$$f \circ f^{-1} = f^{-1} \circ f = e \,,$$

gdje je e identiteta na S. U tom grupoidu ima, međutim, i elemenata koji imaju samo lijeve, odnosno samo desne inverze. Promatrajmo npr. $(\mathbb{N}^{\mathbb{N}}, \circ)$ i preslikavanja

$$\begin{aligned} f(n) &= n+1 \,, \\ g(n) &= \begin{cases} n-1, & n \geq 2 \\ 1, & n = 1 \end{cases} . \end{aligned}$$

Onda je

$$(g \circ f)(n) = g(f(n)) = g(n+1) = n$$

za svaki n, pa je

$$g \circ f = e \,,$$

što pokazuje da je g lijevi inverz za f, a f desni inverz za g. Međutim, f nema desnog inverza niti g lijevog; posebno, **nije**

$$f \circ g = e \,,$$

kako bi se moglo očekivati. Provjeri!

Ljepše ponašanje pokazuju lijevi odnosno desni inverzi, te invertibilni elementi kad je binarna operacija u grupoidu i asocijativna, tj. u monoidu. Tada vrijedi

PROPOZICIJA 1

Neka je $(S, \cdot)$ monoid, i $a \in S$ njegov element. Ako a ima lijevi i desni inverz, oni su nužno jednaki, tj. element a je invertibilan.

Dokaz

Neka je lijevi inverz označen s u, a desni s v. Zbog asocijativnosti je jednoznačno određen trostruki produkt uav. Imamo

$$\left.\begin{aligned} uav &= (ua)v = ev = v \\ uav &= u(av) = ue = u \end{aligned}\right\} =$$

tj. $v = u$. ■

Odatle, naravno, slijedi da, ako postoji desni inverz, ne može biti više od jednog lijevog inverza i obratno.

PROPOZICIJA 2

Neka je $(S, \cdot)$ monoid, a $a \in S$ njegov element. Ako je a invertibilan, njegov inverz je jedinstven.

Dokaz

Neka su $y, \overline{y} \in S$ inverzi od a. Vrijedi dakle

$$\begin{aligned} ya &= ay = e\,, \\ \overline{y}a &= a\overline{y} = e\,. \end{aligned}$$

Kako je binarna operacija u monoidu asocijativna, imamo

$$\begin{aligned} ya\overline{y} &= (ya)\overline{y} = e\overline{y} = \overline{y} \\ ya\overline{y} &= y(a\overline{y}) = ye = y\,, \end{aligned}$$

dakle $\overline{y} = y$, što se i tvrdilo. ■

Ako je u monoidu binarna operacija označena multiplikativno, jedinstveni inverz invertibilnog elementa a označavamo s a^{-1} i zovemo **recipročni element** od a. Ako je pak binarna operacija označena aditivno, jedinstveni inverz od a označavamo s $-a$, i zovemo **suprotni element** od a.

ZADACI

1. Neka je $(\mathbb{R}, *)$ grupoid s binarnom operacijom

$$a * b = a + b - 2a^2b^2\,.$$

Pokaži:

(a) binarna operacija je komutativna, ali nije asocijativna,

(b) 0 je neutralni element za tu operaciju,

(c) svaki $x > -1/2$ ima dva inverza,

(d) nijedan $x < -1/2$ nema inverza, i

(e) $x = -1/2$ ima jedinstveni inverz.

Prema tome, ako inverz nekog elementa i postoji, on nije nužno jedinstven.

2. Promatraj strukturu $(\mathbb{Q}, *)$, gdje je binarna operacija definirana s

$$a * b = a + b - ab.$$

Koja svojstva ima taj grupoid? Što se može reći o invertibilnosti elemenata?

2.5. Grupa

Koristeći se prethodno definiranim pojmovima, nije teško definirati grupu. **Grupa** je **monoid u kojem je svaki element invertibilan**.

Neovisno o ranijim pojmovima, grupu definiramo na ovaj način: Uređeni par $(G, \cdot)$, koji se sastoji iz nepraznog skupa G i binarne operacije

$$\cdot : G \times G \to G$$

nazivamo **grupa**, ako su ispunjeni ovi uvjeti:

(1) binarna operacija je asocijativna, tj. vrijedi

$$(ab)c = a(bc), \quad \text{za svaki } a, b, c \in G\ ;$$

(2) za binarnu operaciju postoji i jednoznačno je određen neutralni element, tj. $e \in G$ sa svojstvom

$$ea = ae = a, \quad \text{za svaki } a \in G\ ;$$

(3) svaki je element invertibilan, tj. za svaki $a \in G$ postoji i jednoznačno je određen $a^{-1} \in G$ sa svojstvom

$$aa^{-1} = a^{-1}a = e\ .$$

Ako je ispunjen i dodatni zahtjev

(4) binarna operacija je komutativna, tj. vrijedi

$$ab = ba, \quad \text{za svaki } a, b \in G\ ,$$

onda kažemo da je grupa $(G, \cdot)$ **komutativna ili Abelova**. Za grupu kažemo da je **konačna** ili **beskonačna**, već prema tome ima li skup G konačno ili beskonačno mnogo elemenata. Kardinalni broj skupa G nazivamo **red grupe**.

Uvjeti (1) – (3) nazivaju se i **aksiomi grupe**. Primijetimo odmah da taj sustav aksioma nije nezavisan, jer sadrži i tvrdnje koje se mogu dokazati. Odmah npr. primjećujemo da je suvišno zahtijevati jedinstvenost neutralnog elementa i jedinstvenost inverza, jer smo pokazali da su oni uvijek jedinstveni, ako postoje. Ta je definicija međutim prikladnija za praktičnu upotrebu; postulirane tvrdnje ne treba dokazivati. Kasnije ćemo se vratiti na to pitanje i popisati minimalne zahtjeve koji karakteriziraju grupu.

Kažimo i ovo. Ako je binarna operacija zapisana multiplikativno, govorimo o **multiplikativnoj grupi**, neutralni element zovemo **jedinica**, a inverz, kako smo već rekli, **recipročnim elementom**. Ako je pak binarna operacija označena aditivno, govorimo o **aditivnoj grupi** i tada neutralni element zovemo **nula** grupe, a inverz **suprotnim elementom**. Običaj je da se u teorijskoj obradi komutativne grupe zapisuju aditivno.

Kad god ne bude razloga za konfuziju, mi ćemo u oznaci $(G, \cdot)$ za grupu ispuštati binarnu operaciju, pa pisati i govoriti jednostavno o grupi G.

Navest ćemo sada nekoliko jednostavnih posljedica definicije grupe.

PROPOZICIJA 1

U grupi se može "skraćivati", tj. za svaki izbor $a, b, c \in G$, sljedeće su tvrdnje ekvivalentne:

(1) $a = b$;

(2) $ca = cb$;

(3) $ac = bc$.

Dokaz

Jasno je da (1) $\Rightarrow$ (2) i (1) $\Rightarrow$ (3). To je istina već u grupoidu ("proširivanje"). Pokažimo npr. da (2) $\Rightarrow$ (1). Kako je G grupa, za dani c postoji jedinstveni c^{-1}, pa imamo redom, množeći (2) s c^{-1} i primjenjujući aksiome grupe

$$\begin{aligned} c^{-1}(ca) &= c^{-1}(cb) \\ (c^{-1}c)a &= (c^{-1}c)b \\ ea &= eb \\ a &= b\,. \end{aligned}$$

Analogno se vidi da (3) $\Rightarrow$ (1). ■

PROPOZICIJA 2

Neka je G grupa i $a, b \in G$. Onda je

$$(ab)^{-1} = b^{-1}a^{-1}\,.$$

Dokaz

Kako je $(ab)^{-1}$ inverz od ab, vrijedi

$$(ab)(ab)^{-1} = (ab)^{-1}(ab) = e\,.$$

U drugu ruku je

$$\begin{aligned}(ab)(b^{-1}a^{-1}) &= a(bb^{-1})a^{-1} = aea^{-1} = aa^{-1} = e\\ (b^{-1}a^{-1})(ab) &= b^{-1}(a^{-1}a)b = b^{-1}eb = b^{-1}b = e\end{aligned}$$

pa je

$$b^{-1}a^{-1} = (ab)^{-1}$$

zbog jedinstvenosti inverza. ■

PROPOZICIJA 3

Neka je G grupa i $a \in G$. Onda je

$$(a^{-1})^{-1} = a\,.$$

Dokaz

$(a^{-1})^{-1}$ je inverz od a^{-1} pa imamo

$$a^{-1}(a^{-1})^{-1} = (a^{-1})^{-1}a^{-1} = e\,.$$

No, također je

$$a^{-1}a = aa^{-1} = e$$

pa je

$$(a^{-1})^{-1} = a$$

zbog jedinstvenosti inverza. ■

Neka je $a \in G$ bilo koji element grupe. Već smo prije (kod polugrupa) definirali pojam potencije a^n tog elementa za svaki $n \in \mathbb{N}$. Sada bismo željeli tu definiciju proširiti na sve $n \in \mathbb{Z}$. Stavljamo

$$\begin{aligned}a^0 &= e\,, \qquad \text{za } n = 0\,,\\ a^n &= (a^{-n})^{-1}\,, \qquad \text{za } n < 0\,,\end{aligned}$$

što ima smisla, jer je $-n > 0$. Uz taj dogovor vrijedi

PROPOZICIJA 4

Neka je $a \in G$ bilo koji element grupe. Onda je

(1) $a^m \cdot a^n = a^{m+n}$;

(2) $(a^m)^n = a^{mn}$,

za svaki izbor $m, n \in \mathbb{Z}$.

Dokaz

Za $m, n > 0$ tvrdnju smo dokazali u Prop.2 u 2.2. I ostale mogućnosti se lako dokazuju služeći se upravo navedenom definicijom. ■

Primijetimo da, iz (2), za $m = -1$ specijalno vrijedi

$$(a^{-1})^n = a^{-n} = (a^n)^{-1} .$$

Neka je $a \in G$ bilo koji element grupe. Promatrajmo skup svih njegovih potencija

$$\{\ldots a^{-2}, a^{-1}, a^0, a^1, a^2, \ldots\} .$$

Ako među tim potencijama nema jednakih, kažemo da je element a **beskonačnog reda**. Ako pak među potencijama ima jednakih, ako je npr. za $k \neq l$

$$a^k = a^l ,$$

onda je prema Prop. 4

$$a^{k-l} = e.$$

Postoje, dakle, netrivijalne potencije od a, koje su jednake jedinici grupe. Kažemo u tom slučaju da je element a **konačnog reda**.

Neka je $n \in \mathbb{N}$ najmanji **prirodni broj** s gornjim svojstvom, tj. takav da je

(1) $a^n = e$

(2) $a^k = e$ i $k \in \mathbb{N}$ povlači $k \geq n$.

Onda kažemo da je n **red elementa** a.

Očito, u svakoj je grupi neutralni element jedinstveni element reda 1. Nadalje, jasno je da su u konačnoj grupi svi elementi konačnog reda. No, to može biti slučaj i kod beskonačnih grupa. Grupa u kojoj su svi elementi konačnog reda zove se **periodična**.

PROPOZICIJA 5

Neka je $a \in G$ *element reda* n. *Onda među potencijama od* a *ima točno* n *različitih, i to su*

$$e, a, a^2, \ldots, a^{n-1} .$$

Dokaz

Najprije, iz definicije reda elementa je jasno da su sve navedene potencije različite. Nadalje, ako je $k \in \mathbb{Z}$ bilo koji broj, imamo

$$k = qn + r, \qquad 0 \leq r \leq n-1$$

i onda, zbog Prop. 4,

$$a^k = (a^n)^q \cdot a^r = a^r \ ,$$

a to je jedna od navedenih potencija, jer je $0 \leq r \leq n-1$ po pretpostavci. ■

Iz dokaza Prop. 5 odmah slijedi

KOROLAR 6

Neka je $a \in G$ reda n. Onda je $a^k = e$ ako i samo ako je k djeljiv s n.

■

ZADACI

1. Generaliziraj tvrdnju Prop. 2, tj. dokaži, da za bilo koji izbor $a_1, a_2, \ldots$ $\ldots, a_n \in G$ vrijedi

$$(a_1 \cdot a_2 \cdot \ldots \cdot a_n)^{-1} = a_n^{-1} \cdot \ldots \cdot a_2^{-1} \cdot a_1^{-1} \ .$$

2. Dokaži: U grupi je jedini idempotentni element njezina jedinica.

3. Elemente reda 2 u grupi zovemo **involutorni**. Nađi involutorne elemente u poznatim primjerima grupa (vidi i točku 2.8.).

2.6. Alternativne definicije grupe

Kako smo rekli, aksiomi u definiciji grupe nisu nezavisni. Sljedeći teorem nam daje minimalne uvjete uz koje je neka struktura grupa.

TEOREM 1

Polugrupa $(G, \cdot)$ je grupa ako i samo ako su ispunjeni ovi zahtjevi:

(1) *postoji bar jedna lijeva jedinica,*

(2) *neka od lijevih jedinica e ima svojstvo da za svaki $a \in G$ postoji $u \in G$ takav da je*

$$ua = e \ .$$

Dokaz

Nužnost je očigledna. Dovoljnost: ako su ispunjeni uvjeti (1) i (2), polugrupa G je grupa. Očito je dovoljno dokazati egzistenciju neutralnog elementa, kao i egzistenciju inverza za svaki element iz G, jer smo jedinstvenost pokazali već prije (Prop. 2 u 2.3. i Prop. 2 u 2.4.).

Neka je $a \in G$ bilo koji element. Po pretpostavci postoji $u \in G$ takav da je

$$ua = e\ .$$

Također, po pretpostavci postoji $v \in G$ takav da je

$$vu = e\ .$$

Zbog asocijacije u G imamo onda redom

$$au = e(au) = (vu)(au) = v(ua)u = v(eu) = vu = e\ ,$$

dakle

$$au = e = ua\ .$$

Kad bi e bio neutralni element u polugrupi, imali bismo zaključak da je u inverz od a. No,

$$ae = a(ua) = (au)a = ea = a\ ,$$

tj. e je zaista i desna jedinica, dakle neutralni element. Time je dokazano da je G grupa. ■

NAPOMENA 2

Posve analogno, u teoremu se mogla pretpostaviti egzistencija desne jedinice kao i egzistencija desnog inverza u odnosu na neku od jedinica.

Važno je međutim primijetiti da promijenjeni uvjeti u tom smislu da se postulira egzistencija **desne** jedinice, ali **lijevog** inverza u odnosu na neku takvu jedinicu, ili obratno, više ne karakteriziraju grupu. Na primjer, polugrupa $(S, *)$, gdje je $a * b = a$, zadovoljava očigledno sve uvjete, jer je svaki $b \in S$ desna jedinica, i nadalje, za bilo koji b kao jedinicu je $b * a = b$, tj. b je lijevi inverz za a, a $(S, *)$, naravno, nije grupa. ■

Dat ćemo sada još jednu korisnu karakterizaciju grupe. Neka je $(S, \cdot)$ grupoid i $a, b \in S$. Ako postoji $x \in S$ takav da je

$$ax = b\ , \tag{1}$$

onda kažemo da je x rješenje "jednadžbe" (1), odnosno da je (1) rješiva u strukturi $(S, \cdot)$. Općenito, rješenja jednadžbi u grupoidu ne moraju postojati, a ako postoje, ne moraju biti jedinstvena. Tako npr. u navedenoj polugrupi $(S, *)$ jednadžba $a * x = b$ nema rješenja za $b \neq a$, dok je u slučaju $a * x = a$ rješenje svaki $x \in S$.

TEOREM 3

Polugrupa $(G, \cdot)$ je grupa ako i samo ako su za svaki izbor elemenata $a, b \in G$ jednadžbe

$$ax = b \quad i \quad ya = b \tag{2}$$

rješive u G.

Dokaz

Nužnost: ako je G grupa, jednadžbe (2) su rješive. Po pretpostavci postoji $a^{-1} \in G$ pa iz $(2)_1$ imamo redom

$$\begin{aligned} a^{-1}(ax) &= a^{-1}b \text{ , tj.} \\ (a^{-1}a)x &= a^{-1}b \text{ , tj.} \\ ex &= a^{-1}b \text{ i otuda} \\ x &= a^{-1}b \text{ ,} \end{aligned}$$

tj. $(2)_1$ ima rješenje. Analogno se vidi da je

$$y = ba^{-1}$$

rješenje za $(2)_2$.

Dovoljnost: ako jednadžbe (2) imaju rješenja za svaki $a, b \in G$, onda je G grupa. Po pretpostavci, postoji dakle rješenje jednadžbe

$$ya = a \text{ .}$$

Označimo ga s $y = e$. Tvrdimo da je e lijeva jedinica za danu binarnu operaciju. Zaista, ako je $b \in G$ bilo koji element, imamo po pretpostavci $x \in G$ takav da je

$$ax = b \text{ .}$$

No, onda zbog asocijativnosti u polugrupi imamo

$$eb = e(ax) = (ea)x = ax = b \text{ ,}$$

tj. e je zaista lijeva jedinica.

Neka je sada $a \in G$ bilo koji element. Onda po pretpostavci postoji $x = u$, koji je rješenje jednadžbe

$$xa = e$$

("lijevi inverz"). Tako smo u uvjetima Tm. 1 pa zaključujemo da je G grupa. ■

KOROLAR 4

U grupi, jednadžbe

$$\begin{aligned} ax &= b\,, \\ ya &= b \end{aligned}$$

imaju jedinstvena rješenja, za svaki $a, b \in G$.

Dokaz

Egzistencija rješenja je dokazana u Tm. 3. Pokažimo jedinstvenost. Kad bi $x_1, x_2 \in G$ bila rješenja od $ax = b$, imali bismo

$$ax_1 = ax_2\,.$$

Odatle skraćivanjem (vidi Prop. 1 u 2.5.) dobivamo $x_1 = x_2$. ■

ZADACI

1. Dokaži ili opovrgni: Polugrupa $(G, \cdot)$ je grupa, ako za svaki $a, b \in G$ jednadžba
$$ax = b$$
ima rješenje u G.

2.7. Podgrupa

Važan je pojam podstrukture za neku zadanu strukturu, tj. podskupa koji je i sam struktura.

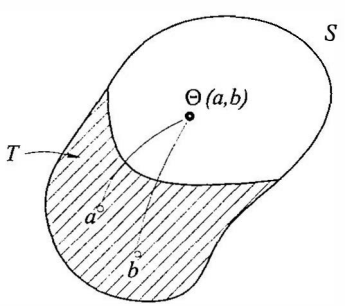
Neka je (S, Θ) grupoid i $T \subset S$ podskup od S. Neka je

$$\Theta/_{T\times T} : T \times T \to S$$

restrikcija binarne operacije Θ na skup T. Ako je

$$\Theta(T \times T) \subset T,$$

onda kažemo da je T **zatvoren** u S s obzirom na binarnu operaciju Θ, ili



također, da je T **stabilan** u S u odnosu na Θ. Primijetimo da je u tom

slučaju $\overline{\Theta} = \Theta/_{T\times T}$ dobro definirana binarna operacija na T i, prema tome, je par $(T, \overline{\Theta})$ grupoid. Za taj grupoid kažemo da je **podgrupoid** od (S, Θ). Ako $(T, \overline{\Theta})$ ima odgovarajuća dodatna svojstva, govorimo o **potpolugrupi** odnosno **podmonoidu** polazne strukture (S, Θ). Na primjer, $(\mathbb{N}, +)$ je potpolugrupa monoida $(\mathbb{N}_0, +)$, $\mathbb{Z} \subset \mathbb{Q}$ je podmonoid multiplikativnog monoida $\mathbb{Q}$, itd.

Posve analogno definiramo pojam podgrupe. Neka je $(G, \cdot)$ grupa, a $H \subset G$ podskup, koji je zatvoren u G s obzirom na množenje u grupi. Ako je podgrupoid $(H, \cdot)$ grupa, onda kažemo da je to **podgrupa** od $(G, \cdot)$. Drugim riječima, neprazni podskup $H \subset G$ je podgrupa od G, ako je H i sam grupa u odnosu na istu binarnu operaciju, koja čini G grupom. Ako je H podgrupa od G, pišemo obično $H < G$.

Na primjer neka je $2\mathbb{Z} \subset \mathbb{Z}$ podskup od $\mathbb{Z}$ definiran sa

$$2\mathbb{Z} = \{2n \mid n \in \mathbb{Z}\} .$$

Onda je $(2\mathbb{Z}, +)$ podgrupa grupe $(\mathbb{Z}, +)$. Nadalje, neka je za dani skup S, $B \subset S^S$ podskup definiran s

$$B = \{f \in S^S \mid f \text{ je bijekcija}\} .$$

Onda je $(B, \circ)$ podgrupa monoida $(S^S, \circ)$. Konačno, neka je označeno $\mathbb{R}^+ = \{x \in \mathbb{R} \mid x > 0\}$. Onda je $\mathbb{R}^+ \subset \mathbb{R}$ i $(\mathbb{R}^+, \cdot)$ je grupa, ali nije podgrupa od $(\mathbb{R}, +)$, jer se ne radi o istoj binarnoj operaciji.

Svaka grupa ima podgrupe. Trivijalne podgrupe su $H = \{e\}$ i $H = G$. Ostale podgrupe od G nazivamo **prave podgrupe**. Kako se pokazuje, svaka beskonačna grupa ima sigurno pravih podgrupa, dok kod konačnih grupa to ne mora biti. Na primjer, ako je red grupe prim broj, takva grupa nema pravih podgrupa. To ćemo kasnije dokazati.

PROPOZICIJA 1

Neka je G grupa i $K \subset H \subset G$. Ako je $K < H$ i $H < G$, onda je $K < G$. Drugim riječima, relacija $<$ tj. relacija "biti podgrupa" je tranzitivna na $\mathcal{P}(G)$ (i naravno, refleksivna, te antisimetrična, pa je to jedna relacija parcijalnog uređaja na $\mathcal{P}(G)$).

Dokaz

Trivijalan. ■

Navest ćemo sada nekoliko karakterizacija podgrupe, tj. kriterija koji omogućuju, da se među podskupovima neke grupe prepoznaju podgrupe.

TEOREM 2

Neprazan podskup $H \subset G$ grupe G je podgrupa od G ako i samo ako su ispunjeni ovi uvjeti:

(1) *za svaki* $a, b \in H$ *je* $ab \in H$;

(2) *za svaki* $a \in H$ *je* $a^{-1} \in H$.

Dokaz

Nužnost: trivijalna, zbog jedinstvenosti neutralnog elementa i inverza.

Dovoljnost: neka je $a \in H$ bilo koji element. Onda je zbog (2) također $a^{-1} \in H$, i nadalje, zbog (1) i $aa^{-1} \in H$, dakle $e \in H$. Kako je asocijativnost naslijeđena iz G, H je grupa, dakle podgrupa od G. ■

Gornja dva uvjeta možemo objediniti, pa imamo

TEOREM 3

Neprazan podskup $H \subset G$ *grupe* G *je podgrupa od* G *onda i samo onda ako je za svaki izbor* $a, b \in H$ *i* $ab^{-1} \in H$.

Dokaz

Nužnost: očigledna.

Dovoljnost: neka je $a \in H$ bilo koji element. Onda je po pretpostavci $aa^{-1} \in H$, dakle $e \in H$. Nadalje, iz $e, a \in H$ slijedi $ea^{-1} \in H$, tj. $a^{-1} \in H$. Konačno, za bilo koje $a, b \in H$ imamo najprije, prema prethodnom, $b^{-1} \in H$, a onda i $a(b^{-1})^{-1} \in H$ tj. $ab \in H$. Kako je asocijativnost naslijeđena iz G, H je grupa, dakle podgrupa od G. ■

Neka su $S, T \subset G$ podskupovi grupe G. Onda uvodimo sljedeće oznake:

$$\begin{aligned} S^{-1} &= \{a^{-1} \mid a \in S\} \\ ST &= \{ab \mid a \in S, b \in T\} . \end{aligned}$$

U ovim oznakama se prethodni teorem može elegantnije formulirati kao

KOROLAR 4

Neprazni podskup $H \subset G$ *grupe* G *je podgrupa od* G *ako i samo ako je*

$$HH^{-1} \subset H .$$

■

Unija dviju podgrupa grupe G ne mora biti podgrupa od G. Imamo međutim

TEOREM 5

Neka su $H_1, H_2 < G$ *podgrupe od* G. *Onda je* $H_1 \cap H_2$ *također podgrupa od* G.

Dokaz

Neka je $a, b \in H_1 \cap H_2$ bilo koji par elemenata. Na osnovi Tm. 3 dovoljno je pokazati da je $ab^{-1} \in H_1 \cap H_2$. No, iz pretpostavke slijedi da je $a, b \in H_1$, pa je onda i $ab^{-1} \in H_1$, jer je H_1 grupa. Isto tako, iz $a, b \in H_2$ slijedi da je $ab^{-1} \in H_2$, jer je H_2 grupa. Dakle je $ab^{-1} \in H_1 \cap H_2$, što je i trebalo dokazati. ■

Slično se vidi da je presjek bilo koje familije, konačne ili beskonačne, podgrupâ od G opet podgrupa od G. Točnije, ako je A neki skup indeksa i $H_\alpha < G$ podgrupa od G za svaki $\alpha \in A$, onda je

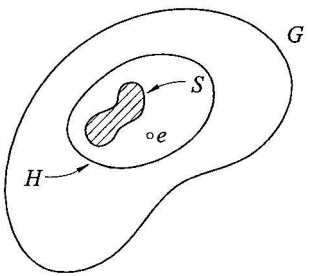
$$\bigcap_{\alpha \in A} H_\alpha$$

podgrupa od G.

Neka je sada $S \subset G$ podskup grupe G. Onda je S sigurno sadržan u nekoj podgrupi od G, npr. u grupi G samoj. Neka je s H označen presjek svih podgrupa od G, koje sadrže S, tj.

$$H = \bigcap_{\alpha} H_\alpha, \quad S \subset H_\alpha, \quad \text{za svaki } \alpha \in A\,.$$

Prema prethodnoj napomeni, H je podgrupa od G. Kažemo da je H pod-



grupa **generirana skupom** S i pišemo

$$H = [S]\,.$$

Ako je S već podgrupa od G, onda je naravno $[S] = S$. Očito, H je najmanja podgrupa od G koja sadrži S, tj. iz činjenice da je $S \subset K$ i K podgrupa u G, slijedi da je $H < K$.

U slučaju kad je $[S] = G$, kažemo još da je S **skup generatora** ili **izvodnica** za grupu G. Na primjer, grupa $(\mathbb{Z}, +)$ je generirana skupom $S = \{1\}$, dok je multiplikativna grupa $(\mathbb{Q}^+, \cdot)$ svih pozitivnih racionalnih brojeva generirana skupom svih prim brojeva.

Općenito, vrijedi ovaj

TEOREM 6

Neka je S skup generatora za grupu G. Onda se svaki element iz G može prikazati kao produkt od konačno mnogo elemenata iz $S \cup S^{-1}$.

Dokaz

Neka je $K \subset G$ skup svih elemenata od G, koji se ne mogu prikazati kao produkt od konačno mnogo elemenata iz $S \cup S^{-1}$. Neka je

$$H = G - K .$$

Pokažimo da je H podgrupa od G. Zaista, za $a, b \in H$ imamo

$$a = x_1 x_2 \cdots x_r$$

$$b = y_1 y_2 \cdots y_s ,$$

gdje su $x_i, y_j \in S \cup S^{-1}$. No, onda je

$$ab^{-1} = x_1 x_2 \cdots x_r y_s^{-1} \cdots y_2^{-1} y_1^{-1} ,$$

dakle $ab^{-1} \in H$, pa je H podgrupa. Nadalje, očito je $S \subset H$. Iz definicije od $[S]$ onda slijedi da je $[S] \subset H$. Ali, po pretpostavci je $[S] = G$, pa je $G \subset H$ i onda $G = H = G - K$, odakle zaključujemo da je $K = \emptyset$. ∎

Kažemo da je grupa G **ciklička**, ako je generirana jednim jedinim elementom, tj. ako postoji $a \in G$ sa svojstvom da je $[\{a\}] = G$. Element a je onda generator za G, pa iz Tm. 6 zaključujemo da je svaki $x \in G$ oblika $x = a^m$, $m \in \mathbb{Z}$. Ako je a beskonačnog reda, grupa G je nužno beskonačna, i zovemo ju **beskonačna ciklička grupa**. Ako je pak generator a reda n, prema Prop. 5 u 2.5. je G konačna grupa i ima točno n elemenata, pa govorimo o **cikličkoj grupi reda** n. Na primjer, $(\mathbb{Z}, +)$ i $(\mathbb{Z}_n, \overset{+}{}_n)$ su cikličke grupe, obje generirane s elementom 1. Prva od njih je beskonačna, a druga reda n.

Neka je sada G bilo koja grupa i $a \in G$ njezin element. Neka je $H = [\{a\}]$ podgrupa od G generirana s a. Onda je H po definiciji ciklička grupa, koju zovemo **ciklička podgrupa od G generirana s a.**

ZADACI

1. Neka je M monoid, a $I = I(M)$ skup svih invertibilnih elemenata u M. Pokaži da je $I \subset M$ podgrupa od M.

2. Neka je $G_m < \mathbb{Z}_m$ podgrupa multiplikativnog monoida od $\mathbb{Z}_m$, koja se sastoji od svih elemenata invertibilnih u $\mathbb{Z}_m$. Pokaži da se G_m sastoji od svih elemenata iz $\mathbb{Z}_m$, koji su relativno prosti s m.

3. Neka je $r(m)$ red grupe G_m. Onda je

$$a^{r(m)} \equiv 1 (\mathrm{mod}\, m)$$

za svaki a, koji je relativno prost s m. To je poznati **Euler-Fermatov teorem** (za definiciju relacije kongruencije $\equiv$ vidi Zad.7. u 3.7.).

4. Neka je $S \subset G$ podskup grupe G. Neka je sa $C(S)$ označen skup svih onih elemenata iz G koji komutiraju sa svim elementima iz S, tj.

$$C(S) = \{a \in G \mid as = sa, \quad \text{za svaki} \quad s \in S\} .$$

Pokaži da je $C(S)$ podgrupa od G. Ta se podgrupa zove **centralizator** skupa S u G. Specijalno, za $S = G$, podgrupu $C(G)$ od G nazivamo **centar** grupe G.

5. Neka je G Abelova grupa, a $H \subset G$ njezina podgrupa. Definiramo

$$K(H) = \{a \in G \mid a^2 \in H\} .$$

Pokaži da je $K(H)$ podgrupa od G.

6. Neka je $S \subset G$ podskup grupe G. Za $a \in G$ definiramo

$$\begin{aligned} aS &= \{as \mid s \in S\} \\ Sa &= \{sa \mid s \in S\} . \end{aligned}$$

Neka je

$$N(S) = \{a \in G \mid aS = Sa\} .$$

Pokaži da je $N(S)$ podgrupa od G. Ta se podgrupa zove **normalizator** od S u G.

7. Neka je $S \subset G$ podskup grupe G sa svojstvom da njegovi elementi komutiraju međusobno. Pokaži da je $[S]$ komutativna podgrupa od G.

8. Za svaki uređeni par $x, y \in G$ definiramo produkt

$$[x, y] = xyx^{-1}y^{-1} \in G ,$$

koji nazivamo **komutator** para x, y. Neka je

$$K = \{[x, y] \mid x, y \in G\} .$$

Onda je $[K]$ podgrupa od G, koja se naziva **komutatorska podgrupa**. Što možeš reći o K, ako je G Abelova?

9. Neka je G ciklička grupa generirana s $a \in G$, koji je reda n. Onda je grupa G reda n (vidi Prop. 5 iz 2.5.).

10. Dokaži: Svaka podgrupa cikličke grupe i sama je ciklička grupa. Nadalje, ako je grupa beskonačna i ciklička, takve su i njezine podgrupe.

11. Dokaži ovaj teorem: Svaka beskonačna grupa ima pravih podgrupa. [Skica dokaza: Uzmi $a \neq e$. Neka je $H = [a]$ ciklička podgrupa od G generirana s a. Ako je a konačnog reda, H je konačna, dakle $H \neq G$. Ako je pak a beskonačnog reda, promatramo

$$K = \{\ldots a^{-2}, e, a^2, a^4, \ldots\} \subset H\ .$$

K je beskonačna podgrupa od G, ali je sigurno $K \neq G$. Naime, $a \notin K$, jer bi $a \in K$ povlačilo $a = a^{2s}$, dakle $a^{2s-1} = e$, protivno pretpostavci da je a beskonačnog reda.]

2.8. Primjeri grupa

Radi boljeg razumijevanja pojma grupe navest ćemo sada mnoštvo raznih primjera grupa. Provjeru grupovnosti ostavljamo čitaocu.

1. Aditivni monoidi $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ su komutativne grupe i vrijedi

$$\mathbb{Z} < \mathbb{Q} < \mathbb{R} < \mathbb{C}\ .$$

Polugrupa $\mathbb{N}$ nije, dakako, grupa.

2. Multiplikativni monoidi $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ nisu, dakako, grupe. Međutim, podmonoidi

$$\begin{aligned}
\mathbb{Q}^* &= \mathbb{Q} - \{0\} \subset \mathbb{Q}\ , \\
\mathbb{Q}^+ &= \{q \in \mathbb{Q} \mid q > 0\} \subset \mathbb{Q}\ , \\
\mathbb{R}^* &= \mathbb{R} - \{0\} \subset \mathbb{R}\ , \\
\mathbb{R}^+ &= \{x \in \mathbb{R} \mid x > 0\} \subset \mathbb{R}\ , \\
\mathbb{C}^* &= \mathbb{C} - \{0\} \subset \mathbb{C}
\end{aligned}$$

jesu komutativne grupe. Pritom vrijedi

$$\begin{array}{ccccc}
\mathbb{Q}^+ < \mathbb{R}^+ & < & \mathbb{R}^* & < & \mathbb{C}^* \\
 & & \vee & & \\
 & \mathbb{Q}^+ & < & \mathbb{Q}^* &
\end{array}\ .$$

3. Neka je $k \in \mathbb{Z}$ dani broj, a

$$k\mathbb{Z} = \{kn \mid n \in \mathbb{Z}\} .$$

Onda je $(k\mathbb{Z}, +)$ komutativna grupa i $k\mathbb{Z} < \mathbb{Z}$. Interesantno je spomenuti da su to jedine podgrupe od $\mathbb{Z}$. Specijalno, $\mathbb{Z}$ nema konačnih podgrupa, osim trivijalne. Primijetimo da je $k\mathbb{Z}$ aditivna grupa i za k racionalan, realan ili kompleksan broj. Na primjer, $\frac{1}{3}\mathbb{Z}$, $\sqrt{2}\mathbb{Z}$, $\pi\mathbb{Z}$ i $i\mathbb{Z}$ su također grupe.

4. $(\mathbb{Z}_m, \overset{+}{m})$ je komutativna grupa za svaki $m \in \mathbb{N}$, i to reda m. Primjer pokazuje da postoje grupe svakoga konačnog reda. Grupa je ciklička. Naprotiv, multiplikativni monoid $(\mathbb{Z}_m, \overset{\cdot}{m})$ nije grupa za $m > 1$.

5. Neka je

$$\mathbb{R}^n = \underbrace{\mathbb{R} \times \cdots \times \mathbb{R}}_{n} = \{(x_1, \ldots, x_n) \mid x_i \in \mathbb{R}\}$$

skup svih uređenih n-torki realnih brojeva. Uz uobičajeno, koordinatno zbrajanje

$$\begin{aligned} x + y &= (x_1, \ldots, x_n) + (y_1, \ldots, y_n) = \\ &= (x_1 + y_1, \ldots, x_n + y_n) \quad , \end{aligned}$$

$\mathbb{R}^n$ je Abelova grupa. Uz uobičajenu identifikaciju

$$(x_1, \ldots, x_{n-1}) \equiv (x_1, \ldots, x_{n-1}, 0)$$

imamo

$$\mathbb{R}^{n-1} < \mathbb{R}^n .$$

Isto tako, grupe su $\mathbb{Z}^n, \mathbb{Q}^n$ i $\mathbb{C}^n$ i, dakako, vrijedi

$$\mathbb{Z}^n < \mathbb{Q}^n < \mathbb{R}^n < \mathbb{C}^n .$$

6. Neka je

$$S^1 = \{z \in \mathbb{C} \mid |z| = 1\} = \{e^{it} \mid t \in \mathbb{R}\} .$$

Uz uobičajeno množenje kompleksnih brojeva to je grupa i, naravno,

$$S^1 < \mathbb{C}^* .$$

Kako u kompleksnoj ravnini brojevi z s navedenim svojstvom leže na kružnici polumjera 1, grupu S^1 nazivamo **grupa kružnice**.

7. Za dani $n \in \mathbb{N}$ promatrajmo jednadžbu $z^n - 1 = 0$, i skup K_n svih njezinih rješenja u skupu kompleksnih brojeva,

$$K_n = \{z \mid z^n = 1\} .$$

Tih rješenja ima točno n i zovu se **korijeni jedinice**, stupnja n,

$$K_n = \{\varepsilon_1 = 1, \varepsilon_2, \ldots, \varepsilon_n\} .$$

Uz uobičajeno, standardno množenje K_n je grupa reda n. Primijetimo da se svi korijeni jedinice mogu dobiti kao potencije jednog od njih, tzv. **primitivnog** korijena jedinice n-tog stupnja. Prema tome je K_n ciklička grupa reda n. I ovaj primjer pokazuje da postoje konačne grupe reda n, za svaki n. Očito je $K_n < S^1$.
Na primjer,

$$K_1 = \{1\}, \quad K_2 = \{-1, 1\},$$

$$K_3 = \left\{1, \frac{-1 + i\sqrt{3}}{2}, \frac{-1 - i\sqrt{3}}{2}\right\}, \quad K_4 = \{1, -1, i, -i\} .$$

8. Neka je K skup korijena jedinice svih stupnjeva, tj.

$$K = \bigcup_{n=1}^{\infty} K_n .$$

Onda je K također multiplikativna grupa i vrijedi $K < S^1$. Je li $K = S^1$? Primijetimo, da je K beskonačna grupa u kojoj je svaki element konačnog reda. Dakle, K je periodična grupa.

9. Promatrajmo skup

$$P = \{p, n\} = \{ \text{ par, nepar } \} .$$

Uz prirodno zbrajanje

$+$	p	n
p	p	n
n	n	p

$(P, +)$ je grupa. Međutim, $(P, \cdot)$ nije grupa. Zašto? Usporedi tu strukturu s Booleovim zbrajanjem i množenjem (Zad. 1. u 2.3.).

10. Promatrajmo skup

$$I_2 = \{-1, 1, -i, i\}$$

jedinica i njima suprotnih elemenata. Uz standardno množenje je I_2 grupa, tzv. **kompleksna grupa**.

11. Slično, promatrajmo

$$I_4 = \{-1, 1, -i, i, -j, j, -k, k\} .$$

Uz množenje $i^2 = j^2 = k^2 = -1$ i $ij = k = -ji$ i dalje ciklički, I_4 je grupa, očito nekomutativna. Kako ćemo vidjeti, elementi od I_4 mogu se interpretirati kao jedinice i njima suprotni elementi u skupu **kvaterniona**, "brojeva" koji se opisuju pomoću 4 jedinice,

$$q = x + iy + jz + kt, \qquad x, y, z, t \in \mathbb{R} .$$

Zato se I_4 zove **kvaternionska grupa**.

Postoje i "brojevi" koji se opisuju pomoću 8 jedinica, tzv. **oktave** ili **Cayleyjevi brojevi**. Pripadna grupa I_8 je reda 16. Kako je u toj shemi očito $I_1 = \{-1, 1\}$, imamo

$$I_1 < I_2 < I_4 < I_8 .$$

12. Neka je S dani skup, a $\mathcal{P}(S)$ njegov partitivni skup. Monoidi $(\mathcal{P}(S), \cup)$ i $(\mathcal{P}(S), \cap)$ nisu grupe. Zašto? Međutim, monoid $(\mathcal{P}(S), \Delta)$, gdje je

$$A \,\Delta\, B = (A - B) \cup (B - A),$$

jest Abelova grupa. Dokaži.

13. Za dani S monoid $(S^S, \circ)$ nije grupa, ako je S brojniji od jednog elementa. Međutim, podmonoid

$$B(S) = \{f \in S^S \mid f \text{ je bijekcija}\}$$

svih bijekcija iz S u S je, kako smo već rekli, grupa i to, općenito, nekomutativna. Tu grupu nazivamo **grupa permutacija** skupa S. Često će nas zanimati specijalne bijekcije, koje imaju neko dodatno svojstvo, kažimo s. Skup $B_s \subset B$ svih bijekcija s tim svojstvom bit će prema Tm. 2 iz 2.7. podgrupa onda i samo onda ako

(a) $f, g \in B_s \Rightarrow g \circ f \in B_s$, i

(b) $f \in B_s \Rightarrow f^{-1} \in B_s$.

Zapamti! Neka je npr. s svojstvo "*biti identiteta na* $A \subset S$". Onda je B_s grupa.

14. Neka je $p : \mathbb{R} \to \mathbb{R}$ polinom u varijabli t s realnim koeficijentima,

$$p(t) = \sum_{k=0}^{m} a_k t^k \quad , \quad a_k \in \mathbb{R} \, .$$

Nadalje, neka je

$$P_n = \{p \mid \mathrm{st}\, p < n\} \cup \{0\}$$

skup svih polinoma čiji je stupanj manji od danog broja $n \in \mathbb{N}$, i kojem je dodan broj 0. Uz standardno zbrajanje polinoma, P_n je grupa. Također je Abelova grupa skup

$$P = \bigcup_{n=0}^{\infty} P_n \, ,$$

tzv. **grupa polinoma**.

15. Promatrajmo realne funkcije realne varijable, zadane formulama

$$\begin{aligned} f_1(x) &= x, \quad f_2(x) = 1 - x, \quad f_3(x) = \frac{1}{x} \, , \\ f_4(x) &= \frac{x-1}{x}, \quad f_5(x) = \frac{1}{1-x}, \quad f_6(x) = \frac{x}{x-1} \, . \end{aligned}$$

Skup

$$F = \{f_1, f_2, f_3, f_4, f_5, f_6\}$$

je, uz kompoziciju kao binarnu operaciju, grupa i to nekomutativna. Prikaži tu grupu Cayleyjevom tablicom.

16. Neka je s E^2 označena ravnina. Kažemo da je preslikavanje

$$f : E^2 \to E^2$$

izometrija ravnine ako je za svaki par točaka $a, b \in E^2$

$$d(f(a), f(b)) = d(a, b),$$

gdje je s d označena udaljenost točaka.

Skup $\mathcal{I}(E^2)$ svih izometrija ravnine je grupa u odnosu na komponiranje preslikavanja. Podgrupe te grupe jesu

(a) skup $\mathcal{T}$ svih translacija ravnine,

(b) skup $\mathcal{R}_a$ svih rotacija ravnine oko dane točke a,

(c) skup $\mathcal{G} = \mathcal{T} \circ \mathcal{R} = \{t \circ r \mid t \in \mathcal{T},\ r \in \mathcal{R}\}$. To je tzv. **grupa gibanja ravnine**.

Dokaži te tvrdnje. Pogodno je rabiti koordinatni prikaz preslikavanja

$$(x, y) \overset{f}{\mapsto} (x', y') \ .$$

Na primjer, translacija je opisana koordinatno s

$$\begin{aligned} x' &= x + x_0 \\ y' &= y + y_0 \ , \end{aligned}$$

a rotacija s

$$\begin{aligned} x' &= x \cos\varphi + y \sin\varphi \\ y' &= -x \sin\varphi + y \cos\varphi \ . \end{aligned}$$

Skup $\mathcal{R} = \bigcup_{a \in E^2} \mathcal{R}_a$ svih rotacija nije grupa.

Ta tvrdnja nije trivijalna, ali konstruktivno i analitički se može dokazati da je kompozicija dviju rotacija opet rotacija ili (iznimno!) translacija.

17. Neka je $f : E^2 \to E^2$ preslikavanje, opisano koordinatno s

$$\begin{aligned} x' &= a_1 x + b_1 y + c_1 \\ y' &= a_2 x + b_2 y + c_2 \ , \end{aligned}$$

gdje su $a_i, b_i, c_i \in \mathbb{R}$ i $a_1 b_2 - a_2 b_1 \neq 0$. Takvo preslikavanje zovemo **afino**. Skup $\mathcal{A}$ svih afinih preslikavanja je grupa, koja se zove **afina grupa ravnine**. Dokaži!

18. Neka je G grupa i $a \in G$ njezin element. Definiramo preslikavanje

$$l_a : G \to G$$

s $l_a(x) = ax$, koje se zove **lijeva translacija** u grupi G. Neka je

$$L(G) = \{l_a \mid a \in G\}$$

skup svih lijevih translacija grupe G. Onda je $L(G)$ grupa u odnosu na kompoziciju. Zaista,

$$\begin{aligned} (l_a \circ l_b)(x) &= l_a\,[l_b(x)] = l_a(bx) = \\ &= a(bx) = (ab)x = l_{ab}(x) \end{aligned}$$

za svaki x, tj.

$$l_a \circ l_b = l_{ab} ,$$

dakle, opet translacija. Odmah se vidi da je $l_a^{-1} = l_{a^{-1}}$ jer imamo

$$l_a^{-1} \circ l_a = l_{a^{-1}} \circ l_a = l_{a^{-1}a} = l_e = e .$$

Tako je $L(G)$ grupa, **grupa lijevih translacija**. Kad je ta grupa komutativna?

Provjeri da su sljedeći skupovi pridruženi grupi G također grupe u odnosu na kompoziciju:

(a) $D(G) = \{d_a \mid a \in G\}$, gdje je $d_a(x) = xa$ (**desna translacija**);
(b) $R(G) = \{r_a \mid a \in G\}$, gdje je $r_a(x) = a^{-1}x$;
(c) $S(G) = \{s_a \mid a \in G\}$, gdje je $s_a(x) = xa^{-1}$;
(d) $T(G) = \{t_a \mid a \in G\}$, gdje je $t_a(x) = axa^{-1}$.

Dakako, svaka od tih grupa je podgrupa grupe $B(G)$ svih bijekcija grupe G.

19. Na skupu $R_3 = \{a_0, a_1, a_2\}$ definiramo binarnu operaciju apstraktno, pomoću tablice

$+$	a_0	a_1	a_2
a_0	a_0	a_1	a_2
a_1	a_1	a_2	a_0
a_2	a_2	a_0	a_1

.

R_3 je uz takvo zbrajanje Abelova grupa trećeg reda. Provjeri!
Ta se grupa može geometrijski interpretirati. Promatrajmo, naime, sve rotacije jednakostraničnog trokuta oko njegova središta, koje prevode trokut na sama sebe, i identificirajmo one koje se razlikuju za višekratnik od 2π. Imamo

$$\begin{aligned} r_0 &= \text{nulrotacija} = e \\ r_1 &= \text{rotacija za } 2\pi/3 \\ r_2 &= \text{rotacija za } 4\pi/3 . \end{aligned}$$

Uz kompoziciju je skup tih rotacija grupa, prikazana tablično

$\circ$	r_0	r_1	r_2
r_0	r_0	r_1	r_2
r_1	r_1	r_2	r_0
r_2	r_2	r_0	r_1

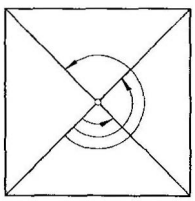
i to je **grupa rotacija trokuta**. Razabiremo da ta grupa ima istu unutrašnju strukturu (istu tablicu množenja) kao i prethodna apstraktna grupa R_3; razlikuju se jedino u naravi svojih elemenata.

20. Analogno, na skupu $R_4 = \{a_0, a_1, a_2, a_3\}$ definiramo "zbrajanje" tablicom

$+$	a_0	a_1	a_2	a_3
a_0	a_0	a_1	a_2	a_3
a_1	a_1	a_2	a_3	a_0
a_2	a_2	a_3	a_0	a_1
a_3	a_3	a_0	a_1	a_2

koju nazivamo "algebra četiriju simbola". Uz takvo zbrajanje je R_4 Abelova grupa. Provjeri!

Grupa R_4 se može geometrijski interpretirati kao **grupa rotacija kvadrata**, tj. svih rotacija kvadrata oko njegova središta, koje ga prevode na sebe, uz prirodnu identifikaciju. Provjeri! Također, provje-



ri da R_4 ima istu strukturu kao kompleksna grupa I_2 (vidi Prim. 10.).

21. Generalizirajući, promatramo skup $R_n = \{a_0, \ldots, \ldots, a_{n-1}\}$ zajedno s "algebrom n simbola" definiranom na njemu. Uz to zbrajanje je R_n Abelova grupa reda n, koja se može geometrijski interpretirati kao **grupa rotacija pravilnog n-terokuta**. Je li ta grupa iste strukture kao $\mathbb{Z}_n$?

22. Promatrajmo opet skup $\{a_0, a_1, a_2, a_3\}$, ali na njemu propišimo "zbrajanje" tablicom

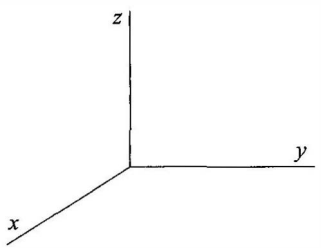
$+$	a_0	a_1	a_2	a_3
a_0	a_0	a_1	a_2	a_3
a_1	a_1	a_0	a_3	a_2
a_2	a_2	a_3	a_0	a_1
a_3	a_3	a_2	a_1	a_0

Lako se provjeri da je i uz tu operaciju ovaj skup grupa, ali strukturalno različita od R_4. U ovoj je, naime, grupi

$$a_i + a_i = a_0$$

za svaki i, tj. svaki je element **reda** 2 ili **involutoran**. Grupa se zove **Kleinova četvorna grupa** i standardno se označava s V (prema njemačkom: die Vierergruppe).

Zakonitost izražena tom tablicom realizirana je u mnogim konkretnim situacijama u geometriji. Grupu V možemo npr. shvatiti kao grupu onih rotacija ortogonalnog trobrida u sebe, koje svaku njegovu os pre-



vode u samu sebe. Pritom elemente od V interpretiramo ovako:

$a_0 \to e$,
$a_1 \to$ rotacija za π oko x ,
$a_2 \to$ rotacija za π oko y ,
$a_3 \to$ rotacija za π oko z ,

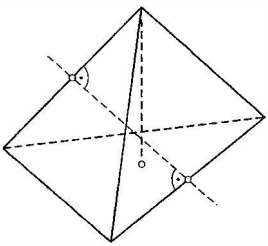
tj. $(x, y, z) \overset{a_1}{\mapsto} (x, -y, -z)$ i slično.

23. Neka je M poligon u ravnini, a

$$G(M) = \{f : M \to M \mid f \text{ je izometrija}\}$$

skup svih izometrija, kongruentnih preslikavanja poligona M na sebe. Uz kompoziciju, $G(M)$ je grupa, tzv. **grupa poligona** M. Očito, što je poligon pravilniji, to je grupa bogatija. Na primjer, **grupa jednakostraničnog trokuta** je reda 6 (i ima R_3 za podgrupu). Pokaži da je **grupa kvadrata** reda 8 i da ima R_4 kao podgrupu. Pokaži nadalje, da je **grupa romba** iste strukture kao Kleinova grupa V (vidi Prim. 22.).

24. Analogno, neka je P poliedar, a $G(P)$ skup svih izometrija tog poliedra. Onda je to također grupa, **grupa poliedra** P. Ako je npr. P pravilni tetraedar, $G(P)$ je grupa reda 24. Provjeri! Važna je podgrupa H



grupe $G(P)$, tzv. **grupa rotacija tetraedra**, koja osim identitete sadrži i rotacije oko svake visine tetraedra za $2\pi/3$, odnosno $4\pi/3$, te rotacije tetraedra za π oko spojnica polovišta svakog para njegovih suprotnih bridova. Uvjeri se da je H zaista grupa reda 12 i da ima točno 8 netrivijalnih podgrupa:

(a) jednu reda 4, koja se sastoji od identitete i triju rotacija za π (ta je iste strukture kao V),

(b) četiri reda 3, od kojih se svaka sastoji iz identitete i dviju rotacija oko dane visine, i

(c) tri reda 2, od kojih se svaka sastoji od identitete i jedne rotacije za π.

Šest daljnjih elemenata u $G(P)$ mogu se dobiti promatranjem zrcaljenja na simetralnim ravninama kroz bridove tetraedra. Ta zrcaljenja zajedno ne čine podgrupu od $G(P)$. Svako od njih, međutim, zajedno s identitetom je očito podgrupa reda 2.

ZADACI

1. Odredi grupu kocke i (pravilnog) oktaedra.

2. Skup $(-1,1) = \{t \in \mathbb{R} \mid -1 < t < 1\}$ je uz binarnu operaciju

$$t * s = \frac{t+s}{1+ts}$$

grupa. Dokaži!

3. Neka je $G = (\mathbb{R} - \{0\}) \times \mathbb{R}$. Na G definiramo binarnu operaciju s

$$(a,b) * (c,d) = (ac, bc+d) .$$

Provjeri da je $(G, *)$ grupa.

2.9. Grupe permutacija. Simetrična grupa

Kako ćemo vidjeti (u 3.4.), grupe permutacija igraju istaknutu ulogu u teoriji grupa, jer su njima u izvjesnom smislu reprezentirane sve moguće apstraktne grupe. Važne su i s povijesnog stajališta jer su se upravo na pojmu permutacija (ili supstitucija, kako se nekad govorilo) rodile, početkom 19. stoljeća, u radovima Lagrangea, Gaussa, Cauchyja i Galoisa, prve svjesne ideje o grupovnosti.

Neka je S dani skup. Kako smo već rekli, svaku bijekciju $S \to S$ nazivamo **permutacija skupa** S. Ako skup svih permutacija od S označimo s $B(S)$, imamo

TEOREM 1

Skup $B(S)$ je grupa u odnosu na kompoziciju kao binarnu operaciju.

Dokaz

Trivijalan. Naime, kompozicija bijekcija je opet bijekcija. Nadalje, bijekcija ima inverz i taj je bijekcija. Konačno, identiteta je, dakako, bijekcija. ■

Grupu $B(S)$ nazivamo **grupa permutacija skupa** S. Lako se vidi da je ta grupa nekomutativna, čim S ima više od dva elementa. I podgrupe od $B(S)$ nazivamo grupama permutacija.

Obratimo sada pažnju na slučaj kad je S **konačan** skup. Primijetimo da je onda preslikavanje

$$p : S \to S$$

surjektivno, ako i samo ako je injektivno. Prema tome, svaki od tih zahtjeva je ekvivalentan činjenici da je p permutacija skupa S. Ako skup S ima n elemenata, možemo bez narušavanja općenitosti umjesto

$$S = \{a_1, a_2, \ldots, a_n\}$$

jednostavnije pisati

$$S = \{1, 2, \ldots, n\} ,$$

shvaćajući te brojeve samo kao oznake, indekse elemenata iz S. U tom slučaju možemo permutaciju p zapisati tablično

i	1	2	$\cdots$	n
$p(i)$	p_1	p_2	$\cdots$	p_n

,

odnosno (u skladu s tradicijom) "matrično" kao

$$p = \begin{pmatrix} 1 & 2 & \ldots & n \\ p(1) & p(2) & \ldots & p(n) \end{pmatrix} =$$

$$= \begin{pmatrix} 1 & 2 & \ldots & n \\ p_1 & p_2 & \ldots & p_n \end{pmatrix} = \begin{pmatrix} i \\ p_i \end{pmatrix} ,$$

gdje su, kako vidimo, u prvom redu popisani elementi domene, a u drugom odgovarajuće vrijednosti funkcije p. Ovo je standardni prikaz permutacije p. Ako elemente domene napišemo u nekom drugom redoslijedu, dolazimo do drugih (matričnih) prikaza iste permutacije.

U ovoj notaciji se množenje, tj. komponiranje permutacija obavlja vrlo jednostavno:

$$\begin{aligned} q \circ p &= \begin{pmatrix} 1 & \dots & n \\ q_1 & \dots & q_n \end{pmatrix} \circ \begin{pmatrix} 1 & \dots & n \\ p_1 & \dots & p_n \end{pmatrix} = \\ &= \begin{pmatrix} p_1 & \dots & p_n \\ q(p_1) & \dots & q(p_n) \end{pmatrix} \circ \begin{pmatrix} 1 & \dots & n \\ p_1 & \dots & p_n \end{pmatrix} = \\ &= \begin{pmatrix} 1 & \dots & n \\ q(p_1) & \dots & q(p_n) \end{pmatrix} = \\ &= \begin{pmatrix} 1 & \dots & n \\ (q \circ p)(1) & \dots & (q \circ p)(n) \end{pmatrix} = \begin{pmatrix} i \\ (q \circ p)(i) \end{pmatrix} . \end{aligned}$$

Čitamo, naime, neposredno $1 \mapsto p_1 \mapsto q(p_1) = (q \circ p)(1)$ itd. Primijetimo još da se identična permutacija (neutralni element!) zapisuje kao

$$e = \begin{pmatrix} 1 & \dots & n \\ 1 & \dots & n \end{pmatrix} ,$$

dok je inverz permutacije p u ovoj oznaci dan s

$$p^{-1} = \begin{pmatrix} p_1 & \dots & p_n \\ 1 & \dots & n \end{pmatrix} .$$

Grupu permutacija skupa $\{1, \dots, n\}$ označavamo obično s

$$B(\{1, \dots, n\}) = S_n$$

i nazivamo je **simetrična grupa stupnja** n.

PROPOZICIJA 2

Grupa S_n je reda $n!$, tj. ima $n!$ elemenata.

Dokaz

Indukcijom. ■

Kao primjer pogledajmo slučaj $n = 3$. Imamo

$$\begin{aligned} S_3 = \Bigg\{ &\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \\ &\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \Bigg\} . \end{aligned}$$

Ista permutacija može, dakako, imati različite zapise. Tako je npr.

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 3 & 2 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 3 & 2 & 1 \\ 3 & 1 & 2 \end{pmatrix} = \text{itd.}$$

Primjenjujući spomenuti zakon množenja za permutacije imamo npr.

$$q \circ p = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix},$$

a

$$p \circ q = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix},$$

što ujedno pokazuje da je $p \circ q \neq q \circ p$, tj. S_3 nije komutativna. Konačno, za permutaciju p je njezin inverz

$$p^{-1} = \begin{pmatrix} 2 & 1 & 3 \\ 1 & 2 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix},$$

tj. $p^{-1} = p$, dok je

$$q^{-1} = \begin{pmatrix} 3 & 1 & 2 \\ 1 & 2 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}.$$

Neka je $p \in S_n$ dana permutacija. Svaki slučaj kad u toj permutaciji vrijedi $i < j$ i $p(i) > p(j)$, nazivamo **inverzija** u permutaciji p. Neka je s $I(p)$ označen ukupan broj inverzija u permutaciji p. Onda preslikavanje

$$\text{sign} : S_n \to \{1, -1\}$$

definirano sa

$$\text{sign}(p) = (-1)^{I(p)}$$

zovemo **parnost ili paritet** (oznaka dolazi od latinske riječi signum – znak, predznak). Permutaciju $p \in S_n$ za koju je $\text{sign}(p) = 1$ nazivamo **parna**, a onu za koju je $\text{sign}(p) = -1$ **neparna** permutacija. Na primjer, za identičnu permutaciju je $\text{sign}(e) = 1$, pa je ona parna. Nadalje,

$$p = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

jest parna permutacija, jer je $I(p) = 2$, pa je $\text{sign}(p) = 1$, dok je

$$q = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

neparna permutacija, jer je $I(q) = 3$, što povlači $\text{sign}(q) = -1$.

PROPOZICIJA 3

Preslikavanje sign *ima ova svojstva*

(1) $\operatorname{sign}(q \circ p) = \operatorname{sign}(q) \cdot \operatorname{sign}(p)$;

(2) $\operatorname{sign}(p^{-1}) = \operatorname{sign}(p)$

za svaki $p, q \in S_n$.

Dokaz

Primijetimo, da je u brojenju inverzija u q dovoljno uspoređivati $p(i)$ i $p(j)$ s $q[p(i)]$ i $q[p(j)]$. Za dane $i < j$ imamo onda četiri mogućnosti:

(a) $p(i) < p(j)$; $(q \circ p)(i) < (q \circ p)(j)$, tj. nema inverzije niti u p niti u q niti u $q \circ p$,

(b) $p(i) < p(j)$; $(q \circ p)(i) > (q \circ p)(j)$, tj. nema inverzije u p, ali imamo inverziju u q i onda u $q \circ p$,

(c) $p(i) > p(j)$; $(q \circ p)(i) < (q \circ p)(j)$, tj. imamo inverziju u p, zatim u q, ali nema inverzije u $q \circ p$,

(d) $p(i) > p(j)$; $(q \circ p)(i) > (q \circ p)(j)$, tj imamo inverziju u p, nema inverzije u q, ali zato postoji u $q \circ p$.

Odavde odmah zaključujemo da se $I(q \circ p)$ razlikuje od $I(q) + I(p)$ za paran broj, pa je

$$(-1)^{I(q \circ p) - [I(q) + I(p)]} = 1 \,,$$

dakle,

$$(-1)^{I(q \circ p)} = (-1)^{I(q) + I(p)} = (-1)^{I(q)} \cdot (-1)^{I(p)},$$

tj. po definiciji

$$\operatorname{sign}(q \circ p) = \operatorname{sign}(q) \cdot \operatorname{sign}(p)$$

i (1) je dokazano. Posebno, iz (1) imamo

$$\operatorname{sign}(p^{-1}) \operatorname{sign}(p) = \operatorname{sign}(p^{-1} \circ p) = \operatorname{sign}(e) = 1 \,,$$

odakle slijedi da je

$$\operatorname{sign}(p^{-1}) = \operatorname{sign}(p)$$

tj. istinito je i (2). ■

Neka je sada s A_n označen skup svih parnih permutacija u S_n. Zbog $e \in A_n$, taj skup nije prazan. I više, vrijedi

TEOREM 4

Skup $A_n \subset S_n$ je podgrupa od S_n.

Dokaz

Neposredno iz Prop. 3 (vidi Tm. 2 u 2.7.). ■

Grupa A_n naziva se **alternirajuća grupa** stupnja n. Na primjer,

$$A_3 = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \right\},$$

i ona je reda $3 = 3!/2$.

Što možemo reći o broju elemenata u A_n u općem slučaju? Pokažimo najprije da vrijedi

PROPOZICIJA 5

Ako je $n > 1$, broj parnih permutacija u S_n jednak je broju neparnih permutacija.

Dokaz

Promatrajmo specijalnu permutaciju

$$t = \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ 2 & 1 & 3 & \dots & n \end{pmatrix},$$

u kojoj je $t(1) = 2$, $t(2) = 1$, a svi ostali elementi ostaju na miru, $t(j) = j$ za $j > 2$. Očito je da u toj permutaciji imamo samo jednu inverziju, pa je ona neparna.

Neka je s $B_n \subset S_n$ označen skup svih neparnih permutacija u S_n. Promatrajmo funkciju

$$f : A_n \to B_n$$

definiranu s

$$f(p) = t \circ p$$

za svaku parnu permutaciju $p \in A_n$. Kako je zbog Prop. 3 $t \circ p$ neparna permutacija, f je dobro definirana. Pokažimo da je bijektivna. Najprije iz $f(p) = f(q)$ slijedi $t \circ p = t \circ q$, odnosno, zbog mogućnosti skraćivanja u grupi, $p = q$, pa je f injekcija. Nadalje, za $r \in B_n$ i iz činjenice da je t^{-1} također neparna permutacija, slijedi da je $t^{-1} \circ r$ parna permutacija i pritom vrijedi

$$f(t^{-1} \circ r) = t \circ (t^{-1} \circ r) = (t \circ t^{-1}) \circ r = r,$$

tj. f je i surjekcija pa je tvrdnja dokazana. ■

KOROLAR 6

Uz $n > 1$ alternirajuća grupa A_n je reda $n!/2$, tj. ima $n!/2$ elemenata.

■

Kažimo nešto o mogućnosti dekompozicije permutacija. Neka je $p \in S_n$ permutacija sa svojstvom da postoje međusobno različiti prirodni brojevi $i_1, i_2, \ldots, i_d \in \{1, \ldots, n\}$ tako da vrijedi

$$p(i_1) = i_2,\ p(i_2) = i_3,\ \ldots,\ p(i_{d-1}) = i_d, p(i_d) = i_1,$$

dok ostali elementi ostaju na miru, tj. $p(j) = j$ za $j \neq i_1, \ldots, i_d$, dakle

$$p = \begin{pmatrix} i_1 & i_2 & \ldots & i_{d-1} & i_d & i_{d+1} & \ldots i_n \\ i_2 & i_3 & \ldots & i_d & i_1 & i_{d+1} & \ldots i_n \end{pmatrix} .$$

Onda pišemo kraće

$$p = (i_1\, i_2 \ldots i_d)$$

i kažemo da je p **ciklička permutacija** ili **ciklus** duljine d. Svaki ciklus duljine 1 je očito identična permutacija. Ciklus duljine 2 zovemo **transpozicija**. Na primjer,

$$\begin{aligned} (1\ 3\ 5\ 6) &= \begin{pmatrix} 1 & 3 & 5 & 6 & 2 & 4 \\ 3 & 5 & 6 & 1 & 2 & 4 \end{pmatrix} = \\ &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 2 & 5 & 4 & 6 & 1 \end{pmatrix} \end{aligned}$$

jest ciklus duljine 4, a

$$\begin{aligned} (2\ 4) &= \begin{pmatrix} 2 & 4 & 1 & 3 & 5 & 6 \\ 4 & 2 & 1 & 3 & 5 & 6 \end{pmatrix} = \\ &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 4 & 3 & 2 & 5 & 6 \end{pmatrix} \end{aligned}$$

jedna je transpozicija iz S_6.

Permutacija, dakako, ne mora biti ciklus, ali se uvijek može prikazati kao produkt ciklusa. Primjerice, imamo

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 5 & 2 & 6 & 1 \end{pmatrix} = (1\,3\,5\,6)(2\,4)\ .$$

Dokažimo tu tvrdnju općenito.

PROPOZICIJA 7

Svaka se permutacija $p \in S_n$ može prikazati kao produkt disjunktnih ciklusa, tj. ciklusa koji ne sadrže isti prirodni broj.

Dokaz

Indukcijom po stupnju n grupe S_n. Ako je $n = 1$, jedina permutacija iz S_1 je $p = (1)$ i tvrdnja je istinita. Pretpostavimo da je istinita za sve $n < k$, pa je dokažimo za $n = k$.

Neka je $p \in S_k$ bilo koja permutacija. Promatrajmo sljedeći niz od $k+1$ prirodnih brojeva

$$1, p(1), p^2(1), \ldots, p^k(1)$$

iz $\{1, \ldots, k\}$. Kako taj skup sadrži samo k elemenata, moraju postojati cijeli brojevi r i s takvi da je

$$p^r(1) = p^s(1)$$

i pritom je

$$0 \leq r < s \leq k$$

i $p^0(1) = 1$. Kako je p bijekcija (pa ima inverz), odatle slijedi

$$p^{s-r}(1) = 1 \, .$$

Neka je d najmanji prirodni broj, za koji vrijedi

$$p^d(1) = 1 \, .$$

Onda je $1 \leq d \leq k$ i prirodni brojevi

$$i_1 = 1, \; i_2 = p(1), \; i_3 = p^2(1), \; \ldots, \; i_d = p^{d-1}(1)$$

jesu svi različiti. Za njih, međutim, vrijedi

$$p(i_1) = p(1) = i_2, \quad p(i_2) = p^2(1) = i_3, \quad \ldots$$

$$\ldots \, , \; p(i_{d-1}) = p^{d-1}(1) = i_d, \quad p(i_d) = p[p^{d-1}(1)] = p^d(1) = 1 = i_1$$

Tako smo došli do ciklusa

$$q_1 = (i_1 \, i_2 \ldots i_d)$$

u S_k, i našu polaznu permutaciju p možemo očito pisati kao

$$p = q_2 \circ q_1 \, ,$$

gdje je q_2 permutacija od preostalih $k - d$ prirodnih brojeva (a $i_1, \ldots, i_d$ ostavlja na miru). Prema pretpostavci indukcije, q_2 se onda može prikazati kao produkt disjunktnih ciklusa od tih $k - d < k$ brojeva i tvrdnja je dokazana. ■

Međutim, ciklusi se mogu dalje dekomponirati.

PROPOZICIJA 8

Svaki se ciklus duljine $d \geq 2$ može prikazati kao produkt od $d-1$ transpozicije.

Dokaz

Očigledan. Odmah se, naime, provjeri da vrijedi

$$(i_1\, i_2 \ldots i_d) = (i_1\, i_d)(i_1\, i_{d-1}) \ldots (i_1\, i_2)\,. \qquad \blacksquare$$

Iz Prop. 7 i Prop. 8 slijedi neposredno

TEOREM 9

Svaka se permutacija može prikazati kao produkt transpozicija. ■

Takav prikaz nije općenito jednoznačan. Ako su, međutim,

$$p = t_1 \circ \ldots \circ t_r = u_1 \circ \ldots \circ u_s$$

dva rastava permutacije p u transpozicije, može se pokazati da je $r-s$ uvijek paran broj, tj. brojevi r i s su ili oba parna ili oba neparna. Pokazuje se, nadalje, da je permutacija parna (neparna) ako i samo ako se može prikazati kao produkt parnog (neparnog) broja transpozicija, pa ta činjenica može poslužiti za alternativnu definiciju pariteta permutacije (vidi Zad. 10.).

ZADACI

1. Neka je S dani skup, a $R(S)$ skup svih onih bijekcija od S koje su gotovo svagdje identiteta, tj. koje ostavljaju na miru sve elemente od S, osim njih konačno mnogo. Pokaži da je $R(S)$ podgrupa od $B(S)$. Ta se grupa naziva **reducirana grupa permutacija** skupa S. Naravno, ako je S konačan skup, $R(S) = B(S)$.

2. Prikaži grupu S_3 tablično.

3. Dokaži: Ako su $p, q \in S_n$ disjunktni ciklusi, onda je $p \circ q = q \circ p$.

4. Ako je $p \in S_n$ ciklus duljine d, onda je p element reda d u grupi S_n. Posebno, svaka je transpozicija reda 2 (involutorna).

5. Dokaži: Red permutacije $p \in S_n$ je najmanji zajednički višekratnik duljina disjunktnih ciklusa u dekompoziciji od p.

6. Alternirajuća grupa A_n je, uz $n \geq 3$, generirana ciklusima duljine 3. Dokaži!

7. Ako je $p \in S_n$ ciklus duljine d, a $q \in S_n$ bilo koja permutacija, onda je $q^{-1} \circ p \circ q$ opet ciklus duljine d. Dokaži!

8. Uvjeri se da je za bilo koji $p \in S_n$ njezin paritet dan formulom

$$\operatorname{sign}(p) = \prod_{i<j} \frac{p(j) - p(i)}{j - i} \ ,$$

gdje je sa $\prod$ označen produkt (realnih brojeva). Odatle odmah vidimo da je svaka transpozicija neparna permutacija.

9. Neka je

$$s : S_n \to \{1, -1\}$$

bilo koja funkcija s ovim svojstvima:

(a) $s(p \circ q) = s(p)\, s(q)$, za svaki izbor $p, q \in S_n$,

(b) $s(e) = 1$, za identičnu permutaciju $e \in S_n$, i

(c) $s(t) = -1$, za svaku transpoziciju $t \in S_n$.

Onda je nužno $s = \operatorname{sign}$. Dokaži. To je aksiomatska karakterizacija funkcije pariteta.

10. Uvjeri se da produkt parnog broja transpozicija ne može biti jednak produktu neparnog broja transpozicija. Definiraj funkciju

$$s : S_n \to \{1, -1\}$$

stavljajući

$s(p) = 1$, ako je p produkt parnog broja transpozicija,
$s(p) = -1$, ako je p produkt neparnog broja transpozicija.

Dokaži da funkcija s zadovoljava aksiome (a)–(c) iz Zad. 9., i zato je $s = \operatorname{sign}$. Prema tome, funkciju pariteta sign možemo alternativno definirati sa

$$\operatorname{sign}(p) = (-1)^{T(p)} \ ,$$

gdje $T(p)$ označava broj transpozicija u (bilo kojem) prikazu permutacije p pomoću transpozicija.

3

PRESLIKAVANJA GRUPA. KVOCIJENT I PRODUKT GRUPA

U općoj, apstraktnoj teoriji grupa (ili grupoida, polugrupa, monoida) zanimaju nas samo ona svojstva koja su posljedica strukture inducirane danom binarnom operacijom u grupi, a ne ovise ni o konkretnoj naravi elemenata grupe, niti o konkretnom karakteru te operacije. Zato je od interesa imati neko sredstvo kojim bi se te strukture mogle uspoređivati i na osnovi toga zaključivati o njihovoj eventualnoj istovjetnosti. To se postiže pomoću preslikavanja između grupa, koja poštuju dane strukture, tzv. homomorfizama, odnosno, izomorfizama grupa, kojima je posvećeno ovo poglavlje.

3.1. Homomorfizam grupa

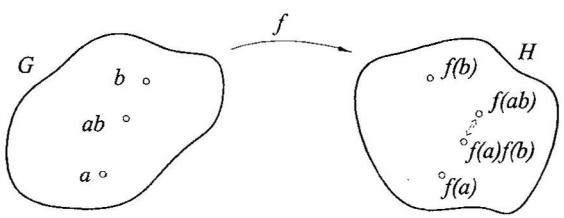
Evo odmah definicije. Neka su G i H dane grupe, a

$$f : G \to H$$

preslikavanje koje komutira s binarnom operacijom, tj. za koje vrijedi

$$f(ab) = f(a) \cdot f(b)$$

za svaki $a, b \in G$. Onda kažemo da je f **homomorfizam** grupe G u grupu H.



U preciznijoj notaciji trebalo bi navedeni uvjet, dakako, pisati kao

$$f(a \cdot_G b) = f(a) \cdot_H f(b) ,$$

jer u G i H imamo općenito različite binarne operacije.

Na primjer, ako je $G < H$, onda je inkluzija $i : G \to H$ očito homomorfizam. Posebno, identiteta $H \to H$ je homomorfizam. Nadalje, homomorfizam je konstantno preslikavanje $f : G \to H$ dano s $f(x) = e^*$, za svaki $x \in G$, gdje je e^* jedinica u H. Takav se f zove **trivijalni** ili **nulhomomorfizam**. Manje je trivijalan primjer ako uzmemo $G = (\mathbb{R}, +)$, a $H = (\mathbb{R}^*, \cdot)$, pa definiramo $f : G \to H$ s

$$f(x) = e^x .$$

To je zaista homomorfizam, jer imamo

$$f(x + y) = e^{x+y} = e^x \cdot e^y = f(x) \cdot f(y).$$

Primijetimo da se u definiciji homomorfizma od f ne zahtijevaju još neka dobra svojstva, kao što su injektivnost, odnosno surjektivnost. Ako je homomorfizam f injekcija, onda se još kaže da je to **monomorfizam**, a ako je surjekcija, onda je to **epimorfizam**. Konačno, ako je f bijekcija, govorimo o **izomorfizmu**, o kojem će još biti riječi. U drugu ruku, ako je, specijalno, $H = G$, za homomorfizam $f : G \to G$ kažemo još da je **endomorfizam**, a ako je i bijekcija, tj. izomorfizam grupe na sebe, govorimo o **automorfizmu** grupe G. Ti se termini dosta često susreću u literaturi. Lako se npr. vidi kako je f u prethodnom primjeru monomorfizam, ali očito nije epimorfizam.

NAPOMENA 1

Posve analogno kao kod grupa, definiramo pojam homomorfizma, pa onda i monomorfizma, epimorfizma i izomorfizma i za druge strukture koje smo spominjali, tj. za grupoide, polugrupe i monoide.

Navedimo neka osnovna svojstva homomorfizma, koja proizlaze neposredno iz definicije.

PROPOZICIJA 2

Neka su G i H grupe s jedinicama e, odnosno e^*, a $f : G \to H$ homomorfizam. Onda je

$$f(e) = e^* .$$

Dokaz

Za $x \in G$ imamo

$$e^* \cdot f(x) = f(x) = f(ex) = f(e) \cdot f(x)$$

pa kraćenjem s $f(x)$ u grupi H dobivamo

$$e^* = f(e)\,.$$

■

PROPOZICIJA 3

Ako je $f : G \to H$ homomorfizam, onda je

$$[f(x)]^{-1} = f(x^{-1})$$

za svaki $x \in G$.

Dokaz

Prema Prop. 2 za bilo koji $x \in G$ imamo

$$e^* = f(e) = f(x \cdot x^{-1}) = f(x) \cdot f(x^{-1})$$

pa množenjem s $[f(x)]^{-1}$ slijeva zaista dobivamo

$$[f(x)]^{-1} = f(x^{-1})\ .$$

■

PROPOZICIJA 4

Neka je $f : G \to H$ homomorfizam grupa i $G_0 < G$ podgrupa od G. Onda je slika $f(G_0) \subset H$ podgrupa od H.

Dokaz

Neka su $a, b \in f(G_0)$. Treba vidjeti da je $ab^{-1} \in f(G_0)$. No, iz $a \in f(G_0)$ slijedi da postoji $x \in G_0$ sa svojstvom da je $f(x) = a$. Slično, zbog $b \in f(G_0)$, postoji $y \in G_0$ takav da je $f(y) = b$. Onda zbog Prop. 3 imamo

$$ab^{-1} = f(x) \cdot [f(y)]^{-1} = f(x) \cdot f(y^{-1}) = f(xy^{-1})\,.$$

Međutim, iz $x, y \in G_0$ i pretpostavke da je G_0 podgrupa, slijedi da je i $xy^{-1} \in G_0$, dakle $f(xy^{-1}) \in f(G_0)$, tj. $ab^{-1} \in f(G_0)$, što je i trebalo dokazati. ■

PROPOZICIJA 5

Neka je $f : G \to H$ homomorfizam grupa i $H_0 < H$ podgrupa od H. Onda je praslika $f^{-1}(H_0) \subset G$ podgrupa od G.

Dokaz

Neka su $x, y \in f^{-1}(H_0)$. Onda su $f(x)$, $f(y) \in H_0$, a kako je H_0 podgrupa po pretpostavci, to je i $f(x) \cdot [f(y)]^{-1} \in H_0$. Odatle, zbog Prop. 3 i pretpostavke da je f homomorfizam, imamo i $f(xy^{-1}) \in H_0$, te zaključujemo da je $xy^{-1} \in f^{-1}(H_0)$, tj. $f^{-1}(H_0)$ je podgrupa od G. ■

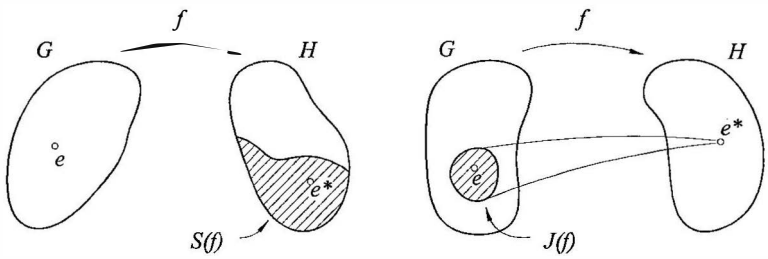
Neka je $f : G \to H$ homomorfizam grupa. Definiramo

(1) **sliku od** f kao skup

$$S(f) = f(G) = \{f(x) \mid x \in G\} \subset H \,,$$

(2) **jezgru od** f kao skup

$$J(f) = f^{-1}(e^*) = \{x \in G \mid f(x) = e^*\} \subset G \,.$$



Još je uobičajena oznaka $S(f) = \mathrm{Im}(f)$ i $J(f) = Ker(f)$. Uoči da slika i jezgra ne ovise o danim grupama, nego o homomorfizmu f.

KOROLAR 6

Neka je $f : G \to H$ homomorfizam grupa. Onda su slika $S(f) \subset H$ i jezgra $J(f) \subset G$ podgrupe od H, odnosno G.

Dokaz

Neposredno iz Prop. 4, odnosno Prop. 5. ■

Spomenimo na kraju da se homomorfizmi grupa dobro ponašaju prema komponiranju. Vrijedi

PROPOZICIJA 7

Neka su $f : G \to H$ i $g : H \to K$ homomorfizmi grupa. Onda je i kompozicija $h = g \circ f$,

$$h : G \to K \,,$$

homomorfizam grupa.

Dokaz

Za $x, y \in G$ imamo redom

$$\begin{aligned} h(xy) &= (g \circ f)(xy) = g[f(xy)] = g[f(x)f(y)] = \\ &= g[f(x)] \cdot g[f(y)] = (g \circ f)(x) \cdot (g \circ f)(y) = \\ &= h(x)\, h(y). \end{aligned}$$

■

ZADACI

1. Neka je $f : S \to T$ homomorfizam grupoida (polugrupa, monoida), dakle preslikavanje za koje vrijedi $f(ab) = f(a)f(b)$, za svaki $a, b \in S$. Koja od svojstava navedenih u Prop.2 – Prop.7 vrijede u ovom slučaju? Specijalno, ako je f homomorfizam monoida, prevodi li f nužno jedinicu u jedinicu? Ako ne, nađi protuprimjer! [Uputa: Promatraj npr. $f : \mathbb{Z} \to \mathbb{Z}$, $f(n) = 0$, za svaki $n \in \mathbb{Z}$, gdje je $\mathbb{Z}$ multiplikativni monoid cijelih brojeva.]

2. Kao posljedicu općeg teorema o kompoziciji preslikavanja, pokaži da vrijedi ova izreka: Neka je $h = g \circ f$ kompozicija homomorfizama (npr. grupa). Ako je h epimorfizam, takav je i g. Ako je pak h monomorfizam, takav je i f.

3. Neka je $f : G \to H$ homomorfizam i $a_1, a_2, \ldots, a_n \in G$ bilo koji izbor elemenata. Onda je

$$f(a_1 \cdot a_2 \cdot \ldots \cdot a_n) = f(a_1) \cdot f(a_2) \cdot \ldots \cdot f(a_n)\ .$$

   Dokaži!

4. Neka su $f, g : G \to H$ dva homomorfizma, npr. grupa. Onda je $K = \{x \in G \mid f(x) = g(x)\}$ podgrupa od G.

5. Neka su f i g kao u prethodnom zadatku, a S skup generatora za G. Onda je $f = g$ ako i samo ako je $f(s) = g(s)$, za svaki $s \in S$. Dokaži!

6. Neka je $f : G \to H$ homomorfizam i G_0 podgrupa od G. Onda je restrikcija $f/_{G_0} : G_0 \to H$ također homomorfizam. Nadalje, ako je f monomorfizam, to je i $f/_{G_0}$. Dokaži!

7. Neka je G dana grupa i $a \in G$. Definiramo preslikavanje $f : \mathbb{Z} \to G$ s $f(n) = a^n$, za svaki $n \in \mathbb{Z}$. Pokaži da je f homomorfizam grupa. Pokaži, nadalje, da je slika $S(f) < G$ ciklička podgrupa od G generirana s a. Kakva je veza između jezgre $J(f)$ i reda elementa a?

8. Malo općenitije, neka je G bilo koja ciklička grupa, a $f : G \to H$ homomorfizam. Onda je $S(f) < H$ ciklička podgrupa od H.

9. Definiramo $f : \mathbb{R} \to S^1$ s $f(x) = e^{2\pi i x}$. Pokaži da je f epimorfizam i da je $J(f) = \mathbb{Z}$. f nazivamo **"namatanje pravca na kružnicu"**.

10. Definiramo $f : \mathbb{Z} \to \mathbb{Z}_m$ s

$$f(k) = \text{ostatak pri dijeljenju } k \text{ s } m .$$

Pokaži da je f homomorfizam i odredi $J(f)$.

11. Dokaži: Kompozicija $g \circ f$ dvaju homomorfizama je trivijalni homomorfizam onda i samo onda ako je $S(f) \subset J(g)$.

12. Neka je S_n simetrična grupa, a $\{-1, 1\} = I_1$ grupa s obzirom na množenje. Onda je funkcija pariteta (vidi točku 2.9.)

$$\text{sign} : S_n \to \{-1, 1\}$$

epimorfizam grupa. Što je njegova jezgra?

3.2. Izomorfizam grupa

Neka su G i H dane grupe. Kako smo već rekli, preslikavanje

$$f : G \to H$$

nazivamo **izomorfizam** grupe G na grupu H ako je ono:

(1) homomorfizam i

(2) bijekcija.

Specijalno, ako je $G = H$, izomorfizam f zovemo i **automorfizam** grupe G.

Kako smo vidjeli, $f : \mathbb{R} \to \mathbb{R}^*$, $f(x) = e^x$, jest homomorfizam, čak monomorfizam, ali nije izomorfizam, jer je uvijek $e^x > 0$. Ako, međutim, promijenimo kodomenu, preslikavanje

$$f : \mathbb{R} \to \mathbb{R}^+$$

bit će i surjekcija, dakle izomorfizam. Odmah se vidi da je i inverzno preslikavanje

$$g : \mathbb{R}^+ \to \mathbb{R} ,$$

dano s

$$g(x) = \ln x \ ,$$

izomorfizam grupa.

Dat ćemo sada jednu karakterizaciju izomorfizma.

PROPOZICIJA 1

Neka je $f : G \to H$ homomorfizam grupa. Onda je

(1) *f epimorfizam, ako i samo ako je $S(f) = H$;*

(2) *f monomorfizam, ako i samo ako je $J(f) = \{e\}$.*

Dokaz

Tvrdnja (1) je očigledna. Dokažimo (2). Pretpostavimo najprije da je f monomorfizam. Kako je prema Prop. 2 iz 3.1. $f(e) = e^*$, to je

$$e \in f^{-1}(e^*) = J(f) \ .$$

U drugu ruku, $J(f)$ ne sadrži više od jednog elementa, jer je f injekcija po pretpostavci. Dakle je zaista $J(f) = \{e\}$.

Obratno, pretpostavimo da je $J(f) = \{e\}$. Tvrdimo da je f monomorfizam. Treba samo vidjeti da je f injekcija. Neka su $x, y \in G$ elementi sa svojstvom da je $f(x) = f(y)$. Onda je, budući da je f homomorfizam,

$$f(x)\,[f(y)]^{-1} = e^* \quad \text{tj.} \quad f(xy^{-1}) = e^* \ ,$$

tj. prema pretpostavci

$$xy^{-1} \in J(f) = \{e\} \ .$$

Dakle je $xy^{-1} = e$, tj. $x = y$, što pokazuje da je f monomorfizam. ■

KOROLAR 2

Homomorfizam $f : G \to H$ je izomorfizam grupa ako i samo ako je surjekcija i vrijedi $J(f) = \{e\}$.

Dokaz

Neposredno iz Prop. 1. ■

PROPOZICIJA 3

Kompozicija $h = g \circ f$ izomorfizama grupa je izomorfizam grupa.

Dokaz

Neposredno iz Prop. 7 u 3.1. i činjenice da je kompozicija bijekcija opet bijekcija. ■

PROPOZICIJA 4

Neka je $f : G \to H$ izomorfizam grupa. Onda je $f^{-1} : H \to G$ također izomorfizam.

Dokaz

Prije svega, jer je f bijekcija, jasno je da f^{-1} postoji i da je bijekcija. Treba, dakle, još dokazati da je f^{-1} homomorfizam. Neka su $x, y \in H$ bilo koja dva elementa. Kako je f bijekcija, postoje jedinstveni elementi $a, b \in G$ takvi da je $f(a) = x$, $f(b) = y$. Onda je

$$f^{-1}(xy) = f^{-1}(f(a)f(b)) = f^{-1}(f(ab)) = ab = f^{-1}(x) \cdot f^{-1}(y) .$$ ■

Neka su G i H dvije grupe. Kažemo da je grupa G **izomorfna** grupi H i pišemo

$$G \cong H ,$$

ako postoji bar jedan izomorfizam

$$f : G \to H .$$

TEOREM 5

Relacija "biti izomorfan" je relacija ekvivalencije.

Dokaz

Treba vidjeti da je $\cong$ refleksivna, simetrična i tranzitivna.
Refleksivnost: $G \cong G$, jer je identiteta $e : G \to G$ očito izomorfizam.
Simetričnost: $G \cong H$ znači da postoji izomorfizam $f : G \to H$. No, onda je prema Prop. 4 i $f^{-1} : H \to G$ izomorfizam, pa je i $H \cong G$.
Tranzitivnost: iz $G \cong H$ i $H \cong K$ slijedi da postoje izomorfizmi $f : G \to H$ i $g : H \to K$. No, prema Prop. 3 je i $g \circ f : G \to K$ izomorfizam, što znači da je $G \cong K$. ■

Na osnovi teorema zaključujemo da se sve grupe mogu razvrstati u disjunktne klase, s time da pojedinu klasu čine one i samo one grupe koje su međusobno izomorfne. Sve grupe unutar jedne klase su, dakle, ekvipotentne i iste strukture, tj. **jednake** s apstraktnog stajališta, pa se za takve dvije grupe umjesto $G \cong H$ često piše i $G = H$.

Zapravo, predmet proučavanja u teoriji grupa su klase izomorfnih grupa, kao i odnosi između tih klasa. Takvu klasu, koju čine sve međusobno izomorfne grupe, nazivamo **apstraktna grupa**. Kako izomorfizam čuva strukturu u strogom smislu, iako na neki način razara individualnost, apstraktnom grupom je reprezentirana struktura zajednička mnogim grupama, koje mogu biti vrlo različite po naravi svojih elemenata.

ZADACI

1. Za dani element $a \in G$ definiramo preslikavanje $f_a : G \to G$ s

$$f_a(x) = axa^{-1} .$$

Pokaži da je f_a izomorfizam, dakle automorfizam grupe G. Taj se automorfizam naziva **unutrašnji automorfizam** od G određen elementom a.

2. Neka je s

$$\mathrm{Int}(G) = \{f_a \mid a \in G\}$$

označen skup svih unutrašnjih automorfizama grupe G. Pokaži da je $\mathrm{Int}(G)$ grupa u odnosu na komponiranje.

3. Neka je $h : G \to \mathrm{Int}(G)$ preslikavanje definirano s $h(a) = f_a$, za svaki $a \in G$. Pokaži da je h epimorfizam kojemu je jezgra centar $C(G)$ grupe G (vidi Zad. 4. u 2.7.).

4. Neka je G dana grupa. Na skupu G definiramo novu binarnu operaciju stavljajući

$$a * b = ba .$$

Pokaži da je $G^* = (G, *)$ također grupa, koju nazivamo **recipročnom grupom** od G. Definiramo

$$f : G \to G^*$$

s

$$f(x) = x^{-1} .$$

Pokaži da je f izomorfizam i prema tome je $G^* \cong G$.

5. Neka su $f : G \to H$ i $g : H \to K$ homomorfizmi sa svojstvom da je $g \circ f$ izomorfizam. Neka je $S = S(f)$, a $J = J(g)$. Onda vrijedi

   (a) $SJ = H = JS$;

   (b) $S \cap J = \{e\}$, gdje je e jedinica u H.

3.3. Primjeri izomorfizama

Navest ćemo nekoliko interesantnih primjera izomorfnih grupa.

1. Sve trivijalne grupe, grupe prvog reda, jesu očito izomorfne. Međutim, izomorfne su i sve grupe drugog reda. To izlazi iz jedinstvene tablice množenja. Neka je, naime, $G = \{a_0, a_1\}$ takva grupa i a_0 njezin neutralni element. Onda je svakako

$$a_0 \cdot a_0 = a_0 \quad \text{i} \quad a_1 \cdot a_0 = a_0 \cdot a_1 = a_1 \, .$$

Kad bi bilo $a_1 \cdot a_1 = a_1$, imali bismo zbog prethodnog $a_1 \cdot a_1 = a_1 \cdot a_0$, odnosno, nakon skraćivanja s a_1,

$$a_1 = a_0 \, ,$$

što nije moguće (jer bi onda G imala samo jedan element). Zato je $a_1 \cdot a_1 = a_0$ i tablica je nužno oblika

$\cdot$	a_0	a_1
a_0	a_0	a_1
a_1	a_1	a_0

.

2. Sve grupe trećeg reda su također izomorfne. I to izlazi iz jedinstvene tablice množenja. Naime, iz $G = \{a_0, a_1, a_2\}$ i činjenice da je a_0 neutralni element, imamo najprije

$$a_0 \cdot a_0 = a_0 \, , \; a_1 \cdot a_0 = a_0 \cdot a_1 = a_1 \, ,$$

$$a_2 \cdot a_0 = a_0 \cdot a_2 = a_2 \, .$$

Nadalje, $a_1 \cdot a_2 = a_1$ povlači $a_2 = a_0$, $a_1 \cdot a_2 = a_2$ povlači $a_1 = a_0$ što nije moguće. Dakle je $a_1 \cdot a_2 = a_0$. Slično se vidi da mora biti $a_2 \cdot a_1 = a_0$. Konačno, $a_1 \cdot a_1 = a_0$ bi zajedno s prethodnim dalo $a_1 \cdot a_1 = a_1 \cdot a_2$, dakle $a_1 = a_2$, što nije moguće. Isto tako $a_1 \cdot a_1 = a_1$ vodi na $a_1 = a_0$. Ostaje dakle mogućnost $a_1 \cdot a_1 = a_2$. Slično se vidi da mora biti $a_2 \cdot a_2 = a_1$, pa je tablica nužno oblika

$\cdot$	a_0	a_1	a_2
a_0	a_0	a_1	a_2
a_1	a_1	a_2	a_0
a_2	a_2	a_0	a_1

.

Na primjer, $\mathbb{Z}_3 \cong K_3 \cong R_3 =$ grupa rotacija trokuta.

3. Svaka grupa četvrtog reda izomorfna je ili s Kleinovom četvornom grupom V ili s grupom R_4 rotacija kvadrata, dakle svakako je komutativna. Pritom V i R_4 **nisu** izomorfne, što pokazuje da imamo dva bitno različita tipa grupa četvrtog reda. Dokaz prve tvrdnje provodi se posve analogno kao u prethodnom primjeru. Pokažimo da V i R_4 nisu izomorfne. Zaista, kad bi postojao izomorfizam

$$f : V \to R_4$$

imali bismo (ako elemente od R_4 označimo s $\overline{a}_i$)

$$f(a_0) = \overline{a}_0$$

i nadalje, za neki $i \neq 0$,

$$f(a_i) = \overline{a}_1 \ .$$

No, onda bi bilo

$$\begin{aligned} f(a_0) &= f(a_i + a_i) = f(a_i) + f(a_i) = \\ &= \overline{a}_1 + \overline{a}_1 = \overline{a}_2 \neq \overline{a}_0 \ , \end{aligned}$$

što je kontradikcija.
Na primjer, $R_4 \cong \mathbb{Z}_4 \cong I_2 = K_4$, a $V \cong G$ (romba) $\cong$ grupa rotacija tetraedra oko transverzala suprotnih bridova.

4. Sve grupe reda 5 su izomorfne. Dokaži!

5. Grupe reda 6 mogu biti i nekomutativne i prema tome nisu sve izomorfne. Na primjer, grupa $\mathbb{Z}_6$ je komutativna, a grupa F iz Prim. 15. u 2.8. nije komutativna. Uvjeri se, da je $F \cong S_3$. Pokaži, nadalje, da je svaka grupa reda 6 izomorfna sa $\mathbb{Z}_6$ ili S_3.

6. Dokaži: $\mathbb{C} \cong \mathbb{R}^2$. Izomorfizam je

$$x + iy \mapsto (x, y) \ .$$

7. Kako smo vidjeli, za svaki $m \in \mathbb{Z}$ je $m\mathbb{Z}$ podgrupa od $\mathbb{Z}$. Neka je $m \neq 0$. Pokaži da je

$$f : \mathbb{Z} \to m\mathbb{Z}$$

definirano s

$$f(x) = mx$$

izomorfizam grupa. Primjer pokazuje da grupa može biti izomorfna svojoj pravoj podgrupi; to je fenomen koji se ne može pojaviti kod konačnih grupa.

8. Grupa tetraedra izomorfna je s grupom S_4. Ako vrhove tetraedra označimo s a_1, a_2, a_3, a_4, imamo prirodni izomorfizam

$$p = \begin{pmatrix} 1 & 2 & 3 & 4 \\ p_1 & p_2 & p_3 & p_4 \end{pmatrix} \mapsto \left\{ \begin{array}{l} a_1 \to a_{p_1} \\ a_2 \to a_{p_2} \\ a_3 \to a_{p_3} \\ a_4 \to a_{p_4} \end{array} \right\} = t \, .$$

Na primjer,

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{pmatrix} \mapsto \left\{ \begin{array}{l} a_1 \to a_1 \\ a_2 \to a_3 \\ a_3 \to a_4 \\ a_4 \to a_2 \end{array} \right\} =$$

$$= \text{rotacija tetraedra za } 2\pi/3 \text{ oko visine kroz } a_1 \, .$$

Uvjeri se da se radi zaista o izomorfizmu. Pokaži, nadalje, da je podgrupa rotacija tetraedra izomorfna s alternirajućom grupom A_4.

ZADACI

1. Dokaži: Grupa G je komutativna onda i samo onda ako je preslikavanje $f : G \to G$ dano s $f(x) = x^{-1}$ automorfizam od G.

2. Svaka beskonačna ciklička grupa je izomorfna s grupom $\mathbb{Z}$, a svaka konačna ciklička grupa reda m je izomorfna sa $\mathbb{Z}_m$. Dokaži!

3. Neka je p prim broj. Onda su sve grupe reda p međusobno izomorfne.

3.4. Cayleyjev teorem

Dokazat ćemo sada klasični teorem A. Cayleyja, koji kaže da se svaka grupa može do na izomorfizam reprezentirati nekom grupom permutacija. Teorem upućuje na važnost i univerzalnost grupa permutacija, tj. na činjenicu da je cijela teorija grupa zapravo obuhvaćena svojstvima grupa permutacija.

Neka je G grupa i $a \in G$ bilo koji njezin element. Onda smo definirali lijevu translaciju u G određenu s a (vidi Prim. 18. u 2.8.) kao preslikavanje

$$l_a : G \to G$$

dano s

$$l_a(x) = a\,x \, .$$

PROPOZICIJA 1

Za svaki $a \in G$ je l_a bijekcija.

Dokaz

Neka su $x, y \in G$ bilo koji elementi, za koje je

$$l_a(x) = l_a(y) \ .$$

Po definiciji to znači da je $ax = ay$, odnosno, nakon skraćivanjanja s a,

$$x = y \ ,$$

što pokazuje da je l_a injekcija. Nadalje, neka je $y \in G$ bilo koji element. Za $x = a^{-1}y$ onda imamo:

$$l_a(x) = l_a(a^{-1}y) = a(a^{-1}y) = (aa^{-1})y = y \ ,$$

što pokazuje da je l_a i surjekcija. ■

Na osnovi Prop. 1 zaključujemo da je l_a permutacija od G, $l_a \in B(G)$, za svaki $a \in G$. Definirajmo sada preslikavanje

$$j : G \to B(G)$$

na prirodan način,

$$j(a) = l_a \ ,$$

za svaki $a \in G$. Vrijedi:

PROPOZICIJA 2

Preslikavanje j je monomorfizam.

Dokaz

Pokažimo najprije da je j homomorfizam. Zaista, neka su $a, b \in G$ bilo koji elementi. Onda za po volji odabrani $x \in G$ vrijedi

$$\begin{aligned} [j(ab)](x) &= l_{ab}(x) = (ab)x = a(bx) = l_a(bx) = \\ &= l_a[l_b(x)] = [l_a \circ l_b](x) = [j(a) \circ j(b)](x) \ , \end{aligned}$$

dakle

$$j(ab) = j(a) \circ j(b) \ ,$$

tj. j je zaista homomorfizam. Ostaje vidjeti da je j injekcija. Zaista, neka je $j(a) = j(b)$. To znači da je $l_a = l_b$, dakle

$$l_a(x) = l_b(x)$$

za svaki $x \in G$. No, ta formula znači da je $ax = bx$, odnosno, nakon skraćivanja s x u grupi G,

$$a = b\,,$$

što pokazuje da je j i injekcija, dakle monomorfizam. ■

TEOREM 3 (Cayley)

Svaka je grupa izomorfna nekoj grupi permutacija. Točnije, grupa G je izomorfna s podgrupom $j(G) < B(G)$ grupe $B(G)$ svih permutacija skupa G.

Dokaz

Kako je j homomorfizam, $j(G) = S(j)$ je podgrupa od $B(G)$. Nadalje, jer je j monomorfizam,

$$j : G \to j(G)$$

je očito izomorfizam. ■

Ako je G konačna grupa, Cayleyjev teorem se može iskazati i u drugačijoj formi. Najprije, imamo

LEMA 4

Ako su skupovi S i T ekvipotentni, pripadne grupe permutacija su izomorfne, tj. $B(S) \cong B(T)$.

Dokaz

Neka je $f : S \to T$ bijekcija, koja postoji jer su skupovi S i T ekvipotentni. Definiramo preslikavanje

$$f^* : B(S) \to B(T)$$

stavljajući za svaku permutaciju $p \in B(S)$

$$f^*(p) = f \circ p \circ f^{-1}\,.$$

Kako je kompozicija bijekcija opet bijekcija, $f^*(p)$ je permutacija od T, tj. f^* je dobro definirano preslikavanje. Tvrdimo da je f^* izomorfizam. Lako se provjeri da je f^* bijekcija. Pokažimo da je homomorfizam. Zaista, za $p, q \in B(S)$ imamo

$$f^*(pq) = f \circ (pq) \circ f^{-1} = (f \circ p \circ \underbrace{f^{-1}}_{e})\,(\underbrace{f}\circ q \circ f^{-1}) = f^*(p) f^*(q)$$

i tvrdnja je dokazana. ■

Odatle

KOROLAR 5

Konačna grupa reda n izomorfna je nekoj podgrupi simetrične grupe S_n stupnja n.

Dokaz

Ako je G reda n, onda je prema prethodnoj lemi

$$B(G) \cong B(1, 2, \ldots, n) = S_n ,$$

pa tvrdnja slijedi iz Tm. 3. ■

3.5. Normalne podgrupe

U daljnjim će nam konstrukcijama biti od važnosti neke specijalne podgrupe dane grupe, tzv. normalne podgrupe.

Neka je G grupa, a $N < G$ njezina podgrupa. Kažemo da je N **normalna podgrupa** od G, ako je ispunjeno

$$x^{-1}Nx \subset N \tag{1}$$

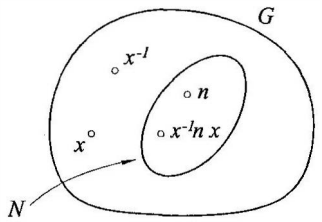
za svaki $x \in G$. Kako je

$$x^{-1}Nx = \{x^{-1}nx \mid n \in N\} ,$$

vidimo da će N biti normalna podgrupa onda i samo onda ako je

$$x^{-1}nx \in N$$

za svaki $x \in G$ i $n \in N$.



Definicijski uvjet (1) može se napisati i u ljepšoj formi. Neka je, naime, $y = x^{-1}$. Onda je po definiciji također

$$y^{-1}Ny \subset N \,,$$

odnosno

$$N \subset yNy^{-1} \,,$$

dakle

$$N \subset x^{-1}Nx \,. \tag{2}$$

Uspoređujući (1) i (2) dobivamo

$$x^{-1}Nx = N$$

kao karakterističnu relaciju za normalnost podgrupe. Ta se relacija zapisuje još u simetričnoj formi kao

$$Nx = xN \quad , \quad \text{za svaki } x \in G \,.$$

Mnogi autori uzimaju upravo tu relaciju kao definicijsku za normalnu podgrupu. Za normalnu podgrupu je uobičajena oznaka

$$N \lhd G \,.$$

Primijetimo da prethodna relacija ne tvrdi da svaki element od N komutira s x. Tvrdnja je blaža, tj. da $\{x\}$ i N komutiraju na razini skupova.

Svaka grupa ima normalnih podgrupa. To su npr. čitava grupa G i jedinica $\{e\}$ te grupe. Ako G osim ovih trivijalnih normalnih podgrupa nema drugih, kažemo da je **jednostavna** ili **prosta**.

Očito je da su u komutativnoj grupi sve podgrupe normalne. Kao daljnji primjer promatrajmo grupu S_3 i njezinu alternirajuću podgrupu

$$A_3 = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \right\} \,.$$

Onda je A_3 normalna podgrupa od S_3. Provjeri! Naprotiv,

$$H = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \right\}$$

jest podgrupa od S_3, ali nije normalna, jer npr.

$$aba^{-1} = \underbrace{\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}}_{a} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \underbrace{\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}}_{a^{-1}} =$$

$$= \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \notin H \quad .$$

Navedimo nekoliko jednostavnih svojstava normalnih podgrupa.

PROPOZICIJA 1

Neka su $M, N \lhd G$ normalne podgrupe od G. Onda je i $M \cap N$ normalna podgrupa od G.

Dokaz

Prije svega, $M \cap N$ je podgrupa od G. Neka su $x \in G$ i $a \in M \cap N$ bilo koji elementi. Treba vidjeti da je $x^{-1}ax \in M \cap N$. Ali, $a \in M$ i M je normalna, pa je $x^{-1}ax \in M$. Slično, zbog normalnosti od N, imamo $x^{-1}ax \in N$, dakle i $x^{-1}ax \in M \cap N$, što se i tvrdilo. ■

Analogno se pokazuje da je presjek bilo kojeg broja normalnih podgrupa od G opet normalna podgrupa od G.

PROPOZICIJA 2

Neka je $f : G \to H$ epimorfizam grupa i $N \lhd G$ normalna podgrupa od G. Onda je slika $f(N) < H$ normalna podgrupa od H.

Dokaz

Znamo da je $f(N)$ podgrupa od H. Treba dokazati normalnost. Neka je $y \in H$ i $b \in f(N)$. Kako je f surjekcija, postoji $x \in G$ tako da je $f(x) = y$. Postoji, naravno, i $a \in N$ sa svojstvom da je $f(a) = b$. Kako je N normalna po pretpostavci, to je

$$x^{-1}ax \in N \ ,$$

dakle $f(x^{-1}ax) \in f(N)$, tj. $[f(x)]^{-1}f(a)f(x) \in f(N)$ i onda

$$y^{-1}by \in f(N) \ ,$$

što pokazuje da je $f(N)$ zaista normalna podgrupa. ■

PROPOZICIJA 3

Neka je $f : G \to H$ homomorfizam grupa i $M \lhd H$ normalna podgrupa od H. Onda je praslika $f^{-1}(M) < G$ normalna podgrupa od G.

Dokaz

Prije svega, $f^{-1}(M)$ je podgrupa od G. Nadalje, za $x \in G$ i $a \in f^{-1}(M)$ imamo

$$[f(x)]^{-1} \cdot \underbrace{f(a)}_{\in M} \cdot f(x) \in M$$

jer je M normalna po pretpostavci. Odatle pak slijedi $f(x^{-1}ax) \in M$, tj.

$$x^{-1}ax \in f^{-1}(M)\,,$$

što pokazuje da je $f^{-1}(M)$ zaista normalna podgrupa. ■

KOROLAR 4

Neka je $f : G \to H$ homomorfizam grupa. Onda je jezgra $J(f)$ normalna podgrupa od G. ■

ZADACI

1. Podgrupe $\mathcal{T}$, $\mathcal{R}_a < \mathcal{G}$ svih translacija, odnosno svih rotacija ravnine sa središtem u danoj točki a jesu normalne podgrupe grupe $\mathcal{G}$ gibanja ravnine. Dokaži!

2. Alternirajuća grupa $A_n < S_n$ je normalna podgrupa od S_n. Dokaži! Zanimljivo je spomenuti da je A_n, uz $n \neq 4$, uvijek jednostavna grupa. To je poznati Jordanov teorem (1870.), koji se dokazuje dosta teško, pomoću **Galoisove teorije**.

3. Dokaži: Podgrupa $H < G$ je normalna onda i samo onda ako je $f(H) = H$ za svaki unutrašnji automorfizam f grupe G. Zato se normalne podgrupe zovu još i **invarijantne podgrupe** od G.

4. Neka je $C(G) < G$ centar grupe G. Svaka podgrupa od $C(G)$ je normalna podgrupa od G. Te se podgrupe zovu **centralne normalne podgrupe** od G. Posebno, sam centar je normalna podgrupa od G.

5. Komutatorska podgrupa $[K] < G$ je normalna podgrupa od G. Dokaži!

6. Neka su $H, N < G$ podgrupe od G i neka je N normalna. Onda je $HN \subset G$ podgrupa od G. Nadalje, ako je i H normalna, onda je HN normalna podgrupa.

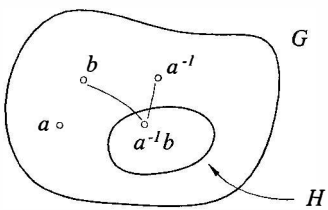
7. Neka je S skup koji se sastoji od bar tri elementa. Neka je $s_0 \in S$ i $B(S, s_0)$ skup svih permutacija $p : S \to S$ sa svojstvom $p(s_0) = s_0$. Pokaži da je $B(S, s_0)$ podgrupa od $B(S)$ i da **nije normalna**.

8. Dokaži da je $\mathrm{Int}(G)$ normalna podgrupa grupe svih automorfizama grupe G.

3.6. Susjedne klase. Lagrangeov teorem

Svakom je podgrupom definirana na prirodan način neka dekompozicija grupe.

Neka je, naime, $H < G$ podgrupa od G. Onda na G možemo definirati



relaciju $\sim$ stavljajući $a \sim b$ za $a, b \in G$ ako i samo ako je $a^{-1}b \in H$.

PROPOZICIJA 1

Relacija $\sim$ je relacija ekvivalencije na grupi G.

Dokaz

Refleksivnost: za svaki je $a \in G$ je $a^{-1}a = e \in H$, pa je $a \sim a$.

Simetričnost: iz $a \sim b$ imamo $a^{-1}b \in H$. No onda je i $(a^{-1}b)^{-1} = b^{-1}a \in H$, tj. $b \sim a$.

Tranzitivnost: iz $a \sim b$ i $b \sim c$ slijedi da je $a^{-1}b \in H$ i $b^{-1}c \in H$, pa je i $(a^{-1}b)(b^{-1}c) = a^{-1}c \in H$ tj. $a \sim c$. ■

Prema tome, relacija $\sim$ dijeli elemente od G u disjunktne podskupove, klase ekvivalencije u odnosu na $\sim$. Neka je za $a \in G$ s

$$[a] = \{x \in G \mid x \sim a\}$$

označena klasa ekvivalencije generirana elementom a.

PROPOZICIJA 2

Za svaki je element $a \in G$

$$[a] = aH = \{ay \mid y \in H\} .$$

Dokaz

Neka je $x \in [a]$. To znači da je $a \sim x$, dakle $a^{-1}x \in H$ i prema tome $x \in aH$, pa je inkluzija $[a] \subset aH$ dokazana. Obratno, neka je $x \in aH$. Onda je $x = ay$, gdje je $y \in H$, dakle $a^{-1}x = y \in H$, što pokazuje da je $a \sim x$, tj. da je $x \in [a]$, pa je dokazano i $aH \subset [a]$. ■

Iz Prop. 1 i Prop. 2 slijedi neposredno

KOROLAR 3

Neka su $a, b \in G$ bilo koji elementi. Onda je

(1) $aH = bH$, *ako je* $a \sim b$,

(2) $aH \cap bH = \emptyset$, *ako* $a \not\sim b$. ■

Skupove aH, za $a \in G$ nazivamo **lijeve susjedne klase** podgrupe H u grupi G. Neka je s Q označen skup svih različitih lijevih susjednih klasa,

$$Q = \{aH \mid a \in G\} .$$

Taj skup se zove **lijevi kvocijentni skup** grupe G po podgrupi H i piše

$$Q = G/H .$$

Posve analogno, definirajući na G relaciju ekvivalencije s $a \sim b$ ako i samo ako je $ab^{-1} \in H$, došli bismo do klasa ekvivalencije $[a] = Ha$, koje nazivamo **desne susjedne klase** podgrupe H u grupi G i do **desnog kvocijentnog skupa**

$$H \setminus G = \{Ha \mid a \in G\} .$$

Općenito je, dakako,

$$G/H \neq H \setminus G ,$$

posebno

$$aH \neq Ha$$

jer H ne mora biti normalna.

Vrijedi međutim

PROPOZICIJA 4

Skupovi G/H i $H \setminus G$ su ekvipotentni.

Dokaz

Za pridruživanje

$$aH \mapsto (aH)^{-1} = Ha^{-1}$$

lako se pokaže da je bijekcija. ■

Taj zajednički kardinalni broj kvocijentnih skupova naziva se **indeks podgrupe** H **u grupi** G i piše

$$\mu = (G : H) .$$

Ako je taj broj konačan, kažemo da je H **podgrupa konačnog indeksa**.

Neka je sada G konačna grupa, kažimo reda m, a H neka njezina podgrupa reda n. Onda vrijedi

PROPOZICIJA 5

Za svaki element $a \in G$ lijeva susjedna klasa aH (desna susjedna klasa Ha) ima točno n elemenata.

Dokaz

Tvrdimo da je $f : H \to aH$, definirano s $f(x) = ax$, bijekcija. Očito je da je f surjekcija, ali je i injekcija, jer iz $f(x) = f(y)$ slijedi $ax = ay$, pa je $x = y$. Prema tome, aH ima isto toliko elemenata kao i H, dakle n. ■

Kako su susjedne klase disjunktne, imamo ovu situaciju

G

n	n	n
n	H	n
n	n	n

.

Odatle odmah razabiremo

KOROLAR 6

Ako je G konačna grupa, za indeks μ podgrupe H u grupi G vrijedi

$$\mu = \frac{m}{n} .$$

■

Prema tome, m/n mora biti cijeli broj, pa odatle neposredno slijedi poznati Lagrangeov teorem

KOROLAR 7 (Lagrange)

Red grupe je višekratnik reda svake njezine podgrupe. ■

Ako je, dakle, red grupe prim broj, ta grupa ne može imati pravih podgrupa. Na primjer, $\mathbb{Z}_3$, $\mathbb{Z}_7$ nemaju pravih podgrupa.

Zanimljivo je spomenuti da obrat Lagrangeova teorema, koji bi tvrdio da ako je n djelitelj od m, grupa reda m sigurno sadrži podgrupe reda n, nije točan. Može se npr. pokazati da grupa A_4 nema podgrupe reda 6.

ZADACI

1. Nađi lijevi i desni kvocijentni skup grupe G po grupi H, ako je $H = G$ odnosno $H = \{e\}$.

2. Nađi G/H i $H \setminus G$, ako je $G = S_3$, a
$$H = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \right\} .$$

3. Dokaži: Red bilo kojeg elementa konačne grupe je mjera reda grupe.

4. Dokaži: Svaka konačna grupa reda koji je prim broj je ciklička i generirana bilo kojim svojim elementom različitim od jedinice.

3.7. Kvocijentna grupa

Kako smo već vidjeli, množenje u grupi G inducira na prirodan način binarnu operaciju, množenje u partitivnom skupu $\mathcal{P}(G)$. Imamo, naime,

$$AB = \{ab \mid a \in A, b \in B\} \subset G ,$$

dakle $AB \in \mathcal{P}(G)$ za svaki $A, B \in \mathcal{P}(G)$. To je množenje skupova očito asocijativno,

$$(AB)C = A(BC) ,$$

ali općenito nije komutativno, tj.

$$BA \neq AB .$$

Zapravo, $\mathcal{P}(G)$, uz to množenje, ima strukturu monoida s jedinicom $\{e\}$.

Vratimo se sada našem problemu. Za danu podgrupu $H < G$ grupe G definirali smo pojam lijevog, odnosno desnoga kvocijentnog skupa. Željeli bismo sada te skupove organizirati u grupu, dakako, uz prirodno množenje klasa inducirano množenjem u G, kako smo to upravo definirali. To, međutim, općenito nije moguće jer npr. za klase $[a], [b] \in G/H$ imamo

$$[a] \cdot [b] = (aH)(bH) \in \mathcal{P}(G) ,$$

a za taj produkt općenito nema razloga da bude oblika xH, dakle klasa, tj. element iz G/H; dakle, u odnosu na takvo množenje skup G/H nije zatvoren.

Stvar se, međutim, može popraviti ako (i samo ako, vidi Zad. 2.) pretpostavimo da je podgrupa $H = N$ normalna podgrupa od G. Prije svega, onda je po definiciji

$$aN = Na$$

za svaki $a \in G$, što pokazuje da se lijeve susjedne klase podudaraju s desnim i, odatle,

$$G/N = N \setminus G\,,$$

tj. lijevi je kvocijent jednak desnom, pa govorimo jednostavno o **kvocijentnom skupu**

$$Q = G/N = \{[a] = aN \mid a \in G\}$$

grupe G po normalnoj podgrupi N. Sada je i prirodno množenje klasa dobro definirana binarna operacija, jer za $[a], [b] \in G/N$ vrijedi

$$\begin{aligned} [a] \cdot [b] &= (aN)(bN) = a(Nb)N = \\ &= a(bN)N = (ab)(NN) = (ab)N = [ab] \in G/N\,. \end{aligned}$$

TEOREM 1

Neka je $N \lhd G$ normalna podgrupa od G. Onda je kvocijentni skup $Q = G/N$, uz prirodno množenje klasa kao binarnu operaciju, grupa.

Dokaz

Asocijativnost slijedi iz definicije množenja u $\mathcal{P}(G)$, ali se može verificirati i neposredno:

$$([a] \cdot [b]) \cdot [c] = [ab] \cdot [c] = [(ab)c] = [a(bc)] = [a] \cdot [bc] = [a] \cdot ([b] \cdot [c])\,.$$

Klasa $[e] = eN = N$ igra ulogu lijeve jedinice, jer je $[e][a] = [ea] = [a]$ za svaku klasu $[a] \in Q$. Konačno, za klasu $[a] \in Q$ je lijevi inverz $[a]^{-1} = [a^{-1}] \in Q$, jer imamo

$$[a^{-1}][a] = [a^{-1}a] = [e]\,.$$

Prema tome je Q zaista grupa (po Tm. 1 iz 2.6.), s $[e] = N$ kao jedinicom i klasom $[a^{-1}] = a^{-1}N$ kao inverzom za $[a] = aN$. ∎

Grupa $Q = G/N$ naziva se **kvocijentna grupa** ili **faktorska grupa** grupe G po normalnoj podgrupi N. U slučaju kad je grupa Q konačna, njezin se red očito podudara s indeksom podgrupe N u grupi G.

Primijetimo još da je $Q \subset \mathcal{P}(G)$ podgrupa monoida $\mathcal{P}(G)$.

Ako je grupa G komutativna, onda je i kvocijentna grupa G/N komutativna, jer imamo

$$[a] \cdot [b] = [ab] = [ba] = [b] \cdot [a] .$$

Obrat, međutim, ne vrijedi općenito. Na primjer, za bilo koju grupu G je kvocijent

$$G/G = \{\text{jedna klasa}\} = \{G\}$$

trivijalna grupa, dakle Abelova.

Klasični primjer kvocijenta čine tzv. **klase ostataka**. Neka je $m \in N$ dani prirodni broj. Onda je

$$m\mathbb{Z} < \mathbb{Z}$$

podgrupa od $\mathbb{Z}$, i to normalna (jer je $\mathbb{Z}$ komutativna), pa prema tome postoji kvocijentna grupa

$$Q = \mathbb{Z}/m\mathbb{Z}$$

i tu grupu nazivamo **grupa klasa ostataka modulo m**.

Elementi te grupe su klase, dakle podskupovi od $\mathbb{Z}$ oblika

$$[k] = k + m\mathbb{Z} ,$$

za $k \in \mathbb{Z}$. Očito je da među klasama ima samo m različitih

$$\left.\begin{array}{rcl} [0] & = & m\mathbb{Z} \\ [1] & = & 1 + m\mathbb{Z} \\ \cdot & \cdot & \cdot \\ [m-1] & = & (m-1) + m\mathbb{Z} \end{array}\right\} m$$

jer je npr.

$$\begin{aligned} [m] &= m + m\mathbb{Z} = m(1 + \mathbb{Z}) = m\mathbb{Z} = [0] , \\ [m+1] &= (m+1) + m\mathbb{Z} = 1 + (m + m\mathbb{Z}) = \\ &= 1 + m\mathbb{Z} = [1] , \\ [-1] &= -1 + m\mathbb{Z} = (m-1) - m + m\mathbb{Z} = \\ &= (m-1) + m(-1 + \mathbb{Z}) = (m-1) + m\mathbb{Z} = \\ &= [m-1] , \quad \text{itd.} \end{aligned}$$

Prema tome je $\mathbb{Z}/m\mathbb{Z}$ grupa reda m. Njezini su elementi skupovi cijelih brojeva koji pri dijeljenju s m imaju redom ostatak $0, 1, \ldots, m-1$, pa se zato i zovu klase ostataka u odnosu na dijeljenje s m ili modulo m.

Spomenimo na kraju, da se uz kvocijentnu grupu $Q = G/N$ prirodno veže preslikavanje

$$p : G \to G/N ,$$

definirano s

$$p(a) = [a] ,$$

koje nazivamo **prirodna projekcija** grupe G na kvocijent G/N.

PROPOZICIJA 2

Prirodna projekcija je epimorfizam s jezgrom

$$J(p) = N .$$

Dokaz

Očito je da je p . Pokažimo da je homomorfizam. Imamo

$$p(ab) = [ab] = [a] \cdot [b] = p(a)\, p(b) .$$

Konačno

$$J(p) = p^{-1}([e]) = p^{-1}(N) = N$$

pa je tvrdnja dokazana. ■

ZADACI

1. Dokaži ovu karakterizaciju normalnosti podgrupe: Podgrupa $N < G$ je normalna onda i samo onda ako je jezgra nekog homomorfizma $h : G \to H$ u neku grupu H (vidi Kor. 4 u 3.5. i Prop. 2).

2. Dokaži: Podgrupa $N < G$ je normalna onda i samo onda ako je

   $$(aN)(bN) = (ab)N$$

   za svaki $a, b \in G$. (Nužnost smo vidjeli u tekstu.)

3. U kvocijentnom skupu G/H definiraj binarnu relaciju formalno s

   $$[a] \cdot [b] = [ab] .$$

   Pokaži da je to dobro definirana relacija, tj. da ne ovisi o izboru reprezentanata klase, onda i samo onda ako je H normalna.

4. Pokaži da je s $a \mapsto [a]$ dan izomorfizam grupa G i $G/\{e\}$. Zato obično pišemo $G/\{e\} = G$.

5. Ispitaj i prikaži tablično grupu $\mathbb{Z}/5\mathbb{Z}$. Što opažaš?

6. Pokaži da je općenito, za svaki $m \in \mathbb{Z}$,

   $$\mathbb{Z}/m\mathbb{Z} \cong \mathbb{Z}_m .$$

7. Za dani $m \in N$ na skupu $\mathbb{Z}$ definiramo relaciju $\equiv$, stavljajući $a \equiv b \pmod{m}$ ako i samo ako je $a - b = km$, $k \in \mathbb{Z}$, koju nazivamo **relacijom kongruencije** modulo m. Pokaži da je $\equiv$ relacija ekvivalencije. Uoči da se radi o relaciji koja razlaže skup $\mathbb{Z}$ u klase ostataka mod m, tj. da je
$$\mathbb{Z}/_{\equiv} = \mathbb{Z}/m\mathbb{Z}$$
(aditivan zapis!). Prema tome klase ostataka možemo pisati i kao
$$[k] = \{x \in \mathbb{Z} \mid x \equiv k \pmod{m}\} .$$

8. Za $\mathbb{Z} < \mathbb{R}$ ispitaj kvocijent $\mathbb{R}/\mathbb{Z}$ koji se naziva **grupa realnih brojeva** mod 1. Kako izgledaju elementi od $\mathbb{R}/\mathbb{Z}$ i koliko ih ima?

9. Za $S^1 < \mathbb{C}^*$ ispitaj kvocijent $\mathbb{C}^*/S^1$ i interpretiraj geometrijski susjedne klase u kompleksnoj ravnini.

10. S_n/A_n je grupa reda dva. Dokaži!

11. Kvocijentna grupa cikličke grupe po nekoj podgrupi je opet ciklička grupa. Dokaži!

12. Interpretiraj geometrijski kvocijente $\mathcal{G}/\mathcal{T}$ i $\mathcal{G}/\mathcal{R}_a$.

13. Neka je $C = C(G)$ centar grupe G. Pokaži da je
$$G/C \cong \mathrm{Int}\,(G) .$$

14. Neka je $[K] < G$ komutatorska podgrupa od G. Pokaži da je $G/[K]$ komutativna grupa. Pokaži, nadalje, da je $[K]$ sadržana u svakoj normalnoj podgrupi N od G, za koju je kvocijentna grupa G/N komutativna.

3.8. Teorem o izomorfizmu

Neka su G i H bilo koje grupe, a $M \lhd G$ i $N \lhd H$ njihove normalne podgrupe. Neka su
$$G^* = G/M \quad , \quad H^* = H/N$$
pripadne kvocijentne grupe, a
$$p : G \to G^* \quad , \quad q : H \to H^*$$
prirodne projekcije.

Neka je sada

$$h : (G, M) \to (H, N)$$

bilo koji **homomorfizam parova**, tj. homomorfizam

$$h : G \to H .$$

sa svojstvom

$$h(M) \subset N .$$

To se svojstvo prenosi onda i na susjedne klase. Vrijedi naime

PROPOZICIJA 1

Za bilo koji $a \in G$ vrijedi

$$h(aM) \subset h(a)N .$$

Dokaz

Neka je $x \in M$ bilo koji element. Onda je

$$h(ax) = h(a)h(x) \in h(a)h(M) \subset h(a)N ,$$

dakle $h(aM) \subset h(a)N$. ■

Tako smo došli do prirodnog pridruženja

$$aM \mapsto h(a)N$$

kojim je definirano preslikavanje

$$h^* : G^* \to H^* .$$

PROPOZICIJA 2

Preslikavanje h^* je homomorfizam kvocijentnih grupa.

Dokaz

Neka su $a, b \in G$ bilo koji elementi. Onda vrijedi

$$\begin{aligned} h^*[(aM)(bM)] &= h^*[(ab)M] = h(ab)N = h(a)h(b)N = \\ &= [h(a)N]\,[h(b)N] = h^*(aM) \cdot h^*(bM) \end{aligned}$$

pa je h^* zaista homomorfizam. ■

Iz definicije od h^* se vidi da to preslikavanje ovisi o izboru homomorfizma h. Zato kažemo da homomorfizam h inducira homomorfizam h^* na razini kvocijentnih grupa ili da je h^* **inducirani homomorfizam od** h.

TEOREM 3

Ako je h^* inducirani homomorfizam od h, sljedeći je dijagram

$$\begin{array}{ccc} G & \xrightarrow{h} & H \\ {\scriptstyle p}\downarrow & & \downarrow{\scriptstyle q} \\ G^* & \xrightarrow{h^*} & H^* \end{array}$$

komutativan, tj. vrijedi

$$q \circ h = h^* \circ p \, .$$

Dokaz

Neka je $a \in G$ bilo koji element. Onda imamo

$$\begin{aligned} (q \circ h)(a) &= q[h(a)] = h(a)N = h^*(aM) = \\ &= h^*[p(a)] = (h^* \circ p)(a) \, . \end{aligned}$$

Kako je to istina za svaki $a \in G$, zaključujemo da je zaista $q \circ h = h^* \circ p$. ■

KOROLAR 4

Vrijedi:

$$\begin{aligned} S(h^*) &= q[S(h)] \\ J(h^*) &= p[h^{-1}(N)] \, . \end{aligned}$$

Dokaz

Kako je p epimorfizam, na osnovi komutativnosti dijagrama u Tm. 3 imamo

$$\begin{aligned} S(h^*) &= h^*(G^*) = h^*[p(G)] = (h^* \circ p)(G) = (q \circ h)(G) = \\ &= q[h(G)] = q[S(h)] \, . \end{aligned}$$

Slično se dokazuje i druga jednakost. ■

Kao posljedicu Tm. 3 i Kor. 4 dobivamo

TEOREM 5 (Teorem o izomorfizmu grupa)

Neka je $h : G \to H$ epimorfizam grupa, a $J = J(h)$ njegova jezgra. Onda je kvocijentna grupa G/J izomorfna s grupom H. I više, postoji izomorfizam

$$h^* : G/J \to H$$

sa svojstvom da je dijagram

$$\begin{array}{ccc} G & \xrightarrow{h} & H \\ & {\scriptstyle p}\searrow \quad \nearrow{\scriptstyle h^*} & \\ & G/J & \end{array}$$

komutativan, tj. da vrijedi $h^* \circ p = h$.

Dokaz

Primijenimo prethodnu konstrukciju na slučaj kad je $M = J =$ jezgra od h, a $N = h(M) = \{e\}$, gdje je e jedinica u grupi H. Onda je $G^* = G/J$, $H^* = H/\{e\} = H$, a q je identiteta, pa se komutativni dijagram iz Tm. 3 reducira na komutativni trokut naveden u izreci teorema. Pokažimo da je h^* izomorfizam. Jasno je da je h^* homomorfizam. Dalje, iz Kor. 4 slijedi (jer je h epimorfizam po pretpostavci)

$$S(h^*) = q[S(h)] = H$$

pa je h^* epimorfizam. Nadalje je

$$J(h^*) = p[h^{-1}(N)] = p[h^{-1}(e)] = p(J) = \{J\}$$

J je jedinica u G/J i, prema tome, h^* je zaista izomorfizam. ■

KOROLAR 6

Neka je $f : G \to H$ homomorfizam grupa. Onda je

$$G/J(f) \cong S(f) \, .$$ ■

ZADACI

1. Dokaži Tm. 5 direktno, neovisno o prethodnim rezultatima. [Uputa: Definiraj $h^* : G/J \to H$ sa $h^*(aJ) = h(a)$, pa pokaži da je to izomorfizam.]

2. Koristeći Tm. 5 dokaži:

   (a) $\mathbb{Z}/m\mathbb{Z} \cong \mathbb{Z}_m$;

   (b) $\mathbb{R}/\mathbb{Z} \cong S^1$;

   (c) $G/C \cong \operatorname{Int} G$ $\quad (C =$ centar grupe $G)$.

3. Pokušaj dokazati ovaj teorem: Neka su $N, H < G$ podgrupe od G, N normalna. Onda je i $H \cap N$ normalna podgrupa od G i vrijedi

$$HN/N \cong H/\, H \cap N \, .$$

4. Dokaži i ovaj teorem: Neka je $H/N \subset G/N$ normalna podgrupa u G/N, gdje je N normalna podgrupa od G. Onda je H normalna podgrupa od G i vrijedi

$$\frac{G/N}{H/N} \cong G/H \, .$$

Napomenimo, da se Tm. 5 iz teksta, te teoremi iz Zad. 3. i 4., u literaturi spominju obično kao **prvi**, **drugi**, odnosno **treći teorem o izomorfizmu grupa**.

3.9. Direktni produkt grupa

Neka su G i H dane grupe. Promatrajmo Kartezijev produkt

$$P = G \times H = \{(a, b) \mid a \in G, b \in H\}$$

skupova G i H. Želimo P organizirati u grupu, na prirodan način. U tu svrhu definiramo na P binarnu operaciju, stavljajući za $c_1, c_2 \in P$

$$c_1 \cdot c_2 = (a_1, b_1) \cdot (a_2, b_2) = (a_1 a_2, b_1 b_2) \in P \, .$$

PROPOZICIJA 1

Uz tako definirano množenje skup $P = G \times H$ je grupa.

Dokaz

Asocijativnost je očigledna, slijedi neposredno iz asocijativnosti množenja u G i H. Nadalje, neutralni element je očito $e = (e_G, e_H)$, jer imamo

$$ec = (e_G, e_H)(a, b) = (e_G a, e_H b) = (a, b) = c \, .$$

Konačno, za element $c = (a, b)$ je inverz $c^{-1} = (a^{-1}, b^{-1})$, jer je onda

$$c^{-1}c = (a^{-1}, b^{-1})(a, b) = (a^{-1}a, b^{-1}b) = (e_G, e_H) = e \, .$$

■

Očito je da će grupa P biti komutativna onda i samo onda ako su G i H komutativne grupe.

Grupa $P = G \times H$ naziva se **direktni produkt** grupa G i H.

Na primjer,

$$S^1 \times S^1 = \{(e^{2\pi i s}, e^{2\pi i t}) \mid s, t \in \mathbb{R}\}$$

jest **grupa torusa**,

$$S^1 \times \mathbb{R}$$

jest **grupa cilindra**, itd.

Uz direktni produkt su prirodno vezana neka preslikavanja. Imamo najprije preslikavanja

$$p_1 : G \times H \to G, \quad p_2 : G \times H \to H$$

definirana s

$$p_1(a, b) = a \quad , \quad p_2(a, b) = b \quad ,$$

koja nazivamo **prirodne projekcije** direktnog produkta na faktore.

PROPOZICIJA 2

Prirodne projekcije su epimorfizmi s jezgrama $J(p_1) \cong H$, *odnosno* $J(p_2) \cong G$.

Dokaz

Jasno je da je p_1 surjekcija. Pokažimo da je homomorfizam. Imamo

$$\begin{aligned} p_1(c_1c_2) &= p_1[(a_1,b_1)(a_2,b_2)] = p_1[(a_1a_2, b_1b_2)] = \\ &= a_1a_2 = p_1(a_1,b_1)\,p_1(a_2,b_2) = p_1(c_1)\,p_1(c_2)\,. \end{aligned}$$

Nadalje,

$$J(p_1) = p_1^{-1}(e_G) = \{(e_G, b) \mid b \in H\} = \{e_G\} \times H\,.$$

No, očito je $\{e_G\} \times H \cong H$ preko izomorfizma $(e_G, b) \mapsto b$, pa je zaista $J(p_1) \cong H$. ■

Definirajmo sada preslikavanja

$$j_1 : G \to G \times H, \qquad j_2 : H \to G \times H$$

s

$$j_1(a) = (a, e_H) \quad , \quad j_2(b) = (e_G, b) \quad ,$$

koja nazivamo **prirodne injekcije** faktora u direktni produkt.

PROPOZICIJA 3

Prirodne injekcije su monomorfizmi.

Dokaz

Trivijalan. ■

Prop. 3 dopušta da grupe G i H **identificiramo** s njihovim slikama $j_1(G) = G \times \{e_H\}$ i $j_2(H) = \{e_G\} \times H$ u produktu $G \times H$, tj. da G i H smatramo podgrupama od $G \times H$. Uz taj dogovor vrijedi

TEOREM 4

Neka je $P = G \times H$ *direktni produkt grupa* G *i* H. *Onda*

(1) G *i* H *su normalne podgrupe od* P,

(2) $GH = P$, *i*

(3) $G \cap H = \{e\}$, *gdje je* $e = (e_G, e_H)$ *jedinica u* P.

Dokaz

Tvrdnja (1) slijedi iz Prop. 2, tj. iz činjenice da je npr. G jezgra homomorfizma $p_2 : P \to H$. Tvrdnje (2) i (3) su očigledne. ■

ZADACI

1. Direktni produkt grupa je komutativan i asocijativan do na izomorfizam, tj. vrijedi

$$G \times H \cong H \times G$$

$$(G \times H) \times K \cong G \times (H \times K) .$$

[Uputa: Traženi izomorfizmi su $(a, b) \mapsto (b, a)$, odnosno $((a, b), c) \mapsto (a, (b, c))$.]

2. Neka je X grupa. Preslikavanje

$$h : X \to P = G \times H$$

jest homomorfizam onda i samo onda ako su kompozicije

$$p_1 \circ h : X \to G, \quad \text{i} \quad p_2 \circ h : X \to H$$

homomorfizmi. Dokaži!

3. Neka su $f : X \to G$ i $g : X \to H$ homomorfizmi grupa. Onda je preslikavanje

$$h : X \to G \times H ,$$

definirano s

$$h(x) = (f(x), g(x))$$

također homomorfizam. Kažemo da je h **direktni produkt homomorfizama f i g** i pišemo

$$h = f \times g .$$

4. Dokaži: Centar direktnog produkta grupa jednak je direktnom produktu centara faktora.

5. Dokaži: Komutatorska podgrupa direktnog produkta je direktni produkt komutatorskih podgrupa faktora.

6. Neka su $A, B \lhd G$ normalne podgrupe od G. Kažemo da se G **može dekomponirati u direktni produkt podgrupa** A **i** B, ako je

$$AB = G \quad , \quad A \cap B = \{e\} \quad ,$$

gdje je e jedinica u G. Dokaži: Ako se G može dekomponirati u direktni produkt podgrupa A i B, onda svaki element $x \in G$ ima jedinstveni zapis oblika

$$x = ab \, ,$$

gdje je $a \in A$, $b \in B$.

7. Ako se G može dekomponirati u direktni produkt podgrupa A i B, onda svaki element od A komutira sa svakim elementom od B.

8. Pretpostavimo da se G može dekomponirati u direktni produkt podgrupa A i B. Neka je nadalje $P = A \times B$ direktni produkt grupa A i B. Onda je

$$G \cong P \, .$$

[Uputa: Definiraj $f : G \to P$ sa $f(x) = f(ab) = (a, b)$.]

9. Neka je G ciklička grupa reda 6, a a njezin generator. Onda $x = a^2$ generira podgrupu $A < G$ reda 3, a $y = a^3$ generira podgrupu $B < G$ reda 2. Pokaži da se G može dekomponirati u direktni produkt podgrupa A i B. Pokaži, nadalje, da elementi od G imaju (jedinstvene!) prikaze

$$e \, , \; a = x^2 y \, , \; a^2 = x \, , \; a^3 = y \, , \; a^4 = x^2 \, , \; a^5 = xy \, .$$

10. Dokaži da se Kleinova četvorna grupa V može dekomponirati u direktni produkt svojih podgrupa

$$A = \{a_0, a_1\} \quad \text{i} \quad B = \{a_0, a_2\} \, .$$

11. Generaliziraj direktni produkt na više (konačno mnogo) faktora, pa pokaži da je

$$\mathbb{R}^n = \underbrace{\mathbb{R} \times \cdots \times \mathbb{R}}_{n} \, .$$

Kako bi se direktni produkt generalizirao na beskonačno mnogo faktora?

4

PRSTENOVI I TIJELA

U skupovima brojeva možemo zbrajati i množiti. Slično, i u drugim se skupovima može definirati više binarnih operacija, što nas vodi do struktura bogatijih od grupe. U ovom ćemo poglavlju izučavati strukture s dvije binarne operacije, međusobno usklađene. To su prsten, integralna domena, tijelo i polje.

4.1. Definicija prstena

Uređenu trojku $(P, +, \cdot)$, koja se sastoji iz nepraznog skupa P i dviju binarnih operacija definiranih na tom skupu (prvu od njih standardno označavamo aditivno, a drugu multiplikativno), nazivamo **prsten**, ako su ispunjeni ovi uvjeti:

(1) skup P je u odnosu na zbrajanje komutativna grupa,

(2) skup P je u odnosu na množenje polugrupa, i

(3) dvije su operacije povezane zakonom distribucije, tj. vrijedi

$$\begin{aligned} a(b+c) &= ab+ac\,, \\ (a+b)c &= ac+bc\,, \end{aligned}$$

za svaki izbor $a, b, c \in P$.

Zahtjeve (1)–(3) nazivamo **aksiomi prstena**. Kad god ne bude opasnosti od zabune, umjesto pune oznake $(P, +, \cdot)$ kraće ćemo pisati P i govoriti o prstenu P.

Grupu $(P, +)$ zovemo **aditivna grupa** prstena P, a polugrupu $(P, \cdot)$ **multiplikativna polugrupa** prstena P. Neutralni element aditivne grupe nazivamo **nula prstena** P i označavamo ga standardno s 0.

Uočimo da prsten nije struktura koja je inducirana s dvije neovisne binarne operacije, nego te operacije moraju biti međusobno usklađene, povezane zakonom distribucije.

Primjećujemo, nadalje, da se od jedne binarne operacije, zbrajanja, zahtijeva najviše što se može zahtijevati, tj. da u odnosu na tu operaciju P bude komutativna grupa. U odnosu na množenje zahtjevi su blaži. Postavljajući dodatne zahtjeve na multiplikativnu polugrupu od P, dolazimo do "boljih" struktura.

Ako je npr. množenje u prstenu P komutativno, kažemo da je P **komutativni prsten**. Ako je multiplikativna polugrupa prstena monoid, kažemo da je P **prsten s jedinicom**. Jedinstveni neutralni element tog monoida nazivamo onda **jedinica prstena**, i standardno označavamo s 1.

PRIMJERI

1. Skup $\mathbb{Z}$ je, uz standardno zbrajanje i množenje, komutativni prsten s jedinicom – **prsten cijelih brojeva**. Skupovi $\mathbb{Q}, \mathbb{R}$ i $\mathbb{C}$ su također prstenovi uz standardne operacije.

2. Za svaki $m \in \mathbb{N}$ je skup $\mathbb{Z}_m = \{0, 1, 2, \ldots, m-1\}$ uz zbrajanje i množenje $\bmod m$ komutativni prsten s jedinicom, koji zovemo **prsten cijelih brojeva** $\bmod m$.

3. Neka je $A = (A, +)$ Abelova grupa, a

$$E = \mathrm{Hom}\,(A, A)$$

skup svih endomorfizama grupe A. Za $f, g \in E$ definiramo zbrajanje i množenje s

$$\begin{aligned} (f+g)(a) &= f(a) + g(a)\,, \\ (f \cdot g)(a) &= (f \circ g)(a)\,, \end{aligned}$$

za svaki $a \in A$. Provjeri da je uz tako definirane binarne operacije E prsten s jedinicom, općenito nekomutativan. Nula u tom prstenu je endomorfizam

$$n : A \to A\,, \qquad n(a) = 0\,,$$

za svaki $a \in A$, a jedinica je identiteta

$$e : A \to A\,, \qquad e(a) = a\,,$$

za svaki $a \in A$. Uvjeri se, da je nuždan zahtjev da grupa A bude komutativna. Prsten E nazivamo **prsten endomorfizama grupe** A.

4. Neka je S dani skup, a

$$F = \mathbb{R}^S = \{f \mid f : S \to \mathbb{R}\}$$

skup svih realnih funkcija definiranih na skupu S. Onda je, uz operacije

$$\begin{aligned}(f+g)(x) &= f(x)+g(x)\,,\\ (f\cdot g)(x) &= f(x)\cdot g(x)\,,\end{aligned}$$

za svaki $x \in S$, skup F komutativni prsten s jedinicom, i to je konstantna funkcija $e : S \to \mathbb{R}$, $e(x) = 1$. Prsten F zovemo **prsten realnih funkcija na skupu** S.

5. Neka je P skup svih polinoma u jednoj varijabli t s realnim (kompleksnim) koeficijentima. Onda je P uz standardno zbrajanje i množenje polinoma prsten s jedinicom, tzv. **prsten polinoma**.

Navedimo nekoliko jednostavnih posljedica definicije prstena.

PROPOZICIJA 1

Neka je P bilo koji prsten. Onda je

$$0 \cdot a = 0 = a \cdot 0\,,$$

za svaki $a \in P$.

Dokaz

Kako je 0 neutralni element aditivne grupe, to je $0 + 0 = 0$. Onda zbog distributivnosti vrijedi

$$0 \cdot a = (0+0) \cdot a = 0 \cdot a + 0 \cdot a$$

pa dodavanjem suprotnog elementa $-(0\cdot a)$ na obje strane dobivamo $0 = 0\cdot a$. Analogno se pokazuje da je $a \cdot 0 = 0$. ■

Prsten $P = \{0\}$, koji se sastoji iz jednog jedinog elementa, nazivamo **nulprsten** ili **trivijalni** prsten. Taj element je, dakako, i nula i jedinica za P. Vrijedi, međutim,

KOROLAR 2

Ako je P prsten s jedinicom i ima bar dva elementa (tj. nije nulprsten), onda je $0 \neq 1$.

Dokaz

Iz Prop.1 i svojstva jedinice slijedi da je

$$\begin{aligned} 0 \cdot a &= 0 , \\ 1 \cdot a &= a , \end{aligned}$$

za svaki $a \in P$. Kad bi bilo $0 = 1$, dobili bismo da je $0 = a$ za svaki $a \in P$, protivno pretpostavci da u P postoje bar dva različita elementa. ■

PROPOZICIJA 3

U svakom prstenu P vrijedi

(1) $(-a)b = -(ab) = a(-b)$;

(2) $(-a)(-b) = ab$;

za svaki $a, b \in P$.

Dokaz

Dokažimo npr. (1). Imamo

$$(-a + a)b = 0 \cdot b = 0$$

ili zbog distributivnosti

$$(-a)b + ab = 0 ,$$

što pokazuje da je $(-a)b$ suprotan element od ab, dakle

$$(-a)b = -(ab).$$

■

PROPOZICIJA 4

U prstenu P je također

$$\begin{aligned} (a - b)c &= ac - bc , \\ a(b - c) &= ab - ac , \end{aligned}$$

za svaki izbor $a, b, c \in P$.

Dokaz

Trivijalan. ■

ZADACI

1. Neka je A Abelova grupa. U A definiramo množenje, stavljajući $ab = 0$ za svaki izbor $a, b \in A$. Pokaži da je A uz to množenje prsten. Tako se svaka Abelova grupa može interpretirati kao prsten s trivijalnim množenjem.

2. Na skupu $P = \{0, a, b, c\}$ definirano je zbrajanje i množenje sljedećim tablicama

$+$	0	a	b	c
0	0	a	b	c
a	a	0	c	b
b	b	c	0	a
c	c	b	a	0

$\cdot$	0	a	b	c
0	0	0	0	0
a	0	a	b	c
b	0	0	0	0
c	0	a	b	c

Provjeri da je P prsten, i to nekomutativan i bez jedinice.

3. Neka je $n \in \mathbb{N}$ dani broj. Pokaži da je grupa $n\mathbb{Z}$, uz standardno množenje, komutativni prsten s jedinicom.

4. Pokaži da su sljedeći skupovi brojeva uz standardne operacije prstenovi:

   (a) $A = \left\{ \frac{a}{p^b} \mid p \text{ je dani prim broj}, \ a, b \in \mathbb{Z} \right\}$;

   (b) $B = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}$;

   (c) $C = \{a + b\sqrt[3]{2} + c\sqrt[3]{4} \mid a, b, c \in \mathbb{Z}\}$.

   Naprotiv, skup

   (d) $D = \{a + b\sqrt[3]{2} \mid a, b \in \mathbb{Z}\}$ nije prsten. Zašto?

5. U prstenu je distributivnost postulirana samo za dva pribrojnika. Dokaži da u svakom prstenu vrijedi

$$(a_1 + a_2 + \cdots a_n) \cdot b = a_1 b + a_2 b + \cdots + a_n b$$

   za svaki izbor $a_i, b \in P$, i svaki n.

6. Ako u aksiomima prstena zahtjev (2) zamijenimo slabijim zahtjevom

   (2') Skup P je u odnosu na množenje grupoid,

tj. ako ne zahtijevamo da množenje u P bude asocijativno, dolazimo do strukture koja se zove **neasocijativni prsten**. Ako su u neasocijativnom prstenu P zadovoljeni još ovi uvjeti:

(4) $a \cdot a = 0$, za svaki a, i

(5) Jacobijev identitet, tj.

$$(ab)c + (bc)a + (ca)b = 0 ,$$

za svaki $a, b, c \in P$, onda P nazivamo **Liejev prsten** (prema norveškom matematičaru Sophusu Lieju). Pokaži da je u Liejevu prstenu množenje **antikomutativno**, tj. da vrijedi

$$a \cdot b = -(b \cdot a) .$$

Nadalje, to množenje je asocijativno onda i samo onda, ako je trivijalno. Konačno, to množenje ne dopušta jedinicu, osim kad je P nulprsten.

7. Neka je $P = (P, +, \cdot)$ bilo koji prsten. U P definiramo novu operaciju množenja s

$$a \circ b = ab - ba ,$$

koja se zove **komutatorsko** ili **Liejevo množenje**. Pokaži da je struktura $P^- = (P, +, \circ)$ Liejev prsten. Na taj se način svakom prstenu P može prirodno pridružiti jedinstveni Liejev prsten. Primijetimo da je množenje u P^- trivijalno onda i samo onda, ako je polazni prsten bio komutativan.

8. Neasocijativni prsten P, u kojem su ispunjeni još i ovi uvjeti:

(4) množenje je komutativno i

(5) vrijedi $[(aa)b]a = (aa)(ba)$,

za svaki $a, b \in P$, naziva se **Jordanov prsten**. Neka je $P = (P, +, \cdot)$ bilo koji prsten. U P definiramo novo množenje s

$$a * b = ab + ba ,$$

koje nazivamo **simetrizirano množenje**. Pokaži da je struktura $P^+ = (P, +, *)$ Jordanov prsten.

4.2. Djelitelji nule. Integralna domena

Kod brojeva, $ab = 0$ uvijek ima za posljedicu, da je bar jedan od faktora jednak nuli. U općim prstenovima to ne mora biti istina.

Neka je P prsten, a $a, b \in P$ njegovi elementi sa svojstvom da je $a \neq 0$ i $b \neq 0$ a vrijedi

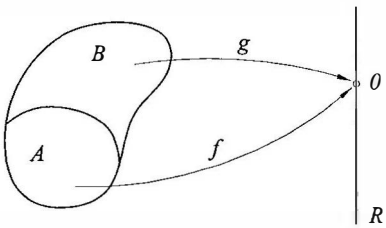
$$ab = 0 .$$

Onda kažemo da su elementi a i b **djelitelji nule** u prstenu P.

Neka je npr. $F = \mathbb{R}^S$ prsten realnih funkcija na skupu S (vidi Prim. 4. u 4.1.). Nula u tom prstenu je funkcija $n : S \to \mathbb{R}$ definirana s

$$n(x) = 0, \qquad \forall x \in S.$$

Neka je $A \subset S$ neprazni podskup od S, a $B = S - A$ njegov komplement.



Neka su $f, g \in \mathbb{R}^S$ funkcije definirane s

$$f(x) = \begin{cases} 0, & x \in A \\ 1, & x \in B \end{cases} \quad , \qquad g(x) = \begin{cases} 1, & x \in A \\ 0, & x \in B \end{cases} \quad .$$

Onda je $f \neq n$ i $g \neq n$, ali vrijedi

$$(f \cdot g)(x) = f(x) \cdot g(x) = 0 = n(x)$$

za svaki $x \in S$, pa je $fg = n$, tj. f i g su djelitelji nule u $\mathbb{R}^S$. Očito je da u $\mathbb{R}^S$ ima mnogo raznih djelitelja nule.

Drugi je primjer prsten $\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$ i njegovi elementi 2 i 3, jer je $2 \dot{}_6 3 = 0$.

Sličan se fenomen pojavljuje u svakom prstenu $\mathbb{Z}_m$, gdje je m složen broj.

Jasno je da prsten P neće imati djelitelja nule onda i samo onda ako je $P - \{0\}$ zatvoren u odnosu na množenje (tj. potpolugrupa multiplikativne polugrupe prstena P). Imamo međutim ovu karakterizaciju:

TEOREM 1

Prsten P nema djelitelja nule ako i samo ako se u njemu može skraćivati sa svakim elementom $x \neq 0$, tj. ako su za bilo koje elemente $a, b \in P$ sljedeće tvrdnje ekvivalentne:

$$(1) \quad a = b \qquad (2) \quad ax = bx \qquad (3) \quad xa = xb .$$

Dokaz

Nužnost: (1) $\Rightarrow$ (2) i (1) $\Rightarrow$ (3) vrijedi u svakom prstenu. Pretpostavimo da u P nema djelitelja nule pa pokažimo da (2) $\Rightarrow$ (1). No, iz $ax = bx$, zbog distributivnosti (vidi Prop. 4 u 4.1.), imamo

$$(a - b)x = ax - bx = 0 .$$

Kako je $x \neq 0$, a u P nema djelitelja nule, mora biti $a - b = 0$, tj. $a = b$, dakle, vrijedi (1). Slično se vidi da (3) $\Rightarrow$ (1). Prema tome, uvjeti (1)–(3) su ekvivalentni.

Dovoljnost: Pretpostavimo da se u P može kratiti sa svakim $x \neq 0$. Tvrdimo da u P nema djelitelja nule. Uzmimo suprotno, da su $a, b \in P$ djelitelji nule, tj. da vrijedi $a \neq 0$, $b \neq 0$ i $ab = 0$. No, uvijek je $a \cdot 0 = 0$, pa imamo $ab = a \cdot 0$. Kako je $a \neq 0$, možemo s a skratiti (implikacija (2) $\Rightarrow$ (1)), pa ostaje $b = 0$, što je u kontradikciji s pretpostavkom $b \neq 0$. Time je tvrdnja dokazana. ■

Prsten s jedinicom, u kojem nema djelitelja nule nazivamo **integralna domena**. Prema tome, prsten P s jedinicom koji nije nulprsten (ima bar dva elementa), bit će integralna domena onda i samo onda, ako je $P - \{0\}$ podmonoid multiplikativnog monoida od P.

Ako je množenje i komutativno, govorimo o **komutativnoj integralnoj domeni**.

Na primjer, prstenovi $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$, i $\mathbb{C}$ su komutativne integralne domene. Prsten $\mathbb{Z}_m$ bit će integralna domena onda i samo onda, ako je m prim broj. Prstenovi $E = \mathrm{Hom}\,(A, A)$ endomorfizama grupe A i $F = \mathbb{R}^S$ realnih funkcija na skupu S nisu općenito integralne domene.

ZADACI

1. Uvjeri se da prsten $E = \mathrm{Hom}\,(A, A)$ ima djelitelje nule i, prema tome, nije integralna domena.

2. Za element $a \in P$ prstena P kažemo da je **nilpotentan** ako postoji $n \in \mathbb{N}$ sa svojstvom da je $a^n = 0$. Pokaži da je jedini nilpotentni element u integralnoj domeni njezina nula.

4.3. Potprstenovi i ideali

Neka je P prsten, a $A \subset P$ njegov neprazni podskup. Kažemo da je A **potprsten** od P, ako je A i sam prsten u odnosu na binarne operacije definirane na P. Pišemo i ovdje $A < P$.

Drugim riječima, $A \subset P$ je potprsten od P, ako je A podgrupa aditivne grupe od P i ako je A zatvoren u odnosu na množenje (tj. potpolugrupa

multiplikativne polugrupe od P). Dakako, zakon distribucije je ispunjen u P, pa onda i u A. Očito vrijedi

PROPOZICIJA 1

Neprazan podskup $A \subset P$ prstena P je potprsten od P onda i samo onda, ako za bilo koje elemente $a, b \in A$ vrijedi $a - b \in A$ i $ab \in A$.

Dokaz

Trivijalan (vidi Tm. 3. u 2.7.). ■

Na primjer, $\mathbb{Z}$ je potprsten od $\mathbb{Q}$, $\mathbb{Q}$ je potprsten od $\mathbb{R}$, a ovaj je potprsten od $\mathbb{C}$. Nadalje, $m\mathbb{Z} \subset \mathbb{Z}$ je potprsten od $\mathbb{Z}$.

Ako je potprsten $A < P$ integralna domena, kažemo da je A **poddomena** prstena P. Tako su $\mathbb{Z} < \mathbb{Q} < \mathbb{R} < \mathbb{C}$ poddomene, dok $m\mathbb{Z} < \mathbb{Z}$, uz $m \neq 1, -1$, nije poddomena, jer ne sadrži jedinicu.

Sljedeća propozicija je očigledna.

PROPOZICIJA 2

Presjek bilo koje familije potprstenova od P je opet potprsten od P. ■

Slično vrijedi i za poddomene. Neka je $S \subset P$ podskup prstena P, a $A(S)$ najmanji potprsten od P koji sadrži S, tj. presjek svih potprstenova od P, koji sadrže S. Onda kažemo da je $A(S)$ **potprsten od P generiran sa S.**

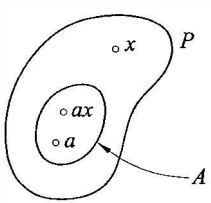
Neka je $A < P$ potprsten od P. Kažemo da je A **lijevi ideal** od P, ako je ispunjeno

$$AP \subset A\,,$$

tj. ako vrijedi $ax \in A$ za svaki $a \in A$ i svaki $x \in P$. Analogno, potprsten $A < P$ je **desni ideal** od P ako je ispunjeno

$$PA \subset A\,.$$

Konačno, potprsten $A \subset P$ je **obostrani ideal** ili jednostavno **ideal** od P,



ako je A istodobno lijevi i desni ideal od P.

Svaki prsten P (kao, uostalom, i svaki čovjek!) ima svoje ideale. Trivijalni su cijeli P i $\{0\}$. Ostale ideale zovemo **pravi** ideali. Na primjer, potprsten $m\mathbb{Z} < \mathbb{Z}$ je ideal od $\mathbb{Z}$, dok $\mathbb{Z} < \mathbb{Q}$ nije ideal od $\mathbb{Q}$.

Neka je $A < P$ potprsten od P. Onda je A podgrupa aditivne grupe od P, koja je komutativna, pa je

$$Q = P/A = \{x + A \mid x \in P\}$$

dobro definirana kvocijentna grupa, i to komutativna. Željeli bismo Q organizirati u prsten.

PROPOZICIJA 3

Neka je $A < P$ ideal od P. Onda je za svaki $x, y \in P$

$$(x + A)(y + A) \subset xy + A\,.$$

Dokaz

Neka su $u \in A$ i $v \in A$. Onda zbog distribucije i činjenice da je A ideal imamo redom

$$\begin{aligned}(x+u)(y+v) &= xy + \underbrace{xv}_{\in A} + \underbrace{uy}_{\in A} + \underbrace{uv}_{\in A} = \\ &= xy + a \in xy + A\,,\end{aligned}$$

pa je tvrdnja dokazana. ■

Sada definiramo množenje klasa s

$$(x + A) * (y + A) = xy + A$$

pa imamo

TEOREM 4

Neka je $A < P$ ideal od P. Onda je, uz upravo definirano množenje,

$$Q = P/A$$

prsten.

Dokaz

Provjerimo, npr. distributivnost. Imamo

$$\begin{aligned}[(x+A) &+ (y+A)] * (z+A) = \\ &= ((x+y)+A) * (z+A) = \\ &= (x+y)z + A = (xz+yz) + A = \\ &= (xz+A) + (yz+A) = \\ &= (x+A) * (z+A) + (y+A) * (z+A).\end{aligned}$$

■

Prsten $Q = P/A$ zove se **kvocijentni prsten** prstena P po idealu A. Ako je P bio prsten s jedinicom, i P/A je prsten s jedinicom, i to je klasa $1+A$. Nadalje, ako je P bio komutativan i P/A je očito komutativni prsten.

ZADACI

1. Dokaži: Presjek bilo koje familije poddomena integralne domene je opet poddomena.

2. Potprsten $A < P$ integralne domene P je poddomena ako i samo ako sadrži jedinicu od P.

3. Neka je P prsten s jedinicom, a $A < P$ ideal koji sadrži tu jedinicu. Onda je $A = P$.

4. Pokaži da je množenje klasa dobro definirano, tj. da ne ovisi o izboru predstavnika klasa. Drugim riječima, pokaži da iz $x' \in x+A$ i $y' \in y+A$ slijedi $x'y' + A = xy + A$.

5. Neka je $F = \mathbb{R}^S$ prsten realnih funkcija na S, i $T \subset S$. Neka je

$$F_T = \{f \in F \mid f(T) = \{0\}\} \subset F\ .$$

   Pokaži da je F_T ideal od F.

6. Neka je P prsten i $n \in \mathbb{N}$ dani prirodni broj. Neka je

$$nP = \{nx \mid x \in P\}\ ,$$

   gdje je $nx = \underbrace{x + x + \cdots + x}_{n}$. Pokaži da je nP ideal od P. Kvocijentni prsten

$$P_n = P/nP$$

   naziva se **reducirani prsten** od P mod n.

7. Neka je P prsten i $n \in \mathbb{N}$ dani prirodni broj. Onda je

$$A = \{x \in P \mid nx = 0\}$$

ideal od P. Dokaži!

8. Presjek bilo koje familije ideala prstena P je ideal od P.

9. Ako je $S \subset P$ podskup od P, najmanji ideal $J(S)$ koji sadrži S nazivamo **ideal od P generiran sa S**. Neka je $a \in P$, a $J(a)$ ideal generiran elementom a. Onda $J(a)$ nazivamo **glavni ideal** od P. Provjeri da je $J(0) = \{0\}$, a $J(1) = P$.

10. Ako je svaki ideal od P glavni, kažemo da je P **prsten glavnih ideala**. Pokaži da je $\mathbb{Z}$ prsten glavnih ideala.

11. Neka je $S \subset P$ podskup od P. Pokaži da je

$$C(S) = \{c \in P \mid cs = sc, \quad \text{za svaki } s \in S\}$$

potprsten od P. Specijalno, $C(P)$ se naziva **centar** od P.

12. Ako je P generiran sa S, onda je $C(S) = S(P)$. Dokaži!

13. Za ideal $A < P$ kažemo da je **primideal** od P, ako iz $x, y \in P$ i $xy \in A$ slijedi da je $x \in A$ ili $y \in A$. Dokaži: Kvocijentni prsten P/A komutativnog prstena P s jedinicom po idealu A, integralna je domena ako i samo ako je A primideal od P.

4.4. Homomorfizam prstenova

Kod prstenova će nas također zanimati samo ona preslikavanja koja poštuju danu strukturu, strukturu prstena.

Neka su P i Q prstenovi, a

$$f : P \to Q$$

preslikavanje. Kažemo da je f **homomorfizam** prstena P u prsten Q ako je za svaki izbor $a, b \in P$ ispunjeno

(1) $f(a+b) = f(a) + f(b)$ i

(2) $f(ab) = f(a) \cdot f(b)$,

tj. ako f komutira s obje binarne operacije.

Drugim riječima, f je homomorfizam prstenova ako je to homomorfizam aditivnih grupa prstenova i, istodobno, homomorfizam multiplikativnih polugrupa prstenova.

Na očigledan način definiraju se onda specijalni homomorfizmi prstenova, kao što su monomorfizam, epimorfizam, izomorfizam prstenova, zatim endomorfizam i automorfizam. Nadalje, preko izomorfizma dolazimo do relacije $\cong$, tj. relacije "**biti izomorfan**" za prstenove, i onda do klasifikacije prstenova na disjunktne klase međusobno izomorfnih prstenova, koje smatramo jednakima s apstraktnog stajališta.

Na primjer, ako je $A < P$ potprsten od P, inkluzija $i : A \to P$ je monomorfizam prstenova. Preslikavanje

$$f : \mathbb{Z} \to \mathbb{Z}_m ,$$

definirano zahtjevom da je $f(x)$ jedinstveni broj iz $\mathbb{Z}_m$ sa svojstvom da je $x - f(x)$ djeljivo s m, jest epimorfizam prstenova.

Za homomorfizam prstenova $f : P \to Q$ definiramo **sliku** $S(f)$ i **jezgru** $J(f)$ posve analogno kao u slučaju homomorfizama grupa, tj. sa $S(f) = f(P)$, odnosno $J(f) = f^{-1}(0_Q)$. Onda imamo

TEOREM 1

Neka je $f : P \to Q$ homomorfizam prstenova. Onda je

(1) $S(f) \subset Q$ *potprsten od* Q,

(2) $J(f) \subset P$ *ideal od* P.

Dokaz

Lako se provjeri da su slika i jezgra potprstenovi od Q odnosno P. Pokažimo da je jezgra ideal. Neka su $a \in J(f)$ i $x \in P$ bilo koji elementi. Onda je

$$f(ax) = f(a) \cdot f(x) = 0 \cdot f(x) = 0 ,$$

što pokazuje da je $ax \in J(f)$. Slično se vidi da je $xa \in J(f)$, pa zaključujemo da je $J(f)$ zaista ideal. ■

Neka je $A < P$ ideal od P, P/A pripadni kvocijentni prsten, a

$$p : P \to P/A$$

prirodna projekcija, tj. preslikavanje definirano s

$$p(x) = x + A ,$$

za svaki $x \in P$.

PROPOZICIJA 2

Prirodna projekcija $p : P \to P/A$ je epimorfizam s jezgrom $J(p) = A$.

Dokaz

Već smo vidjeli da je p epimorfizam na razini aditivnih grupa prstenova. Imamo, nadalje, za $x, y \in P$

$$p(xy) = xy + A = (x + A) * (y + A) = p(x) * p(y) ,$$

pa je p zaista epimorfizam prstenova. ■

Neka su sada $A < P$ i $B < Q$ ideali prstena P, odnosno Q, a

$$h : (P, A) \to (Q, B)$$

homomorfizam parova. Analogno onom kod grupa (vidi točku 3.8.), taj homomorfizam inducira preslikavanje

$$h^* : P/A \to Q/B$$

na razini kvocijentnih prstenova, dano s

$$h^*(x + A) = h(x) + B .$$

PROPOZICIJA 3

Preslikavanje h^* je homomorfizam kvocijentnih prstenova.

Dokaz

Već smo vidjeli da je h^* homomorfizam na razini aditivnih grupa prstenova. Kako je, nadalje,

$$\begin{aligned} &h^*[(x + A) * (y + A)] = \\ &= h^*[(xy + A)] = h(xy) + B = \\ &= h(x)h(y) + B = (h(x) + B) * (h(y) + B) = \\ &= h^*(x + A) * h^*(y + A) , \end{aligned}$$

to je h^* zaista homomorfizam prstenova. ■

Homomorfizam prstenova h^* nazivamo **inducirani homomorfizam** od h. Na osnovi Prop. 2, kao i Tm. 3 iz 3.8. zaključujemo, da je dijagram

$$\begin{array}{ccc} P & \xrightarrow{h} & Q \\ {\scriptstyle p}\downarrow & & \downarrow{\scriptstyle q} \\ P/A & \xrightarrow{h^*} & Q/B \end{array}$$

komutativan, tj. za homomorfizme prstenova vrijedi

$$h^* \circ p = q \circ h$$

gdje su p i q prirodne projekcije.

Kao specijalni slučaj onda dobivamo

TEOREM 4 (Teorem o izomorfizmu prstenova)

Neka je $h : P \to Q$ epimorfizam prstenova, a $J = J(h)$ njegova ***jezgra.*** *Onda je kvocijentni prsten P/J izomorfan s prstenom Q. I više,* ***postoji*** *izomorfizam $h^* : P/J \to Q$ sa svojstvom da dijagram*

$$\begin{array}{ccc} P & \xrightarrow{h} & Q \\ & {\scriptstyle p}\searrow \quad \nearrow{\scriptstyle h^*} & \\ & P/J & \end{array}$$

komutira, tj. vrijedi $h^* \circ p = h$.

Dokaz

Kao dokaz Tm. 5 u 3.8. ■

ZADACI

1. Neka su P i Q prstenovi s jedinicom, a $h : P \to Q$ homomorfizam prstenova. Je li nužno $h(1) = 1^*$, gdje je 1^* jedinica u Q?

2. Dokaži ovu karakterizaciju ideala: Potprsten $A < P$ je ideal onda i samo onda, ako postoji homomorfizam $h : P \to Q$ u neki prsten Q, koji ima svojstvo da je $J(h) = A$. [Uputa: Koristi Tm. 1 i Prop. 2.]

3. Dokaži da su sljedeća svojstva prstenova **invarijantna** u odnosu na izomorfizam:

   (a) biti komutativan;

   (b) imati jedinicu;

   (c) biti integralna domena.

   Drugim riječima, ako je $h : P \to Q$ izomorfizam prstenova, a P ima neko od svojstava (a)–(c), onda to isto svojstvo ima prsten Q.

4. Pokaži da su jedini endomorfizmi prstena $\mathbb{Z}$ cijelih brojeva nulhomomorfizam i identiteta. Isto vrijedi za prsten racionalnih brojeva.

5. Neka je $h : P \to P$ endomorfizam prstena P, a

$$A = \{a \in P \mid h(a) = a\}$$

skup svih fiksnih elemenata od h. Pokaži da je $A \subset P$ potprsten od P.

6. Pokaži da je za svaki $m \in \mathbb{N}$, $\mathbb{Z}/m\mathbb{Z} \cong \mathbb{Z}_m$ na razini prstenova.

7. Neka je P prsten, a $E = \mathrm{Hom}\,(P, P)$ prsten svih endomorfizama **aditivne grupe** od P. Neka je $a \in P$ bilo koji element, a

$$h_a : P \to P$$

preslikavanje, dano s

$$h_a(x) = ax\ ,$$

koje nazivamo **lijevo množenje s** a. Pokaži da je $h_a \in E$.

8. Neka je $h : P \to E$ preslikavanje definirano s $h(a) = h_a$. Pokaži da je h homomorfizam prstenova. Pokaži, nadalje, da je jezgra tog homomorfizma

$$J(h) = \{a \in P \mid ax = 0,\ \ \forall x \in P\}\ .$$

Taj se ideal $J(h)$ zove **lijevi anihilator** od P.

9. Ako je P prsten s jedinicom, onda je lijevi anihilator $J(h) = \{0\}$, pa je $h : P \to E$ monomorfizam. Dokaži! Prema tome je prsten s jedinicom uvijek izomorfan **nekom** prstenu endomorfizama (tog prstena).

10. Neka je P bilo koji prsten, a

$$Q = P \times \mathbb{Z}$$

direktni produkt aditivnih grupa od P i $\mathbb{Z}$. U Q definiramo množenje s

$$(a, m) \cdot (b, n) = (ab + na + mb, mn)$$

za $a, b \in P$, $m, n \in \mathbb{Z}$. Pokaži da je uz to množenje Q prsten s jedinicom $(0, 1)$. Pokaži, nadalje, da je preslikavanje $j : P \to Q$ definirano sa $j(x) = (x, 0)$ monomorfizam prstenova. Tako se P može identificirati s potprstenom $j(P) < Q$ (koji je prsten s jedinicom).

4.5. Karakteristika

Prisjetimo se pojma reda nekog elementa u danoj grupi. Neka je A aditivna grupa i $a \in A$. Kažemo da je a reda m, ako je m najmanji prirodni broj za koji vrijedi (aditivno pisano)

$$ma = \underbrace{a + a + \cdots + a}_{m} = 0 .$$

Ako takav broj ne postoji, kažemo da je a beskonačnog reda. Kako je svaki prsten i aditivna grupa, ima smisla govoriti i o redu elementa u prstenu.

Neka je P prsten. Kažemo da je P

(1) **karakteristike** m, ako je m najmanji prirodni broj sa svojstvom da je $ma = 0$, za **svaki** $a \in P$;

(2) **karakteristike** 0, ako takav broj ne postoji.

Za karakteristiku prstena obično pišemo $k(P)$. Drugim riječima, P je karakteristike 0, ako je $m = 0$ jedini cijeli broj sa svojstvom da je $ma = 0$ za sve $a \in P$. U tom slučaju za svaki prirodni broj k postoji element u P čiji je red veći od k. U slučaju pak, kad je P karakteristike $m \neq 0$, svaki je element od P konačnog reda, i taj je red divizor (mjera) od m. Na primjer, $\mathbb{Z}$ je karakteristike 0. U $\mathbb{Z}_4$ je $4 \cdot 1 = 0$, $2 \cdot 2 = 0$, $4 \cdot 3 = 0$ pa je karakteristike 4. Općenito, karakteristika od $\mathbb{Z}_m$ je m. Karakteristika prstena u Zad. 2. u 4.1. je dva (jer je Abelova grupa tog prstena Kleinova četvorna grupa).

PROPOZICIJA 1

Neka je P prsten s jedinicom. Onda se karakteristika od P podudara s redom te jedinice, tj.

$$k(P) = \begin{cases} 0, & \textit{ako je 1 beskonačnog reda} \\ m, & \textit{ako je 1 reda } m \end{cases} .$$

Dokaz

Očito je da je karakteristika 0, ako je 1 beskonačnog reda. Pretpostavimo zato da je 1 konačnog reda, i to m. Neka je $a \in P$ bilo koji element. Onda je

$$\begin{aligned} ma &= \underbrace{a + \cdots + a}_{m} = a \cdot 1 + \cdots + a \cdot 1 = a(\underbrace{1 + \cdots + 1}_{m}) = \\ &= a(m \cdot 1) = a \cdot 0 = 0 , \end{aligned}$$

što pokazuje da je P zaista karakteristike m. ■

PROPOZICIJA 2

Ako je P prsten u kojem nema djelitelja nule, red svih njegovih elemenata različitih od nule je isti.

Dokaz

Neka su $a \neq 0 \neq b$ bilo koja dva elementa od P. Ako su oba beskonačnog reda, tvrdnja je dokazana. Pretpostavimo zato da je a konačnog reda, kažimo m. Pokažimo da je $mb = 0$. Imamo

$$\begin{aligned} a(mb) &= a(\underbrace{b + \cdots + b}_{m}) = \underbrace{ab + \cdots + ab}_{m} = (\underbrace{a + \cdots + a}_{m})b \\ &= (ma)b = 0 \cdot b = 0 \,. \end{aligned}$$

Kako u P nema djelitelja nule i $a \neq 0$, mora biti $mb = 0$. Time smo pokazali da red od b nije veći od reda od a. Posve analogno bismo vidjeli da red od a ne može biti veći od reda elementa b, pa zaključujemo da elementi a i b imaju isti red. ■

KOROLAR 3

Neka je P integralna domena čija je karakteristika različita od nule. Onda se ta karakteristika podudara s redom bilo kojeg elementa od P, različitog od nule, npr.

$$k(P) = \textit{red od } 1 \,.$$ ■

Ta se formula često uzima i kao definicija karakteristike. Razabiremo da je u dobrim strukturama, kao što je integralna domena, karakteristika zajedničko svojstvo svih elemenata različitih od nule. Zato se i zove karakteristika te strukture.

PROPOZICIJA 4

Neka je P netrivijalan prsten u kojem nema djelitelja nule. Ako karakteristika od P nije 0, onda je prim broj.

Dokaz

Neka je $m \neq 0$ karakteristika od P. Kako je P netrivijalan, postoji $a \in P$ sa svojstvom $a \neq 0$. Prema Prop. 2, a je reda m, tj. $ma = 0$. Pretpostavimo da se m može prikazati kao $m = pq$, gdje su p i q prirodni brojevi. Onda imamo

$$\begin{aligned} (pa)(qa) &= (\underbrace{a + \cdots + a}_{p})(\underbrace{a + \cdots + a}_{q}) = \\ &= \underbrace{a^2 + \cdots + a^2}_{pq} = a(\underbrace{a + \cdots + a}_{pq}) = \\ &= a[(pq)a] = a(ma) = a \cdot 0 = 0 \,. \end{aligned}$$

Kako u P po pretpostavci nema djelitelja nule, ili je $pa = 0$ ili je $qa = 0$. Kako je a reda m i $p, q \leq m$ to jedan od brojeva p i q mora biti jednak m, a onda je drugi 1, što pokazuje da je m zaista prim broj. ■

ZADACI

1. Neka je P integralna domena karakteristike 0. Onda je aditivna podgrupa od P generirana jedinicom, poddomena od P, izomorfna sa $\mathbb{Z}$. [Uputa: Definiraj $f : \mathbb{Z} \to P$ sa $f(k) = k \cdot 1$.]

2. Neka je P integralna domena karakteristike $m \geq 2$. Onda je aditivna podgrupa od P generirana jedinicom poddomena od P, izomorfna sa $\mathbb{Z}_m$.

3. Neka je P komutativni prsten karakteristike p, gdje je p prim broj. Onda je

   (a) $(a + b)^p = a^p + b^p$;
   (b) $(a - b)^p = a^p - b^p$.

4. Neka je P komutativna integralna domena karakteristike $m \geq 2$. Neka je $f : P \to P$ preslikavanje, definirano s $f(a) = a^m$. Pokaži da je f monomorfizam i $S(f) \subset P$ poddomena.

5. Neka je $P = (\mathbb{Q}, +, *)$ skup racionalnih brojeva sa standardnim zbrajanjem i trivijalnim množenjem. Onda je P komutativni prsten. Pokaži da je svaki različiti od nule element od P beskonačnog reda, pa je karakteristika od P jednaka 0.

4.6. Tijelo i polje

Kako smo vidjeli, u definiciji prstena su na jednu od binarnih operacija, zbrajanje, postavljeni maksimalni zahtjevi (komutativna grupa), dok se od druge binarne operacije, množenja, zahtijevala samo asocijativnost. Postuliranjem daljnjih svojstava za množenje dolazimo do novih, boljih struktura. Tako nas je zahtjev da množenje ima jedinicu i nema djelitelja nule doveo do integralne domene. Daljnji zahtjev, koji bismo mogli postaviti, jest da svaki element prstena ima multiplikativni inverz. No, za nulu $0 \in P$ bi to značilo postojanje takvog elementa $a \in P$, da bude ispunjeno

$$0 \cdot a = a \cdot 0 = 1 .$$

Međutim, u prstenu je uvijek

$$0 \cdot a = a \cdot 0 = 0,$$

što pokazuje da u netrivijalnom prstenu ($0 \neq 1$) nula ne može imati inverz. Prema tome je maksimalni zahtjev koji možemo postaviti, da svaki element različit od nule ima multiplikativni inverz.

To nas vodi ovoj definiciji: Integralna domena u kojoj svaki element različit od nule ima multiplikativni inverz naziva se **tijelo**. Tijelo u kojem je množenje i komutativno, naziva se **polje**.

Međutim, zahtjev da polazimo od integralne domene može se ublažiti. Vrijedi naime

PROPOZICIJA 1

Netrivijalni prsten P je tijelo onda i samo onda ako je $P - \{0\}$ grupa u odnosu na množenje, tj. podgrupa multiplikativne polugrupe od P.

Dokaz

Nužnost je očigledna. Pokažimo dovoljnost. Neka je dakle $P - \{0\}$ multiplikativna grupa, a 1 njezina jedinica. Onda je $a \cdot 1 = 1 \cdot a = a$ za svaki $a \in P - \{0\}$ i također $0 \cdot 1 = 1 \cdot 0 = 0$ po općem svojstvu, pa je 1 i jedinica prstena. Nadalje, kad bi postojali djelitelji nule u P, tj. $a \neq 0$ i $b \neq 0$ takvi da je $a \cdot b = 0$, to bi bilo u kontradikciji s činjenicom da je $P - \{0\}$ kao grupa zatvorena u odnosu na množenje. Prema tome je P integralna domena, a jer je svaki element iz $P - \{0\}$ i invertibilan, P je tijelo po definiciji. ■

Možemo, dakle, **alternativno definirati tijelo** kao prsten P u kojem je $P - \{0\}$ multiplikativna grupa. Uočimo da je po toj definiciji tijelo uvijek netrivijalno, tj. ima bar dva elementa, i vrijedi $1 \neq 0$.

U tijelu je, dakle, $P - \{0\}$ podgrupa multiplikativnog monoida od P, i zove se **multiplikativna grupa** tijela P.

PRIMJERI

1. Skupovi $\mathbb{Q}, \mathbb{R}$ i $\mathbb{C}$ su, uz standardne operacije, polja. To su temeljni, klasični primjeri polja.

2. Skup $\mathbb{Z}$ nije polje, jer elementi različiti od ± 1 nemaju multiplikativni inverz.

3. Prsten $\mathbb{Z}_m$ cijelih brojeva mod m je polje onda i samo onda ako je m prim broj.

4. Neka je
$$\mathbb{H} = \mathbb{R} \times \mathbb{R} \times \mathbb{R} \times \mathbb{R}$$
direktni produkt aditivnih grupa realnih brojeva, dakle Abelova grupa u odnosu na standardno (koordinatno) zbrajanje. U $\mathbb{H}$ definiramo

množenje stavljajući za $a, b \in \mathbb{H}$

$$\begin{aligned} a \cdot b &= (a_1, a_2, a_3, a_4) \cdot (b_1, b_2, b_3, b_4) = \\ &= (c_1, c_2, c_3, c_4) = c \in \mathbb{H} , \end{aligned}$$

gdje je

$$\begin{aligned} c_1 &= a_1 b_1 - a_2 b_2 - a_3 b_3 - a_4 b_4 \\ c_2 &= a_1 b_2 + a_2 b_1 + a_3 b_4 - a_4 b_3 \\ c_3 &= a_1 b_3 + a_3 b_1 + a_4 b_2 - a_2 b_4 \\ c_4 &= a_1 b_4 + a_4 b_1 + a_2 b_3 - a_3 b_2 . \end{aligned}$$

Skup $\mathbb{H}$ je uz tako definirane binarne operacije tijelo, s $(1, 0, 0, 0)$ kao jedinicom, koje nazivamo **tijelo kvaterniona**. Uvjeri se da $\mathbb{H}$ nije komutativno, i prema tome nije polje.

Uvodeći oznake

$$\begin{aligned} 1 &= (1,0,0,0), \quad i = (0,1,0,0), \\ j &= (0,0,1,0), \quad k = (0,0,0,1), \end{aligned}$$

svaki element $q = (a_1, a_2, a_3, a_4) \in \mathbb{H}$, **kvaternion**, možemo jednoznačno zapisati u obliku

$$q = a_1 \cdot 1 + a_2 \cdot i + a_3 \cdot j + a_4 \cdot k .$$

Provjeri da za "jedinice" vrijedi ova tablica množenja

	1	i	j	k
1	1	i	j	k
i	i	-1	k	$-j$
j	j	$-k$	-1	i
k	k	j	$-i$	-1

,

odakle se odmah razabire da je množenje antikomutativno.

Navest ćemo sada neka osnovna svojstva tijela, odnosno polja.

TEOREM 2

Svaka konačna integralna domena je tijelo.

Dokaz

Neka je

$$P = \{0, a_1, a_2, \ldots, a_n\}$$

konačna integralna domena. Treba pokazati da je $P - \{0\}$ grupa u odnosu na množenje. Neka je $a \in P - \{0\}$ bilo koji element. Promatrajmo n produkata

$$a \cdot a_1,\ a \cdot a_2,\ \ldots,\ a \cdot a_n\ .$$

Oni su svi različiti, jer bi

$$a \cdot a_i = a \cdot a_k$$

za $i \neq k$ povlačilo

$$a(a_i - a_k) = 0$$

uz $a \neq 0$ i $a_i - a_k \neq 0$, dakle egzistenciju djelitelja nule, protivno pretpostavci da je P integralna domena. Prema tome, za svaki $b \in P - \{0\}$ jednadžba $ax = b$ ima rješenje u $P - \{0\}$. Slično se vidi da je rješiva i jednadžba $ya = b$ u $P - \{0\}$, pa je $P - \{0\}$ grupa prema Tm. 3 iz 2.6. ■

Iz teorema se npr. može neposredno zaključiti da je $\mathbb{Z}_m$ polje onda i samo onda ako je m prim broj.

Na očigledan način, posve analogno kao pojam potprstena, definiramo pojam **podtijela** odnosno **potpolja**. Na primjer, $\mathbb{Q} < \mathbb{R} < \mathbb{C}$ su u odnosu potpolje – polje, a $\mathbb{Z} < \mathbb{Q}$ je potprsten, poddomena polja $\mathbb{Q}$, ali nije potpolje. Očito vrijedi

PROPOZICIJA 3

Potprsten $A < P$ tijela P je podtijelo od P onda i samo onda ako za svaki $a \in A$ i $a \neq 0$ vrijedi $a^{-1} \in A$. ■

Naravno, presjek bilo koje familije podtijela (potpolja) je opet podtijelo (potpolje) polaznog tijela. Također se govori o podtijelu generiranom danim skupom u polaznom tijelu.

Kod prstenova smo uveli i pojam ideala. Interesantan je

TEOREM 4

U tijelu nema pravih ideala.

Dokaz

Neka je P tijelo. Kako smo rekli, trivijalni su ideali $\{0\}$ i čitav P; ostale smo nazvali pravim idealima od P. Neka je $I \neq \{0\}$ bilo koji ideal od P. Pokazat ćemo da je onda nužno $I = P$. Zaista, kako je $I \neq \{0\}$, postoji

$a \in I$ sa svojstvom $a \neq 0$. Jer je P tijelo, a ima inverz $a^{-1} \in P$. Nadalje, budući da je I ideal, imamo

$$\underbrace{a}_{\in I} \cdot \underbrace{a^{-1}}_{\in P} \in I$$

dakle, $1 \in I$. Onda imamo redom

$$P = 1 \cdot P \subset IP \subset I$$

tj. $P \subset I$. Odatle slijedi da je $I = P$. ■

Iz teorema zaključujemo da u teoriji tijela nema smisla pojam kvocijentnog tijela, jer se kvocijent radi po idealu, kojih u tijelu nema (osim trivijalnih).

Konačno, za tijela, odnosno polja, definiramo pojam homomorfizma, kao i kod prstenova. Odmah se vidi da vrijedi

PROPOZICIJA 5

Neka je $f : P \to Q$ homomorfizam tijela. Onda je

(1) $f(1_P) = 1_Q$, *i*

(2) $f(a^{-1}) = [f(a)]^{-1}$, *za svaki* $a \in P$, $a \neq 0$. ■

Analogno se definira i pojam monomorfizma, epimorfizma i, konačno, izomorfizma za tijela i polja. Jasno je da je izomorfizam $f : P \to Q$ tijela izomorfizam aditivnih grupa P i Q i izomorfizam multiplikativnih grupa $P - \{0\}$ i $Q - \{0\}$ tih tijela. Naravno, izomorfizam generira jednu relaciju ekvivalencije, koja klasificira tijela i polja, pa govorimo o klasama izomorfnih tijela, odnosno polja.

Spomenimo na kraju jedan interesantan rezultat u vezi s karakteristikom polja.

TEOREM 6

Neka je P polje karakteristike 0. Onda je potpolje od P generirano jedinicom izomorfno s poljem $\mathbb{Q}$ racionalnih brojeva.

Dokaz

Neka je $q \in \mathbb{Q}$ bilo koji element. Onda možemo pisati $q = a/b$, gdje je $a \in \mathbb{Z}$, $b \in \mathbb{N}$. Uz dogovor da su pritom a i b relativno prosti i da je $0 = 0/1$, gornji je prikaz jednoznačan. Definiramo preslikavanje $h : \mathbb{Q} \to P$ stavljajući

$$h(q) = h(a/b) = (a \cdot 1)(b \cdot 1)^{-1}$$

za svaki $q \in \mathbb{Q}$. Lako se provjeri da je h homomorfizam polja. Nadalje, jezgra $J = J(h) < \mathbb{Q}$ je ideal od $\mathbb{Q}$. Kako je $h(1) = 1 \neq 0$, $J \neq \mathbb{Q}$. No, jer je $\mathbb{Q}$ polje, po Tm. 4 zaključujemo da je $J = \{0\}$. Odatle slijedi da je h monomorfizam. Konačno, jasno je da je $S = S(h) < P$ potpolje od P generirano jedinicom u P, pa je teorem dokazan. ■

ZADACI

1. Neka je $\mathbb{H}$ tijelo kvaterniona, a

$$j : \mathbb{C} \to \mathbb{H}$$

preslikavanje, dano s

$$j(z) = j(x + iy) = (x, y, 0, 0) .$$

Provjeri da je j monomorfizam. Prema tome se polje $\mathbb{C}$ kompleksnih brojeva može identificirati s potpoljem $j(\mathbb{C}) < \mathbb{H}$ tijela kvaterniona i jednostavno pisati $\mathbb{C} < \mathbb{H}$.

2. Kažemo da je ideal $A < P$ prstena P **maksimalan** ako su jedini ideali, koji sadrže A, sam A i čitav P. Neka je P komutativni prsten s jedinicom. Onda je P/A polje ako i samo ako je A maksimalni ideal. Dokaži!

3. Neka je P tijelo i h endomorfizam od P različit od nulhomomorfizma. Neka je

$$A = \{a \in P \mid h(a) = a\} .$$

Pokaži da je A podtijelo od P.

4. Pokaži da su svojstva biti tijelo, odnosno biti polje, invarijantna u odnosu na izomorfizam prstenova.

5. Neka je $f : P \to Q$ homomorfizam tijela. Onda je slika podtijela od P podtijelo u Q i praslika podtijela od Q podtijelo od P. Dokaži! Isto, dakako, vrijedi i za polja.

6. Pokaži da je skup $P = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$ polje, potpolje polja $\mathbb{R}$ realnih brojeva.

7. U polje se može uvesti tradicionalna oznaka $a^{-1} = \frac{1}{a}$ i $ab^{-1} = \frac{a}{b}$. Pokaži da uz te oznake u svakom polju vrijede standardna svojstva "*algebre razlomaka*":

(a) $\frac{a}{b} = \frac{c}{d} \iff ad = bc$;

(b) $\frac{a}{b} = \frac{ac}{bc}$, uz $c \neq 0$;

(c) $\frac{a}{b} \pm \frac{c}{d} = \frac{ad \pm bc}{bd}$;

(d) $\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$;

(e) $\frac{-a}{b} = -\frac{a}{b} = \frac{a}{-b}$.

8. Pokušaj definirati pojam direktnog produkta prstenova, tijela, odnosno polja.

5

KLASIČNA ALGEBRA VEKTORA

U ovom je poglavlju obrađen klasični vektorski račun koji će poslije poslužiti kao motivacija i kao izvor inspiracija u aksiomatskom opisu i istraživanju važnih matematičkih struktura, kao što su linearni i unitarni prostori.

5.1. Uvodne napomene

U egzaktnim se znanostima susrećemo s dvije vrste veličina: u jednu spadaju veličine poput duljine, površine, mase, topline itd., a u drugu veličine kao što su orijentirana dužina, brzina, akceleracija, sila i sl. Prve su određene jednim jedinim podatkom, mjernim brojem, i nazivamo ih **skalarima**. Naprotiv, za potpuno određenje drugog tipa veličina je osim mjernog broja potrebno znati i njihov smjer. Takve veličine nazivamo **vektori**. Iako su vektorske veličine po svom karakteru vrlo različite, iskustvo je pokazalo da se s njima računa po istoj shemi, tzv. **vektorskoj algebri**. To je prvi, još u 16. stoljeću, zapazio nizozemski fizičar S. Stevin, od koga potječe tzv. **paralelogram sila**. Kasnije, u devetnaestom stoljeću, vektorski su račun kao samostalnu matematičku disciplinu razvili H. Grassman, W. R. Hamilton, i mnogi drugi. Danas vektorska metoda nailazi na široke primjene u svim granama matematike,u fizici i u drugim egzaktnim znanostima.

Naravno, u suvremenom ruhu, radi se o strogo aksiomatiziranoj, apstraktnoj teoriji vektorskih prostora koja je samo motivirana klasičnim pristupom i rezultatima. Naš je krajnji cilj upravo detaljno izučavanje te važne matematičke strukture. Međutim, u ovom ćemo poglavlju, kao uvod u kasnija apstraktna razmatranja, dati elemente klasične, naivne vektorske algebre, i to na njezinu standardnom – **geometrijskom modelu**. Razlozi su metodičkog karaktera; u sažetijem pristupu to bi se poglavlje moglo i ispustiti.

5.2. Orijentirane dužine

Neka je s E^3 označen naš standardni, trodimenzionalni prostor za koji pretpostavljamo da ima točkovnu strukturu. Mi ga nećemo ovdje strogo aksiomatski zasnivati (što bi se moglo npr. na osnovi Hilbertove aksiomatizacije euklidske geometrije), jer bi to prešlo okvire ovog udžbenika, nego smatramo da je on intuitivno dan, a njegova osnovna svojstva poznata.

Neka su $A, B \in E^3$ bilo koje dvije točke. Uređeni par (A, B) tih točaka nazivamo **orijentirana dužina**, za koju je točka A **početak**, a B **kraj**. Tu orijentiranu dužinu standardno označavamo s

$$\overrightarrow{AB}$$

i zorno predočavamo kao dužinu određenu točkama A i B i sa strelicom u



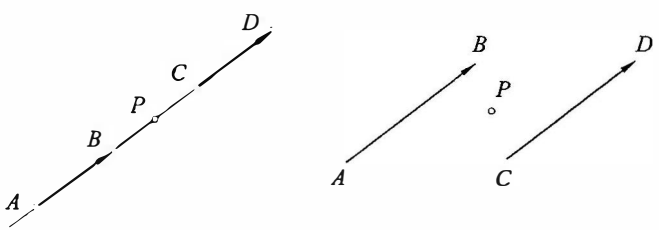
krajnjoj točki B (tj. orijentiranu od A prema B). Odmah uočavamo da $\overrightarrow{AB}$ nije isto što i $\overrightarrow{BA}$. Neka je s

$$\mathcal{D} = E^3 \times E^3$$

označen skup svih orijentiranih dužina u E^3. Na skupu $\mathcal{D}$ definiramo jednu relaciju na ovaj način: Kažemo da je orijentirana dužina $\overrightarrow{AB}$ **ekvivalentna** orijentiranoj dužini $\overrightarrow{CD}$ i pišemo

$$\overrightarrow{AB} \equiv \overrightarrow{CD}\,,$$

ako i samo ako dužine $\overline{AD}$ i $\overline{BC}$ imaju zajedničko polovište. Iz definicije razabiremo da i u slučaju kad sve četiri točke A, B, C i D ne leže na istom



pravcu, te točke sigurno leže u jednoj ravnini (jer se pravci AD i BC sijeku), i u njoj određuju četverokut čije se dijagonale raspolavljaju. Prema tome je $ABDC$ paralelogram.

TEOREM 1

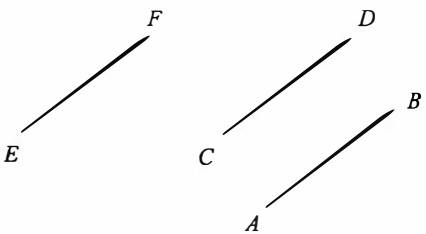
Relacija $\equiv$ *je relacija ekvivalencije na skupu* $\mathcal{D}$.

Dokaz

(1) relacija $\equiv$ je refleksivna, tj. $\overrightarrow{AB} \equiv \overrightarrow{AB}$. Zaista, za svaku orijentiranu dužinu $\overrightarrow{AB}$ dužine $\overline{AB}$ i $\overline{BA}$ imaju isto polovište pa je $\overrightarrow{AB} \equiv \overrightarrow{AB}$ po definiciji.

(2) relacija $\equiv$ je simetrična, tj. iz $\overrightarrow{AB} \equiv \overrightarrow{CD}$ slijedi $\overrightarrow{CD} \equiv \overrightarrow{AB}$. Zaista, iz $\overrightarrow{AB} \equiv \overrightarrow{CD}$ zaključujemo da dužine $\overline{AD}$ i $\overline{BC}$ imaju isto polovište. No, onda i dužine $\overline{CB}$ i $\overline{DA}$ imaju isto polovište, jer su to iste dužine kao prethodne, pa je $\overrightarrow{CD} \equiv \overrightarrow{AB}$.

(3) relacija $\equiv$ je tranzitivna, tj. iz $\overrightarrow{AB} \equiv \overrightarrow{CD}$ i $\overrightarrow{CD} \equiv \overrightarrow{EF}$ slijedi $\overrightarrow{AB} \equiv \overrightarrow{EF}$. Pretpostavimo najprije da orijentirane dužine $\overrightarrow{AB}, \overrightarrow{CD}$ i $\overrightarrow{EF}$ leže



na tri različita pravca u E^3. Onda iz pretpostavke slijedi da je $ABDC$ paralelogram, pa je $\overline{AB} \parallel \overline{CD}$ i također $\overline{AB} = \overline{CD}$ (gdje znak jednakosti ovdje znači da su te dužine sukladne, kongruentne). Isto tako, iz pretpostavke slijedi da je $CDFE$ paralelogram, tj. $\overline{CD} \parallel \overline{EF}$ i $\overline{CD} = \overline{EF}$. No, iz tranzitivnosti relacija paralelnosti i kongruencije dužina zaključujemo da je $\overline{AB} \parallel \overline{EF}$ i $\overline{AB} = \overline{EF}$, što pokazuje da je $ABFE$ paralelogram, dakle $\overrightarrow{AB} \equiv \overrightarrow{EF}$. Slično se pokazuje tranzitivnost u ostalim mogućim slučajevima. Time je teorem dokazan. ■

Korisna je i ova

PROPOZICIJA 2

Iz $\overrightarrow{AB} \equiv \overrightarrow{CD}$ *slijedi* $\overrightarrow{AC} \equiv \overrightarrow{BD}$.

Dokaz

$\overrightarrow{AB} \equiv \overrightarrow{CD}$ znači da dužine $\overline{AD}$ i $\overline{BC}$ imaju zajedničko polovište. No, onda će i $\overline{AD}$ i $\overline{CB}$ imati zajedničko polovište, što znači da je $\overrightarrow{AC} \equiv \overrightarrow{BD}$. ■

ZADACI

1. Pokaži tranzitivnost relacije $\equiv$, kad neke od orijentiranih dužina leže na istom pravcu.

5.3. Vektori

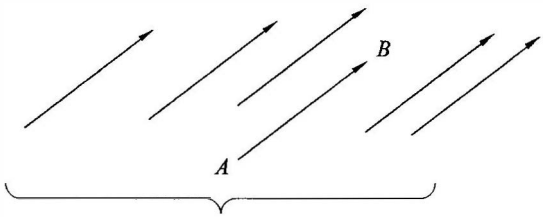
Kako smo vidjeli, $\equiv$ je dobro definirana relacija ekvivalencije na skupu $\mathcal{D} = E^3 \times E^3$ svih orijentiranih dužina. Klasu ekvivalencije određenu orijentiranom dužinom $\overrightarrow{AB}$ označavamo s $[\overrightarrow{AB}]$, tj.

$$[\overrightarrow{AB}] = \{\overrightarrow{PQ} \in \mathcal{D} \mid \overrightarrow{PQ} \equiv \overrightarrow{AB}\} .$$

Promatrajmo sada skup svih klasa ekvivalencije, tj. kvocijentni skup

$$V^3 = \mathcal{D}/_{\equiv} = \{[\overrightarrow{AB}] \mid \overrightarrow{AB} \in \mathcal{D}\} .$$

Svaki element iz skupa V^3, tj. svaku klasu ekvivalencije orijentiranih dužina nazivamo **vektor**, a skup V^3 nazivamo onda **prostor vektora** ili (trodimenzionalni) **vektorski prostor**.



vektor $[\overrightarrow{AB}]$

Vektori se kraće i standardno označavaju malim latiničnim slovima sa strelicom, tj. kao $\vec{a}, \vec{b}, \vec{c}, .., \vec{x}, \vec{y}, \vec{z}$. Ako je, dakle, $\overrightarrow{AB} \in \vec{a}$, tj. orijentirana dužina koja generira vektor $\vec{a}$, onda pišemo

$$\vec{a} = [\overrightarrow{AB}]$$

i kažemo da je $\overrightarrow{AB}$ **predstavnik** ili **reprezentant** vektora $\vec{a}$. Očito vrijedi ova

PROPOZICIJA 1

Neka je $\vec{a} \in V^3$ bilo koji vektor, a $A \in E^3$ bilo koja točka. Onda postoji jedna i samo jedna točka $B \in E^3$ sa svojstvom da je

$$[\overrightarrow{AB}] = \vec{a} .$$

Dokaz

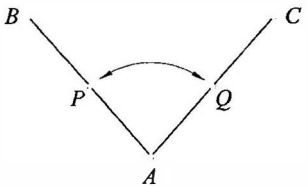
Neka je $\overrightarrow{CD} \in \vec{a}$ odabrana tako da točka A ne leži na pravcu CD. Onda konstruiramo paralelogram $CDBA$ sa stranicama $\overline{CD}$ i $\overline{CA}$ i dokaz je gotov. Egzistencija i jednoznačnost točke B je osigurana aksiomima euklidske geometrije. ■

Kažemo popularno da smo vektor $\vec{a}$ "nanijeli" iz točke A kao početka.

Neka su $A, B \in E^3$ bilo koje dvije točke. Onda je očito $\overrightarrow{AA} \equiv \overrightarrow{BB}$ jer dužine $\overline{AB}$ i $\overline{AB}$ imaju isto polovište (jer je to ista dužina). Prema tome, sve orijentirane dužine oblika

$$\overrightarrow{XX}\,,$$

gdje je $X \in E^3$, tj. orijentirane dužine koje imaju isti početak i kraj, pripadaju istoj klasi ekvivalencije, tj. predstavnici su istog vektora u V^3. Ali i obratno: ako je neka orijentirana dužina u toj klasi, ona je nužno navedenog oblika. Zaista, neka je $\overrightarrow{BC} \equiv \overrightarrow{AA}$. Onda dužine $\overline{BA}$ i $\overline{CA}$ imaju isto polovište, a to je moguće jedino uz uvjet da je $B = C$.



Prema tome, sve orijentirane dužine oblika $\overrightarrow{XX}$ i samo one pripadaju jednoj klasi ekvivalencije, istom elementu u V^3. Taj vektor nazivamo **nulvektor** i označavamo ga s $\vec{0}$. Dakle,

$$\vec{0} = [\overrightarrow{XX}] = \{\overrightarrow{XX} \mid X \in E^3\}\,.$$

Uvedimo sada i pojam suprotnog vektora. Najprije ćemo dokazati da vrijedi

PROPOZICIJA 2

Neka je $\overrightarrow{AB} \equiv \overrightarrow{CD}$. Onda je $\overrightarrow{BA} \equiv \overrightarrow{DC'}$ ako i samo ako je $C' = C$.

Dokaz

Neka je $C' = C$. Iz pretpostavke $\overrightarrow{AB} \equiv \overrightarrow{CD}$ slijedi da $\overline{AD}$ i $\overline{BC}$ imaju isto polovište. No, onda $\overline{BC}$ i $\overline{AD}$ imaju isto polovište, pa je $\overrightarrow{BA} \equiv \overrightarrow{DC}$ po definiciji. Obratno, ako je $\overrightarrow{BA} \equiv \overrightarrow{DC'}$, onda bi zajedno s prethodno dokazanom tvrdnjom $\overrightarrow{BA} \equiv \overrightarrow{DC}$, zbog simetrije i tranzitivnosti dobili $\overrightarrow{DC'} \equiv \overrightarrow{DC}$, što bi značilo da dužine $\overline{DC}$ i $\overline{C'D}$ imaju isto polovište, a to je moguće jedino tako da bude $C' = C$. ■

Na osnovi propozicije imamo, dakle, ovaj zaključak: Ako svim orijentiranim dužinama neke klase, vektora $\vec{a}$, zamijenimo ulogu početka i kraja, dobivamo opet orijentirane dužine neke klase, kažimo vektora $\vec{b}$; i nadalje, svi predstavnici tog vektora mogu se dobiti na taj način. Kažemo da je vektor $\vec{b}$ **suprotan** vektoru $\vec{a}$ i pišemo

$$\vec{b} = -\vec{a}\,.$$

Očito je iz definicije kako je taj odnos simetričan, tj. da je tada i

$$\vec{a} = -\vec{b}$$

pa govorimo o **paru suprotnih vektora**. Zato je uvijek

$$-(-\vec{a}) = \vec{a}\,.$$

Ako je $\overrightarrow{AB}$ reprezentant vektora $\vec{a}$, onda je $\overrightarrow{BA}$ reprezentant vektora $-\vec{a}$. Za takve dvije orijentirane dužine također kažemo da su **suprotne** i pišemo

$$\overrightarrow{BA} = -\overrightarrow{AB}\,.$$

Neka je sada $O \in E^3$ bilo koja dana točka. Neka je s

$$V^3(O)$$

označen skup svih orijentiranih dužina koje imaju početak u točki O, tj.

$$V^3(O) = \{\overrightarrow{OX} \mid X \in E^3\}\,.$$

Svaki element tog skupa nazivamo **radijvektor** u točki O i pišemo kraće

$$\overrightarrow{OX} = \vec{r}_x\,.$$

Skup $V^3(O)$ nazivamo i **prostor radijvektora** (u točki O).

ZADACI

1. Pokaži da postoje bijektivna preslikavanja $f : E^3 \to V^3(O)$ i $g : V^3(O) \to V^3$ pa onda i bijekcija $h : E^3 \to V^3$ kao njihova kompozicija. Posebno, bijekcija g pokazuje da se vektorski prostor V^3 može **reprezentirati** prostorom $V^3(O)$ radijvektora, što je katkad prikladnije, a svakako zornije, jer su tu elementi orijentirane dužine, a ne klase. [Uputa: Definiraj $f(X) = \overrightarrow{OX}$ i $g(\overrightarrow{OX}) = [\overrightarrow{OX}] = \vec{x}$ i koristi Prop. 1.]

5.4. Modul, smjer i orijentacija vektora

Kako smo već rekli, ako točke A, B, C i D ne leže na istom pravcu, iz činjenice da je $\overrightarrow{AB} \equiv \overrightarrow{CD}$ slijedi da je $ABDC$ paralelogram. Zbog toga su dužine $\overline{AB}$ i F $\overline{CD}$ paralelne i jednakih duljina. To opravdava definicije koje slijede.

Neka je $\vec{a} = [\overrightarrow{AB}]$ bilo koji vektor iz V^3. Pod **modulom** ili **duljinom** $|\vec{a}|$ vektora $\vec{a}$ razumijevamo duljinu predstavnika $\overrightarrow{AB}$ tog vektora, tj. broj koji se dobiva mjerenjem dužine $\overline{AB}$ danom jediničnom dužinom $\overline{OE}$*).

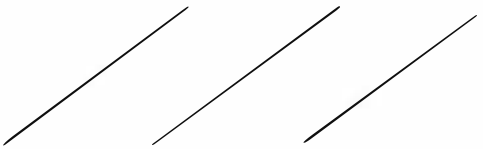
$$|\vec{a}| = \frac{\overline{AB}}{\overline{OE}} \in \mathbb{R} .$$

Iz prethodne je napomene jasno da je modul dobro definirano preslikavanje

$$V^3 \to \mathbb{R} ,$$

tj. da ne ovisi o izboru reprezentanta vektora. Očito je, nadalje, da je $|\vec{0}| = 0$, i da je to jedini vektor toga svojstva.

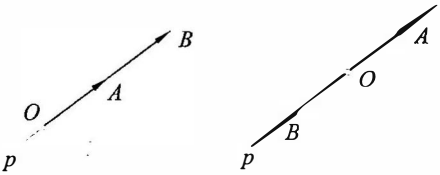
Pod **smjerom** $s_{\vec{a}}$ vektora $\vec{a}$ podrazumijevamo smjer s_{AB} pravca AB (vidi Zad.1.) određenog predstavnikom $\overrightarrow{AB}$ vektora $\vec{a}$. Očito je da smjer vektora ne ovisi o izboru predstavnika jer su pravci koje određuju orijentirane dužine



iz iste klase paralelni, a paralelni pravci imaju isti smjer. Jasno je, nadalje, da je nulvektor $\vec{0}$ jedini vektor za koji smjer nije određen.

Orijentacija ili **smisao** vektora $\vec{a}$ inducirana je orijentacijom bilo kojeg predstavnika tog vektora (vidi i Zad. 2.).

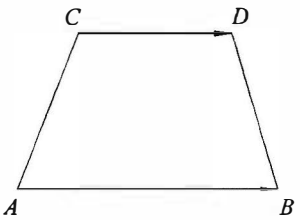
Ako su $\vec{a}, \vec{b} \in V^3$ vektori istog smjera, a $\overrightarrow{OA}$ i $\overrightarrow{OB}$ predstavnici tih vektora s istim početkom O, onda je jasno da će točke O, A i B ležati na istom pravcu p.

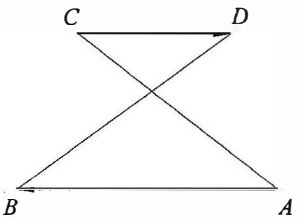


Kažemo da vektori $\vec{a}$ i $\vec{b}$ imaju **istu orijentaciju**, ako točke A i B leže na pravcu p s iste strane točke O. Vektori $\vec{a}$ i $\vec{b}$ su **suprotnih orijentacija** ako su A i B s različitih strana točke O. Jasno je da ti pojmovi ne ovise o predstavnicima, tj. o izboru točke O. Razabiremo da će vektori $\vec{a}$ i $\vec{b}$ imati istu orijentaciju ako i samo ako bilo koji predstavnici $\overrightarrow{AB}$ i $\overrightarrow{CD}$ tih vektora, koji ne leže na istom pravcu, određuju trapez $ABDC$ čiji se krakovi ne sijeku.

*) U daljnjem ćemo tekstu, zbog jednostavnosti, i duljinu dužine $\overline{AB}$ označivati s $\overline{AB}$.

Ako se krakovi tog trapeza sijeku, vektori $\vec{a}$ i $\vec{b}$ imaju suprotne orijentacije.





Iz svega navedenog zaključujemo da vrijedi

PROPOZICIJA 1

Vektor iz V^3 jednoznačno je određen svojim modulom, smjerom i orijentacijom. ■

Isto je tako jasno da vrijedi

PROPOZICIJA 2

Dva suprotna vektora imaju isti modul i isti smjer, ali suprotne orijentacije. ■

ZADACI

1. Na skupu $\mathcal{P}$ svih pravaca u E^3 definiramo relaciju $\|$, tj. relaciju "*biti paralelan*" na uobičajen način. Uvjeri se da je to dobro definirana relacija ekvivalencije. Kvocijentni skup $\mathcal{P}/_{\|}$ nazivamo **skup smjerova** u E^3, a svaku klasu, element u tom skupu, nazivamo **smjer** u E^3; klasu generiranu pravcem p označavamo s $[p]$. Neka je

$$s : \mathcal{P} \to \mathcal{P}/_{\|}$$

kvocijentno preslikavanje, $s(p) = [p]$. Onda $s_p = s(p)$ nazivamo **smjer pravca** p.

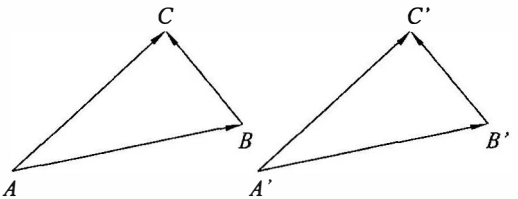
2. Pojam orijentacije vektora može se definirati precizno: Neka je S skup svih vektora iz V^3, koji imaju isti smjer. Za svaki $\vec{x} \in S$ neka je $\overrightarrow{OX}$ predstavnik tog vektora s početkom u danoj točki O. Na skupu S definiramo relaciju $\sim$ stavljajući $\vec{a} \sim \vec{b}$ ako i samo ako pripadne točke A i B leže s iste strane točke O (na pravcu koji ih nosi). Uvjeri se da je $\sim$ relacija ekvivalencije i da se kvocijentni skup $S/_{\sim}$ sastoji od točno dvije klase. Kvocijentno preslikavanje $S \to S/_{\sim}$ pridružuje svakom vektoru $\vec{a} \in S$ jednu od tih klasa, $[\vec{a}]$, koju zovemo **orijentacija vektora** $\vec{a}$. Dakako, vektori $\vec{a}, \vec{b} \in S$ su iste orijentacije ako je $[\vec{a}] = [\vec{b}]$, a suprotnih orijentacija ako je $[\vec{a}] \neq [\vec{b}]$.

5.5. Zbrajanje vektora

Na V^3 definirat ćemo sada razne strukture, prije svega operaciju zbrajanja vektora. U tu svrhu najprije dokažimo da vrijedi

PROPOZICIJA 1
Neka je $\overrightarrow{AB} \equiv \overrightarrow{A'B'}$ *i* $\overrightarrow{BC} \equiv \overrightarrow{B'C'}$. *Onda je i* $\overrightarrow{AC} \equiv \overrightarrow{A'C'}$.

Dokaz
Prema Prop.2 u 5.2. imamo da $\overrightarrow{AB} \equiv \overrightarrow{A'B'}$ povlači $\overrightarrow{AA'} \equiv \overrightarrow{BB'}$ i isto



tako da $\overrightarrow{BC} \equiv \overrightarrow{B'C'}$ povlači $\overrightarrow{BB'} \equiv \overrightarrow{CC'}$. No, onda zbog tranzitivnosti imamo

$$\overrightarrow{AA'} \equiv \overrightarrow{BB'} \equiv \overrightarrow{CC'},$$

dakle $\overrightarrow{AA'} \equiv \overrightarrow{CC'}$, odnosno prema već navedenoj propoziciji $\overrightarrow{AC} \equiv \overrightarrow{A'C'}$, što se i tvrdilo. ■

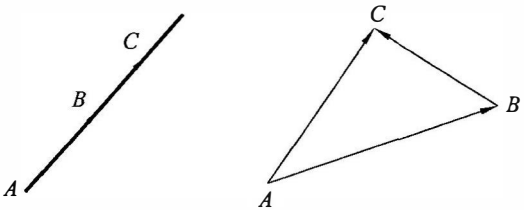
Na V^3 sada definiramo binarnu operaciju

$$s : V^3 \times V^3 \to V^3$$

koju nazivamo **zbrajanje vektora** i bilježimo sa

$$s(\vec{a}, \vec{b}) = \vec{a} + \vec{b} = \vec{c},$$

gdje za vektor $\vec{c}$ kažemo da je **zbroj** vektora $\vec{a}$ i $\vec{b}$ i do njega dolazimo na ovaj način: Neka je $\overrightarrow{AB} \in \vec{a}$ bilo koji predstavnik vektora $\vec{a}$, a $\overrightarrow{BC} \in \vec{b}$ onaj



predstavnik vektora $\vec{b}$ koji ima početak u točki B (taj je jedinstven). Onda definiramo

$$\vec{c} = \vec{a} + \vec{b} = [\overrightarrow{AB}] + [\overrightarrow{BC}] = [\overrightarrow{AC}] ,$$

tj. vektor $\vec{c}$ je klasa generirana orijentiranom dužinom $\overrightarrow{AC}$. Navedena konstrukcija se iz očiglednih razloga naziva **pravilo trokuta** pa kažemo, popularno, kako vektore zbrajamo po zakonu trokuta.

Razabiremo da je zbrajanje vektora dobro definirano, tj. da ne ovisi o izboru predstavnika. Ako je, naime, $\overrightarrow{A'B'} \in \vec{a}$ neki drugi predstavnik vektora $\vec{a}$, a $\overrightarrow{B'C'} \in \vec{b}$ onaj predstavnik vektora $\vec{b}$ kojemu je početak u točki B', imamo po definiciji zbrajanja

$$\vec{a} + \vec{b} = [\overrightarrow{A'B'}] + [\overrightarrow{B'C'}] = [\overrightarrow{A'C'}] ,$$

ali je prema Prop. 1 $\overrightarrow{A'C'} \equiv \overrightarrow{AC}$, pa je

$$[\overrightarrow{A'C'}] = [\overrightarrow{AC}] = \vec{c} ,$$

tj. dobivamo isti rezultat. Zbrajanjem je na V^3 definirana jedna dobra struktura. Vrijedi naime

TEOREM 2

Skup V^3 je u odnosu na zbrajanje vektora komutativna grupa.

Dokaz

(1) Zbrajanje je asocijativno. Zaista, neka su $\vec{a}, \vec{b}, \vec{c} \in V^3$ bilo koja tri vektora, i neka je $\vec{a} = [\overrightarrow{AB}]$, $\vec{b} = [\overrightarrow{BC}]$ i $\vec{c} = [\overrightarrow{CD}]$. Onda po zakonu trokuta imamo

$$(\vec{a} + \vec{b}) + \vec{c} = ([\overrightarrow{AB}] + [\overrightarrow{BC}]) + [\overrightarrow{CD}] = [\overrightarrow{AC}] + [\overrightarrow{CD}] = [\overrightarrow{AD}]$$

$$\vec{a} + (\vec{b} + \vec{c}) = [\overrightarrow{AB}] + ([\overrightarrow{BC}] + [\overrightarrow{CD}]) = [\overrightarrow{AB}] + [\overrightarrow{BD}] = [\overrightarrow{AD}] ,$$

pa je asocijativnost dokazana.

(2) Za zbrajanje postoji lijeva nula i to je nulvektor $\vec{0}$. Zaista, neka je $\vec{a} = [\overrightarrow{AB}]$ bilo koji vektor i $\vec{0} = [\overrightarrow{AA}]$. Onda imamo

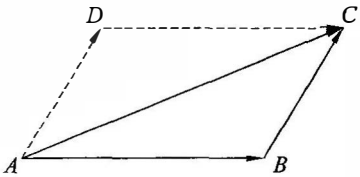
$$\vec{0} + \vec{a} = [\overrightarrow{AA}] + [\overrightarrow{AB}] = [\overrightarrow{AB}] = \vec{a} .$$

(3) Za svaki vektor postoji lijevi suprotni element, i to je upravo njemu suprotni vektor. Zaista, ako je $\vec{a} = [\overrightarrow{AB}]$ bilo koji vektor, onda je $-\vec{a} = [\overrightarrow{BA}]$ pa imamo

$$(-\vec{a}) + \vec{a} = [\overrightarrow{BA}] + [\overrightarrow{AB}] = [\overrightarrow{BB}] = \vec{0} .$$

Iz (1)–(3), a na osnovi Tm. 1 iz 2.6. zaključujemo da je V^3 grupa. Konačno, imamo:

(4) Zbrajanje vektora je komutativno. Neka su $\vec{a}, \vec{b} \in V^3$ bilo koji vektori i neka je $\vec{a} = [\overrightarrow{AB}]$ i $\vec{b} = [\overrightarrow{BC}]$. Onda je, naravno, $\vec{a} + \vec{b} = [\overrightarrow{AC}]$. U drugu ruku, neka je $D \in E^3$ točka sa svojstvom da je $\overrightarrow{AD} \equiv \overrightarrow{BC}$. Onda je prema



Prop. 2 iz 5.2. i $\overrightarrow{AB} \equiv \overrightarrow{DC}$, pa imamo

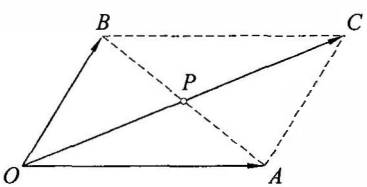
$$\vec{b} + \vec{a} = [\overrightarrow{BC}] + [\overrightarrow{AB}] = [\overrightarrow{AD}] + [\overrightarrow{DC}] = [\overrightarrow{AC}] ,$$

tj. $\vec{a} + \vec{b} = \vec{b} + \vec{a}$ i komutativnost je dokazana. ■

Iz činjenice da je V^3 komutativna grupa, slijedi neposredno da možemo zbrajati tri i više vektora neovisno o njihovu poretku u zbroju i ispuštati zagrade ili ih prema potrebi stavljati.

ZADACI

1. U V^3 definiraj zbrajanje na ovaj način: Neka su $\vec{a}, \vec{b} \in V^3$ bilo koja dva vektora, $O \in E^3$ bilo koja točka, a $\overrightarrow{OA}$ i $\overrightarrow{OB}$ predstavnici vektora $\vec{a}$, odnosno $\vec{b}$, s istom početnom točkom O. Neka je $C \in E^3$ točka



sa svojstvom da dužine $\overline{OC}$ i $\overline{AB}$ imaju zajedničko polovište. Onda definiramo

$$\vec{a} + \vec{b} = [\overrightarrow{OA}] + [\overrightarrow{OB}] = [\overrightarrow{OC}] .$$

Ako točke O, A, B i C ne leže na istom pravcu, one nužno leže u jednoj ravnini i to tako da je $OACB$ paralelogram. Zato se taj zakon zbrajanja popularno zove **pravilo paralelograma** (paralelogram sila). Rezultirajući vektor je, naime, dijagonala paralelograma razapetog sumandima. Pokaži:

(a) Ovako definirano zbrajanje ne ovisi o izboru predstavnika, tj. o izboru točke O.

(b) Ovako definirano zbrajanje vektora je ekvivalentno u tekstu definiranom zbrajanju po zakonu trokuta.

2. Oduzimanje vektora svodi se na zbrajanje, tj. za $\vec{a}, \vec{b} \in V^3$ definiramo njihovu **razliku** s
$$\vec{a} - \vec{b} = \vec{a} + (-\vec{b}) .$$
Pokaži: Ako je $\vec{a} = [\overrightarrow{OA}]$ i $\vec{b} = [\overrightarrow{OB}]$, onda je $\vec{a} - \vec{b} = [\overrightarrow{BA}]$. Ilustriraj taj rezultat grafički.

3. Neka su $\vec{a}, \vec{b}, \vec{c} \in V^3$ bilo koji vektori, a $\overrightarrow{AB}, \overrightarrow{BC}$ i $\overrightarrow{CD}$ njihovi predstavnici. Onda je
$$\vec{a} + \vec{b} + \vec{c} = \vec{0}$$
ako i samo ako je $D = A$. Dokaži!

4. Prethodni rezultat može se generalizirati. Neka su $A_1, \ldots, A_n \in E^3$ bilo koje točke. Onda je
$$[\overrightarrow{A_1A_2}] + [\overrightarrow{A_2A_3}] + \cdots + [\overrightarrow{A_{n-1}A_n}] + [\overrightarrow{A_nA_1}] = \vec{0} .$$
To je tzv. **Charlesova relacija**.

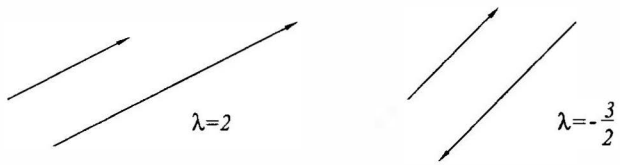
5.6. Množenje vektora skalarom

Daljnja operacija s vektorima, koju ćemo definirati, jest produljivanje (rastezanje, dilatacija) i skraćivanje (stezanje, kontrakcija) vektora, tj. množenje vektora skalarom, realnim brojem. Neka je $\mathbb{R}$ polje realnih brojeva. Tada pod **množenjem vektora realnim brojevima** razumijevamo preslikavanje
$$m : \mathbb{R} \times V^3 \to V^3$$
gdje vektor $m(\lambda, \vec{a}) \in V^3$ pišemo kratko kao $\lambda\vec{a}$ i nazivamo **produktom realnog broja i vektora**, a definiran je na ovaj način:

(1) modul: $|\lambda\vec{a}| = |\lambda| \cdot |\vec{a}|$, tj. jednak je produktu apsolutne vrijednosti realnog broja λ i modula vektora $\vec{a}$,

(2) smjer: $s_{\lambda\vec{a}} = s_{\vec{a}}$, tj. smjer vektora $\lambda\vec{a}$ isti je kao smjer vektora $\vec{a}$,

(3) orijentacija: vektori $\lambda\vec{a}$ i $\vec{a}$ su istih, odnosno suprotnih orijentacija već prema tome je li $\lambda > 0$ ili $\lambda < 0$.



Time je prema Prop. 1 u 5.4. vektor $\lambda\vec{a} \in V^3$ određen jednoznačno.

PROPOZICIJA 1

$\lambda\vec{a} = \vec{0}$ onda i samo onda, ako je $\lambda = 0$ ili $\vec{a} = \vec{0}$.

Dokaz

Iz definicije slijedi da je $0 \cdot \vec{a} = \vec{0}$, i također, da je $\lambda \cdot \vec{0} = \vec{0}$. Obratno, neka je $\lambda\vec{a} = \vec{0}$. Onda je $|\lambda\vec{a}| = |\vec{0}| = 0$, tj. $|\lambda| \cdot |\vec{a}| = 0$, a budući da su to realni brojevi, to je ili $|\lambda| = 0$ ili $|\vec{a}| = 0$. Prema tome je ili $\lambda = 0$ ili $\vec{a} = \vec{0}$, što se i tvrdilo. ■

Karakteristična svojstva operacije množenja vektora skalarima su sadržana u:

TEOREM 2

Množenje vektora realnim brojevima ima ova osnovna svojstva:

(1) *kvaziasocijativnost, tj.*

$$\lambda(\mu\vec{a}) = (\lambda\mu)\vec{a}\,;$$

(2) *posjedovanje "jedinice" za to množenje, tj.*

$$1 \cdot \vec{a} = \vec{a}\,;$$

(3) *distributivnost u odnosu na zbrajanje skalara, tj.*

$$(\lambda + \mu)\vec{a} = \lambda\vec{a} + \mu\vec{a}\,;$$

(4) *distributivnost u odnosu na zbrajanje vektora, tj.*

$$\lambda(\vec{a} + \vec{b}) = \lambda\vec{a} + \lambda\vec{b}\,,$$

sve za svaki izbor $\lambda, \mu \in \mathbb{R}$ i vektora $\vec{a}, \vec{b} \in V^3$.

Dokaz

(1) Ako je $\lambda = 0$ ili $\mu = 0$ tvrdnja je trivijalna. Pretpostavimo zato, da je $\lambda \neq 0$ i $\mu \neq 0$. Imamo najprije

$$|\lambda(\mu\vec{a})| = |\lambda| \cdot |\mu\vec{a}| = |\lambda|(|\mu| \cdot |\vec{a}|) = (|\lambda| \cdot |\mu|) \cdot |\vec{a}| = |\lambda\mu| \cdot |\vec{a}| = |(\lambda\mu)\vec{a}|\,,$$

tj. vektori u (1) imaju isti modul. Očito je, nadalje, da ti vektori imaju isti smjer (i taj je jednak smjeru vektora $\vec{a}$). Ostaje utvrditi da se podudaraju i u orijentaciji. No, $\vec{a}$ i $\mu\vec{a}$ imaju istu, odnosno suprotne orijentacije, već prema tome je li $\mu > 0$ ili $\mu < 0$. Nadalje, $\mu\vec{a}$ i $\lambda(\mu\vec{a})$ imaju istu ili suprotne orijentacije u ovisnosti o tome je li $\lambda > 0$ ili $\lambda < 0$. Sada je lako provjeriti (četiri mogućnosti predznaka za λ i μ) da će $\vec{a}$ i $\lambda(\mu\vec{a})$ biti iste ili suprotnih orijentacija, već prema tome je li $\lambda\mu > 0$ ili $\lambda\mu < 0$. U drugu ruku, $\vec{a}$ i $(\lambda\mu)\vec{a}$ će imati, po definiciji, iste ili suprotne orijentacije u zavisnosti od toga, je li $\lambda\mu > 0$ ili $\lambda\mu < 0$. Prema tome, vektori $\lambda(\mu\vec{a})$ i $(\lambda\mu)\vec{a}$ imaju uvijek istu orijentaciju (istu kao $\vec{a}$, ako je $\lambda\mu > 0$, odnosno suprotnu od $\vec{a}$, ako je $\lambda\mu < 0$), pa je time jednakost u (1) provjerena.

(2) Trivijalno.

(3) Tu imamo različite mogućnosti, u ovisnosti o predznaku i apsolutnoj vrijednosti skalara λ i μ. Pokažimo, na primjer, tvrdnju u slučaju kad je $\lambda > 0$, $\mu < 0$ i $|\lambda| > |\mu|$, dakle $\lambda + \mu > 0$. Neka je $\lambda\vec{a} = [\overrightarrow{AB}]$ i $\mu\vec{a} = [\overrightarrow{BC}]$. Kako su ti vektori istog smjera, točke A, B i C leže na istom pravcu. Nadalje, ti su vektori, zbog $\lambda > 0$ i $\mu < 0$, suprotnih orijentacija, a jer je $|\lambda| > |\mu|$, to je

$$\overline{AB} = |\lambda\vec{a}| = |\lambda| \cdot |\vec{a}| > |\mu| \cdot |\vec{a}| = |\mu\vec{a}| = \overline{BC}$$

pa je točka C očito između točaka A i B. Imamo zato, zbog $\lambda\vec{a} + \mu\vec{a} = [\overrightarrow{AC}]$, redom

$$\begin{aligned} |\lambda\vec{a} + \mu\vec{a}| &= \overline{AC} = \overline{AB} - \overline{BC} = |\lambda| \cdot |\vec{a}| - |\mu| \cdot |\vec{a}| = \\ &= (\text{zbog } \lambda > 0, \mu < 0) = \lambda|\vec{a}| + \mu|\vec{a}| = (\lambda + \mu)|\vec{a}| = \\ &= (\text{zbog } \lambda + \mu > 0) = |\lambda + \mu| \cdot |\vec{a}| = |(\lambda + \mu)\vec{a}| \end{aligned}$$

tj. vektori $\lambda\vec{a} + \mu\vec{a}$ i $(\lambda + \mu)\vec{a}$ su jednaki po modulu. Očito je da su ti vektori jednaki i po smjeru, jer oba imaju isti smjer kao vektor $\vec{a}$. Konačno, jer su točke C i B s iste strane točke A, vektori $\lambda\vec{a} + \mu\vec{a} = [\overrightarrow{AC}]$ i $\lambda\vec{a} = [\overrightarrow{AB}]$ imaju istu orijentaciju i, nadalje, zbog $\lambda > 0$, $\lambda\vec{a}$ i $\vec{a}$ imaju istu orijentaciju. Prema tome, $\lambda\vec{a} + \mu\vec{a}$ i $\vec{a}$ imaju istu orijentaciju. U drugu ruku, zbog $\lambda + \mu > 0$ vektori $\vec{a}$ i $(\lambda + \mu)\vec{a}$ imaju istu orijentaciju. Odatle slijedi da vektori $\lambda\vec{a} + \mu\vec{a}$ i $(\lambda + \mu)\vec{a}$ imaju istu orijentaciju, pa je zaista

$$\lambda\vec{a} + \mu\vec{a} = (\lambda + \mu)\vec{a}\,,$$

kako se i tvrdilo. Slično se tvrdnja dokazuje i u ostalim mogućim slučajevima (njih **pet**, ne računajući trivijalne slučajeve, tj. kad je $\lambda = 0$ ili $\mu = 0$ ili $\lambda + \mu = 0$).

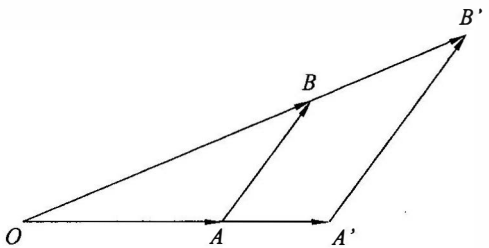
(4) Ako je $\lambda = 0$, tvrdnja je trivijalna. Neka je zato $\lambda \neq 0$. Pretpostavimo najprije da $\vec{a}$ i $\vec{b}$ nemaju isti smjer. Neka je $\vec{a} = [\overrightarrow{OA}]$ i $\vec{b} = [\overrightarrow{AB}]$.

Onda je, po pravilu trokuta, $\vec{a} + \vec{b} = [\overrightarrow{OB}]$. Neka je, nadalje, $\lambda\vec{a} = [\overrightarrow{OA'}]$. Jasno je da su točke O, A i A' na istom pravcu. Odaberimo točku B' na pravcu OB tako da trokuti OAB i $OA'B'$ budu slični,

$$\Delta OAB \simeq \Delta OA'B' .$$

Iz sličnosti slijedi da je $A'B' \parallel AB$ i da je $\overline{A'B'} = \lambda\,\overline{AB}$ (jer je $\overline{OA'} = \lambda\,\overline{OA}$), pa zaključujemo da je

$$[\overrightarrow{A'B'}] = \lambda\vec{b} .$$



U drugu ruku, također iz sličnosti, imamo $\overline{OB'} = \lambda\,\overline{OB}$, a jer su točke O, B i B' na istom pravcu, zaključujemo

$$[\overrightarrow{OB'}] = \lambda[\overrightarrow{OB}] .$$

Prema tome je

$$\lambda\vec{a} + \lambda\vec{b} = [\overrightarrow{OA'}] + [\overrightarrow{A'B'}] = [\overrightarrow{OB'}] = \lambda[\overrightarrow{OB}] = \lambda(\vec{a} + \vec{b}) ,$$

što se i tvrdilo. Slično se tvrdnja dokazuje i kad su vektori $\vec{a}$ i $\vec{b}$ istog smjera, pa je dokaz završen. ■

Dodajmo na kraju još ovo: Ako je za elemente bilo koje aditivne grupe definirano i množenje elementima nekog polja, pa ako to množenje ima svojstva (1) – (4) nabrojena u Tm. 2, onda takvu strukturu zovemo **linearni** ili **vektorski prostor nad danim poljem**. Prema tome vrijedi

TEOREM 3

Skup V^3 je u odnosu na operacije zbrajanja vektora i množenja vektora realnim brojevima vektorski prostor nad poljem $\mathbb{R}$ realnih brojeva. ■

Time smo opravdali naziv vektorski prostor za V^3. O linearnim ili vektorskim prostorima, u svoj njihovoj općenitosti, govori se kasnije (vidi sedmo poglavlje).

ZADACI

1. Iz definicije množenja vektora skalarom slijedi da je $(-1)\vec{a} = -\vec{a}$. Koristeći Tm. 2 pokaži da vrijedi općenitije:

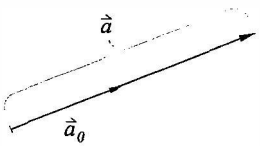
$$(-\lambda)\vec{a} = -(\lambda\vec{a}) ,$$

za svaki $\lambda \in \mathbb{R}$ i $\vec{a} \in V^3$.

2. Za vektor $\vec{e} \in V^3$ kažemo da je **jedinični vektor** ili **ort**, ako je $|\vec{e}| = 1$. Svakom vektoru $\vec{a} \neq \vec{0}$ možemo pridružiti vektor

$$\vec{a}_0 = \frac{1}{|\vec{a}|} \cdot \vec{a} ,$$

koji nazivamo **jedinični vektor u smjeru vektora** $\vec{a}$. Pokaži da je $\vec{a}_0$



zaista jedinični vektor, i da ima isti smjer i istu orijentaciju kao vektor $\vec{a}$.

3. Struktura vektorskog prostora na V^3 može se definirati i bez metrike, tj. **bez pojma modula vektora**. Zaista, taj nam pojam nije bio potreban u definiciji zbrajanja vektora. Pri definiciji množenja vektora skalarom može se također izbjeći. Naime, ako je $n \in \mathbb{N}$ bilo koji prirodni broj, lako je za dani vektor $\vec{a} \in V^3$ geometrijski definirati vektor $n \cdot \vec{a}$ i $1/n \cdot \vec{a}$, pa onda i $m/n \cdot \vec{a} = m\,(1/n \cdot \vec{a})$. Konačno, za bilo koji $\lambda \in \mathbb{R}$ definiramo $\lambda\vec{a} = \lim_{i\to\infty} r_i\vec{a}$, gdje je $(r_i) \to \lambda$ bilo koji niz racionalnih brojeva koji aproksimira realni broj λ. Provjeri te tvrdnje.

4. Neka je s E^2 označena ravnina sa svojom točkovnom strukturom, s $E^2 \times E^2$ skup svih orijentiranih dužina u ravnini, a s

$$V^2 = E^2 \times E^2/_{\equiv}$$

skup klasa ekvivalentnih orijentiranih dužina, prema prije definiranoj relaciji ekvivalencije $\equiv$. Svaku takvu klasu nazivamo **vektorom u ravnini**. Pokaži da je skup V^2 svih vektora ravnine u odnosu na prije definirane operacije zbrajanja vektora i množenja vektora skalarom također vektorski prostor. Slično, i skup V^1 svih **vektora na pravcu** E^1 je vektorski prostor.

5.7. Kolinearni i komplanarni vektori

Za vektore iz V^3 kažemo da su **kolinearni** ako imaju isti smjer. Dogovorom također smatramo da je vektor $\vec{0}$ kolinearan sa svakim vektorom iz V^3. Na primjer, iz definicije množenja vektora skalarom slijedi da su vektori $\vec{a}$ i $\lambda\vec{a}$ uvijek kolinearni za svaki izbor $\lambda \in \mathbb{R}$ i $\vec{a} \in V^3$. Prema tome, ako za vektore $\vec{a}, \vec{b} \in V^3$ vrijedi $\vec{b} = \lambda\vec{a}$, ti su vektori kolinearni. Vrijedi, međutim, ovaj obrat:

PROPOZICIJA 1

Neka su $\vec{a}, \vec{b} \in V^3$ kolinearni vektori i $\vec{a} \neq \vec{0}$. Tada postoji i jednoznačno je određen $\lambda \in \mathbb{R}$ sa svojstvom da je

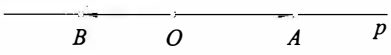
$$\vec{b} = \lambda\vec{a}\,.$$

Dokaz

Neka su $\vec{a} = [\overrightarrow{OA}]$ i $\vec{b} = [\overrightarrow{OB}]$. Onda iz pretpostavke da su $\vec{a}$ i $\vec{b}$ kolinearni vektori zaključujemo da točke O, A i B leže na istom pravcu p. Neka je $k \in \mathbb{R}$ mjerni broj dužine $\overline{OB}$ izmjeren dužinom $\overline{OA}$,

$$k = \frac{\overline{OB}}{\overline{OA}} \geq 0. \tag{1}$$

Primijetimo da je k dobro definiran jer je $A \neq O$ zbog pretpostavke da je $\vec{a} \neq \vec{0}$. Neka je onda $\lambda = k$, odnosno $\lambda = -k$, već prema tome jesu li točke

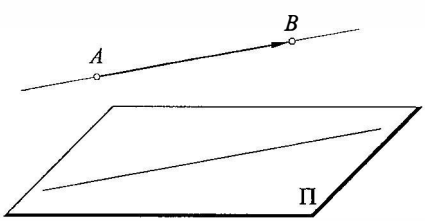


A i B s iste strane ili sa suprotnih strana točke O na pravcu p. Onda je

$$\vec{b} = \lambda\vec{a}\,. \tag{2}$$

Zaista, iz (1) odmah slijedi da su vektori $\vec{b}$ i $\lambda\vec{a}$ istog modula. Nadalje, $\vec{b}$ i $\lambda\vec{a}$ su istog smjera, jer su $\vec{b}$ i $\vec{a}$ istog smjera po pretpostavci. Konačno, kako su vektori $\vec{b}$ i $\vec{a}$ iste orijentacije odnosno suprotnih orijentacija, već prema tome je li $\lambda > 0$ ili $\lambda < 0$, imamo zaključak da su $\vec{b}$ i $\lambda\vec{a}$ uvijek iste orijentacije, pa je tvrdnja (2) provjerena. ■

Kažemo da je **vektor** $\vec{a} = [\overrightarrow{AB}]$ **paralelan s ravninom** $\Pi \subset E^3$ i pišemo



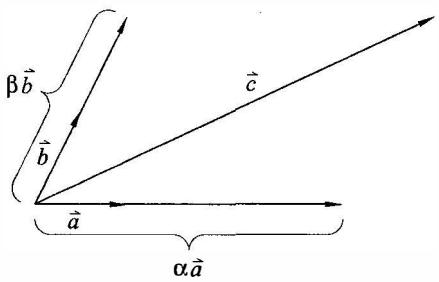
$\vec{a} \parallel \Pi$, ako je pravac AB paralelan s ravninom Π (a to je ako i samo ako je AB paralelan s nekim pravcem u ravnini Π). Očito se radi o dobro definiranom pojmu koji ne ovisi o izboru predstavnika $\overrightarrow{AB}$ vektora $\vec{a}$.

Za vektore iz V^3 koji su paralelni s istom ravninom kažemo da su **komplanarni**. Kolinearni vektori su uvijek i komplanarni. Nadalje, bilo koja dva vektora iz V^3 su komplanarna. Očito je da vrijedi i ova

PROPOZICIJA 2

Neka su $\vec{a}, \vec{b} \in V^3$ bilo koja dva vektora i $\alpha, \beta \in \mathbb{R}$. Neka je $\vec{c} = \alpha\vec{a} + \beta\vec{b}$. Onda su vektori $\vec{a}, \vec{b}, \vec{c}$ komplanarni.

Dokaz



Neposredno iz definicije zbrajanja vektora. ■

Važan je, međutim, ovaj obrat:

TEOREM 3

Neka su $\vec{a}, \vec{b} \in V^3$ nekolinearni vektori, a $\vec{c} \in V^3$ bilo koji vektor s njima komplanaran. Onda postoje i jednoznačno su određeni skalari $\alpha, \beta \in \mathbb{R}$, takvi da je

$$\vec{c} = \alpha\vec{a} + \beta\vec{b}\,.$$

Dokaz

Neka je $O \in E^3$ bilo koja točka i neka je $\vec{a} = [\overrightarrow{OA}]$, $\vec{b} = [\overrightarrow{OB}]$, $\vec{c} = [\overrightarrow{OC}]$. Kako su po pretpostavci vektori $\vec{a}, \vec{b}, \vec{c}$ komplanarni, očito je da točke O, A, B i C leže u istoj ravnini Π. Nadalje, jer $\vec{a}$ i $\vec{b}$ nisu kolinearni, točke O, A, B ne leže na istom pravcu. Neka je

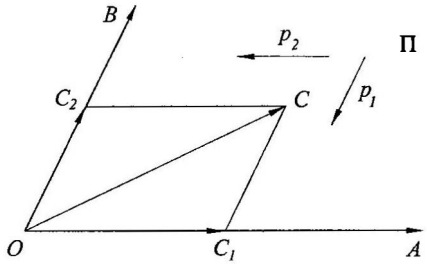
$$p_1 : \Pi \to OA$$

paralelna projekcija ravnine Π na pravac OA u smjeru pravca OB, i analogno

$$p_2 : \Pi \to OB$$

paralelna projekcija ravnine Π na pravac OB u smjeru pravca OA. Neka je $C_1 = p_1(C)$, a $C_2 = p_2(C)$. Tada su vektori $[\overrightarrow{OA}]$ i $[\overrightarrow{OC_1}]$ kolinearni i pritom

je $[\overrightarrow{OA}] = \vec{a} \neq \vec{0}$, jer bi inače $\vec{a}$ i $\vec{b}$ bili kolinearni. Zato prema Prop. 1



postoji $\alpha \in \mathbb{R}$ takav da je

$$[\overrightarrow{OC}_1] = \alpha\,[\overrightarrow{OA}] = \alpha\vec{a}\,.$$

Analogno zaključujemo da postoji $\beta \in \mathbb{R}$ sa svojstvom da je

$$[\overrightarrow{OC}_2] = \beta\,[\overrightarrow{OB}] = \beta\vec{b}\,.$$

No, po konstrukciji je $\overrightarrow{C_1C} \equiv \overrightarrow{OC}_2$, pa imamo

$$\begin{aligned} \vec{c} &= [\overrightarrow{OC}] = [\overrightarrow{OC}_1] + [\overrightarrow{C_1C}] = [\overrightarrow{OC}_1] + [\overrightarrow{OC}_2] = \\ &= \alpha\vec{a} + \beta\vec{b} \end{aligned} \tag{3}$$

kako se i tvrdilo.

Kad bi postojali $\alpha', \beta' \in \mathbb{R}$ tako da je

$$\vec{c} = \alpha'\vec{a} + \beta'\vec{b}, \tag{4}$$

dobili bismo oduzimanjem (4) od (3)

$$(\alpha - \alpha')\vec{a} + (\beta - \beta')\vec{b} = \vec{0}\ . \tag{5}$$

Kad bi bilo $\beta' \neq \beta$, imali bismo

$$\vec{b} = \frac{\alpha - \alpha'}{\beta' - \beta}\,\vec{a}\,,$$

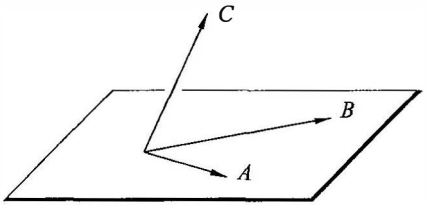
što bi značilo da su vektori $\vec{a}$ i $\vec{b}$ kolinearni, protivno pretpostavci. Zato je $\beta = \beta'$. No, onda je iz (5)

$$(\alpha - \alpha')\vec{a} + 0 \cdot \vec{b} = \vec{0}\,,$$

a kako je $\vec{a} \neq \vec{0}$, to po Prop. 1 iz 5.6. mora biti $\alpha - \alpha' = 0$, dakle $\alpha = \alpha'$, čime je dokazana i jednoznačnost prikaza (3). ■

Evidentno je da se u V^3 uvijek mogu naći tri vektora koja nisu komplanarna. Naime, u aksiomatskom zasnivanju geometrije u E^3 se postulira (a to je i intuitivno jasno) da postoje četiri točke, kažimo O, A, B i C, koje ne leže sve u istoj ravnini. Onda je jasno da vektori generirani orijentiranim

dužinama $\overrightarrow{OA}, \overrightarrow{OB}$ i $\overrightarrow{OC}$ ne mogu biti komplanarni.



Upravo je tim aksiomom utvrđena činjenica da je naš prostor **trodimenzionalan**, točnije, bar trodimenzionalan. Da nije više nego trodimenzionalan dokazuje

TEOREM 4

Neka su $\vec{a}, \vec{b}, \vec{c} \in V^3$ tri nekomplanarna vektora. Ako je $\vec{d} \in V^3$ bilo koji vektor, onda postoje i jednoznačno su određeni skalari $\alpha, \beta, \gamma \in \mathbb{R}$ sa svojstvom da je

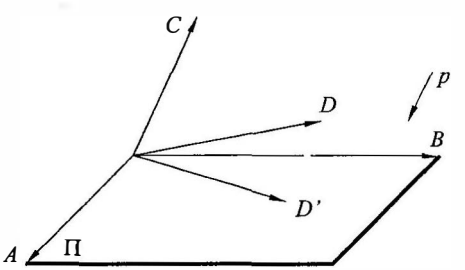
$$\vec{d} = \alpha\vec{a} + \beta\vec{b} + \gamma\vec{c}\,.$$

Dokaz

Neka je $\vec{a} = [\overrightarrow{OA}]$, $\vec{b} = [\overrightarrow{OB}]$, $\vec{c} = [\overrightarrow{OC}]$, $\vec{d} = [\overrightarrow{OD}]$. Kako vektori $\vec{a}, \vec{b}, \vec{c}$ nisu komplanarni, točke O, A, B i C ne leže u istoj ravnini. Zbog toga O, A i B ne leže na istom pravcu, pa određuju neku ravninu, kažimo Π. Neka je

$$p : E^3 \to \Pi$$

paralelna projekcija prostora na ravninu Π, u smjeru pravca OC. Neka je nadalje $D' = p(D)$. Sada su vektori $[\overrightarrow{OD'}]$, $\vec{a}$ i $\vec{b}$ očito komplanarni, a jer su



vektori $\vec{a}$ i $\vec{b}$ nekolinearni, prema Tm. 3 postoje $\alpha, \beta \in \mathbb{R}$, tako da je

$$[\overrightarrow{OD'}] = \alpha\vec{a} + \beta\vec{b}\,.$$

Nadalje, jer je p paralelna projekcija u smjeru OC, vektori $[\overrightarrow{OC}] = \vec{c} \neq \vec{0}$ i $[\overrightarrow{D'D}]$ su očito kolinearni, pa prema Prop. 1 postoji $\gamma \in \mathbb{R}$ takav da je

$$[\overrightarrow{D'D}] = \gamma\vec{c}\,.$$

Po zakonu trokuta je onda

$$[\overrightarrow{OD}] = [\overrightarrow{OD'}] + [\overrightarrow{D'D}] ,$$

dakle

$$\vec{d} = \alpha\vec{a} + \beta\vec{b} + \gamma\vec{c} .$$

Pretpostavimo da postoji i drugi prikaz

$$\vec{d} = \alpha'\vec{a} + \beta'\vec{b} + \gamma'\vec{c} .$$

Tada bismo oduzimanjem dobili

$$(\alpha - \alpha')\vec{a} + (\beta - \beta')\vec{b} + (\gamma - \gamma')\vec{c} = \vec{0} .$$

Kad bi bilo $\gamma \neq \gamma'$, imali bismo

$$\vec{c} = \frac{1}{\gamma' - \gamma} [(\alpha - \alpha')\vec{a} + (\beta - \beta')\vec{b}] ,$$

što bi značilo da su vektori $\vec{a}, \vec{b}$ i $\vec{c}$ komplanarni (Prop. 2), protivno pretpostavci. Dakle je $\gamma = \gamma'$. Slično se vidi da mora biti i $\alpha = \alpha'$ i $\beta = \beta'$ pa je jednoznačnost dokazana. ■

ZADACI

1. Upotrijebi Prop. 1 da elegantno dokažeš tvrdnju (4) u Tm. 2 iz 5.6., u slučaju kad su vektori $\vec{a}$ i $\vec{b}$ kolinearni.

2. Dokaži: Vektori $\vec{a}, \vec{b} \in V^3$ su kolinearni ako i samo ako postoje skalari $\alpha, \beta \in \mathbb{R}$, od kojih je bar jedan različit od nule, takvi da vrijedi

$$\alpha\vec{a} + \beta\vec{b} = \vec{0} .$$

3. Dokaži: Vektori $\vec{a}, \vec{b}, \vec{c} \in V^3$ su komplanarni ako i samo ako postoje $\alpha, \beta, \gamma \in \mathbb{R}$, od kojih je bar jedan različit od nule, takvi da vrijedi

$$\alpha\vec{a} + \beta\vec{b} + \gamma\vec{c} = \vec{0} .$$

4. Dokaži: Za četiri vektora $\vec{a}, \vec{b}, \vec{c}, \vec{d} \in V^3$ uvijek postoji izbor skalara $\alpha, \beta, \gamma, \delta \in \mathbb{R}$, takav da je bar jedan od njih različit od nule, i da vrijedi

$$\alpha\vec{a} + \beta\vec{b} + \gamma\vec{c} + \delta\vec{d} = \vec{0} .$$

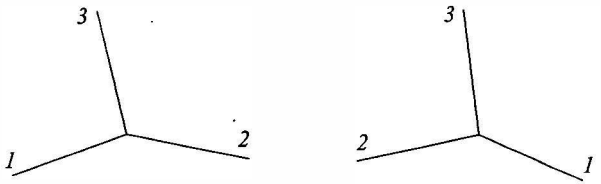
5.8. Baza prostora V^3. Koordinatizacija

Svaku uređenu trojku

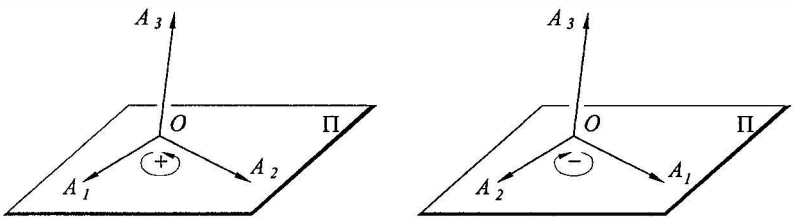
$$B = (\vec{a}_1, \vec{a}_2, \vec{a}_3) \tag{1}$$

nekomplanarnih vektora iz V^3 nazivamo **baza** prostora V^3. Govori se također o **koordinatnoj bazi** ili **koordinatnom sustavu** za V^3. Vektore $\vec{a}_i$ iz baze zovemo **koordinatni vektori**.

Najprije nešto o pojmu orijentacije baze. Intuitivno je jasno da, s obzirom na relativni položaj koordinatnih vektora, imamo samo dva bitno različita tipa koordinatnih baza.



Taj se fenomen može i precizno definirati. Neka je $B = (\vec{a}_1, \vec{a}_2, \vec{a}_3)$ bilo koja koordinatna baza za V^3, a $\overrightarrow{OA}_1, \overrightarrow{OA}_2, \overrightarrow{OA}_3$ neka su predstavnici vektora baze s istim početkom. Neka je, nadalje, s Π označena ravnina, jednoznačno određena točkama O, A_1 i A_2. Ta ravnina dijeli prostor u dva potprostora. Promatrajmo trokut OA_1A_2 u ravnini Π. Kažemo da je baza B **desno orijentirana** ili **desna**, ako je trokut OA_1A_2, gledan iz potprostora koji sadrži



desna *lijeva*

točku A_3, pozitivno orijentiran (tj. njegov je obilazak u danom poretku vrhova protivan gibanju kazaljke na satu). Baza B je **lijevo orijentirana** ili **lijeva**, ako je, gledano iz potprostora u kojemu je točka A_3, trokut OA_1A_2 negativno orijentiran (tj. njegov se obilazak u danom poretku vrhova podudara s gibanjem kazaljke na satu). Očito je kako se radi o dobro definiranim pojmovima, neovisnim o izboru reprezentanata koordinatnih vektora. Naziv desna (lijeva) baza je uveden zato što se lako može provjeriti da su vektori u takvoj bazi u istom relativnom položaju kao ispruženi palac, ispruženi kažiprst i savinuti srednji prst desne (lijeve) ruke.

Osnovno svojstvo baze dokazano je u Tm. 4 iz 5.7., a sastoji se u tome da **svaki** vektor $\vec{a} \in V^3$ ima **jedinstveni prikaz** oblika

$$\vec{a} = \alpha_1\vec{a}_1 + \alpha_2\vec{a}_2 + \alpha_3\vec{a}_3, \tag{2}$$

tj. kao linearna kombinacija triju vektora iz baze. Upravo zbog tog svojstva smatramo da je prostor V^3 **trodimenzionalan.**

Kako je prikaz (2) jednoznačan, putem koordinatne baze dolazimo do preslikavanja

$$k : V^3 \to \mathbb{R}^3$$

definiranog s

$$k(\vec{a}) = k(\alpha_1\vec{a}_1 + \alpha_2\vec{a}_2 + \alpha_3\vec{a}_3) = (\alpha_1, \alpha_2, \alpha_3)\ ,$$

koje nazivamo **koordinatizacija** prostora V^3 (u odnosu na bazu B).

PROPOZICIJA 1

Preslikavanje k je bijekcija.

Dokaz

Trivijalan. ■

Prema tome, vektori su karakterizirani trojkama realnih brojeva. Ako je

$$k(\vec{a}) = (\alpha_1, \alpha_2, \alpha_3)\ ,$$

brojeve $\alpha_1, \alpha_2, \alpha_3$ zovemo **koordinate** vektora $\vec{a}$ u odnosu na danu bazu (1), a uređenu trojku $(\alpha_1, \alpha_2, \alpha_3)$ **koordinatna trojka** ili **koordinatni slog** tog vektora. Kako je k bijekcija, obično identificiramo vektor s njegovim koordinatnim slogom i pišemo jednostavno

$$\vec{a} = (\alpha_1, \alpha_2, \alpha_3)\ .$$

Spomenimo još da se katkada (posebno u fizici) jednoznačno određeni vektori $\alpha_1\vec{a}_1, \alpha_2\vec{a}_2, \alpha_3\vec{a}_3$ u prikazu (2) nazivaju **komponentama** vektora $\vec{a}$ u smjerovima koordinatnih vektora.

Navedimo sada nekoliko posljedica postojanja koordinatizacije.

PROPOZICIJA 2

Neka su $\vec{a} = (\alpha_1, \alpha_2, \alpha_3)$ i $\vec{b} = (\beta_1, \beta_2, \beta_3)$ vektori iz V^3, dani svojim koordinatama u danoj bazi. Onda je u toj bazi

$$\vec{a} + \vec{b} = (\alpha_1 + \beta_1, \alpha_2 + \beta_2, \alpha_3 + \beta_3)\ .$$

Dokaz

Imamo

$$\begin{aligned}\vec{a}+\vec{b} &= (\alpha_1\vec{a}_1+\alpha_2\vec{a}_2+\alpha_3\vec{a}_3)+(\beta_1\vec{a}_1+\beta_2\vec{a}_2+\beta_3\vec{a}_3)\\ &= (\alpha_1+\beta_1)\vec{a}_1+(\alpha_2+\beta_2)\vec{a}_2+(\alpha_3+\beta_3)\vec{a}_3\end{aligned}$$

pa je zaista

$$\vec{a}+\vec{b}=(\alpha_1+\beta_1,\alpha_2+\beta_2,\alpha_3+\beta_3).$$

■

Slično se vidi da vrijedi

PROPOZICIJA 3

Neka je $\vec{a}=(\alpha_1,\alpha_2,\alpha_3)$ *bilo koji vektor iz* V^3, *a* $\lambda\in\mathbb{R}$ *po volji odabran skalar. Onda je*

$$\lambda\vec{a}=(\lambda\alpha_1,\lambda\alpha_2,\lambda\alpha_3)\,.$$

Specijalno je, dakle,

$$-\vec{a}=(-\alpha_1,-\alpha_2,-\alpha_3)\,.$$

■

PROPOZICIJA 4

Neka su $\vec{a}=(\alpha_1,\alpha_2,\alpha_3)$ *i* $\vec{b}=(\beta_1,\beta_2,\beta_3)$ *vektori iz* V^3, *različiti od nulvektora. Ti su vektori kolinearni ako i samo ako su im koordinate proporcionalne, tj. vrijedi*

$$\alpha_1:\alpha_2:\alpha_3=\beta_1:\beta_2:\beta_3\,.$$

Dokaz

Ako su $\vec{a}$ i $\vec{b}$ kolinearni, prema Prop. 1 u 5.7., postoji $\lambda\in\mathbb{R}$ takav da je $\vec{b}=\lambda\vec{a}$. Onda je zbog Prop. 3

$$(\beta_1,\beta_2,\beta_3)=(\lambda\alpha_1,\lambda\alpha_2,\lambda\alpha_3)\,,$$

dakle

$$\beta_i=\lambda\alpha_i\,,$$

za $i=1,2,3$, pa je proporcionalnost koordinata dokazana. Slično se vidi obrat. ■

ZADACI

1. Svaki uređeni par $(\vec{a}_1,\vec{a}_2)$ nekolinearnih vektora iz V^2 nazivamo **baza prostora** V^2. Definiraj koordinatizaciju za V^2 i ispitaj njezina svojstva. Svaki vektor $\vec{a}\neq\vec{0}$ iz V^1 je **baza** za V^1.

2. Pokaži da, uz koordinatno zbrajanje i množenje skalarom, i $\mathbb{R}^3$ postaje vektorski prostor. Pritom bijekcija k ima svojstva

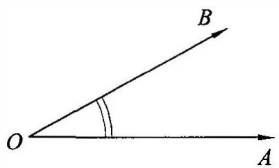
$$k(\vec{a}+\vec{b}) = k(\vec{a}) + k(\vec{b}) \quad \text{i} \quad k(\lambda\vec{a}) = \lambda k(\vec{a}) ,$$

tj. čuva operacije, pa za nju kažemo da je **izomorfizam vektorskih prostora** V^3 i $\mathbb{R}^3$.

3. Ako je koordinatna baza $(\vec{a}_1, \vec{a}_2, \vec{a}_3)$ desna, onda su baze $(\vec{a}_2, \vec{a}_3, \vec{a}_1)$ i $(\vec{a}_3, \vec{a}_1, \vec{a}_2)$ desne, dok su baze $(\vec{a}_2, \vec{a}_1, \vec{a}_3)$, $(\vec{a}_1, \vec{a}_3, \vec{a}_2)$ i $(\vec{a}_3, \vec{a}_2, \vec{a}_1)$ lijeve. Dokaži.

5.9. Skalarni produkt

Neka su $\vec{a} \neq \vec{0}$ i $\vec{b} \neq \vec{0}$ bilo koja dva vektora iz V^3. Neka je $\vec{a} = [\overrightarrow{OA}]$, $\vec{b} = [\overrightarrow{OB}]$. Onda **kut** $\sphericalangle(\vec{a}, \vec{b})$ (točnije bi bilo reći mjerni broj kuta) tih vektora definiramo kao mjerni broj neorijentiranog kuta $\sphericalangle AOB$, koji pada u interval $[0, \pi]$. Ako je bar jedan od vektora $\vec{a}$ i $\vec{b}$ nulvektor, pojam kuta se ne definira. Lako se vidi da je kut dvaju vektora dobro definiran pojam, tj. da ne ovisi o izboru predstavnika (kutovi s paralelnim kracima!).



Nadalje, iz definicije odmah slijedi da je

$$\sphericalangle(\vec{a}, \vec{b}) = \sphericalangle(\vec{b}, \vec{a}) .$$

Ako je $\sphericalangle(\vec{a}, \vec{b}) = \pi/2$, kažemo da su vektori $\vec{a}$ i $\vec{b}$ **okomiti** i pišemo $\vec{a} \perp \vec{b}$. Nadalje, jasno je da će vektori $\vec{a}$ i $\vec{b}$ biti kolinearni onda i samo onda kad je $\sphericalangle(\vec{a}, \vec{b}) = 0$ (vektori iste orijentacije) ili $\sphericalangle(\vec{a}, \vec{b}) = \pi$ (vektori suprotnih



orijentacija).

Sada ćemo u V^3 definirati jednu novu operaciju, koju zovemo skalarni produkt vektora. Neka je

$$u : V^3 \times V^3 \to \mathbb{R}$$

preslikavanje, definirano na ovaj način:

(1) ako je bar jedan od vektora $\vec{a}$ i $\vec{b}$ nulvektor, onda je

$$u(\vec{a}, \vec{b}) = 0 ;$$

(2) ako je $\vec{a} \neq \vec{0}, \vec{b} \neq \vec{0}$, onda je

$$u(\vec{a}, \vec{b}) = |\vec{a}| \cdot |\vec{b}| \cdot \cos \sphericalangle(\vec{a}, \vec{b}).$$

Preslikavanje u zovemo **skalarnim množenjem** u prostoru V^3, a vrijednost $u(\vec{a}, \vec{b}) \in \mathbb{R}$ **skalarnim produktom** vektora $\vec{a}$ i $\vec{b}$. Obično pišemo

$$u(\vec{a}, \vec{b}) = \vec{a} \cdot \vec{b} = \vec{a}\,\vec{b}$$

i također kraće $\cos \sphericalangle(\vec{a}, \vec{b}) = \cos(\vec{a}, \vec{b})$.

Pomoću skalarnog produkta možemo jednostavno karakterizirati okomitost dvaju vektora. Vrijedi

PROPOZICIJA 1

Neka su $\vec{a} \neq \vec{0}$ i $\vec{b} \neq \vec{0}$ bilo koji vektori iz V^3. Ti su vektori okomiti ako i samo ako je $\vec{a} \cdot \vec{b} = 0$.

Dokaz

Neka je $\vec{a} \perp \vec{b}$. Onda je $\sphericalangle(\vec{a}, \vec{b}) = \pi/2$, pa imamo

$$\vec{a} \cdot \vec{b} = |\vec{a}| \cdot |\vec{b}| \cos \frac{\pi}{2} = 0 .$$

Obratno, neka je $\vec{a} \cdot \vec{b} = 0$. Onda je

$$|\vec{a}||\vec{b}| \cdot \cos(\vec{a}, \vec{b}) = 0 ,$$

a kako je $\vec{a} \neq \vec{0}$ i $\vec{b} \neq \vec{0}$, to je $\cos(\vec{a}, \vec{b}) = 0$. No, u intervalu $[0, \pi]$ je kut $\sphericalangle(\vec{a}, \vec{b}) = \pi/2$ jedini kut s tim svojstvom pa je $\vec{a} \perp \vec{b}$. ■

Primijetimo da iz definicije neposredno slijedi da je za svaki $\vec{a} \in V^3$

$$\vec{a} \cdot \vec{a} = |\vec{a}|^2 \geq 0 ,$$

tj. **skalarni kvadrat** vektora je jednak kvadratu modula tog vektora i zato nenegativan. Pišemo kraće $\vec{a} \cdot \vec{a} = \vec{a}^2$. Slično se vidi da je $(-\vec{a})\vec{a} = -|\vec{a}|^2$. Slijedi

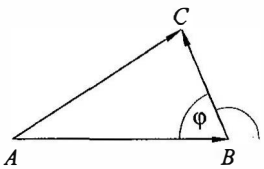
PROPOZICIJA 2

Za svaki je izbor $\vec{a}, \vec{b} \in V^3$

$$\begin{aligned} (\vec{a} + \vec{b})^2 &= \vec{a}^2 + \vec{b}^2 + 2\vec{a}\vec{b} \quad i \\ (\vec{a} - \vec{b})^2 &= \vec{a}^2 + \vec{b}^2 - 2\vec{a}\vec{b} . \end{aligned}$$

Dokaz

Dokažimo npr. prvu tvrdnju. Pretpostavimo da vektori $\vec{a}$ i $\vec{b}$ nisu kolinearni. Neka je $\vec{a} = [\overrightarrow{AB}]$ i $\vec{b} = [\overrightarrow{BC}]$. Onda je $\vec{c} = \vec{a} + \vec{b} = [\overrightarrow{AC}]$.



Promatrajmo trokut ABC i primijenimo kosinusov poučak. Imamo (vidi sliku)

$$\begin{aligned}(\vec{a}+\vec{b})^2 &= \vec{c}^2 = |\vec{c}|^2 = |\vec{a}|^2 + |\vec{b}|^2 - 2|\vec{a}||\vec{b}|\cos\varphi \\ &= |\vec{a}^2| + |\vec{b}^2| + 2|\vec{a}||\vec{b}|\cos(\vec{a},\vec{b}) = \vec{a}^2 + \vec{b}^2 + 2\vec{a}\vec{b}\,.\end{aligned}$$

Tvrdnja se lako provjeri i kad su $\vec{a}$ i $\vec{b}$ kolinearni. ■

Daljnja svojstva skalarnog produkta sabrana su u sljedećem teoremu:

TEOREM 3

Skalarno množenje vektora ima ova osnovna svojstva:

(1) *komutativnost, tj.*

$$\vec{a}\vec{b} = \vec{b}\vec{a} \quad ,\forall\, \vec{a},\vec{b} \in V^3\,;$$

(2) *kvaziasocijativnost, tj.*

$$(\lambda\vec{a})\vec{b} = \lambda(\vec{a}\vec{b}) \quad ,\forall\, \lambda \in \mathbb{R},\ \vec{a},\vec{b} \in V^3\,;$$

(3) *distributivnost prema zbrajanju, tj.*

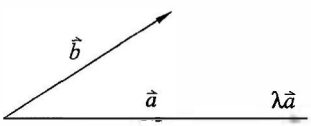
$$\vec{a}(\vec{b}+\vec{c}) = \vec{a}\vec{b} + \vec{a}\vec{c} \quad ,\forall\, \vec{a},\vec{b},\vec{c} \in V^3\,;$$

(4) *pozitivnu definitnost, tj.* $\vec{a}^2 \geq 0$; $\vec{a}^2 = 0$ *ako i samo ako je* $\vec{a} = \vec{0}$.

Dokaz

(1) Neposredno iz definicije množenja.

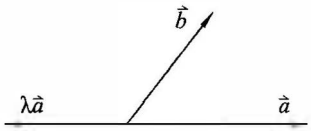
(2) Ako je $\lambda = 0$ ili je $\vec{a} = \vec{0}$ odnosno $\vec{b} = \vec{0}$, tvrdnja je trivijalna.



Uzmimo zato da je $\lambda \neq 0$ i $\vec{a} \neq \vec{0}$, $\vec{b} \neq \vec{0}$. Ako je $\lambda > 0$, onda je $|\lambda\vec{a}| = \lambda|\vec{a}|$ i $\sphericalangle(\lambda\vec{a}, \vec{b}) = \sphericalangle(\vec{a}, \vec{b})$, pa imamo redom

$$(\lambda\vec{a})\vec{b} = |\lambda\vec{a}| \cdot |\vec{b}| \cdot \cos(\lambda\vec{a}, \vec{b}) = \lambda|\vec{a}| \cdot |\vec{b}| \cdot \cos(\vec{a}, \vec{b}) = \lambda(\vec{a}\vec{b}) \,.$$

Ako je pak $\lambda < 0$, onda je $|\lambda\vec{a}| = -\lambda|\vec{a}|$ i nadalje $\sphericalangle(\lambda\vec{a}, \vec{b}) = \pi - \sphericalangle(\vec{a}, \vec{b})$,



pa je

$$\begin{aligned}(\lambda\vec{a})\vec{b} &= |\lambda\vec{a}| \cdot |\vec{b}| \cos(\lambda\vec{a}, \vec{b}) = -\lambda|\vec{a}| \cdot |\vec{b}| \cdot \cos(\pi - \sphericalangle(\vec{a}, \vec{b})) \\ &= \lambda|\vec{a}| \cdot |\vec{b}| \cdot \cos(\vec{a}, \vec{b}) = \lambda(\vec{a}\vec{b})\end{aligned}$$

i tvrdnja je dokazana.

(3) Dokaz je formalne prirode i oslanja se samo na višekratnu primjenu Prop. 2. Imamo redom

$$\begin{aligned}4\vec{a}(\vec{b}+\vec{c}) &= [2\vec{a} + (\vec{b}+\vec{c})]^2 - 4\vec{a}^2 - (\vec{b}+\vec{c})^2 = \\ &= [2\vec{a} + (\vec{b}+\vec{c})]^2 - 4\vec{a}^2 + (\vec{b}-\vec{c})^2 - 2\vec{b}^2 - 2\vec{c}^2 = \\ &= [(\vec{a}+\vec{b}) + (\vec{a}+\vec{c})]^2 + [(\vec{a}+\vec{b}) - (\vec{a}+\vec{c})]^2 - 4\vec{a}^2 - 2\vec{b}^2 - 2\vec{c}^2 = \\ &= 2(\vec{a}+\vec{b})^2 + 2(\vec{a}+\vec{c})^2 - 4\vec{a}^2 - 2\vec{b}^2 - 2\vec{c}^2 = \\ &= 4\vec{a}^2 + 4\vec{a}\vec{b} + 4\vec{a}\vec{c} + 2\vec{b}^2 + 2\vec{c}^2 - 4\vec{a}^2 - 2\vec{b}^2 - 2\vec{c}^2 = \\ &= 4\vec{a}\vec{b} + 4\vec{a}\vec{c} = 4(\vec{a}\vec{b} + \vec{a}\vec{c})\end{aligned}$$

pa dijeljenjem s 4 zaista dobivamo

$$\vec{a}(\vec{b}+\vec{c}) = \vec{a}\vec{b} + \vec{a}\vec{c} \,.$$

(4) Trivijalno. ■

KOROLAR 4

Za skalarno množenje također vrijedi

(5) $\vec{a}(\lambda\vec{b}) = \lambda(\vec{a}\vec{b}) \quad , \forall\, \lambda \in \mathbb{R},\ \forall\, \vec{a}, \vec{b} \in V^3$;

(6) $(\vec{a}+\vec{b})\vec{c} = \vec{a}\vec{c} + \vec{b}\vec{c} \quad , \forall\, \vec{a}, \vec{b}, \vec{c} \in V^3$.

Dokaz

Iz tvrdnji (1) i (2) Tm. 3 imamo

$$\vec{a}(\lambda\vec{b}) = (\lambda\vec{b})\vec{a} = \lambda(\vec{b}\vec{a}) = \lambda(\vec{a}\vec{b})$$

pa je tvrdnja (5) verificirana. Slično se vidi tvrdnja (6). ■

Spomenimo na kraju i ovo: Ako u nekom linearnom prostoru nad poljem $\mathbb{R}$ definiramo množenje vektora s vrijednostima u tom polju (tzv. skalarno množenje), pa ako to množenje ima svojstva (1)–(4) iz Tm. 3, onda takvu strukturu zovemo (realni) **unitarni prostor**. Prema tome, dokazali smo upravo ovaj

TEOREM 5

Vektorski prostor V^3 je uz skalarno množenje vektora realni unitarni prostor. ■

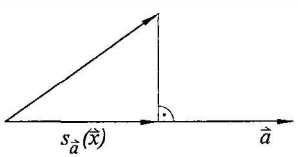
ZADACI

1. Pri skalarnom množenju nema smisla govoriti o asocijativnosti. Zašto? Uvjeri se, nadalje, da za skalarno množenje ne vrijedi pravilo "skraćivanja", tj. $\vec{a}\vec{c} = \vec{b}\vec{c}$ ne povlači općenito $\vec{a} = \vec{b}$.

2. Neka je $\vec{a} \neq \vec{0}$ bilo koji vektor. Onda za svaki vektor $\vec{x} \in V^3$ definiramo skalar

$$s_{\vec{a}}(\vec{x}) = |\vec{x}| \cdot \cos(\vec{a}, \vec{x})$$

koji nazivamo **skalarna projekcija** ili koordinata vektora $\vec{x}$ u smjeru



vektora $\vec{a}$. Dokaži da je funkcija $s_{\vec{a}}$ aditivna, tj. da je

$$s_{\vec{a}}(\vec{x} + \vec{y}) = s_{\vec{a}}(\vec{x}) + s_{\vec{a}}(\vec{y}) \, .$$

3. Odmah se vidi da je $\vec{a}\vec{b} = |\vec{a}| s_{\vec{a}}(\vec{b}) = |\vec{b}| s_{\vec{b}}(\vec{a})$. Iskoristi tu činjenicu i aditivnost funkcije s za jednostavni dokaz tvrdnje (3) u Tm. 3, tj. distributivnosti skalarnog množenja prema zbrajanju.

4. Uvjeri se da i prostor V^2 dopušta strukturu unitarnog prostora. A prostor V^1?

5.10. Ortonormirana baza. Koordinatni prikaz skalarnog produkta

Neka je $B = (\vec{i}, \vec{j}, \vec{k})$ koordinatna baza u V^3 sa svojstvom da za koordinatne vektore vrijedi

$$|\vec{i}| = |\vec{j}| = |\vec{k}| = 1$$

i

$$\vec{j} \perp \vec{k}, \quad \vec{k} \perp \vec{i}, \quad \vec{i} \perp \vec{j},$$

tj. da su ti vektori jedinični i u parovima okomiti. Onda kažemo da je B jedna **ortonormirana baza** za prostor V^3. Nije se teško uvjeriti da u V^3 ima takvih baza.

Koordinate vektora u odnosu na ortonormiranu bazu nazivamo **ortogonalne** ili **pravokutne koordinate**.

Pogledajmo sada, kako se može izraziti skalarni produkt dvaju vektora uz pomoć pravokutnih koordinata tih vektora.

Prije svega, iz definicije odmah slijedi da za koordinatne vektore neke ortonormirane baze vrijedi ova tablica skalarnih produkata

$\cdot$	$\vec{i}$	$\vec{j}$	$\vec{k}$
$\vec{i}$	1	0	0
$\vec{j}$	0	1	0
$\vec{k}$	0	0	1

jer je npr. $\vec{i} \cdot \vec{i} = |\vec{i}|^2 = 1$, $\vec{i} \cdot \vec{j} = |\vec{i}||\vec{j}| \cos \pi/2 = 0$.

PROPOZICIJA 1

Neka su $\vec{a} = (\alpha_1, \alpha_2, \alpha_3)$ *i* $\vec{b} = (\beta_1, \beta_2, \beta_3)$ *bilo koji vektori iz* V^3, *dani svojim pravokutnim koordinatama. Onda je*

$$\vec{a}\vec{b} = \alpha_1\beta_1 + \alpha_2\beta_2 + \alpha_3\beta_3 \, .$$

Dokaz

Iz tablice za koordinatne vektore i svojstava skalarnog množenja navedenih u 5.9. imamo

$$\begin{aligned} \vec{a}\vec{b} &= (\alpha_1\vec{i} + \alpha_2\vec{j} + \alpha_3\vec{k})(\beta_1\vec{i} + \beta_2\vec{j} + \beta_3\vec{k}) = \\ &= \alpha_1\beta_1\vec{i}^{\,2} + \alpha_1\beta_2\,\vec{i}\,\vec{j} + \alpha_1\beta_3\vec{i}\,\vec{k} + \alpha_2\beta_1\,\vec{j}\,\vec{i} + \\ &+ \alpha_2\beta_2\,\vec{j}^{\,2} + \alpha_2\beta_3\,\vec{j}\,\vec{k} + \alpha_3\beta_1\,\vec{k}\,\vec{i} + \alpha_3\beta_2\,\vec{k}\,\vec{j} + \alpha_3\beta_3\,\vec{k}^{\,2} = \\ &= \alpha_1\beta_1 + \alpha_2\beta_2 + \alpha_3\beta_3 \, . \end{aligned}$$

■

Koja su sve svojstva skalarnog produkta upotrijebljena u dokazu?

KOROLAR 2

Neka je $\vec{a} = (\alpha_1, \alpha_2, \alpha_3)$ *bilo koji vektor. Onda je njegov modul dan sa*

$$|\vec{a}| = \sqrt{\alpha_1^2 + \alpha_2^2 + \alpha_3^2} \ ,$$

gdje treba uzeti pozitivnu determinaciju drugog korijena.

Dokaz

Neposredno iz Prop. 1. Imamo naime

$$|\vec{a}|^2 = \vec{a}^2 = \vec{a} \cdot \vec{a} = \alpha_1^2 + \alpha_2^2 + \alpha_3^3 \ ,$$

odakle slijedi tvrdnja. ■

KOROLAR 3

Neka su $\vec{a} = (\alpha_1, \alpha_2, \alpha_3)$ *i* $\vec{b} = (\beta_1, \beta_2, \beta_3)$ *bilo koji vektori iz* V^3*, različiti od nulvektora. Onda je kut tih vektora dan formulom*

$$\cos(\vec{a}, \vec{b}) = \frac{\alpha_1\beta_1 + \alpha_2\beta_2 + \alpha_3\beta_3}{\sqrt{\alpha_1^2 + \alpha_2^2 + \alpha_3^2} \cdot \sqrt{\beta_1^2 + \beta_2^2 + \beta_3^2}} \ .$$

Dokaz

Iz definicije skalarnog produkta imamo

$$\cos(\vec{a}, \vec{b}) = \frac{\vec{a} \cdot \vec{b}}{|\vec{a}| \cdot |\vec{b}|}$$

pa tvrdnju dobivamo primjenom Prop. 1. i Kor. 2. ■

Iz gornje formule neposredno čitamo uvjet za okomitost dvaju vektora.

KOROLAR 4

Vektori $\vec{a}$ *i* $\vec{b}$ *su okomiti onda i samo onda ako za njihove koordinate vrijedi*

$$\alpha_1\beta_1 + \alpha_2\beta_2 + \alpha_3\beta_3 = 0 \ .$$ ■

Vratimo se formuli za kut dvaju vektora. Od posebnog je interesa slučaj kad je jedan od tih vektora koordinatni vektor. Ako je, npr. $\vec{b} = \vec{\imath}$, onda je $\beta_1 = 1, \beta_2 = \beta_3 = 0$, pa iz Kor. 3 slijedi, uz oznaku $\sphericalangle(\vec{a}, \vec{\imath}) = \varphi_1$,

$$\cos\varphi_1 = \frac{\alpha_1}{\sqrt{\alpha_1^2 + \alpha_2^2 + \alpha_3^2}} = \frac{\alpha_1}{|\vec{a}|} \ .$$

Analogno bi odredili kutove $\varphi_2 = \sphericalangle(\vec{a}, \vec{j})$ i $\varphi_3 = \sphericalangle(\vec{a}, \vec{k})$ vektora $\vec{a}$ s ostalim koordinatnim vektorima. Skalare

$$\cos\varphi_1 = \frac{\alpha_1}{|\vec{a}|}\,, \quad \cos\varphi_2 = \frac{\alpha_2}{|\vec{a}|}\,, \quad \cos\varphi_3 = \frac{\alpha_3}{|\vec{a}|}$$

nazivamo **kosinusi smjera** vektora $\vec{a}$, jer je njima određen smjer tog vektora u prostoru.

Kosinusi smjera nisu, međutim, neovisni. Vrijedi

PROPOZICIJA 5

Za kosinuse smjera bilo kojeg vektora $\vec{a}$ vrijedi

$$\cos^2\varphi_1 + \cos^2\varphi_2 + \cos^2\varphi_3 = 1$$

Dokaz

Relacija se dobiva kvadriranjem i zbrajanjem kosinusa smjera i primjenom Kor. 2. ■

Ako je $\vec{a}$ specijalno jedinični vektor, $|\vec{a}| = 1$, imamo

$$\cos\varphi_1 = \alpha_1,\ \cos\varphi_2 = \alpha_2,\ \cos\varphi_3 = \alpha_3\ ,$$

tj. pravokutne koordinate jediničnog vektora podudaraju se s kosinusima smjera tog vektora. Zato vrijedi (vidi Zad. 2. u 5.6.)

PROPOZICIJA 6

Kosinusi smjera vektora $\vec{a} \in V^3$ jednaki su pravokutnim koordinatama jediničnog vektora $\vec{a}_0$ u smjeru tog vektora. ■

ZADACI

1. Dokaži: Za bilo koji izbor $\alpha_1, \alpha_2, \alpha_3, \beta_1, \beta_2, \beta_3 \in \mathbb{R}$ realnih brojeva vrijedi

$$(\alpha_1\beta_1 + \alpha_2\beta_2 + \alpha_3\beta_3)^2 \leq (\alpha_1^2 + \alpha_2^2 + \alpha_3^2)(\beta_1^2 + \beta_2^2 + \beta_3^2)$$

i to je tzv. **nejednakost Schwarz-Cauchy-Bunjakovskog** . Kada vrijedi znak jednakosti? [Uputa: Interpretiraj $(\alpha_1, \alpha_2, \alpha_3)$ i $(\beta_1, \beta_2, \beta_3)$ kao koordinate vektora, pa primijeni Kor. 3.]

2. Za bilo koji izbor $\alpha_1, \alpha_2, \alpha_3, \beta_1, \beta_2, \beta_3 \in \mathbb{R}$ vrijedi nejednakost

$$\sqrt{(\alpha_1 + \beta_1)^2 + (\alpha_2 + \beta_2)^2 + (\alpha_3 + \beta_3)^2} \leq$$
$$\leq \sqrt{\alpha_1^2 + \alpha_2^2 + \alpha_3^2} + \sqrt{\beta_1^2 + \beta_2^2 + \beta_3^2}$$

i to je tzv. **nejednakost trokuta**.

3. Pokaži da je površina paralelograma određenog vektorima $\vec{a}$ i $\vec{b}$ dana formulom

$$P = \sqrt{\vec{a}^2 \cdot \vec{b}^2 - (\vec{a}\vec{b})^2}\,.$$

Pomoću te formule izvedi Heronovu formulu za površinu trokuta.

5.11. Vektorski produkt

Definirat ćemo još jedno množenje vektora, i to takvo da je (za razliku od skalarnog množenja) rezultat množenja opet vektor. Radi se o tzv. vektorskom množenju koje je posebnost prostora V^3, jer nema svog analogona u V^2, niti prikladne generalizacije u višim dimenzijama. Neka je

$$v : V^3 \times V^3 \to V^3$$

preslikavanje pri kojem je za svaki izbor $\vec{a}, \vec{b} \in V^3$ vektor $v(\vec{a}, \vec{b}) = \vec{c}$ definiran na ovaj način:

(1) ako su $\vec{a}$ i $\vec{b}$ kolinearni, onda je $\vec{c} = \vec{0}$;

(2) ako $\vec{a}$ i $\vec{b}$ nisu kolinearni, onda je

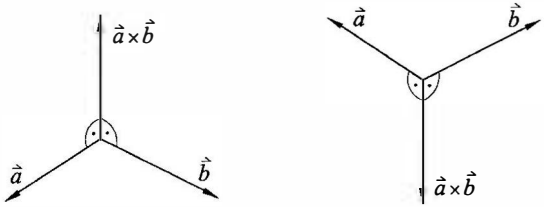
(a) modul od $\vec{c}$ dan sa $|\vec{c}| = |\vec{a}| \cdot |\vec{b}| \cdot \sin(\vec{a}, \vec{b})$,

(b) smjer od $\vec{c}$ propisan zahtjevom $s_{\vec{c}} \perp s_{\vec{a}}$ i $s_{\vec{c}} \perp s_{\vec{b}}$,

(c) orijentacija od $\vec{c}$ takva da uređena trojka $(\vec{a}, \vec{b}, \vec{c})$ predstavlja jednu desnu bazu u V^3 (vidi 5.8.).

Ovim je vektor $\vec{c}$ određen jednoznačno (Prop. 1 u 5.4.).

Onda preslikavanje v nazivamo **vektorsko množenje**, a sliku $v(\vec{a}, \vec{b}) \in V^3$



vektorskim produktom vektora $\vec{a}$ i $\vec{b}$. Pišemo kraće

$$v(\vec{a}, \vec{b}) = \vec{a} \times \vec{b}\,.$$

Popularno se još kaže da orijentacija vektorskog produkta poštuje **pravilo desnog vijka**, tj. dana je smislom napredovanja vijka pri njegovou zakretanju od prvog faktora prema drugom, najkraćim putem.

Evo nekoliko neposrednih posljedica definicije vektorskog produkta.

PROPOZICIJA 1

Vektorsko množenje je antikomutativno, tj. vrijedi

$$\vec{b} \times \vec{a} = -(\vec{a} \times \vec{b}) ,$$

za sve $\vec{a}, \vec{b} \in V^3$.

Dokaz

Neposredno iz definicije. ■

PROPOZICIJA 2

$\vec{a} \times \vec{b} = \vec{0}$ *onda i samo onda ako su vektori* $\vec{a}$ *i* $\vec{b}$ *kolinearni.*

Dokaz

Ako su $\vec{a}$ i $\vec{b}$ kolinearni, $\vec{a} \times \vec{b} = \vec{0}$ po definiciji. Obratno, neka je $\vec{a} \times \vec{b} = \vec{0}$. Pretpostavimo da $\vec{a}$ i $\vec{b}$ nisu kolinearni. Onda bismo prema (2) imali

$$|\vec{a} \times \vec{b}| = |\vec{a}| \cdot |\vec{b}| \cdot \sin(\vec{a}, \vec{b}) = 0 ,$$

tj. ili $\vec{a} = \vec{0}$ ili $\vec{b} = \vec{0}$ ili $\sphericalangle(\vec{a}, \vec{b}) \in \{0, \pi\}$, dakle u svakom bi slučaju $\vec{a}$ i $\vec{b}$ bili kolinearni, protivno pretpostavci. ■

Zapišimo posebno sljedeću propoziciju.

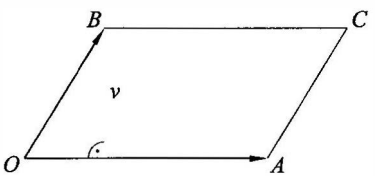
PROPOZICIJA 3

Za svaki je vektor $\vec{a} \in V^3$

$$\vec{a} \times \vec{a} = \vec{0} .$$

■

Pretpostavimo sada da vektori $\vec{a}$ i $\vec{b}$ nisu kolinearni. Neka je $\vec{a} = [\overrightarrow{OA}]$ i $\vec{b} = [\overrightarrow{OB}]$. Onda točke O, A, B ne leže na istom pravcu i prema tome



određuju jedan paralelogram, kažimo $OACB$.

PROPOZICIJA 4

Ako vektori $\vec{a}$ *i* $\vec{b}$ *nisu kolinearni,* $|\vec{a} \times \vec{b}|$ *je jednak površini paralelograma* $OACB$.

Dokaz

Imamo

$$P = \text{baza} \times \text{visina} = |\vec{a}| \cdot v = |\vec{a}||\vec{b}| \sin(\vec{a}, \vec{b}) = |\vec{a} \times \vec{b}|$$

i dokaz je gotov. ■

Nadalje, $s_{\vec{a}\times\vec{b}}$ se očito podudara sa smjerom okomitim na ravninu OAB. Za tu se ravninu još kaže da je **razapeta** predstavnicima vektora $\vec{a}$ i $\vec{b}$.

Važna svojstva vektorskog produkta sakupljena su u ovom teoremu.

TEOREM 5

Vektorsko množenje ima ova osnovna svojstva:

(1) *kvaziasocijativnost, tj.*

$$(\lambda\vec{a}) \times \vec{b} = \lambda(\vec{a} \times \vec{b}), \quad \forall\, \lambda \in \mathbb{R}, \forall\, \vec{a}, \vec{b} \in V^3\,;$$

(2) *distributivnost, tj.*

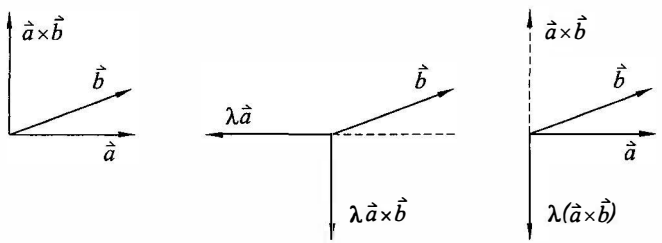
$$\vec{a} \times (\vec{b} + \vec{c}) = (\vec{a} \times \vec{b}) + (\vec{a} \times \vec{c}), \quad \forall\, \vec{a}, \vec{b}, \vec{c} \in V^3\,.$$

Dokaz

(1) Ako je $\lambda = 0$, relacija (1) je ispunjena trivijalno. Ako je $\lambda > 0$, vektori $\vec{a}$ i $\lambda\vec{a}$ su iste orijentacije pa je $\sphericalangle(\lambda\vec{a}, \vec{b}) = \sphericalangle(\vec{a}, \vec{b})$, i imamo

$$\begin{aligned} |(\lambda\vec{a}) \times \vec{b}| &= |\lambda\vec{a}||\vec{b}| \cdot \sin(\lambda\vec{a}, \vec{b}) = \lambda|\vec{a}||\vec{b}| \sin(\vec{a}, \vec{b}) = \\ &= \lambda|\vec{a} \times \vec{b}| = |\lambda||\vec{a} \times \vec{b}| = |\lambda(\vec{a} \times \vec{b})|\,, \end{aligned}$$

a kako su $(\lambda\vec{a}) \times \vec{b}$ i $\lambda(\vec{a} \times \vec{b})$ očito istog smjera i iste orijentacije (iste kao $\vec{a} \times \vec{b}$), tvrdnja je u tom slučaju dokazana. Konačno, ako je $\lambda < 0$ imamo

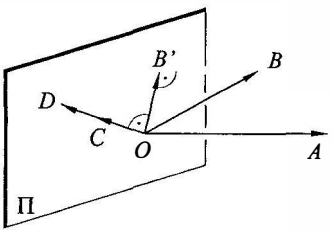


da je $\sphericalangle(\lambda\vec{a}, \vec{b}) = \pi - \sphericalangle(\vec{a}, \vec{b})$, dakle

$$\begin{aligned} |(\lambda\vec{a}) \times \vec{b}| &= |\lambda\vec{a}||\vec{b}| \sin(\lambda\vec{a}, \vec{b}) = |\lambda||\vec{a}||\vec{b}| \cdot \sin[\pi - \sphericalangle(\vec{a}, \vec{b})] \\ &= -\lambda|\vec{a}||\vec{b}| \cdot \sin(\vec{a}, \vec{b}) = -\lambda|\vec{a} \times \vec{b}| = \\ &= |\lambda||\vec{a} \times \vec{b}| = |\lambda(\vec{a} \times \vec{b})|\,. \end{aligned}$$

Nadalje, $(\lambda\vec{a})\times\vec{b}$ i $\vec{a}\times\vec{b}$ imaju očito suprotne orijentacije, a isto tako i vektori $\vec{a}\times\vec{b}$ i $\lambda(\vec{a}\times\vec{b})$ imaju suprotne orijentacije, čime je tvrdnja dokazana.

(2) I opet, ako je bilo koji od vektora $\vec{a},\vec{b}$ i $\vec{c}$ nulvektor, tvrdnja je trivijalna. Pretpostavimo, zato, da su ti vektori različiti od nulvektora. Neka je $\vec{a}=[\overrightarrow{OA}],\vec{b}=[\overrightarrow{OB}]$ i $\varphi=\sphericalangle(\vec{a},\vec{b})$. Neka je Π ravnina kroz točku O, okomita na vektor $\vec{a}$. Neka je B' ortogonalna projekcija točke B na ravninu Π.



Promatrajmo orijentiranu dužinu $\overrightarrow{OB'}$. Vidimo da je

$$|\overrightarrow{OB'}|=|\vec{b}|\cdot\cos(\frac{\pi}{2}-\varphi)=|\vec{b}|\sin\varphi\,.$$

Neka je $C\in\Pi$ odabrana tako da je $|\overrightarrow{OC}|=|\overrightarrow{OB'}|$, $\overrightarrow{OC}\perp\overrightarrow{OB'}$ i da $(\overrightarrow{OA},\overrightarrow{OB},\overrightarrow{OC})$ čine desnu bazu. Onda je također $\overrightarrow{OC}\perp\overrightarrow{OB}$ (poučak o tri normale!). Konačno, neka je $D\in\Pi$ odabrana tako da je

$$\overrightarrow{OD}=|\vec{a}|\cdot\overrightarrow{OC}\,.$$

Onda je

$$|\overrightarrow{OD}|=|\vec{a}|\cdot|\overrightarrow{OC}|=|\vec{a}||\vec{b}|\sin\varphi=|\vec{a}\times\vec{b}|\,.$$

Nadalje je $\overrightarrow{OD}\perp\overrightarrow{OA},\overrightarrow{OB}$ po konstrukciji i $(\overrightarrow{OA},\overrightarrow{OB},\overrightarrow{OD})$ čine desnu bazu, pa je

$$[\overrightarrow{OD}]=\vec{a}\times\vec{b}\,.$$

Neka je sada $\vec{s}=\vec{b}+\vec{c}$. To znači da reprezentanti tih vektora zatvaraju trokut. Konstrukciju koju smo proveli za par vektora $\vec{a},\vec{b}$, provedimo onda za parove $\vec{a},\vec{c}$, odnosno $\vec{a},\vec{s}$. Tako u ravnini Π (okomitoj na $\vec{a}$!) dolazimo do reprezentanata vektora

$$\vec{a}\times\vec{b}\ ,\ \vec{a}\times\vec{c}\ ,\ \vec{a}\times\vec{s}\,.$$

Jasno je, međutim, da ti reprezentanti također zatvaraju trokut. Naime, projekcije reprezentanata vektora $\vec{b},\vec{c}$ i $\vec{s}$ u ravnini Π zatvaraju trokut, zatim rotacijom za $\pi/2$ trokut prelazi u trokut i konačno, množenjem svih stranica rotiranog trokuta s $|\vec{a}|$ dobivamo opet trokut, njemu sličan. No, stranice tog

trokuta su upravo reprezentanti vektora $\vec{a} \times \vec{b}$, $\vec{a} \times \vec{c}$ i $\vec{a} \times \vec{s}$ u ravnini Π. Imamo dakle

$$(\vec{a} \times \vec{b}) + (\vec{a} \times \vec{c}) = \vec{a} \times \vec{s}\,,$$

odnosno

$$(\vec{a} \times \vec{b}) + (\vec{a} \times \vec{c}) = \vec{a} \times (\vec{b} + \vec{c})$$

i tvrdnja je dokazana. ■

KOROLAR 6

Za vektorsko množenje također vrijedi

(3) $\vec{a} \times (\lambda\vec{b}) = \lambda(\vec{a} \times \vec{b})\,, \quad \forall\, \lambda \in \mathbb{R},\ \forall\, \vec{a}, \vec{b} \in V^3$;

(4) $(\vec{a} + \vec{b}) \times \vec{c} = (\vec{a} \times \vec{c}) + (\vec{b} \times \vec{c})\,, \quad \forall\, \vec{a}, \vec{b}, \vec{c} \in V^3$.

Dokaz

Tvrdnje izlaze iz antikomutativnosti vektorskog množenja. Na primjer, za (3) imamo:

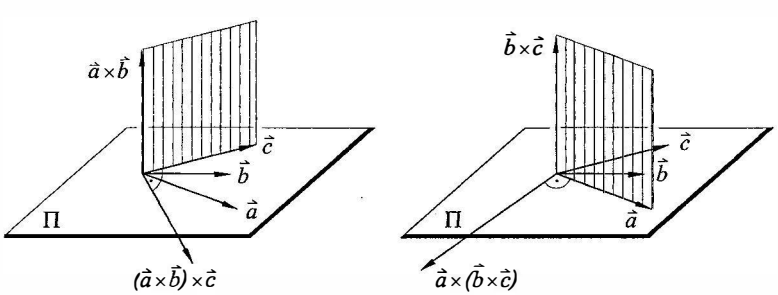
$$\begin{aligned} \vec{a} \times (\lambda\vec{b}) &= -[(\lambda\vec{b}) \times \vec{a}] = -[\lambda(\vec{b} \times \vec{a})] = \\ &= [(-1)\lambda] \cdot (\vec{b} \times \vec{a}) = [\lambda(-1)](\vec{b} \times \vec{a}) = \\ &= \lambda[(-1)(\vec{b} \times \vec{a})] = \lambda(\vec{a} \times \vec{b})\,. \end{aligned}$$

■

Primijetimo da vektorsko množenje nije asocijativno, tj. općenito je

$$(\vec{a} \times \vec{b}) \times \vec{c} \neq \vec{a} \times (\vec{b} \times \vec{c})\,.$$

To pokazuje ovaj jednostavan primjer: neka su specijalno vektori $\vec{a}, \vec{b}$ i $\vec{c}$ komplanarni, tj. paralelni s istom ravninom Π i, nadalje, neka $\vec{a}$ i $\vec{c}$ nisu kolinearni. Pogledajmo sliku



Očito je da su vektori $(\vec{a} \times \vec{b}) \times \vec{c}$ i $\vec{a} \times (\vec{b} \times \vec{c})$ paralelni s ravninom Π, ali je

$$(\vec{a} \times \vec{b}) \times \vec{c} \perp \vec{c}, \quad \vec{a} \times (\vec{b} \times \vec{c}) \perp \vec{a}$$

pa je, zbog pretpostavke da $\vec{a}$ i $\vec{c}$ nisu kolinearni, jasno da je

$$(\vec{a} \times \vec{b}) \times \vec{c} \neq \vec{a} \times (\vec{b} \times \vec{c}) .$$

Nadalje, vektorsko množenje ne posjeduje jedinicu, tj. vektor $\vec{e} \in V^3$ takav da je

$$\vec{e} \times \vec{a} = \vec{a} \times \vec{e} = \vec{a}$$

za svaki $\vec{a} \in V^3$. Naime, to bi proturječilo antikomutativnosti vektorskog množenja (a i činjenici da je $\vec{e} \times \vec{a} \perp \vec{a}$).

Kažimo sada ovo: Ako je u vektorskom prostoru nad nekim poljem definirana još jedna binarna operacija, množenje vektora, pa ako to množenje ima svojstva nabrojena u Tm. 5 i Kor. 6, tj. za njega vrijede obje kvaziasocijativnosti i obje distributivnosti, onda takvu strukturu nazivamo **algebra nad danim poljem**.

Prema tome smo pokazali

TEOREM 7

Vektorski prostor V^3 je uz vektorsko množenje algebra nad poljem $\mathbb{R}$ realnih brojeva, i to neasocijativna, nekomutativna i bez jedinice. ■

Kako smo već vidjeli, vektorsko množenje nije asocijativno. Preciznije, vrijedi ovaj

TEOREM 8

Za svaki izbor $\vec{a}, \vec{b}, \vec{c} \in V^3$ je

(1) $(\vec{a} \times \vec{b}) \times \vec{c} = (\vec{a}\vec{c})\vec{b} - (\vec{b}\vec{c})\vec{a}$;

(2) $\vec{a} \times (\vec{b} \times \vec{c}) = (\vec{a}\vec{c})\vec{b} - (\vec{a}\vec{b})\vec{c}$.

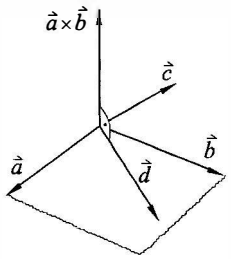
Dokaz

Dokažimo (1). Neka je $\vec{d} = (\vec{a} \times \vec{b}) \times \vec{c}$. Po definiciji je $\vec{d} \perp \vec{a} \times \vec{b}$ i $\vec{d} \perp \vec{c}$. Iz činjenice da je $\vec{d}$ okomit na $\vec{a} \times \vec{b}$, slijedi da je $\vec{d}$ komplanaran s vektorima $\vec{a}$ i $\vec{b}$, pa prema Tm. 3 iz 5.7. postoje α i $\beta \in \mathbb{R}$ takvi da je

$$\vec{d} = \alpha\vec{a} + \beta\vec{b} .$$

Ostaje odrediti α i β. No, iz činjenice da je $\vec{d} \perp \vec{c}$, imamo

$$\vec{d} \cdot \vec{c} = (\alpha\vec{a} + \beta\vec{b})\vec{c} = 0 ,$$



dakle

$$\alpha(\vec{a}\vec{c}) + \beta(\vec{b}\vec{c}) = 0\,.$$

Odatle odmah razabiremo da mora biti

$$\alpha = -\lambda(\vec{b}\vec{c})\,,$$

$$\beta = \lambda(\vec{a}\vec{c})\,.$$

Može se pokazati (vidi Zad. 2. u 5.13.) da faktor proporcionalnosti λ mora biti jednak 1, pa je time relacija (1) verificirana. Slično se vidi da vrijedi relacija (2). ■

KOROLAR 9

Za svaki izbor $\vec{a}, \vec{b}, \vec{c} \in V^3$ vrijedi tzv. Jacobijev identitet:

$$(\vec{a}\times\vec{b})\times\vec{c} + (\vec{b}\times\vec{c})\times\vec{a} + (\vec{c}\times\vec{a})\times\vec{b} = \vec{0}\,.$$

Dokaz

Neposredno iz Tm. 8. Imamo naime

$$\begin{aligned}(\vec{a}\times\vec{b})\times\vec{c} &= (\vec{a}\vec{c})\vec{b} - (\vec{b}\vec{c})\vec{a}\,,\\ (\vec{b}\times\vec{c})\times\vec{a} &= (\vec{b}\vec{a})\vec{c} - (\vec{c}\vec{a})\vec{b}\,,\\ (\vec{c}\times\vec{a})\times\vec{b} &= (\vec{c}\vec{b})\vec{a} - (\vec{a}\vec{b})\vec{c}\,.\end{aligned}$$

Zbog komutativnosti skalarnog produkta, zbrajanjem dobivamo tvrdnju. ■

Primijetimo da iz Kor. 9 slijedi da su vektori $(\vec{a}\times\vec{b})\times\vec{c}$, $(\vec{b}\times\vec{c})\times\vec{a}$ i $(\vec{c}\times\vec{a})\times\vec{b}$ komplanarni.

Općenito, (neasocijativna) algebra nad nekim poljem, u kojoj je množenje antikomutativno*) i za to množenje vrijedi Jacobijev identitet, naziva se **Liejeva algebra** nad danim poljem.

Prema onom što smo dokazali, imamo

*) Koji put se u definiciji Liejeve algebre umjesto antikomutativnosti zahtijeva da množenje ima svojstvo da je kvadrat svakog vektora jednak nulvektoru. Taj zahtjev povlači antikomutativnost, a i ekvivalentan je antikomutativnosti, ako polje nije karakteristike 2.

TEOREM 10

Vektorski prostor V^3 je uz vektorsko množenje Liejeva algebra nad poljem $\mathbb{R}$ realnih brojeva. ■

ZADACI

1. Neka su $\vec{a}, \vec{b}, \vec{c} \in V^3$ i neka je $\vec{a} = [\overrightarrow{OA}]$, $\vec{b} = [\overrightarrow{OB}]$, $\vec{c} = [\overrightarrow{OC}]$. Neka je pravac BC paralelan s pravcem OA. Onda je $\vec{a} \times \vec{b} = \vec{a} \times \vec{c}$. Dokaži!

2. Pokaži da je veza između skalarnog i vektorskog produkta dana relacijom
$$(\vec{a}\vec{b})^2 + (\vec{a} \times \vec{b})^2 = \vec{a}^2 \cdot \vec{b}^2 .$$
To je tzv. **Lagrangeov identitet**.

3. Uvjeri se da je struktura $(V^3, +, \times)$ Liejev prsten (vidi Zad. 6. u 4.1.).

4. Dokaži:
$$\begin{aligned}(\vec{a} \times \vec{b}) \times (\vec{c} \times \vec{d}) &= ((\vec{a} \times \vec{b})\vec{d})\vec{c} - ((\vec{a} \times \vec{b})\vec{c})\vec{d} \\ &= (\vec{a}(\vec{c} \times \vec{d}))\vec{b} - (\vec{b}(\vec{c} \times \vec{d}))\vec{a} .\end{aligned}$$

5. Dokaži da ako za $\vec{a}, \vec{b}, \vec{c} \in V^3$ vrijedi
$$\vec{a} + \vec{b} + \vec{c} = \vec{0} ,$$
onda je uvijek
$$\vec{a} \times \vec{b} = \vec{b} \times \vec{c} = \vec{c} \times \vec{a} .$$
Koristeći se navedenom činjenicom, dokaži teorem o sinusima.

6. Obilježimo plohe tetraedra redom s F_1, F_2, F_3, F_4. Neka je $\vec{v}_i$ $(i = 1, 2, 3, 4)$ vektor s modulom jednakim površini F_i, okomit na nju i orijentiran prema van. Dokaži da onda vrijedi:
$$\vec{v}_1 + \vec{v}_2 + \vec{v}_3 + \vec{v}_4 = \vec{0} .$$

5.12. Koordinatni prikaz vektorskog produkta

Ovdje ćemo, radi prikladnijeg formuliranja nekih rezultata vektorske algebre, uvesti pojam determinante drugog i trećeg reda. Opću teoriju determinanata obradit ćemo kasnije.

Neka su $\alpha, \beta, \gamma, \delta \in \mathbb{R}$ bilo koja četiri broja. Onda definiramo

$$\begin{vmatrix} \alpha & \beta \\ \gamma & \delta \end{vmatrix} = \alpha\delta - \beta\gamma$$

i simbol na lijevoj strani zovemo **determinanta drugog reda**. Na primjer,

$$\begin{vmatrix} 2 & -3 \\ 1 & -5 \end{vmatrix} = 2(-5) - (-3)1 = -10 + 3 = -7 ,$$

$$\begin{vmatrix} \sin\alpha & \cos\alpha \\ -\cos\alpha & \sin\alpha \end{vmatrix} = \sin^2\alpha + \cos^2\alpha = 1 .$$

Determinantu trećeg reda definiramo sa

$$\begin{vmatrix} \alpha_1 & \alpha_2 & \alpha_3 \\ \beta_1 & \beta_2 & \beta_3 \\ \gamma_1 & \gamma_2 & \gamma_3 \end{vmatrix} = \alpha_1 \begin{vmatrix} \beta_2 & \beta_3 \\ \gamma_2 & \gamma_3 \end{vmatrix} - \alpha_2 \begin{vmatrix} \beta_1 & \beta_3 \\ \gamma_1 & \gamma_3 \end{vmatrix} + \alpha_3 \begin{vmatrix} \beta_1 & \beta_2 \\ \gamma_1 & \gamma_2 \end{vmatrix} .$$

Kažemo da smo determinantu izračunali razvijanjem po elementima njezina prvog retka. Na primjer,

$$\begin{vmatrix} 3 & 1 & 2 \\ -1 & 2 & 5 \\ -3 & -2 & 1 \end{vmatrix} = 3 \begin{vmatrix} 2 & 5 \\ -2 & 1 \end{vmatrix} - \begin{vmatrix} -1 & 5 \\ -3 & 1 \end{vmatrix} + 2 \begin{vmatrix} -1 & 2 \\ -3 & -2 \end{vmatrix}$$

$$= 3 \cdot 12 - 14 + 2 \cdot 8 = 32 \quad .$$

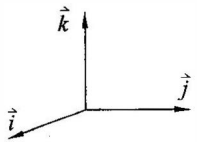
Iz definicije se odmah razabire da će zamjenom dvaju redaka (ili stupaca) determinanta promijeniti predznak. Odatle pak slijedi da je vrijednost determinante u kojoj su dva retka ista (ili proporcionalna), jednaka nuli.

Napomenimo, konačno, da ćemo s determinantama formalno operirati u skladu s danim definicijama i u slučaju kad se u **jednom** retku (stupcu) determinante umjesto realnih brojeva pojave vektori. Na primjer,

$$\begin{vmatrix} \vec{a} & \vec{b} \\ 2 & 5 \end{vmatrix} = 5\vec{a} - 2\vec{b} .$$

Vratimo se sada problemu koordinatnog prikaza vektorskog produkta. Neka je $(\vec{i}, \vec{j}, \vec{k})$ bilo koja ortonormirana baza u V^3. Iz definicije dobivamo odmah sljedeću tablicu za množenje koordinatnih vektora:

$\times$	$\vec{i}$	$\vec{j}$	$\vec{k}$
$\vec{i}$	0	$\vec{k}$	$-\vec{j}$
$\vec{j}$	$-\vec{k}$	0	$\vec{i}$
$\vec{k}$	$\vec{j}$	$-\vec{i}$	0



Neka su sada

$$\left.\begin{aligned}\vec{a} &= (\alpha_1, \alpha_2, \alpha_3)\\ \vec{b} &= (\beta_1, \beta_2, \beta_3)\end{aligned}\right\} \quad (1)$$

bilo koji vektori iz V^3, zadani svojim koordinatama u odnosu na danu ortonormiranu bazu. Vektor $\vec{a} \times \vec{b}$ želimo izraziti pomoću tih koordinata.

PROPOZICIJA 1

Koordinate vektorskog produkta dane su s

$$\vec{a} \times \vec{b} = (\alpha_2\beta_3 - \alpha_3\beta_2, \alpha_3\beta_1 - \alpha_1\beta_3, \alpha_1\beta_2 - \alpha_2\beta_1) .$$

Dokaz

Zbog distributivnosti, kvaziasocijativnosti i antikomutativnosti vektorskog množenja te tablice za vektorske produkte koordinatnih vektora imamo redom

$$\begin{aligned}\vec{a} \times \vec{b} &= (\alpha_1\vec{i} + \alpha_2\vec{j} + \alpha_3\vec{k}) \times (\beta_1\vec{i} + \beta_2\vec{j} + \beta_3\vec{k}) =\\ &= \alpha_1\beta_1(\vec{i} \times \vec{i}) + \alpha_1\beta_2(\vec{i} \times \vec{j}) + \alpha_1\beta_3(\vec{i} \times \vec{k}) +\\ &\quad + \alpha_2\beta_1(\vec{j} \times \vec{i}) + \alpha_2\beta_2(\vec{j} \times \vec{j}) + \alpha_2\beta_3(\vec{j} \times \vec{k}) +\\ &\quad + \alpha_3\beta_1(\vec{k} \times \vec{i}) + \alpha_3\beta_2(\vec{k} \times \vec{j}) + \alpha_3\beta_3(\vec{k} \times \vec{k}) =\\ &= (\alpha_2\beta_3 - \alpha_3\beta_2)\vec{i} + (\alpha_3\beta_1 - \alpha_1\beta_3)\vec{j} +\\ &\quad + (\alpha_1\beta_2 - \alpha_2\beta_1)\vec{k} ,\end{aligned}$$

pa je tvrdnja dokazana. ■

Odmah se razabire da se vektorski produkt može formalno i pregledno zapisati pomoću determinante. Imamo

KOROLAR 2

Ako su vektori $\vec{a}, \vec{b}$ dani svojim koordinatama (1), onda je

$$\vec{a} \times \vec{b} = \begin{vmatrix} \vec{i} & \vec{j} & \vec{k} \\ \alpha_1 & \alpha_2 & \alpha_3 \\ \beta_1 & \beta_2 & \beta_3 \end{vmatrix} .$$

Dokaz

Razvij determinantu po elementima prvog retka. ■

Iz ovog prikaza vektorskog produkta neposredno čitamo činjenicu (koju smo već prije dokazali) da je $\vec{a} \times \vec{b} = \vec{0}$ onda i samo onda, ako je bar jedan od faktora nulvektor, ili ako su koordinate vektora proporcionalne, dakle onda i samo onda kad su vektori $\vec{a}$ i $\vec{b}$ kolinearni.

ZADACI

1. Za bilo kojih šest brojeva $\alpha_1, \alpha_2, \alpha_3, \beta_1, \beta_2, \beta_3 \in \mathbb{R}$ vrijedi tzv. **Lagrangeov identitet**

$$\begin{aligned}&(\alpha_1\beta_1 + \alpha_2\beta_2 + \alpha_3\beta_3)^2 + (\alpha_2\beta_3 - \alpha_3\beta_2)^2 + \\ &+(\alpha_3\beta_1 - \alpha_1\beta_3)^2 + (\alpha_1\beta_2 - \alpha_2\beta_1)^2 = \\ &= (\alpha_1^2 + \alpha_2^2 + \alpha_3^2)(\beta_1^2 + \beta_2^2 + \beta_3^2) \quad .\end{aligned}$$

   [Uputa: Interpretiraj dane brojeve kao koordinate vektora $\vec{a}$ i $\vec{b}$, pa primijeni relaciju iz Zad. 2. u 5.11.]

2. Neka su $A = (\vec{a}_1, \vec{a}_2, \vec{a}_3)$ i $B = (\vec{b}_1, \vec{b}_2, \vec{b}_3)$ bilo koje baze (ne nužno ortonormirane) prostora V^3, a

$$\vec{b}_k = (\alpha_{1k}, \alpha_{2k}, \alpha_{3k}) \,,$$

   $k = 1, 2, 3$, koordinatni slogovi vektora iz B s obzirom na bazu A. Neka je

$$D = \begin{vmatrix} \alpha_{11} & \alpha_{12} & \alpha_{13} \\ \alpha_{21} & \alpha_{22} & \alpha_{23} \\ \alpha_{31} & \alpha_{32} & \alpha_{33} \end{vmatrix} \quad .$$

   Baze A i B su jednako orijentirane (tj. obje desne ili obje lijeve) ako i samo ako je $D > 0$. Dokaži!

5.13. Mješoviti produkt

Neka je

$$m : V^3 \times V^3 \times V^3 \to \mathbb{R}$$

preslikavanje definirano s

$$m(\vec{a}, \vec{b}, \vec{c}) = (\vec{a} \times \vec{b})\vec{c} \,,$$

za svaki $\vec{a}, \vec{b}, \vec{c} \in V^3$. Onda m nazivamo **mješovito** ili **vektorskoskalarno množenje** u V^3, a rezultat tog množenja **mješovitim produktom** triju vektora. Pišemo kraće

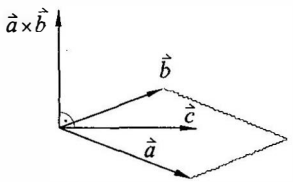
$$m(\vec{a}, \vec{b}, \vec{c}) = (\vec{a}, \vec{b}, \vec{c}) \,.$$

PROPOZICIJA 1

Mješoviti produkt triju vektora jednak je nuli onda i samo onda ako su ti vektori komplanarni.

Dokaz

Neka su $\vec{a}, \vec{b}, \vec{c} \in V^3$ komplanarni. Ako je bilo koji od vektora $\vec{a} \times \vec{b}$ i $\vec{c}$ nulvektor, očito je $(\vec{a}, \vec{b}, \vec{c}) = 0$. Uzmimo zato da to nije slučaj. Onda su dani vektori paralelni s ravninom, razapetom predstavnicima vektora $\vec{a}$ i $\vec{b}$, kažimo II. Prema tome je $\vec{a} \times \vec{b} \perp$ II, dakle $\vec{a} \times \vec{b} \perp \vec{c}$, pa je $(\vec{a}, \vec{b}, \vec{c}) = (\vec{a} \times \vec{b})\vec{c} = 0$.



Obratno, neka je $(\vec{a}, \vec{b}, \vec{c}) = 0$. To znači da je $\vec{a} \times \vec{b} = \vec{0}$ ili $\vec{c} = \vec{0}$ ili je pak $\vec{a} \times \vec{b} \perp \vec{c}$, tj. vektor $\vec{c}$ je paralelan s ravninom razapetom predstavnicima vektora $\vec{a}$ i $\vec{b}$. U svakom slučaju, vektori $\vec{a}, \vec{b}$ i $\vec{c}$ su komplanarni. ■

Neka su vektori dani svojim koordinatama

$$\left.\begin{aligned} \vec{a} &= (\alpha_1, \alpha_2, \alpha_3) \\ \vec{b} &= (\beta_1, \beta_2, \beta_3) \\ \vec{c} &= (\gamma_1, \gamma_2, \gamma_3) \end{aligned}\right\} \tag{1}$$

u odnosu na neku ortonormiranu bazu. Onda možemo i njihov mješoviti produkt izraziti pomoću tih koordinata.

PROPOZICIJA 2

Ako su vektori $\vec{a}, \vec{b}, \vec{c} \in V^3$ dani svojim koordinatama (1), *onda je*

$$(\vec{a}, \vec{b}, \vec{c}) = \begin{vmatrix} \alpha_1 & \alpha_2 & \alpha_3 \\ \beta_1 & \beta_2 & \beta_3 \\ \gamma_1 & \gamma_2 & \gamma_3 \end{vmatrix} .$$

Dokaz

Imamo redom

$$\begin{aligned} (\vec{a}, \vec{b}, \vec{c}) &= (\vec{a} \times \vec{b})\vec{c} = \vec{c}(\vec{a} \times \vec{b}) = (\gamma_1\vec{i} + \gamma_2\vec{j} + \gamma_3\vec{k}) \cdot \\ &\cdot ((\alpha_2\beta_3 - \alpha_3\beta_2)\vec{i} + (\alpha_3\beta_1 - \alpha_1\beta_3)\vec{j} + (\alpha_1\beta_2 - \alpha_2\beta_1)\vec{k}) = \\ &= \gamma_1(\alpha_2\beta_3 - \alpha_3\beta_2) + \gamma_2(\alpha_3\beta_1 - \alpha_1\beta_3) + \gamma_3(\alpha_1\beta_2 - \alpha_2\beta_1) = \\ &= \begin{vmatrix} \gamma_1 & \gamma_2 & \gamma_3 \\ \alpha_1 & \alpha_2 & \alpha_3 \\ \beta_1 & \beta_2 & \beta_3 \end{vmatrix} = \begin{vmatrix} \alpha_1 & \alpha_2 & \alpha_3 \\ \beta_1 & \beta_2 & \beta_3 \\ \gamma_1 & \gamma_2 & \gamma_3 \end{vmatrix} . \end{aligned}$$

■

KOROLAR 3

Tri su vektora komplanarna onda i samo onda ako za njihove koordinate (1) *vrijedi*

$$\begin{vmatrix} \alpha_1 & \alpha_2 & \alpha_3 \\ \beta_1 & \beta_2 & \beta_3 \\ \gamma_1 & \gamma_2 & \gamma_3 \end{vmatrix} = 0 \ .$$

Dokaz

Neposredno iz Prop. 1 i Prop. 2. ■

Iz prikaza mješovitog produkta danog s Prop. 2 neposredno čitamo neka njegova daljnja svojstva.

PROPOZICIJA 4

Parnom permutacijom trojke vektora, mješoviti produkt $(\vec{a}, \vec{b}, \vec{c})$ *se ne mijenja, dok neparnom permutacijom mješoviti produkt mijenja samo predznak. Drugim riječima, vrijedi:*

$$(\vec{a}, \vec{b}, \vec{c}) = (\vec{b}, \vec{c}, \vec{a}) = (\vec{c}, \vec{a}, \vec{b}) = -(\vec{a}, \vec{c}, \vec{b}) = -(\vec{c}, \vec{b}, \vec{a}) = -(\vec{b}, \vec{a}, \vec{c}) \ .$$

Dokaz

Neposredno iz Prop. 2 i činjenice da determinanta pri zamjeni dvaju redaka mijenja predznak. Pri parnoj permutaciji faktora provode se dvije, a pri neparnoj jedna ili tri zamjene redaka. ■

KOROLAR 5

Uvijek je

$$(\vec{a} \times \vec{b})\vec{c} = \vec{a}(\vec{b} \times \vec{c}) \ .$$

Dokaz

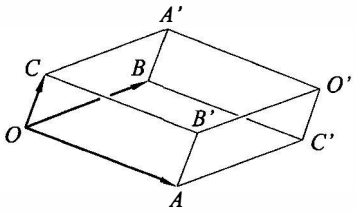
Prema Prop. 4 imamo

$$\vec{a}(\vec{b} \times \vec{c}) = (\vec{b} \times \vec{c})\vec{a} = (\vec{a} \times \vec{b})\vec{c} \, .$$ ■

Prema tome, možemo alternativno definirati $(\vec{a}, \vec{b}, \vec{c}) = \vec{a}(\vec{b} \times \vec{c})$. Drugim riječima, u mješovitom se produktu, uz zadržani poredak faktora, može zamijeniti uloga vektorskog i skalarnog množenja (dakako, uz pomicanje zagrade), čime je opravdana oznaka $(\vec{a}, \vec{b}, \vec{c})$ za mješoviti produkt, u kojoj se vektori pojavljuju ravnopravno.

Mješovitom se produktu može dati i izvjesna geometrijska interpretacija. Neka su $\vec{a}, \vec{b}, \vec{c} \in V^3$ tri nekomplanarna vektora, a $\overrightarrow{OA}, \overrightarrow{OB}, \overrightarrow{OC}$ njihovi predstavnici s istom početnom točkom O. Onda oni određuju u prostoru jedan paralelepiped, kažimo $OBA'CAC'O'B'$. Za taj paralelepiped kažemo da je

razapet vektorima $\vec{a}, \vec{b}$ i $\vec{c}$.



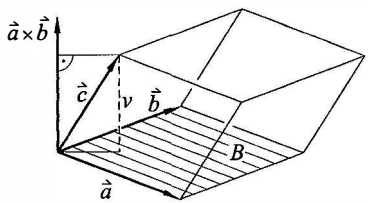
Želimo odrediti volumen tog paralelepipeda. Uzevši u obzir da je volumen uvijek pozitivan realan broj, vrijedi

TEOREM 6

Volumen paralelepipeda razapetog vektorima $\vec{a}, \vec{b}$ i $\vec{c}$ jednak je mješovitom produktu $(\vec{a}, \vec{b}, \vec{c})$ tih vektora ili njemu suprotan, već prema tome čine li vektori $\vec{a}, \vec{b}, \vec{c}$ u tom poretku desnu ili lijevu bazu.

Dokaz

Neka najprije $\vec{a}, \vec{b}, \vec{c}$ čine desnu bazu.



Kako vektori $\vec{a}, \vec{b}, \vec{a} \times \vec{b}$ uvijek čine desnu bazu, to su vektori $\vec{c}$ i $\vec{a} \times \vec{b}$ s iste strane ravnine razapete s $\vec{a}$ i $\vec{b}$, pa je $\sphericalangle(\vec{a} \times \vec{b}, \vec{c}) < \pi/2$, tj. $\cos(\vec{a} \times \vec{b}, \vec{c}) > 0$. Nadalje, iz slike vidimo da je

$$V = \text{baza} \times \text{visina} = |\vec{a} \times \vec{b}| \cdot v = |\vec{a} \times \vec{b}| \cdot |\vec{c}| \cdot \cos(\vec{a} \times \vec{b}, \vec{c}) =$$

$$= (\vec{a} \times \vec{b})\vec{c} = (\vec{a}, \vec{b}, \vec{c}) > 0 \,.$$

Ako je pak $\vec{a}, \vec{b}, \vec{c}$ lijeva baza, vektori $\vec{b}, \vec{a}, \vec{c}$ čine u tom poretku desnu bazu pa, prema prethodnom, imamo

$$V = (\vec{b}, \vec{a}, \vec{c}) = -(\vec{a}, \vec{b}, \vec{c}) > 0 \,,$$

čime je teorem dokazan. ■

Iz Prop. 2 onda neposredno slijedi

KOROLAR 7

Ako su vektori koji razapinju paralelepiped dani svojim koordinatama (1), *njegov je volumen dan formulom*

$$V = \pm \begin{vmatrix} \alpha_1 & \alpha_2 & \alpha_3 \\ \beta_1 & \beta_2 & \beta_3 \\ \gamma_1 & \gamma_2 & \gamma_3 \end{vmatrix} ,$$

gdje predznak treba odabrati tako, da volumen bude pozitivan. ■

ZADACI

1. Dokaži: Mješovito množenje ima ova svojstva:

   (1) $(\lambda\vec{a}, \mu\vec{b}, \nu\vec{c}) = \lambda\mu\nu(\vec{a}, \vec{b}, \vec{c})$;

   (2) $(\vec{a}_1 + \vec{a}_2, \vec{b}, \vec{c}) = (\vec{a}_1, \vec{b}, \vec{c}) + (\vec{a}_2, \vec{b}, \vec{c})$,
   $(\vec{a}, \vec{b}_1 + \vec{b}_2, \vec{c}) = (\vec{a}, \vec{b}_1, \vec{c}) + (\vec{a}, \vec{b}_2, \vec{c})$,
   $(\vec{a}, \vec{b}, \vec{c}_1 + \vec{c}_2) = (\vec{a}, \vec{b}, \vec{c}_1) + (\vec{a}, \vec{b}, \vec{c}_2)$.

2. Dokaži Tm. 8 iz 5.11. [Uputa: Tamo smo već vidjeli da je

   $$(\vec{a} \times \vec{b}) \times \vec{c} = \lambda[(\vec{a}\vec{c})\vec{b} - (\vec{b}\vec{c})\vec{a}] ,$$

   pa ostaje pokazati da je $\lambda = 1$. Uvjerimo se najprije da λ ne ovisi o izboru vektora $\vec{c}$. Imamo

   $$(\vec{a} \times \vec{b}) \times \vec{c}_1 = \lambda_1[(\vec{a}\vec{c}_1)\vec{b} - (\vec{b}\vec{c}_1)\vec{a}] ,$$

   $$(\vec{a} \times \vec{b}) \times \vec{c}_2 = \lambda_2[(\vec{a}\vec{c}_2)\vec{b} - (\vec{b}\vec{c}_2)\vec{a}] .$$

   Pomnožimo prvu relaciju skalarno s $\vec{c}_2$, a drugu s $\vec{c}_1$. Zbog Kor. 5 imamo

   $$[(\vec{a} \times \vec{b}) \times \vec{c}_1]\vec{c}_2 = (\vec{a} \times \vec{b}) \cdot (\vec{c}_1 \times \vec{c}_2) = \lambda_1[(\vec{a}\vec{c}_1)(\vec{b}\vec{c}_2) - (\vec{b}\vec{c}_1)(\vec{a}\vec{c}_2)]$$

   i

   $$[(\vec{a} \times \vec{b}) \times \vec{c}_2]\vec{c}_1 = (\vec{a} \times \vec{b}) \cdot (\vec{c}_2 \times \vec{c}_1) = \lambda_2[(\vec{a}\vec{c}_2)(\vec{b}\vec{c}_1) - (\vec{b}\vec{c}_2)(\vec{a}\vec{c}_1)] .$$

   Kako je $\vec{c}_2 \times \vec{c}_1 = -\vec{c}_1 \times \vec{c}_2$, dijeljenjem tih relacija dobivamo $\lambda_1 = \lambda_2$, tj. λ zaista ne ovisi o izboru vektora $\vec{c}$. Uzmimo zato specijalno $\vec{c} = \vec{a}$. Imamo

   $$(\vec{a} \times \vec{b}) \times \vec{a} = \lambda[(\vec{a}\vec{a})\vec{b} - (\vec{b}\vec{a})\vec{a}]$$

pa množenjem skalarno s $\vec{b}$ dobivamo

$$[(\vec{a}\times\vec{b})\times\vec{a}]\cdot\vec{b} = (\vec{a}\times\vec{b})\cdot(\vec{a}\times\vec{b}) = \lambda[(\vec{a}\vec{a})(\vec{b}\vec{b}) - (\vec{b}\vec{a})(\vec{a}\vec{b})]\,,$$

dakle

$$(\vec{a}\times\vec{b})^2 = \lambda[\vec{a}^2\vec{b}^2 - (\vec{a}\vec{b})^2]\,.$$

No, u Zad. 2. iz 5.11. smo imali

$$(\vec{a}\times\vec{b})^2 = \vec{a}^2\cdot\vec{b}^2 - (\vec{a}\vec{b})^2\,,$$

pa uspoređivanjem dobivamo $\lambda = 1$.]

3. Primijeni prethodni rezultat da dokažeš

$$(\vec{a}\times\vec{b})\cdot(\vec{c}\times\vec{d}) = \begin{vmatrix} \vec{a}\vec{c} & \vec{a}\vec{d} \\ \vec{b}\vec{c} & \vec{b}\vec{d} \end{vmatrix}\,.$$

4. Dokaži:

$$\vec{a}\times[\vec{b}\times(\vec{c}\times\vec{d})] = \begin{vmatrix} \vec{a}\times\vec{c} & \vec{a}\times\vec{d} \\ \vec{b}\cdot\vec{c} & \vec{b}\cdot\vec{d} \end{vmatrix}\,.$$

5. Dokaži:

$$\begin{aligned}(\vec{a}\times\vec{b})\times(\vec{c}\times\vec{d}) &= (\vec{a},\vec{c},\vec{d})\vec{b} - (\vec{b},\vec{c},\vec{d})\vec{a} = \\ &= (\vec{a},\vec{b},\vec{d})\vec{c} - (\vec{a},\vec{b},\vec{c})\vec{d}\,.\end{aligned}$$

Ako vektori $\vec{a},\vec{b},\vec{c}$ nisu komplanarni, odatle slijedi

$$\vec{d} = \frac{(\vec{b},\vec{c},\vec{d})}{(\vec{a},\vec{b},\vec{c})}\cdot\vec{a} - \frac{(\vec{c},\vec{d},\vec{a})}{(\vec{a},\vec{b},\vec{c})}\cdot\vec{b} + \frac{(\vec{d},\vec{a},\vec{b})}{(\vec{a},\vec{b},\vec{c})}\cdot\vec{c}\,,$$

tj. $\vec{d}$ je prikazan uz pomoć triju vektora $\vec{a},\vec{b}$ i $\vec{c}$.

6. Vektori $\vec{a},\vec{b},\vec{c}\in V^3$ dani svojim koordinatama (1) u desnoj bazi, čine u danom prostoru desnu, odnosno lijevu bazu, onda i samo onda ako je

$$\begin{vmatrix} \alpha_1 & \alpha_2 & \alpha_3 \\ \beta_1 & \beta_2 & \beta_3 \\ \gamma_1 & \gamma_2 & \gamma_3 \end{vmatrix} \gtrless 0\,.$$

Dokaži!

5.14. Operatori na V^3

Običaj je da se preslikavanja

$$f : V^3 \to V^3$$

vektorskog prostora V^3 u sebe nazivaju **operatorima**. Kažemo da je operator f **linearan**, ako je ispunjeno

(1) $f(\vec{a} + \vec{b}) = f(\vec{a}) + f(\vec{b})$;

(2) $f(\alpha\vec{a}) = \alpha f(\vec{a})$,

za svaki izbor $\vec{a}, \vec{b} \in V^3$ i $\alpha \in \mathbb{R}$. Uvjet (1) naziva se **aditivnost** operatora i zapravo kaže da se od linearnog operatora traži da bude homomorfizam aditivne grupe V^3, dok je uvjetom (2) opisana **homogenost** operatora u odnosu na množenje vektora skalarima. Odmah se vidi da se dva uvjeta iz definicije mogu objediniti: operator f će biti linearan ako i samo ako vrijedi

$$f(\alpha\vec{a} + \beta\vec{b}) = \alpha f(\vec{a}) + \beta f(\vec{b}),$$

za sve $\vec{a}, \vec{b} \in V^3$ i $\alpha, \beta \in \mathbb{R}$. Linearni operator se katkad naziva i **homomorfizam prostora V^3**. Ako je operator i bijektivan, govorimo o **regularnom operatoru** ili **izomorfizmu prostora**. Primijetimo kako iz činjenice da je linearni operator f homomorfizam na razini grupa, slijedi da f preslikava nulvektor u nulvektor, $f(\vec{0}) = \vec{0}$.

TEOREM 1

Kompozicija linearnih operatora je linearni operator.

Dokaz

Neka su $f, g : V^3 \to V^3$ linearni operatori i $h = f \circ g$. Onda je h homomorfizam grupe V^3 kao kompozicija homomorfizama, pa je dovoljno provjeriti homogenost. Imamo

$$\begin{aligned} h(\alpha\vec{a}) &= (f \circ g)(\alpha\vec{a}) = f[g(\alpha\vec{a})] = f[\alpha g(\vec{a})] = \\ &= \alpha[f(g(\vec{a}))] = \alpha[(f \circ g)(\vec{a})] = \alpha h(\vec{a}) \end{aligned}$$

i tvrdnja je dokazana. ■

Linearni operator jednoznačno je određen svojim djelovanjem na bazi prostora. Vrijedi naime

TEOREM 2

Neka je $(\vec{i},\vec{j},\vec{k})$ baza prostora V^3 (ne nužno ortonormirana), a $(\vec{a}_1,\vec{a}_2,\vec{a}_3)$ bilo koja uređena trojka vektora. Onda postoji jedan i samo jedan linearni operator $f: V^3 \to V^3$ sa svojstvom da je

$$f(\vec{i}) = \vec{a}_1, \quad f(\vec{j}) = \vec{a}_2, \quad f(\vec{k}) = \vec{a}_3 \ .$$

Dokaz

Neka je $\vec{a} \in V^3$ bilo koji vektor, a $(\alpha_1,\alpha_2,\alpha_3)$ njegov koordinatni slog u danoj bazi. Onda definiramo operator

$$f: V^3 \to V^3$$

stavljajući

$$f(\vec{a}) = f(\alpha_1\vec{i}+\alpha_2\vec{j}+\alpha_3\vec{k}) = \alpha_1\vec{a}_1 + \alpha_2\vec{a}_2 + \alpha_3\vec{a}_3 \ .$$

Odmah razabiremo da će po toj definiciji biti

$$f(\vec{i}) = \vec{a}_1, \quad f(\vec{j}) = \vec{a}_2, \quad f(\vec{k}) = \vec{a}_3 \ .$$

Pokažimo da je operator f linearan. Ako je $\vec{b} = (\beta_1,\beta_2,\beta_3)$ neki drugi vektor, imamo

$$\begin{aligned} f(\alpha\vec{a}+\beta\vec{b}) &= f[\alpha(\alpha_1\vec{i}+\alpha_2\vec{j}+\alpha_3\vec{k}) + \beta(\beta_1\vec{i}+\beta_2\vec{j}+\beta_3\vec{k})] = \\ &= f[(\alpha\alpha_1+\beta\beta_1)\vec{i}+(\alpha\alpha_2+\beta\beta_2)\vec{j}+(\alpha\alpha_3+\beta\beta_3)\vec{k}] = \\ &= (\alpha\alpha_1+\beta\beta_1)\vec{a}_1 + (\alpha\alpha_2+\beta\beta_2)\vec{a}_2 + (\alpha\alpha_3+\beta\beta_3)\vec{a}_3 = \\ &= \alpha(\alpha_1\vec{a}_1+\alpha_2\vec{a}_2+\alpha_3\vec{a}_3) + \beta(\beta_1\vec{a}_1+\beta_2\vec{a}_2+\beta_3\vec{a}_3) = \\ &= \alpha f(\vec{a}) + \beta f(\vec{b}) \end{aligned}$$

i linearnost je provjerena. Kad bi postojao još jedan linearni operator

$$g: V^3 \to V^3$$

sa svojstvom

$$g(\vec{i}) = \vec{a}_1, \quad g(\vec{j}) = \vec{a}_2, \quad g(\vec{k}) = \vec{a}_3 \ ,$$

imali bismo

$$\begin{aligned} g(\vec{a}) &= g(\alpha_1\vec{a}_1+\alpha_2\vec{a}_2+\alpha_3\vec{a}_3) = \alpha_1 g(\vec{i}) + \alpha_2 g(\vec{j}) + \alpha_3 g(\vec{k}) = \\ &= \alpha_1\vec{a}_1+\alpha_2\vec{a}_2+\alpha_3\vec{a}_3 = f(\vec{a}) \end{aligned}$$

za svaki $\vec{a} \in V^3$, dakle $g = f$, pa je dokazana i jedinstvenost. ■

Ako je, dakle, $f : V^3 \to V^3$ bilo koji linearni operator, a slike vektora baze $B = (\vec{i}, \vec{j}, \vec{k})$ imaju u toj bazi prikaze

$$\begin{aligned} f(\vec{i}) &= \alpha_1\vec{i} + \alpha_2\vec{j} + \alpha_3\vec{k} \ , \\ f(\vec{j}) &= \beta_1\vec{i} + \beta_2\vec{j} + \beta_3\vec{k} \ , \\ f(\vec{k}) &= \gamma_1\vec{i} + \gamma_2\vec{j} + \gamma_3\vec{k} \ , \end{aligned} \tag{1}$$

onda je iz Tm. 2 jasno da će operator f biti određen jednoznačno skalarima $\alpha_i, \beta_i, \gamma_i$, $i = 1, 2, 3$. Te skalare obično zapisujemo pregledno u kvadratnu shemu

$$\begin{bmatrix} \alpha_1 & \beta_1 & \gamma_1 \\ \alpha_2 & \beta_2 & \gamma_2 \\ \alpha_3 & \beta_3 & \gamma_3 \end{bmatrix} \ ,$$

koju nazivamo **matrični zapis** ili **matrica operatora** f u bazi B. Uočimo da su koordinate slika vektora baze popisane u stupcima sheme. Dakako, isti će operator u nekoj drugoj bazi imati općenito drugu matricu.

Prije nego navedemo primjere linearnih operatora, uvedimo pojam **potprostora** u V^3. Neka je $\vec{a} \neq \vec{0}$ bilo koji vektor iz V^3. Onda skup

$$[\vec{a}] = \{\lambda\vec{a} | \lambda \in \mathbb{R}\}$$

svih vektora kolinearnih s vektorom $\vec{a}$ nazivamo **jednodimenzionalni potprostor** ili **pravac** u V^3. Nadalje, ako je $\vec{a}, \vec{b} \in V^3$ par nekolinearnih vektora, skup

$$[\vec{a}, \vec{b}] = \{\lambda\vec{a} + \mu\vec{b} \mid \lambda, \mu \in \mathbb{R}\}$$

svih vektora koji su s njima komplanarni nazivamo **dvodimenzionalni potprostor** ili **ravnina** u V^3.

Dakako, pravci i ravnine su također vektorski prostori, prvi s bazom $(\vec{a})$, a drugi s bazom $(\vec{a}, \vec{b})$, pa zato govorimo o jednodimenzionalnim, odnosno dvodimenzionalnim potprostorima.

Vratimo se sada linearnim operatorima u V^3 i navedimo nekoliko tipičnih primjera.

PRIMJERI

Svaki od sljedećih operatora je linearan, a pripadne matrice se odnose na ortonormiranu bazu $(\vec{i}, \vec{j}, \vec{k})$ u V^3:

1. **Nuloperator**, $n(\vec{a}) = \vec{0}$, i **jedinični** ili **identični operator** (identiteta), $e(\vec{a}) = \vec{a}$. Njihove matrice su redom

$$\begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} \text{ i } \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \ .$$

2. Operator **centralne simetrije**, $c(\vec{a}) = -\vec{a}$, ima matrični zapis

$$\begin{bmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{bmatrix} .$$

3. Operator **homotetije s koeficijentom** $\lambda \in \mathbb{R}$ definiran je s $h(\vec{a}) = \lambda\vec{a}$. Matrica tog operatora je

$$\begin{bmatrix} \lambda & 0 & 0 \\ 0 & \lambda & 0 \\ 0 & 0 & \lambda \end{bmatrix} .$$

Uočimo da kao specijalne slučajeve za $\lambda = 0$ dobivamo nuloperator, za $\lambda = 1$ identitetu, a za $\lambda = -1$ centralnu simetriju.

4. Operatori **zrcaljenja na ravninama** u V^3. S obzirom na danu bazu i uz $\vec{a} = \alpha_1\vec{\imath} + \alpha_2\vec{\jmath} + \alpha_3\vec{k}$, definiramo npr. zrcaljenje na ravnini

$$\begin{array}{lll} [\vec{\jmath}, \vec{k}] & \text{sa} & s_1(\vec{a}) = -\alpha_1\vec{\imath} + \alpha_2\vec{\jmath} + \alpha_3\vec{k} , \\ [\vec{k}, \vec{\imath}] & \text{sa} & s_2(\vec{a}) = \alpha_1\vec{\imath} - \alpha_2\vec{\jmath} + \alpha_3\vec{k} , \\ [\vec{\imath}, \vec{\jmath}] & \text{sa} & s_3(\vec{a}) = \alpha_1\vec{\imath} + \alpha_2\vec{\jmath} - \alpha_3\vec{k} , \end{array}$$

i pripadne matrice su očito

$$\begin{bmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} , \quad \begin{bmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{bmatrix} , \quad \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{bmatrix} .$$

Slično, sa

$$s(\vec{a}) = \alpha_2\vec{\imath} + \alpha_1\vec{\jmath} + \alpha_3\vec{k}$$

definirano je zrcaljenje na simetralnoj ravnini $[\vec{\imath} + \vec{\jmath}, \vec{k}]$, i taj operator ima matricu

$$\begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix} .$$

5. Operatori **zrcaljenja na pravcima**. Na primjer, opisujemo zrcaljenje na pravcu

$$\begin{array}{lll} [\vec{\imath}] & \text{sa} & a_1(\vec{a}) = \alpha_1\vec{\imath} - \alpha_2\vec{\jmath} - \alpha_3\vec{k} , \\ [\vec{\jmath}] & \text{sa} & a_2(\vec{a}) = -\alpha_1\vec{\imath} + \alpha_2\vec{\jmath} - \alpha_3\vec{k} , \\ [\vec{k}] & \text{sa} & a_3(\vec{a}) = -\alpha_1\vec{\imath} - \alpha_2\vec{\jmath} + \alpha_3\vec{k} , \end{array}$$

odnosno pomoću matrica

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{bmatrix}, \quad \begin{bmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{bmatrix}, \quad \begin{bmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

6. Operatori **rotacija oko** danog **pravca**. Tako je npr. s

$$r_1(\vec{a}) = (\alpha_1 \cos\varphi - \alpha_2 \sin\varphi)\vec{i} + (\alpha_1 \sin\varphi + \alpha_2 \cos\varphi)\vec{j} + \alpha_3\vec{k}$$

opisana rotacija oko pravca $[\vec{k}]$ za dani kut φ. Analogno se definiraju rotacije oko $[\vec{j}]$ i $[\vec{i}]$. U matričnoj formi te su rotacije opisane s

$$\begin{bmatrix} cos\varphi & -\sin\varphi & 0 \\ \sin\varphi & \cos\varphi & 0 \\ 0 & 0 & 1 \end{bmatrix}, \quad \begin{bmatrix} \cos\varphi & 0 & -\sin\varphi \\ 0 & 1 & 0 \\ \sin\varphi & 0 & \cos\varphi \end{bmatrix},$$

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & \cos\varphi & -\sin\varphi \\ 0 & \sin\varphi & \cos\varphi \end{bmatrix}.$$

7. Operatori (ortogonalnog) **projiciranja na ravninu**. Projiciranje na ravninu

$$\begin{array}{lllllll} [\vec{j},\vec{k}] & \text{dano je s} & p_1(\vec{a}) = & & \alpha_2\vec{j} & +\alpha_3\vec{k}, \\ [\vec{k},\vec{i}] & \text{dano je s} & p_2(\vec{a}) = & \alpha_1\vec{i} & & +\alpha_3\vec{k}, \\ [\vec{i},\vec{j}] & \text{dano je s} & p_3(\vec{a}) = & \alpha_1\vec{i} & +\alpha_2\vec{j} & . \end{array}$$

Pripadne matrice su, dakako,

$$\begin{bmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix} \text{ i } \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{bmatrix}.$$

8. Operatori (ortogonalnog) **projiciranja na pravac**. Primjeri su projiciranje na pravac

$$\begin{array}{llllll} [\vec{i}] & \text{definirano s} & q_1(\vec{a}) & = \alpha_1\vec{i} & & , \\ [\vec{j}] & \text{definirano s} & q_2(\vec{a}) & = & \alpha_2\vec{j} & , \\ [\vec{k}] & \text{definirano s} & q_3(\vec{a}) & = & & \alpha_3\vec{k}, \end{array}$$

ili u matričnom zapisu

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

Linearnost navedenih operatora lako se provjerava. Također se lako vidi, a i geometrijski je jasno, da su identiteta, kao i operatori opisani u Prim. 2.– 6. regularni, dok nuloperator i projekcije to nisu. Kako ćemo vidjeti kasnije (i općenitije), postoji jednostavan kriterij za prepoznavanje regularnog operatora: Linearni operator $f : V^3 \to V^3$ je regularan ako i samo ako je determinanta matrice tog operatora, tj.

$$\det f = \det \begin{bmatrix} \alpha_1 & \beta_1 & \gamma_1 \\ \alpha_2 & \beta_2 & \gamma_2 \\ \alpha_3 & \beta_3 & \gamma_3 \end{bmatrix} = \begin{vmatrix} \alpha_1 & \beta_1 & \gamma_1 \\ \alpha_2 & \beta_2 & \gamma_2 \\ \alpha_3 & \beta_3 & \gamma_3 \end{vmatrix}$$

različita od nule.

Primijetimo da u svim našim primjerima linearni operator prevodi bar jedan pravac iz V^3 u sama sebe. Zaključak je općenit, to svojstvo ima svaki linearni operator na V^3 (vidi Zad. 7.).

Uočimo da među primjerima nismo spomenuli operator **translacije**, definiran s

$$t(\vec{a}) = \vec{a} + \vec{c}$$

za dani $\vec{c} \neq \vec{0}$. No, za njega je

$$t(\vec{a} + \vec{b}) = (\vec{a} + \vec{b}) + \vec{c} \neq (\vec{a} + \vec{c}) + (\vec{b} + \vec{c}) = t(\vec{a}) + t(\vec{b}) \,,$$

tj. taj operator nije aditivan, dakle ni linearan.

Navedimo sada neke specijalne tipove linearnih operatora. Za linearni operator $f : V^3 \to V^3$ kažemo da je **simetričan**, ako vrijedi

$$f(\vec{a}) \cdot \vec{b} = \vec{a} \cdot f(\vec{b}) \,,$$

za sve $\vec{a}, \vec{b} \in V^3$. Ako je $(\vec{i}, \vec{j}, \vec{k})$ ortonormirana baza, a u prikazu (1) za simetrični operator f pomnožimo prvu relaciju skalarno vektorom $\vec{j}$, a drugu s $\vec{i}$, imat ćemo zbog ortonormiranosti

$$\beta_1 = f(\vec{j}) \cdot \vec{i} = \vec{i} \cdot f(\vec{j}) = f(\vec{i}) \cdot \vec{j} = \alpha_2 \,,$$

dakle, $\beta_1 = \alpha_2$. Slično se vidi da mora vrijediti $\gamma_1 = \alpha_3$ i $\gamma_2 = \beta_3$. Odatle slijedi da simetrični operator ima u ortonormiranoj bazi matricu

$$\begin{bmatrix} \alpha_1 & \alpha_2 & \alpha_3 \\ \alpha_2 & \beta_2 & \beta_3 \\ \alpha_3 & \beta_3 & \gamma_3 \end{bmatrix}$$

koja je **simetrična** s obzirom na glavnu dijagonalu. Otud potječe naziv za simetrični operator. Vrijedi i obrat te tvrdnje (vidi Zad. 8.).

Tipični simetrični operatori su tzv. kontrakcije, odnosno dilatacije prostora. Za dani broj $\lambda \in \mathbb{R}$, i uz $\vec{a} = \alpha_1\vec{\imath} + \alpha_2\vec{\jmath} + \alpha_3\vec{k}$, definiramo operator

$$f : V^3 \to V^3$$

stavljajući

$$f(\vec{a}) = \alpha_1\vec{\imath} + \alpha_2\vec{\jmath} + \lambda\alpha_3\vec{k} \, .$$

Lako se provjeri da je f linearan. Nadalje, ako je $\vec{b} = \beta_1\vec{\imath} + \beta_2\vec{\jmath} + \beta_3\vec{k}$ bilo koji drugi vektor, imamo

$$\begin{aligned} f(\vec{a}) \cdot \vec{b} &= \alpha_1\beta_1 + \alpha_2\beta_2 + (\lambda\alpha_3)\beta_3 = \\ &= \alpha_1\beta_1 + \alpha_2\beta_2 + \alpha_3(\lambda\beta_3) = \vec{a} \cdot f(\vec{b}) \, , \end{aligned}$$

što pokazuje da je operator f simetričan. Ako je specijalno $\lambda = 1$, f je identiteta, ako je $\lambda = -1$ dobivamo zrcaljenje na ravnini $[\vec{\imath}, \vec{\jmath}]$, a ako je $\lambda = 0$, f je projiciranje na ravninu $[\vec{\imath}, \vec{\jmath}]$. Kad je $0 <\mid \lambda \mid< 1$, operator f nazivamo **kontrakcija** (stezanje) prostora u smjeru pravca $[\vec{k}]$, prema ravnini $[\vec{\imath}, \vec{\jmath}]$, a kada je $\mid \lambda \mid > 1$, operator f nazivamo **dilatacija** (rastezanje) prostora u smjeru pravca $[\vec{k}]$. Broj λ zovemo **koeficijent kontrakcije** odnosno **dilatacije**. Naziv dolazi odatle što je, primjerice, u slučaju kontrakcije jasno da vrijedi

$$|f(\vec{a})| \leq |\vec{a}| \, ,$$

tj. vektori se pri tom preslikavanju skraćuju. To skraćivanje je maksimalno u smjeru $[\vec{k}]$ (za faktor λ), a bez efekta ako vektor pripada ravnini $[\vec{\imath}, \vec{\jmath}]$. Slično, pri dilataciji se vektori produžuju,

$$|f(\vec{a})| \geq |\vec{a}| \quad .$$

Matrica kontrakcije (dilatacije) je

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & \lambda \end{bmatrix} \quad ,$$

dakle simetrična, kako smo i očekivali.

Općenitije, neka su $\lambda_1, \lambda_2, \lambda_3 \in \mathbb{R}$ bilo koji brojevi. Onda definiramo operator

$$s : V^3 \to V^3$$

stavljajući

$$s(\vec{a}) = \lambda_1\alpha_1\vec{\imath} + \lambda_2\alpha_2\vec{\jmath} + \lambda_3\alpha_3\vec{k} \quad , \tag{2}$$

za koji se također lako provjeri da je simetričan. Njegova je matrica

$$\begin{bmatrix} \lambda_1 & 0 & 0 \\ 0 & \lambda_2 & 0 \\ 0 & 0 & \lambda_3 \end{bmatrix} . \tag{3}$$

Odatle vidimo da je

$$\det s = \lambda_1 \lambda_2 \lambda_3$$

pa zaključujemo da će operator s biti regularan ako i samo ako su svi $\lambda_i \neq 0$. Ako je $\lambda_1 = \lambda_2 = \lambda_3$, dobivamo, kao specijalan slučaj, homotetiju.

Primijetimo da se s može dobiti kao kompozicija,

$$s = f_1 \circ f_2 \circ f_3 ,$$

operatora

$$\begin{aligned} f_1(\vec{a}) &= \lambda_1\alpha_1\vec{\imath} + \quad \alpha_2\vec{\jmath} + \quad \alpha_3\vec{k} , \\ f_2(\vec{a}) &= \quad \alpha_1\vec{\imath} + \lambda_2\alpha_2\vec{\jmath} + \quad \alpha_3\vec{k} , \\ f_3(\vec{a}) &= \quad \alpha_1\vec{\imath} + \quad \alpha_2\vec{\jmath} + \lambda_3\alpha_3\vec{k} , \end{aligned}$$

tj. kao kompozicija dilatacija (kontrakcija) u smjerovima $[\vec{\imath}], [\vec{\jmath}], [\vec{k}]$, s koeficijentima λ_1, λ_2 odnosno λ_3.

Zanimljivo je da za svaki simetrični operator postoji ortonormirana baza u kojoj je on definiran s (2) i, prema tome, ima matricu (3) (vidi Zad. 9.).

Drugi važan tip linearnih operatora su ortogonalni operatori. Operator $f : V^3 \to V^3$ je **ortogonalan** ako čuva skalarni produkt, tj. ako vrijedi

$$f(\vec{a}) \cdot f(\vec{b}) = \vec{a} \cdot \vec{b}$$

za sve $\vec{a}, \vec{b} \in V^3$. Iz definicije odmah razabiremo da će takav operator preslikavati okomite vektore u okomite, pa mu odatle i naziv. I više, ortogonalni operator čuva modul vektora:

$$| f(\vec{a}) | = \sqrt{f(\vec{a}) \cdot f(\vec{a})} = \sqrt{\vec{a} \cdot \vec{a}} = | \vec{a} | ,$$

a također i kutove između vektora, zbog

$$\cos(f(\vec{a}), f(\vec{b})) = \frac{f(\vec{a}) \cdot f(\vec{b})}{|f(\vec{a})| \cdot |f(\vec{b})|} = \frac{\vec{a} \cdot \vec{b}}{|\vec{a}| \cdot |\vec{b}|} = \cos(\vec{a}, \vec{b}) .$$

Prema tome, operator f čuva metriku, pa se za njega kaže da je **izometrički operator** ili **izometrija** prostora V^3. Nije teško vidjeti da je svaki ortogonalni operator bijektivan, dakle regularan.

Ako je $(\vec{i}, \vec{j}, \vec{k})$ ortonormirana baza u V^3, njezina slika

$$(f(\vec{i}), f(\vec{j}), f(\vec{k}))$$

bit će također jedna ortonormirana baza, tj. i za nju će vrijediti:

$$|f(\vec{i})| = |f(\vec{j})| = |f(\vec{k})| = 1 ,$$

$$f(\vec{j}) \cdot f(\vec{k}) = f(\vec{k}) \cdot f(\vec{i}) = f(\vec{i}) \cdot f(\vec{j}) = 0 .$$

Ako to uvažimo u prikazu (1), odmah vidimo da će skalari u matrici

$$\begin{bmatrix} \alpha_1 & \beta_1 & \gamma_1 \\ \alpha_2 & \beta_2 & \gamma_2 \\ \alpha_3 & \beta_3 & \gamma_3 \end{bmatrix}$$

ortogonalnog operatora f zadovoljavati sljedeće uvjete:

$$\begin{aligned} \alpha_1^2 + \alpha_2^2 + \alpha_3^2 &= 1 , \\ \beta_1^2 + \beta_2^2 + \beta_3^2 &= 1 , \\ \gamma_1^2 + \gamma_2^2 + \gamma_3^2 &= 1 , \end{aligned}$$

i nadalje

$$\begin{aligned} \beta_1\gamma_1 + \beta_2\gamma_2 + \beta_3\gamma_3 &= 0 , \\ \gamma_1\alpha_1 + \gamma_2\alpha_2 + \gamma_3\alpha_3 &= 0 , \\ \alpha_1\beta_1 + \alpha_2\beta_2 + \alpha_3\beta_3 &= 0 . \end{aligned}$$

Kažemo kratko, da stupci u toj matrici čine jedan **ortonormirani sustav**. Može se pokazati da i redci matrice čine ortonormirani sustav. Matricu s tim svojstvom nazivamo **ortogonalnom**. Dakle, ortogonalni operator ima u ortonormiranoj bazi ortogonalnu matricu. Vrijedi i obrat te tvrdnje (vidi Zad. 11.).

Tipični primjeri ortogonalnih operatora su rotacije i zrcaljenja. Ako je npr. $r : V^3 \to V^3$ rotacija oko pravca $[\vec{k}]$ za kut φ, prema Prim. 6. za bilo koje $a, b \in V^3$ imamo

$$\begin{aligned} r(\vec{a}) &= (\alpha_1 \cos\varphi - \alpha_2 \sin\varphi)\vec{i} + (\alpha_1 \sin\varphi + \alpha_2 \cos\varphi)\vec{j} + \alpha_3\vec{k} , \\ r(\vec{b}) &= (\beta_1 \cos\varphi - \beta_2 \sin\varphi)\vec{i} + (\beta_1 \sin\varphi + \beta_2 \cos\varphi)\vec{j} + \beta_3\vec{k} \end{aligned}$$

i odatle

$$\begin{aligned} r(\vec{a})r(\vec{b}) &= \alpha_1\beta_1 \cos^2\varphi - (\alpha_1\beta_2 + \alpha_2\beta_1) \sin\varphi \cos\varphi + \\ &+\alpha_2\beta_2 \sin^2\varphi + \alpha_1\beta_1 \sin^2\varphi + (\alpha_1\beta_2 + \alpha_2\beta_1) \sin\varphi \cos\varphi + \\ &+\alpha_2\beta_2 \cos^2\varphi + \alpha_3\beta_3 = \alpha_1\beta_1 + \alpha_2\beta_2 + \alpha_3\beta_3 = \vec{a}\vec{b} , \end{aligned}$$

tj. r je zaista ortogonalan. Slično se vidi da su zrcaljenja na pravcu (zapravo rotacije za $\varphi = \pi$) i zrcaljenja na ravninama također ortogonalni operatori. To su u suštini i jedini ortogonalni operatori, jer se može dokazati da je svaki ortogonalni operator ili rotacija, ili zrcaljenje na nekoj ravnini, ili kompozicija takvih operatora (Zad. 19.).

ZADACI

1. Neka su $f, g : V^3 \to V^3$ linearni operatori. Onda definiramo njihov zbroj s
$$(f+g)(\vec{a}) = f(\vec{a}) + g(\vec{a})$$
i množenje operatora skalarom s
$$(\lambda f)(\vec{a}) = \lambda f(\vec{a}) .$$
Pokaži da su $f+g$ i λf također linearni operatori.

2. Neka je s $\operatorname{Hom} V^3$ označen skup svih linearnih operatora koji djeluju na prostoru V^3. Pokaži da je, uz upravo definirano zbrajanje operatora i množenje operatora skalarom, $\operatorname{Hom} V^3$ jedan vektorski prostor. Zanimljivo je da je taj prostor 9-dimenzionalan (vidi točku 7.4.).

3. Prostor $\operatorname{Hom} V^3$ je, uz kompoziciju operatora kao operaciju množenja (Tm. 1), jedna algebra nad poljem $\mathbb{R}$, asocijativna, s jedinicom, ali nekomutativna. Dokaži!

4. Neka su $f, f' \in \operatorname{Hom} V^3$ bilo koji operatori, a
$$\begin{bmatrix} \alpha_1 & \beta_1 & \gamma_1 \\ \alpha_2 & \beta_2 & \gamma_2 \\ \alpha_3 & \beta_3 & \gamma_3 \end{bmatrix} , \quad \begin{bmatrix} \alpha'_1 & \beta'_1 & \gamma'_1 \\ \alpha'_2 & \beta'_2 & \gamma'_2 \\ \alpha'_3 & \beta'_3 & \gamma'_3 \end{bmatrix}$$
njihove matrice u danoj bazi $(\vec{\imath}, \vec{\jmath}, \vec{k})$. Onda operator $f+f'$ ima u toj bazi matricu
$$\begin{bmatrix} \alpha_1+\alpha'_1 & \beta_1+\beta'_1 & \gamma_1+\gamma'_1 \\ \alpha_2+\alpha'_2 & \beta_2+\beta'_2 & \gamma_2+\gamma'_2 \\ \alpha_3+\alpha'_3 & \beta_3+\beta'_3 & \gamma_3+\gamma'_3 \end{bmatrix} ,$$
a operator λf ima matricu
$$\begin{bmatrix} \lambda\alpha_1 & \lambda\beta_1 & \lambda\gamma_1 \\ \lambda\alpha_2 & \lambda\beta_2 & \lambda\gamma_2 \\ \lambda\alpha_3 & \lambda\beta_3 & \lambda\gamma_3 \end{bmatrix} .$$

Matrica kompozicije operatora, $f \circ f'$, nešto je složenija i ima oblik

$$\begin{bmatrix} \alpha_1\alpha_1' + \beta_1\alpha_2' + \gamma_1\alpha_3' & \alpha_1\beta_1' + \beta_1\beta_2' + \gamma_1\beta_3' & \alpha_1\gamma_1' + \beta_1\gamma_2' + \gamma_1\gamma_3' \\ \alpha_2\alpha_1' + \beta_2\alpha_2' + \gamma_2\alpha_3' & \alpha_2\beta_1' + \beta_2\beta_2' + \gamma_2\beta_3' & \alpha_2\gamma_1' + \beta_2\gamma_2' + \gamma_2\gamma_3' \\ \alpha_3\alpha_1' + \beta_3\alpha_2' + \gamma_3\alpha_3' & \alpha_3\beta_1' + \beta_3\beta_2' + \gamma_3\beta_3' & \alpha_3\gamma_1' + \beta_3\gamma_2' + \gamma_3\gamma_3' \end{bmatrix} .$$

Prouči strukturu te matrice. Zapamti ove rezultate, koji će nam kasnije služiti kao motivacija za definicije operacija s matricama (deveto poglavlje).

5. Ako je $[\vec{a}, \vec{b}]$ ravnina u V^3, onda predstavnici vektora iz $[\vec{a}, \vec{b}]$, s istom početnom točkom, leže u nekoj ravnini prostora E^3. Analogna tvrdnja vrijedi za pravac $[\vec{a}]$ u V^3. Dokaži!

6. Opiši formulom operator rotacije (specijalno zrcaljenja) oko pravca $[\vec{i} + \vec{j}]$, odnosno pravca $[\vec{i} + \vec{j} + \vec{k}]$, i nađi matrice tih operatora u bazi $(\vec{i}, \vec{j}, \vec{k})$.

7. Pokaži da za svaki linearni operator $f : V^3 \to V^3$ postoji bar jedan skalar $\lambda \in \mathbb{R}$ takav da vrijedi

$$f(\vec{a}) = \lambda\vec{a}$$

za neki $\vec{a} \in V^3$, $\vec{a} \neq \vec{0}$. Uvjeri se, nadalje, da skup S svih vektora $\vec{a}$ koji zadovoljavaju tu relaciju (uz fiksni λ) zajedno s $\vec{0}$ čini potprostor od V^3. Taj potprostor je očito **invarijantan** s obzirom na f, tj. vrijedi $f(S) \subset S$, i prema tome svaki operator u V^3 prevodi bar jedan pravac u sama sebe (fenomen koji se ne pojavljuje u V^2). Kažemo da je λ **svojstvena vrijednost** operatora f, svaki $\vec{a} \in S$ **svojstveni vektor**, a S **svojstveni potprostor** operatora, za taj λ. [Uputa: Za $\vec{a} \neq \vec{0}$ promatraj vektore $\vec{a}, f(\vec{a}), f^2(\vec{a}), f^3(\vec{a})$ i koristi se činjenicom da moraju postojati skalari $\alpha, \beta, \gamma, \delta \in \mathbb{R}$, od kojih bar jedan nije nula, takvi da vrijedi

$$\alpha\vec{a} + \beta f(\vec{a}) + \gamma f^2(\vec{a}) + \delta f^3(\vec{a}) = \vec{0}$$

(Zad. 4. u 5.7.). Analiziraj razne mogućnosti.]

8. Vrijedi ovaj obrat tvrdnje iz teksta: Ako linearni operator ima u nekoj ortonormiranoj bazi simetričnu matricu, taj je operator nužno simetričan.

9. Dokaži: Za svaki simetrični operator $f : V^3 \to V^3$ postoje brojevi $\lambda_1, \lambda_2, \lambda_3 \in \mathbb{R}$ i ortonormirana baza $(\vec{i}, \vec{j}, \vec{k})$, takvi da je

$$f(\vec{i}) = \lambda_1\vec{i}, \quad f(\vec{j}) = \lambda_2\vec{j}, \quad f(\vec{k}) = \lambda_3\vec{k} .$$

Naravno, λ_i su onda svojstvene vrijednosti za taj operator (Zad. 7.), a vektori baze pripadni svojstveni vektori. Matrica operatora f ima u toj bazi **dijagonalnu formu**

$$\begin{bmatrix} \lambda_1 & 0 & 0 \\ 0 & \lambda_2 & 0 \\ 0 & 0 & \lambda_3 \end{bmatrix}$$

pa kažemo da se simetrični operator **može dijagonalizirati**. [Uputa: Koristi se Zad. 7.]

10. Nađi primjere koji pokazuju da kompozicija simetričnih operatora ne mora biti simetričan operator. Međutim, suma simetričnih operatora i produkt simetričnog operatora i skalara su simetrični operatori. Simetrični operatori na V^3 čine linearni prostor, potprostor od $\mathrm{Hom}\, V^3$.

11. Dokaži ovaj obrat tvrdnje u tekstu: Ako je linearni operator zapisan u ortonormiranoj bazi ortogonalnom matricom, taj je operator nužno ortogonalan.

12. Vrijedi ovaj obrat: Ako linearni operator prevodi (neku) ortonormiranu bazu u ortonormiranu bazu, taj operator je ortogonalan.

13. Ortogonalni operator nije općenito simetričan. To će biti ako i samo ako je involutoran, tj. ako vrijedi $f^2 = e$. Takvi su npr. operatori zrcaljenja na pravcima i ravninama. Ima li i drugih?

14. Regularni operatori na prostoru V^3 čine grupu u odnosu na komponiranje. To je tzv. **opća linearna grupa** $GL(3)$.

15. Ortogonalni operatori na V^3 čine grupu u odnosu na komponiranje. To je **ortogonalna grupa** $O(3)$. Naravno, $O(3) < GL(3)$.

16. Kompozicija dviju rotacija (oko raznih pravaca, za razne kutove) jest opet rotacija. To je čuveni **Eulerov teorem**. Nadalje, sve rotacije u V^3 čine grupu. To je **grupa rotacija** ili **specijalna ortogonalna grupa** $SO(3)$.

17. Kompozicija dvaju zrcaljenja na ravninama je uvijek rotacija.

18. Za ortogonalni operator f je $\det f = \pm 1$. Pritom je $\det f = 1$ ako i samo ako je f rotacija. Dokaži!

19. Dokaži: Svaki je ortogonalni operator ili rotacija ili kompozicija jedne rotacije i zrcaljenja na nekoj ravnini.

20. U tekstu smo spomenuli operator translacije za dani vektor $\vec{c}$ i vidjeli da taj operator nije linearan ako je $\vec{c} \neq \vec{0}$. Pokaži da je skup svih translacija u V^3, uz komponiranje, grupa, **grupa translacija** $T(3)$.

21. Preslikavanja
$$l : V^3 \to \mathbb{R}$$
nazivamo **funkcionali**. Funkcional je **linearan**, ako vrijedi
$$l(\alpha\vec{a} + \beta\vec{b}) = \alpha l(\vec{a}) + \beta l(\vec{b}) ,$$
za svaki α, $\beta \in \mathbb{R}$ i svaki izbor $\vec{a}$, $\vec{b} \in V^3$. Navedi nekoliko primjera linearnih funkcionala. Pokaži da je za dani $\vec{a} \in V^3$
$$l_{\vec{a}}(\vec{x}) = \vec{x} \cdot \vec{a}$$
linearni funkcional. Uvjeri se da se svaki linearni funkcional može opisati na taj način.

22. Skup svih linearnih funkcionala definiranih na V^3 organiziraj u linearni prostor (vidi Zad. 1. i 2.). To je tzv. **dualni prostor** prostora V^3.

23. Za dani $\vec{a} \in V^3$ definiramo operator $f : V^3 \to V^3$ s
$$f(\vec{x}) = \vec{x} \times \vec{a} .$$
Je li taj operator linearan? Regularan? Simetričan?

24. Promatraj linearne operatore na V^2. Navedi tipične primjere. Koji su od njih simetrični, a koji ortogonalni operatori? Kakve strukture ti operatori čine? Što možeš reći o linearnim operatorima na V^1?

6

ELEMENTI ANALITIČKE GEOMETRIJE U E^3

U raznim je kolegijima (analiza, teorijska mehanika, fizika, itd.) potrebno znanje nekih činjenica iz područja analitičke geometrije prostora. Zato ćemo učiniti malu digresiju i dati pregled tih činjenica, koristeći se vektorskom algebrom, koju smo upravo zaokružili. Pritom ne pretendiramo na veliku sustavnost i potpunost.

6.1. Kartezijev koordinatni sustav

Posvetimo malo pažnje prostoru radijvektora. Neka je $O \in E^3$ po volji odabrana točka, a

$$V^3(O) = \{\vec{r}_T \mid T \in E^3\}$$

skup radijvektora vezan uz tu točku. Kako smo spomenuli (Zad. 1. u 5.3.), postoji prirodna bijekcija

$$r : V^3 \to V^3(O)\,,$$

dana sa $r(\vec{a}) = \vec{r}_A$, gdje je $\vec{r}_A = \overrightarrow{OA}$ predstavnik vektora $\vec{a}$, $[\vec{r}_A] = \vec{a}$. Nadalje, jer su sve operacije s vektorima u V^3 definirane preko predstavnika, u $V^3(O)$ znamo zbrajati radijvektore (po pravilu paralelograma!) i množiti ih skalarom, a isto tako ih znamo skalarno i vektorski množiti. Prema tome, i na $V^3(O)$ imamo sve strukture (grupe, linearnog prostora itd.) koje smo promatrali na V^3 i pritom je jasno da će navedena bijekcija te strukture poštivati, tj. uspostavljati **izomorfizam** na svakoj razini.

Odaberimo u $V^3(O)$ jednu ortonormiranu bazu, pa ju radi jednostavnosti i ovdje označimo s $(\vec{i}, \vec{j}, \vec{k})$; tu su, dakako, $\vec{i} = \overrightarrow{OI}$, $\vec{j} = \overrightarrow{OJ}$ i $\vec{k} = \overrightarrow{OK}$ radijvektori. Ako je $\vec{r} \in V^3(O)$ bilo koji radijvektor, on će imati jednoznačni

prikaz

$$\vec{r} = x\vec{\imath} + y\vec{\jmath} + z\vec{k}\,,$$

gdje su $x, y, z \in \mathbb{R}$. Uređenu trojku

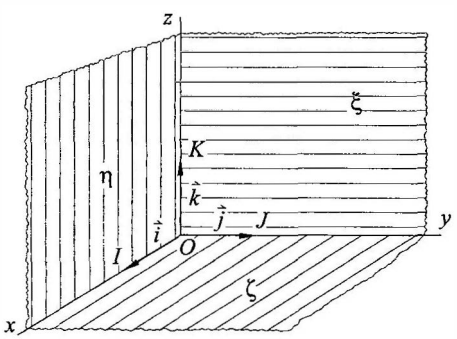
$$(x, y, z)$$

nazivamo **pravokutne koordinate radijvektora** $\vec{r}$, s obzirom na danu bazu.

Sada ćemo uvesti koordinatni sustav u E^3. Ako je $O \in E^3$ bilo koja točka, a $(\vec{\imath}, \vec{\jmath}, \vec{k})$ neka ortonormirana baza u $V^3(O)$, onda izbor

$$\{O\,;\,(\vec{\imath}, \vec{\jmath}, \vec{k})\}$$

nazivamo **pravokutni** ili **Kartezijev koordinatni sustav u** E^3. Točka O njegovo je **ishodište**, a $\vec{\imath}, \vec{\jmath}, \vec{k}$ **koordinatni vektori**. Nadalje, pravce $x = [\vec{\imath}]$, $y = [\vec{\jmath}]$, $z = [\vec{k}]$, koji su u parovima okomiti, nazivamo **osi** koordinatnog sustava, i to redom: x je **os apscisa**, y je **os ordinata**, a z je **os aplikata**. Ravnine $\xi = [\vec{\jmath}, \vec{k}]$, $\eta = [\vec{k}, \vec{\imath}]$, $\zeta = [\vec{\imath}, \vec{\jmath}]$, određene koordinatnim osima, nazivamo **koordinatne ravnine** danog sustava.



Za Kartezijev sustav kažemo da je **lijevi** odnosno **desni**, već prema tome, je li $(\vec{\imath}, \vec{\jmath}, \vec{k})$ lijevo ili desno orijentirana baza (vidi i Zad. 2.). Mi ćemo ubuduće sva razmatranja obavljati u desnom koordinatnom sustavu, dok se npr. u nacrtnoj geometriji dosljedno upotrebljava lijevi koordinatni sustav.

Posredovanjem koordinatnog sustava možemo točke iz E^3 karakterizirati realnim brojevima. Neka je, naime, $T \in E^3$ bilo koja točka. Onda je jednoznačno određen radijvektor $\vec{r}_T = \overrightarrow{OT} \in V^3(O)$ te točke, a taj u danoj bazi za $V^3(O)$ jednoznačno određuje uređenu trojku realnih brojeva, svoje koordinate. Imamo tako pridruženje

$$T \mapsto \vec{r}_T = x\vec{\imath} + y\vec{\jmath} + z\vec{k} \mapsto (x, y, z)\,,$$

kojim je definirano preslikavanje

$$k : E^3 \to \mathbb{R}^3 .$$

Za to preslikavanje se lako vidi da je bijektivno i nazivamo ga **koordinatizacija prostora** E^3.

Ako je $k(T) = (x, y, z)$, uređenu trojku (x, y, z) realnih brojeva nazivamo **pravokutne** ili **Kartezijeve koordinate** točke T u odnosu na dani sustav. Poimence, broj x nazivamo **apscisa**, y **ordinata**, a z **aplikata** ili **kota** točke T. Kako je k bijekcija, često ćemo točku iz E^3 poistovjećivati s njezinim koordinatama i pisati

$$T = (x, y, z) .$$

Također je običaj da se koordinate točke T pišu kao $T(x, y, z)$.

Uočimo i zapamtimo da se, prema našoj konstrukciji, **koordinate točke podudaraju s koordinatama radijvektora te točke.**

U izgradnji analitičke geometrije ćemo, osim točkovne strukture u E^3, rabiti i vektorske strukture $V^3(O)$, odnosno V^3, koje se prirodno prožimaju. Vrijedi tako

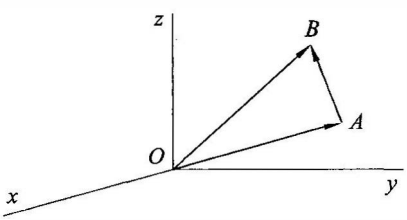
PROPOZICIJA 1

Neka su $A = (x_1, y_1, z_1)$ *i* $B = (x_2, y_2, z_2)$ *točke iz* E^3, *dane svojim koordinatama u odnosu na neki Kartezijev koordinatni sustav. Onda vektor* $[\overrightarrow{AB}]$ *ima u tom sustavu koordinate*

$$[\overrightarrow{AB}] = (x_2 - x_1, y_2 - y_1, z_2 - z_1) .$$

Dokaz

Po zakonu trokuta imamo



$$[\overrightarrow{OA}] + [\overrightarrow{AB}] = [\overrightarrow{OB}] ,$$

pa je, uz identifikaciju koja proizlazi iz činjenice da je preslikavanje r izomorfizam,

$$\begin{aligned} [\overrightarrow{AB}] &= [\vec{r}_B] - [\vec{r}_A] = \vec{r}_B - \vec{r}_A \\ &= (x_2\vec{i} + y_2\vec{j} + z_2\vec{k}) - (x_1\vec{i} + y_1\vec{j} + z_1\vec{k}) = \\ &= (x_2 - x_1)\vec{i} + (y_2 - y_1)\vec{j} + (z_2 - z_1)\vec{k} \end{aligned}$$

i tvrdnja je dokazana. ■

PROPOZICIJA 2

Ako su točke $A = (x_1, y_1, z_1)$, $B = (x_2, y_2, z_2)$ *dane svojim pravokutnim koordinatama, njihova je udaljenost izražena formulom*

$$d(A, B) = \sqrt{(x_2 - x_1)^2 + (y_2 - y_1)^2 + (z_2 - z_1)^2}\,.$$

Dokaz

Kako je $d(A, B) = \overline{AB} = |[\overrightarrow{AB}]|$, tvrdnja slijedi neposredno iz Kor. 2 u 5.10. i prethodne propozicije. ■

ZADACI

1. Koordinatne ravnine dijele prostor E^3 u osam područja koja zovemo **oktanti**. Karakteriziraj pojedine oktante pomoću predznaka koordinata točaka. Čime su karakterizirane točke koje leže u koordinatnim ravninama, odnosno na koordinatnim osima?

2. Orijentaciju koordinatnog sustava možemo definirati i na ovaj način: Na skupu svih pravokutnih sustava u prostoru definiramo relaciju ekvivalencije, smatrajući dva sustava ekvivalentnim ako se gibanjem u prostoru može jedan sustav prevesti u drugi, i to tako da se svaka os poklopi s korespondentnom osi. Svaku klasu ekvivalencije nazivamo **orijentacija**. Uvjeri se da postoje točno dvije orijentacije koordinatnih sustava, koje možemo razlikovati kao lijevu i desnu. Sustav kojem je pridružena lijeva (desna) orijentacija zvat ćemo lijevi (desni) sustav. Uvjeri se da je ova definicija ekvivalentna s definicijom lijevog (desnog) sustava iz teksta.

3. Dokaži da funkcija udaljenosti dviju točaka (Prop. 2) zadovoljava relaciju
$$d(A, B) \leq d(A, C) + d(C, B)$$
za bilo koje $A, B, C \in E^3$. Kad će vrijediti znak jednakosti? To je tzv. **relacija trokuta**.

4. Neka su $A = (x_1, y_1, z_1)$ i $B = (x_2, y_2, z_2)$ bilo koje točke u E^3, a $T \in E^3$ neka točka na pravcu koji ih spaja. Kažemo da T **dijeli dužinu** $\overline{AB}$ u omjeru $\lambda \neq 1$, ako vrijedi
$$[\overrightarrow{AT}] = \lambda \cdot [\overrightarrow{BT}]\,.$$

Pokaži da su koordinate točke T jednake

$$\left(\frac{x_1 - \lambda x_2}{1-\lambda}, \frac{y_1 - \lambda y_2}{1-\lambda}, \frac{z_1 - \lambda z_2}{1-\lambda}\right).$$

Nađi, specijalno, koordinate polovišta dužine, kao i koordinate težišta trokuta.

5. Neka su $T_i = (x_i, y_i, z_i)$, $i = 1, 2, 3$, tri točke prostora koje ne leže na istom pravcu. Nađi formulu za površinu trokuta $T_1T_2T_3$. [Uputa: Uoči da je $P = \frac{1}{2}|[\overrightarrow{T_1T_2}] \times [\overrightarrow{T_1T_3}]|$.]

6. Neka su $T_i = (x_i, y_i, z_i)$, $i = 1, 2, 3, 4$, četiri točke u E^3 koje ne leže u istoj ravnini. Nađi formulu za volumen tetraedra koji te točke određuju. [Uputa: Uoči da je $V = \pm\frac{1}{6} \cdot ([\overrightarrow{T_1T_2}] \times [\overrightarrow{T_1T_3}]) \cdot [\overrightarrow{T_1T_4}]$.]

7. Ako je $O \in E^3$ bilo koja točka, a $(\vec{a}_1, \vec{a}_2, \vec{a}_3)$ bilo koja baza (ne nužno ortonormirana) za prostor $V^3(O)$, onda izbor $\{O\,;\,(\vec{a}_1, \vec{a}_2, \vec{a}_3)\}$ nazivamo **afini koordinatni sustav u** E^3. Preko tog sustava također dolazimo do koordinatizacije prostora E^3, a trojku (x, y, z) pridruženu točki T nazivamo **afinim koordinatama** te točke. Cijela se linearna analitička geometrija može bez teškoća izgraditi i u afinim koordinatama.

8. Definiraj Kartezijev (afini) koordinatni sustav i koordinatizaciju u ravnini E^2 i na pravcu E^1.

6.2. Udaljenost točke od ravnine

Neka je u prostoru E^3 dana ravnina Π i točka T_0. Želimo naći udaljenost $d = d(T_0, \Pi)$ te točke od ravnine.

Neka je $\{O\,;\,(\vec{i}, \vec{j}, \vec{k})\}$ pravokutni koordinatni sustav.

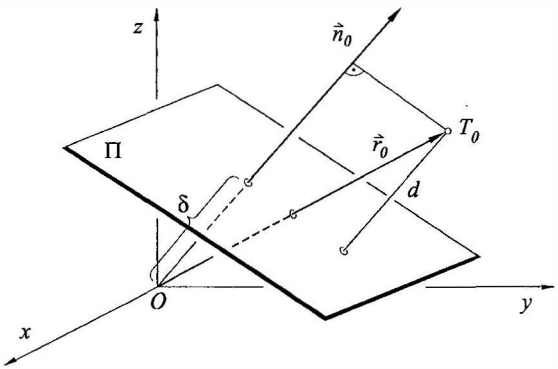
Pretpostavimo da je položaj ravnine fiksiran jediničnim vektorom $\vec{n}_0$ normale na tu ravninu i udaljenošću $\delta \geq 0$ ravnine od ishodišta, a položaj točke T_0 neka je zadan radijvektorom $\vec{r}_0$. Onda iz slike razabiremo da je

$$\vec{r}_0\vec{n}_0 = |\vec{r}_0| \cdot |\vec{n}_0| \cdot \cos(\vec{r}_0, \vec{n}_0) = |\vec{r}_0| \cdot \cos(\vec{r}_0, \vec{n}_0) = d + \delta$$

i odatle

$$d = \vec{r}_0\vec{n}_0 - \delta\,. \tag{1}$$

Nije teško zaključiti da će ta udaljenost biti pozitivna ili negativna, već prema tome jesu li točke T_0 i O s raznih strana ili s iste strane ravnine Π.



Ako su vektor $\vec{n}_0$ i točka T_0 zadani svojim koordinatama u odnosu na dani sustav,

$$\vec{n}_0 = (\cos\alpha, \cos\beta, \cos\gamma) \quad \text{i} \quad T_0 = (x_0, y_0, z_0)\,,$$

iz (1) dobivamo formulu

$$d = x\,\cos\alpha + y\,\cos\beta + z_0\,\cos\gamma - \delta \tag{2}$$

po kojoj se računa udaljenost točke od ravnine.

ZADACI

1. Nađi formulu za udaljenost točke od pravca u ravnini.

6.3. Razni oblici jednadžbe ravnine

Neka je Π bilo koja ravnina u prostoru, pa neka je njezin položaj u koordinatnom sustavu opet fiksiran jediničnim vektorom normale $\vec{n}_0$ i udaljenošću δ od ishodišta.

Točka $T \in E^3$ će ležati u ravnini Π onda i samo onda ako je $d(T, \Pi) = 0$. No, zbog (1) u 6.2. to će biti ako i samo ako je za radijvektor $\vec{r}$ točke T ispunjeno

$$\vec{r}\vec{n}_0 - \delta = 0\,, \tag{1}$$

odnosno, u koordinatnom obliku, ako i samo ako je

$$x\,\cos\alpha + y\,\cos\beta + z\,\cos\gamma - \delta = 0\,. \tag{2}$$

Prema tome, (2) je nuždan i dovoljan uvjet da bi točka $T = (x, y, z)$ ležala u ravnini Π. Uz varijabilno x, y, z, to je, dakle, jednadžba ravnine Π. Taj oblik nazivamo **normalni** ili **Hesseov** oblik jednadžbe ravnine.

Neka je sada položaj ravnine Π u prostoru zadan podacima da ta ravnina prolazi danom točkom T_0 i paralelna je s dva nekolinearna vektora $\vec{a}$ i $\vec{b}$ (tj. "razapeta" vektorima $\vec{a}$ i $\vec{b}$). Ako je $T \in \Pi$ bilo koja točka, vektori $[\overrightarrow{T_0T}], \vec{a}, \vec{b}$ su očito komplanarni, pa prema Tm. 3 iz 5.7. postoje $\lambda, \mu \in \mathbb{R}$ takvi da je

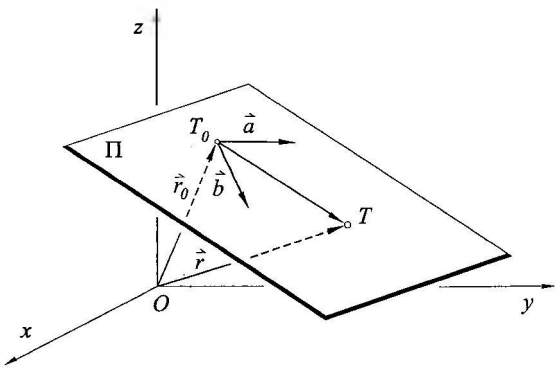
$$[\overrightarrow{T_0T}] = \lambda\vec{a} + \mu\vec{b}\,, \tag{3}$$

odnosno

$$\vec{r} - \vec{r}_0 = \lambda\vec{a} + \mu\vec{b}\,;$$

dakle

$$\vec{r} = \vec{r}_0 + \lambda\vec{a} + \mu\vec{b}\,. \tag{4}$$



Ako variramo parametre λ i μ, dobit ćemo radijvektore svih točaka u ravnini Π, i samo tih točaka. U tom smislu je (4) jednadžba ravnine i to njezin **vektorski parametarski oblik**.

Ako su vektori $\vec{a}$ i $\vec{b}$ dani svojim koordinatama

$$\left.\begin{aligned}\vec{a} &= (\alpha_1, \alpha_2, \alpha_3)\\ \vec{b} &= (\beta_1, \beta_2, \beta_3)\end{aligned}\right\}\,, \tag{5}$$

iz (4) odmah dobivamo tzv. **parametarske jednadžbe ravnine**

$$\left.\begin{aligned}x &= x_0 + \lambda\alpha_1 + \mu\beta_1\\ y &= y_0 + \lambda\alpha_2 + \mu\beta_2\\ z &= z_0 + \lambda\alpha_3 + \mu\beta_3\end{aligned}\right\}\,. \tag{6}$$

Ako želimo imati koordinate (x, y, z) točaka u ravnini Π povezane neposredno jednom jednadžbom, potrebno je iz (6) eliminirati parametre λ i μ. Ta se eliminacija lako provodi na osnovi činjenice da vektori $\vec{r} - \vec{r}_0$, $\vec{a}$ i $\vec{b}$ moraju biti komplanarni, a to će biti onda i samo onda ako njihov mješoviti produkt iščezava, tj. ako je

$$(\vec{r} - \vec{r}_0, \vec{a}, \vec{b}) = 0\,. \tag{7}$$

No, taj uvjet u koordinatnom obliku glasi

$$\begin{vmatrix} x-x_0 & y-y_0 & z-z_0 \\ \alpha_1 & \alpha_2 & \alpha_3 \\ \beta_1 & \beta_2 & \beta_3 \end{vmatrix} = 0 \,, \tag{8}$$

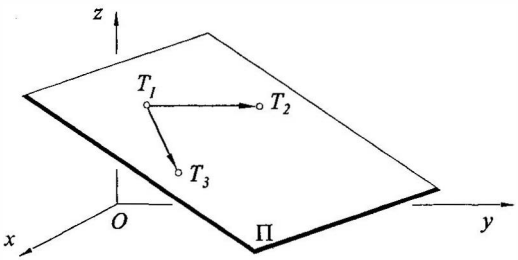
i to je **jednadžba ravnine određene fiksnom točkom i dvama nekolinearnim vektorima.**

Neka su sada $T_i = (x_i, y_i, z_i)$, $i = 1, 2, 3$, tri točke prostora koje ne leže na jednom pravcu. Želimo naći jednadžbu ravnine Π koju te točke (jednoznačno) određuju.

Neka je

$$\vec{a} = [\overrightarrow{T_1T_2}] = \vec{r}_2 - \vec{r}_1 \,,$$

$$\vec{b} = [\overrightarrow{T_1T_3}] = \vec{r}_3 - \vec{r}_1 \,.$$



Ako je $T \in \Pi$ bilo koja točka, vektor $[\overrightarrow{T_1T}] = \vec{r} - \vec{r}_1$ mora biti komplanaran s vektorima $\vec{a}$ i $\vec{b}$ pa prema (7) imamo

$$(\vec{r} - \vec{r}_1, \vec{r}_2 - \vec{r}_1, \vec{r}_3 - \vec{r}_1) = 0 \,, \tag{9}$$

odnosno u koordinatnom obliku

$$\begin{vmatrix} x-x_1 & y-y_1 & z-z_1 \\ x_2-x_1 & y_2-y_1 & z_2-z_1 \\ x_3-x_1 & y_3-y_1 & z_3-z_1 \end{vmatrix} = 0 \,, \tag{10}$$

i to je jednadžba ravnine, određene s tri svoje točke T_i, tj. **jednadžba ravnine kroz tri točke**. Kako ćemo kasnije vidjeti (Zad. 1. u 9.9.), ta se jednadžba može pisati u ekvivalentnom obliku, ali preglednije, kao

$$\begin{vmatrix} x & y & z & 1 \\ x_1 & y_1 & z_1 & 1 \\ x_2 & y_2 & z_2 & 1 \\ x_3 & y_3 & z_3 & 1 \end{vmatrix} = 0 \,. \tag{11}$$

Iz dosadašnjih je razmatranja jasno da se svaka ravnina u prostoru (bez obzira na to, kojim je elementima fiksiran njezin položaj u odnosu na Kartezijev koordinatni sustav) može analitički predočiti pomoću jednadžbe koja je linearna u x,y i z, dakle tipa

$$Ax + By + Cz + D = 0\,, \tag{12}$$

gdje su $A, B, C, D \in \mathbb{R}$. Lako se, međutim, vidi da vrijedi i obrnuto: (12) je, uz uvjet da je bar jedan od koeficijenata A, B i C različit od nule, uvijek jednadžba neke ravnine u prostoru (Zad. 1.). U tom smislu, (12) zovemo **opći oblik jednadžbe ravnine**.

Koje je geometrijsko značenje koeficijenata u jednadžbi (12)?

Neka je (12) jednadžba ravnine Π, a (2) normalni oblik jednadžbe te iste ravnine. Onda se očito te jednadžbe mogu razlikovati samo za konstantni faktor, tj. postoji $\varrho \neq 0$ takav da su jednadžbe (2) i

$$\varrho Ax + \varrho By + \varrho Cz + \varrho D = 0$$

identične. Uspoređivanjem dobivamo

$$\left.\begin{array}{ll} \varrho A & = \cos\alpha \\ \varrho B & = \cos\beta \\ \varrho C & = \cos\gamma \\ \varrho D & = -\delta \end{array}\right\}\,. \tag{13}$$

Kako je uvijek $\delta \geq 0$, iz posljednje relacije (13) zaključujemo da je predznak

$$\operatorname{sign}\varrho = -\operatorname{sign} D\,.$$

Nadalje, jer su $\cos\alpha$, $\cos\beta$, $\cos\gamma$ kosinusi smjera, kvadriranjem i zbrajanjem prvih triju relacija dobivamo

$$\varrho = \frac{1}{-\operatorname{sign} D\,\sqrt{A^2 + B^2 + C^2}}\,. \tag{14}$$

Prema tome, s (14) je dan faktor kojim treba pomnožiti opći oblik jednadžbe ravnine, kako bismo dobili normalni oblik.

Neka je sada s $\vec{n}$ označen vektor dan koordinatama

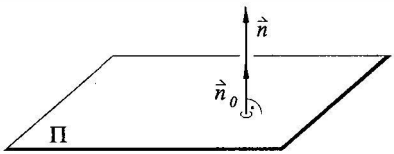
$$\vec{n} = (A, B, C)\,. \tag{15}$$

Iz (13) razabiremo da je

$$\vec{n} = \frac{1}{\varrho}\,\vec{n}_0\,,$$

tj. da je vektor $\vec{n}$ kolinearan s $\vec{n}_0$. Odatle zaključujemo da su koeficijenti A,

B i C u jednadžbi (12) koordinate vektora normale (ne općenito jediničnog)



na ravninu Π. Razabiremo da, zbog (15), opći oblik jednadžbe ravnine (12) možemo pisati kraće kao

$$\vec{n}\vec{r} + D = 0\,. \tag{16}$$

ZADACI

1. Dokaži da jednadžba ravnine, koja prolazi točkom $T_0 = (x_0, y_0, z_0)$ i okomita je na vektor $\vec{n} = (A, B, C)$, ima oblik

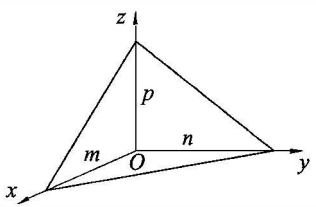
$$A(x - x_0) + B(y - y_0) + C(z - z_0) = 0\,. \tag{17}$$

Koristeći se tom činjenicom, pokaži da je

$$Ax + By + Cz + D = 0\,, \tag{18}$$

uz uvjet da je bar jedan od koeficijenata A, B, C različit od nule, jednadžba neke ravnine u prostoru. [Uputa: Ako je npr. $A \neq 0$, (18) će biti jednadžba ravnine kroz točku $T_0 = (-\frac{D}{A}, 0, 0)$, okomite na vektor (A, B, C).]

2. Neka su m,n i p segmenti koje ravnina odsijeca na koordinatnim osima.



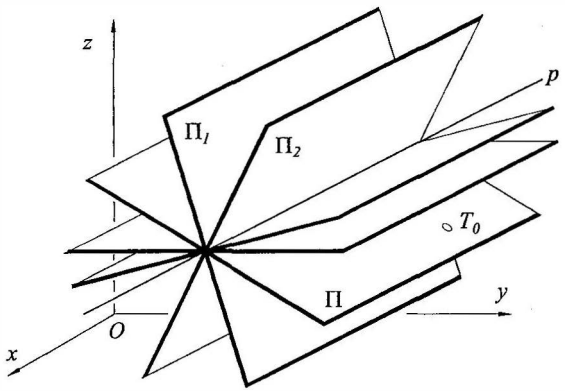
Pokaži da jednadžba te ravnine glasi

$$\frac{x}{m} + \frac{y}{n} + \frac{z}{p} = 1\,. \tag{19}$$

To je tzv. **segmentni oblik** jednadžbe ravnine. Kakva je veza između općeg i segmentnog oblika jednadžbe ravnine?

3. Koristeći se s (19), odredi jednadžbe ravnina koje su paralelne s koordinatnim osima, odnosno koordinatnim ravninama.

4. Pod **sveskom (pramenom) ravnina** razumijevamo sve ravnine prostora koje prolaze istim pravcem p, tzv. **osi sveska**. Očito je da je sve-



zak ravnina određen s dvije svoje ravnine, kažimo Π_1 i Π_2. Neka su te ravnine dane svojim jednadžbama

$$\Pi_i \ \ldots \ \vec{n}_i\vec{r} + D_i = 0\,, \quad i = 1, 2\,.$$

Onda je

$$\lambda_1(\vec{n}_1\vec{r} + D_1) + \lambda_2(\vec{n}_2\vec{r} + D_2) = 0 \tag{20}$$

jednadžba sveska ravnina u tom smislu da za svaki izbor $\lambda_1, \lambda_2 \in \mathbb{R}$, u kojem je bar jedan λ_i različit od nule, (20) predočuje jednadžbu neke ravnine sveska i obratno, za svaku se ravninu sveska mogu odabrati λ_1, λ_2 tako da (20) bude jednadžba upravo te ravnine. Dokaži tu tvrdnju i napiši jednadžbu (20) koordinatno.

5. Dokaži: Tri ravnine

$$\Pi_i \ \ldots \ \vec{n}_i\vec{r} + D_i = 0\,, \quad i = 1, 2, 3$$

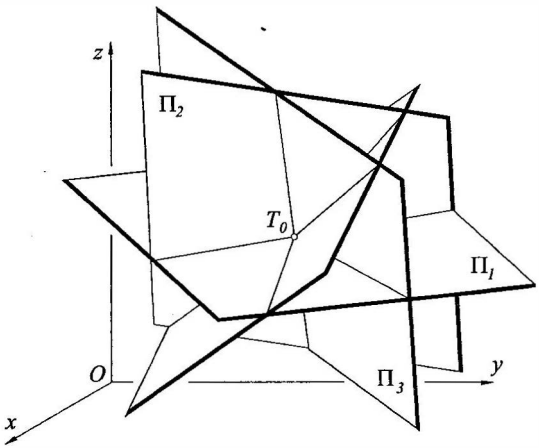
pripadaju istom svesku ako i samo ako je mješoviti produkt

$$(\vec{n}_1, \vec{n}_2, \vec{n}_3) = 0\,.$$

6. Pod **svežnjem (snopom) ravnina** razumijevamo skup svih ravnina prostora, koje prolaze istom točkom T_0, tzv. **vrhom svežnja**. Neka je $\vec{r}_0$ radijvektor točke T_0. Onda je, uz varijabilni vektor $\vec{n}$,

$$\vec{n}(\vec{r} - \vec{r}_0) = 0 \tag{21}$$

jednadžba svežnja ravnina. Dokaži, te napiši jednadžbu (21) koordinatno.



7. Svežanj ravnina određen je i s tri svoje ravnine (jer one određuju jednu točku). Ako su

$$\Pi_i \ \ldots \ \vec{n}_i\vec{r} + D_i = 0\,, \quad i = 1,2,3$$

jednadžbe tih ravnina, pokaži da se jednadžba svežnja ravnina može napisati u obliku

$$\lambda_1(\vec{n}_1\vec{r} + D_1) + \lambda_2(\vec{n}_2\vec{r} + D_2) + \lambda_3(\vec{n}_3\vec{r} + D_3) = 0\,,$$

gdje su $\lambda_i \in \mathbb{R}$, $i = 1, 2, 3$, varijabilni parametri, od kojih je bar jedan različit od nule.

8. Nađi nužan i dovoljan uvjet da četiri ravnine pripadaju istom svežnju.

9. Nađi normalnu jednadžbu pravca u ravnini i jednadžbu pravca kroz dvije točke. Pokaži da je

$$Ax + By + C = 0\,,$$

uz uvjet da je bar jedan od koeficijenata A, B različit od nule, jednadžba nekog pravca u ravnini. To je opći oblik jednadžbe pravca.

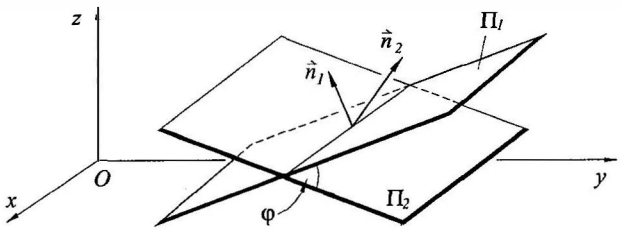
6.4. Kut dviju ravnina

Neka su u prostoru dane dvije ravnine Π_1 i Π_2. Onda pod kutom $\varphi = \sphericalangle(\Pi_1, \Pi_2)$ razumijevamo mjerni broj manjeg od dvaju suplementarnih kutova koje one zatvaraju. Primijetimo da je po toj definiciji uvijek $\varphi \leq \pi/2$.

Neka su ravnine Π_i, $i = 1, 2$, dane u odnosu na koordinatni sustav svojim jednadžbama u općem obliku

$$\Pi_i \ \ldots \ \vec{n}_i\vec{r} + D_i = 0 \,,$$

gdje je $\vec{n}_i = (A_i, B_i, C_i)$ vektor normale na ravninu Π_i.



Onda je

$$\varphi = \sphericalangle(\vec{n}_1, \vec{n}_2)$$

ili

$$\varphi = \pi - \sphericalangle(\vec{n}_1, \vec{n}_2) \,.$$

U svakom slučaju imamo, dakle,

$$\cos\varphi = \frac{|\vec{n}_1\vec{n}_2|}{|\vec{n}_1| \cdot |\vec{n}_2|} \,, \tag{1}$$

odnosno

$$\cos\varphi = \frac{|A_1A_2 + B_1B_2 + C_1C_2|}{\sqrt{A_1^2 + B_1^2 + C_1^2}\sqrt{A_2^2 + B_2^2 + C_2^2}} \,, \tag{2}$$

i to je formula za izračunavanje kuta između dviju ravnina. Uočimo da je uvijek $\cos\varphi \geq 0$, dakle $\varphi \leq \pi/2$, kako definicija i traži.

Iz (2) neposredno slijedi da je nuždan i dovoljan uvjet za **okomitost dviju ravnina** dan s

$$A_1A_2 + B_1B_2 + C_1C_2 = 0 \,. \tag{3}$$

Ako su pak ravnine Π_1 i Π_2 paralelne, onda su vektori normale $\vec{n}_1$ i $\vec{n}_2$ kolinearni, tj.

$$\vec{n}_1 = \lambda\,\vec{n}_2,$$

pa je nuždan i dovoljan uvjet za **paralelnost ravnina** dan s

$$A_1 \,:\, B_1 \,:\, C_1 = A_2 \,:\, B_2 \,:\, C_2. \tag{4}$$

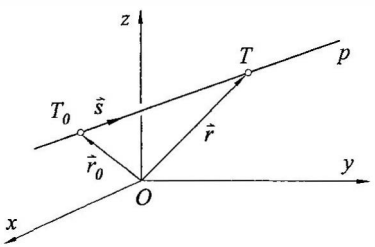
ZADACI

1. Ako su u ravnini dana dva pravca svojim jednadžbama u općem obliku, nađi formulu za kut između tih pravaca. Koji su uvjeti za okomitost odnosno paralelnost pravaca?

6.5. Analitička predočenja pravca

Postoje razna analitička predočenja pravca u E^3, već prema tome kojim je elementima fiksiran njegov položaj u odnosu na koordinatni sustav.

Neka je npr. položaj pravca $p \subset E^3$ određen podacima da prolazi točkom



T_0 i da je istog smjera kao zadani vektor $\vec{s}$. Ako je sada $T \in p$ bilo koja točka na pravcu, imamo

$$[\overrightarrow{OT}] = [\overrightarrow{OT_0}] + [\overrightarrow{T_0T}] .$$

Kako je očito

$$[\overrightarrow{T_0T}] = \lambda\vec{s} ,$$

imamo konačno

$$\vec{r} = \vec{r}_0 + \lambda\vec{s} . \tag{1}$$

Za svaku točku $T \in p$ postoji, dakle, jedinstveni $\lambda \in \mathbb{R}$, takav da je s (1) dan radijvektor te točke; i obratno, za svaki λ je (1) radijvektor neke točke pravca p. Tako je, uz varijabilni λ, (1) analitičko predočenje pravca p, tzv. **parametarska jednadžba pravca u vektorskom obliku**.

Ako su, u odnosu na dani sustav,

$$\begin{aligned} \vec{r}_0 &= (x_0, y_0, z_0) = T_0 , \\ \vec{s} &= (\alpha, \beta, \gamma) , \end{aligned}$$

iz (1) dobivamo

$$\left.\begin{aligned} x &= x_0 + \lambda\alpha \\ y &= y_0 + \lambda\beta \\ z &= z_0 + \lambda\gamma \end{aligned}\right\} , \tag{2}$$

i to su **parametarske jednadžbe pravca** p (u skalarnom obliku).

Ako želimo uvjet kojemu moraju udovoljavati radijvektori odnosno koordinate točaka na pravcu, bez posredovanja parametra λ, moramo iz (1), odnosno (2), taj parametar eliminirati. No, iz (1) imamo

$$\vec{r} - \vec{r}_0 = \lambda\vec{s}$$

pa množenjem vektorski sa $\vec{s}$ dobivamo

$$(\vec{r}-\vec{r}_0)\times\vec{s}=\vec{0}\,, \tag{3}$$

i to je tražena veza, tzv. **vektorski oblik normalne jednadžbe pravca**. Pomoću koordinata možemo (3) pisati i kao

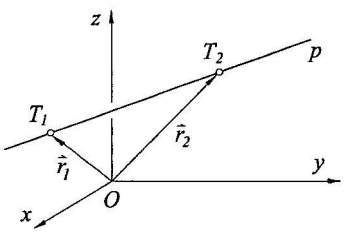
$$\begin{vmatrix} \vec{i} & \vec{j} & \vec{k} \\ x-x_0 & y-y_0 & z-z_0 \\ \alpha & \beta & \gamma \end{vmatrix} = \vec{0}\,,$$

odakle razvijanjem po prvom retku i sređivanjem (sve su koordinate vektora na lijevoj strani jednake nuli!) izlazi

$$\frac{x-x_0}{\alpha}=\frac{y-y_0}{\beta}=\frac{z-z_0}{\gamma} \tag{4}$$

i to su tzv. **kanonske** ili **normalne jednadžbe pravca**. Do jednadžbi (4) možemo doći i direktno iz (2), eliminacijom parametra λ.

Neka je sada pravac p zadan kao spojnica dviju točaka, kažimo T_1 i T_2.



Taj će pravac imati isti smjer kao vektor

$$\vec{s}=[\overrightarrow{T_1T_2}]=\vec{r}_2-\vec{r}_1$$

pa prema (1) imamo

$$\vec{r}=\vec{r}_1+\lambda(\vec{r}_2-\vec{r}_1)\,,$$

odnosno

$$\vec{r}=(1-\lambda)\vec{r}_1+\lambda\vec{r}_2\,, \tag{5}$$

i to je (parametarska) **vektorska jednadžba pravca kroz dvije dane točke**. Ako jednadžbu (5) zapišemo koordinatno, tj. u obliku

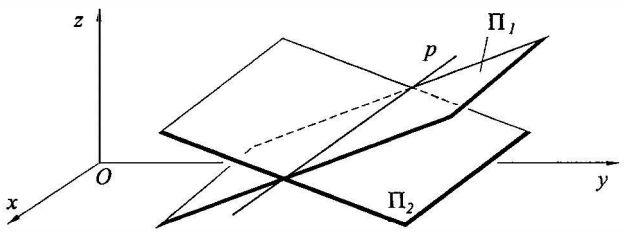
$$\left.\begin{aligned} x &= (1-\lambda)x_1+\lambda x_2 \\ y &= (1-\lambda)y_1+\lambda y_2 \\ z &= (1-\lambda)z_1+\lambda z_2 \end{aligned}\right\}\,, \tag{6}$$

dobivamo **parametarske jednadžbe pravca kroz dvije točke**. Konačno, eliminacijom parametra λ iz (6), dobivamo

$$\frac{x-x_1}{x_2-x_1}=\frac{y-y_1}{y_2-y_1}=\frac{z-z_1}{z_2-z_1}\ , \tag{7}$$

i to su **kanonske** ili **normalne jednadžbe pravca kroz dvije točke**.

Napokon, neka je pravac p zadan kao presječnica dviju ravnina, kažimo



Π_1 i Π_2. Ako su te ravnine dane svojim općim jednadžbama

$$\left.\begin{array}{lll}\Pi_1 & \ldots & \vec{n}_1\vec{r}+D_1=0\\ \Pi_2 & \ldots & \vec{n}_2\vec{r}+D_2=0\end{array}\right\}\ , \tag{8}$$

onda je očito da će točka T ležati na pravcu p onda i samo onda, ako njezin radijvektor zadovoljava obje jednadžbe (8). U tom je smislu sustav (8) analitičko predočenje pravca p, tzv. **vektorski oblik općih jednadžbi pravca**.

Uz pomoć koordinata, (8) možemo pisati kao

$$\left.\begin{array}{l}A_1x+B_1y+C_1z+D_1=0\\ A_2x+B_2y+C_2z+D_2=0\end{array}\right\}\ , \tag{9}$$

gdje, naravno, mora biti ispunjeno

$$A_1 : B_1 : C_1 \neq A_2 : B_2 : C_2\ , \tag{10}$$

jer bi u protivnom ravnine (9) bile paralelne i ne bi određivale pravac. Sustav (9), uz uvjet (10), nazivamo **opće jednadžbe pravca**.

ZADACI

1. Pokaži da se pravac u prostoru može analitički predočiti kao

$$\left.\begin{array}{ll}x & =Kz+L\\ y & =Mz+N\end{array}\right\}\ , \tag{11}$$

gdje su $K, L, M, N \in \mathbb{R}$, tj. kao presjek dviju ravnina od kojih je jedna paralelna s osi y, a druga s osi x. Sustav (11) nazivamo **reducirane jednadžbe pravca**. Naziv potječe odatle što je u predočenju (11) broj konstanti kojima je određen položaj pravca sveden na minimum. Kako vidimo, pravac je određen s 4 realna broja, tj. skup svih pravaca u prostoru predstavlja jednu **četveroparametarsku** familiju (pa se kaže da je skup svih pravaca u E^3 četverodimenzionalan). Uređenu četvorku (K, L, M, N) nazivamo i **koordinatama danog pravca**.

2. Nađi veze između pojedinih oblika analitičkih predočenja pravca. Posebice, ako je pravac zadan svojim općim jednadžbama, nađi njegove reducirane, kanonske, odnosno parametarske jednadžbe.

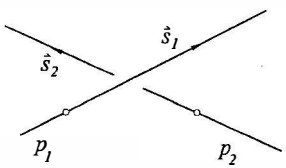
3. Pod **snopom pravaca** u prostoru razumijevamo skup svih pravaca iz E^3 koji prolaze danom točkom $T_0 \in E^3$. Pokaži da je analitičko predočenje snopa dano s

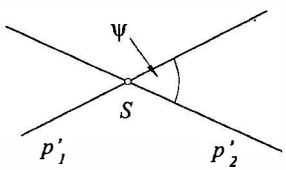
$$(\vec{r} - \vec{r}_0) \times \vec{s} = \vec{0}\,,$$

uz varijabilni vektor $\vec{s}$. Napiši tu jednadžbu skalarno.

6.6. Kut dvaju pravaca. Kut pravca i ravnine

Neka su p_1 i p_2 dva pravca u E^3. Onda pod **kutom** $\psi = \sphericalangle(p_1, p_2)$ tih **pravaca** razumijevamo mjerni broj manjeg od dva suplementarna kuta, koje





zatvaraju pravci paralelni zadanima, a koji prolaze istom točkom. Tako je uvijek $\psi \leq \pi/2$.

Ako su pravci dani analitički s

$$p_i \ldots \vec{r} = \vec{r}_i + \lambda \vec{s}_i, \quad i = 1, 2\,,$$

onda je

$$\psi = \begin{cases} \sphericalangle(\vec{s}_1, \vec{s}_2) & , \text{ ako je } \quad \sphericalangle(\vec{s}_1, \vec{s}_2) \leq \pi/2 \\ \pi - \sphericalangle(\vec{s}_1, \vec{s}_2) & , \text{ ako je } \quad \sphericalangle(\vec{s}_1, \vec{s}_2) > \pi/2 \end{cases}.$$

U svakom je, dakle, slučaju

$$\cos\psi = |\cos(\vec{s}_1, \vec{s}_2)| ,$$

tj.

$$\cos\psi = \frac{|\vec{s}_1 \cdot \vec{s}_2|}{|\vec{s}_1| \cdot |\vec{s}_2|} . \tag{1}$$

Ako su vektori smjera $\vec{s}_i$ dani svojim koordinatama

$$\vec{s}_i = (\alpha_i, \beta_i, \gamma_i), \quad i = 1, 2 ,$$

(1) možemo pisati kao

$$\cos\psi = \frac{|\alpha_1\alpha_2 + \beta_1\beta_2 + \gamma_1\gamma_2|}{\sqrt{\alpha_1^2 + \beta_1^2 + \gamma_1^2}\sqrt{\alpha_2^2 + \beta_2^2 + \gamma_2^2}} , \tag{2}$$

i to je formula za računanje kuta dvaju pravaca.

Specijalno, pravci će biti **okomiti** onda i samo onda ako je

$$\alpha_1\alpha_2 + \beta_1\beta_2 + \gamma_1\gamma_2 = 0 , \tag{3}$$

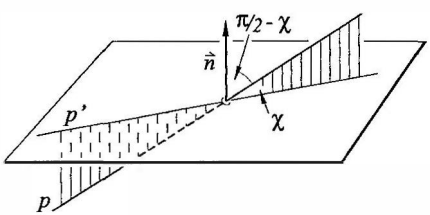
a **paralelni** ako je

$$\vec{s}_2 = \lambda\vec{s}_1 ,$$

dakle, uz uvjet

$$\alpha_1 : \beta_1 : \gamma_1 = \alpha_2 : \beta_2 : \gamma_2 . \tag{4}$$

Neka je sada u prostoru dan pravac p i ravnina Π. **Kut** $\chi = \sphericalangle(p, \Pi)$ **pravca i ravnine** onda definiramo kao kut između pravca p i ortogonalne projekcije p' pravca p na ravninu Π. Primijetimo da smo tako kut pravca i ravnine sveli na kut dvaju pravaca koji je definiran prije, i da je zbog toga uvijek $\chi \leq \pi/2$.



Neka su pravac i ravnina dani analitički s

$$\begin{aligned} p \quad &\ldots \quad \vec{r} = \vec{r}_0 + \lambda\vec{s} , \\ \Pi \quad &\ldots \quad \vec{n}\vec{r} + D = 0 . \end{aligned}$$

Razabiremo odmah da je

$$\cos(\frac{\pi}{2} - \chi) = |\cos(\vec{s}, \vec{n})| = \frac{|\vec{s} \cdot \vec{n}|}{|\vec{s}| \cdot |\vec{n}|} ,$$

dakle

$$\sin \chi = \frac{|\vec{s} \cdot \vec{n}|}{|\vec{s}| \cdot |\vec{n}|} , \tag{5}$$

odnosno, ako su vektori $\vec{s}$ i $\vec{n}$ dani svojim koordinatama,

$$\sin \chi = \frac{|\alpha A + \beta B + \gamma C|}{\sqrt{\alpha^2 + \beta^2 + \gamma^2}\sqrt{A^2 + B^2 + C^2}} , \tag{6}$$

i to je formula za kut pravca i ravnine.

Specijalno, pravac i ravnina će biti **paralelni** ako je $\chi = 0$, dakle uz uvjet

$$\alpha A + \beta B + \gamma C = 0 , \tag{7}$$

a **okomiti** ako je

$$\alpha : \beta : \gamma = A : B : C . \tag{8}$$

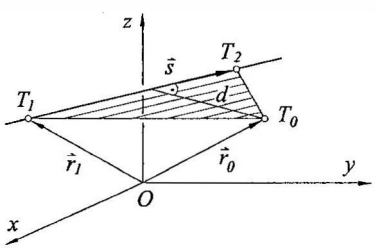
ZADACI

1. Nađi uvjet za okomitost i paralelnost pravaca ako su pravci zadani svojim općim jednadžbama.

2. Kako glase uvjeti za paralelnost, odnosno okomitost pravca i ravnine, ako je pravac dan općim jednadžbama?

6.7. Udaljenost točke od pravca

Neka je u prostoru dan pravac p i točka T_0 izvan njega. Želimo naći udaljenost $d = d(T_0, p)$ te točke od pravca, tj. duljinu okomice spuštene iz T_0



na p.

Neka je pravac dan s

$$p \ldots \vec{r} = \vec{r}_1 + \lambda \vec{s}\,,$$

a točka T_0 neka je zadana svojim radijvektorom $\vec{r}_0$. Neka je $T_2 \in p$ odabrana tako da je $[\overrightarrow{T_1T_2}] = \vec{s}$.

Udaljenost d ćemo izračunati jednim trikom, tj. tako da površinu trokuta $T_0T_1T_2$ izračunamo na dva načina. Najprije elementarno geometrijski imamo

$$P = \frac{1}{2}(\text{baza} \times \text{visina}) = \frac{1}{2}|\vec{s}| \cdot d\,, \tag{1}$$

ali također i

$$P = \frac{1}{2}|[\overrightarrow{T_1T_0}] \times [\overrightarrow{T_1T_2}]| = \frac{1}{2}|(\vec{r}_0 - \vec{r}_1) \times \vec{s}|\,. \tag{2}$$

Uspoređivanjem (1) i (2) onda dobivamo

$$d = \frac{|(\vec{r}_0 - \vec{r}_1) \times \vec{s}|}{|\vec{s}|}\,, \tag{3}$$

i to je tražena formula za udaljenost. Uz uvođenje pokrata

$$X = \begin{vmatrix} y_0 - y_1 & z_0 - z_1 \\ \beta & \gamma \end{vmatrix}, \quad Y = \begin{vmatrix} z_0 - z_1 & x_0 - x_1 \\ \gamma & \alpha \end{vmatrix},$$

$$Z = \begin{vmatrix} x_0 - x_1 & y_0 - y_1 \\ \alpha & \beta \end{vmatrix},$$

tu formulu možemo pisati pomoću koordinata kao

$$d = \sqrt{\frac{X^2 + Y^2 + Z^2}{\alpha^2 + \beta^2 + \gamma^2}}\,. \tag{4}$$

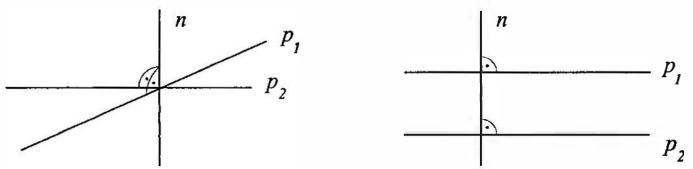
ZADACI

1. Karakteriziraj pravac p kao skup svih točaka prostora za koje je udaljenost od pravca p jednaka nuli, pa iz (4) izvedi kanonske jednadžbe pravca.

2. Neka je $d(T, T_0)$ udaljenost točke T_0 od točke $T \in p$. Pokaži analitički da je
$$d(T_0, p) = \min\{d(T, T_0) \mid T \in p\}\,.$$

6.8. Zajednička normala i najkraća udaljenost dvaju pravaca

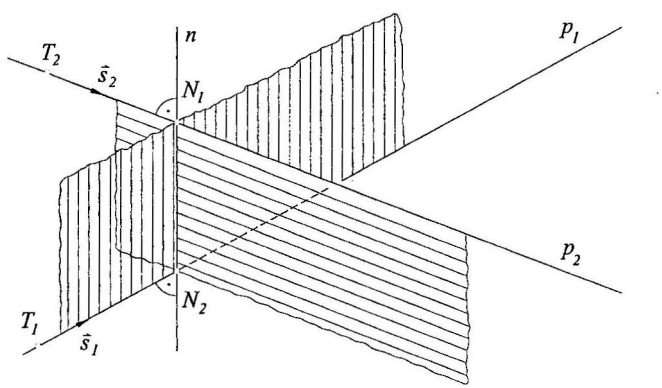
Jasno je da dva pravca koji se sijeku ili su paralelni imaju **zajedničku normalu**, tj. pravac koji siječe oba pravca i okomit je na njih. Intuitivno



je manje jasno, ali se lako može dokazati (Zad.1.), da i dva mimosmjerna pravca p_1 i p_2 imaju jedinstvenu zajedničku normalu. Neka su pravci dani analitički s

$$p_i \ \ldots \ \vec{r} = \vec{r}_i + \lambda \vec{s}_i, \quad i = 1, 2 \ . \tag{1}$$

Želimo naći analitičko predočenje zajedničke normale n. Kako po definiciji



pravac n mora biti okomit na p_1 i p_2, to je vektor $\vec{s}$ smjera zajedničke normale očito dan sa

$$\vec{s} = \vec{s}_1 \times \vec{s}_2 \ . \tag{2}$$

Primijetimo, nadalje, da se pravci p_1 i n sijeku, pa prema tome određuju neku ravninu Π_1. Ta ravnina prolazi točkom T_1 i razapeta je vektorima $\vec{s}_1$ i $\vec{s}$ pa, prema (7) u 6.3., ima jednadžbu

$$(\vec{r} - \vec{r}_1, \vec{s}_1, \vec{s}) = 0 \ . \tag{3}$$

Analogno, pravci p_2 i n se sijeku pa određuju ravninu Π_2, kojoj je jednadžba

$$(\vec{r} - \vec{r}_2, \vec{s}_2, \vec{s}) = 0 \ . \tag{4}$$

No, iz konstrukcije je očito da je

$$n = \Pi_1 \cap \Pi_2 ,$$

tj. normala n je određena kao presjek dviju ravnina te zbog (2), (3) i (4) ima analitičko predočenje

$$\left.\begin{aligned}(\vec{r} - \vec{r}_1, \vec{s}_1, \vec{s}_1 \times \vec{s}_2) = 0 \\ (\vec{r} - \vec{r}_2, \vec{s}_2, \vec{s}_1 \times \vec{s}_2) = 0\end{aligned}\right\} . \tag{5}$$

Odmah se vidi da je sustav (5) i analitičko predočenje zajedničke normale dvaju pravaca koji se sijeku.

Pod **najkraćom udaljenošću dvaju pravaca** razumijevamo broj $d = d(p_1, p_2)$ definiran kao

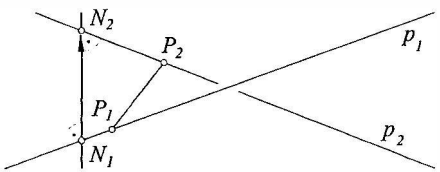
$$d = \inf\{d(P_1, P_2) \mid P_1 \in p_1, P_2 \in p_2\} .$$

Neka su s N_1 i N_2 označena nožišta zajedničke normale n na pravcima p_1, odnosno p_2, $N_i = p_i \cap n$, $i = 1, 2$. Onda tvrdimo da je

$$d = d(N_1, N_2) , \tag{6}$$

tj. da je najkraća udaljenost pravaca p_1 i p_2 jednaka upravo udaljenosti tih nožišta.

Zaista, neka je $P_i \in p_i$, $i = 1, 2$, bilo koji izbor točaka na pravcu p_1, odnosno p_2. Neka je s $\vec{r}_3$ označen radijvektor točke N_1, a s $\vec{r}_4$ radijvektor



točke N_2. Onda su radijvektori točaka P_1 i P_2 dani s

$$[\overrightarrow{OP_1}] = [\overrightarrow{ON_1}] + [\overrightarrow{N_1P_1}] = \vec{r}_3 + \lambda_1\vec{s}_1 ,$$

$$[\overrightarrow{OP_2}] = [\overrightarrow{ON_2}] + [\overrightarrow{N_2P_2}] = \vec{r}_4 + \lambda_2\vec{s}_2$$

i odatle

$$[\overrightarrow{P_1P_2}] = (\vec{r}_4 + \lambda_2\vec{s}_2) - (\vec{r}_3 + \lambda_1\vec{s}_1) .$$

Prema tome je

$$d(P_1, P_2) = |[\overrightarrow{P_1P_2}]| = |(\vec{r}_4 - \vec{r}_3) + (\lambda_2\vec{s}_2 - \lambda_1\vec{s}_1)| ,$$

dakle

$$\begin{aligned}[d(P_1,P_2)]^2 &= (\vec{r}_4-\vec{r}_3)^2+2\lambda_2(\vec{r}_4-\vec{r}_3)\vec{s}_2- \\ &- 2\lambda_1(\vec{r}_4-\vec{r}_3)\vec{s}_1+(\lambda_2\vec{s}_2-\lambda_1\vec{s}_1)^2\ .\end{aligned}$$

Ali $\vec{r}_4-\vec{r}_3=[\overrightarrow{N_1N_2}]$, a kako je taj vektor okomit na $\vec{s}_1$ i $\vec{s}_2$, ostaje

$$[d(P_1,P_2)]^2=[d(N_1,N_2)]^2+(\lambda_2\vec{s}_2-\lambda_1\vec{s}_1)^2$$

i prema tome je

$$d(P_1,P_2)\geq d(N_1,N_2)\ , \tag{7}$$

što pokazuje da je zaista $d(N_1,N_2)$ infimum udaljenosti točaka s pravca p_1 od točaka pravca p_2, tj. tvrdnja (6) je provjerena.

Primijetimo da će u (7) vrijediti znak jednakosti onda i samo onda kad je

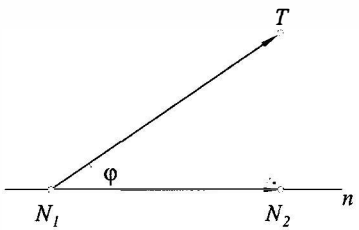
$$\lambda_2\vec{s}_2=\lambda_1\vec{s}_1\ ,$$

a to će, u slučaju kad pravci p_1 i p_2 nisu paralelni, biti ako i samo ako je

$$\lambda_1=\lambda_2=0\ ,$$

dakle kada je $P_1=N_1$, $P_2=N_2$.

Želimo sada naći formulu za računanje najkraće udaljenosti d pravaca p_1 i p_2, uz pretpostavku da su ti pravci dani svojim jednadžbama (1). Uočimo najprije da je N_i ortogonalna projekcija točke T_i na pravac n. Onda je, dakako, orijentirana dužina $\overrightarrow{N_1N_2}$ ortogonalna projekcija orijentirane dužine $\overrightarrow{T_1T_2}$ na pravac n. Neka je $\overrightarrow{N_1T}$ reprezentant vektora $[\overrightarrow{T_1T_2}]$ s početkom u točki N_1. Onda imamo (vidi sliku)



$$\begin{aligned}d &= d(N_1,N_2)=|[\overrightarrow{N_1N_2}]|=|[\overrightarrow{N_1T}]|\cos\varphi= \\ &= |[\overrightarrow{N_1T}]|\cdot|\vec{s}_0|\cos\varphi=|[\overrightarrow{T_1T_2}]|\cdot|\vec{s}_0|\cos\varphi= \\ &= [\overrightarrow{T_1T_2}]\cdot\vec{s}_0=(\vec{r}_2-\vec{r}_1)\vec{s}_0\ ,\end{aligned}$$

gdje je $\vec{s}_0$ jedinični vektor u smjeru pravca n,

$$\vec{s}_0 = \frac{\vec{s}_1 \times \vec{s}_2}{|\vec{s}_1 \times \vec{s}_2|} \ .$$

Zato je konačno

$$d = (\vec{r}_2 - \vec{r}_1) \cdot \frac{\vec{s}_1 \times \vec{s}_2}{|\vec{s}_1 \times \vec{s}_2|}$$

ili

$$d = \frac{(\vec{r}_2 - \vec{r}_1, \vec{s}_1, \vec{s}_2)}{\sqrt{(\vec{s}_1 \times \vec{s}_2)^2}} \ , \tag{8}$$

i to je tražena formula za udaljenost dvaju pravaca. U koordinatnom obliku tu formulu možemo pisati kao

$$d = \frac{\begin{vmatrix} x_2 - x_1 & y_2 - y_1 & z_2 - z_1 \\ \alpha_1 & \beta_1 & \gamma_1 \\ \alpha_2 & \beta_2 & \gamma_2 \end{vmatrix}}{\sqrt{(\alpha_1^2 + \beta_1^2 + \gamma_1^2)(\alpha_2^2 + \beta_2^2 + \gamma_2^2) - (\alpha_1\alpha_2 + \beta_1\beta_2 + \gamma_1\gamma_2)^2}} \ , \tag{9}$$

gdje smo nazivnik pojednostavnili upotrebom Lagrangeova identiteta (vidi Zad. 2. u 5.11.).

Primijetimo i ovo: Ako se pravci p_1 i p_2 sijeku, bit će $d = d(p_1, p_2) = 0$, odnosno, zbog (8),

$$(\vec{r}_2 - \vec{r}_1, \vec{s}_1, \vec{s}_2) = 0 \ . \tag{10}$$

Ako su pak ti pravci paralelni, bit će $\vec{s}_1 = \lambda \vec{s}_2$, pa će (10) također biti ispunjeno. Prema tome, ako dva pravca leže u istoj ravnini, mora vrijediti (10). Obratno, ako je ispunjeno (10), vektori $\vec{r}_1 - \vec{r}_2$, $\vec{s}_1$ i $\vec{s}_2$ su komplanarni; odatle odmah zaključujemo da pravci p_1 i p_2 leže u istoj ravnini. Prema tome je (10), odnosno u koordinatnom obliku

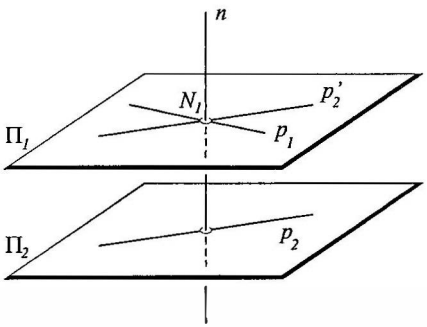
$$\begin{vmatrix} x_2 - x_1 & y_2 - y_1 & z_2 - z_1 \\ \alpha_1 & \beta_1 & \gamma_1 \\ \alpha_2 & \beta_2 & \gamma_2 \end{vmatrix} = 0 \ ,$$

nuždan i dovoljan uvjet da bi dva pravca ležala u istoj ravnini, tj. **uvjet za komplanarnost dvaju pravaca**.

ZADACI

1. Dokaži geometrijski egzistenciju i jedinstvenost zajedničke normale dvaju mimosmjernih pravaca. [Uputa: Pokaži da takvi pravci, p_1 i p_2, nužno leže u paru paralelnih ravnina Π_1 i Π_2. Neka je p_2' ortogonalna projekcija od p_2 na Π_1 i $N_1 = p_1 \cap p_2'$. Onda je pravac n kroz N_1, okomit na Π_1, zajednička normala. Kad bi postojale dvije normale, n_1 i n_2, bilo bi $n_1 \parallel n_2$, pa bi p_1 i p_2 ležali u jednoj ravnini, protivno

pretpostavci.]



2. Napiši analitičko predočenje (5) zajedničke normale u koordinatnom obliku. Nađi parametarske i kanonske jednadžbe te normale.

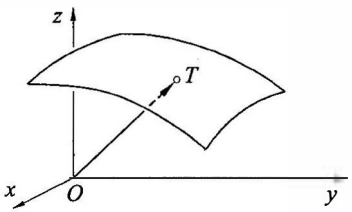
6.9. Analitičko predočenje ploha. Plohe 2. reda

Detaljnije će o fundiranju pojma plohe biti govora u drugim matematičkim disciplinama. Ovdje ćemo kazati samo nekoliko riječi, oslanjajući se na intuitivnu predodžbu.

Neka je

$$\vec{r} = \vec{r}(u, v) \tag{1}$$

vektorska funkcija, neprekidna u dvije (realne) varijable u, v. Ako za svaki izbor $u, v \in \mathbb{R}$ interpretiramo (1) kao radijvektor neke točke, uz varijabilne parametre u i v dobit ćemo u prostoru jednu dvoparametarsku familiju to-



čaka (dvodimenzionalni kontinuum!), koju nazivamo **ploha**. U tom slučaju kažemo da je (1) **vektorska jednadžba** te **plohe**.

Ako (1) pišemo koordinatno

$$\left.\begin{aligned} x &= f(u, v) \\ y &= g(u, v) \\ z &= h(u, v) \end{aligned}\right\}, \tag{2}$$

dobivamo tzv. **parametarske jednadžbe plohe**. Ako iz jednadžbe (2) eliminiramo parametre u i v, dobivamo

$$z = \varphi(x, y) \tag{3}$$

kao **eksplicitni**, odnosno

$$F(x, y, z) = 0 \tag{4}$$

kao **implicitni oblik jednadžbe plohe**. Na primjer, (4) je jednadžba plohe u tom smislu da je to nuždan i dovoljan uvjet kojemu moraju udovoljavati koordinate točaka na danoj plohi.

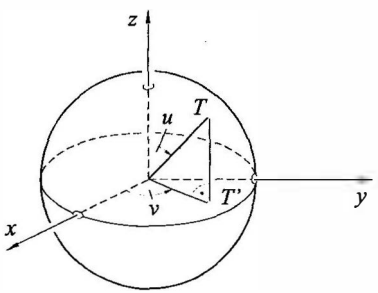
PRIMJERI

1. **Ravnina**. Kako smo vidjeli, svaka se ravnina može analitički predočiti s

   $$Ax + By + Cz + D = 0\,,$$

   tj. linearnom jednadžbom tipa (4).

2. **Sfera**. Kako je $\overline{OT'} = R \cdot \sin u$, gdje je R polumjer sfere (vidi sliku),



   imamo

   $$\begin{aligned} x &= R \sin u \cos v \\ y &= R \sin u \sin v \\ z &= R \cos u \end{aligned}$$

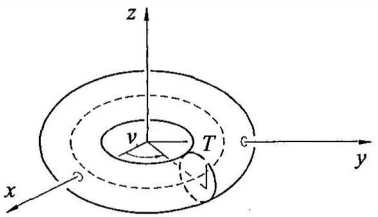
   i to su parametarske jednadžbe sfere. Eliminacijom parametara dobivamo

   $$x^2 + y^2 + z^2 - R^2 = 0,$$

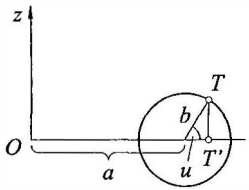
   tj. implicitnu jednadžbu sfere.

3. **Torus**. Neka je s a označen "polumjer" torusa, s b polumjer normalnog presjeka torusa i neka je koordinatni sustav smješten simetrično, kao

na slici.



U ravnini određenoj s osi z i točkom T imamo ovu sliku:



Vidimo da je $\overline{OT'} = a + b\cos u$. Onda lako izlazi da je

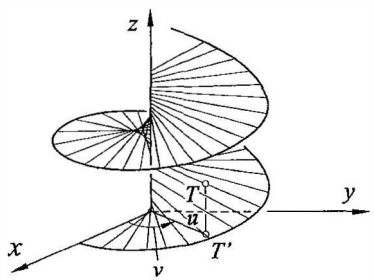
$$\begin{aligned} x &= (a + b\cos u)\cos v \\ y &= (a + b\cos u)\sin v \\ z &= b\sin u \end{aligned}$$

i to su parametarske jednadžbe torusa. Eliminacijom parametara u i v dolazimo do implicitne jednadžbe

$$(x^2 + y^2 + z^2 - a^2 - b^2)^2 - 4a^2(b^2 - z^2) = 0\,,$$

kojom je analitički opisan torus u Kartezijevim koordinatama.

4. **Helikoid** (prema helix – zavoj). Ta je ploha izgrađena od pravaca. Nastaje jednolikom rotacijom pravca i istodobnom translacijom u danom smjeru.



Iz slike vidimo da su

$$\begin{aligned} x &= u\cos v \\ y &= u\sin v \\ z &= cv \end{aligned}$$

parametarske jednadžbe, odnosno

$$y - x\,\mathrm{tg}\,\frac{z}{c} = 0$$

implicitna jednadžba helikoida.

Kažemo da je **ploha algebarska**, odnosno **transcendentna**, već prema tome je li njezino implicitno analitičko predočenje u Kartezijevim koordinatama algebarska ili transcendentna jednadžba. Na primjer, ravnina, sfera i torus su algebarske plohe, a helikoid je transcendentna ploha.

Za algebarsku plohu kažemo da je **reda** n ako je analitički predočena jednadžbom koja je n–tog stupnja u nepoznanicama x, y i z. Na primjer, ravnina je ploha prvog reda, sfera drugog reda, a torus četvrtog reda.

Od posebnog su interesa **plohe 2. reda** ili **kvadrike**. Opća je jednadžba takvih ploha dana s

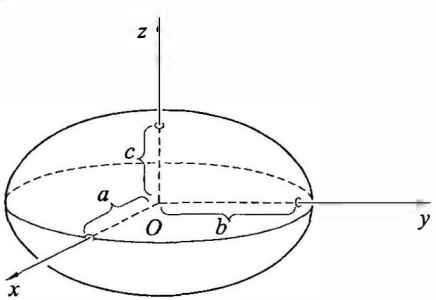
$$Ax^2 + By^2 + Cz^2 + Dyz + Ezx + Fxy + Gx + Hy + Iz + K = 0\,,$$

gdje su koeficijenti $A, \ldots, K \in \mathbb{R}$ i vrijedi da je bar jedan od koeficijenata $A, \ldots, F$ različit od nule (jer bi se u protivnom jednadžba reducirala na linearnu, pa bi to bila jednadžba ravnine).

Ta se jednadžba, međutim, znatno pojednostavnjuje ako izaberemo pogodni sustav, tj. takav koji za svoje elemente (osi i ravnine) rabi elemente simetrije plohe.

Navest ćemo analitička predočenja osnovnih tipova (realnih i nedegeneriranih) ploha 2. reda u njihovu najjednostavnijem, **kanonskom obliku**.

1. **Elipsoid**

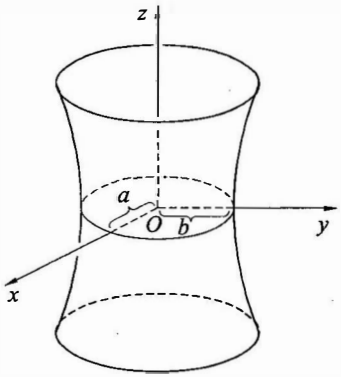


$$\frac{x^2}{a^2} + \frac{y^2}{b^2} + \frac{z^2}{c^2} = 1\,.$$

Uz $a \neq b \neq c$ govorimo o troosnom elipsoidu. Ako je npr. $a = b$, imamo rotacijski elipsoid. Uz $a = b = c$ dobivamo, naravno, sferu.

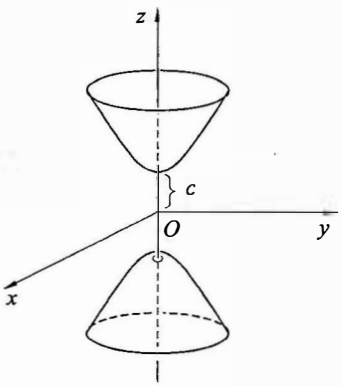
2. **Jednoplohi hiperboloid**

$$\frac{x^2}{a^2}+\frac{y^2}{b^2}-\frac{z^2}{c^2}=1\,.$$



Uz $a=b$ imamo rotacijski jednoplohi hiperboloid.

3. **Dvoplohi hiperboloid**

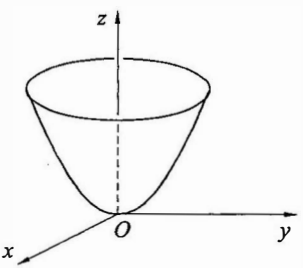


$$-\frac{x^2}{a^2}-\frac{y^2}{b^2}+\frac{z^2}{c^2}=1\,.$$

Za $a=b$ imamo i ovdje rotacijsku plohu.

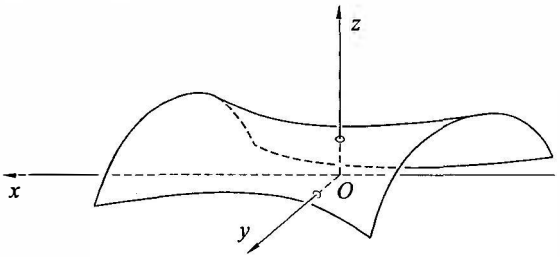
4. **Eliptički paraboloid**

$$\frac{x^2}{a^2}+\frac{y^2}{b^2}=2pz\,.$$



Uz $a=b$ imamo rotacijsku plohu.

5. **Hiperbolički paraboloid**



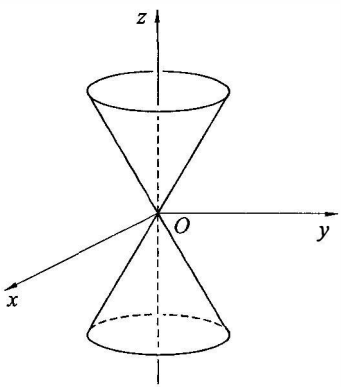
$$\frac{x^2}{a^2} - \frac{y^2}{b^2} = 2pz\,.$$

Ta se ploha iz očitih razloga zove još i "sedlasta ploha".

6. **Konus 2. reda**

Neka je $C \subset E^3$ dana krivulja, a $V \in E^3$ točka koja ne leži na C. Plohu izgrađenu od pravaca koju dobijemo spajanjem točke V sa svim točkama krivulje C nazivamo **konusna ploha** generirana krivuljom C. Ako je C bilo koja krivulja 2. reda, dobivamo:

$$\frac{x^2}{a^2} + \frac{y^2}{b^2} - \frac{z^2}{c^2} = 0$$

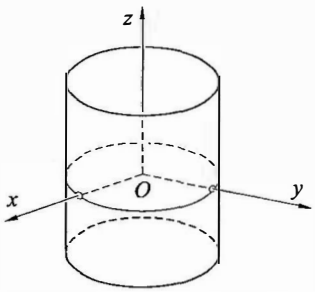


i tu plohu nazivamo **konus 2. reda**. Uz $a = b$ imamo rotacijski konus.

7. **Cilindri 2. reda**

Neka je $C \subset E^3$ bilo koja krivulja i neka je zadan određeni smjer u prostoru. Ploha koju dobijemo tako da svakom točkom krivulje C položimo pravac tog danog smjera nazivamo **cilindrična ploha** generirana krivuljom C. Ako je C krivulja 2. reda, imamo tri tipa takvih ploha:

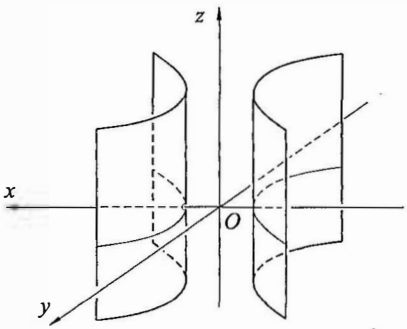
(a) **eliptički cilindar**



$$\frac{x^2}{a^2} + \frac{y^2}{b^2} = 1 .$$

Posebno, za $a = b$ imamo rotacijski cilindar.

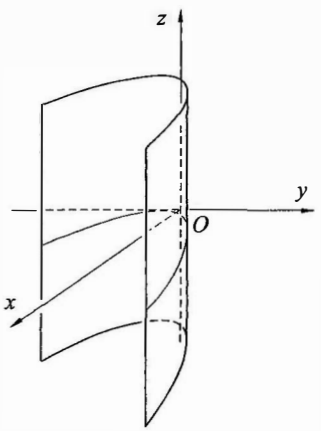
(b) **hiperbolički cilindar**



$$\frac{x^2}{a^2} - \frac{y^2}{b^2} = 1 .$$

(c) **parabolički cilindar**

$$y^2 = 2px .$$



ZADACI

1. Napiši jednadžbu sfere kojoj je središte u točki $S = (x_0, y_0, z_0)$ i polumjer R.

2. Utvrdi što se dobiva kao presjek pojedinih ploha 2. reda i ravnina koje su paralelne s koordinatnim ravninama.

3. Nađi parametarske jednadžbe za svaki od navedenih tipova ploha 2. reda.

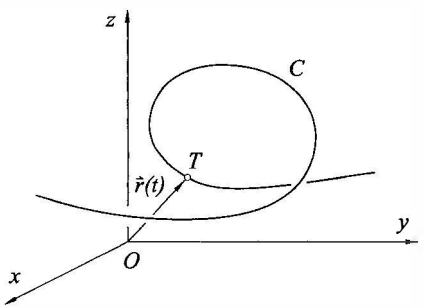
4. Kako smo vidjeli, helikoid je ploha izgrađena od pravaca, tzv. **pravčasta ploha**. Pokaži da su jednoplohi hiperboloid, hiperbolički paraboloid, konus i svi cilindri 2. reda također pravčaste plohe, te da su to jedine pravčaste plohe 2. reda.

6.10. Analitičko predočenje krivulja

Neka je

$$\vec{r} = \vec{r}(t) \tag{1}$$

vektorska funkcija, neprekidna u realnoj varijabli t. Shvaćajući (1) za svaki $t \in \mathbb{R}$ kao radijvektor neke točke u prostoru, dobit ćemo, uz varijabilni t, jednoparametarsku familiju točaka, dakle neku krivulju C u prostoru. Za



(1) kažemo da je **vektorska jednadžba krivulje** C. Pisano u koordinatnoj formi, (1) postaje

$$\left.\begin{aligned} x &= x(t) \\ y &= y(t) \\ z &= z(t) \end{aligned}\right\}, \tag{2}$$

i to su **parametarske jednadžbe krivulje** C. Eliminacijom parametra t dobivamo npr.

$$\left.\begin{aligned} x &= f(z) \\ y &= g(z) \end{aligned}\right\} \tag{3}$$

ili nešto općenitije

$$\left.\begin{aligned} F(x,y,z) &= 0 \\ G(x,y,z) &= 0 \end{aligned}\right\}. \tag{4}$$

Kako svaka od jednadžbi u sustavu (3), odnosno u sustavu (4) predočuje analitički neku plohu, svakim od tih sustava je krivulja C predočena kao

presjek dviju ploha. Posebno s (3) je ta krivulja dana kao presjek dviju cilindričnih ploha. Sustave (3), odnosno (4) nazivamo **opće jednadžbe krivulje** u prostoru.

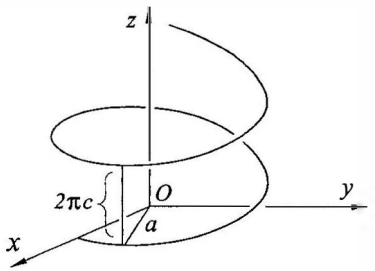
PRIMJERI

1. **Pravac.** Opće jednadžbe pravca,

$$\begin{aligned} A_1x + B_1y + C_1z + D_1 &= 0 \\ A_2x + B_2y + C_2z + D_2 &= 0 \end{aligned} ,$$

jesu, dakako, tipa (4) i određuju pravac kao presječnicu dviju ravnina. Posebno, reducirane jednadžbe pravca su tipa (3).

2. **Cilindrična spirala.** Tu krivulju opisuje točka u prostoru, koja jednoliko rotira u prostoru i istodobno obavlja jednoliku translaciju u danom smjeru.



Njezine su parametarske jednadžbe

$$\begin{aligned} x &= a\cos t \\ y &= a\sin t \\ z &= c\cdot t \ . \end{aligned}$$

Eliminacijom parametra t dobivamo

$$\begin{aligned} x &= a\cos z/c \\ y &= a\sin z/c \ , \end{aligned}$$

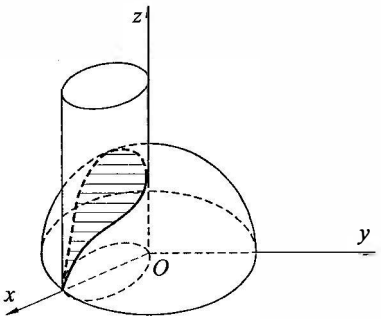
odnosno, ekvivalentno,

$$\begin{aligned} x^2 + y^2 - a^2 &= 0 \\ y - x\ \mathrm{tg}\, z/c &= 0 \ , \end{aligned}$$

što pokazuje da cilindričnu spiralu možemo zadati kao presjek dvaju sinusoidalnih cilindara, odnosno kao presjek kružnog cilindra i helikoida.

3. **Vivianijev prozor.** Ta je krivulja zadana kao presjek sfere i cilindra

(vidi sliku),



pa je njezino analitičko predočenje

$$\begin{aligned} x^2 + y^2 + z^2 - R^2 &= 0 \\ (x - \tfrac{R}{2})^2 + y^2 - \tfrac{R^2}{4} &= 0 \end{aligned} .$$

ZADACI

1. Nađi jednu parametrizaciju (parametarske jednadžbe) za Vivianijev prozor.

2. Krivulja zadana parametarskim jednadžbama

$$\begin{aligned} x &= a \cdot t \\ y &= b \cdot t^2 \\ z &= c \cdot t^3 \end{aligned} ,$$

gdje su $a, b, c \in \mathbb{R}$, naziva se **kubna parabola**. Skiciraj tu krivulju i nađi njezine opće jednadžbe.

3. Predoči analitički krivulje koje se dobivaju kao presjeci pojedinih ploha 2. reda s ravninama paralelnim s koordinatnim ravninama.

6.11. Neki drugi koordinatni sustavi u prostoru

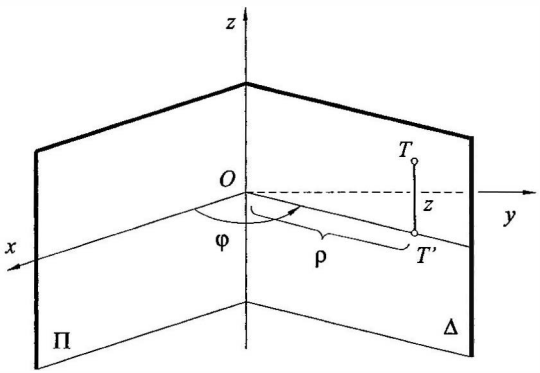
U raznim će nam primjenama osim Kartezijevih koordinata biti od koristi i neke druge koordinate u prostoru.

Cilindrične koordinate

Odaberimo u prostoru bilo koju točku O, orijentirani pravac z koji prolazi točkom O i poluravninu Π omeđenu sa z. Te fiksne elemente nazivamo redom **pol**, **polarna os** i **polarna poluravnina**. Neka je $T \in E^3$ bilo

koja točka, Δ ravnina određena tom točkom i pravcem z, a T' ortogonalna projekcija od T na okomicu u polu koja leži u Δ. Onda definiramo

$$\left.\begin{array}{ll} \varphi & = \sphericalangle(\Pi, \Delta) \\ \varrho & = \overline{OT'} \\ z & = \overline{TT'} \end{array}\right\} . \tag{1}$$



Uređenu trojku

$$(\varphi, \varrho, z) , \tag{2}$$

uz ograničenja

$$\left.\begin{array}{l} 0 \leq \varphi < 2\pi \\ \varrho \geq 0 \end{array}\right\} , \tag{3}$$

nazivamo **cilindrične koordinate** točke T u prostoru, a dane fiksne elemente, uz zakon pridruživanja (1), **cilindrični koordinatni sustav**.

Ako u prostoru odaberemo pravokutni koordinatni sustav u združenom položaju s cilindričnim sustavom (vidi sliku), odmah razabiremo da su veze između pravokutnih i cilindričnih koordinata dane ovim relacijama:

$$\left.\begin{array}{l} x = \varrho \cos\varphi \\ y = \varrho \sin\varphi \\ z = z \end{array}\right\} , \quad \text{odnosno} \quad \left.\begin{array}{l} \varphi = \operatorname{arctg} y/x \\ \varrho = \sqrt{x^2 + y^2} \\ z = z \end{array}\right\} .$$

Sferne koordinate

Odaberimo u prostoru iste fiksne elemente kao za cilindrični sustav. Neka je Δ opet poluravnina kroz danu točku $T \in E^3$ i polarnu os. Onda definiramo

$$\left.\begin{array}{ll} \varphi & = \sphericalangle(\Pi, \Delta) \\ r & = \overline{OT} \\ \vartheta & = \sphericalangle(z, \overline{OT}) \end{array}\right\} \tag{4}$$

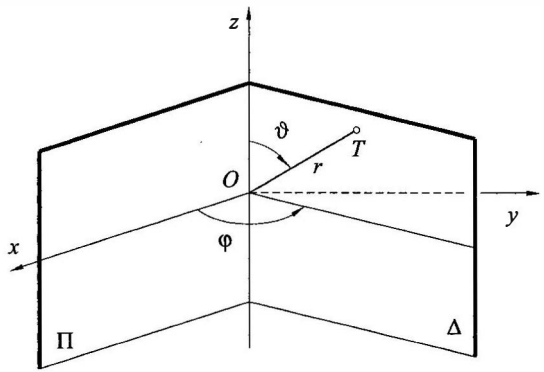
i te brojeve iz tradicionalnih razloga (zbog primjene u astronomiji) nazivamo redom **azimut, radijvektor** i **zenitna distanca točke** T. Uređenu trojku

$$(\varphi, r, \vartheta)\,, \tag{5}$$

uz ograničenje

$$\left.\begin{array}{c} 0 \leq \varphi < 2\pi \\ r \geq 0 \\ 0 \leq \vartheta < \pi \end{array}\right\}\,, \tag{6}$$

nazivamo **sferne koordinate** točke T, a fiksne elemente, zajedno sa zakonom pridruživanja (4), **sfernim koordinatnim sustavom** u prostoru.



Ako odaberemo pravokutni koordinatni sustav u združenom položaju sa sfernim koordinatnim sustavom, veze sfernih i pravokutnih koordinata dane su s

$$\left.\begin{array}{l} x = r\,\sin\vartheta\,\cos\varphi \\ y = r\,\sin\vartheta\,\sin\varphi \\ z = r\,\cos\vartheta \end{array}\right\}\,,$$

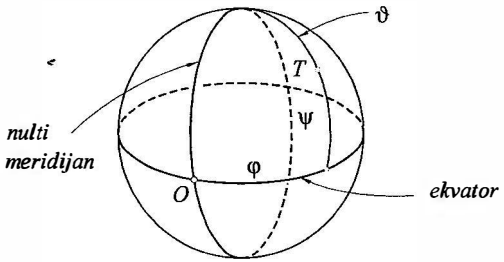
odnosno

$$\left.\begin{array}{rcl} \varphi & = & \operatorname{arctg} y/x \\ r & = & \sqrt{x^2+y^2+z^2} \\ \vartheta & = & \arccos z/\sqrt{x^2+y^2+z^2} \end{array}\right\}\,.$$

Primijetimo da uz $r = const.$ dobivamo u prostoru sferu, a preostale dvije sferne koordinate fiksiraju položaj točke na toj sferi. Standardno definiramo

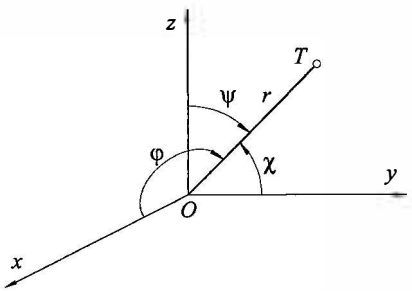
$$\varphi = \text{geografska dužina}\,,$$
$$\psi = \pi/2 - \vartheta = \text{geografska širina}$$

i uređeni par (φ, ψ) nazivamo **geografske koordinate** na sferi.



Polarne koordinate u prostoru

Odaberimo u prostoru fiksnu točku O i tri orijentirana pravca x, y, z kroz tu točku, koji ne leže u istoj ravnini nego su npr. u parovima okomiti.



Točku O nazivamo **pol**, a te pravce **polarne osi**. Za točku $T \in E^3$ onda definiramo:

$$\begin{aligned} r &= \overline{OT}\,, \\ \varphi &= \sphericalangle(x, OT)\,, \\ \psi &= \sphericalangle(y, OT)\,, \\ \chi &= \sphericalangle(z, OT) \end{aligned}$$

i pridružujemo

$$T \mapsto (r, \varphi, \psi, \chi)\,.$$

Uređenu četvorku, uz ograničenje kutova na interval $[0, \pi]$, nazivamo **polarne koordinate** točke T u prostoru. Odmah se vidi da te koordinate nisu nezavisne, nego vezane relacijom

$$\cos^2\varphi + \cos^2\psi + \cos^2\chi = 1\,.$$

Primijetimo da je polarnim koordinatama zapravo opisan radijvektor $\overrightarrow{OT}$ točke T, i to svojim modulom i kosinusima smjera.

ZADACI

1. Nađi veze između Kartezijevih i polarnih koordinata u prostoru.

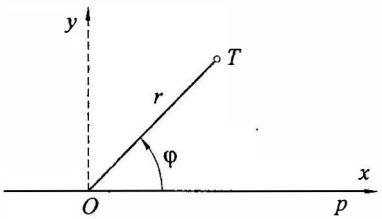
2. Ako je u prostoru dan neki koordinatni sustav, skup točaka koje imaju svojstvo da im je jedna od koordinata konstantna, nazivamo **koordinatna ploha**. Odredi familije koordinatnih ploha u Kartezijevu, cilindričnom i sfernom koordinatnom sustavu.

3. Neka je $\{O;(\vec{i},\vec{j})\}$ pravokutni koordinatni sustav u E^2. U odnosu na taj sustav nađi kanonske jednadžbe nedegeneriranih **krivulja 2. reda** (elipse, hiperbole, parabole), tzv. **konika**.

4. Odaberimo u ravnini točku O i orijentirani pravac p kroz tu točku, **pol** i **polarnu os**. Točki $T \in E^2$ pridružujemo brojeve

$$r = \overline{OT}\,,$$
$$\varphi = \sphericalangle(p, OT)\,.$$

Uređeni par (r,φ), uz ograničenje $r \geq 0$, $0 \leq \varphi < 2\pi$, nazivamo **polarne koordinate** točke T **u ravnini**, a $\{O;p\}$, uz navedeni zakon

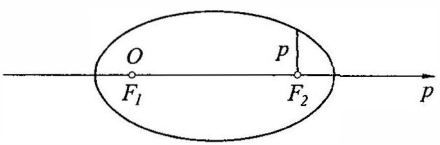


pridruživanja, **polarni koordinatni sustav u ravnini**. Nađi:

(a) veze između polarnih i pravokutnih koordinata, ako su sustavi u združenom položaju (vidi sliku),

(b) jednadžbe pravca i kružnice u polarnim koordinatama.

5. Neka je u ravnini dana krivulja 2. reda (konika) i polarni koordinatni sustav odabran tako da mu je pol u jednom fokusu krivulje, a polarna os se podudara s jednom osi simetrije krivulje (vidi sliku).



Dokaži da u odnosu na taj sustav konika ima jednadžbu

$$r = \frac{p}{1 - \varepsilon \cos \varphi}, \tag{7}$$

gdje je p tzv. parametar, a ε numerički ekscentricitet ($\varepsilon = e/a$). Uoči da gornja jednadžba predočuje elipsu, parabolu ili hiperbolu, već prema tome je li $\varepsilon \gtreqless 1$. Jednadžba se zove **polarna jednadžba konike**.

6. U fiksnoj ravnini Δ u prostoru, koja prolazi kroz polarnu os, cilindrične se koordinate reduciraju na Kartezijeve, a sferne na polarne. Dokaži!

7

LINEARNI PROSTOR

U petom poglavlju smo detaljno izučavali skup V^3 klasa orijentiranih dužina (vektora) u prostoru i konstatirali da u odnosu na operacije zbrajanja vektora i množenja vektora realnim brojevima taj skup postaje struktura, koju smo nazvali vektorski ili linearni prostor.

Kako smo rekli, iste takve strukture pojavljuju se u raznim situacijama u gotovo svim matematičkim disciplinama i primjenama, s time da se od svog osnovnog modela, prostora V^3, razlikuju eventualno u naravi svojih elemenata i prirodi operacija te dimenzionalnim karakteristikama. Ovo je poglavlje posvećeno sustavnom studiranju zajedničkih svojstava svih tih modela, odnosno aksiomatskoj izgradnji teorije linearnih prostora.

Posebno ćemo se baviti konačnodimenzionalnim linearnim prostorima, jer studij beskonačnodimenzionalnih prostora zahtijeva poznavanje mnogih činjenica iz teorije skupova, analize i topologije, što prelazi okvire ove knjige (i izučava se u funkcionalnoj analizi).

7.1. Definicija i osnovna svojstva

Kako smo već skicirali u petom poglavlju, linearni prostor se definira na sljedeći način:

Neka je $V = (V, +)$ aditivno zapisana Abelova grupa, a $F = (F, +, \cdot)$ bilo koje polje. Neka je, nadalje,

$$h : F \times V \to V$$

preslikavanje koje zovemo **vanjsko** ili **hibridno množenje** i kratko označavamo s

$$h(\alpha, a) = \alpha a \ ,$$

i koje ima ova svojstva:

(1) kvaziasocijativnost, tj.

$$\alpha(\beta a) = (\alpha\beta)a\,, \qquad \forall\, \alpha, \beta \in F,\ a \in V\ ;$$

(2) posjedovanje jedinice, tj.

$$1a = a, \qquad \text{za } 1 \in F \quad \text{i} \quad \forall\, a \in V\ ;$$

(3) distributivnost u odnosu na zbrajanje u F

$$(\alpha + \beta)a = \alpha a + \beta a \qquad \forall\, \alpha, \beta \in F,\ a \in V\ ;$$

(4) distributivnost u odnosu na zbrajanje u V

$$\alpha(a + b) = \alpha a + \alpha b, \qquad \forall\, \alpha, \in F,\ a, b \in V\ .$$

Onda uređenu trojku (V, F, h) nazivamo **linearni** ili **vektorski prostor**.

Kaže se još da je V **linearni prostor nad poljem** F, u odnosu na vanjsko množenje h. Elemente od V nazivamo **vektori**. Posebno, nulu te grupe nazivamo **nulvektor** i označavamo sa Θ. Nasuprot tome, elemente polja F zovemo **skalari**, a samo polje F zovemo katkad i **osnovnim poljem** (u kojem nulu i jedinicu označavamo standardno sa 0 i 1).

Ako je specijalno $F = \mathbb{R}$, govorimo o **realnom linearnom prostoru**, a ako je $F = \mathbb{C}$, o **kompleksnom linearnom prostoru**.

NAPOMENA 1

Primijetimo da se nigdje ne tvrdi da su zahtjevi u definiciji, tzv. **aksiomi linearnog prostora**, logički nezavisni. Na primjer, nije potrebno postulirati da je V Abelova grupa jer se iz činjenice da je V grupa i ostalih aksioma komutativnost od V može dokazati. Naime, imamo za $a, b \in V$, koristeći se aksiomima:

$$(1 + 1)(a + b) = 1(a + b) + 1(a + b) = a + b + a + b$$

i

$$(1 + 1)(a + b) = (1 + 1)a + (1 + 1)b = a + a + b + b\,,$$

dakle ,

$$a + b + a + b = a + a + b + b$$

pa dodavanjem $-a$ slijeva i $-b$ zdesna dobivamo

$$b + a = a + b$$

i komutativnost zbrajanja je dokazana.

NAPOMENA 2

Ako se u definiciji linearnog prostora zahtjev da je F polje zamijeni slabijim zahtjevom da je F (komutativni) prsten s jedinicom, dobivamo strukturu koju nazivamo **modul** nad prstenom F ili, kraće, **F-modul**.

Navedimo neke elementarne posljedice definicije linearnog prostora.

PROPOZICIJA 3

Za svaki $a \in V$ vrijedi $0\,a = \Theta$.

Dokaz

Imamo

$$a + \Theta = a = 1\,a = (1+0)a = 1a + 0\,a = a + 0\,a$$

i odatle $0\,a = \Theta$. ■

PROPOZICIJA 4

Za svaki $\alpha \in F$ vrijedi $\alpha\,\Theta = \Theta$.

Dokaz

Neka je $a \in V$ bilo koji vektor. Onda je

$$\Theta + \alpha\,a = \alpha a = \alpha(\Theta + a) = \alpha\,\Theta + \alpha\,a\,,$$

dakle $\alpha\,\Theta = \Theta$. ■

PROPOZICIJA 5

Iz $\alpha a = \Theta$ slijedi da je $\alpha = 0$ ili $a = \Theta$.

Dokaz

Ako je $\alpha = 0$, dokaz je gotov. Uzmimo zato da je $\alpha \neq 0$. Kako je F polje, postoji α^{-1} pa imamo

$$\alpha^{-1}(\alpha a) = \alpha^{-1}\Theta\,.$$

No, zbog (1) i Prop. 4 je

$$(\alpha^{-1}\alpha)a = \Theta\,,$$

dakle

$$1\,a = \Theta$$

i onda, zbog (2),

$$a = \Theta\,,$$

kako se i tvrdilo. ■

Prop. 3, 4 i 5 dakle daju

KOROLAR 6

Jednakost $\alpha a = \Theta$ *vrijedi ako i samo ako je* $a = \Theta$ *ili* $\alpha = 0$. ■

PROPOZICIJA 7

Za svaki izbor $\alpha \in F$ *i* $a \in V$ *je* $(-\alpha)a = -(\alpha a)$.

Dokaz

Imamo

$$\alpha a + (-\alpha)a = [\alpha + (-\alpha)]a = 0\,a = \Theta\,,$$

pa je zaista $(-\alpha)a = -(\alpha a)$. Specijalno je, dakle, $(-1)a = -a$. ■

ZADACI

1. Dokaži da je

$$(\alpha - \beta)a = \alpha a - \beta a, \quad \forall\, \alpha, \beta \in F,\, a \in V\,,$$

$$\alpha(a - b) = \alpha a - \alpha b, \quad \forall\, \alpha, \in F,\, a, b \in V\,.$$

2. U linearnom prostoru vrijedi opći zakon distribucije

$$\left(\sum_{i=1}^{m} \alpha_i\right)\left(\sum_{j=1}^{n} a_j\right) = \sum_{i=1}^{m}\sum_{j=1}^{n} \alpha_i a_j\,.$$

   Dokaži indukcijom!

3. Dokaži da je za svaki $n \in \mathbb{N}$

$$n(\alpha a) = (n\alpha)a\,,$$

   gdje su $\alpha \in F$ i $a \in V$.

4. Neka je F polje karakteristike p. Onda je

$$pa = \Theta\,,$$

   za svaki $a \in V$. Dokaži!

5. Za svaki $\alpha \in F - \{0\}$ definiramo preslikavanje

$$d_\alpha : V \to V$$

   s

$$d_\alpha(a) = \alpha a\,,$$

koje nazivamo **dilatacija** (**homotetija**) u V za faktor α. Pokaži da je d_α automorfizam grupe V. Neka je

$$\mathrm{Dil}\, V = \{d_\alpha \mid \alpha \in F - \{0\}\}$$

skup svih dilatacija. Pokaži da je $\mathrm{Dil}\, V$ komutativna grupa s obzirom na kompoziciju. Neka je, konačno,

$$p : F - \{0\} \to \mathrm{Dil}\, V$$

preslikavanje, dano s $p(\alpha) = d_\alpha$. Pokaži da je p izomorfizam multiplikativne grupe $F - \{0\}$ i grupe $\mathrm{Dil}\, V$.

6. Neka je $a \in V$ bilo koji vektor. Tada definiramo

$$l_a : F \to V$$

s $l_a(\alpha) = \alpha a$. Pokaži da je l_a homomorfizam aditivne grupe F u grupu V. Odatle, specijalno, slijedi da je $0\, a = \Theta$. Kako?

7.2. Primjeri linearnih prostora

Navest ćemo neke tipične primjere vektorskih prostora, iz kojih se razabire da su istom apstraktnom shemom pokrivena vrlo raznorodna područja matematike.

1. Kako smo dokazali u petom poglavlju, skup V^3 svih klasa orijentiranih dužina u prostoru, jest uz standardno zbrajanje vektora i množenje skalarima primjer **realnog** vektorskog prostora. Isto tako, vektorski prostori su V^2 i V^1. Prostori radijvektora $V^3(O), V^2(O)$ i $V^1(O)$ su također primjeri realnih linearnih prostora.

2. Kako smo vidjeli, skup

$$\mathbb{R}^n = \{(\alpha_1, ..., \alpha_n) \mid \alpha_i \in \mathbb{R}\}$$

je uz koordinatno zbrajanje

$$(\alpha_1, \ldots, \alpha_n) + (\beta_1, \ldots, \beta_n) = (\alpha_1 + \beta_1, \ldots, \alpha_n + \beta_n)$$

Abelova grupa. Ako za svaki $\alpha \in \mathbb{R}$ definiramo vanjsko množenje

$$\alpha(\alpha_1, ..., \alpha_n) = (\alpha\alpha_1, ..., \alpha\alpha_n)\ ,$$

onda $\mathbb{R}^n$ postaje realni linearni prostor koji nazivamo **realni n-dimenzionalni koordinatni prostor**.

3. Neka je

$$\mathbb{R}^\infty = \{(\alpha_1, \alpha_2, ...) \mid \alpha_i \in \mathbb{R}\}$$

skup svih nizova realnih brojeva. Uz prirodno koordinatno zbrajanje i množenje nizova skalarom

$$(\alpha_i) + (\beta_i) = (\alpha_i + \beta_i) ,$$

$$\alpha(\alpha_i) = (\alpha\alpha_i) ,$$

$\mathbb{R}^\infty$ postaje realni linearni prostor. Neka je $\mathbb{R}_0^\infty \subset \mathbb{R}^\infty$ skup svih onih nizova realnih brojeva koji su **skoro svuda nula** (tj. imaju samo konačno mnogo članova različitih od nule). Onda je, uz navedene operacije, i $\mathbb{R}_0^\infty$ vektorski prostor.

4. Konstrukcije iz primjera 2 i 3 možemo generalizirati. Neka je F bilo koje polje, a

$$F^n = \{(\alpha_1, ..., \alpha_n) \mid \alpha_i \in F\}$$

skup svih uređenih n-torki iz tog polja. Onda je, uz koordinatno definirane operacije, F^n linearni prostor nad poljem F koji se naziva **n-dimenzionalni koordinatni prostor nad poljem F** ili također **standardni n-dimenzionalni prostor nad poljem F**, iz razloga koji će uskoro biti objašnjeni. Posve se analogno definiraju prostori F^∞ i F_0^∞. Tako npr. imamo kompleksne linearne prostore $\mathbb{C}^n, \mathbb{C}^\infty, \mathbb{C}_0^\infty$; racionalne $\mathbb{Q}^n$, $\mathbb{Q}^\infty$, $\mathbb{Q}_0^\infty$; prostor $\mathbb{Z}_p^n$ uređenih n-torki cijelih brojeva mod p (gdje je p prim broj) itd.

5. Neka je $n \in \mathbb{N}$ dani prirodni broj, a

$$P_n = \{p \mid p \text{ je polinom }, st\, p < n\} \cup \{0\}$$

skup svih polinoma jedne varijable t, s realnim koeficijentima, čiji stupanj ne premašuje $n-1$, zajedno s nulpolinomom. Onda je P_n, uz uobičajeno zbrajanje polinoma i množenje polinoma realnim brojevima, realni vektorski prostor. Isto tako je skup

$$P = \bigcup_{n=0}^{\infty} P_n$$

svih polinoma, realni linearni prostor, **prostor polinoma** . Analogno se definiraju prostori polinoma nad bilo kojim poljem F (tj. polinoma s koeficijentima iz F).

6. Generalizirajući prethodni primjer, možemo promatrati skup

$$\mathbb{R}^{\mathbb{R}} = \{f : \mathbb{R} \to \mathbb{R}\}$$

svih realnih funkcija (realne varijable). Taj je skup, uz standardne operacije zbrajanja funkcija i množenja funkcija realnim brojevima,

$$(f+g)(t) = f(t) + g(t)\ ,$$

$$(\alpha f)(t) = \alpha \cdot f(t),\ \alpha \in \mathbb{R}\ ,$$

također linearni prostor.

7. Daljnji važan primjer realnog vektorskog prostora jest skup svih **neprekidnih realnih funkcija** $f : \mathbb{R} \to \mathbb{R}$, označen obično s $C(\mathbb{R})$.

8. Još općenitije, neka je S bilo koji neprazan skup, a F bilo koje polje. Neka je

$$V = F^S = \{f \mid f : S \to F\}$$

skup svih preslikavanja skupa S u polje F. Onda je, uz prirodne operacije, V linearni prostor nad poljem F. Prostor V nazivamo **prostor funkcija** ili **funkcijski prostor**.

9. Iz Prim.2., stavljajući $n = 1$, zaključujemo da je sam $\mathbb{R}$ realni linearni prostor. Isto tako su $\mathbb{C}$ i $\mathbb{Q}$ linearni prostori nad samim sobom. Nadalje, odmah se vidi da se npr. $\mathbb{C}$ može shvatiti kao linearni prostor nad poljem $\mathbb{R}$ i nad poljem $\mathbb{Q}$.

   Općenito, svako se polje može interpretirati kao linearni prostor nad samim sobom i nad svakim svojim potpoljem.

10. Nad svakim poljem F postoji jedinstveni linearni prostor $V = \{\Theta\}$, koji se sastoji iz jednog jedinog vektora, tzv. **trivijalni prostor** nad poljem F.

ZADACI

1. Neka je $\mathbb{Z}$ prsten cijelih brojeva, a A bilo koja Abelova grupa. Definiramo

$$h : \mathbb{Z} \times A \to A$$

s $h(n, a) = na$. Provjeri da su, uz takvo vanjsko množenje, ispunjeni aksiomi (1)–(4) iz definicije linearnog prostora. Prema tome, svaka se Abelova grupa može shvatiti kao modul nad prstenom $\mathbb{Z}$, tj. kao **$\mathbb{Z}$–modul**.

2. Neka je A Abelova grupa, a

$$E = \mathrm{Hom}\,(A, A)$$

prsten svih endomorfizama grupe A. Definiramo

$$h : E \times A \to A$$

s $h(f, a) = f(a)$. Pokaži da je, uz takvo vanjsko množenje, A modul nad prstenom E. Prema tome, svaka se Abelova grupa može također shvatiti kao modul nad prstenom svojih endomorfizama.

3. Neka je $V = \mathbb{R}_{[0,1]} = \{f \mid f : [0,1] \to \mathbb{R}\}$ skup svih realnih funkcija definiranih na segmentu $[0,1]$. Onda je, uz uobičajene operacije,

   (a) skup V,
   (b) skup neprekidnih funkcija iz V,
   (c) skup derivabilnih funkcija iz V,
   (d) skup integrabilnih funkcija iz V,
   (e) skup funkcija iz V oblika $\alpha e^t + \beta e^{2t}$, $\alpha, \beta \in \mathbb{R}$,

   realni linéarni prostor. Dokaži! Uoči kojim se važnim teoremima iz analize ovdje moraš koristiti.

4. Neka je $V = \mathbb{R}^+$, a $F = \mathbb{R}$. Definiramo

$$a + b = ab\,,$$

$$\alpha a = a^\alpha\,.$$

   Pokaži da je, uz te operacije, $\mathbb{R}^+$ linearni prostor nad $\mathbb{R}$.

5. Neka je $V = \mathbb{R}^2$, a $F = \mathbb{R}$. Uz standardno zbrajanje, u $\mathbb{R}^2$ definiramo vanjsko množenje s

$$\alpha(\alpha_1, \alpha_2) = (\alpha\alpha_1, 0)\,.$$

   Dokaži da je V linearni prostor nad F.

6. Pokaži da sva (realna) rješenja diferencijalne jednadžbe

$$\frac{d^2y}{dx^2} + y = 0$$

   čine realni linearni prostor.

7. Dokaži: Ako je F konačno polje s m elemenata, onda linearni prostor F^n ima m^n elemenata. Na primjer, $\mathbb{Z}_p^n$ ima p^n elemenata.

8. Dokaži: Netrivijalni prostor nad beskonačnim poljem ima beskonačno mnogo elemenata.

7.3. Linearna zavisnost i nezavisnost

Neka je V linearni prostor nad poljem F. Ako su $a_1, a_2, ..., a_k \in V$ bilo koji vektori, a $\alpha_1, \alpha_2, ..., \alpha_k \in F$ po volji odabrani skalari, onda je jednoznačno određen vektor

$$\alpha_1 a_1 + \alpha_2 a_2 + ... + \alpha_k a_k \tag{1}$$

iz V, koji nazivamo **linearna kombinacija** ili **linearni spoj vektora** $a_1, a_2, ..., a_k$ s **koeficijentima** $\alpha_1, \alpha_2, ..., \alpha_k$.

Neka je $S = \{a_1, a_2, ..., a_k\}$ **konačan** skup vektora iz V. Kažemo da je taj skup **linearno nezavisan**, ako se nulvektor $\Theta \in V$ može na **jedan jedini** način prikazati kao linearna kombinacija vektora iz S, tj. ako iz

$$\Theta = \alpha_1 a_1 + ... + \alpha_k a_k \tag{2}$$

slijedi da je $\alpha_i = 0$, za sve $i = 1, ..., k$. Ako pak Θ dopušta više prikaza oblika (2), za skup S kažemo da je **linearno zavisan**. Drugim riječima, skup S je linearno zavisan ako i samo ako postoji izbor skalara $\alpha_1, \alpha_2, ..., \alpha_k \in F$ takav da vrijedi (2) i pritom je bar jedan od skalara α_i različit od nule.

Kraće ćemo govoriti da je skup S linearno nezavisan ako Θ dopušta **samo trivijalan** prikaz pomoću vektora iz S, odnosno da je S linearno zavisan ako Θ ima i **netrivijalnih** prikaza.

Definiciju linearne nezavisnosti, odnosno zavisnosti, koja se odnosila samo na konačne skupove vektora iz V lako je proširiti i na beskonačne skupove. Neka je $S \subset V$ bilo koji skup vektora. Kažemo da je S linearno nezavisan ako je **svaki** njegov konačni podskup linearno nezavisan. Skup S je linearno zavisan ako postoji **bar jedan** konačni podskup od S koji je linearno zavisan. Iz praktičnih razloga se obično postulira da je prazan skup linearno nezavisan.

Primijetimo da je linearna nezavisnost, odnosno zavisnost, svojstvo skupa vektora (jer daje neku informaciju o relativnom odnosu vektora u tom skupu), a ne svojstvo pojedinih vektora iz tog skupa. Zbog toga treba govoriti "linearno nezavisni skup vektora", a nipošto "skup linearno nezavisnih vektora" (kako se to često čini!).

PRIMJERI

1. Neka su $a = (1, 0)$ i $b = (0, 1)$ vektori iz linearnog prostora $\mathbb{R}^2$. Onda je $\{a, b\}$ linearno nezavisan skup vektora. Naime, iz

$$\alpha a + \beta b = \Theta ,$$

tj.

$$\alpha(1,0)+\beta(0,1)=(0,0)\ ,$$

slijedi

$$(\alpha,\beta)=(0,0)\ ,$$

tj. $\alpha=0$ i $\beta=0$, što pokazuje da se nulvektor u tom prostoru može napisati kao linearna kombinacija vektora a i b **samo** na trivijalan način.

2. Neka su $a=(2,3)$ i $b=(4,6)$ vektori iz $\mathbb{R}^2$. Onda je skup $\{a,b\}$ linearno zavisan. Zaista,

$$\alpha(2,3)+\beta(4,6)=(0,0)$$

povlači

$$2\alpha+4\beta=0\ ,$$

$$3\alpha+6\beta=0\ .$$

Međutim, taj sustav jednadžbi, osim trivijalnog rješenja $\alpha=\beta=0$, ima i netrivijalna rješenja, npr. $\alpha=-2$, $\beta=1$. Prema tome, nulvektor u $\mathbb{R}^2$ može se prikazati kao linearna kombinacija vektora a i b i na netrivijalan način, pa zaključujemo da je skup $\{a,b\}$ linearno zavisan.

3. Neka su

$$\begin{aligned} e_1 &= (1,0,...,0)\\ e_2 &= (0,1,...,0)\\ &\vdots\\ e_n &= (0,0,...,1) \end{aligned}$$

vektori iz prostora $\mathbb{R}^n$ ili, općenitije, iz F^n. Lako se vidi da ti vektori čine linearno nezavisan skup.

4. Neka je $\{1,t,t^2,...,t^k\}$, $k\leq n-1$, skup vektora u prostoru P_n, svih polinoma čiji stupanj ne premašuje $n-1$. Taj skup je linearno nezavisan u P_n jer je iz algebre poznato da identična jednakost (za svaki t)

$$\alpha_0+\alpha_1 t+...+\alpha_k t^k\equiv 0$$

povlači $\alpha_1=\alpha_2=...=\alpha_k=0$.

5. Skup $\{1,t,...,t^k,...\}$ monoma iz prostora P svih polinoma je primjer beskonačnog (prebrojivog) skupa koji je linearno nezavisan.

Navedimo sada neke jednostavne posljedice definicije linearne nezavisnosti, odnosno zavisnosti.

PROPOZICIJA 1

Podskup linearno nezavisnog skupa vektora je i sam linearno nezavisan. Nadskup linearno zavisnog skupa je linearno zavisan.

Dokaz

Tvrdnja je zapravo posljedica opće definicije linearne nezavisnosti, odnosno zavisnosti, a u slučaju konačnih skupova se lako može dokazati. Pokažimo npr. drugi dio tvrdnje. Neka je $\{a_1, ..., a_k\} \subset V$ linearno zavisan skup, a $\{a_1, ..., a_k, b_1, ..., b_l\} \subset V$ neki njegov nadskup. Po pretpostavci, postoje $\alpha_i \in F$ takvi da je

$$\sum_{i=1}^{k} \alpha_i a_i = \Theta$$

i pritom je bar jedan $\alpha_i \neq 0$. No, onda je

$$\sum_{i=1}^{k} \alpha_i a_i + \sum_{j=1}^{l} 0 b_j = \Theta + \Theta = \Theta\,,$$

što pokazuje da Θ ima netrivijalni prikaz pomoću vektora iz nadskupa pa je i on linearno zavisan. ■

PROPOZICIJA 2

Skup $\{a\} \subset V$, koji se sastoji iz jednog jedinog vektora iz V, linearno je zavisan ako i samo ako je $a = \Theta$.

Dokaz

Neka je $\{a\}$ linearno zavisan skup. To znači da postoji $\alpha \neq 0$ takav da je $\alpha a = \Theta$. No, onda je, prema Prop. 5 iz 7.1., $a = \Theta$.

Obratno, ako je $a = \Theta$ to je $\alpha a = \Theta$ za svaki $\alpha \in F$ (Prop. 4 iz 7.1.), pa je $\{a\}$ linearno zavisan. ■

KOROLAR 3

Skup vektora iz V koji sadrži $\Theta \in V$ linearno je zavisan.

Dokaz

Neposredno iz Prop. 1 i Prop. 2. ■

PROPOZICIJA 4

Skup vektora $S = \{a_1, ..., a_s\}$ iz V je linearno zavisan ako i samo ako se bar jedan od vektora iz S može prikazati kao linearna kombinacija preostalih vektora iz S.

Dokaz

Ako je $s = 1$, tvrdnja nema smisla. Pretpostavimo zato da je $s > 1$. Neka je S linearno zavisan skup. To znači da vrijedi

$$\alpha_1 a_1 + ... + \alpha_i a_i + ... + \alpha_s a_s = \Theta$$

i pritom je bar jedan od skalara $\alpha_1, ..., \alpha_s \in F$ različit od nule. Neka je npr. $\alpha_i \neq 0$. Onda možemo pisati

$$\alpha_i a_i = -\alpha_1 a_1 - ... - \alpha_{i-1} a_{i-1} - \alpha_{i+1} a_{i+1} - ... - \alpha_s a_s \ .$$

No, jer je F polje, postoji $\alpha_i^{-1} \in F$ pa množenjem dobivamo

$$\begin{aligned} a_i \ = \ & (-\alpha_1 \alpha_i^{-1}) a_1 + \ldots + (-\alpha_{i-1} \alpha_i^{-1}) a_{i-1} + \\ & + (-\alpha_{i+1} \alpha_i^{-1}) a_{i+1} + \ldots + (-\alpha_s \alpha_i^{-1}) a_s \ , \end{aligned}$$

tj. vektor a_i je izražen kao linearna kombinacija vektora iz skupa

$$\{a_1, ..., a_{i-1}, a_{i+1}, ..., a_s\} = S - \{a_i\} \ .$$

Obratno, neka je jedan od vektora iz skupa S prikazan kao linearna kombinacija preostalih vektora iz S, npr.

$$a_i = \alpha_1 a_1 + ... + \alpha_{i-1} a_{i-1} + \alpha_{i+1} a_{i+1} + ... + \alpha_s a_s \ .$$

Onda je

$$\alpha_1 a_1 + \ldots + \alpha_{i-1} a_{i-1} + \underbrace{(-1)}_{\neq 0} a_i + \alpha_{i+1} a_{i+1} + ... + \alpha_s a_s = 0$$

netrivijalni prikaz nulvektora, pa je skup vektora S linearno zavisan. ■

ZADACI

1. Dokaži: Skup od dva vektora iz prostora V^3 je linearno zavisan ako i samo ako su ti vektori kolinearni. Skup od tri vektora iz V^3 je linearno zavisan ako i samo ako su ti vektori komplanarni. Skup od četiri vektora iz V^3 je uvijek linearno zavisan (vidi Zad. 2.–4. u 5.7.).

   Prema tome, svaka baza u V^3 predstavlja linearno nezavisan skup.

2. U prostoru $\mathbb{R}^4$ promatrajmo sljedeće skupove vektora:

   (a) (1,2,-3,1), (2,0,4,1), (5,-4,14,-3) ;

   (b) (2,1,2,1), (6,3,6,3), (5,1,4,3) ;

   (c) (1,1,0,0), (1,0,1,0), (0,1,1,0) .

   Utvrdi koji su od tih skupova linearno zavisni, a koji linearno nezavisni. Izrazi pojedini vektor iz skupa kao linearnu kombinaciju ostalih, kad god je to moguće.

3. Neka je F^∞ prostor svih nizova elemenata iz polja F. Za $\lambda \in F$ definiramo

$$a_\lambda = (\lambda, \lambda^2, \ldots) .$$

   Onda je

$$\{a_\lambda | \lambda \in F, \lambda \neq 0\}$$

   linearno nezavisan skup u F^∞. Dokaži!

4. Neka je $\{f : \mathbb{R} \to \mathbb{R} \mid f \text{ je neprekidna}\}$ prostor svih neprekidnih realnih funkcija. Za $\lambda \in \mathbb{R}$ definiramo

$$f_\lambda : \mathbb{R} \to \mathbb{R}$$

   s

$$f_\lambda(t) = e^{\lambda t} .$$

   Pokaži da je skup

$$\{f_\lambda \mid \lambda \in \mathbb{R}\}$$

   linearno nezavisan u navedenom prostoru. Primjer pokazuje da ima prostora s neprebrojivim linearno nezavisnim podskupovima.

5. Neka je V linearni prostor nad poljem F, i neka je karakteristika $k(F) \neq 2$. Ako je $\{a, b, c\}$ linearno nezavisan skup vektora iz V, onda je i $\{b + c, c + a, a + b\}$ linearno nezavisan skup. Dokaži! Što možeš reći o skupu $\{b - c, c - a, a - b\}$?

6. Dokaži: Neka je $a \in V$ linearna kombinacija vektora iz skupa $S = \{a_1, \ldots, a_s\}$, a svaki od vektora a_i linearna kombinacija vektora iz skupa $T = \{b_1, \ldots, b_t\}$. Dokaži da se a može prikazati kao linearna kombinacija vektora iz skupa T.

7. Neka su $S, T \subset V$ linearno nezavisni (zavisni) skupovi. Što možeš reći o skupovima $S \cup T$ i $S \cap T$?

7.4. Skup izvodnica linearnog prostora. Baza i dimenzija

Neka je V linearni prostor nad poljem F, a $G \subset V$ njegov podskup. Kažemo da je G **skup izvodnica** za prostor V ako je svaki vektor iz tog prostora moguće prikazati kao linearnu kombinaciju (konačnog broja) vektora iz skupa G. Drugim riječima, G je skup izvodnica za V ako za svaki vektor $a \in V$ postoji $k \in \mathbb{N}$ i vektori $a_1, \ldots, a_k \in G$ takvi da je

$$a = \sum_{i=1}^{k} \alpha_i a_i$$

za neki izbor $\alpha_i \in F$.

Kaže se, također, da je G **skup generatora** za prostor V, odnosno da skup G **razapinje** ili **generira** prostor V.

Svaki linearni prostor sadrži skupove izvodnica, općenito raznovrsne i raznobrojne. Trivijalni je primjer $G = V$, tj. čitav prostor V shvaćen kao skup izvodnica za taj prostor. Jasno je, također, da je svaki nadskup skupa izvodnica i sam skup izvodnica. Od interesa su, međutim, minimalni skupovi izvodnica. Proces traženja najekonomičnijeg, minimalnog skupa izvodnica za prostor V dovodi nas do pojma baze.

Za **uređeni** podskup $B \subset V$ prostora V kažemo da je **baza prostora** V, ako je B

(1) skup izvodnica za V,

(2) linearno nezavisan skup u V.

Za skup B su još uobičajeni nazivi **Hamelova** ili **algebarska** baza prostora V (za razliku od npr. topološke baze o kojoj ovdje neće biti riječi, vidi Zad. 8. u točki 12.6.).

PRIMJERI

1. Svaki uređeni skup $(\vec{a}_1, \vec{a}_2, \vec{a}_3) \in V^3$, koji se sastoji od tri nekomplanarna vektora, predstavlja jednu bazu za V^3, u smislu dane definicije. Zaista, takav je skup linearno nezavisan (Zad. 1. u 7.3.), i nadalje, za svaki $\vec{a} \in V^3$, prema Tm. 4 iz 5.7., postoje skalari $\alpha_i \in \mathbb{R}$ takvi da je

$$a\vec{a} = \alpha_1 \vec{a}_1 + \alpha_2 \vec{a}_2 + \alpha_3 \vec{a}_3 \,,$$

tj. $(\vec{a}_1, \vec{a}_2, \vec{a}_3)$ je skup izvodnica.

2. U prostoru $\mathbb{R}^2$ jedna baza je uređeni par

$$B = ((1,0), (0,1)) .$$

Pokazali smo, naime, da je to linearno nezavisan skup, a kako je za bilo koji $(\alpha, \beta) \in \mathbb{R}^2$

$$(\alpha, \beta) = (\alpha, 0) + (0, \beta) = \alpha(1,0) + \beta(0,1) ,$$

to je B i skup izvodnica.

3. Općenitije, skup $(e_1, e_2, \ldots, e_n)$, gdje su

$$\begin{aligned} e_1 &= (1,0,...,0) , \\ e_2 &= (0,1,...,0) , \\ &\vdots \\ e_n &= (0,0,...,1) , \end{aligned}$$

predstavlja jednu jednostavnu bazu, tzv. **kanonsku bazu**, za prostor $\mathbb{R}^n$, odnosno F^n.

4. Lako se vidi da je skup $(1, i)$ jedna baza za $\mathbb{C}$, shvaćen kao prostor nad poljem realnih brojeva.

5. U prostoru P_n, svih polinoma stupnja $\leq n-1$, jest skup

$$B = (1, t, \ldots, t^{n-1})$$

linearno nezavisan, a kako svaki $p \in P_n$ možemo prikazati kao

$$p(t) = \sum_{i=0}^{n-1} \alpha_i t^i ,$$

tj. kao linearnu kombinaciju vektora iz B, to je B baza za P_n.

6. Analogno zaključujemo da je

$$B = (1, t, \ldots, t^k, \ldots)$$

jedna baza za prostor P svih polinoma.

Postavlja se, dakako, pitanje egzistencije i jedinstvenosti baze za bilo koji linearni prostor. Na to pitanje daje odgovor ovaj osnovni

TEOREM 1

Svaki netrivijalni linearni prostor V (tj. prostor $V \neq \{\Theta\}$) ima bar jednu bazu. Svake dvije baze prostora su ekvipotentne. ■

Za dokaz tog teorema bila bi potrebna neka složenija sredstva teorije skupova, kao što su transfinitna indukcija, teorem o dobrom uređenju ili Zornova lema. Mi ga zato nećemo dokazivati u ovoj generalnosti nego za jednu užu klasu vektorskih prostora, tzv. **konačnodimenzionalne linearne prostore**. Naime, jedino će ti prostori biti predmet našeg interesa i daljnjeg izučavanja u okvirima ovog kolegija, jer se sva njihova svojstva mogu utvrditi korištenjem isključivo algebarskih sredstava. Istraživanjem beskonačnodimenzionalnih prostora bavi se zasebna matematička disciplina, **funkcionalna analiza**.

Iz Tm. 1, zaključujemo da ima smisla ova definicija:

Dimenzija netrivijalnog prostora $V \neq \{\Theta\}$ je kardinalni broj (neke) baze prostora V. Nadalje, dimenzija trivijalnog prostora $V = \{\Theta\}$ je, po definiciji, jednaka nuli. Dimenziju prostora V označavamo s $\dim V$, odnosno s $\dim_F V$, ako želimo naglasiti da se radi o prostoru nad poljem F. U upotrebi je i naziv **algebarska dimenzija prostora** .

Kako su sve baze danog linearnog prostora jednakobrojne, dimenzija prostora je dobro definiran pojam, neovisan o izboru baze.

Tako npr. zaključujemo, da je $\dim V^3 = \dim \mathbb{R}^3 = 3$, a $\dim \mathbb{R}^n = \dim F^n = n$. Nadalje je $\dim_{\mathbb{R}} \mathbb{C} = 2$, $\dim_{\mathbb{C}} \mathbb{C} = 1$, dok je $\dim P_n = n$. Konačno, $\dim P = \aleph_0$, a $\dim \mathbb{R}^{\mathbb{R}} = c$.

ZADACI

1. Neka je $G \subset V$ **bilo koji** skup izvodnica prostora V te $a \in G$ vektor koji se može prikazati kao linearna kombinacija preostalih vektora iz G. Onda je $G - \{a\}$ također skup izvodnica za V. Dokaži!

2. Pokaži da je $((0,1,1),(1,0,1),(1,1,0))$ jedna baza za $\mathbb{R}^3$.

3. Utvrdi je li skup $(1, 1+t, 1+t+t^2, 1+t+t^2+t^3)$ baza za skup P_4.

7.5. Konačnodimenzionalni prostori

Za linearni prostor kažemo da je **konačnodimenzionalan** ako sadrži **bar jedan** konačan skup izvodnica. U protivnom, kažemo da je prostor **beskonačnodimenzionalan**.

Od sada pa nadalje bavit ćemo se samo konačnodimenzionalnim prostorima. Zato ćemo ispustiti taj atribut, tj. pod **pojmom linearni prostor ćemo uvijek podrazumijevati konačnodimenzionalni prostor.**

Ova je točka posvećena dokazu Tm. 1 iz 7.4. u konačnodimenzionalnom slučaju.

LEMA 1

Neka je $G = \{a_1, ..., a_k, ..., a_n\}$ *skup izvodnica za prostor* V. *Ako je vektor* $a_k \in G$ *linearna kombinacija preostalih vektora iz* G, *onda je* $G - \{a_k\}$ *opet skup izvodnica za* V.

Dokaz

Po pretpostavci je

$$a_k = \sum_{i=1}^{n\ '} \alpha_i a_i \ ,$$

gdje crtica označava da se pri sumiranju ispušta $i = k$. Neka je $a \in V$ bilo koji vektor. Kako je G skup izvodnica, imamo

$$a = \sum_{i=1}^{n} \beta_i a_i$$

i onda redom

$$a = \sum_{i=1}^{n\ '} \beta_i a_i + \beta_k a_k = \sum_{i=1}^{n\ '} \beta_i a_i + \beta_k \sum_{i=1}^{n\ '} \alpha_i a_i \ ,$$

dakle

$$a = \sum_{i=1}^{n\ '} (\beta_i + \beta_k \alpha_i) a_i = \sum_{i=1}^{n\ '} \gamma_i a_i \ ,$$

što pokazuje da je a prikazan kao linearna kombinacija vektora $a_1, \ldots, a_{k-1}$, $a_{k+1}, \ldots, a_n$, pa je tvrdnja dokazana. ■

TEOREM 2

Neka je V *netrivijalni linearni prostor, a* $G = \{a_1, ..., a_n\}$ *konačan skup izvodnica za* V. *Onda* G *sadrži podskup koji je baza u* V.

Dokaz

Kako je $V \neq \{\Theta\}$, očito je da G mora sadržavati bar jedan vektor različit od nulvektora. Ako je skup G linearno nezavisan, dokaz je gotov. Uzmimo zato da je linearno zavisan. Onda se, prema Prop. 4 u 7.3., bar jedan

od vektora iz G, kažimo $a_k \in G$, može prikazati kao linearna kombinacija preostalih vektora iz G. No, prema Lemi 1 taj se vektor može ispustiti, tako da je $G' = G - \{a_k\}$ opet skup izvodnica za V. Ako je G' linearno nezavisan, dokaz je gotov; ako nije, postupak ponovimo. Nastavljajući tako, nakon konačno mnogo koraka (najviše njih $n-1$) dolazimo do linearno nezavisnog skupa izvodnica, a to je po definiciji baza prostora V. ■

KOROLAR 3

Svaki netrivijalni linearni prostor ima bazu.

Dokaz

Svaki prostor ima konačni skup izvodnica, a onda po Tm. 2 i bazu. ■

Time je dokazana egzistencija baze za konačnodimenzionalne prostore. Posebno, svaki takav prostor **ima bar jednu konačnu bazu**.

Kako bismo dokazali jednakobrojnost baza, potrebna nam je ova modifikacija Prop. 4 iz 7.3.:

LEMA 4

Neka je $S = (a_1, ..., a_s)$ uređeni skup vektora iz V, koji je linearno zavisan. Neka je $a_1 \neq \Theta$. Onda se bar jedan od vektora iz S može izraziti kao linearna kombinacija svojih prethodnika u S.

Dokaz

U netrivijalnom prikazu

$$\sum_{i=1}^{s} \alpha_i a_i = \Theta \,,$$

neka je α_j zadnji koeficijent različit od nule. Kad bi bilo $j = 1$, imali bismo $\alpha_1 a_1 = \Theta$, pa bi zbog $\alpha_1 \neq 0$ bilo $a_1 = \Theta$, protivno pretpostavci. Zato je $j > 1$ i polazna se relacija reducira na

$$\alpha_1 a_1 + \ldots + \alpha_j a_j = \Theta \,,$$

pa množenjem s α_j^{-1} dobivamo traženi prikaz. ■

Imamo sada ovaj važan

TEOREM 5 (Steinitz)

Svake dvije baze danog linearnog prostora V su ekvipotentne.

Dokaz

Kako smo vidjeli, prostor V ima bar jednu konačnu bazu, kažimo

$$B = (a_1, ..., a_n) .$$

Neka je

$$X = (x_\alpha | \alpha \in A)$$

bilo koja druga baza za V. Elemente te baze smo indeksirali pomoću nekog skupa indeksa A, ne želeći prejudicirati da je skup X konačan ili prebrojiv. Očito je dovoljno pokazati da je

$$\text{card } X = \text{card } B , \tag{1}$$

jer onda tvrdnja teorema slijedi iz tranzitivnosti jednakosti kardinalnih brojeva. Pokazat ćemo da je

$$\text{card } X \leq \text{card } B ,$$

i time utvrditi da je i broj vektora u bazi X konačan. Posve analogno bi se onda pokazalo da je i

$$\text{card } B \leq \text{card } X ,$$

dakle da vrijedi jednakost (1).

Pretpostavimo najprije, zbog jednostavnosti, da je $B \cap X = \emptyset$. Neka je $x_{\alpha_1} \in X$ bilo koji vektor. Promatrajmo uređeni skup vektora

$$(x_{\alpha_1}, a_1, ..., a_n) . \tag{2}$$

To je očito skup izvodnica za V, i to linearno zavisan, jer je npr. x_{α_1} linearna kombinacija preostalih vektora iz (2). Zbog Leme 4 postoji neki a_i (jer to ne može biti x_{α_1}), koji je moguće izraziti kao linearnu kombinaciju njegovih **prethodnika** u (2). Taj je vektor onda suvišan, pa je, prema Lemi 1,

$$(x_{\alpha_1}, a_1, ..., a_{i-1}, a_{i+1}, ..., a_n) \tag{3}$$

opet skup izvodnica za V. Odaberimo sada $x_{\alpha_2} \in X$, uz $\alpha_2 \neq \alpha_1$, i promatrajmo skup

$$(x_{\alpha_2}, x_{\alpha_1}, a_1, ..., a_{i-1}, a_{i+1}, ..., a_n) . \tag{4}$$

To je također skup izvodnica za V, i to linearno zavisan, jer se npr. x_{α_2} može izraziti kao linearna kombinacija ostalih vektora iz (4), budući da je (3) bio skup izvodnica. Tada opet, prema Lemi 4, postoji neki vektor u (4) koji je moguće predočiti kao linearnu kombinaciju prethodnih vektora. To očito nije x_{α_2}, ali ni x_{α_1}, jer je skup $\{x_{\alpha_1}, x_{\alpha_2}\}$ linearno nezavisan po

pretpostavci, kao dio baze X. Dakle je to neki od a-ova, kažimo a_j. Taj je vektor onda suvišan, tj. po Lemi 1

$$(x_{\alpha_2}, x_{\alpha_1}, a_1, ..., a_{i-1}, a_{i+1}, ..., a_{j-1}, a_{j+1}, ..., a_n)$$

također je skup izvodnica. Proces nastavljamo, uključujući $x_{\alpha_3} \in X$, za $\alpha_3 \neq \alpha_1$, α_2, i izbacujući neki a_k, itd. Kad bi broj vektora u X bio veći od n, postupnom bismo zamjenom nakon n koraka došli do skupa

$$(x_{\alpha_n}, x_{\alpha_{n-1}}, ..., x_{\alpha_2}, x_{\alpha_1}) \,, \tag{5}$$

koji bi zbog Leme 1 bio sigurno opet skup izvodnica za V. No, onda bi postojao vektor $x_{\alpha_{n+1}} \in X$ i on bi se dao izraziti kao linearna kombinacija vektora iz (5), što bi značilo da je skup X linearno zavisan, protivno pretpostavci da je to baza. Prema tome je

$$\text{card } X \leq n = \text{card } B$$

i dokaz je gotov. Posve analogno se teorem dokazuje u slučaju kad $B \cap X$ nije prazan. ■

Teorem pokazuje da je u konačnodimenzionalnom slučaju pojam dimenzije prostora (kao broja vektora u bazi) dobro definirano svojstvo prostora, neovisno o izboru baze. Ako je $\dim V = n$, kažemo da je V **n-dimenzionalni linearni prostor**.

Kako smo vidjeli (Tm. 2), svaki se skup izvodnica za V može **reducirati** na podskup koji je linearno nezavisan, dakle do baze prostora V. Pokazat ćemo sada obrnuto, tj. da se svaki linearno nezavisni skup vektora u V može **proširiti**, dopuniti, do nadskupa koji je skup izvodnica, tj. baza prostora V. Točnije, imamo ovaj

TEOREM 6

Neka je $S = \{a_1, ..., a_s\} \subset V$ linearno nezavisan skup vektora u V. Onda je S podskup neke baze prostora V.

Dokaz

Ako je S i skup izvodnica za V, onda je sam S baza, i dokaz je gotov. Uzmimo zato da nije tako. Neka je

$$B = (b_1, \ldots, b_n)$$

bilo koja baza prostora V. Promatrajmo uređeni skup

$$(a_1, \ldots, a_s, b_1, \ldots, b_n) \,. \tag{6}$$

Kako već B razapinje V, to je (6) pogotovo skup izvodnica za V, i to linearno zavisan (jer je npr. svaki a_i moguće izraziti kao linearnu kombinaciju vektora iz B). Prema Lemi 4 se onda bar jedan od vektora iz (6) može izraziti kao linearna kombinacija svojih prethodnika. To očito ne može biti niti jedan od vektora a_i, jer su ti vektori po pretpostavci linearno nezavisni. Dakle, to je jedan od b-ova, kažimo b_j. Prema Lemi 1 se taj vektor može ukloniti, tako da

$$(a_1, \ldots, a_s, b_1, \ldots, b_{j-1}, b_{j+1}, \ldots, b_n) \tag{7}$$

bude opet skup izvodnica za V. Ako je (7) linearno nezavisan skup, to je baza prostora, a jer sadrži S kao podskup, dokaz je gotov. Ako je pak (7) linearno zavisan skup, postupak ponovimo. Tako ćemo nakon konačno mnogo koraka doći do skupa

$$(a_1, \ldots, a_s, b_{i_1}, \ldots, b_{i_l}) ,$$

koji razapinje V i pritom je linearno nezavisan, dakle baza za V. Kako je $S = (a_1, \ldots, a_s)$ dio te baze, teorem je dokazan. ■

Primijetimo da proširenje skupa S do baze prostora očito nije jednoznačno.

KOROLAR 7

Neka je V n-dimenzionalni linearni prostor. Onda je svaki linearno nezavisni skup u V koji se sastoji od n vektora, baza za prostor V. Nadalje, bilo koji skup vektora iz V koji sadrži više od n vektora, linearno je zavisan.

Dokaz

Neka je $\{a_1, \ldots, a_n\}$ linearno nezavisan skup vektora iz V. Kad to ne bi bila baza za V, taj skup bi se, prema Tm. 6, mogao dopuniti do baze pa bi bilo $\dim V > n$, protivno pretpostavci.

Kako je svaki nadskup linearno zavisnog skupa vektora opet linearno zavisan, drugu tvrdnju dovoljno je dokazati za skup $S = \{a_1, \ldots, a_n, a_{n+1}\}$, koji se sastoji od $n+1$ vektora iz V. Ako je već $\{a_1, \ldots, a_n\} \subset S$ linearno zavisan, tvrdnja je dokazana. Ako je pak taj skup linearno nezavisan, on je, prema prethodnom i baza prostora pa se a_{n+1} može prikazati kao linearna kombinacija vektora tog skupa, što prema Prop. 4 iz 7.3. znači da je skup S linearno zavisan. ■

Iz Kor. 7 zaključujemo da je maksimalni broj linearno nezavisnih vektora u nekom prostoru jednak dimenziji tog prostora.

Navedimo na kraju i ovo važno svojstvo linearno nezavisnog skupa:

TEOREM 8

Neka je $S = \{a_1, ..., a_s\} \subset V$ linearno nezavisan skup. Ako se vektor $a \in V$ može prikazati kao linearna kombinacija vektora iz S, taj prikaz je jednoznačan.

Dokaz

Pretpostavimo da su

$$a = \sum_{i=1}^{s} \alpha_i a_i \quad \text{i} \quad a = \sum_{i=1}^{s} \beta_i a_i$$

prikazi vektora a pomoću vektora iz S. Onda oduzimanjem dobivamo

$$\Theta = \sum_{i=1}^{s} (\alpha_i - \beta_i) a_i \, .$$

No, budući da je po pretpostavci skup S linearno nezavisan, slijedi da je $\alpha_i - \beta_i = 0$ za svaki $i = 1, \ldots, s$, dakle $\alpha_i = \beta_i$ za svaki $i = 1, \ldots, s$, što pokazuje da je prikaz vektora a jedinstven. ■

KOROLAR 9

Neka je $B \subset V$ baza prostora V. Onda je prikaz svakog vektora iz V kao linearne kombinacije vektora iz B jednoznačan. ■

ZADACI

1. Dokaži: Neka je $S = \{a_1, ..., a_n\}$ skup od n vektora u n-dimenzionalnom prostoru V. S je baza prostora V onda i samo onda, ako je S skup izvodnica za V. Nadalje, skup vektora iz V koji sadrži manje od n vektora ne može biti skup izvodnica za V.

7.6. Potprostori

Za svaku smo strukturu do sada uvodili pojam podstrukture. To ćemo učiniti i za linearne prostore.

Neka je V linearni prostor nad poljem F, a $L \neq \emptyset$ podskup od V. Kažemo da je L linearni potprostor ili, kraće, **potprostor** prostora V ako je L i sam linearni prostor nad poljem F, s obzirom na iste operacije zbrajanja i množenja skalarom, koje su već definirane u prostoru V. U tom slučaju pišemo $L < V$. Svaki prostor V ima potprostore. **Trivijalni** potprostori su $L = V$ i $L = \{\Theta\}$. Ako je L potprostor od V i $L \neq V$, kažemo da je L **pravi** potprostor od V.

PROPOZICIJA 1

Neprazan podskup $L \subset V$ je **potprostor** *prostora V ako i samo ako je* **zatvoren** *u odnosu na operacije u V, tj. ako i samo ako vrijedi:*

(1) *za svaki $a, b \in L$ je $a + b \in L$,*

(2) *za svaki $a \in L, \alpha \in F$ je $\alpha a \in L$.*

Dokaz

Nužnost je očigledna. Dokažimo dovoljnost. Neka je, dakle, ispunjen (1) i (2). Iz (2) specijalno slijedi da je za svaki $a \in L$ i $-a = (-1)a \in L$, što zajedno s (1) pokazuje da je $L \subset V$ podgrupa aditivne grupe V. Nadalje, kako su aksiomi (1) – (4) iz definicije linearnog prostora ispunjeni u V, oni su očito ispunjeni i u L, pa je L linearni prostor, dakle potprostor od V i tvrdnja je dokazana. ■

Uvjeti iz Prop. 1 mogu se objediniti, pa imamo ovaj **kriterij za prepoznavanje potprostora**:

KOROLAR 2

Neprazan podskup $L \subset V$ je potprostor od V onda i samo onda, ako je za svaki izbor $a, b \in L$ i $\alpha, \beta \in F$ također $\alpha a + \beta b \in L$.

Dokaz

Uzimamo specijalno $\alpha = \beta = 1$, odnosno $b = \Theta$, pa primijenimo Prop. 1. ■

PRIMJERI

1. $V^2 \subset V^3$ je potprostor od V^3.

2. Uz dogovor o inkluziji (vidi Prim. 5. u 2.8.) je u nizu

$$\mathbb{R} \subset \mathbb{R}^2 \subset \ldots \subset \mathbb{R}^n \subset \ldots \subset \mathbb{R}^\infty$$

svaki prethodni prostor potprostor svakog sljedećeg. Isto vrijedi za niz prostora $\{F^k\}$ gdje je F bilo koje polje.

3. Neka je $0 < k \leq n$, a $L \subset \mathbb{R}^n$ skup definiran s

$$L = \{(x_1, \ldots, x_k, \ldots, x_n) \mid x_1 = x_2 = \ldots = x_k = 0\} .$$

Onda je L potprostor od $\mathbb{R}^n$.

4. U nizu
$$P_1 \subset P_2 \subset \ldots \subset P_n \subset \ldots \subset P$$
je svaki prethodni prostor polinoma potprostor svakog sljedećeg.

5. $\{\Theta\}$ je potprostor svakog potprostora $L < V$.

Neka je sada $S \subset V$ bilo koji podskup od V. Onda definiramo **linearnu ljusku** ili **linearni omotač** $[S]$ skupa S na ovaj način:

(1) ako je $S = \emptyset$, onda je $[S] = \{\Theta\}$;

(2) ako je $S \neq \emptyset$, onda je $[S]$ skup svih linearnih kombinacija vektora iz skupa S.

PROPOZICIJA 3

Za svaki skup $S \subset V$ linearna ljuska $[S]$ je potprostor od V.

Dokaz

Ako je $S = \emptyset$, tvrdnja izlazi iz definicije. Neka je zato $S \neq \emptyset$ i neka je $x, y \in [S]$. Onda imamo

$$x = \sum_{i=1}^{n} \alpha_i a_i \,, \quad y = \sum_{i=1}^{n} \beta_i a_i$$

(gdje, bez narušavanja općenitosti, možemo pretpostaviti da su x i y prikazani kao linearna kombinacija **istih** vektora $a_i \in S$), pa za bilo koji izbor skalara $\lambda, \mu \in F$ vrijedi

$$\begin{aligned} \lambda x + \mu y &= \lambda \sum_{i=1}^{n} \alpha_i a_i + \mu \sum_{i=1}^{n} \beta_i a_i = \\ &= \sum_{i=1}^{n} (\underbrace{\lambda \alpha_i + \mu \beta_i}_{\in F}) a_i \,, \end{aligned}$$

tj. $\lambda x + \mu y \in [S]$ i tvrdnja izlazi iz Kor. 2. ■

Očito je da je, uz $S \neq \emptyset$, skup S skup izvodnica za $[S]$, tj. da S razapinje ili generira potprostor $[S] < V$.

Kako je potprostor linearnog prostora i sam linearni prostor, i on ima svoju dimenziju. Pritom vrijedi

TEOREM 4

Ako je L potprostor od V, onda je $\dim L \leq \dim V$. ■

Dokazat ćemo teorem u konačnodimenzionalnom slučaju, tj. dokazat ćemo

TEOREM 5

Neka je V n-dimenzionalan linearni prostor i $L < V$ potprostor od V. Onda je i L konačnodimenzionalan prostor i vrijedi

$$\dim L \leq n\,.$$

Dokaz

Ako je $L = \{\Theta\}$, L je 0-dimenzionalan. Uzmimo zato da postoji $a_1 \in L$, $a_1 \neq \Theta$. Ako je $[\{a_1\}] = L$, L je 1-dimenzionalan. U protivnom, odaberimo $a_2 \notin [\{a_1\}]$ i nastavimo induktivno. Pretpostavimo da smo dobili linearno nezavisan skup $\{a_1, \ldots, a_k\}$ koji ne razapinje L. Onda postoji $a_{k+1} \in L$ takav da

$$a_{k+1} \notin [\{a_1, \ldots, a_k\}]\,.$$

Lako se provjeri da je skup $\{a_1, \ldots, a_k, a_{k+1}\}$ linearno nezavisan. Prema tome, svaki se linearno nezavisan skup u L, koji ne razapinje L, može proširiti do većeg linearno nezavisnog skupa u L. Međutim, taj proces ne može biti beskonačan jer bismo u tom slučaju dobili više od n linearno nezavisnih vektora u L, pa onda i u V, što je u suprotnosti s Kor. 7 iz 7.5. Prema tome, postoji m takav da je $[\{a_1, \ldots, a_m\}] = L$. Jasno je da pritom vrijedi $\dim L = m \leq n$. ∎

ZADACI

1. Opiši sve potprostore od V^3.

2. Koji su od podskupova $S \subset \mathbb{R}^n$ potprostori tog prostora:

   (a) $S = \{(\alpha_1, \ldots, \alpha_n) \mid \alpha_i \in \mathbb{Z}\,,\ \forall i\}$;

   (b) $S = \{(\alpha_1, \ldots, \alpha_n) \mid \alpha_1 = 2\alpha_2\}$;

   (c) $S = \{(\alpha_1, \ldots, \alpha_n) \mid \sum_{i=1}^{n} \alpha_i = 0\}$;

   (d) $S = \{(\alpha_1, \ldots, \alpha_n) \mid \sum_{i=1}^{n} \alpha_i = 1\}$;

   (e) $S = \{(\alpha_1, \ldots, \alpha_n) \mid \sum_{i=1}^{n} \alpha_i^2 = 0\}$;

   (f) $S = \{(\alpha_1, \ldots, \alpha_n) \mid \alpha_1 = \alpha_n\}$;

   (g) $S = \{(\alpha_1, \ldots, \alpha_n) \mid \alpha_{2i} = 0,\ \forall i\}$;

   (h) $S = \{(\alpha_1, \ldots, \alpha_n) \mid \alpha_2 = \ldots = \alpha_{2i} = \ldots\}$;

   (i) $S = \{(\alpha, \beta, \alpha, \beta, \ldots) \mid \alpha, \beta \in \mathbb{R}\}$?

U slučaju kad se radi o potprostorima, odredi jednu bazu i dimenziju za te potprostore.

3. Neka je $V = \mathbb{R}^{\mathbb{R}}$ skup svih realnih funkcija. Jesu li

   (a) skup svih parnih funkcija;

   (b) skup svih neparnih funkcija;

   (c) skup P svih polinoma;

   (d) skup svih neprekidnih funkcija,

   potprostori od V?

4. Koji su od podskupova prostora P potprostori:

   (a) $\{p \in P \mid p(1) = 0\}$;

   (b) $\{p \in P \mid \text{konstantni član od } p \text{ je } 0\}$?

5. Neka je $\{t_1, t_2, \ldots, t_k\}$ konačan skup realnih brojeva. Promatramo podskup od P_n dan s

$$L = \{p \in P_n \mid p(t_1) = p(t_2) = \ldots = p(t_k) = 0\} .$$

   Pokaži da je $L \subset P_n$ potprostor od P_n. Što možeš reći za slučaj kad je $k > n - 1$?

6. Neka je $\mathcal{L} = \mathcal{L}(V)$ skup svih potprostora prostora V. Pokaži da je "biti potprostor" relacija na $\mathcal{L}$, koja je refleksivna, antisimetrična i tranzitivna.

7. Za svaki $S \subset V$ je $[[S]] = [S]$. Dokaži!

8. Ako je $S \subset T \subset V$, onda je $[S] < [T]$. Dokaži!

9. Neka je prostor V konačnodimenzionalan i $L < V$ potprostor od V. Dokaži da je $\dim L < \dim V$ ako i samo ako je L pravi potprostor od V. Teorem nije točan u beskonačnodimenzionalnom slučaju. Neka je, naime, P prostor polinoma, a

$$P_0 = [\{1, t^2, t^4, \ldots\}] .$$

   Onda je $P_0 \subset P$ pravi potprostor od P (prostor parnih polinoma), a ipak je $\dim P_0 = \dim P = \aleph_0$.

7.7. Presjek i suma potprostora

Sada ćemo proučavati neke (binarne) operacije definirane na skupu $\mathcal{L} = \mathcal{L}(V)$ svih potprostora linearnog prostora V.

Neka su $L, M < V$ potprostori od V, a $L \cap M \subset V$ njihov presjek. Kako je $\Theta \in L$ i $\Theta \in M$, sigurno je $L \cap M \neq \emptyset$. Vrijedi i više, tj.

PROPOZICIJA 1

$L \cap M \subset V$ je potprostor od V. Nadalje, to je najveći potprostor od V koji je sadržan u L i M.

Dokaz

Neka su $a, b \in L \cap M$ bilo koji vektori, a $\alpha, \beta \in F$ skalari. Kako su $a, b \in L$, a L je potprostor, to je očito i $\alpha a + \beta b \in L$. Analogno zaključujemo da je $\alpha a + \beta b \in M$. Prema tome je $\alpha a + \beta b \in L \cap M$, pa je $L \cap M$ potprostor prema Kor. 2. iz 7.6. Druga tvrdnja je evidentna: $L \cap M$ je najveći podskup, pa onda i najveći potprostor sadržan u L i M. ■

Lako se provjeri da Prop. 1 vrijedi i u općenitijoj situaciji, tj. za bilo koju familiju (konačnu ili beskonačnu)

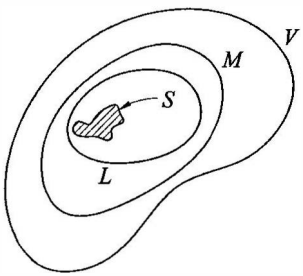
$$\{L_\alpha < V | \alpha \in A\}$$

potprostora iz V. Drugim riječima,

$$\bigcap_{\alpha \in A} L_\alpha \subset V$$

je potprostor od V, koji nazivamo **presjekom familije potprostora** $\{L_\alpha\}$.

Neka je sada $S \subset V$ bilo koji podskup. Zanima nas **najmanji potprostor** od V koji sadrži S, tj. takav potprostor $L < V$ za koji je $S \subset L$ i ima



svojstvo da za bilo koji potprostor M od V, za koji je $S \subset M$, vrijedi i $L < M$.

Očito je L najmanji potprostor koji sadrži S onda i samo onda ako je

$$L = \bigcap_{\alpha} L_\alpha \,, \qquad S \subset L_\alpha \,,$$

tj. ako je L presjek svih potprostora u V koji sadrže skup S. Vrijedi međutim i

PROPOZICIJA 2

Neka je $S \subset V$ bilo koji skup, a $L < V$ najmanji potprostor koji sadrži S. Onda je

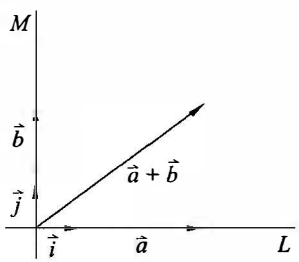
$$L = [S] \,,$$

tj. L se podudara s linearnim omotačem skupa S.

Dokaz

Ako je $S = \emptyset$, očito je $[S] = \{\Theta\} = L$ i tvrdnja je ispravna. Pretpostavimo zato da je $S \neq \emptyset$. Najprije, jer je $[S]$ potprostor od V i sadrži S, po definiciji minimalnosti je $L < [S]$. Obratno, neka je $x \in [S]$. To znači da postoje vektori $a_1, \ldots, a_k \in S$ takvi da je $x = \sum_{i=1}^{k} \alpha_i a_i$. No, jer je $S \subset L$, također je i $a_1, \ldots, a_k \in L$, a kako je L linearni prostor, zaključujemo da je i $\sum_{i=1}^{k} \alpha_i a_i \in L$, dakle $x \in L$. Prema tome je i $[S] < L$, dakle $[S] = L$ i tvrdnja je dokazana. ■

Neka su $L, M < V$ potprostori od V. Onda njihova unija $L \cup M \subset V$ općenito neće biti potprostor od V. Na primjer, u prostoru radijvektora



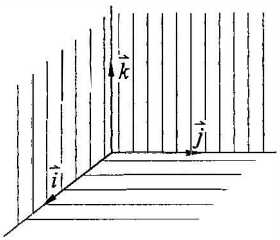
unija potprostora razapetih vektorima $\vec{i}$, odnosno $\vec{j}$, očito nije potprostor; najmanji potprostor koji tu uniju sadrži je čitava ravnina.

Lako se vidi da je $L \cup M$ potprostor sasvim iznimno, tj. ako i samo ako je $L < M$ ili $M < L$ (tada je $L \cup M = M$ ili $L \cup M = L$).

No, za svaki izbor potprostora $L, M < V$ jednoznačno je određen najmanji potprostor koji ih sadrži. Taj potprostor nazivamo **suma potprostora** L i M i označavamo s $L + M$. Dakle, po definiciji je

$$L + M = [L \cup M] \,.$$

Na primjer, $[\vec{i},\vec{j}]+[\vec{k}]=V^3$, ali je i $[\vec{i},\vec{j}]+[\vec{i},\vec{k}]=V^3$.



PROPOZICIJA 3

Neka su $L, M < V$ potprostori od V. Onda je

$$L+M=\{a+b \mid a\in L,\ b\in M\}\,.$$

Dokaz

Treba dokazati obje inkluzije. Neka je $x=a+b$, gdje je $a\in L, b\in M$. Onda je $a,b\in L\cup M$, pa je $a+b\in[L\cup M]=L+M$, tj. $x\in L+M$.

Obratno, neka je $y\in L+M=[L\cup M]$. Onda je $y=\sum_{i=1}^{k}\gamma_i c_i$, gdje je svaki $c_i\in L\cup M$, tj. $c_i\in L$ ili $c_i\in M$. Neka su vektori c_i numerirani tako da je $c_1,\ldots,c_r\in L$, a $c_{r+1},\ldots,c_k\in M$. Onda je i $\sum_{i=1}^{r}\gamma_i c_i=a\in L$, i nadalje $\sum_{i=r+1}^{k}\gamma_i c_i=b\in M$, jer su L i M potprostori, pa je

$$y=a+b\,,\ a\in L,\ b\in M$$

i tvrdnja je dokazana. ■

Pojam sume se poopćava i za više (konačno ili beskonačno) sumanada. Neka je $\{L_\alpha \mid \alpha\in A\}$ bilo koja familija potprostora od V. Onda definiramo njihovu sumu kao

$$\mathop{+}_{\alpha\in A} L_\alpha=\left[\bigcup_{\alpha} L_\alpha\right].$$

Prop. 3 lako se generalizira i za taj slučaj. Na primjer, za konačan broj sumanada vrijedi

$$L_1+L_2+\cdots+L_n=\{x=\sum_{i=1}^{n}a_i \mid a_i\in L_i\}\,.$$

Dimenzije sume i presjeka dvaju potprostora su u izvjesnom odnosu. O tome govori ovaj

TEOREM 4 (Teorem o dimenziji)
Neka su L i M potprostori od V. Onda vrijedi

$$\dim (L + M) = \dim L + \dim M - \dim (L \cap M) .$$

Dokaz
Označimo redom $\dim L = l, \dim M = m, \dim (L \cap M) = t$. Neka je

$$B_0 = (c_1, \ldots, c_t)$$

bilo koja baza za prostor $L \cap M$. No, skup vektora $\{c_k\}$ je linearno nezavisan u prostoru L, odnosno u prostoru M pa ga je prema Tm. 6 u 7.5. moguće dopuniti do baze prostora L, odnosno M. Postoje, dakle, vektori $\{a_i\} \subset L$ takvi da je skup

$$B_1 = (c_1, \ldots, c_t, a_1, \ldots, a_r) \tag{1}$$

baza prostora L. Isto tako, postoje vektori $\{b_j\} \subset M$ sa svojstvom da je

$$B_2 = (c_1, \ldots, c_t, b_1, \ldots, b_s) \tag{2}$$

baza za M. Primijetimo da iz definicije dimenzije slijedi

$$t + r = l \ , \qquad t + s = m \, . \tag{3}$$

Promatrajmo uređeni skup vektora

$$B = B_1 \cup B_2 = (a_1, \ldots, a_r, c_1, \ldots, c_t, b_1, \ldots, b_s) \, . \tag{4}$$

Očito je $B \subset L \cup M \subset [L \cup M] = L + M$. Ako pokažemo da je B baza za prostor $L + M$, teorem je dokazan, jer bismo iz (3) onda imali

$$\begin{aligned} \dim (L + M) &= r + t + s = (r + t) + (s + t) - t = \\ &= l + m - t = \dim L + \dim M - \dim (L \cap M) \, , \end{aligned}$$

što se i tvrdilo. Pokažimo da je B zaista baza za $L + M$. Prije svega, za $x \in L + M$ imamo prikaz $x = a + b$, gdje je $a \in L$, $b \in M$. No, jer je B_1 baza za L, a B_2 baza za M, x se očito može izraziti kao linearna kombinacija vektora iz B, što dokazuje da je B skup izvodnica za $L + M$. Ostaje dokazati da je B linearno nezavisan skup. Neka je

$$\alpha_1 a_1 + \ldots + \alpha_r a_r + \gamma_1 c_1 + \ldots + \gamma_t c_t + \beta_1 b_1 + \ldots + \beta_s b_s = \Theta \tag{5}$$

bilo koji prikaz nulvektora pomoću vektora iz skupa (4). Treba vidjeti da je nužno trivijalan. Označimo

$$\sum_{j=1}^{s} \beta_j b_j = b \, .$$

Kako su vektori $b_j \in B_2$, a B_2 je baza za M, to je $b \in M$. U drugu ruku, iz (5) dobivamo prikaz

$$b = -\alpha_1 a_1 - \cdots - \alpha_r a_r - \gamma_1 c_1 - \cdots - \gamma_t c_t \,, \tag{6}$$

iz kojeg, zbog (1), odmah razabiremo da je $b \in L$. Prema tome je

$$b \in L \cap M \,.$$

Odatle odmah slijedi da u (6) mora biti

$$\alpha_1 = \ldots = \alpha_r = 0 \,. \tag{7}$$

No, onda se (5) reducira na

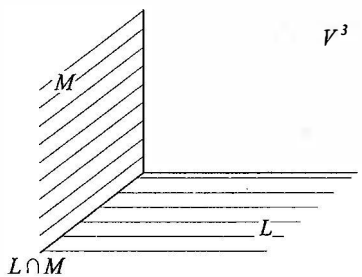
$$\gamma_1 c_1 + \cdots + \gamma_t c_t + \beta_1 b_1 + \cdots + \beta_s b_s = \Theta \,. \tag{8}$$

Međutim, vektori u relaciji (8) su iz baze B_2, dakle linearno nezavisni pa je prema tome i

$$\gamma_1 = \ldots = \gamma_t = \beta_1 = \ldots = \beta_s = 0 \,. \tag{9}$$

(7) i (9) pokazuju da je prikaz (5) nužno trivijalan, i dokaz je gotov. ■

Ilustrirajmo teorem jednim primjerom (vidi sliku).



Tu je

$$\begin{aligned} \dim V^3 &= \dim (L+M) = \dim L + \dim M - \dim (L \cap M) = \\ &= 2 + 2 - 1 = 3 \,. \end{aligned}$$

Od posebnog je interesa suma potprostora, koji se sijeku minimalno. Neka su $L, M < V$ potprostori, a $L + M < V$ njihova suma. Kažemo da je ta suma **direktna**, i pišemo

$$L \oplus M \,,$$

ako i samo ako je ispunjeno $L \cap M = \{\Theta\}$. Imamo npr. $V^3 = [\vec{i}, \vec{j}] \oplus [\vec{k}]$, $P = [\{1, t^2, t^4, \ldots\}] \oplus [\{t, t^3, t^5, \ldots\}]$.

PROPOZICIJA 5

Suma $L + M$ je direktna ako i samo ako svaki vektor $x \in L + M$ ima jednoznačan prikaz oblika

$$x = a + b\,,$$

gdje je $a \in L$, $b \in M$.

Dokaz

Tu je naglasak na jednoznačnosti prikaza. Neka je suma $L+M$ direktna, tj. neka vrijedi $L \cap M = \{\Theta\}$. Neka je $x \in L + M$ bilo koji vektor. Pretpostavimo da ima dva prikaza

$$x = a + b\,,$$

$$x = a' + b'\,,$$

gdje su $a, a' \in L$, $b, b' \in M$. Oduzimanjem dobivamo

$$\Theta = (a - a') + (b - b')\,. \tag{10}$$

No, jer je L potprostor, zaključujemo da je $a - a' \in L$. U drugu ruku, iz (10) imamo

$$a - a' = -(b - b') \in M\,,$$

jer je i M potprostor. Zato je

$$a - a' \in L \cap M = \{\Theta\}\,,$$

dakle $a - a' = \Theta$, tj. $a = a'$. Iz (10) onda slijedi i $b = b'$, pa je jednoznačnost prikaza dokazana. Obratno, neka je prikaz vektora iz $L + M$ jednoznačan. Pretpostavimo da suma nije direktna, tj. da je $L \cap M \neq \{\Theta\}$. Onda postoji $a \in L \cap M$, $a \neq \Theta$. Kako je $L \cap M$ potprostor, bit će i $-a \in L \cap M$. Možemo pisati

$$\Theta = a + (-a) \tag{11}$$

i interpretirati $a \in L, -a \in M$. No, prikaz (11) zajedno s trivijalnim prikazom Θ pokazuju da prikaz Θ nije jednoznačan, što je kontradikcija. ■

Imamo još jednu karakterizaciju direktne sume, pomoću Tm. 4.

PROPOZICIJA 6

Suma $L + M$ je direktna ako i samo ako vrijedi

$$\dim (L + M) = \dim L + \dim M\,. \tag{12}$$

Dokaz

Ako je suma $L+M$ direktna, imamo $L\cap M = \{\Theta\}$, pa je $\dim(L\cap M) = 0$ i tvrdnja slijedi iz Tm. 4.

Obratno, iz (12) i Tm. 4 slijedi da je $\dim(L\cap M) = 0$, odakle je $L\cap M = \{\Theta\}$, tj. suma $L + M$ je direktna. ■

Kao posljedica prethodnih rezultata lako se dokazuje i ovaj

KOROLAR 7

Ako je suma $L + M$ direktna, onda je unija baza za L i M jedna baza za $L + M$. ■

Pojam direktne sume se prirodno generalizira na više sumanada (vidi Zad. 5.). Pritom se lako provjeri da i u tom slučaju vrijede tvrdnje analogne Prop. 5, Prop. 6 i Kor. 7.

Od posebnog je interesa slučaj kada su potprostori $L, M \subset V$ takvi da je njihova direktna suma čitav V, tj. kada vrijedi

$$L \oplus M = V\,.$$

U tom slučaju kažemo da su L i M **direktni sumandi** prostora V ili da smo V **rastavili** u direktnu sumu potprostora L i M. Na primjer, $[\vec{i}, \vec{j}]$ i $[\vec{k}]$ su direktni sumandi prostora V^3.

PROPOZICIJA 8

Neka je $L < V$ bilo koji potprostor prostora V. Onda postoji potprostor $M < V$ takav da je

$$V = L \oplus M\,.$$

Dokaz

Ako je $L = \{\Theta\}$ ili $L = V$, tvrdnja je trivijalna. Neka je $(a_1, \ldots, a_k)$ jedna baza za L. Prema Tm 6 iz 7.5. ona se može vektorima $(a_{k+1}, \ldots, a_n)$ dopuniti do baze prostora V. Neka je

$$M = [\{a_{k+1}, \ldots, a_n\}]\,.$$

Za $x \in V$ imamo da je

$$x = \sum_{i=1}^{n} \alpha_i a_i = \sum_{i=1}^{k} \alpha_i a_i + \sum_{i=k+1}^{n} \alpha_i a_i = a + b,$$

gdje je $a \in L, b \in M$, pa je (Prop. 3) $x \in L+M$. Prema tome je $V \subset L+M$, dakle $V = L + M$. Nadalje, neka je $y \in L \cap M$. Onda je

$$y = \sum_{i=1}^{k} \beta_i a_i = \sum_{i=k+1}^{n} \beta_i a_i$$

pa imamo

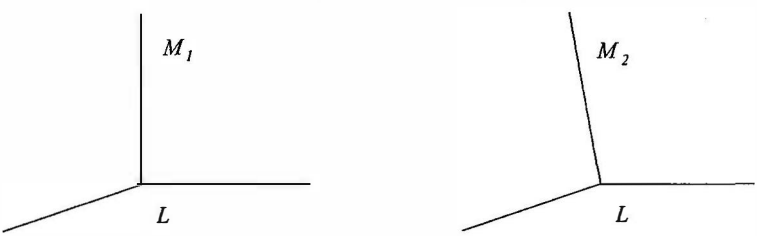
$$\sum_{i=1}^{k} \beta_i a_i - \sum_{i=k+1}^{n} \beta_i a_i = \Theta \, .$$

Kako je $(a_1, \ldots, a_n)$ baza prostora, dakle i linearno nezavisan skup, odatle slijedi

$$\beta_1 = \cdots = \beta_n = 0$$

pa je $y = \Theta$, tj. $L \cap M = \{\Theta\}$. Zato imamo $V = L \oplus M$. ■

Za potprostor M kažemo da je **direktni komplement** potprostora L u prostoru V. Kako je to svojstvo simetrično, govorimo također da su L i M **par komplementarnih potprostora** od V. Iz konstrukcije je jasno da direktni komplement nije jednoznačno određen s L.



Piše se katkad i $M = V \ominus L$ i kaže da je M **direktna razlika** prostora V i prostora L.

ZADACI

1. Neka je $\mathcal{L}$ skup svih potprostora prostora V. Pokaži da su strukture $(\mathcal{L}, \cap)$ i $(\mathcal{L}, +)$ komutativni monoidi.

2. Neka su $L, M, N \in \mathcal{L}$. Dokaži da vrijedi

$$L \cap (M + (L \cap N)) = (L \cap M) + (L \cap N) \, .$$

Nadalje, uvjeri se da distribucija

$$L \cap (M + N) = (L \cap M) + (L \cap N)$$

općenito nije istinita. Uvijek je, međutim,

$$L \cap (M + N) \supseteq (L \cap M) + (L \cap N) \, .$$

Dokaži i generaliziraj!

3. Dokaži ovu generalizaciju Prop. 3:

$$\underset{\alpha \in A}{+} L_\alpha = \{a_{\alpha_1} + \cdots + a_{\alpha_k} | a_{\alpha_i} \in L_{\alpha_i}\} \, .$$

4. Dokaži: Dimenzija presjeka dvaju potprostora od V nije manja od sume dimenzija tih potprostora, umanjene za dimenziju prostora V. Tako je npr. za $\mathbb{R}^3, \mathbb{R}^5 < \mathbb{R}^7$, $\dim(\mathbb{R}^3 \cap \mathbb{R}^5) \geq 3 + 5 - 7 = 1$.

5. Generalizirajmo pojam direktne sume. Neka su $L_i < V$ potprostori u V, a $L = L_1 + L_2 + \cdots + L_k$ njihova suma. Kažemo da je L **direktna suma** i pišemo

$$L = \bigoplus_{i=1}^{k} L_i = L_1 \oplus \cdots \oplus L_k \,,$$

ako vrijedi

$$(L_1 + \cdots + L_{i-1} + L_{i+1} + \cdots + L_k) \cap L_i = \{\Theta\} \tag{13}$$

za svaki $i = 1, \ldots, k$. Dokaži u ovoj generalnijoj situaciji Prop. 5, Prop. 6 i Kor. 7. Pokaži da je definicijski zahtjev (13) ekvivalentan sa zahtjevom

$$(L_1 + \cdots + L_{i-1}) \cap L_i = \{\Theta\}, \quad \forall\, i = 2, \ldots, k \,.$$

6. Neka je $(a_1, \ldots, a_n)$ baza za prostor V, a $L_i = [\{a_i\}]$, za $i = 1, \ldots, n$. Onda je

$$V = \bigoplus_{i=1}^{n} L_i \,.$$

Dokaži!

7. Dokaži: Suma $L_1 + \cdots + L_k < V$ je direktna ako i samo ako je prikaz $\Theta = \sum_{i=1}^{k} a_i$, $a_i \in L_i$, jedinstven, tj. ako i samo ako povlači $a_i = \Theta$, za $i = 1, \ldots, k$.

8. Neka su $L, M, N < V$ potprostori od V. Pokaži da $L \cap M = L \cap N$, $L + M = L + N$ i $M < N$ povlači $M = N$.

9. Neka su $A, B < P$ potprostori definirani s

$$A = \{p \in P \mid p(1) = 0\} \,, \quad B = \{p \in P \mid p(2) = 0\}.$$

Odredi $A \cap B$ i $A + B$.

10. Pokaži da bilo koja dva potprostora iste dimenzije danog (konačnodimenzionalnog) prostora imaju zajednički direktni komplement. Uvjeri se da tvrdnja nije točna za tri potprostora.

7.8. Kvocijentni prostor. Direktni produkt prostora

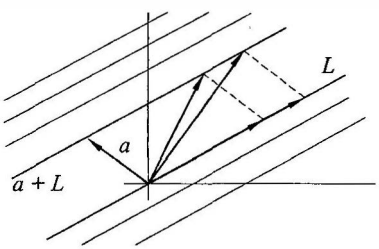
Neka je V linearni prostor nad poljem F, a $L < V$ potprostor od V. Posebno, L je podgrupa aditivne grupe V, i to normalna (jer je zbrajanje vektora komutativno), pa je dobro definirana kvocijentna grupa V/L. Podsjetimo se (vidi 3.7.), da je kvocijentni skup oblika

$$V/L = \{a + L \mid a \in V\} ,$$

a grupovna operacija (zbrajanje klasa) inducirana je zbrajanjem u V, tj.

$$(a + L) + (b + L) = (a + b) + L .$$

Elemente grupe V/L nazivamo **linearnim mnogostrukostima** u V. Točnije, za $a + L$ kažemo da je linearna mnogostrukost generirana vektorom a, "paralelna" s potprostorom L. Kaže se, također, da je mnogostrukost $a + L$ dobivena translacijom potprostora L za vektor a. Ti nazivi imaju svoje geometrijsko opravdanje. Na primjer, u prostoru radijvektora slika izgleda ovako



Imamo, dakle, dekompoziciju prostora V u mnogostrukosti, "paralelne" s potprostorom L. Spomenimo da se **dimenzija linearne mnogostrukosti** definira kao

$$\dim(a + L) = \dim L .$$

Grupu V/L željeli bismo organizirati u linearni prostor nad poljem F. U tu svrhu dokažimo najprije da vrijedi

LEMA 1

Za bilo koji skalar $\alpha \in F$ i bilo koju klasu $a + L \in V/L$ imamo

$$\alpha(a + L) \subset (\alpha a) + L .$$

Dokaz

Ovdje je, naravno,

$$\alpha(a + L) = \{\alpha(a + x) \mid x \in L\} .$$

Kako je $L < V$ potprostor, za $x \in L$ će biti također $\alpha x \in L$, pa imamo

$$\alpha(a + x) = \alpha a + \alpha x \in \alpha a + L$$

i tvrdnja je dokazana. ■

Na osnovi leme onda definiramo **množenje mnogostrukosti skalarima**,

$$F \times V/L \to V/L\,,$$

stavljajući

$$\alpha(a + L) = \alpha a + L$$

za svaki $\alpha \in F$ i $a + L \in V/L$. Za to množenje kažemo da je **inducirano** operacijom množenja vektora skalarima (hibridnim množenjem) u prostoru V.

TEOREM 2

Skup V/L je, uz inducirane operacije zbrajanja i množenja skalarom, linearni prostor nad poljem F.

Dokaz

Već smo vidjeli da je V/L aditivna grupa, u kojoj je neutralni element klasa L. Ostaje provjeriti aksiome (1) – (4) iz definicije linearnog prostora. Provjerimo npr. (4). Neka je $\alpha \in F$ bilo koji skalar, a $\overline{a}, \overline{b} \in V/L$ bilo koje klase. Onda je $\overline{a} = a + L$ i $\overline{b} = b + L$, pa imamo redom

$$\begin{aligned}
\alpha(\overline{a} + \overline{b}) &= \alpha[(a + L) + (b + L)] = \alpha[(a + b) + L] = \\
&= \alpha(a + b) + L = (\alpha a + \alpha b) + L = \\
&= (\alpha a + L) + (\alpha b + L) = \\
&= \alpha(a + L) + \alpha(b + L) = \alpha\overline{a} + \alpha\overline{b}\,.
\end{aligned}$$

■

Linearni prostor V/L nazivamo **kvocijentni prostor** prostora V po prostoru L. Na primjer, $V^3/V^1 = V^2$, $\mathbb{R}^n/\mathbb{R}^k = \mathbb{R}^{n-k}$, $P/[\{1, t^2, t^4, ...\}] = [\{t, t^3, t^5, ...\}]$, gdje jednakosti treba shvatiti u smislu izomorfnosti (na razini grupa, zasad!).

Sljedeći teorem govori o dimenziji kvocijentnog prostora.

TEOREM 3

Neka je V linearni prostor, a $L < V$ njegov potprostor. Onda je

$$\dim V/L = \dim V - \dim L\,.$$

Dokaz

Neka je $\dim V = n$, $\dim L = l \leq n$. Treba vidjeti da je $\dim V/L = n - l$. Neka je $M < V$ komplementarni potprostor od L, $L \oplus M = V$ (Prop. 8 u 7.7.). Onda je $\dim M = \dim V - \dim L = n - l$. Neka je

$$(a_1, \ldots, a_{n-l}) \tag{1}$$

jedna baza za M. Promatrajmo vektore

$$(\overline{a}_1, \ldots, \overline{a}_{n-l}) \tag{2}$$

iz V/L, definirane s

$$\overline{a}_i = a_i + L, \quad i = 1, \ldots, n - l\,. \tag{3}$$

Tvrdimo da ti vektori čine bazu za V/L. Ako to dokažemo, onda smo gotovi, jer je tada zaista

$$\dim V/L = n - l\,.$$

Pretpostavimo

$$\sum_{i=1}^{n-l} \alpha_i \overline{a}_i = \Theta_{V/L}\,. \tag{4}$$

Zbog (3) imamo

$$\sum_{i=1}^{n-l} \alpha_i (a_i + L) = L\,,$$

i odatle

$$(\sum_{i=1}^{n-l} \alpha_i a_i) + L = L\,,$$

pa je

$$\sum_{i=1}^{n-l} \alpha_i a_i \in L\,.$$

S druge strane, kao linearna kombinacija vektora iz M je

$$\sum_{i=1}^{n-l} \alpha_i a_i \in M\,.$$

Prema tome je

$$\sum_{i=1}^{n-l} \alpha_i a_i \in L \cap M = \{\Theta\}\,,$$

tj.

$$\sum_{i=1}^{n-l} \alpha_i a_i = \Theta ,$$

a jer je skup (1) linearno nezavisan, izlazi da je

$$\alpha_1 = \ldots = \alpha_{n-l} = 0 ,$$

što zbog (4) znači da je i (2) linearno nezavisan skup vektora u V/L.

Ostaje pokazati da je (2) skup izvodnica. Neka je $\overline{x} \in V/L$ bilo koji vektor. Onda je $\overline{x} = x + L$, gdje je $x \in V$. No, x se može prikazati kao $x = a + b$, gdje je $a \in M$, $b \in L$. Onda imamo

$$\overline{x} = x + L = (a + b) + L = (a + L) + (b + L) = (a + L) + L = a + L .$$

Kako je (1) baza za M, imamo

$$\overline{x} = (\sum_{i=1}^{n-l} \beta_i a_i) + L = \sum_{i=1}^{n-l} \beta_i (a_i + L) = \sum_{i=1}^{n-l} \beta_i \overline{a}_i ,$$

pa je (2) i skup izvodnica te je dokaz gotov. ■

Za $\dim V/L$ se kaže da je **kodimenzija** potprostora L u prostoru V.

Neka su sada U i V linearni prostori nad istim poljem F, a

$$U \times V = \{(a, b) \mid a \in U, b \in V\}$$

Kartezijev produkt skupova U i V. Taj skup želimo na prirodan način organizirati u linearni prostor. Na $U \times V$ definiramo operacije zbrajanja i množenja skalarom koordinatno s

$$x + y = (a_1, b_1) + (a_2, b_2) = (a_1 + a_2, b_1 + b_2) ,$$

odnosno, za $\lambda \in F$,

$$\lambda x = \lambda(a, b) = (\lambda a, \lambda b) .$$

TEOREM 4

Skup $U \times V$ je, uz upravo definirane operacije zbrajanja i množenja skalarom, linearni prostor nad poljem F.

Dokaz

Jasno je da je $U \times V$ Abelova grupa u kojoj ulogu nule ima par nulvektora (Θ_U, Θ_V). Ostaje provjeriti aksiome (1)–(4) linearnog prostora. Imamo npr. za aksiom (1):

$$\begin{aligned} \lambda(\mu x) &= \lambda[\mu(a,b)] = \lambda(\mu a, \mu b) = \\ &= (\lambda(\mu a), \lambda(\mu b)) = ((\lambda\mu)a, (\lambda\mu)b) = \\ &= (\lambda\mu)(a,b) = (\lambda\mu)x \ . \end{aligned}$$

Slično se provjere i ostali aksiomi. ■

Prostor $U \times V$ nazivamo **direktni produkt prostora** U i V. O dimenziji tog prostora govori

TEOREM 5

Neka je $U \times V$ direktni produkt prostora U i V. Onda je

$$\dim(U \times V) = \dim U + \dim V \ .$$

Dokaz

Neka su $A = (a_1, \ldots a_m)$ i $B = (b_1, \ldots b_n)$ baze prostora U, odnosno V. Promatramo skup

$$C = ((a_1, \Theta_V), \ldots, (a_m, \Theta_V), (\Theta_U, b_1), \ldots, (\Theta_U, b_n)) \ .$$

Tvrdimo da je C baza za $U \times V$. Ako to dokažemo, onda smo gotovi, jer će tada biti

$$\dim\,(U \times V) = m + n = \dim U + \dim V \ ,$$

kako teorem i tvrdi. No, C je skup izvodnica jer za bilo koji $(a,b) \in U \times V$ imamo

$$\begin{aligned} (a,b) &= (\sum_{i=1}^{m} \alpha_i a_i, \sum_{k=1}^{n} \beta_k b_k) = (\sum_{i=1}^{m} \alpha_i a_i, \Theta_V) + (\Theta_U, \sum_{k=1}^{n} \beta_k b_k) = \\ &= \sum_{i=1}^{m} \alpha_i (a_i, \Theta_V) + \sum_{k=1}^{n} \beta_k (\Theta_U, b_k) \ . \end{aligned}$$

Da bismo dokazali linearnu nezavisnost skupa C, promatramo

$$\sum_{i=1}^{m} \alpha_i (a_i, \Theta_V) + \sum_{k=1}^{n} \beta_k (\Theta_U, b_k) = \Theta_{U \times V} \ ,$$

dakle

$$(\sum_{i=1}^{m} \alpha_i a_i, \sum_{k=1}^{n} \beta_k b_k) = (\Theta_U, \Theta_V) \ .$$

Odatle slijedi

$$\sum_{i=1}^{m} \alpha_i a_i = \Theta_U \quad \text{i} \quad \sum_{k=1}^{n} \beta_k b_k = \Theta_V \ ,$$

a kako su A, odnosno B, baze za U i V, zaključujemo da je nužno

$$\alpha_1 = \ldots = \alpha_m = 0 \quad \text{i} \quad \beta_1 = \ldots = \beta_n = 0 \ ,$$

pa je skup C zaista linearno nezavisan i tvrdnja je dokazana. ■

Napomenimo na kraju da se, zbog Tm. 5 i Tm. 3, katkada govori, da se dimenzija linearnog prostora ravna po **logaritamskom zakonu**.

ZADACI

1. Neka je $V = L \oplus M$. Pokaži da je onda V/L izomorfan s M (na razini grupa, zasad!). Što npr. možeš reći o prostorima $V/\{\Theta\}$ i V/V?

2. Što možeš reći o prostoru P/P_n? Je li taj prostor konačnodimenzionalan? Neka je, nadalje, $L = \{p \in P \mid t^n \mid p\}$ potprostor od P, koji se sastoji od svih polinoma djeljivih s t^n. Kako izgleda prostor P/L?

3. Neka je V prostor svih neprekidnih realnih funkcija definiranih na $[-1, 1]$, a L potprostor svih parnih funkcija iz V. Što možeš reći o prostoru V/L?

4. Pokaži da su $U \times \{\Theta_V\} \subset U \times V$ i $\{\Theta_U\} \times V \subset U \times V$ potprostori od $U \times V$, izomorfni s U odnosno V.

5. Neka su $L, M < V$ potprostori od V takvi da je $L \cap M = \{\Theta\}$. Onda je $L \oplus M$ izomorfan s $L \times M$ (na razini aditivnih grupa, zasad!). Dokaži!

6. Generaliziraj definiciju i svojstva direktnog produkta prostora na više faktora (konačno, prebrojivo, neprebrojivo). Uvjeri se npr. da je

$$F^n = \underbrace{F \times F \times \cdots \times F}_{n}$$

za bilo koje polje F.

7. Podskup direktnog produkta od beskonačno mnogo faktora, koji se sastoji od nizova (funkcija) koji su skoro svagdje nula (tj. nisu nula najviše na konačno mnogo mjesta), naziva se **direktna suma** danih **prostora**. Pokaži da je direktna suma potprostor direktnog produkta prostora.

8

LINEARNI OPERATORI

Kao i do sada, i u slučaju linearnih prostora će nas posebno zanimati ona preslikavanja među njima, koja poštuju njihovu strukturu. To su tzv. linearna preslikavanja ili linearni operatori. Njihovo izučavanje čini veći i sigurno najvažniji dio linearne algebre.

8.1. Definicija i osnovna svojstva

Neka su U i V linearni prostori nad istim poljem F, a

$$f : U \to V$$

neko preslikavanje. Kažemo da je to preslikavanje **linearni operator** ako ima ova svojstva:

(1) aditivnost, tj.

$$f(a+b) = f(a) + f(b)\,, \quad \forall\, a, b \in U\,,$$

(2) Homogenost, tj.

$$f(\alpha a) = \alpha\, f(a)\,, \quad \forall\, \alpha \in F\,,\ a \in U\,.$$

Naziv linearni operator proizlazi iz njegovih svojstava i činjenice da se preslikavanja kojima su domena U i kodomena V linearni prostori tradicionalno nazivaju **operatorima**. Kaže se još da operator djeluje na prostoru U i prima vrijednosti u prostoru V. Uobičajeni nazivi za linearni operator su još **homomorfizam linearnih prostora**, kao i **linearno preslikavanje**, odnosno **linearna transformacija**.

Primijetimo da je, zbog uvjeta (1), svaki linearni operator f homomorfizam na razini aditivnih grupa linearnih prostora. Zato je uvijek

$$\begin{aligned} f(\Theta_U) &= \Theta_V \quad \text{i} \\ f(-a) &= -f(a)\,, \quad \forall a \in U\,. \end{aligned}$$

Uvjete (1) i (2) u definiciji linearnog operatora možemo objediniti, pa imamo ovaj kriterij za prepoznavanje linearnog operatora:

PROPOZICIJA 1

Preslikavanje $f : U \to V$ je linearni operator onda i samo onda, ako za svaki izbor $\alpha, \beta \in F$ i svaki izbor $a, b \in U$ vrijedi

$$f(\alpha a + \beta b) = \alpha f(a) + \beta f(b)\,.$$

Dokaz

Ako je f linearni operator, imamo

$$f(\alpha a + \beta b) = (1) = f(\alpha a) + f(\beta b) = (2) = \alpha f(a) + \beta f(b).$$

Obratno, odabirom $\alpha = \beta = 1$ dobivamo (1), a stavljanjem $b = \Theta$ dobivamo (2), pa je f linearni operator po definiciji. ■

Uvjet iz Prop. 1. možemo generalizirati. Vrijedi, naime,

PROPOZICIJA 2

Neka su $a_i \in U$ bilo koji vektori, a $\alpha_i \in F$ skalari, $i = 1, \ldots, k$. Onda za linearni operator f vrijedi

$$f(\sum_{i=1}^{k} \alpha_i a_i) = \sum_{i=1}^{k} \alpha_i\, f(a_i)\,.$$

Dokaz

Indukcijom. Za $k = 1$ to je uvjet (2) iz definicije. Pretpostavimo da je tvrdnja istinita za $k - 1$ vektor. Onda imamo redom, rabeći uvjete (1) i (2) te pretpostavku indukcije,

$$\begin{aligned} f(\sum_{i=1}^{k} \alpha_i a_i) &= f(\sum_{i=1}^{k-1} \alpha_i a_i + \alpha_k a_k) = \\ &= f(\sum_{i=1}^{k-1} \alpha_i a_i) + f(\alpha_k a_k) = \\ &= \sum_{i=1}^{k-1} \alpha_i\, f(a_i) + \alpha_k\, f(a_k) = \sum_{i=1}^{k} \alpha_i\, f(a_i). \end{aligned}$$

■

Propozicija zapravo tvrdi da linearna kombinacija vektora prelazi linearnim preslikavanjem u linearnu kombinaciju slika tih vektora (s istim koeficijentima).

PROPOZICIJA 3

Kompozicija linearnih operatora je linearni operator.

Dokaz

Neka su $f : U \to V$ i $g : V \to W$ linearni operatori, a $h = g \circ f : U \to W$ njihova kompozicija. Kao kompozicija homomorfizama, h je homomorfizam aditivnih grupa, dakle aditivan. Nadalje je

$$\begin{aligned} h(\alpha a) &= (g \circ f)(\alpha a) = g[f(\alpha a)] = g[\alpha f(a)] = \\ &= \alpha[g(f(a))] = \alpha[(g \circ f)(a)] = \alpha h(a) \end{aligned}$$

pa je h zaista linearni operator. ■

ZADACI

1. Da bi $f : U \to V$ bio linearni operator, nužno je i dovoljno da vrijedi $f(\alpha a + b) = \alpha f(a) + f(b)$, za svaki $\alpha \in F$ i $a, b \in U$. Dokaži!

2. Neka je $f : U \to V$ linearni operator, a $L < U$ potprostor od U. Neka je $g = f/L$. Pokaži da je **restrikcija** $g : L \to V$ linearni operator.

3. Neka je $U = L \oplus M$, a $f : L \to V$ i $g : M \to V$ neka su linearni operatori. Onda postoji jedinstveni operator $h : U \to V$ sa svojstvom da je $h/L = f$ i $h/M = g$. Dokaži! Drugim riječima, linearni operator je jednoznačno određen ako je poznato njegovo djelovanje na direktnim sumandima prostora. Pišemo $h = f \oplus g$. [Uputa: Definiraj $h(x) = h(a + b) = f(a) + g(b)$.]

4. Neka je $L < U$ potprostor i $g : L \to V$ linearni operator. Onda postoji **proširenje** $f : U \to V$ od g, $f|_L = g$, koje je linearni operator. Je li f jednoznačno određen s g?

5. Generaliziraj pojam linearnog operatora za slučaj kad je U linearni prostor nad poljem E, V prostor nad poljem F i $E < F$ potpolje od F.

6. Dokaži: Svaki homomorfizam linearnih prostora nad poljem $\mathbb{Q}$ racionalnih brojeva (shvaćen kao homomorfizam aditivnih grupa) jest linearni operator. Tvrdnja je istinita i za vektorske prostore nad poljem $\mathbb{Z}_p$.

7. Neka je $f : U \to V$ linearni operator, a $a \in V$ dani vektor. Onda operator

$$\theta : U \to V ,$$

definiran s

$$\theta(x) = f(x) + a ,$$

nazivamo **afini operator**. Pokaži da je operator $\theta : U \to V$ afini ako i samo ako vrijedi

$$\theta(\sum \alpha_i a_i) = \sum \alpha_i \theta(a_i) ,$$

za svaki izbor $a_i \in U$ i svaki izbor $\alpha_i \in F$, za koje je $\sum \alpha_i = 1$.

8.2. Primjeri linearnih operatora

Navest ćemo nekoliko tipičnih primjera linearnih operatora, koji su i od teorijskog značenja.

1. Neka je V linearni prostor nad poljem F, a $\lambda \in F$ dani skalar. Neka je $h : V \to V$ operator definiran s

$$h(x) = \lambda x ,$$

koji nazivamo **homotetija u prostoru** V, s **koeficijentom** λ. Kako je

$$\begin{aligned} h(\alpha x + \beta y) &= \lambda(\alpha x + \beta y) = \lambda(\alpha x) + \lambda(\beta y) = \\ &= (\lambda\alpha)x + (\lambda\beta)y = (\alpha\lambda)x + (\beta\lambda)y = \\ &= \alpha(\lambda x) + \beta(\lambda y) = \alpha\, h(x) + \beta\, h(y) , \end{aligned}$$

to je h linearni operator.

Specijalno, odabirući $\lambda = 0$, odnosno $\lambda = 1$, vidimo da su **nuloperator**

$$n(x) = 0 , \qquad \forall x \in V ,$$

i **jedinični operator** (identiteta)

$$e(x) = x , \qquad \forall x \in V ,$$

linearni operatori.

2. Neka je $L < V$ potprostor, a $i : L \to V$ preslikavanje definirano s $i(x) = x$, $\forall x \in L$, tj. **inkluzija**. Lako se provjeri da je i linearni operator.

3. Neka je $L < V$ potprostor od V. Neka je M direktni komplement od L, $V = L \oplus M$. Onda definiramo operator

$$p_M : V \to L$$

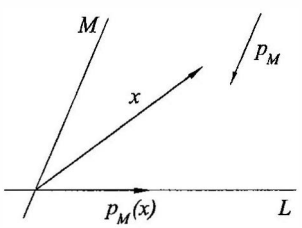
na ovaj način: Svaki $x \in V$ ima jednoznačan prikaz $x = a + b$, gdje je $a \in L$, $b \in M$, pa stavljamo

$$p_M(x) = p_M(a + b) = a \, .$$

Operator p_M zovemo **projekcija** ili **projektor** prostora V na potprostor L, u smjeru M. Kako je

$$\begin{aligned} p_M(\alpha x + \beta y) &= p_M[\alpha(a_1 + b_1) + \beta(a_2 + b_2)] = \\ &= p_M[\underbrace{(\alpha a_1 + \beta a_2)}_{\in L} + \underbrace{(\alpha b_1 + \beta b_2)}_{\in M}] = \\ &= \alpha a_1 + \beta a_2 = \alpha\, p_M(x) + \beta\, p_M(y) \, , \end{aligned}$$

vidimo da je p_M linearni operator.



Na taj način možemo prostor $V = L \oplus M$ projicirati na njegove direktne sumande. Kad bi bilo samo $V = L + M$, konstrukcija ne bi funkcionirala. Zašto?

4. Neka je opet $L < V$ potprostor od V. Onda definiramo

$$q : V \to V/L \, ,$$

stavljajući

$$q(x) = x + L \, ,$$

i taj operator nazivamo **prirodna projekcija** prostora V na kvocijentni prostor ili, također, **kvocijentni operator**. Imamo

$$\begin{aligned} &q(\alpha x + \beta y) = (\alpha x + \beta y) + L = \\ &= \alpha(x + L) + \beta(y + L) = \alpha\, q(x) + \beta\, q(y) \, , \end{aligned}$$

što pokazuje da je prirodna projekcija linearni operator.

5. Neka je P prostor polinoma, a

$$\mathrm{d} : P \to P$$

operator definiran s

$$\mathrm{d}(p) = \mathrm{d}(\sum_{j=0}^{k} \alpha_j t^j) = \sum_{j=0}^{k} j \cdot \alpha_j t^{j-1} ,$$

koji nazivamo **operator deriviranja** na P. Pišemo kraće $\mathrm{d}(p) = p'$. Lako se provjeri da je d linearni operator. Primijetimo da je i

$$\mathrm{d}/P_n : P_n \to P_{n-1}$$

linearni operator.

6. Neka je P opet prostor polinoma, a

$$s : P \to P$$

operator dan sa

$$s(p) = s(\sum_{j=0}^{k} \alpha_j t^j) = \sum_{j=0}^{k} \frac{\alpha_j}{j+1} \cdot t^{j+1} ,$$

koji nazivamo **operatorom integriranja** na P. Pišemo

$$s(p) = \int_0^t p(t)\,\mathrm{d}t \quad .$$

Odmah se vidi da je s linearni operator. Također, restrikcija

$$s/P_n : P_n \to P_{n+1}$$

je linearni operator.

ZADACI

1. Neka je $V^2(O)$ prostor radijvektora. Svaka rotacija (oko O) u tom prostoru je linearni operator. Dokaži! Slično, definiramo

$$r_\alpha : \mathbb{R}^2 \to \mathbb{R}^2$$

s

$$r_\alpha(x, y) = (x\cos\alpha - y\sin\alpha,\ x\sin\alpha + y\cos\alpha) ,$$

i taj operator nazivamo **rotacija** u $\mathbb{R}^2$ za kut α. Pokaži da je r_α linearni operator za svaki $\alpha \in \mathbb{R}$. Što dobivaš za $\alpha = \pi$, odnosno $\alpha = 2\pi$?

2. **Zrcaljenje**

$$z : \mathbb{R}^2 \to \mathbb{R}^2 ,$$

definirano s

$$z(x, y) = (y, x) ,$$

je linearni operator. Dokaži!

3. Je li **translacija** za $(a, b) \in \mathbb{R}^2$,

$$t : \mathbb{R}^2 \to \mathbb{R}^2$$

dana s

$$t(x, y) = (x + a, y + b) ,$$

linearni operator? A afini?

4. Neka je F bilo koje polje, a

$$f : F^2 \to F^3 \quad \text{i} \quad g : F^3 \to F^2$$

operatori dani s $f(\alpha, \beta) = (\alpha, \beta, \alpha + \beta)$, odnosno $g(\alpha, \beta, \gamma) = (\alpha, \beta)$. Pokaži da su f i g linearni operatori (g je očigledno projektor na $F^2 < F^3$). Što možeš reći o kompozicijama $f \circ g$ i $g \circ f$? Koja je od njih identiteta?

5. Za svaki $i = 1, \ldots, n$ definiramo operator

$$p_i : F^n \to F$$

s

$$p_i(x) = p_i(\alpha_1, \ldots, \alpha_i, \ldots, \alpha_n) = \alpha_i ,$$

koji zovemo **i-ta koordinatna funkcija** ili **projektor na i-tu koordinatu**. Pokaži da je p_i linearni operator.

6. Neka je V linearni prostor nad F, a $a_1, \ldots, a_n \in V$ bilo koji izbor vektora. Definiramo

$$f : F^n \to V ,$$

stavljajući

$$f(\alpha_1, \ldots, \alpha_n) = \alpha_1 a_1 + \cdots + \alpha_n a_n .$$

Dokaži da je f linearni operator. Neka je

$$e_i = (0, \ldots, \underset{i}{1}, \ldots, 0) \in F^n .$$

Onda je očito

$$f(e_i) = a_i , \quad i = 1, \ldots, n .$$

Dokaži da je f jedini linearni operator $F^n \to V$ s tim svojstvom.

7. Neka je p bilo koja permutacija skupa $\{1, \ldots, n\}$. Neka je $\overline{p} : F^n \to F^n$ preslikavanje, dano s

$$\overline{p}(\alpha_1, \ldots, \alpha_n) = (\alpha_{p(1)}, \ldots, \alpha_{p(n)}) .$$

Pokaži da je $\overline{p}$ linearni operator.

8. Neka je P prostor polinoma, a $f : P \to P$ operator dan s

(a) $f(p) = p \circ q$, gdje je $q \in P$ dani polinom;

(b) $f(p) = q$, gdje je $q(t) = p(t+1) - p(t), \ \forall t \in \mathbb{R}$;

(c) $f(p) = q \cdot p$, gdje je $q \in P$ dani polinom.

Pokaži da je f u svakom slučaju linearni operator.

9. Neka je $V = \mathbb{R}^{\mathbb{R}}$ prostor svih realnih funkcija. Za $f \in V$ definiramo pridruženja

(a) $f(t) \mapsto f(t+1)$;

(b) $f(t) \mapsto f(t) + 1$;

(c) $f(t) \mapsto [f(t)]^2$;

(d) $f(t) \mapsto (f \circ f)(t)$.

Koja su od tih pridruženja linearni operatori na V? Deriviranje i integriranje nisu linearni operatori na V. Zašto? Na kojim su potprostorima od V to dobro definirani linearni operatori?

10. Na prostoru $\mathbb{C}$ kompleksnih brojeva nad $\mathbb{R}$ definiramo preslikavanje

$$k : \mathbb{C} \to \mathbb{C}$$

s

$$k(x + iy) = x - iy ,$$

koje zovemo **konjugiranje**. Uvjeri se da je k linearni operator.

11. **Projekcije** $U \times V \to U$ i $U \times V \to V$ direktnog produkta prostora na faktore su linearni operatori. Dokaži!

8.3. Egzistencija i način zadavanja linearnih operatora

Za bilo koji par prostora U i V, nad istim poljem F, postoje linearni operatori $U \to V$. Takav je npr. nuloperator $n(a) = \Theta_V$, $\forall a \in U$. Pokazat ćemo, međutim, da u slučaju kad su $U, V \neq \{\Theta\}$ uvijek postoje i netrivijalni linearni operatori. To slijedi iz ovog rezultata:

TEOREM 1

Neka je $(a_1, \ldots, a_k) \subset U$ linearno nezavisan skup vektora iz U, a skup $(b_1, \ldots, b_k) \subset V$ bilo koji skup vektora iz V. Onda postoji bar jedan linearni operator $f : U \to V$ koji ima svojstvo

$$f(a_i) = b_i\,, \qquad \forall i = 1, \ldots, k\,.$$

Dokaz

Ako skup $(a_1, \ldots, a_k)$ nije baza za U, možemo ga (Tm. 6. u 7.5.), **i to na više načina**, dopuniti do baze prostora U. Neka je

$$(a_1, \ldots, a_k, a_{k+1}, \ldots, a_n)$$

jedno takvo proširenje. Neka je, nadalje,

$$(b_1, \ldots, b_k, b_{k+1}, \ldots, b_n) \subset V$$

bilo koje proširenje danog skupa vektora $(b_1, \ldots, b_k)$ iz V.

Neka je $a \in U$ bilo koji vektor. Onda postoji jednoznačan prikaz

$$a = \sum_{i=1}^{n} \alpha_i a_i\,,$$

pa definiramo operator $f : U \to V$ s

$$f(a) = f(\sum_{i=1}^{n} \alpha_i a_i) = \sum_{i=1}^{n} \alpha_i b_i \in V\,. \tag{1}$$

Tvrdimo da je f linearni operator i da ima traženo svojstvo. Zaista, stavljajući u (1) $\alpha_i = 1$, $\alpha_j = 0$, $j \neq i$, dobivamo

$$f(a_i) = b_i\,, \qquad \forall\, i = 1, \ldots, n\,,$$

kako se i tražilo. Pokažimo linearnost od f. Imamo

$$\begin{aligned} f(\alpha a + \beta b) &= f(\alpha \sum \alpha_i a_i + \beta \sum \beta_i a_i) = \\ &= f(\sum (\alpha\alpha_i + \beta\beta_i) a_i) = \sum (\alpha\alpha_i + \beta\beta_i) b_i = \\ &= \alpha \sum \alpha_i b_i + \beta \sum \beta_i b_i = \\ &= \alpha f(\sum \alpha_i a_i) + \beta f(\sum \beta_i a_i) = \\ &= \alpha f(a) + \beta f(b) , \end{aligned}$$

tj. f je zaista linearni operator. ■

Time smo dokazali egzistenciju netrivijalnih linearnih operatora. Naravno, ako dani skup (a_i) nije baza, takvih će linearnih operatora biti više, ovisno o izboru proširenja do baze. Međutim, ako je (a_i) baza, linearni operator iz Tm. 1 je jedinstven. Točnije, imamo

KOROLAR 2

Ako je $(a_1, \ldots, a_n) \subset U$ baza za U, a $(b_1, \ldots, b_n) \subset V$ bilo koji uređeni skup vektora, onda postoji jedan jedini linearni operator $f : U \to V$ sa svojstvom $f(a_i) = b_i$, za svaki $i = 1, \ldots, n$.

Dokaz

Egzistencija od f je dokazana u Tm. 1. Dokažimo jedinstvenost. Kad bi postojao još jedan linearni operator $g : U \to V$ sa svojstvom $g(a_i) = b_i$, za svaki $i = 1, \ldots, n$, za bilo koji $a \in U$ imali bismo

$$\begin{aligned} g(a) &= g(\sum \alpha_i a_i) = \sum \alpha_i g(a_i) = \\ &= \sum \alpha_i b_i = \sum \alpha_i f(a_i) = f(\sum \alpha_i a_i) = f(a) , \end{aligned}$$

pa bi zaista bilo $g = f$. ■

Tvrdnja iz Tm. 1 i Kor. 2 je istinita i u slučaju kad dani prostori nisu konačnodimenzionalni.

Iz Kor. 2 razabiremo kako se standardno zadaje linearni operator. Imamo

KOROLAR 3

Neka je $B = (a_1, \ldots, a_n)$ baza prostora U, a $f : B \to V$ bilo koje preslikavanje. Onda postoji jedinstveni linearni operator $g : U \to V$ koji proširuje f, tj. za koji vrijedi

$$g/B = f.$$

Dokaz

Uzmi $f(a_i) = b_i$ i primijeni Kor. 2. ■

Prema tome, linearni je operator dovoljno zadati na bazi prostora. Dva su linearna operatora $U \to V$ jednaka ako i samo ako imaju isto djelovanje na bilo kojoj bazi prostora U.

ZADACI

1. Neka je $L < V$ potprostor, a $i : L \to V$ inkluzija. Nađi neka netrivijalna linearna proširenja od i na cijeli V.

2. U prostoru P definiramo

$$f(t^k) = \sum_{j=0}^{k} j \cdot t^j , \qquad \forall\, k = 1, 2, \ldots \ .$$

Kako izgleda linearni operator $g : P \to P$, koji proširuje f?

8.4. Izomorfizam linearnih prostora

U ovoj točki ćemo riješiti važan problem klasifikacije linearnih prostora.

Neka su U i V linearni prostori nad istim poljem F, a

$$f : U \to V$$

operator. Kažemo da je f **izomorfizam linearnih prostora** ako je f

(1) linearni operator, i

(2) bijekcija.

Izomorfizam prostora U na sebe samog zove se **automorfizam** od U, ili također **regularni operator**. Za operator koji nije regularan kažemo da je **singularan**.

Kako je izomorfizam $f : U \to V$ i bijekcija, to je dobro definiran inverzni operator $f^{-1} : V \to U$. Vrijedi

PROPOZICIJA 1

Jedinični operator je izomorfizam. Inverz izomorfizma linearnih prostora je opet izomorfizam. Kompozicija izomorfizama je izomorfizam.

Dokaz

Prva i treća tvrdnja su trivijalne. Dokažimo drugu tvrdnju. Neka je $f : U \to V$ izomorfizam linearnih prostora. Onda je f izomorfizam i na razini aditivnih grupa tih prostora, pa je i $f^{-1} : V \to U$ izomorfizam aditivnih grupa (Prop. 4 u 3.2.). Neka je $b \in V$ bilo koji vektor i neka je $f^{-1}(b) = a \in U$. Onda za $\beta \in F$ imamo

$$\begin{aligned} f^{-1}(\beta b) &= f^{-1}(\beta f(a)) = f^{-1}[f(\beta a)] = \\ &= (f^{-1} \circ f)(\beta a) = \beta a = \beta f^{-1}(b) , \end{aligned}$$

što pokazuje da je f^{-1} i homogen, dakle zaista linearni operator, pa onda i izomorfizam. ■

Kažemo da je prostor U **izomorfan** s prostorom V i pišemo $U \cong V$, ako postoji bar jedan izomorfizam $f : U \to V$. Imamo

TEOREM 2

Relacija $\cong$, tj. relacija "biti izomorfan" je relacija ekvivalencije na klasi svih linearnih prostora nad istim poljem.

Dokaz

Neposredno iz Prop. 1. ■

Prema tome, relacija izomorfnosti među linearnim prostorima provodi rastav u disjunktne klase; u pojedinoj su klasi oni i samo oni linearni prostori nad istim poljem F koji su izomorfni. Takvi su prostori iste apstraktne strukture, a mogu se razlikovati jedino u naravi svojih elemenata.

Ovu posljednju tvrdnju ilustrira sljedeća

PROPOZICIJA 3

Neka je $f : U \to V$ izomorfizam linearnih prostora. Neka je $S \subset U$ bilo koji skup vektora iz U, a $T \subset V$ skup njihovih slika po f, $T = f(S)$. Skup S je linearno nezavisan ako i samo ako je T linearno nezavisan. Skup S razapinje U ako i samo ako skup T razapinje V.

Dokaz

Neka je skup $S = \{a_1 , \ldots , a_s\}$ linearno nezavisan, i neka je $f(a_i) = b_i \in T$, za $i = 1, \ldots, s$. Promatrajmo

$$\sum_{i=1}^{s} \beta_i b_i = \Theta_V .$$

Imamo

$$\sum_{i=1}^{s} \beta_i f(a_i) = f(\sum_{i=1}^{s} \beta_i a_i) = \Theta_V .$$

No, uvijek je $f(\Theta_U) = \Theta_V$, a kako je f bijekcija, iz prethodnog zaključujemo da je

$$\sum_{i=1}^{s} \beta_i a_i = \Theta_U ,$$

pa je zbog linearne nezavisnosti od S nužno $\beta_i = 0$, $i = 1, \ldots, s$, što pokazuje da je i T linearno nezavisan skup. Obrat slijedi iz činjenice da je i f^{-1} izomorfizam. Neka je sada S skup izvodnica za U, a $b \in V$ bilo koji vektor. Onda imamo

$$f^{-1}(b) = \sum_{i=1}^{s} \alpha_i a_i ,$$

pa je

$$b = f[f^{-1}(b)] = f(\sum_{i=1}^{s} \alpha_i a_i) = \sum_{i=1}^{s} \alpha_i f(a_i) = \sum_{i=1}^{s} \alpha_i b_i ,$$

tj. T je zaista skup izvodnica za V. Slično se vidi i obrat. ■

KOROLAR 4

Neka je $f : U \to V$ izomorfizam linearnih prostora. Onda svaka baza od U prelazi po f u neku bazu prostora V i obratno, svaka baza prostora V je slika neke baze prostora U.

Dokaz

Neposredno iz Prop. 3. ■

Iz Kor. 4 imamo odmah i ovaj zaključak

KOROLAR 5

Ako su U i V izomorfni prostori, onda je

$$\dim U = \dim V .$$ ■

Interesantan je, međutim, ovaj obrat

PROPOZICIJA 6

Neka su U i V linearni prostori nad poljem F, koji su iste dimenzije. Onda su ti prostori izomorfni, tj. $U \cong V$.

Dokaz

Neka je $\dim U = \dim V = n$, i nadalje, neka su $A = (a_1, \ldots, a_n) \subset U$ i $B = (b_1, \ldots, b_n) \subset V$ baze za te prostore. Definiramo linearni operator

$$f : U \to V$$

stavljajući

$$f(a_i) = b_i\,, \quad \text{za} \quad i = 1, \ldots, n\,,$$

i proširujući linearno (vidi Kor. 3 u 8.3.). Treba vidjeti da je f bijekcija. No, f je očito surjekcija. Nadalje, neka su

$$x = \sum_{i=1}^{n} \alpha_i a_i \qquad \text{i} \qquad y = \sum_{i=1}^{n} \beta_i a_i$$

vektori iz U, sa svojstvom da je

$$f(x) = f(\sum_{i=1}^{n} \alpha_i a_i) = f(\sum_{i=1}^{n} \beta_i a_i) = f(y)\,.$$

Kako je f linearni operator, imamo

$$\sum_{i=1}^{n} \alpha_i\, f(a_i) = \sum_{i=1}^{n} \beta_i\, f(a_i)\,,$$

dakle

$$\sum_{i=1}^{n} (\alpha_i - \beta_i)\, b_i = \Theta_V\,.$$

No, vektori iz B su linearno nezavisni pa ova relacija povlači $\alpha_i - \beta_i = 0$, za svaki i, dakle $x = y$, čime je dokazano da je f i injekcija. Prema tome je f izomorfizam pa je $U \cong V$. ■

Tako imamo ovu važnu karakterizaciju izomorfnih prostora

TEOREM 7

Dva linearna prostora nad istim poljem F su izomorfna ako i samo ako imaju istu dimenziju.

Dokaz

Iz Kor. 5 i Prop. 6. ■

Prema tome, svi prostori iste dimenzije, i samo oni, jesu ravnopravni, tj. imaju istu apstraktnu strukturu. Među njima je jedan koji zbog jednostavnosti i konkretnosti svoje definicije ima istaknutu ulogu. Imamo

KOROLAR 8

Svaki je n-dimenzionalni linearni prostor V nad poljem F izomorfan s koordinatnim prostorom F^n. ■

Svi zaključci do kojih možemo doći izučavajući konkretni prostor F^n vrijede i za svaki drugi n-dimenzionalni linearni prostor nad F. Kažemo da F^n **reprezentira** ili da je **standardni model** za linearne prostore dimenzije n.

ZADACI

1. Neka je V konačnodimenzionalni linearni prostor, a $L < V$ njegov potprostor. Ako je $f : L \to V$ izomorfizam, onda je $L = V$; dokaži! Nađi primjere koji pokazuju da zaključak nije točan u beskonačnodimenzionalnom slučaju.

2. Neka je V n-dimenzionalan prostor nad F, a $(a_1, \ldots, a_n)$ njegova baza. Definiramo $f : V \to F^n$ stavljajući

$$f(a) = f(\sum_{i=1}^{n} \alpha_i a_i) = (\alpha_1, \ldots, \alpha_n) .$$

   Pokaži da je f izomorfizam. Time je direktno dokazan Kor. 8, a onda i Tm. 7 (zbog Tm. 2).

3. Neka su $L, M < V$ potprostori i $L \cap M = \{\Theta\}$. Onda je

   (a) $L \oplus M \cong L \times M$;

   (b) $L \oplus M/L \cong M$ (vidi Tm. 3 u 7.8.).

   Dokaži neposredno i primjenom Tm. 7.

4. Uvjeri se da je
   $V^3/V^1 \cong V^2$, $\mathbb{R}^n/\mathbb{R}^k \cong \mathbb{R}^{n-k}$, $P/[\{1, t^2, \ldots\}] \cong [\{t, t^3, \ldots\}]$.

5. Neka su $L, M, N < V$ linearni potprostori, takvi da je $L \oplus M = L \oplus N$. Dokaži da je $M \cong N$. Posebno, direktni komplement od L je određen jednoznačno, do na izomorfizam.

6. Neka je $U_1 \cong U_2$ i $V_1 \cong V_2$. Onda je $U_1 \times V_1 \cong U_2 \times V_2$. Dokaži!

7. Pokaži da je za svaki $L < V$

$$V \cong L \times V/L .$$

8. Neka je Aut V skup svih automorfizama (regularnih operatora) prostora V. Pokaži da je to grupa u odnosu na kompoziciju.

8.5. Rang i defekt

Pokažimo najprije da se linearni operator dobro ponaša prema potprostorima. Vrijedi

PROPOZICIJA 1

Neka je $f : U \to V$ linearni operator. Ako je $L < U$ potprostor od U, onda je slika $f(L) \subset V$ potprostor od V. Ako je $M < V$ potprostor od V, onda je praslika $f^{-1}(M) \subset U$ potprostor od U.

Dokaz

Pokažimo da je $f(L)$ potprostor od V. Neka su $a, b \in f(L)$ bilo koji vektori, a $\alpha, \beta \in F$ po volji odabrani skalari. Neka su $x, y \in L$ takvi da je $f(x) = a$, a $f(y) = b$. Primijetimo da je $L \subset U$ potprostor po pretpostavci, pa je $z = \alpha x + \beta y \in L$. Imamo onda

$$\alpha a + \beta b = \alpha f(x) + \beta f(y) = f(\alpha x + \beta y) = f(z) \in f(L)$$

i tvrdnja je dokazana. Slično se pokazuje i tvrdnja da je $f^{-1}(M)$ potprostor od U. ■

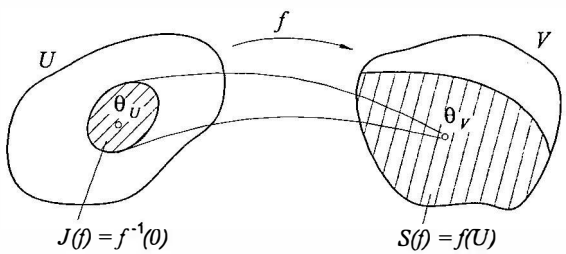
Uz svaki linearni operator $f : U \to V$ vežemo dva specijalna skupa. To su:

(1) **slika** od f, tj. skup

$$S = S(f) = f(U) = \{f(x) \mid x \in U\} \subset V ;$$

(2) **jezgra** od f, tj. skup

$$J = J(f) = f^{-1}(\Theta_V) = \{x \in U \mid f(x) = \Theta_V\} \subset U .$$



Kako je $U < U$ potprostor od U, a $\{\Theta_V\} < V$ potprostor od V, iz Prop. 1 odmah zaključujemo

KOROLAR 2

Slika $S(f) \subset V$ i jezgra $J(f) \subset U$ linearnog operatora f su potprostori od V, odnosno U. ■

Kao potprostori, slika i jezgra su linearni prostori, pa imaju svoju dimenziju. Definiramo:

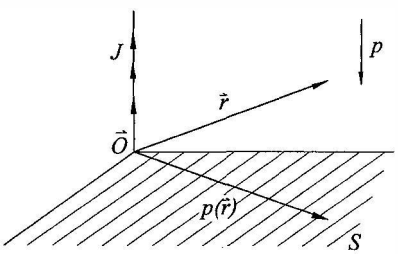
(1) **rang** linearnog operatora f, kao dimenziju njegove slike, tj.

$$r = r(f) = \dim S(f) ;$$

(2) **defekt** linearnog operatora f, kao dimenziju njegove jezgre, tj.

$$d = d(f) = \dim J(f) .$$

Neka su npr. $V^3(O)$ i $V^2(O)$ prostori radijvektora, a $p : V^3(O) \to V^2(O)$ neka je ortogonalna projekcija. Onda je p linearni operator, i njegov



je rang $r = 2$, a defekt $d = 1$. Pritom je $r + d = 2 + 1 = 3 = \dim V^3(O)$. Zaključak je općenit, i to je jedno važno svojstvo linearnih operatora.

TEOREM 3 (Teorem o rangu i defektu)

Neka je $f : U \to V$ linearni operator. Onda je suma ranga i defekta od f jednaka dimenziji prostora U, tj.

$$r(f) + d(f) = \dim U \ .$$

Dokaz

Neka je $S < V$ slika od f, $\dim S = r$, i nadalje, neka je $J < U$ jezgra od f, $\dim J = d$. Teorem tvrdi da je

$$r + d = \dim U \ .$$

Neka je $B = (b_1, \ldots, b_r)$ jedna baza prostora S. Neka su, nadalje, vektori $a_1, \ldots, a_r \in U$ odabrani tako da je

$$f(a_i) = b_i \ , \qquad \forall\, i = 1, \ldots, r \ .$$

(Dakako, taj izbor nije općenito jednoznačan.) Tvrdimo da je tada skup $A = (a_1, \ldots, a_r) \subset U$ linearno nezavisan. Zaista, iz

$$\sum_{i=1}^{r} \alpha_i a_i = \Theta_U$$

slijedi

$$f(\sum_{i=1}^{r} \alpha_i a_i) = f(\Theta_U) = \Theta_V \, .$$

Kako je f linearno preslikavanje, imamo

$$\sum_{i=1}^{r} \alpha_i f(a_i) = \Theta_V \, ,$$

odnosno

$$\sum_{i=1}^{r} \alpha_i b_i = \Theta_V \, ,$$

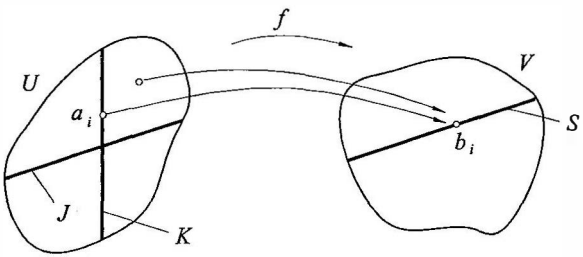
i odatle

$$\alpha_1 = \cdots = \alpha_r = 0 \, ,$$

jer je skup B bio baza, dakle linearno nezavisan po pretpostavci. Neka je

$$K = [A] \subset U$$

potprostor u U razapet skupom vektora A. Kako je taj skup linearno neza-



visan, on je i baza za K. Prema tome je

$$\dim K = r \, .$$

Tvrdimo da je

$$U = K \oplus J \, . \tag{1}$$

Ako to uspijemo dokazati, onda smo gotovi jer prema Prop. 6 u 7.7. imamo

$$\dim U = \dim K + \dim J = r + d \,,$$

što teorem i tvrdi. No, po definiciji direktne sume (1) znači da je

$$K + J = U \,, \tag{2}$$

$$K \cap J = \{\Theta_U\} \,. \tag{3}$$

Pokažimo najprije (3). Neka je $a \in K \cap J$ bilo koji vektor. Jer je $a \in K$, možemo ga prikazati kao

$$a = \sum_{i=1}^{r} \alpha_i \, a_i \,,$$

budući da vektori iz A razapinju K. No, jer je $a \in J$, to je $f(a) = \Theta_V$, pa imamo

$$f(\sum_{i=1}^{r} \alpha_i \, a_i) = \Theta_V \,,$$

dakle

$$\sum_{i=1}^{r} \alpha_i \, b_i = \Theta_V \,.$$

Kako je skup B linearno nezavisan, odatle slijedi da je $\alpha_1 = \cdots = \alpha_r = 0$, i prema tome je nužno

$$a = \Theta_U \,,$$

pa je zaista $K \cap J = \{\Theta_U\}$.

Ostaje provjeriti (2). Neka je $x \in U$ bilo koji vektor. Onda je $f(x) \in f(U) = S$, pa ima prikaz

$$f(x) = \sum_{i=1}^{r} \beta_i \, b_i \,. \tag{4}$$

Neka je $a \in K$ vektor definiran s

$$a = \sum_{i=1}^{r} \beta_i \, a_i \tag{5}$$

(uoči da su u (5) isti koeficijenti kao u (4)). Onda je

$$f(a) = \sum_{i=1}^{r} \beta_i \, f(a_i) = \sum_{i=1}^{r} \beta_i \, b_i = f(x) \,. \tag{6}$$

Konačno, neka je $b \in V$ vektor definiran s

$$b = x - a\,. \tag{7}$$

Tvrdimo da je $b \in J$. Zaista, zbog (6) je

$$f(b) = f(x-a) = f(x) - f(a) = f(a) - f(a) = \Theta_V\,,$$

pa je b iz jezgre. No, iz (7) onda čitamo da je

$$x = a + b\,, \quad a \in K\,,\ b \in J\,,$$

čime je dokazano (vidi Prop. 3 u točki 7.7.) da je $U = K + J$ i teorem je dokazan. ■

Teorem zapravo pokazuje da je za sve operatore koji djeluju na istom prostoru U suma ranga i defekta konstantna (i jednaka $\dim U$).

ZADACI

1. Dokaži: Linearni operator $f : U \to V$ je izomorfizam linearnih prostora ako i samo ako je surjekcija i vrijedi $J(f) = \{\Theta_U\}$.

2. Neka je $L < V$ potprostor. Ako je $p : V \to L$ projektor na potprostor, onda je rang od p jednak dimenziji, a defekt od p kodimenziji od L. Ako je pak $q : V \to V/L$ kvocijentni operator, onda je rang od q jednak kodimenziji, a defekt od q dimenziji od L. Dokaži!

3. Neka je $f : U \to V$ linearni operator, a $L < U$ potprostor. Onda vrijedi
$$\dim L - \dim J(f) \leq \dim f(L) \leq \dim L\,.$$
Dokaži!

4. Neka je $f : U \to V$ surjektivni linearni operator, a J njegova jezgra. Onda postoji jedinstveni izomorfizam $h : U/J \to V$ sa svojstvom da dijagram
$$\begin{array}{ccc} U & \xrightarrow{\ f\ } & V \\ & {\scriptstyle q}\searrow \quad \nearrow{\scriptstyle h} & \\ & U/J & \end{array}$$
komutira, tj. da je $h \circ q = f$, gdje je q prirodna projekcija (Zad. 2.). Dokaži!

5. Konačni ili beskonačni niz

$$\ldots \xrightarrow{f_{i-2}} V_{i-1} \xrightarrow{f_{i-1}} V_i \xrightarrow{f_i} V_{i+1} \xrightarrow{f_{i+1}} \ldots$$

linearnih prostora i pripadnih linearnih operatora nazivamo **egzaktni niz** ako je za **svaki** i

$$S(f_{i-1}) = J(f_i) .$$

Egzaktni niz oblika

$$\{\Theta\} \longrightarrow U \xrightarrow{f} V \xrightarrow{g} W \longrightarrow \{\Theta\}$$

zovemo **kratki egzaktni niz**. Pokaži da je u takvom nizu uvijek $U \cong M$ i $V/M \cong W$, gdje je $M = S(f) = J(g) < V$.

6. Neka je $L < V$ potprostor. Pokaži da je

$$\{\Theta\} \longrightarrow L \xrightarrow{i} V \xrightarrow{q} V/L \longrightarrow \{\Theta\} ,$$

gdje je i inkluzija, a q prirodna projekcija, kratki egzaktni niz. Pokaži, nadalje, da je

$$V \cong L \times V/L .$$

7. Ako je $\dim U = m$, $\dim V = n$ i $f : U \to V$ je linearni operator, onda je rang $r(f) \leq \min\{m, n\}$. Dokaži!

8. Linearni operator $f : U \to V$ je injektivan ako i samo ako je $d(f) = 0$, a surjektivan ako i samo ako je $r(f) = \dim V$, dokaži!

9. Neka je $\dim U = \dim V = n$ i $f : U \to V$ linearni operator. Dokaži da je f izomorfizam ako i samo ako je injektivan (surjektivan).

10. Neka su $f : U \to V$ i $g : V \to W$ linearni operatori. Dokaži da vrijedi

$$r(f) = r(g \circ f) + \dim [S(f) \cap J(g)] .$$

Odatle, zbog Tm. 4 u 7.7., slijedi

$$r(g \circ f) = \dim [S(f) + J(g)] - d(g) .$$

Ako je specijalno $J(g) \subset S(f)$, onda imamo

$$r(f) = r(g \circ f) + d(g).$$

11. Za kompoziciju linearnih operatora uvijek vrijedi

$$r(g \circ f) \leq \min\{r(f), r(g)\} .$$

Dokaži!

12. Ako je f surjektivni operator, onda je $r(g \circ f) = r(g)$; ako je g injektivni operator, onda je $r(g \circ f) = r(f)$. Dokaži! Specijalno, rang operatora se ne mijenja ako ga s bilo koje strane komponiramo s izomorfizmom.

13. Operator f je surjektivan ako i samo ako $g \circ f = n$ povlači $g = n$. Operator g je injektivan ako i samo ako $g \circ f = n$ povlači $f = n$ (ovdje je s n označen nuloperator). Dokaži!

14. Operator f je surjektivan ako i samo ako $g_1 \circ f = g_2 \circ f$ povlači $g_1 = g_2$ (skraćivanje zdesna). Operator g je injektivan ako i samo ako $g \circ f_1 = g \circ f_2$ povlači $f_1 = f_2$ (skraćivanje slijeva). Dokaži!

15. Dokaži da vrijedi

$$\begin{aligned} \max\{\dim U - \dim V + d(g),\, d(f)\} \leq \quad & d(g \circ f) \leq \\ \leq \min\{\dim U,\, d(f) + d(g)\} \quad & . \end{aligned}$$

Za $\dim U = \dim V$ ta se nejednakost reducira na tzv. **Sylvesterov zakon defekta**.

8.6. Prostor $\mathrm{Hom}(U, V)$

Neka su U i V linearni prostori nad istim poljem F, a s

$$\mathrm{Hom}(U, V) = \{f : U \to V \mid f \text{ je linearan}\}$$

neka je označen skup **svih** linearnih operatora koji djeluju na prostoru U i primaju vrijednosti u prostoru V. Katkad se taj skup označuje i kao $\{U \to V\}$ ili kao $\mathrm{Lin}(U, V)$.

Skup $\mathrm{Hom}(U, V)$ može se na prirodan način snabdjeti strukturom linearnog prostora. Za bilo koja dva linearna operatora $f, g : U \to V$ definiramo njihov **zbroj** kao operator

$$f + g : U \to V$$

dan s

$$(f + g)(x) = f(x) + g(x) .$$

PROPOZICIJA 1

Operator $f + g : U \to V$ je linearan.

Dokaz

Imamo redom

$$\begin{aligned}(f+g)(\alpha x+\beta y) &= f(\alpha x+\beta y)+g(\alpha x+\beta y)= \\ &= \alpha f(x)+\beta f(y)+\alpha g(x)+\beta g(y)= \\ &= \alpha(f(x)+g(x))+\beta(f(y)+g(y))= \\ &= \alpha\,(f+g)(x)+\beta\,(f+g)(y).\end{aligned}$$

■

Prema tome je zbrajanje operatora dobro definirana binarna operacija na Hom(U, V). I više

PROPOZICIJA 2

Skup Hom(U, V) *je u odnosu na zbrajanje linearnih operatora Abelova grupa.*

Dokaz

To se lako provjeri. Neutralni element je nuloperator $n : U \to V$, $n(x) = \Theta_V$, a za operator f je suprotan operator $g : U \to V$, definiran kao $g(x) = -f(x)$, za svaki $x \in U$. Uvjeri se da je g zaista linearan. ■

Nadalje, za bilo koji linearni operator $f : U \to V$ i bilo koji skalar $\lambda \in F$ definiramo **produkt** tog skalara i operatora kao operator

$$\lambda f : U \to V$$

definiran s

$$(\lambda f)(x) = \lambda f(x)\,.$$

PROPOZICIJA 3

Operator $\lambda f : U \to V$ je linearan.

Dokaz

Imamo

$$\begin{aligned}(\lambda f)(\alpha x+\beta y) &= \lambda f(\alpha x+\beta y)=\lambda[\alpha f(x)+\beta f(y)]= \\ &= \lambda[\alpha f(x)]+\lambda[\beta f(y)]=(\lambda\alpha)\,f(x)+(\lambda\beta)\,f(y)= \\ &= (\alpha\lambda)\,f(x)+(\beta\lambda)\,f(y)=\alpha[\lambda\,f(x)]+\beta[\lambda\,f(y)]= \\ &= \alpha(\lambda f)(x)+\beta(\lambda f)(y)\,.\end{aligned}$$

■

Konačno imamo

TEOREM 4

$\mathrm{Hom}(U,V)$ *je, uz definirane operacije zbrajanja linearnih operatora i množenja skalarom, linearni prostor nad poljem* F.

Dokaz

Već smo vidjeli (Prop. 2) da je $\mathrm{Hom}(U,V)$ aditivna grupa. Treba još provjeriti aksiome (1)-(4) iz definicije linearnog prostora. Provjerimo npr. (4). Imamo

$$\begin{aligned}[\lambda(f+g)](x) &= \lambda[(f+g)(x)] = \lambda[f(x)+g(x)] = \\ &= \lambda f(x) + \lambda g(x) = (\lambda f)(x) + (\lambda g)(x) = \\ &= (\lambda f + \lambda g)(x)\ ,\end{aligned}$$

i to za svaki $x \in U$, pa je

$$\lambda(f+g) = \lambda f + \lambda g\ .$$

Slično se provjere i ostali aksiomi. ■

Postavlja se pitanje koliko ima operatora koji djeluju na danom prostoru U i s vrijednostima u V. Točnije, pitanje je kolika je dimenzija prostora $\mathrm{Hom}(U,V)$. Imamo

TEOREM 5

Neka su U *i* V *konačnodimenzionalni prostori nad istim poljem. Onda je*

$$\dim \mathrm{Hom}(U,V) = \dim U \cdot \dim V\ .$$

Dokaz

Neka je $\dim U = m$, a $\dim V = n$. Neka je $A = (a_1, \ldots, a_m)$ baza za U, a $B = (b_1, \ldots, b_n)$ baza za V. Za svaki $i = 1, \ldots, n$, $j = 1, \ldots, m$, neka je s

$$f_{ij} : U \to V$$

označen linearni operator, definiran na bazi s

$$f_{ij}(a_k) = \begin{cases} b_i & , \quad k = j \\ \Theta_V & , \quad k \neq j \end{cases}$$

i proširen linearno na čitav U. Takav operator uvijek postoji i jednoznačno je određen prema Kor. 3 iz 8.3. Ponovimo, radi se o linearnom operatoru

$$f_{ij} : \begin{array}{ccccccc} a_1 & , \ldots , & a_j & , \ldots , & a_m \\ \downarrow & & \downarrow & & \downarrow \\ \Theta_V & , \ldots , & b_i & , \ldots , & \Theta_V \end{array}\ .$$

Na taj način dolazimo do familije

$$F = \{f_{ij} \mid i = 1, \ldots, n,\ j = 1, \ldots, m\} \tag{1}$$

od $m \cdot n$ linearnih operatora, dakle elemenata iz $\mathrm{Hom}(U, V)$. Tvrdimo da oni čine bazu za $\mathrm{Hom}\,(U, V)$. Ako to pokažemo, teorem je dokazan, jer ćemo imati

$$\dim \mathrm{Hom}(U, V) = mn = \dim U \cdot \dim V\,.$$

Pokažimo najprije da je (1) skup izvodnica za $\mathrm{Hom}(U, V)$. Zaista, neka je $f \in \mathrm{Hom}(U, V)$ bilo koji linearni operator. Neka je, nadalje, $a \in U$ po volji odabran vektor. Kako je A baza za U, možemo pisati

$$a = \sum_{j=1}^{m} \alpha_j\, a_j\,. \tag{2}$$

Nadalje, jer je f linearan, imamo

$$f(a) = f(\sum_{j=1}^{m} \alpha_j a_j) = \sum_{j=1}^{m} \alpha_j\, f(a_j)\,. \tag{3}$$

No, $f(a_j)$ je vektor u V, a B je njegova baza, pa za svaki $j = 1, \ldots, m$ imamo

$$f(a_j) = \sum_{i=1}^{n} \beta_{ij}\, b_i\,. \tag{4}$$

Konačno, u igru uvodimo operatore f_{ik}. Po definiciji je

$$b_i = f_{ij}(a_j)$$

i, nadalje, $f_{ik}(a_j) = \Theta_V$, za $k \neq j$, pa možemo pisati

$$\beta_{ij} b_i = \beta_{ij}\, f_{ij}(a_j) = \sum_{k=1}^{m} \beta_{ik}\, f_{ik}(a_j)\,. \tag{5}$$

Na osnovi (3), (4), (5) i na kraju (2), onda imamo

$$\begin{aligned} f(a) &= \sum_{j=1}^{m} \alpha_j f(a_j) = \sum_{j=1}^{m} \alpha_j \sum_{i=1}^{n} \beta_{ij} b_i = \\ &= \sum_{j=1}^{m} \alpha_j \sum_{i=1}^{n} \sum_{k=1}^{m} \beta_{ik} f_{ik}(a_j) = \\ &= \sum_{i=1}^{n} \sum_{k=1}^{m} \beta_{ik} \sum_{j=1}^{m} \alpha_j f_{ik}(a_j) = \\ &= \sum_{i=1}^{n} \sum_{k=1}^{m} \beta_{ik} f_{ik}(\sum_{j=1}^{m} \alpha_j a_j) = \\ &= \sum_{i=1}^{n} \sum_{k=1}^{m} \beta_{ik} f_{ik}(a) = \\ &= (\sum_{i=1}^{n} \sum_{k=1}^{m} \beta_{ik} f_{ik})(a) \, . \end{aligned}$$

Kako je to istina za svaki $a \in U$, imamo zaključak

$$f = \sum_{i=1}^{n} \sum_{k=1}^{m} \beta_{ik} f_{ik} \, ,$$

tj. f je zaista linearna kombinacija vektora iz (1). Ostaje pokazati da je skup operatora (1) linearno nezavisan. U tu svrhu promatramo

$$\sum_{i=1}^{n} \sum_{k=1}^{m} \alpha_{ik} f_{ik} = n \, , \tag{6}$$

gdje je s n označen nuloperator iz U u V. Treba vidjeti da je ta relacija moguća jedino na trivijalan način, tj. kad su svi $\alpha_{ik} = 0$. Primijenimo li (6) na vektor a_j iz baze A u U, imamo

$$(\sum_{i=1}^{n} \sum_{k=1}^{m} \alpha_{ik} f_{ik})(a_j) = n(a_j) = \Theta_V \, ,$$

odnosno

$$\sum_{i=1}^{n} \sum_{k=1}^{m} \alpha_{ik} f_{ik}(a_j) = \Theta_V \, .$$

No, iz definicije operatora f_{ik} slijedi

$$\sum_{i=1}^{n} \alpha_{ij} f_{ij}(a_j) = \Theta_V \, ,$$

dakle

$$\sum_{i=1}^{n} \alpha_{ij}\, b_i = \Theta_V \ .$$

Kako je B baza za V, odatle zaključujemo da je

$$\alpha_{ij} = 0 \ ,$$

za svaki $i = 1, \ldots, n$ i prije izabrani j. To je zaključivanje, međutim, ispravno za svaki vektor a_j, $j = 1, \ldots, m$, iz baze od U, pa je nužno

$$\alpha_{ij} = 0$$

za svaki i i za svaki j, što pokazuje da je skup operatora F zaista linearno nezavisan i teorem je dokazan. ■

Prema Tm. 5 je npr. $\dim \mathrm{Hom}(V^3, V^2) = \dim \mathrm{Hom}(V^2, V^3) = 3 \cdot 2 = 6$, a $\dim \mathrm{Hom}(V^3, V^3) = 3^2 = 9$, kako smo prije i najavili (Zad. 2. u 5.14.). Primijetimo da teorem nije točan u beskonačnodimenzionalnom slučaju.

Kažimo na kraju nešto više o slučaju kad je $U = V$, dakle o prostoru $\mathrm{Hom}(V,V)$ svih linearnih operatora koji preslikavaju V **u sama sebe**. Taj prostor obično označavamo kraće kao $\mathrm{Hom}\, V$. Na temelju Tm. 5 odmah zaključujemo da je

$$\dim \mathrm{Hom}\, V = (\dim V)^2 \ .$$

Primijetimo da se operatori iz $\mathrm{Hom}\, V$ mogu komponirati, pa za bilo koja dva linearna operatora $f, g : V \to V$ definiramo njihov **produkt** kao operator

$$fg : V \to V$$

koji dobivamo komponiranjem, tj.

$$fg(x) = (f \circ g)(x) = f[g(x)] \ , \qquad \forall\, x \in V \ .$$

Kako je kompozicija linearnih operatora opet linearni operator, množenje operatora je dobro definirana binarna operacija u $\mathrm{Hom}\, V$.

PROPOZICIJA 6

Množenje linearnih operatora u prostoru $\mathrm{Hom}\, V$ *ima svojstva*

(1) *kvaziasocijativnosti, tj.*

$$(\lambda f)g = \lambda(fg) = f(\lambda g) \ ,$$

za svaki $\lambda \in F$ *i* $f, g \in \mathrm{Hom}\, V$,

(2) *distributivnosti prema zbrajanju, tj.*

$$\begin{aligned}(f+g)h &= fh+gh \quad i\\ f(g+h) &= fg+fh\ ,\end{aligned}$$

za svaki izbor $f, g, h \in \operatorname{Hom} V$.

Dokaz

Kvaziasocijativnost se lako provjeri. Pokažimo prvu relaciju distributivnosti. Imamo, za $x \in V$,

$$\begin{aligned}[(f+g)h](x) &= (f+g)[h(x)] = f[h(x)]+g[h(x)] =\\ &= (fh)(x)+(gh)(x) = (fh+gh)(x)\ ,\end{aligned}$$

dakle

$$(f+g)h = fh+gh\ .$$

■

Kako smo već spomenuli u petom poglavlju, točka 5.11., linearni prostor nad poljem F u kojem je definirana dodatna binarna operacija (tzv. množenje vektora), sa svojstvima (1) i (2) iz Prop. 6, nazivamo **algebra nad poljem** F. Prema tome je $\operatorname{Hom} V$ jedna algebra. Množenje operatora ima još neka svojstva: asocijativno je (jer je kompozicija preslikavanja uvijek asocijativna) i posjeduje neutralni element, jedinicu. To je, dakako, jedinični operator $e : V \to V$. Primijetimo još da to množenje nije komutativno (jer kompozicija nije takva).

Zaključno, dakle, imamo

TEOREM 7

Neka je V *linearni prostor nad poljem* F. *Onda je prostor* $\operatorname{Hom} V$, *uz komponiranje operatora kao množenje, jedna algebra nad poljem* F, *asocijativna, s jedinicom, ali nekomutativna (kad* V *nije trivijalan).* ■

Kako su elementi u algebri $\operatorname{Hom} V$ linearni operatori, za nju se nekad upotrebljavao i naziv **linearna algebra**. Međutim, taj termin ima danas mnogo šire značenje.

Neka je $f \in \operatorname{Hom} V$ bilo koji linearni operator. Onda je $f^2 = ff$ također linearni operator, i onda je to, induktivno, i $f^m = f^{m-1}f$, za svaki $m \in \mathbb{N}$. Još se, po definiciji, uzima da je $f^0 = e$. Tako u algebri $\operatorname{Hom} V$ možemo promatrati polinome u danom operatoru f, dakle polinome oblika

$$p(f) = \alpha_m f^m + \cdots + \alpha_1 f + \alpha_0 e\ , \qquad \alpha_i \in F\ ,$$

i svaki takav polinom je opet linearni operator, element od $\mathrm{Hom}\,V$. Za te polinome vrijede standardna pravila računanja. Isto tako, lako se vidi da vrijede neki uobičajeni identiteti, npr.

$$f^2 - e = (f+e)(f-e)\,.$$

Je li istina $f^2 - g^2 = (f+g)(f-g)$ za bilo koje $f, g \in \mathrm{Hom}\,V$? Uopće, koje poteškoće nastupaju ako se promatraju operatorski polinomi u dvije ili više varijabli?

ZADACI

1. Neka je $L < V$ potprostor od V. Neka je, nadalje,

$$T = \{f \in \mathrm{Hom}\,V \mid f(a) = \Theta,\ \forall a \in L\}$$

skup svih onih linearnih operatora f na V, za koje je restrikcija f/L nuloperator. Pokaži da je T potprostor od $\mathrm{Hom}\,V$ i nađi njegovu dimenziju.

2. Neka su $f, g \in \mathrm{Hom}\,V$ bilo koja dva operatora. Dokaži da je

   (a) $r(f+g) \leq r(f) + r(g)$;
   (b) $d(fg) \leq d(f) + d(g)$;
   (c) $r(fg) \leq \min\{r(f), r(g)\}$;
   (d) $r(fg) \geq r(f) + r(g) - \dim V$,

   gdje je s r označen rang, a s d defekt linearnog operatora.

3. Neka su $f, g \in \mathrm{Hom}\,P$ operatori, definirani s $f(p) = \dfrac{\mathrm{d}p}{\mathrm{d}t}$, $g(p) = t \cdot p$, za svaki polinom $p \in P$. Pokaži:

   (a) $fg - gf = e$,
   (b) $f^m g - g f^m = m f^{m-1}, \quad \forall m \in \mathbb{N}$.

4. Neka su $f, g \in \mathrm{Hom}\,P_n$, gdje je f opet operator deriviranja, a g definiran s $[g(p)](t) = p(t+1)$. Dokaži da je

$$g = e + \frac{f}{1!} + \frac{f^2}{2!} + \cdots + \frac{f^{n-1}}{(n-1)!}\,.$$

5. Pokaži (generalizaciju Zad. 3.): ako su $f, g \in \mathrm{Hom}\,V$ takvi da $fg - gf$ komutira s f, onda je

$$f^m g - g f^m = m f^{m-1}(fg - gf)$$

za svaki $m \in \mathbb{N}$.

6. Zaključi pomoću Zad. 5. (ili dokaži direktno): Ako operatori f i g komutiraju, onda komutiraju i operatori f^m i g^m, za svaki $m \in \mathbb{N}$. Je li istinit i obrat?

7. Dokaži: Ako je $f \in \operatorname{Hom} V$, $\dim V = n$, onda postoji netrivijalni polinom p, stupnja koji ne premašuje n^2, sa svojstvom da je $p(f) = n$, gdje je n nuloperator.

8. Neka je $f \in \operatorname{Hom} V$ dani operator, a

$$K = \{g \in \operatorname{Hom} V \mid fg = n\} .$$

Pokaži da je K potprostor od $\operatorname{Hom} V$. Može li se svaki potprostor od $\operatorname{Hom} V$ dobiti na taj način (pogodnim izborom operatora f)?

9. Neka je $f \in \operatorname{Hom} V$ dani operator. Definiramo

$$\Phi : \operatorname{Hom} V \to \operatorname{Hom} V$$

s

$$\Phi(g) = fg , \qquad \forall g \in \operatorname{Hom} V .$$

Pokaži da je Φ linearni operator (tj. $\Phi \in \operatorname{Hom}(\operatorname{Hom} V)$). Može li se svaki linearni operator na $\operatorname{Hom} V$ dobiti na taj način (pogodnim izborom operatora f)?

10. Algebra nad poljem realnih brojeva naziva se **realna algebra**. Neka je S bilo koji skup, a $A = \mathbb{R}^S$ skup svih realnih funkcija na S. Uz standardno zbrajanje i množenje skalarom, te uz množenje

$$(fg)(x) = f(x)g(x) , \quad \forall x \in S ,$$

A je realna algebra, asocijativna, komutativna i s jedinicom. Dokaži! Posebno, uzimajući $S = \{1, \ldots, m\}$, vidimo da je prostor $\mathbb{R}^m$ jedna realna algebra.

11. Pojam **podalgebre** definira se na prirodan način. Pokaži da je u nizu $\mathbb{R}^1 \subset \mathbb{R}^2 \subset \cdots$ svaka prethodna algebra podalgebra svake sljedeće. Nađi neke podalgebre u algebrama V^3 i $\operatorname{Hom} V$.

12. Svaka je asocijativna algebra prsten u odnosu na zbrajanje i množenje vektora. Imajući to na umu, definiraj pojam ideala za takvu algebru, kao i pojam kvocijenta algebre po danom idealu.

13. Kažemo da je A **algebra s dijeljenjem** ako je A u odnosu na zbrajanje i množenje vektora tijelo. Pokaži da su realni brojevi $\mathbb{R}$, kompleksni brojevi $\mathbb{C}$ i kvaternioni $\mathbb{H}$ realne algebre s dijeljenjem (ova posljednja, dakako, nekomutativna). Zanimljiv je Frobeniusov teorem koji kaže da su to jedine tri realne algebre s dijeljenjem.

14. Analogno kao u prstenu, i u algebri definiramo pojam **djelitelja nule**. Neka je f operator deriviranja u $\operatorname{Hom} P_n$. Uvjeri se da su operatori f^{n-k} i f^k djelitelji nule u algebri $\operatorname{Hom} P_n$.

15. Neasocijativna algebra u kojoj je množenje antikomutativno i za koje vrijedi Jacobijev identitet (tj. kod koje je pripadni prsten Liejev prsten), naziva se **Liejeva algebra** (vidi peto poglavlje, točka 5.11.). Kako smo već rekli, $V^3(+,\cdot,\times)$ je primjer takve algebre. Pokaži da svaka asocijativna algebra postaje uvođenjem novoga, **komutatorskog množenja**, $(a,b)\mapsto[a,b]=ab-ba$, Liejeva algebra.

16. Operator $f\in\operatorname{Hom} V$ zove se **idempotentan**, ako je $f^2=f$. Pokaži da je operator f idempotentan ako i samo ako je $(2f-e)^2=e$. Slično vrijedi u bilo kojoj algebri s jedinicom.

17. Neka je A asocijativna algebra s jedinicom e, a $a_1,\ldots,a_m$ njezini elementi sa svojstvom da je $a_i^2=a_i$, za svaki $i=1,\ldots,m$, i da vrijedi $\sum_{i=1}^m a_i=e$. Onda je $\sum_{\substack{i,j=1\\ i\neq j}}^m a_ia_j=\Theta$; dokaži.

18. Neka su A i B algebre nad istim poljem F, a $f:A\to B$ preslikavanje. Kažemo da je f **Homomorfizam algebri**, ako je f linearni operator i vrijedi
$$f(xy)=f(x)\,f(y)\,,$$
za svaki $x,y\in A$. Ako je f i bijekcija, onda, dakako, govorimo o **izomorfizmu algebri**. Navedi primjere izomorfnih algebri. Jesu li npr. algebre $V^3(+,\cdot,\times)$ i $\mathbb{R}^3$ izomorfne?

19. Neka je $f\in\operatorname{Hom} V$ dani operator, $P_n(f)$ skup polinoma u f čiji je stupanj manji od n, a $P(f)$ skup svih polinoma u f. Onda je skup $P_n(f)\subset\operatorname{Hom} V$ potprostor algebre $\operatorname{Hom} V$. Je li podalgebra? A potprostor $P(f)$?

8.7. Linearni funkcionali. Dualni prostor

Neka je V bilo koji linearni prostor nad poljem F. Kako smo prije primijetili, to se polje može također shvatiti i kao linearni prostor (nad samim sobom),

i onda je $\dim F = 1$. Zato ima smisla promatrati linearne operatore

$$l : V \to F ,$$

koji djeluju na prostoru V i primaju vrijednosti u pripadnom polju F. Takve specijalne linearne operatore zovemo **linearni funkcionali**. Općenito, običaj je da se sva preslikavanja linearnog prostora u pripadno polje nazivaju **funkcionali**.

Naravno, linearni funkcionali imaju sva svojstva, tj. za njih vrijede svi rezultati koji su u ovom poglavlju dokazani za linearne operatore. Tako npr. za rang r i defekt d linearnog funkcionala l vrijedi

$$r + d = \dim V.$$

Kako je, nadalje, očigledno

$$r \leq 1 ,$$

imamo zaključak da je kod linearnih funkcionala uvijek

$$d \geq \dim V - 1 .$$

PRIMJERI

1. Neka je F^n koordinatni prostor nad poljem F, a

$$p_i : F^n \to F ,$$

$$p_i(\alpha_1, \ldots, \alpha_i, \ldots, \alpha_n) = \alpha_i ,$$

i-ta koordinatna funkcija za svaki $i = 1, \ldots, n$ (vidi Zad. 5. u 8.2.). Onda je p_i linearni funkcional.

2. Općenitije, neka je $\lambda_1, \ldots, \lambda_n \in F$ bilo koji fiksni izbor skalara. Definiramo

$$l : F^n \to F$$

s

$$l(\alpha_1, \ldots, \alpha_n) = \sum_{i=1}^{n} \lambda_i \alpha_i .$$

Onda je l linearni funkcional. Pokaži da se na taj način mogu dobiti *svi linearni funkcionali na* F^n.

3. Neka je P prostor polinoma, a $v : P \to \mathbb{R}$ definirano s

$$v(p) = p(0) .$$

Onda je v linearni funkcional, tzv. **valuacija**.

4. Općenitije, ako su $t_1, \ldots, t_k \in \mathbb{R}$ i $\alpha_1, \ldots, \alpha_k \in \mathbb{R}$ bilo koji izbori realnih brojeva, onda je s

$$w(p) = \sum_{i=1}^{k} \alpha_i \, p(t_i)$$

definiran linearni funkcional $w : P \to \mathbb{R}$.

5. Neka je $V < \mathbb{R}^{\mathbb{R}}$ prostor svih realnih funkcija integrabilnih na intervalu $[a, b]$, a $I : V \to \mathbb{R}$ neka je definiran s

$$I(f) = \int_a^b f(t) \, \mathrm{d}t \, .$$

Onda je I linearni funkcional.

Neka je sada

$$V^* = \mathrm{Hom}(V, F)$$

skup svih linearnih funkcionala koji djeluju na prostoru V. Kako smo vidjeli (Tm. 4 u 8.6.), to je opet linearni prostor, koji nazivamo **dualni prostor** ili, kraće, **dual** prostora V. Nadalje, kako je $\dim F = 1$, prema Tm. 5 iz 8.6., imamo

$$\dim V^* = \dim V \cdot \dim F = \dim V \, ,$$

tj. u konačnodimenzionalnom slučaju prostor i njegov dual imaju istu dimenziju. Primijetimo da to nije istina kad je V beskonačne dimenzije. Pokazuje se, naime, da je tada

$$\dim V^* = 2^{\dim V} \, .$$

Na primjer, za prostor P polinoma je $\dim P^* = 2^{\dim P} = 2^{\aleph_0} = c =$ kontinuum. Kako jednakost dimenzija povlači izomorfnost, vrijedi

PROPOZICIJA 1

Neka je V konačnodimenzionalni linearni prostor. Onda je dualni prostor V^* prostora V izomorfan s V. ■

Postavlja se pitanje kako taj izomorfizam realizirati? Neka je

$$B = (a_1, \ldots, a_n)$$

bilo koja baza za prostor V. Kako je F jednodimenzionalan, njegova se baza sastoji od jednog jedinog elementa. Uzmimo za bazu u F specijalno skup

$\{1\}$, gdje je $1 \in F$ jedinica polja. Prema konstrukciji u Tm. 5 iz 8.6., baza za V^* onda je dana funkcionalima definiranim s

$$f_{1j}(a_k) = \begin{cases} 1, & k = j \\ 0, & k \neq j \end{cases},$$

gdje su $j, k = 1, \ldots, n$. Ovdje nam nisu potrebna dva indeksa, pa pišemo $f_{1j} = l_j$. Svojstvo tih funkcionala onda jednostavnije zapisujemo s

$$l_j(a_k) = \delta_{jk},$$

gdje je s δ_{jk} označen tzv. **Kroneckerov simbol**, definiran s

$$\delta_{jk} = \begin{cases} 1, & j = k \\ 0, & j \neq k \end{cases}.$$

Prema tome je

$$B^* = (l_1, \ldots, l_n)$$

baza za prostor V^*. Iz konstrukcije je jasno da je ta baza jednoznačno određena izborom baze B za prostor V. Bazu B^* nazivamo **dualna baza** za bazu B. Svaka baza $B \subset V$ definira, dakle, jedan standardni izomorfizam

$$\Phi_B : V \to V^*$$

određen s

$$\Phi_B(a_i) = l_i, \quad i = 1, \ldots, n.$$

Kako je V^* također linearni prostor, i on ima svoj dual $(V^*)^*$, koji označujemo kraće s V^{**} i zovemo **bidual od** V. Vektori u V^{**} su, dakako, linearni funkcionali definirani na prostoru V^* svih linearnih funkcionala na prostoru V. Pritom je

$$\dim V^{**} = \dim V^* = \dim V.$$

Nastavljajući tu konstrukciju, dolazimo do niza

$$V, V^*, V^{**}, V^{***}, \ldots$$

linearnih prostora nad istim poljem F, u kojem je svaki prostor dual svog prethodnika. Svi su ti prostori iste dimenzije, **dakle izomorfni**. Kako smo vidjeli, konstrukcija tih izomorfizama će općenito **ovisiti o izboru baze**. Zanimljivo je, međutim, da je moguće definirati izomorfizam $V \to V^{**}$ na prirodan način, bez posredovanja baze. Pokazat ćemo kako.

Neka je $a \in V$ dani vektor. Onda definiramo funkcional

$$u_a : V^* \to F$$

na V^*, stavljajući

$$u_a(l) = l(a)\,, \quad \forall\, l \in V^*\,.$$

Dakle, funkcija u_a pridružuje svakom linearnom funkcionalu $l \in V^*$ vrijednost tog funkcionala, $l(a) \in F$, na danom vektoru a.

PROPOZICIJA 2

Funkcional u_a je linearan na V^*, dakle, element prostora V^{**}.

Dokaz

Za $l, m \in V^*$ i bilo koje skalare $\alpha, \beta \in F$ imamo

$$\begin{aligned} u_a(\alpha l + \beta m) &= (\alpha l + \beta m)(a) = \\ &= \alpha\, l(a) + \beta\, m(a) = \alpha\, u_a(l) + \beta\, u_a(m)\,. \end{aligned}$$

■

Na taj smo način opisali **neke** elemente u prostoru V^{**}. Pitanje je jesu li to svi, tj. može li se svaki linearni funkcional na V^* prikazati na navedeni način? Odgovor je pozitivan ako je prostor V konačnodimenzionalan.

Neka je, dakle,

$$\Phi : V \to V^{**}$$

operator definiran na prirodan način, tj. s

$$\Phi(a) = u_a\,, \quad \forall a \in V\,.$$

Pokažimo najprije da je Φ injekcija. U tu nam je svrhu potrebna

LEMA 3

Neka je $a \in V$ vektor sa svojstvom da je $l(a) = 0$ za svaki funkcional $l \in V^*$. Onda je $a = \Theta$.

Dokaz

Neka je $(a_1, \ldots, a_n) \subset V$ baza za V, a $(l_1, \ldots, l_n) \subset V^*$ njoj dualna baza u V^*. Neka je

$$a = \sum_{i=1}^{n} \alpha_i a_i$$

prikaz danog vektora u zadanoj bazi. Onda je

$$l_j(a) = l_j(\sum_{i=1}^{n} \alpha_i a_i) = \sum_{i=1}^{n} \alpha_i\, l_j(a_i) = \sum_{i=1}^{n} \alpha_i \delta_{ji} = \alpha_j\,.$$

Kako se po pretpostavci svaki funkcional poništava na vektoru a, imamo

$$\alpha_j = l_j(a) = 0$$

za svaki $j = 1, \ldots, n$, dakle $a = \Theta$, kako se i tvrdilo. ■

PROPOZICIJA 4

Operator Φ je injekcija.

Dokaz

Neka je $\Phi(a) = \Phi(b)$. Onda je, po definiciji, $u_a = u_b$, dakle $u_a(l) = u_b(l)$ za svaki $l \in V^*$. No, to znači da je $l(a) = l(b)$, ili zbog linearnosti $l(a-b) = 0$, za svaki $l \in V^*$. Onda je, prema Lemi 3, $a - b = \Theta$, dakle $a = b$, što je i trebalo dokazati. ■

Vrijedi, međutim, i više. Imamo

TEOREM 5

Neka je V konačnodimenzionalni prostor. Onda je Φ izomorfizam linearnih prostora.

Dokaz

Pokažimo najprije da je Φ linearni operator. Za $l \in V^*$ imamo

$$\begin{aligned}[\Phi(\alpha a + \beta b)](l) &= u_{\alpha a+\beta b}(l) = l(\alpha a + \beta b) = \\ &= \alpha\, l(a) + \beta\, l(b) = \alpha\, u_a(l) + \beta\, u_b(l) = \\ &= (\alpha u_a + \beta u_b)(l) = [\alpha\, \Phi(a) + \beta\, \Phi(b)](l)\,.\end{aligned}$$

Kako to vrijedi za svaki l, imamo

$$\Phi(\alpha a + \beta b) = \alpha\, \Phi(a) + \beta\, \Phi(b)\,,$$

pa je linearnost dokazana.

Kako je prema Prop. 4 Φ i injekcija, zaključujemo da je prostor V izomorfan s potprostorom $\Phi(V) < V^{**}$ i prema tome je $\dim \Phi(V) = \dim V$. U drugu ruku, jer je V konačnodimenzionalan, imamo $\dim V^{**} = \dim V$, pa je

$$\dim \Phi(V) = \dim V^{**}.$$

Odatle pak slijedi (vidi Zad. 9. u 7.6.) da je

$$\Phi(V) = V^{**}\,,$$

tj. Φ je i surjekcija. Time je teorem dokazan. ■

Primijetimo kako smo dokazali i to da je svaki linearni funkcional w na V^* oblika u_a, jer iz surjektivnosti slijedi da postoji $a \in V$ tako da je $\Phi(a) = w$, dakle je $w = u_a$.

Preslikavanje $\Phi : V \to V^{**}$ nazivamo **prirodni** ili **kanonski izomorfizam** između prostora V i njegova biduala V^{**}.

Inspirirani tom prirodnom korespondencijom vektora u V i V^{**}, **identificiramo** funkcional $u_a \in V^{**}$ s vektorom $a \in V$ koji ga određuje, i pišemo $u_a = a$, pa onda i

$$V^{**} = V \ ,$$

tj. kažemo da je kod konačnodimenzionalnih prostora dual duala jednak polaznom prostoru. To se svojstvo prostora naziva **refleksivnost**.

Preciznije, linearni prostor V je **refleksivan**, ako je prirodno izomorfan (tj. izomorfan bez posredovanja baze) sa svojim bidualom V^{**}, tj. ako vrijedi $V^{**} = V$. Kako smo pokazali, svaki je konačnodimenzionalni prostor refleksivan. Može se, međutim, pokazati da vrijedi i obrat (vidi primjedbu o dimenziji duala beskonačnodimenzionalnog prostora ispred Prop. 1), tj. da svojstvo refleksivnosti karakterizira konačnodimenzionalne prostore. Zapišimo

TEOREM 6

Linearni prostor je konačne dimenzije ako i samo ako je refleksivan. ■

ZADACI

1. Kako smo rekli, preslikavanje linearnog prostora u pripadno polje naziva se funkcional. Koji su od sljedećih funkcionala $l : P \to \mathbb{R}$ linearni, a koji to nisu:

   (a) $l(p) = \int_0^1 p(t)\,\mathrm{d}t$;

   (b) $l(p) = \int_0^1 [p(t)]^2\,\mathrm{d}t$;

   (c) $l(p) = \int_0^1 t^2\,p(t)\,\mathrm{d}t$;

   (d) $l(p) = \int_0^1 p(t^2)\,\mathrm{d}t$;

   (e) $l(p) = \int_0^1 p(t)\,\mathrm{d}t + 1$.

2. Za dani vektor $\vec{a} \in V^3$ je skalarno množenje

   $$l_{\vec{a}} : V^3 \to \mathbb{R} \ , \ l_{\vec{a}}(\vec{x}) = \vec{a} \cdot \vec{x} \ ,$$

   linearni funkcional na V^3; dokaži. Mogu li se na taj način opisati svi linearni funkcionali na V^3?

3. Pokaži direktno: Ako je $(a_1, \ldots, a_n)$ baza za V, a $(\lambda_1, \ldots, \lambda_n)$ bilo koji izbor skalara iz F, onda postoji jedinstveni linearni funkcional

$l : V \to F$, tako da je $l(a_i) = \lambda_i$, za svaki $i = 1, \ldots, n$. Za svaki vektor $a = \sum_{i=1}^{n} \alpha_i a_i \in V$ imamo onda

$$l(a) = \sum_{i=1}^{n} \alpha_i \lambda_i \, .$$

Pokaži da se na taj način (varirajući λ_i-ove) mogu opisati **svi linearni funkcionali** koji djeluju na V.

4. Pokaži direktno: Neka je $(a_1, \ldots, a_n)$ baza za V, a $l_i : V \to F$ familija funkcionala, definirana na toj bazi s $l_i(a_j) = \delta_{ij}$, $i = 1, \ldots, n$. Onda je $(l_1, \ldots, l_n)$ baza za V^*.

5. Neka su $L, M < V$ potprostori konačnodimenzionalnog prostora V, i neka je $L \cap M = \{\Theta\}$. Ako su $l : L \to F$ i $m : M \to F$ linearni funkcionali, onda postoji bar jedan linearni funkcional

$$v : V \to F$$

sa svojstvom da je $v(a) = l(a)$, za svaki $a \in L$, i $v(b) = m(b)$, za svaki $b \in M$. Dokaži! Kada je takav v jednoznačno određen? Pod kojim se uvjetom može ispustiti pretpostavka da je $L \cap M = \{\Theta\}$?

6. Ako su $a, b \in V$, $a \neq b$, različiti vektori, dokaži da postoji linearni funkcional $l \in V^*$ takav da je $l(a) \neq l(b)$!

7. Za linearni funkcional $l : V \to F$ je rang $r = 0$, ako i samo ako je l nulfunkcional. Dokaži!

8. Neka je $S \subset V$ bilo koji podskup od V. Onda definiramo **anihilator** S^0 skupa S sa

$$S^0 = \{l \in V^* \mid l(a) = 0 \, , \quad \forall a \in S\} \subset V^* \, ,$$

tj. kao skup svih linearnih funkcionala na V koji S preslikavaju u nulu. Na primjer, $\{\Theta\}^0 = V^*$, a $V^0 = \{n\} < V^*$, gdje je n nulfunkcional. Pokaži da je S^0 uvijek potprostor od V^*!

9. Dokaži: Neka je V n-dimenzionalni prostor, a $L < V$ njegov l-dimenzionalni potprostor. Onda je L^0 $(n - l)$-dimenzionalni potprostor od V^*.

10. Neka je $L < V$ potprostor (konačnodimenzionalnog) prostora V. Dokaži da je $L^{00} = (L^0)^0 = L$ (jednakost u smislu konvencije o identifikaciji).

11. Dokaži još ova svojstva anihilatora:

    (a) ako je $S \subset V$ bilo koji podskup, onda je $S^{00} = [S]$;

    (b) za podskupove $S, T \subset V$, $S \subset T$ povlači $T^0 < S^0$;

    (c) ako su $L, M < V$ potprostori, onda je $(L \cap M)^0 = L^0 + M^0$, a $(L + M)^0 = L^0 \cap M^0$;

    (d) iz (c) posebno slijedi da $V = L \oplus M$ povlači da je $V^* = L^0 \oplus M^0$.

    Posljednja tvrdnja nije istinita za rastav prostora V u više od dva direktna sumanda.

12. Pokaži da je (uz konvenciju o identifikaciji) za svaku bazu $B \subset V$ $B^{**} = B$.

13. Neka je $f : U \to V$ linearni operator. Onda definiramo (kontravarijantni) operator

$$\widehat{f} : V^* \to U^*$$

    stavljajući

$$\widehat{f}(l) = l \circ f$$

    za svaki funkcional $l \in V^*$. Dokaži da je $\widehat{f}$ linearni operator (koji djeluje na dualnom prostoru). Taj se operator zove **dualni operator** od f.

14. Dokaži da je preslikavanje

$$\Phi : \mathrm{Hom}(U, V) \to \mathrm{Hom}(V^*, U^*)$$

    dano s

$$\Phi(f) = \widehat{f}$$

    linearni operator. Je li Φ izomorfizam?

15. Pokaži: Preslikavanje

$$\Psi : \mathrm{Hom}(U, V) \to \mathrm{Hom}(U^{**}, V^{**})$$

    definirano s

$$\Psi(f) = \left(\widehat{f}\right)\widehat{\ }$$

    jest prirodni izomorfizam (neovisan o bazi). Tako, uz prirodnu identifikaciju, imamo $\left(\widehat{f}\right)\widehat{\ } = f$.

16. Neka su U, V prostori konačne dimenzije, a $f : U \to V$ linearni operator. Dokaži da je

$$[S(f)]^0 = J(\widehat{f}),$$

$$[J(f)]^0 = S(\widehat{f}).$$

17. Neka je $l \neq n$ linearni funkcional na V i $\alpha \in F$ bilo koji skalar. Postoji li nužno vektor $a \in V$ takav, da je $l(a) = \alpha$?

18. Neka su $l, m \in V^*$ funkcionali sa svojstvom da je $l(x) = 0$ čim je $m(x) = 0$. Pokaži da onda postoji skalar $\lambda \in F$ takav da je $l = \lambda m$. [Uputa: Uzmi $\lambda = l(a)/m(a)$, $m(a) \neq 0$.]

19. Neka su $l_1, \ldots, l_m$ linearni funkcionali na prostoru V, $m < n = \dim V$. Dokaži da uvijek postoji vektor $a \neq \Theta$, takav da je $l_i(a) = 0$, za sve $i = 1, \ldots, m$. Ako su $\alpha_1, \ldots, \alpha_m \in F$ skalari, uz koje će uvjete na njih postojati $a \in V$ takav da je $l_i(a) = \alpha_i$, $i = 1, \ldots, m$?

20. Dokaži: Ako je V linearni prostor nad konačnim poljem i $\dim V = n$, onda se broj k-dimenzionalnih potprostora od V podudara s brojem $(n-k)$-dimenzionalnih potprostora od V^*, za svaki $0 \leq k \leq n$.

21. Neka je $\alpha_1, \ldots, \alpha_n \in F$ izbor skalara iz polja F, a $\varphi : F^n \to F$ preslikavanje dano s

$$\varphi(t) = \varphi(t_1, \ldots, t_n) = \sum_{i=1}^{n} \alpha_i t_i \,.$$

Onda φ nazivamo **linearna forma** u n varijabli nad poljem F. Neka je $\mathcal{F}$ skup svih takvih linearnih formi. Pokaži da je uz standardno definirane operacije, tj. zbrajanje

$$(\varphi + \psi)(t) = \sum_{i=1}^{n} (\alpha_i + \beta_i) t_i$$

i množenje skalarom

$$(\lambda\varphi)(t) = \sum_{i=1}^{n} \lambda\alpha_i \, t_i \,,$$

$\mathcal{F}$ linearni prostor, za koji su forme $(\varphi_1, \ldots, \varphi_n)$, $\varphi_i(t) = t_i$, jedna baza (dakle $\dim \mathcal{F} = n$).

Neka je V linearni prostor, $\dim V = n$, a $(a_1, \ldots, a_n)$ njegova baza. Neka je $l \in V^*$ linearni funkcional i $l(a_i) = \alpha_i$, za $i = 1, \ldots, n$. Dokaži da je preslikavanje

$$\Phi : V^* \to \mathcal{F}$$

dano s

$$[\Phi(l)](t_1, \ldots, t_n) = \sum_{i=1}^{n} \alpha_i t_i$$

izomorfizam koji prevodi dualnu bazu (l_i) od (a_i) na bazu (φ_i), $\Phi(l_i) = \varphi_i$. Dokaži da se vrijednost $l(a)$ funkcionala l na vektoru a podudara s vrijednošću pripadne linearne forme $\Phi(l)$ na varijablama $t_1, \ldots, t_n$, koje su koeficijenti u prikazu vektora a u bazi (a_i), $a = \sum_{i=1}^{n} t_i a_i$, tj.

$$l(a) = [\Phi(l)](t_1, \ldots, t_n) .$$

22. Neka su U i V linearni prostori nad istim poljem F, a

$$\Phi : U \times V \to F$$

funkcional, koji je linearan na svakom faktoru, dakle takav da vrijedi

(1) biaditivnost, tj.

$$\Phi(a_1 + a_2, b) = \Phi(a_1, b) + \Phi(a_2, b),$$

$$\Phi(a, b_1 + b_2) = \Phi(a, b_1) + \Phi(a, b_2);$$

(2) bihomogenost, tj.

$$\Phi(\alpha a, b) = \alpha\, \Phi(a, b),$$

$$\Phi(a, \beta b) = \beta\, \Phi(a, b).$$

Onda kažemo da je Φ **bilinearni funkcional** na produktu $U \times V$. Neka su V i V^* linearni prostor i njegov dual, a

$$\Phi : V \times V^* \to F$$

preslikavanje definirano s

$$\Phi(a, l) = l(a) = \text{oznaka} = \langle a, l \rangle.$$

Pokaži da Φ nije linearni funkcional na $V \times V^*$, ali je bilinearni funkcional na tom produktu. Nadalje, uz identifikaciju $V^{**} = V$ vrijedi

$$\langle a, l \rangle = \langle l, a \rangle$$

pa govorimo o **simetriji** tog funkcionala.

23. Za prostore U i V nad poljem F kažemo da su **dualni**, ako postoji bilinearni funkcional

$$\Phi : U \times V \to F$$

sa svojstvima

(1) $\Phi(a, b) = 0$, za svako $a \in U$, povlači da je $b = \Theta_V$;

(2) $\Phi(a, b) = 0$, za svako $b \in V$, povlači da je $a = \Theta_U$.

Pokaži da su, i u smislu ove (šire) definicije, prostori V i V^* također dualni prostori. Provjeri koji se rezultati o dualnosti iz točke 8.7. prenose i na ovaj generalniji pojam dualnosti prostora.

9

MATRICE I DETERMINANTE

U rudimentarnom obliku smo se s pojmom determinante, pa onda i matrice (trećeg reda), susreli na nekoliko mjesta već u petom i šestom poglavlju. U ovom poglavlju matrice i determinante izučavamo u svoj njihovoj (dimenzionalnoj) općenitosti, sustavno i detaljno, navodeći velik broj njihovih svojstava. Jedna od motivacija usmjeravanja tolike pažnje tim pojmovima u okviru linearne algebre dana je u uvodnoj točki, koja slijedi.

9.1. Uvodne napomene

Neka je $f : U \to V$ linearni operator, a $A = (a_1, \ldots, a_n)$ i $B = (b_1, \ldots, b_m)$ baze u prostorima U, odnosno V. Kako znamo, linearni je operator zadan svojim djelovanjem na bazi A (vidi Kor. 3 u 8.3.), dakle s

$$f(a_k) = \sum_{i=1}^{m} \alpha_{ik} b_i, \quad k = 1, \ldots, n.$$

Prema tome, taj je operator jednoznačno određen skupom skalara $\alpha_{ik} \in F$, koji pregledno zapisujemo u obliku pravokutne sheme

$$\begin{bmatrix} \alpha_{11} & \alpha_{12} & \cdots & \alpha_{1n} \\ \alpha_{21} & \alpha_{22} & \cdots & \alpha_{2n} \\ \vdots & \vdots & & \vdots \\ \alpha_{m1} & \alpha_{m2} & \cdots & \alpha_{mn} \end{bmatrix}$$

koju nazivamo **matrica operatora** f u paru baza (A, B). Razabiremo da su u k-tom stupcu sheme popisani koeficijenti u prikazu vektora $f(a_k)$ u bazi B. Vidjet ćemo da je, uz prikladno definirane operacije s matricama (vidi Zad. 4. u 5.14.), to pridruživanje izomorfizam, tj. da se uz dane baze

A i B linearni operatori iz $\mathrm{Hom}\,(U, V)$ mogu **reprezentirati** pridruženim matricama. Prednost takve reprezentacije je u tome što se s matricama kao kolekcijama brojeva (relativno) lako računa, posebno pomoću računala.

Slične sheme, matrice, prirodno se pojavljuju i u vezi s raznim drugim problemima u algebri, geometriji i matematici općenito, pa i u fizici, kemiji, ekonomiji itd. Nama će biti od posebne koristi i pri problemu rješavanja sustava linearnih jednadžbi (vidi jedanaesto poglavlje). To nam sugerira da se pojam i svojstva matrica izučavaju zasebno, neovisno o situaciji u kojoj dolaze.

Kažimo nekoliko povijesnih napomena. Pojam matrice je svjesno i neovisno o primjenama uveden u matematiku tek potkraj 19. stoljeća. Imena vezana za početak teorije matrica su J. J. Sylvester i A. Cayley. U daljnjoj izgradnji teorije zapažene su priloge dali M. E. C. Jordan (normalna forma), C. Hermite (hermitska forma), K. Weierstrass (elementarni divizori), pa L. Kronecker, G. Frobenius itd.

9.2. Definicija matrice

Neka je F bilo koje polje, koje ćemo zvati **osnovno polje**, a njegove elemente **skalarima**. Neka su, nadalje, $m, n \in \mathbb{N}$ prirodni brojevi, a s D_{mn} neka je označen Kartezijev produkt

$$D_{mn} = \{1, 2, \ldots, m\} \times \{1, 2, \ldots, n\}.$$

Svako preslikavanje

$$A : D_{mn} \to F$$

tog produkta u osnovno polje nazivamo **matrica tipa** (m, n) **nad poljem** F. Vrijednost funkcije A na mjestu (i, k) označavamo s

$$A(i, k) = \alpha_{ik} \in F\ .$$

Kako je domena od A konačna, tradicionalno matricu A zapisujemo tablično kao

$$A = \begin{bmatrix} \alpha_{11} & \cdots & \alpha_{1n} \\ \vdots & & \vdots \\ \alpha_{m1} & \cdots & \alpha_{mn} \end{bmatrix}\ .$$

Još je uobičajeno da se matrica zapisuje

$$\begin{pmatrix} \alpha_{11} & \cdots & \alpha_{1n} \\ \vdots & & \vdots \\ \alpha_{m1} & \cdots & \alpha_{mn} \end{pmatrix} \quad \text{ili} \quad \left\| \begin{matrix} \alpha_{11} & \cdots & \alpha_{1n} \\ \vdots & & \vdots \\ \alpha_{m1} & \cdots & \alpha_{mn} \end{matrix} \right\|\ ,$$

odnosno u teorijskim razmatranjima, kad je iz konteksta poznata domena, simbolički kao

$$[\alpha_{ik}] \ , \quad (\alpha_{ik}) \quad \text{ili} \quad \|\alpha_{ik}\| \ .$$

Skalare α_{ik}, $i = 1, \ldots, m$, $k = 1, \ldots, n$, nazivamo **elementima matrice** A, a α_{ik} u prethodnom zapisu njihov je **reprezentant**.

Kažemo da uređena n-torka

$$(\alpha_{i1}, \alpha_{i2}, \ldots, \alpha_{in})$$

elemenata iz A čini i-ti **redak** matrice A, a uređena m-torka

$$(\alpha_{1k}, \alpha_{2k}, \ldots, \alpha_{mk})$$

njezin k-ti **stupac**. Prema tome, matrica tipa (m, n) ima m redaka i n stupaca. Kažemo također da se element α_{ik} nalazi na presjeku i-tog retka i k-tog stupca. Na primjer,

$$\begin{bmatrix} 2 & 1 & 5 \\ 0 & -1 & 3 \end{bmatrix}$$

je matrica tipa $(2, 3)$, a njezin se element 5 nalazi na presjeku prvog retka i trećeg stupca.

Od posebne je važnosti matrica u kojoj su svi elementi $\alpha_{ik} = 0$, tj. matrica

$$O = \begin{bmatrix} 0 & \cdots & 0 \\ \vdots & & \vdots \\ 0 & \cdots & 0 \end{bmatrix},$$

koju nazivamo **nulmatrica** tipa (m, n).

Matrica tipa $(1, n)$, tj. oblika

$$\begin{bmatrix} \alpha_{11} & \alpha_{12} & \cdots & \alpha_{1n} \end{bmatrix},$$

naziva se **redčana matrica** ili matrica redak, a matrica tipa $(m, 1)$, dakle oblika

$$\begin{bmatrix} \alpha_{11} \\ \vdots \\ \alpha_{m1} \end{bmatrix},$$

naziva se **stupčana matrica** ili matrica stupac.

Ako se specijalno za matricu A broj stupaca i redaka podudara, tj. ako je tipa (n, n), kažemo da je A **kvadratna matrica**, i to **reda** n. Za kvadratnu matricu definiramo **glavnu dijagonalu**, kao n-torku njezinih elemenata

$$(\alpha_{11}, \alpha_{22}, \ldots, \alpha_{nn}),$$

i **sporednu dijagonalu**, kao n-torku

$$(\alpha_{1n}, \alpha_{2\,n-1}, \ldots, \alpha_{n1}).$$

Nadalje, za takvu matricu A definiramo **trag**, kao sumu elemenata na glavnoj dijagonali,

$$\operatorname{tr} A = \sum_{i=1}^{n} \alpha_{ii} .$$

Kvadratnu matricu s elementima $\alpha_{ik} = \delta_{ik}$, tj. matricu

$$E = \begin{bmatrix} 1 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & 1 \end{bmatrix} ,$$

nazivamo **jedinična matrica** reda n.

Kako su matrice specijalno i funkcije, matrice $A = [\alpha_{ik}]$ i $B = [\beta_{ik}]$ nad istim poljem F će biti **jednake**,

$$A = B ,$$

ako su istog tipa (ista domena) i ako je

$$\alpha_{ik} = \beta_{ik} ,$$

za svaki i i k. Na primjer, matrice

$$\begin{bmatrix} 2 & 3 & 0 \\ 4 & 1 & 0 \end{bmatrix} \quad \text{i} \quad \begin{bmatrix} 2 & 3 \\ 4 & 1 \end{bmatrix}$$

nisu jednake, jer nisu istog tipa.

Matricom $A = [\alpha_{ik}]$ tipa (m, n) jednoznačno je određena matrica $B = [\beta_{ki}]$ tipa (n, m), definirana s

$$\beta_{ki} = \alpha_{ik} ,$$

za svaki $i = 1, \ldots, m$, $k = 1, \ldots, n$. Tu matricu nazivamo **transponirana matrica** matrice A i označavamo je s A'. Prema tome, transponirana se matrica dobiva iz polazne zamjenom stupaca s redcima, tj. i-ti stupac matrice A' se podudara s i-tim retkom matrice A, za svaki $i = 1, \ldots, m$. Imamo npr.

$$A = \begin{bmatrix} 2 & 3 \\ 4 & 1 \\ 0 & 2 \end{bmatrix} \quad \text{i} \quad A' = \begin{bmatrix} 2 & 4 & 0 \\ 3 & 1 & 2 \end{bmatrix} .$$

Očito je uvijek

$$(A')' = A\,.$$

Primijetimo, nadalje, da je transponirana matrica kvadratne matrice opet kvadratna matrica istog reda.

Neka su s $M_{mn}(F)$ i $M_n(F)$ označeni skup svih matrica tipa (m,n) nad poljem F, odnosno skup svih kvadratnih matrica reda n nad tim poljem. Ako je iz konteksta jasno o kojem se osnovnom polju radi, te ćemo skupove kraće označivati kao M_{mn} i M_n. Naš je sljedeći zadatak da na tim skupovima definiramo standardne strukture.

ZADACI

1. Matrice nad poljem realnih brojeva zovemo **realne matrice**, a one nad poljem kompleksnih brojeva **kompleksne matrice**. Neka je $A = [\alpha_{ik}]$ kompleksna matrica tipa (m,n). Matricu $B = [\beta_{ik}]$ istog tipa, definiranu s

$$\beta_{ik} = \overline{\alpha_{ik}}\,,$$

za svaki i i k, gdje potez označava kompleksno konjugiranje, nazivamo **konjugirana matrica** matrice A i označavamo je s $\overline{A}$. Na primjer, za

$$A = \begin{bmatrix} 3+2i & 1 \\ i & 0 \end{bmatrix} \quad \text{je} \quad \overline{A} = \begin{bmatrix} 3-2i & 1 \\ -i & 0 \end{bmatrix}\,.$$

Pokaži:

(a) $\overline{A} = A$ onda i samo onda, kad je matrica A realna;

(b) $\overline{(\overline{A})} = A$;

(c) Ako je $B = \overline{A}$, onda je $A = \overline{B}$ (pa se govori o paru konjugiranih matrica);

(d) $(\overline{A})' = \overline{(A')}$, tj. operacije konjugiranja i transponiranja komutiraju.

2. Neka je $A = [\alpha_{ik}]$ kompleksna matrica tipa (m,n). Matricu $B = [\beta_{ki}]$ tipa (n,m), definiranu s

$$\beta_{ki} = \overline{\alpha_{ik}}\,,$$

za $i = 1,\ldots,m,\ k = 1,\ldots,n$, nazivamo **hermitski konjugirana** ili, također, **adjungirana matrica** matrice A i označavamo s A^*. Prema tome je

$$A^* = (\overline{A})'.$$

Na primjer, za

$$A = \begin{bmatrix} 2-i & 3i \\ 1+2i & 5 \end{bmatrix} \quad \text{je} \quad A^* = \begin{bmatrix} 2+i & 1-2i \\ -3i & 5 \end{bmatrix} .$$

Pokaži:

(a) $A^* = A'$ ako i samo ako je A realna;

(b) $(A^*)^* = A$;

(c) $B = A^*$ povlači $A = B^*$ (pa se govori o paru adjungiranih matrica).

9.3. Linearni prostor M_{mn}

Neka je $M_{mn} = M_{mn}(F)$ skup svih matrica tipa (m, n) nad poljem F. Pokazat ćemo da ga na prirodan način možemo snabdjeti strukturom linearnog prostora.

Ako su $A, B \in M_{mn}$, $A = [\alpha_{ik}]$, $B = [\beta_{ik}]$, bilo koje matrice, definiramo (kao kod funkcija!) njihov **zbroj**, kao matricu $C = [\gamma_{ik}]$ istog tipa kao A i B, čiji su elementi dani s

$$\gamma_{ik} = \alpha_{ik} + \beta_{ik} ,$$

za svaki $i = 1, \ldots, m$, $k = 1, \ldots, n$. Pišemo

$$C = A + B .$$

Kako je $A+B \in M_{mn}$, radi se o dobro definiranoj binarnoj operaciji. Imamo na primjer

$$\begin{bmatrix} 2 & 3 & 5 \\ 3 & 1 & 2 \end{bmatrix} + \begin{bmatrix} 1 & 0 & 1 \\ -2 & 4 & -4 \end{bmatrix} = \begin{bmatrix} 3 & 3 & 6 \\ 1 & 5 & -2 \end{bmatrix} .$$

Ako A i B nisu istog tipa, njihov **zbroj se ne definira**.

PROPOZICIJA 1

Skup M_{mn} je uz operaciju zbrajanja matrica komutativna grupa.

Dokaz

To se lako provjeri. Neutralni element je nulmatrica O, a za matricu $A = [\alpha_{ik}]$ je suprotna matrica $-A = [-\alpha_{ik}]$. ∎

Za $\lambda \in F$ i bilo koju matricu $A \in M_{mn}$, $A = [\alpha_{ik}]$, definiramo **produkt te matrice sa skalarom** λ kao matricu $C = [\gamma_{ik}]$, koja je istog tipa kao A, a za čije elemente vrijedi

$$\gamma_{ik} = \lambda\alpha_{ik} ,$$

za sve $i = 1, \ldots, m$, $k = 1, \ldots, n$. Pišemo

$$C = \lambda A \, .$$

Tako je npr.

$$3 \begin{bmatrix} 2 & 3 & 1 \\ 1 & 0 & -2 \end{bmatrix} = \begin{bmatrix} 6 & 9 & 3 \\ 3 & 0 & -6 \end{bmatrix} \, .$$

Kako očito vrijedi

(1) $\lambda(\mu A) = (\lambda\mu)A$;

(2) $1\,A = A$;

(3) $(\lambda + \mu)A = \lambda A + \mu A$;

(4) $\lambda(A + B) = \lambda A + \lambda B$,

za svaki izbor λ, $\mu \in F$ i $A, B \in M_{mn}$, jer se te tvrdnje svode na analogne tvrdnje u polju F, imamo zaključak

TEOREM 2

Skup M_{mn} je, uz standardne operacije zbrajanja matrica i množenja skalarom, linearni prostor nad poljem F i $\dim M_{mn} = mn$.

Dokaz

Tvrdnja o dimenziji slijedi iz činjenice da je skup matrica

$$\{A_{ik} \mid i = 1, \ldots, m, \;\; k = 1, \ldots, n\} \subset M_{mn},$$

gdje A_{ik} ima elemente

$$\alpha_{rs} = \begin{cases} 1, & \text{ako je} \quad r = i, \;\; s = k \\ 0, & \text{inače} \end{cases} \, ,$$

baza za prostor M_{mn}, što se lako dokaže. ■

Prema tome je (Prop. 6 u 8.4.) $M_{mn} \cong F^{mn}$. Taj se izomorfizam može prirodno uspostaviti, imajući na umu da je matrica zapravo specifičan zapis uređene mn-torke elemenata iz polja F. Tako je preslikavanje

$$\begin{bmatrix} \alpha_{11} & \cdots & \alpha_{1n} \\ \vdots & & \vdots \\ \alpha_{m1} & \cdots & \alpha_{mn} \end{bmatrix} \mapsto (\alpha_{11}, \ldots, \alpha_{1n}, \ldots, \alpha_{m1}, \ldots, \alpha_{mn}) \in F^{mn}$$

izomorfizam linearnih prostora M_{mn} i F^{mn}. Specijalno je skup M_n linearni prostor nad F i $M_n \cong F^{n^2}$, pa je $\dim M_n = n^2$. Za $n = 1$ imamo odatle

$M_1 \cong F$, pa identificirajući matrice prvog reda sa svojim jedinim elementom, $[\alpha_{11}] = \alpha_{11}$, pišemo $M_1 = F$ i kažemo da su matrice prvog reda skalari.

ZADACI

1. Za kvadratnu matricu A kažemo da je **simetrična** ako je $A' = A$, a **antisimetrična** ako je $A' = -A$. Ako je $A = [\alpha_{ik}]$, u prvom slučaju imamo

$$\alpha_{ki} = \alpha_{ik} ,$$

za svaki i, k, tj. u simetričnoj su matrici elementi, simetrični u odnosu na glavnu dijagonalu, jednaki. Slično, u antisimetričnoj matrici vrijedi

$$\alpha_{ki} = -\alpha_{ik} ,$$

za svaki i, k. Tako su

$$\begin{bmatrix} 3 & 2 & 4 \\ 2 & 1 & 3 \\ 4 & 3 & 2 \end{bmatrix} , \quad \begin{bmatrix} 0 & 2 & -1 \\ -2 & 0 & 7 \\ 1 & -7 & 0 \end{bmatrix}$$

primjeri simetrične, odnosno antisimetrične matrice. Pokaži da su skup svih simetričnih matrica reda n i skup svih antisimetričnih matrica reda n potprostori linearnog prostora M_n. Koje su dimenzije tih prostora?

2. Dokaži: Ako polje F nije karakteristike 2, svi su elementi na glavnoj dijagonali antisimetrične matrice nad poljem F jednaki nuli.

3. Dokaži: Svaka se kvadratna matrica nad poljem kompleksnih brojeva može prikazati kao suma jedne simetrične i jedne antisimetrične matrice. [Uputa: rabi prikaz $A = \frac{1}{2}(A + A') + \frac{1}{2}(A - A')$.]

4. Kompleksna kvadratna martica A je **hermitski simetrična** ili **hermitska** ako je $A^* = A$, a **hermitski antisimetrična** ili **antihermitska** ako je $A^* = -A$. Na primjer, matrica

$$A = \begin{bmatrix} 5 & 3 + 2i \\ 3 - 2i & 1 \end{bmatrix}$$

je hermitska, a matrica

$$B = \begin{bmatrix} 3i & 2 + i \\ -(2 - i) & 5i \end{bmatrix}$$

je antihermitska. Ako je specijalno matrica A realna, hermitska se simetrija i antisimetrija podudaraju s običnom simetrijom, odnosno antisimetrijom. Pokaži da je u hermitskoj matrici glavna dijagonala uvijek realna, a u antihermitskoj čisto imaginarna. Pokaži, nadalje, da skup svih hermitskih (antihermitskih) matrica reda n čini aditivnu grupu. Da li i linearni prostor?

5. Dokaži: Svaka se kompleksna matrica može prikazati kao suma hermitske i antihermitske matrice.

6. Preslikavanje
$$t : M_{mn} \to M_{nm} ,$$
dano s
$$t(A) = A'$$
i zvano **transponiranje**, jest izomorfizam linearnih prostora. Dokaži!

7. **Konjugiranje**
$$k : M_{mn}(\mathbb{C}) \to M_{mn}(\mathbb{C}) ,$$
dano s
$$k(A) = \overline{A} ,$$
nije linearni operator, ali je bijekcija. Dokaži!

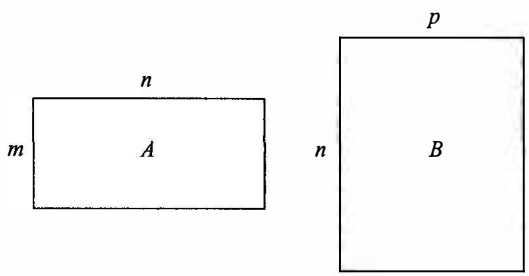
8. Bijekciju $f : U \to V$ između kompleksnih linearnih prostora nazivamo **antiizomorfizam**, ako vrijedi
$$f(\alpha a + \beta b) = \overline{\alpha} f(a) + \overline{\beta} f(b) ,$$
za svaki izbor $\alpha, \beta \in \mathbb{C}$ i $a, b \in U$. Pokaži da su **konjugiranje** i **adjungiranje**
$$a : M_{mn} \to M_{nm} ,$$
tj. operator definiran s
$$a(A) = A^* ,$$
antiizomorfizmi. Uvjeri se, nadalje, da je $a = t \circ k$.

9. Preslikavanje
$$l : M_n \to F ,$$
dano s
$$l(A) = \operatorname{tr} A ,$$
jest linearni funkcional. Dokaži!

9.4. Množenje matrica. Algebra M_n

Za razliku od zbrajanja i množenja skalarom, matrice se ne množe po standardnom zakonu množenja funkcija. Naoko osebujan, specifičan način množenja matrica je inspiriran našom motivacijom uvođenja matrica kao reprezentanata linearnih operatora. Definicija će biti takva da kompoziciji (produktu) linearnih operatora odgovara produkt matrica tih operatora (vidi Zad. 4. u 5.14.).

Množenje matrica se definira samo za matrice kod kojih su dimenzije u specijalnom odnosu, tj. za tzv. **ulančane matrice**. Za uređeni par matrica (A, B) kažemo da je ulančan ako druga matrica ima toliko redaka, koliko prva ima stupaca. Na primjer, matrice A i B su ulančane ako je matrica A tipa (m, n), a matrica B tipa (n, p). Posebno, dakle, bit će uvijek ulančane kvadratne matrice istog reda. Primijetimo da iz činjenice da je par



(A, B) matrica ulančan, ne slijedi da je i par (B, A) ulančan (to će biti ako i samo ako je $p = m$).

Neka su sada $A = [\alpha_{ik}]$ i $B = [\beta_{ik}]$ ulančane matrice nad istim poljem F, prva tipa (m, n), a druga (n, p). Onda **produkt** tih matrica definiramo kao matricu $C = [\gamma_{ik}]$ nad poljem F, koja je tipa (m, p), a čiji su elementi dani s

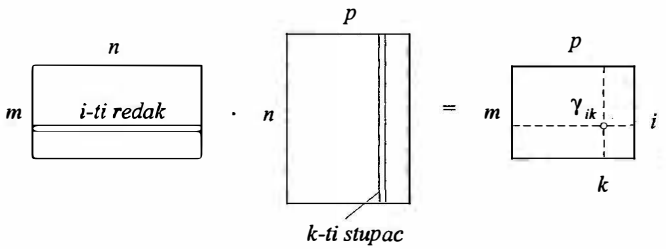
$$\gamma_{ik} = \sum_{j=1}^{n} \alpha_{ij}\beta_{jk} \ ,$$

za svaki $i = 1, \ldots, m$, $k = 1, \ldots, p$. Drugim riječima, element γ_{ik} na presjeku i-tog retka i k-tog stupca matrice C dobiva se kao suma produkata korespondentnih elemenata iz i-tog retka matrice A i k-tog stupca matrice B. Pišemo

$$C = AB \ .$$

Uočimo da je, po definiciji, matrica $C = AB$ tipa (m, p), tj. ima isto toliko redaka kao matrica A i onoliko stupaca koliko matrica B.

Shematski možemo operaciju množenja prikazati kao



odnosno, eksplicitno zapisano

$$AB = \begin{bmatrix} \alpha_{11} & \cdots & \alpha_{1n} \\ \vdots & & \vdots \\ \alpha_{i1} & \cdots & \alpha_{in} \\ \vdots & & \vdots \\ \alpha_{m1} & \cdots & \alpha_{mn} \end{bmatrix} \cdot \begin{bmatrix} \beta_{11} & \cdots & \beta_{1k} & \cdots & \beta_{1p} \\ \vdots & & \vdots & & \vdots \\ \beta_{n1} & \cdots & \beta_{nk} & \cdots & \beta_{np} \end{bmatrix} =$$

$$= \begin{bmatrix} \sum_j \alpha_{1j}\beta_{j1} & \cdots & \sum_j \alpha_{1j}\beta_{jp} \\ \vdots & \sum_j \alpha_{ij}\beta_{jk} & \vdots \\ \sum_j \alpha_{mj}\beta_{j1} & \cdots & \sum_j \alpha_{mj}\beta_{jp} \end{bmatrix} .$$

Imamo tako npr.

$$\begin{bmatrix} 3 & 5 \\ 1 & 2 \\ 0 & 3 \end{bmatrix} \cdot \begin{bmatrix} 4 & 1 & 5 & 2 \\ 1 & 2 & 3 & 4 \end{bmatrix} = \begin{bmatrix} 17 & 13 & 30 & 26 \\ 6 & 5 & 11 & 10 \\ 3 & 6 & 9 & 12 \end{bmatrix} .$$

Da zaključimo: Produkt je definiran samo za ulančane matrice. Prema tome je množenje matrica preslikavanje (operator)

$$M_{mn} \times M_{np} \to M_{mp} .$$

Općenito se, dakle, matrice istog tipa ne mogu množiti. To će biti moguće onda i samo onda ako su matrice kvadratne i istog reda. U tom je slučaju i produkt kvadratna matrica tog reda.

Navedimo sada neka svojstva množenja matrica. Primijetimo, prije svega, da to množenje **nije komutativno**. Lako se naime provjeri da će oba produkta AB i BA biti definirana, i da će to biti matrice istog tipa (što je nuždan uvjet za jednakost matrica) onda i samo onda ako su matrice A

i B kvadratne i istog reda. No, i u tom specijalnom slučaju produkt nije komutativan, kako pokazuje ovaj jednostavan primjer:
za

$$A = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}, \quad B = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$$

je

$$AB = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}, \text{ a } BA = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix},$$

dakle

$$AB \neq BA .$$

Ima, dakako, i matrica za koje vrijedi $AB = BA$. Za takav par matrica A i B kažemo da **komutiraju**. Na primjer, matrice

$$A = \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} \text{ i } B = \begin{bmatrix} 3 & 0 \\ 0 & 3 \end{bmatrix}$$

komutiraju.

PROPOZICIJA 1

Množenje matrica je asocijativno, tj. vrijedi

$$A(BC) = (AB)C,$$

kad god su ti produkti definirani.

Dokaz

Neka su $A = [\alpha_{ij}]$, $B = [\beta_{jk}]$ i $C = [\gamma_{kl}]$ tri matrice, redom tipa (m, n), (n, p) i (p, q). Onda su oba produkta $A(BC)$ i $(AB)C$ definirana i to su matrice (istog) tipa (m, q). Tvrdimo da su jednake. Označimo $BC = [\sigma_{jl}]$. Onda je po definiciji množenja

$$\sigma_{jl} = \sum_{k=1}^{p} \beta_{jk}\gamma_{kl} .$$

Ako je, nadalje,

$$A(BC) = [\xi_{il}] ,$$

imamo

$$\xi_{il} = \sum_{j=1}^{n} \alpha_{ij}\sigma_{jl} = \sum_{j=1}^{n} \alpha_{ij} \sum_{k=1}^{p} \beta_{jk}\gamma_{kl} = \sum_{j=1}^{n} \sum_{k=1}^{p} \alpha_{ij}\beta_{jk}\gamma_{kl} . \qquad (1)$$

U drugu ruku, uz oznaku $AB = [\tau_{ik}]$, imamo

$$\tau_{ik} = \sum_{j=1}^{n} \alpha_{ij}\beta_{jk} ,$$

pa ako je

$$(AB)C = [\eta_{il}] ,$$

računamo

$$\eta_{il} = \sum_{k=1}^{p} \tau_{ik}\gamma_{kl} = \sum_{k=1}^{p} \left(\sum_{j=1}^{n} \alpha_{ij}\beta_{jk} \right) \gamma_{kl} = \sum_{j=1}^{n} \sum_{k=1}^{p} \alpha_{ij}\beta_{jk}\gamma_{kl} . \qquad (2)$$

Uspoređujući (1) i (2) vidimo da je

$$\xi_{il} = \eta_{il} ,$$

za svaki $i = 1, \ldots, m$, $l = 1, \ldots, q$, pa je

$$A(BC) = (AB)C ,$$

tj. asocijativnost je dokazana. ■

Nadalje vrijedi

PROPOZICIJA 2

Množenje matrica je

(1) *kvaziasocijativno, tj.*

$$(\lambda A)B = \lambda(AB) = A(\lambda B), \qquad \forall \lambda \in F \ ;$$

(2) *distributivno prema zbrajanju, tj.*

$$\begin{aligned} (A+B)C &= AC + BC , \\ A(B+C) &= AB + AC . \end{aligned}$$

Dokaz

Dokažimo, npr., (1). Ako je $A = [\alpha_{ij}]$, $B = [\beta_{jk}]$, imamo

$$\begin{aligned} (\lambda A)B &= [\lambda\alpha_{ij}]\,[\beta_{jk}] = \left[\sum_{j} (\lambda\alpha_{ij})\beta_{jk} \right] = \\ &= \left[\lambda \sum_{j} \alpha_{ij}\beta_{jk} \right] = \lambda \left[\sum_{j} \alpha_{ij}\beta_{jk} \right] = \lambda(AB) . \end{aligned}$$

■

Promatrajmo sada specijalno vektorski prostor M_n svih kvadratnih matrica reda n nad poljem F. Za takve je matrice produkt uvijek definiran, i množenje matrica je dobro definirana binarna operacija

$$M_n \times M_n \to M_n$$

na skupu M_n. Ta je operacija asocijativna (Prop. 1) i posjeduje jedinicu, a to je jedinična matrica E, jer očito vrijedi

$$EA = AE = A \ ,$$

za svaki $A \in M_n$. Nadalje, u odnosu na stukturu linearnog prostora u M_n, množenje ima svojstva popisana u Prop. 2. Tako imamo ovaj zaključak

TEOREM 3

Prostor M_n je, s obzirom na množenje matrica, jedna algebra nad poljem F, asocijativna, s jedinicom, ali nekomutativna, ako je $n > 1$. ■

ZADACI

1. Neka su U_1, U_2, i V linearni prostori. Preslikavanje

$$f : U_1 \times U_2 \to V$$

nazivamo **bilinearni operator**, ako je f linearan na svakom faktoru domene, tj. ako vrijedi

$$\begin{aligned} f(\lambda_1 a_1 + \lambda_2 a_2, b) &= \lambda_1 f(a_1, b) + \lambda_2 f(a_2, b) \ , \\ f(a, \mu_1 b_1 + \mu_2 b_2) &= \mu_1 f(a, b_1) + \mu_2 f(a, b_2) \ . \end{aligned}$$

Pokaži da množenje matrica

$$m : M_{mn} \times M_{np} \to M_{mp}$$

nije linearni, ali je bilinearni operator.

2. Skup M_n je uz zbrajanje i množenje matrica prsten s jedinicom. Uvjeri se da uz $n > 1$ dopušta djelitelje nule, tj. da nije integralna domena (vidi primjer u tekstu).

3. Ako su oba produkta AB i BA definirana, onda je uvijek

$$\text{tr}\,(AB) = \text{tr}\,(BA) \ .$$

Dokaži!

4. Neka je A kvadratna matrica. Onda definiramo $A^0 = E$, $A^1 = A$, $A^2 = A \cdot A$, i onda induktivno $A^n = A^{n-1} \cdot A$. Pokaži da za $p, q \in \mathbb{N}$ vrijedi $A^p \cdot A^q = A^{p+q}$, $(A^p)^q = A^{pq}$. Specijalno, dakle, potencije iste matrice komutiraju.

5. Pokaži da je

$$\begin{bmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{bmatrix}^n = \begin{bmatrix} \cos n\alpha & -\sin n\alpha \\ \sin n\alpha & \cos n\alpha \end{bmatrix} .$$

Slično, izračunaj

$$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}^n \quad \text{i} \quad \begin{bmatrix} \lambda & 1 \\ 0 & \lambda \end{bmatrix}^n .$$

6. Za operaciju transponiranja vrijedi

$$(AB)' = B'A' .$$

Dokaži! Vrijedi i generalnije, tj.

$$(A_1 A_2 \dots A_n)' = A_n' A_{n-1}' \dots A_2' A_1' .$$

7. Uvjeri se da produkt simetričnih matrica nije općenito simetrična matrica. To će biti ako i samo ako simetrične matrice komutiraju. Specijalno, svaka potencija simetrične matrice je simetrična matrica. Prema tome, simetrične matrice čine potprostor, ali ne i podalgebru od M_n. Isto vrijedi i za antisimetrične matrice.

8. Neka su A i B kompleksne matrice. Dokaži da za operaciju konjugiranja vrijedi

$$\overline{(AB)} = \overline{A}\ \overline{B} .$$

9. Dokaži da za operaciju adjungiranja vrijedi

$$(AB)^* = B^* A^* .$$

10. Dokaži: Produkt hermitskih matrica nije općenito hermitska matrica. To je ako i samo ako hermitske matrice komutiraju. Isto vrijedi i za antihermitske matrice.

11. Kvadratna matrica $A = [\alpha_{ik}]$ je **dijagonalna** ako je $\alpha_{ik} = 0$ za $i \neq k$, tj. ako je oblika

$$A = \begin{bmatrix} \alpha_{11} & & 0 \\ & \ddots & \\ 0 & & \alpha_{nn} \end{bmatrix} .$$

Pokaži da je skup svih dijagonalnih matrica reda n nad poljem F, uz standardne operacije, jedna algebra, podalgebra od M_n.

12. Pokaži: Kvadratna matrica komutira sa svim dijagonalnim matricama istog reda ako i samo ako je i sama dijagonalna.

13. Dijagonalna matrica A je **skalarna**, ako je

$$\alpha_{11} = \alpha_{22} = \ldots = \alpha_{nn} = \alpha \,,$$

tj. ako je oblika

$$A = \begin{bmatrix} \alpha & & 0 \\ & \ddots & \\ 0 & & \alpha \end{bmatrix} ,$$

gdje je $\alpha \in F$ dani skalar. Očito je

$$A = \alpha E \,.$$

Pokaži da skalarne matrice reda n nad poljem F čine algebru, podalgebru algebre dijagonalnih matrica. Pokaži, nadalje, da je ta algebra izomorfna s F (vidi Zad. 18. u 8.6.).

14. Dokaži: Kvadratna matrica komutira sa svim kvadratnim matricama istog reda ako i samo ako je skalarna.

15. Kvadratna matrica $A = [\alpha_{ik}]$ naziva se **gornja trokutasta matrica**, ako je $\alpha_{ik} = 0$ za sve $i > k$. Takva je matrica oblika

$$A = \begin{bmatrix} \alpha_{11} & \alpha_{12} & \cdots & \alpha_{1n} \\ 0 & \alpha_{22} & \cdots & \alpha_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \alpha_{nn} \end{bmatrix} ,$$

tj. svi su joj elementi ispod glavne dijagonale jednaki nuli. Pokaži da gornje trokutaste matrice reda n čine algebru, podalgebru od M_n. Koja je dimenzija te algebre? Slično se definiraju **donje trokutaste matrice**. I one, dakako, čine algebru.

16. Dokaži: Ako je matrica A simetrična (antisimetrična), onda je simetrična (antisimetrična) i matrica $T'AT$, gdje je T bilo koja kvadratna matrica.

17. Dokaži: Ako je A bilo koja matrica (ne mora biti kvadratna), $A'A$ i AA' su simetrične matrice.

18. Kvadratna matrica A je **normalna**, ako je $AA^* = A^*A$. Kakvu strukturu čine normalne matrice istog reda?

9.5. Regularne matrice. Opća linearna grupa

Promatrajmo skup M_n svih kvadratnih matrica nad poljem F. Kako je množenje matrica asocijativno i posjeduje jedinicu, struktura $(M_n, \cdot)$ je (nekomutativni) monoid. Kao u općoj teoriji, i tu uvodimo pojam inverza.

Za matricu $A \in M_n$ kažemo da je **invertibilna** ako postoji matrica $X \in M_n$ takva, da vrijedi

$$AX = XA = E\,,$$

gdje je E jedinična matrica. Matricu X u tom slučaju zovemo **inverzna matrica** ili **inverz** matrice A. Kako smo vidjeli (Prop. 2 u 2.4.), ako je matrica A invertibilna, njezin je inverz jednoznačno određen pa ćemo ga standardno označiti s A^{-1}.

Invertibilnu matricu nazivamo još i **regularna** matrica, a za matricu koja nije regularna kažemo da je **singularna**. Na primjer, matrica

$$A = \begin{bmatrix} 2 & 3 \\ 4 & 1 \end{bmatrix}$$

jest regularna jer iz

$$AX = \begin{bmatrix} 2 & 3 \\ 4 & 1 \end{bmatrix} \cdot \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = E$$

dobivamo

$$\begin{array}{rcl} 2\alpha + 3\gamma = 1 & \qquad & 2\beta + 3\delta = 0 \\ 4\alpha + \gamma = 0 & & 4\beta + \delta = 1 \end{array}\,,$$

i odatle, rješavajući te sustave,

$$\alpha = -\frac{1}{10},\quad \beta = \frac{3}{10},\quad \gamma = \frac{4}{10},\quad \delta = -\frac{2}{10}\,.$$

No, onda je i

$$XA = \begin{bmatrix} -1/10 & 3/10 \\ 4/10 & -2/10 \end{bmatrix} \cdot \begin{bmatrix} 2 & 3 \\ 4 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = E\,,$$

pa zaključujemo da je

$$X = \begin{bmatrix} -1/10 & 3/10 \\ 4/10 & -2/10 \end{bmatrix} = A^{-1}$$

inverz matrice A.

Postoje, dakako, i singularne matrice. Nulmatrica O je sigurno takva, ali ima i drugih. Lako se npr. vidi da je

$$A = \begin{bmatrix} 2 & 3 \\ 4 & 6 \end{bmatrix}$$

singularna matrica.

U općoj smo teoriji utvrdili (vidi Zad. 1. u 2.7.) da skup invertibilnih elemenata nekog monoida čini grupu. Dokažimo to još jednom u našem specijalnom slučaju.

TEOREM 1

Skup svih regularnih matrica reda n nad poljem F čini u odnosu na množenje (nekomutativnu) grupu.

Dokaz

Očito je dovoljno dokazati da je produkt regularnih matrica opet regularna matrica, i da je inverz regularne matrice regularna matrica. Neka su, dakle, A i B regularne matrice, a A^{-1} i B^{-1} njihovi inverzi. Onda zbog asocijativnosti množenja matrica imamo

$$(AB)(B^{-1}A^{-1}) = E \quad \text{i} \quad (B^{-1}A^{-1})(AB) = E\,,$$

što pokazuje da matrica AB ima inverz

$$(AB)^{-1} = B^{-1}A^{-1}\,.$$

Slično, iz

$$AA^{-1} = A^{-1}A = E$$

čitamo da je inverz A^{-1} regularne matrice A također invertibilan, i da je njegov inverz

$$(A^{-1})^{-1} = A.$$

Time je teorem dokazan. ■

Grupu regularnih matrica reda n nad poljem F standardno označavamo s

$$GL(n, F)$$

i zovemo je **opća linearna grupa** (matrica reda n nad poljem F).

Važnu podgrupu opće linearne grupe čine tzv. ortogonalne matrice. Za matricu $A \in M_n$ kažemo da je **ortogonalna** ako vrijedi

$$AA' = A'A = E\,.$$

Iz definicije je jasno da je svaka ortogonalna matrica A regularna i da je

$$A^{-1} = A' .$$

Ta relacija karakterizira ortogonalne matrice i često služi za njihovu alternativnu definiciju. Na primjer, matrica

$$A = \begin{bmatrix} 3/5 & 4/5 \\ -4/5 & 3/5 \end{bmatrix}$$

je ortogonalna jer imamo

$$AA' = \begin{bmatrix} 3/5 & 4/5 \\ -4/5 & 3/5 \end{bmatrix} \cdot \begin{bmatrix} 3/5 & -4/5 \\ 4/5 & 3/5 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = E ,$$

i slično, $A'A = E$. Isto tako je ortogonalna matrica i

$$A = \begin{bmatrix} \sin\alpha & \cos\alpha \\ \cos\alpha & -\sin\alpha \end{bmatrix} ,$$

za svaki $\alpha \in \mathbb{R}$.

TEOREM 2

Ortogonalne matrice reda n nad poljem F čine podgrupu od $GL(n, F)$.

Dokaz

Neka su A i B ortogonalne matrice, $A^{-1} = A'$, $B^{-1} = B'$. Treba vidjeti da je AB^{-1} također ortogonalna matrica. Imamo (vidi Zad. 6. u 9.4.)

$$\begin{aligned} (AB^{-1})^{-1} &= (B^{-1})^{-1}A^{-1} = BA' = (B')'A' = \\ &= (AB')' = (AB^{-1})' , \end{aligned}$$

što pokazuje da je AB^{-1} zaista ortogonalna. ■

Grupu ortogonalnih matrica označavamo s

$$O(n, F)$$

i nazivamo je **ortogonalna grupa** (matrica reda n nad poljem F).

Sljedeća propozicija govori o strukturi ortogonalne matrice.

PROPOZICIJA 3

Neka je $A = [\alpha_{ik}]$ ortogonalna matrica. Onda je za svaki $i, k = 1, \ldots, n$

$$\sum_{j=1}^{n} \alpha_{ij}\alpha_{kj} = \delta_{ik} , \qquad (1)$$

i također

$$\sum_{j=1}^{n} \alpha_{ji}\alpha_{jk} = \delta_{ik} \, . \tag{2}$$

Dokaz

Neposredno iz definicije ortogonalnosti. Kako je, naime,

$$A' = [\beta_{ik}] = [\alpha_{ki}] \, , \quad E = [\delta_{ik}] \quad i \quad AA' = E,$$

imamo

$$\delta_{ik} = \sum_{j=1}^{n} \alpha_{ij}\beta_{jk} = \sum_{j=1}^{n} \alpha_{ij}\alpha_{kj} \, ,$$

kako se i tvrdilo. Slično se iz relacije $A'A = E$ dokazuje druga tvrdnja. ■

Prema tome za $i = k$ imamo

$$\sum_{j=1}^{n} \alpha_{ij}^2 = 1 \, ,$$

tj. suma kvadrata elemenata nekog retka ortogonalne matrice jednaka je jedinici, a za $i \neq k$ imamo

$$\sum_{j=1}^{n} \alpha_{ij}\alpha_{kj} = 0 \, ,$$

tj. suma produkata korespondentnih elemenata (tzv. "skalarni produkt") dvaju različitih redaka jednaka je nuli. Zbog očigledne analogije s V^3, kažemo da redci u ortogonalnoj matrici čine **ortonormirani sustav**. Naravno, i stupci u ortogonalnoj matrici čine ortonormirani sustav. Zbog tog svojstva i imamo naziv ortogonalna matrica.

Odmah se vidi da vrijedi i ovaj obrat Prop. 3.

PROPOZICIJA 4

Neka je $A = [\alpha_{ik}]$ kvadratna matrica u kojoj i redci i stupci čine ortonormirani sustav. Onda je matrica A ortogonalna.

Dokaz

Neka je $A' = [\beta_{ik}] = [\alpha_{ki}]$ i $AA' = [\gamma_{ik}]$. Onda zbog (1) imamo redom

$$\gamma_{ik} = \sum_{j=1}^{n} \alpha_{ij}\beta_{jk} = \sum_{j=1}^{n} \alpha_{ij}\alpha_{kj} = \delta_{ik} \, ,$$

za svaki $i, k = 1, \ldots, n$, pa je

$$AA' = [\gamma_{ik}] = [\delta_{ik}] = E \ .$$

Slično iz (2) slijedi da je $A'A = E$ pa je matrica A ortogonalna po definiciji. ■

ZADACI

1. Dokaži: Matrica A je regularna onda i samo onda ako postoji matrica X takva da je $AX = E$. (Drugim riječima, $AX = E$ povlači $XA = E$, vidi 2.6.)

2. Provjeri da zbroj regularnih matrica nije općenito regularna matrica. Prema tome, $GL(n, F)$ ne dopušta bolju strukturu od grupe.

3. Dokaži: Uz definiciju $A^{-n} = (A^{-1})^n$ vrijedi $A^p A^q = A^{p+q}$ i $(A^p)^q = A^{pq}$, za svaku regularnu matricu A i svaki par **cijelih** brojeva $p, q \in \mathbb{Z}$ (vidi Zad. 4. u 9.4.).

4. Dokaži: Ako je matrica A regularna, onda su i A', $\overline{A}$ i A^* regularne. Nadalje je

   (a) $(A^{-1})' = (A')^{-1}$;

   (b) $\overline{(A^{-1})} = (\overline{A})^{-1}$;

   (c) $(A^{-1})^* = (A^*)^{-1}$.

5. Matrica A je ortogonalna ako i samo ako je $AA' = E$. Dokaži! Zaključi odatle da je za ortogonalnost matrice dovoljno provjeriti čine li bilo redci bilo stupci ortonormirani sustav.

6. Kažemo da je matrica A **involutorna** ako je $A^2 = E$. Ako neka matrica A posjeduje bilo koja dva od tri svojstva:

   (a) A je simetrična,

   (b) A je ortogonalna,

   (c) A je involutorna,

   onda nužno posjeduje i treće svojstvo. Dokaži!

7. Zbroj ortogonalnih matrica nije (nikada) ortogonalna matrica. Dokaži!

8. Kompleksna kvadratna matrica A je **unitarna** ako je

$$AA^* = A^*A = E\,.$$

Takva je matrica očito invertibilna i karakterizirana s $A^{-1} = A^*$. Na primjer,

$$\begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix} \quad \text{i} \quad \begin{bmatrix} e^{it} & 0 \\ 0 & e^{it} \end{bmatrix}$$

jesu unitarne matrice. Dokaži da unitarne matrice reda n čine multiplikativnu grupu, podgrupu od $GL(n, \mathbb{C})$. Ta se grupa označava s $U(n)$ i zove **unitarna grupa**.

9. Dokaži: Matrica $A = [\alpha_{ik}]$ je unitarna ako i samo ako je ispunjen bilo koji od ova dva uvjeta

(a) $\displaystyle\sum_{j=1}^{n} \alpha_{ij}\overline{\alpha_{kj}} = \delta_{ik}$;

(b) $\displaystyle\sum_{j=1}^{n} \alpha_{ji}\overline{\alpha_{jk}} = \delta_{ik}$,

za svaki $i, k = 1, \ldots, n$. To je tzv. **hermitska ortonormiranost** za retke, odnosno stupce.

10. Ako kompleksna matrica A posjeduje bilo koja dva od tri svojstva

(a) A je realna,

(b) A je ortogonalna,

(c) A je unitarna,

onda A nužno posjeduje i treće svojstvo. Dokaži!

11. Dijagonalna matrica je unitarna ako i samo ako je modul svakog njezina elementa na dijagonali jednak 1; dokaži!

12. Matrica A je **idempotentna** ako je $A^2 = A$. Idempotentna matrica je regularna ako i samo ako je jedinična. Pokaži da je

$$\begin{bmatrix} 25 & -20 \\ 30 & -24 \end{bmatrix}$$

idempotentna matrica (i prema tome singularna).

13. Neka su A i B matrice sa svojstvom $2A-B=E$. Dokaži da je matrica A idempotentna ako i samo ako je matrica B **involutorna**, tj. vrijedi $B^2=E$.

14. Dokaži: Inverz simetrične matrice je simetrična matrica. Isto vrijedi za antisimetrične, hermitske i antihermitske matrice.

15. Dokaži: Svaka antisimetrična matrica neparnog reda je singularna.

16. Neka su $A,B\in M_n$ kvadratne matrice istog reda. Kažemo da je matrica A **slična** matrici B, i pišemo $A\simeq B$, ako i samo ako postoji regularna matrica $T\in M_n$ tako da vrijedi $B=T^{-1}AT$. Za matricu T u tom slučaju kažemo da obavlja **konjugiranje** (ili **sprezanje**) **matrica** A i B. Dokaži da je sličnost matrica relacija ekvivalencije na skupu M_n.

17. Ako su $A,B\in M_n$, za matricu A kažemo da je **kongruentna** (ili sukladna) s matricom B, i pišemo $A\cong B$, ako postoji regularna matrica $T\in M_n$ takva da je $B=T'AT$. Pokaži da je kongruentnost matrica relacija ekvivalencije na skupu M_n. Povlači li kongruencija matrica nužno sličnost?

18. Ako su $A,B\in M_n$, za matricu A kažemo da je **ortogonalno kongruentna** s matricom B, i pišemo $A\overset{\cong}{o}B$, ako je matrica T iz Zad. 17. ortogonalna. Dokaži da je ortogonalna kongruentnost matrica relacija ekvivalencije na skupu M_n. Mogli bismo govoriti i o ortogonalnoj sličnosti. Zašto?

19. Ako su $A,B\in M_n(\mathbb{C})$ kompleksne matrice, kažemo da je A **hermitski kongruentna** s matricom B, i pišemo $A\overset{\cong}{h}B$, ako postoji regularna matrica $S\in M_n(\mathbb{C})$ takva da je $B=S^*AS$. Pokaži da je hermitska kongruencija relacija ekvivalencije na $M_n(\mathbb{C})$.

20. Ako su $A,B\in M_n(\mathbb{C})$, kažemo da je matrica A **unitarno kongruentna** s matricom B, i pišemo $A\overset{\cong}{u}B$, ako je matrica S iz Zad. 19. unitarna. Pokaži da je unitarna kongruencija relacija ekvivalencije na $M_n(\mathbb{C})$. Mogli bismo u tom slučaju govoriti i o unitarnoj sličnosti. Zašto?

9.6. Rang matrice

Svakoj se matrici

$$A = \begin{bmatrix} \alpha_{11} & \alpha_{12} & \cdots & \alpha_{1n} \\ \vdots & \vdots & & \vdots \\ \alpha_{m1} & \alpha_{m2} & \cdots & \alpha_{mn} \end{bmatrix} \tag{1}$$

može određenim postupkom pridružiti nenegativni cijeli broj, rang matrice, koji daje informaciju o stupnju "degeneriranosti" te matrice.

Promatrajmo linearni prostor

$$M_{m1} = \left\{ \begin{bmatrix} \alpha_1 \\ \vdots \\ \alpha_m \end{bmatrix} \mid \alpha_i \in F \right\}$$

svih stupčanih matrica s m redaka nad poljem F, očito izomorfan s F^m i dimenzije $\dim M_{m1} = m$. Vektore u tom prostoru kraće nazivamo **stupcima**. Neka je sada $A \in M_{mn}(F)$ bilo koja matrica, zapisana s (1). Uočimo stupčane matrice

$$S_k = \begin{bmatrix} \alpha_{1k} \\ \vdots \\ \alpha_{mk} \end{bmatrix}, \quad k = 1, \ldots, n,$$

određene stupcima matrice A. Tako dolazimo do pridruženja

$$A \mapsto (S_1, \ldots, S_n),$$

kojim se matrici A pridružuje jednoznačno određena n-torka stupaca iz M_{m1}. To je tzv. **stupčana reprezentacija** matrice A.

Kažemo da je za matricu A **rang po stupcima** $r(A)$ jednak r ako se maksimalni linearno nezavisni podskup u stupčanoj reprezentaciji

$$(S_1, \ldots, S_n) \subset M_{m1}$$

te matrice, sastoji od r vektora. Kratko (i neprecizno) bismo rekli da je rang po stupcima matrice jednak maksimalnom broju linearno nezavisnih stupaca te matrice. Očito je

$$r(A) = \dim [\{S_1, \ldots, S_n\}],$$

gdje je $[\{S_1, \ldots, S_n\}]$ potprostor od M_{m1}, razapet vektorima $S_1, \ldots, S_n$. Primijetimo da je za matricu A, koja je tipa (m, n), uvijek

$$r(A) \leq \min\{m, n\}.$$

Posve analogno, možemo promatrati prostor

$$M_{1n} = \{[\alpha_1 \ \dots \ \alpha_n] \mid \alpha_i \in F\} ,$$

dimenzije $\dim M_{1n} = n$, čije vektore obično zovemo **redci**. Ako uočimo vektore

$$R_i = [\alpha_{i1} \ \dots \ \alpha_{in}] , \quad i = 1, \dots, m ,$$

u tom prostoru, koji su određeni redcima naše matrice (1), dolazimo do pridruženja

$$A \mapsto (R_1, \dots, R_m) ,$$

koje zovemo **redčana reprezentacija** matrice A.

Kažemo da je za matricu A **rang po redcima** $r'(A)$ jednak r', ako se maksimalni linearno nezavisni podskup u redčanoj reprezentaciji

$$(R_1, \dots, R_m) \subset M_{1n}$$

te matrice sastoji od r' vektora. Očito je

$$r'(A) = \dim [\{R_1, \dots, R_m\}] ,$$

i nadalje, uvijek je

$$r'(A) \leq \min\{m, n\} .$$

Dakako, posebno bi nas veselilo da je rang matrice neovisan o tome računamo li ga u odnosu na stupce ili retke matrice. Pokazat ćemo da je to zaista točno. Vrijedi najprije

LEMA 1

Za svaku matricu A je

$$r'(A) \leq r(A) ,$$

tj. rang po redcima nije veći od ranga po stupcima.

Dokaz

Neka je A tipa (m, n) i neka je $r(A) = r$. Bez smanjenja općenitosti možemo pretpostaviti da upravo prvih r stupaca $(S_1, \dots, S_r)$ matrice A čini maksimalni linearno nezavisni skup. Tada za preostale stupce vrijedi

$$S_k = \sum_{j=1}^{r} \sigma_{jk} S_j , \tag{2}$$

za svaki $k = r+1, \ldots, n$, tj. na razini matričnih elemenata,

$$\alpha_{ik} = \sum_{j=1}^{r} \sigma_{jk}\alpha_{ij} \,, \tag{3}$$

za svaki $i = 1, \ldots, m,\ \ k = r+1, \ldots, n$.

Označimo s $\widehat{A}$ matricu koja se dobiva iz matrice A uklanjanjem njezinih stupaca $S_{r+1}, \ldots, S_n$. Neka je p maksimalni broj linearno nezavisnih redaka u $\widehat{A}$, $p = r'(\widehat{A})$. Kako je $\widehat{A}$ matrica tipa (m, r), očito je $p \leq r$. Bez smanjenja općenitosti, možemo pretpostaviti da u redčanoj reprezentaciji $(\widehat{R}_1, \ldots, \widehat{R}_m)$ matrice $\widehat{A}$ upravo prvih p redaka čini maksimalni linearno nezavisni skup. Zato je za svaki $i = p+1, \ldots, m$

$$\widehat{R}_i = \sum_{l=1}^{p} \tau_{li}\widehat{R}_l \,, \tag{4}$$

tj.

$$\alpha_{ik} = \sum_{l=1}^{p} \tau_{li}\alpha_{lk} \,, \tag{5}$$

za svaki $i = p+1, \ldots, m,\ \ k = 1, \ldots, r$.

Tvrdimo da i za korespondentne retke polazne matrice A vrijedi

$$R_i = \sum_{l=1}^{p} \tau_{li}R_l \,, \tag{6}$$

za $i = p+1, \ldots, m$. Ako to dokažemo, imali bismo zaključak da su svi redci matrice A linearne kombinacije njezinih prvih p redaka, a odatle da je

$$r'(A) \leq p \leq r = r(A) \,,$$

i lema bi bila dokazana.

Ostaje, dakle, dokazati matričnu jednakost (6) za svaki $i = p+1, \ldots, m$. No, ta se relacija može preko matričnih elemenata ekvivalentno zapisati kao

$$\alpha_{ik} = \sum_{l=1}^{p} \tau_{li}\alpha_{lk} \,, \tag{7}$$

za $i = p+1, \ldots, m,\ \ k = 1, \ldots, n$. Relacija (5) nam pokazuje da je (7) ispunjeno za svaki $k \leq r$. Ostaje vidjeti da je to istina i za $r+1 \leq k \leq n$. Zbog (3) i (5) za α_{ik}, $i = p+1, \ldots, m,\ \ k = r+1, \ldots, n$, dobivamo

$$\alpha_{ik} = \sum_{j=1}^{r} \sigma_{jk}\alpha_{ij} = \sum_{j=1}^{r} \sigma_{jk}\Big(\sum_{l=1}^{p} \tau_{li}\alpha_{lj}\Big) = \sum_{j=1}^{r}\sum_{l=1}^{p} \sigma_{jk}\tau_{li}\alpha_{lj} \,. \tag{8}$$

U drugu ruku, primjenom (3) na desnu stranu relacije (7) imamo redom

$$\sum_{l=1}^{p} \tau_{li}\alpha_{lk} = \sum_{l=1}^{p} \tau_{li}(\sum_{j=1}^{r} \sigma_{jk}\alpha_{lj}) = \sum_{j=1}^{r}\sum_{l=1}^{p} \sigma_{jk}\tau_{li}\alpha_{lj} \ . \tag{9}$$

Iz (8) i (9) slijedi (6) i tvrdnja je dokazana. ■

Odatle slijedi

TEOREM 2

Za svaku matricu A je rang po stupcima jednak rangu po redcima,

$$r(A) = r'(A) \ .$$

Dokaz

Neka je A' transponirana matrica matrice A. Onda je očito $r(A') = r'(A)$. Prema tome, iz Leme 1 imamo

$$r(A') \leq r(A) \ .$$

Ako tu istu lemu primijenimo na transponiranu matricu A', dobivamo

$$r(A) \leq r(A') \ ,$$

dakle

$$r'(A) = r(A') = r(A) \ ,$$

što se i tvrdilo. ■

Upravo dokazani teorem nam dopušta govoriti jednostavo o **rangu matrice**, i pisati $r(A)$, neovisno o tome kako smo taj rang računali.

Zapišimo odmah i ovu korisnu posljedicu teorema:

KOROLAR 3

Matrica i njoj transponirana matrica imaju isti rang, $r(A') = r(A)$. ■

Evo nekoliko primjera:

$$r\begin{bmatrix} 2 & 4 & 1 \\ 3 & 6 & 1 \end{bmatrix} = 2 \quad , \quad r\begin{bmatrix} 2 & 4 & 6 \\ 3 & 6 & 9 \end{bmatrix} = 1 \ .$$

Nadalje, svaka je nulmatrica ranga 0, i to su očito jedine matrice tog ranga. Jedinična matrica reda n je, dakako, ranga n.

Postavlja se problem efektivnog računanja ranga neke matrice. U tu svrhu uvodimo pojam **elementarnih transformacija nad matricom** A. Imamo tri tipa takvih transformacija:

I. Zamjena dvaju stupaca (redaka) matrice A;

II. Množenje nekog stupca (retka) matrice A skalarom različitim od nule;

III. Dodavanje nekog stupca (retka) matrice A nekom drugom stupcu (retku) te matrice.

Primijetimo da, s logičkog stajališta, te operacije nisu nezavisne. Lako se, naime, vidi da se operacija I. može realizirati iteracijom operacija II. i III. Međutim, za naše svrhe je prikladnije imati više takvih transformacija na raspolaganju.

Neka su $A, B \in M_{mn}$ dvije matrice istog tipa. Kažemo da je matrica A **ekvivalentna** matrici B, i pišemo

$$A \sim B\,,$$

ako postoji konačan niz matrica istog tipa

$$A = A_1, A_2, \ldots, A_{k-1}, A_k = B$$

sa svojstvom da se matrica A_i dobiva primjenom jedne od elementarnih transformacija I.–III. na matricu A_{i-1}, za svaki $i = 2, 3, \ldots, k$. Očito je da je $\sim$ jedna relacija ekvivalencije na skupu M_{mn}.

PROPOZICIJA 4

Ekvivalentne matrice imaju isti rang.

Dokaz

Očito je dovoljno provjeriti da se rang matrice ne mijenja pri elementarnim transformacijama. Nadalje, zbog Kor. 3 je jasno da je to dovoljno utvrditi za elementarne transformacije stupaca. Konačno, evidentno je da se rang matrice neće promijeniti ako na matricu primijenimo elementarnu transformaciju I. ili II. tipa. Ostaje, dakle, vidjeti da se rang matrice ne mijenja ni pri elementarnoj transformaciji tipa III., tj. dodavanjem nekog stupca matrice nekom drugom stupcu te matrice.

Neka je npr. matrica B dobivena iz matrice A dodavanjem drugog stupca matrice A njezinu prvom stupcu. Onda matrice A i B imaju stupčane reprezentacije

$$(S_1, S_2, \ldots, S_n)\,,$$

odnosno

$$(S_1 + S_2, S_2, \ldots, S_n)\,.$$

Promatrajmo potprostore

$$L = [(S_1, S_2, \ldots, S_n)] < M_{m1}$$

i

$$M = [(S_1 + S_2, S_2, \ldots, S_n)] < M_{m1} ,$$

razapete tim stupcima. Tvrdimo da je $L = M$. Ako to dokažemo, onda smo gotovi jer ćemo imati

$$r(A) = \dim L = \dim M = r(B) .$$

Neka je, dakle, $x \in L$. Onda je

$$\begin{aligned} x &= \alpha_1 S_1 + \alpha_2 S_2 + \cdots + \alpha_n S_n = \\ &= \alpha_1 S_1 + \alpha_1 S_2 - \alpha_1 S_2 + \alpha_2 S_2 + \cdots + \alpha_n S_n = \\ &= \alpha_1 (S_1 + S_2) + (\alpha_2 - \alpha_1) S_2 + \cdots + \alpha_n S_n , \end{aligned}$$

pa je $x \in M$ i $L \subset M$. Obratno, neka je $y \in M$, dakle

$$\begin{aligned} y &= \beta_1 (S_1 + S_2) + \beta_2 S_2 + \cdots + \beta_n S_n = \\ &= \beta_1 S_1 + (\beta_1 + \beta_2) S_2 + \cdots + \beta_n S_n , \end{aligned}$$

što pokazuje da je $y \in L$ i, prema tome, $M \subset L$. Zaista je, dakle, $L = M$ i tvrdnja je dokazana. ■

Problem određivanja ranga matrice se, dakle, svodi na transformaciju matrice u njoj ekvivalentnu matricu, kojoj je rang evidentan.

Neka je $r \leq m, n$ nenegativni cijeli broj, a $D_r = [\alpha_{ik}]$ matrica tipa (m, n), kojoj su elementi dani s

$$\alpha_{ik} = \begin{cases} 1, & i = k \leq r \\ 0, & \text{inače} \end{cases} ,$$

dakle oblika

$$D_r = \begin{bmatrix} 1 & 0 & \cdots & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & & \vdots \\ 0 & 0 & \cdots & 1 & \cdots & 0 \\ \vdots & \vdots & & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 & \cdots & 0 \end{bmatrix} .$$

Ta je matrica očito ranga r i nazivamo je **kanonska matrica ranga** r tipa (m, n). Odmah vidimo da je $D_0 = 0$.

TEOREM 5

Svaka je matrica ekvivalentna kanonskoj matrici D_r istog tipa, za neki r.

Dokaz

Neka je $A = [\alpha_{ik}]$ bilo koja matrica tipa (m, n). Ako je $\alpha_{ik} = 0$ za sve i i k, tj. ako je A nulmatrica, onda je $A = D_0$ i dokaz je gotov. Uzmimo zato da postoji $\alpha_{ik} \neq 0$. Primjenom transformacija I. tipa na stupce i retke, možemo postići da taj element bude u gornjem lijevom kutu, a primjenom II. transformacije možemo ga nadomjestiti jedinicom. Uzastopnom primjenom II. i III. transformacije imamo

$$A = \begin{bmatrix} \alpha_{11} & \alpha_{12} & \cdots & \alpha_{1n} \\ \alpha_{21} & \alpha_{22} & \cdots & \alpha_{2n} \\ \vdots & \vdots & & \vdots \\ \alpha_{m1} & \alpha_{m2} & \cdots & \alpha_{mn} \end{bmatrix} \sim \begin{bmatrix} 1 & \beta_{12} & \cdots & \beta_{1n} \\ \beta_{21} & \beta_{22} & \cdots & \beta_{2n} \\ \vdots & \vdots & & \vdots \\ \beta_{m1} & \beta_{m2} & \cdots & \beta_{mn} \end{bmatrix} \sim$$

$$\sim \begin{bmatrix} 1 & 0 & \cdots & 0 \\ 0 & \gamma_{22} & \cdots & \gamma_{2n} \\ \vdots & \vdots & & \vdots \\ 0 & \gamma_{m2} & \cdots & \gamma_{mn} \end{bmatrix} .$$

Ako je sada $\gamma_{ik} = 0$ za sve i i k, dobivamo $A \sim D_1$. Ako postoji bar jedan $\gamma_{ik} \neq 0$, elementarnim transformacijama I. tipa dovedemo ga na presjek drugog retka i stupca, transformacijom II. tipa zamijenimo ga jedinicom, a nakon toga uzastopnom primjenom transformacija II. i III. tipa postignemo da svi ostali elementi drugog retka i drugog stupca postanu nula. Postupak na isti način nastavimo i dalje. Nakon konačno koraka dolazimo do matrice

$$\begin{matrix} & & & \text{r} & \\ & \begin{bmatrix} 1 & \cdots & 0 & \cdots & 0 \\ \vdots & \ddots & \vdots & & \vdots \\ 0 & \cdots & 1 & \cdots & 0 \\ \vdots & & \vdots & & \vdots \\ 0 & \cdots & 0 & \cdots & 0 \end{bmatrix} & \end{matrix} \begin{matrix} \\ \\ r \\ \\ \\ \end{matrix} = D_r ,$$

i pritom je $A \sim D_r$, pa je teorem dokazan. ■

Na osnovi Prop. 4 i Tm. 5 onda imamo

KOROLAR 6

Matrica A je ranga r ako i samo ako je ekvivalentna s D_r.

Dokaz

Neka je A ranga r. Po Tm. 5 je $A \sim D_s$ za neki s, a po Prop. 4 je onda $s = r$. Obrat je očigledan. ■

Na taj način jednostavnim algoritmom, tj. svođenjem matrice na kanonsku matricu, možemo odrediti njezin rang. Primijetimo da rang, dakako, ne

ovisi o načinu svođenja na kanonski oblik.

Ilustrirajmo taj postupak na jednom primjeru. Imamo

$$A = \begin{bmatrix} 0 & 2 & 3 \\ 2 & 2 & 4 \end{bmatrix} \sim \begin{bmatrix} 2 & 2 & 4 \\ 0 & 2 & 3 \end{bmatrix} \sim \begin{bmatrix} 1 & 1 & 2 \\ 0 & 2 & 3 \end{bmatrix} \sim$$
$$\sim \begin{bmatrix} 1 & 0 & 0 \\ 0 & 2 & 3 \end{bmatrix} \sim \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 3/2 \end{bmatrix} \sim \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix},$$

pa je $r(A) = 2$.

Uočimo da rang **karakterizira** klase ekvivalentnih matrica. Naime imamo

KOROLAR 7

Dvije matrice istog tipa su ekvivalentne ako i samo ako imaju isti rang.

Dokaz

Neposredno iz Prop. 4 i Kor. 6. ■

Prema tome, u skupu M_{mn} ima točno $k+1$ klasa ekvivalencije, gdje je $k = \min\{m, n\}$, i pojedine su klase reprezentirane kanonskim matricama $D_0, D_1, \ldots, D_k$.

ZADACI

1. Uvjeri se da je stupčana reprezentacija matrice zapravo izomorfizam

$$M_{mn} \to \underbrace{M_{m1} \times \ldots \times M_{m1}}_{n}$$

linearnih prostora.

2. Neka je A matrica tipa (m, n), a $(R_1, \ldots, R_m)$ njezina redčana reprezentacija. Neka je, nadalje, B matrica tipa (n, p), a $(S_1, \ldots, S_p)$ njezina stupčana reprezentacija. Uvjeri se da je

$$AB = \begin{bmatrix} R_1 S_1 & \cdots & R_1 S_p \\ \vdots & & \vdots \\ R_m S_1 & \cdots & R_m S_p \end{bmatrix},$$

gdje je s $R_i\ S_k$ označen "skalarni produkt".

3. Neka je

$$A : D_{mn} \to F$$

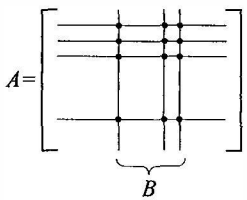
dana matrica, a

$$\begin{aligned} D_{pq} &= \{i_1, \ldots, i_p\} \times \{j_1, \ldots, j_q\} \subset \\ &\subset \{1, \ldots, m\} \times \{1, \ldots, n\} = D_{mn} \end{aligned}$$

podskup od D_{mn}. Onda se matrica

$$B = A/D_{pq} : D_{pq} \to F$$

zove **submatrica** ili **podmatrica** od A, tipa (p, q). Ona se, dakako, dobiva uklanjanjem $m - p$ redaka i $n - q$ stupaca iz matrice A. Nađi koliko A ima submatrica tipa (p, q), za svaki $p \leq m$, $q \leq n$. Pokaži da



rang matrice B nije veći od ranga matrice A.

4. Neka su $E_1(i, j)$, $E_2(i, \lambda)$ i $E_3(i, j)$ matrice koje se dobivaju primjenom elementarnih transformacija tipa I., II. odnosno III. na stupce jedinične matrice E reda n. Na primjer, za $n = 2$ je

$$E_1(1,2) = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad E_2(1,5) = \begin{bmatrix} 5 & 0 \\ 0 & 1 \end{bmatrix}, \quad E_3(1,2) = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}.$$

Slično se definiraju matrice oblika E^1, E^2, E^3, koje se dobivaju primjenom elementarnih transformacija na retke jedinične matrice E reda m. Matrice oblika E_i i E^j zovu se **elementarne matrice**. Pokaži da su regularne, i da su njihovi inverzi također elementarne matrice.

5. Ako je A matrica tipa (m, n), onda su AE_1, AE_2, AE_3 redom matrice koje se dobivaju iz A primjenom I.–III. elementarne transformacije na stupce. Isto tako su E^1A, E^2A i E^3A matrice, koje se iz A dobivaju primjenom tih transformacija na retke. Prema tome (Tm. 5), za matricu A ranga r možemo pisati

$$PAQ = D_r \,,$$

gdje je P produkt matrica tipa E^j, a Q produkt matrica tipa E_i (P i Q su regularne!). Dokaži!

6. Ako su A i B ekvivalentne matrice, onda postoje regularne matrice S i T takve da je $B = SAT$. Dokaži!

7. Kvadratna matrica je regularna onda i samo onda ako je ekvivalentna jediničnoj matrici, tj. onda i samo onda ako je maksimalnog ranga. Dokaži!

8. Dokaži: Svaka se regularna matrica može prikazati kao produkt elementarnih matrica. Vrijedi dakako i obrat.

9. Matrica neće promijeniti svoj rang pomnožimo li je regularnom matricom (bilo slijeva ili zdesna). Dokaži!

10. Iz Zad. 6. i Zad. 9. zaključi da vrijedi ovaj teorem: Matrice A i B su ekvivalentne onda i samo onda ako postoje regularne matrice S i T takve da je $B = SAT$.

11. Uvjeri se da matrice $\overline{A}$ i A^* imaju isti rang kao kompleksna matrica A.

12. Slične matrice, kongruentne matrice i hermitski kongruentne matrice (vidi Zad. 16., 17. i 19. u točki 9.5.) imaju isti rang. Dokaži!

9.7. Pojam determinante. Osnovna svojstva

Već smo uzgred spominjali determinante drugog i trećeg reda. Sada ćemo ih definirati i izučavati u svoj njihovoj općenitosti. Povijesno gledano, determinante su u algebru uvedene najprije kao prikladno sredstvo u rješavanju sustava linearnih jednadžbi. Kasnije je njihova teorija razvijena i neovisno o tom pristupu. Danas one igraju važnu ulogu u raznim poglavljima linearne algebre, pa tako i u teoriji matrica. Pomoću determinanata možemo dobiti izvjesnu informaciju o danoj matrici, posebno o njezinu rangu. Napose, pomoću njih dobivamo jednostavan kriterij za prepoznavanje regularnih matrica.

Neka je p bilo koja permutacija skupa $\{1, \ldots, n\}$ (vidi točku 2.9.),

$$p = \begin{pmatrix} 1 & 2 & \cdots & n \\ p(1) & p(2) & \cdots & p(n) \end{pmatrix} ,$$

a $I(p)$ broj inverzija u toj permutaciji. Kako smo rekli, ta je permutacija parna, odnosno neparna, već prema tome je li $\operatorname{sign}(p) = (-1)^{I(p)}$ jednak 1 ili -1. Vidjeli smo također (Prop. 3 u 2.9.), da je inverzna permutacija p^{-1} iste parnosti kao i permutacija p, tj.

$$\operatorname{sign}(p^{-1}) = \operatorname{sign}(p) .$$

Neka je M_n prostor svih kvadratnih matrica reda n nad poljem F. Onda definiramo funkcional

$$\det : M_n \to F \ ,$$

stavljajući za svaku matricu $A \in M_n$, $A = [\alpha_{ik}]$,

$$\det A = \sum_{p \in S_n} (-1)^{I(p)} \alpha_{1p(1)} \alpha_{2p(2)} \cdots \alpha_{np(n)} \ ,$$

gdje se sumira po svim permutacijama skupa $\{1, \ldots, n\}$, tj. po svim elementima simetrične grupe S_n, njih $n!$. Funkcional det nazivamo **determinantna funkcija**, a njezinu vrijednost,

$$\det A \in F \ ,$$

na matrici A nazivamo **determinanta matrice** A.

Kako razabiremo iz definicijske formule, svaki je sumand u $\det A$, tzv. **osnovni sumand**, oblika

$$(-1)^{I(p)} \alpha_{1p(1)} \cdots \alpha_{np(n)} \ ,$$

tj. dobiva se kao produkt od n elemenata matrice A, od kojih nikoja dva nisu ni iz istog retka ni iz istog stupca, zajedno s predznakom $+$ ili $-$, već prema tome je li permutacija p drugih indeksa elemenata parna ili neparna.

Za determinantu matrice A još su uobičajene oznake

$$\det A = |A| = |\alpha_{ik}|$$

ili, ako je važno elemente matrice A imati eksplicitno,

$$\det A = \begin{vmatrix} \alpha_{11} & \alpha_{12} & \cdots & \alpha_{1n} \\ \alpha_{21} & \alpha_{22} & \cdots & \alpha_{2n} \\ \vdots & \vdots & & \vdots \\ \alpha_{n1} & \alpha_{n2} & \cdots & \alpha_{nn} \end{vmatrix} \ .$$

U ovoj notaciji red determinante, njezine elemente, retke, stupce, glavnu i sporednu dijagonalu definiramo posve analogno kao i u pripadnoj matrici.

Imamo tako, za $n = 1$,

$$|\alpha| = \alpha \ ,$$

tj. determinanta matrice prvog reda je jednaka svom jedinom elementu. Za $n = 2$ je

$$\begin{vmatrix} \alpha_{11} & \alpha_{12} \\ \alpha_{21} & \alpha_{22} \end{vmatrix} = (-1)^0 \alpha_{11}\alpha_{22} + (-1)^1 \alpha_{12}\alpha_{21} = \\ = \alpha_{11}\alpha_{22} - \alpha_{12}\alpha_{21} \ ,$$

tj. determinanta drugog reda jednaka je razlici produkata elemenata na

glavnoj i sporednoj dijagonali. Za $n = 3$ dobivamo

$$\begin{vmatrix} \alpha_{11} & \alpha_{12} & \alpha_{13} \\ \alpha_{21} & \alpha_{22} & \alpha_{23} \\ \alpha_{31} & \alpha_{32} & \alpha_{33} \end{vmatrix} = (-1)^0\alpha_{11}\alpha_{22}\alpha_{33} + (-1)^1\alpha_{11}\alpha_{23}\alpha_{32} +$$

$$+(-1)^1\alpha_{12}\alpha_{21}\alpha_{33} + (-1)^2\alpha_{12}\alpha_{23}\alpha_{31} +$$

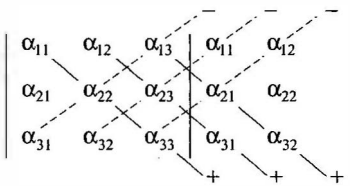
$$+(-1)^2\alpha_{13}\alpha_{21}\alpha_{32} + (-1)^3\alpha_{13}\alpha_{22}\alpha_{31} =$$

$$= \alpha_{11}\alpha_{22}\alpha_{33} + \alpha_{12}\alpha_{23}\alpha_{31} + \alpha_{13}\alpha_{21}\alpha_{32} -$$

$$-\alpha_{11}\alpha_{23}\alpha_{32} - \alpha_{12}\alpha_{21}\alpha_{33} - alpha_{13}\alpha_{22}\alpha_{31} \ .$$

Zakon računanja determinante trećeg reda lako se pamti primjenom tzv. **Sarrusova pravila**:

Determinanti dopišemo zdesna prva dva njezina stupca, pa onda zbrojimo produkte elemenata na glavnoj dijagonali i njoj paralelnim pravcima (puna crta) i od toga oduzmemo produkte elemenata na sporednoj dijagonali i njoj paralelnim pravcima (crtkano).
Po tom pravilu imamo

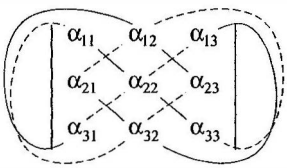


$$= \alpha_{11}\alpha_{22}\alpha_{33} + \alpha_{12}\alpha_{23}\alpha_{31} + \alpha_{13}\alpha_{21}\alpha_{32} -$$

$$-\alpha_{13}\alpha_{22}\alpha_{31} - \alpha_{11}\alpha_{23}\alpha_{32} - \alpha_{12}\alpha_{21}\alpha_{33} \ .$$

Uspoređivanjem s prethodnim računom odmah razabiremo da se tim algoritmom dobiva ispravan rezultat. Analogno pravilo dobivamo ako ispod determinante pripišemo njezina prva dva retka.

Konačno, ispravan rezultat dobivamo i ako determinantu računamo po shemi



gdje najprije zbrojimo produkte elemenata spojene punom crtom, a zatim oduzmemo produkte elemenata spojenih crtkano, dakle

$$\alpha_{11}\alpha_{22}\alpha_{33} + \alpha_{12}\alpha_{23}\alpha_{31} + \alpha_{21}\alpha_{32}\alpha_{13} -$$

$$- \alpha_{13}\alpha_{22}\alpha_{31} - \alpha_{12}\alpha_{21}\alpha_{33} - \alpha_{23}\alpha_{32}\alpha_{11} \ .$$

Po tom je pravilu npr.

$$\begin{vmatrix} 7 & 4 & 1 \\ 3 & 1 & 2 \\ 4 & 1 & 1 \end{vmatrix} = 7 + 32 + 3 - 4 - 12 - 14 = 12 \ .$$

Kod determinanata višeg reda nastupaju poteškoće pri njihovu efektivnom računanju. Naime, iako je teorijski moguće izračunati svaku determinantu služeći se njezinom definicijom, to je često u praksi nemoguće, jer broj osnovnih sumanada raste astronomski s redom determinante. Tako npr. determinanta desetog reda ima $10! \doteq 3{,}6$ milijuna osnovnih sumanada, pa bi samo za popisivanje tih sumanada trebalo 36 knjiga, s 1000 stranica svaka. Tu, dakako, danas pomažu računala, ali se račun može znatno pojednostavniti koriste li se neka svojstva determinanata.

Navest ćemo sada osnovna svojstva determinanata.

PROPOZICIJA 1

Za bilo koju matricu $A \in M_n$, $A = [\alpha_{ik}]$, također je

$$\det A = \sum_{q \in S_n} (-1)^{I(q)} \alpha_{q(1)1} \alpha_{q(2)2} \cdots \alpha_{q(n)n} \ ,$$

tj. determinanta je jednaka sumi osnovnih sumanada, kojima su faktori svrstani po prirodnom poretku indeksa stupaca.

Dokaz

Tvrdnja izlazi iz komutativnosti množenja u polju, iz činjenice da je

$$\alpha_{q(1)1} \cdots \alpha_{q(n)n} = \alpha_{1q^{-1}(1)} \cdots \alpha_{nq^{-1}(n)}$$

i da su permutacija q i njoj inverzna permutacija q^{-1} iste parnosti. ■

KOROLAR 2

Neka je A' transponirana matrica matrice A. Onda je

$$\det A' = \det A \ .$$ ■

Odatle slijedi da će svi zaključci u vezi s redcima determinante vrijediti i za njezine stupce, i obratno.

PROPOZICIJA 3

Ako je matrica B dobivena iz matrice A zamjenom dvaju njezinih susjednih redaka (stupaca), onda je

$$\det B = -\det A \ .$$

Dokaz

Neposredno iz činjenice da zamjenom dvaju susjeda permutacija mijenja parnost. ■

KOROLAR 4

Ako je matrica B dobivena iz matrice A zamjenom bilo koja dva njezina retka (stupca), onda je

$$\det B = -\det A\,.$$

Dokaz

Ta se zamjena može realizirati neparnim brojem sukcesivnih zamjena susjednih redaka, pa tvrdnja izlazi iz Prop. 3. ■

Prema tome, elementarnom transformacijom tipa I. determinanta matrice mijenja predznak.

KOROLAR 5

Ako matrica A ima dva jednaka retka (stupca), onda je

$$\det A = 0\,.$$

Dokaz

Neposredno iz Kor. 4. Imamo, naime, $\det A = -\det A$, pa je $\det A = 0$. (U slučaju kad je F polje karakteristike 2, to zaključivanje nije točno, ali je tvrdnja ipak istinita.) ■

PROPOZICIJA 6

Ako je matrica B dobivena iz matrice A množenjem jednog njezina retka (stupca) skalarom $\lambda \in F$, onda je

$$\det B = \lambda \det A\,.$$

Dokaz

Neposredno iz definicije determinante. ■

Prema tome, primjenom elementarne transformacije tipa II. na matricu, njezina se determinanta promijeni za faktor λ.

KOROLAR 7

Ako matrica A ima dva proporcionalna retka (stupca), onda je

$$\det A = 0\,.$$

Dokaz

Neposredno iz Prop. 6 i Kor. 5. ■

KOROLAR 8

Za matricu A reda n i bilo koji skalar $\lambda \in F$ je

$$\det(\lambda A) = \lambda^n \det A \,.$$ ■

PROPOZICIJA 9

Neka su $A = [\alpha_{ik}]$, $B = [\beta_{ik}]$ i $C = [\gamma_{ik}]$ matrice istog reda n, sa svojstvom

$$\gamma_{ik} = \begin{cases} \alpha_{ik} + \beta_{ik}, & i = s \\ \alpha_{ik} = \beta_{ik}, & i \neq s \end{cases},$$

za odabrani $s \leq n$ i za sve k. Onda je

$$\det C = \det A + \det B \,.$$

Isto vrijedi i za dani stupac.

Dokaz

$$\begin{aligned} \det C &= \sum_{p \in S_n} (-1)^{I(p)} \gamma_{1p(1)} \cdots \gamma_{sp(s)} \cdots \gamma_{np(n)} = \\ &= \sum_{p \in S_n} (-1)^{I(p)} \alpha_{1p(1)} \cdots (\alpha_{sp(s)} + \beta_{sp(s)}) \cdots \alpha_{np(n)} = \\ &= \sum_{p \in S_n} (-1)^{I(p)} \alpha_{1p(1)} \cdots \alpha_{sp(s)} \cdots \alpha_{np(n)} + \\ &\quad + \sum_{p \in S_n} (-1)^{I(p)} \alpha_{1p(1)} \cdots \beta_{sp(s)} \cdots \alpha_{np(n)} = \\ &= \sum_{p \in S_n} (-1)^{I(p)} \alpha_{1p(1)} \cdots \alpha_{np(n)} + \\ &\quad + \sum_{p \in S_n} (-1)^{I(p)} \beta_{1p(1)} \cdots \beta_{np(n)} = \det A + \det B \,. \end{aligned}$$ ■

Imamo npr.

$$\begin{vmatrix} \alpha_1 + \alpha_2 & \beta_1 + \beta_2 \\ \gamma & \delta \end{vmatrix} = \begin{vmatrix} \alpha_1 & \beta_1 \\ \gamma & \delta \end{vmatrix} + \begin{vmatrix} \alpha_2 & \beta_2 \\ \gamma & \delta \end{vmatrix} .$$

Razabiremo da je općenito

$$\det(A+B) \neq \det A + \det B\ ,$$

ali se $\det(A+B)$ (Prop. 9) može uvijek razviti u sumu od 2^n determinanata koje za retke (stupce) imaju retke (stupce) matrica A odnosno B.

KOROLAR 10

Ako je matrica B dobivena iz matrice A dodavanjem nekog njezina retka (stupca) nekom drugom njezinu retku (stupcu), onda je

$$\det B = \det A\ .$$

Dokaz

Neposredno iz Prop. 9 i Kor. 5. ■

Odatle slijedi da se primjenom elementarne transformacije tipa III. na matricu njezina determinanta ne mijenja.

Malo uopćenije imamo

KOROLAR 11

Ako nekom retku (stupcu) matrice dodamo linearnu kombinaciju ostalih redaka (stupaca), njezina se determinanta ne mijenja. Ako je neki redak (stupac) matrice linearna kombinacija ostalih redaka (stupaca), determinanta te matrice jednaka je nuli. ■

ZADACI

1. Dokaži: Ako se u matrici A jedan redak (stupac) sastoji iz samih nula, onda je $\det A = 0$. Specijalno, nulmatrica ima determinantu jednaku nuli.

2. Dokaži: Za jediničnu matricu E je $\det E = 1$. Nadalje, ako je matrica $A = [\alpha_{ik}] \in M_n$

   (a) dijagonalna (vidi Zad. 11. u 9.4.), onda je $\det A = \prod_{i=1}^{n} \alpha_{ii}$;

   (b) skalarna (vidi Zad. 13. u 9.4.), onda je $\det A = \alpha^n$;

   (c) gornja (donja) trokutasta matrica (vidi Zad. 15. u 9.4.), onda je $\det A = \prod_{i=1}^{n} \alpha_{ii}$.

3. Dokaži da je

$$\begin{vmatrix} 1 & \cos\alpha & \cos\beta \\ \cos\alpha & 1 & \cos\gamma \\ \cos\beta & \cos\gamma & 1 \end{vmatrix} = \begin{vmatrix} 0 & \cos\alpha & \cos\beta \\ \cos\alpha & 0 & \cos\gamma \\ \cos\beta & \cos\gamma & 0 \end{vmatrix}$$

ako i samo ako su $\cos\alpha$, $\cos\beta$ i $\cos\gamma$ kosinusi smjera nekog vektora iz V^3.

4. Determinantu oblika

$$V_n(x_1,\ldots,x_n)=\begin{vmatrix} 1 & 1 & \cdots & 1 \\ x_1 & x_2 & \cdots & x_n \\ x_1^2 & x_2^2 & \cdots & x_n^2 \\ \vdots & \vdots & & \vdots \\ x_1^{n-1} & x_2^{n-1} & \cdots & x_n^{n-1} \end{vmatrix}$$

nazivamo **Vandermondeova determinanta** reda n. Dokaži da je

$$V_n(x_1,\ldots,x_n)=\prod_{i>j}(x_i-x_j)\,.$$

Prema tome, ako su $x_1,\ldots,x_n$ međusobno različiti skalari, onda je

$$V_n(x_1,\ldots,x_n)\neq 0\,.$$

5. Neka je $d: M_n \to F$ bilo koja funkcija koja zadovoljava ove aksiome

   (1) d je linearna na stupcima matrice A;

   (2) $d(A)=0$ ako A ima dva jednaka stupca;

   (3) $d(E)=1$ za jediničnu matricu E.

   Dokaži da je onda nužno $d=\det$, tj. da je d jednaka determinantnoj funkciji. To je alternativni, aksiomatski pristup pojmu determinante.

9.8. Binet-Cauchyjev teorem

Iz do sada navedenih svojstava determinanata (Kor. 8 i Prop. 9 u 9.7.) vidi se da determinantna funkcija

$$\det: M_n \to F$$

ne poštuje linearnu strukturu prostora, tj. da **nije linearni funkcional** na M_n. Međutim, taj se funkcional dobro ponaša u odnosu na množenje matrica. Imamo, naime, ovaj poznati

TEOREM 1 (Binet-Cauchy)
Funkcional

$$\det: M_n \to F$$

je homomorfizam multiplikativnih monoida, tj. za svaki par matrica $A, B \in M_n$ *vrijedi*

$$\det AB = \det A \det B\,.$$

Dokaz

Tvrdnja slijedi uzastopnom primjenom Prop. 9, Prop. 6, Kor. 5 i Kor. 4 iz 9.7. Ilustrirajmo to najprije na primjeru kad su matrice $A = [\alpha_{ik}]$ i $B = [\beta_{ik}]$ drugog reda. Imamo

$$\begin{aligned}
\det AB &= \det\left(\begin{bmatrix} \alpha_{11} & \alpha_{12} \\ \alpha_{21} & \alpha_{22} \end{bmatrix} \cdot \begin{bmatrix} \beta_{11} & \beta_{12} \\ \beta_{21} & \beta_{22} \end{bmatrix}\right) = \\
&= \det \begin{bmatrix} \alpha_{11}\beta_{11} + \alpha_{12}\beta_{21} & \alpha_{11}\beta_{12} + \alpha_{12}\beta_{22} \\ \alpha_{21}\beta_{11} + \alpha_{22}\beta_{21} & \alpha_{21}\beta_{12} + \alpha_{22}\beta_{22} \end{bmatrix} = \\
&= \det \begin{bmatrix} \alpha_{11}\beta_{11} & \alpha_{11}\beta_{12} \\ \alpha_{21}\beta_{11} & \alpha_{21}\beta_{12} \end{bmatrix} + \det \begin{bmatrix} \alpha_{11}\beta_{11} & \alpha_{12}\beta_{22} \\ \alpha_{21}\beta_{11} & \alpha_{22}\beta_{22} \end{bmatrix} + \\
&\quad + \det \begin{bmatrix} \alpha_{12}\beta_{21} & \alpha_{11}\beta_{12} \\ \alpha_{22}\beta_{21} & \alpha_{21}\beta_{12} \end{bmatrix} + \det \begin{bmatrix} \alpha_{12}\beta_{21} & \alpha_{12}\beta_{22} \\ \alpha_{22}\beta_{21} & \alpha_{22}\beta_{22} \end{bmatrix} = \\
&= \beta_{11}\beta_{12} \det \begin{bmatrix} \alpha_{11} & \alpha_{11} \\ \alpha_{21} & \alpha_{21} \end{bmatrix} + \beta_{11}\beta_{22} \det \begin{bmatrix} \alpha_{11} & \alpha_{12} \\ \alpha_{21} & \alpha_{22} \end{bmatrix} + \\
&\quad + \beta_{21}\beta_{12} \det \begin{bmatrix} \alpha_{12} & \alpha_{11} \\ \alpha_{22} & \alpha_{21} \end{bmatrix} + \beta_{21}\beta_{22} \det \begin{bmatrix} \alpha_{12} & \alpha_{12} \\ \alpha_{22} & \alpha_{22} \end{bmatrix} = \\
&= \det \begin{bmatrix} \alpha_{11} & \alpha_{12} \\ \alpha_{21} & \alpha_{22} \end{bmatrix} (\beta_{11}\beta_{22} - \beta_{12}\beta_{21}) = \\
&= \det \begin{bmatrix} \alpha_{11} & \alpha_{12} \\ \alpha_{21} & \alpha_{22} \end{bmatrix} \cdot \det \begin{bmatrix} \beta_{11} & \beta_{12} \\ \beta_{21} & \beta_{22} \end{bmatrix} = \det A \cdot \det B.
\end{aligned}$$

Posve analogno teče dokaz i u općem slučaju:

$$\begin{aligned}
\det AB &= \det\left(\begin{bmatrix} \alpha_{11} & \cdots & \alpha_{1n} \\ \vdots & & \vdots \\ \alpha_{n1} & \cdots & \alpha_{nn} \end{bmatrix} \cdot \begin{bmatrix} \beta_{11} & \cdots & \beta_{1n} \\ \vdots & & \vdots \\ \beta_{n1} & \cdots & \beta_{nn} \end{bmatrix}\right) = \\
&= \begin{vmatrix} \sum_{j_1} \alpha_{1j_1}\beta_{j_1 1} & \sum_{j_2} \alpha_{1j_2}\beta_{j_2 2} & \cdots & \sum_{j_n} \alpha_{1j_n}\beta_{j_n n} \\ \vdots & \vdots & & \vdots \\ \sum_{j_1} \alpha_{nj_1}\beta_{j_1 1} & \sum_{j_2} \alpha_{nj_2}\beta_{j_2 2} & \cdots & \sum_{j_n} \alpha_{nj_n}\beta_{j_n n} \end{vmatrix} = \\
&= \text{(primjena Prop. 9 na prvi stupac)} =
\end{aligned}$$

$$= \sum_{j_1=1}^{n} \begin{vmatrix} \alpha_{1j_1}\beta_{j_1 1} & \sum_{j_2} \alpha_{1j_2}\beta_{j_2 2} & \cdots & \sum_{j_n} \alpha_{1j_n}\beta_{j_n n} \\ \vdots & \vdots & & \vdots \\ \alpha_{nj_1}\beta_{j_1 1} & \sum_{j_2} \alpha_{nj_2}\beta_{j_2 2} & \cdots & \sum_{j_n} \alpha_{nj_n}\beta_{j_n n} \end{vmatrix} =$$

$=$ (na drugi stupac) $=$

$$= \sum_{j_1=1}^{n}\sum_{j_2=1}^{n} \begin{vmatrix} \alpha_{1j_1}\beta_{j_1 1} & \alpha_{1j_2}\beta_{j_2 2} & \cdots & \sum_{j_n} \alpha_{1j_n}\beta_{j_n n} \\ \vdots & \vdots & & \vdots \\ \alpha_{nj_1}\beta_{j_1 1} & \alpha_{nj_2}\beta_{j_2 2} & \cdots & \sum_{j_n} \alpha_{nj_n}\beta_{j_n n} \end{vmatrix} =$$

$=$ (analogno na ostale stupce, pa imamo n suma) $=$

$$= \sum_{j_1,\ldots,j_n=1}^{n} \begin{vmatrix} \alpha_{1j_1}\beta_{j_1 1} & \alpha_{1j_2}\beta_{j_2 2} & \cdots & \alpha_{1j_n}\beta_{j_n n} \\ \vdots & \vdots & & \vdots \\ \alpha_{nj_1}\beta_{j_1 1} & \alpha_{nj_2}\beta_{j_2 2} & \cdots & \alpha_{nj_n}\beta_{j_n n} \end{vmatrix} =$$

$=$ (primjena Prop. 6 i Kor. 5, pa ostaje suma po svim permutacijama skupa $\{1,\ldots,n\}$) $=$

$$= \sum_{j_1\neq j_2\neq\ldots\neq j_n} \begin{vmatrix} \alpha_{1j_1} & \cdots & \alpha_{1j_n} \\ \vdots & & \vdots \\ \alpha_{nj_1} & \cdots & \alpha_{nj_n} \end{vmatrix} \cdot \beta_{j_1 1}\cdots\beta_{j_n n} =$$

$=$ (Kor. 4) $=$

$$= \sum_{j_1\neq\ldots\neq j_n} (-1)^{I(j_1,\ldots,j_n)} \begin{vmatrix} \alpha_{11} & \cdots & \alpha_{1n} \\ \vdots & & \vdots \\ \alpha_{n1} & \cdots & \alpha_{nn} \end{vmatrix} \cdot \beta_{j_1 1}\cdots\beta_{j_n n} =$$

$$= \begin{vmatrix} \alpha_{11} & \cdots & \alpha_{1n} \\ \vdots & & \vdots \\ \alpha_{n1} & \cdots & \alpha_{nn} \end{vmatrix} \cdot \sum_{j_1\neq\ldots\neq j_n} (-1)^{I(j_1,\ldots,j_n)} \beta_{j_1 1}\cdots\beta_{j_n n} =$$

$=$ (Prop. 1) $=$

$$= \begin{vmatrix} \alpha_{11} & \cdots & \alpha_{1n} \\ \vdots & & \vdots \\ \alpha_{n1} & \cdots & \alpha_{nn} \end{vmatrix} \cdot \begin{vmatrix} \beta_{11} & \cdots & \beta_{1n} \\ \vdots & & \vdots \\ \beta_{n1} & \cdots & \beta_{nn} \end{vmatrix} = \det A \cdot \det B$$

i teorem je dokazan. ■

Kako znamo, matrice općenito ne komutiraju. Vrijedi međutim

KOROLAR 2

Za bilo koje matrice A i B istog reda je

$$\det BA = \det AB \,.$$

Dokaz

Neposredno iz Tm. 1. ■

Kako smo rekli, matrica A je ortogonalna ako je $AA' = E$.

PROPOZICIJA 3

Ako je matrica A ortogonalna, onda je

$$\det A = \pm 1 \,.$$

Dokaz

Iz $AA' = E$ slijedi $\det(AA') = \det E$, pa je, po Tm. 1,

$$\det A \det A' = 1 \,,$$

a jer je $\det A' = \det A$, to je $(\det A)^2 = 1$, dakle, $\det A = \pm 1$. ■

Obrat međutim nije istinit. Na primjer, za matricu

$$A = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix}$$

je $\det A = 1$, a matrica A nije ortogonalna jer je npr. za prvi redak $1^2 + 1^2 = 2 \neq 1$ (vidi Prop. 3 u 9.5.).

ZADACI

1. Funkcional $\det : M_n \to F$ doduše nije linearan, ali je multilinearan na stupcima (redcima) matrica. Točnije, ako identificiramo $M_n = \underbrace{M_{n1} \times \cdots \times M_{n1}}_{n}$, imamo $A = (S_1, \ldots, S_n)$, gdje su S_i stupci matrice A. Onda za svaki $i = 1, \ldots, n$ vrijedi

$$\begin{aligned} &\det(S_1, \ldots, \alpha S_i + \alpha' S_i', \ldots, S_n) = \\ &\quad = \alpha \det(S_1, \ldots, S_i, \ldots, S_n) + \alpha' \det(S_1, \ldots, S_i', \ldots, S_n) \,. \end{aligned}$$

Dokaži!

2. Ako je matrica A unitarna, onda je

$$\det A \cdot \overline{\det A} = 1 ,$$

tj. modul determinante te matrice jednak je jedinici. Dokaži!

3. Dokaži neposredno Binet-Cauchyjev teorem za elementarne matrice, pa onda, koristeći se tom činjenicom, dokaži Binet-Cauchyjev teorem u općem slučaju.

4. Kako su determinante $|\alpha_{ik}|, |\beta_{ik}| \in F$ skalari, njihov se produkt može definirati, jer je to potpuno određeni skalar $|\alpha_{ik}| \cdot |\beta_{ik}|$ iz polja F. Katkad je, međutim, prikladno da produkt determinanata bude prikazan u obliku determinante. Dokaži da za determinante istog reda vrijedi

$$|\alpha_{ik}| \cdot |\beta_{ik}| = |\gamma_{ik}| ,$$

gdje se elementi γ_{ik} mogu računati na bilo koji od ova četiri načina:

(a) $\gamma_{ik} = \sum_j \alpha_{ij}\beta_{jk}$, tj. "skalarnim množenjem" redaka sa stupcima;

(b) $\gamma_{ik} = \sum_j \alpha_{ij}\beta_{kj}$, tj. "skalarnim množenjem" redaka s redcima;

(c) $\gamma_{ik} = \sum_j \alpha_{ji}\beta_{jk}$, tj. "skalarnim množenjem" stupaca sa stupcima;

(d) $\gamma_{ik} = \sum_j \alpha_{ji}\beta_{kj}$, tj. "skalarnim množenjem" stupaca s redcima.

Specijalno, dakle, determinante možemo množiti po istom zakonu kao i matrice.

5. Neka je $\Delta : M_n \to F$ preslikavanje sa svojstvima

(a) $\Delta(AB) = \Delta(A)\Delta(B)$,

(b) $\Delta(\lambda E) = \lambda^n$.

Pokaži da je nužno $\Delta = \det$. To je daljnja karakterizacija determinante.

6. Dokaži ovu generalizaciju Binet-Cauchyjeva teorema: Neka je A matrica tipa (m, n), a B matrica tipa (n, m). Onda je:

(a) uz $m > n$, $\det AB = 0$;

(b) uz $m = n$, $\det AB = \det A \det B$;

(c) uz $m < n$, $\det AB$ jednaka je zbroju svih produkata koji se dobiju množenjem determinante svake submatrice od A reda m determinantom odgovarajuće submatrice reda m iz B.

Naravno, (c) uz $m = n$ obuhvaća i (b).

7. Dokaži: Slične matrice imaju istu determinantu.

9.9. Laplaceov razvoj determinante

Ovdje ćemo izložiti još jednu metodu koja olakšava izračunavanje determinante visokog reda. Njome smo se već u specijalnom slučaju poslužili u 5.12., kad smo rekli da se determinanta trećeg reda računa razvijanjem po elementima nekog, npr. prvog, retka, tj. ovako:

$$\begin{vmatrix} \alpha_{11} & \alpha_{12} & \alpha_{13} \\ \alpha_{21} & \alpha_{22} & \alpha_{23} \\ \alpha_{31} & \alpha_{32} & \alpha_{33} \end{vmatrix} = \alpha_{11} \begin{vmatrix} \alpha_{22} & \alpha_{23} \\ \alpha_{32} & \alpha_{33} \end{vmatrix} - \alpha_{12} \begin{vmatrix} \alpha_{21} & \alpha_{23} \\ \alpha_{31} & \alpha_{33} \end{vmatrix} + \alpha_{13} \begin{vmatrix} \alpha_{21} & \alpha_{22} \\ \alpha_{31} & \alpha_{32} \end{vmatrix} .$$

Lako se provjeri da je rezultat dobiven na taj način u skladu s našom definicijom determinante.

Sada ćemo tu metodu generalizirati. Neka je $A = [\alpha_{ik}]$ matrica reda n, a

$$\begin{aligned} \det A &= \begin{vmatrix} \alpha_{11} & \alpha_{12} & \cdots & \alpha_{1n} \\ \vdots & \vdots & & \vdots \\ \alpha_{i1} & \alpha_{i2} & \cdots & \alpha_{in} \\ \vdots & \vdots & & \vdots \\ \alpha_{n1} & \alpha_{n2} & \cdots & \alpha_{nn} \end{vmatrix} = \\ &= \sum_{p \in S_n} (-1)^{I(p)} \alpha_{1p(1)} \cdots \alpha_{ip(i)} \cdots \alpha_{np(n)} \end{aligned}$$

njezina determinanta. Uočimo jedan, npr. i-ti redak u toj determinanti,

$$(\alpha_{i1}, \ldots, \alpha_{ik}, \ldots, \alpha_{in}) . \tag{1}$$

Kako po definiciji svaki osnovni sumand sadrži jedan i samo jedan element iz svakog retka, svaki će osnovni sumand sadržavati točno jedan od elemenata skupa (1). Uočimo sve osnovne sumande koji sadrže element α_{ik} kao faktor, njih $(n-1)!$. Ako izlučimo taj zajednički faktor,

$$\alpha_{ik}(\ldots\ldots\ldots) ,$$

u zagradi će ostati suma produkata od $n-1$ elemenata iz promatrane determinante, od kojih očito nijedan nije iz njezina i-tog retka ili k-tog stupca. Izraz u zagradi nazivamo **algebarski komplement** ili **kofaktor** elementa α_{ik}, i označavamo ga s

$$A_{ik} .$$

Na primjer, u determinanti trećeg reda algebarski komplement A_{12} njezina elementa α_{12} nalazimo ovako:

$$-\alpha_{12}\alpha_{21}\alpha_{33} + \alpha_{12}\alpha_{23}\alpha_{31} = \alpha_{12}(\alpha_{23}\alpha_{31} - \alpha_{21}\alpha_{33}) ,$$

pa je

$$A_{12} = \alpha_{23}\alpha_{31} - \alpha_{21}\alpha_{33} .$$

Analogna razmatranja možemo provoditi i za fiksni stupac dane determinante. Kako je determinanta suma svih svojih osnovnih sumanada, odmah zaključujemo da vrijedi

PROPOZICIJA 1 (Laplace)
Za matricu $A = [\alpha_{ik}]$ *jest*

(1) $\det A = \sum_{j=1}^{n} \alpha_{ij} A_{ij}$, *za svaki* $i = 1, \ldots, n$;

(2) $\det A = \sum_{j=1}^{n} \alpha_{jk} A_{jk}$, *za svaki* $k = 1, \ldots, n$.

Kažemo da je (1) *razvoj* $\det A$ *po njezinu* i*-tom retku, a* (2) *razvoj* $\det A$ *po njezinu* k*-tom stupcu.* ■

Za praktično korištenje tih razvoja potrebno je pobliže ispitati strukturu algebarskih komplemenata, tj. naći jednostavni postupak za njihovo računanje. Neka je α_{ik} bilo koji element matrice A. Uočimo submatricu (vidi Zad. 3. u 9.6.) od A, koja se dobiva ispuštanjem iz A retka i stupca u kojima se taj element nalazi. Neka je s Δ_{ik} označena determinanta te kvadratne submatrice, tj.

$$\Delta_{ik} = \det \begin{bmatrix} \alpha_{11} & \cdots & \alpha_{1,k-1} & \alpha_{1,k+1} & \cdots & \alpha_{1n} \\ \vdots & & \vdots & \vdots & & \vdots \\ \alpha_{i-1,1} & \cdots & \alpha_{i-1,k-1} & \alpha_{i-1,k+1} & \cdots & \alpha_{i-1,n} \\ \alpha_{i+1,1} & \cdots & \alpha_{i+1,k-1} & \alpha_{i+1,k+1} & \cdots & \alpha_{i+1,n} \\ \vdots & & \vdots & \vdots & & \vdots \\ \alpha_{n1} & \cdots & \alpha_{n,k-1} & \alpha_{n,k+1} & \cdots & \alpha_{nn} \end{bmatrix} .$$

Ta je determinanta $(n-1)$-og reda. Nazivamo je **subdeterminanta** ili **minora** matrice A, određena elementom α_{ik}. Imamo onda

TEOREM 2

Za svaki $i, k = 1, \ldots, n$ *je*

$$A_{ik} = (-1)^{i+k} \Delta_{ik} ,$$

tj. algebarski komplement elementa α_{ik} *jednak je ili suprotan minori određenoj tim elementom, već prema tome je li suma* $i + k$, *rednog broja retka i stupca u kojem se* α_{ik} *nalazi, paran ili neparan broj.*

Dokaz

Uzmimo najprije da je $i = k = n$. Onda je

$$\alpha_{nn} A_{nn} = \sum_{p \in S_{n-1}} (-1)^{I(p')} \alpha_{1p(1)} \cdots \alpha_{n-1\, p(n-1)} \alpha_{nn} ,$$

gdje se sumira po svim permutacijama skupa $\{1, \ldots, n-1\}$, njih $(n-1)!$, i pritom je $I(p') = I(p)$, gdje je

$$p' = \begin{pmatrix} 1 & 2 & \cdots & n-1 & n \\ p(1) & p(2) & \cdots & p(n-1) & n \end{pmatrix} \in S_n .$$

Odavde dijeljenjem s α_{nn} dobivamo

$$\begin{aligned} A_{nn} &= \sum_{p \in S_{n-1}} (-1)^{I(p)} \alpha_{1p(1)} \cdots \alpha_{n-1\, p(n-1)} = \\ &= \begin{vmatrix} \alpha_{11} & \cdots & \alpha_{1,n-1} \\ \vdots & & \vdots \\ \alpha_{n-1,1} & \cdots & \alpha_{n-1,n-1} \end{vmatrix} = \Delta_{nn} , \end{aligned}$$

po definiciji. Kako je $(-1)^{n+n} = (-1)^{2n} = 1$, u tom specijalnom slučaju je tvrdnja verificirana.

Da bismo odredili algebarski komplement A_{ik} bilo kojeg elementa α_{ik}, izvedimo najprije u polaznoj determinanti, $D = \det A$, $n - i$ sukcesivne zamjene redaka, dovodeći tako i-ti redak na mjesto posljednjeg retka, a zatim $n - k$ zamjena stupaca, dovodeći k-ti stupac na mjesto posljednjeg

stupca. Nakon tih promjena dobivamo determinantu

$$D_{ik} = \det \begin{vmatrix} \alpha_{11} & \cdots & \alpha_{1,k-1} & \alpha_{1,k+1} & \cdots & \alpha_{1n} & \alpha_{1k} \\ \vdots & & \vdots & \vdots & & \vdots & \vdots \\ \alpha_{i-1,1} & \cdots & \alpha_{i-1,k-1} & \alpha_{i-1,k+1} & \cdots & \alpha_{i-1,n} & \alpha_{i-1,k} \\ \alpha_{i+1,1} & \cdots & \alpha_{i+1,k-1} & \alpha_{i+1,k+1} & \cdots & \alpha_{i+1,n} & \alpha_{i+1,k} \\ \vdots & & \vdots & \vdots & & \vdots & \vdots \\ \alpha_{n1} & \cdots & \alpha_{n,k-1} & \alpha_{n,k+1} & \cdots & \alpha_{nn} & \alpha_{n,k} \\ \alpha_{i1} & \cdots & \alpha_{i,k-1} & \alpha_{i,k+1} & \cdots & \alpha_{in} & \alpha_{i,k} \end{vmatrix} .$$

Kako je provedeno ukupno $(n-i)+(n-k) = 2n-(i+k)$ zamjena stupaca, odnosno redaka, i kako je

$$(-1)^{2n-(i+k)} = (-1)^{i+k} ,$$

po Prop. 3 iz 9.7. je

$$D = (-1)^{i+k} D_{ik} . \tag{2}$$

No, suma svih osnovnih sumanada u D koji sadrže α_{ik} po definiciji je jednaka $\alpha_{ik}A_{ik}$. U drugu ruku, jer se u determinanti D_{ik} element α_{ik} nalazi u zadnjem retku i zadnjem stupcu, prema prethodnom je njegov algebarski komplement jednak pripadnoj minori, a ta je po konstrukciji baš jednaka Δ_{ik}, pa je suma osnovnih sumanada koji sadrže α_{ik} jednaka

$$\alpha_{ik}\Delta_{ik} .$$

Iz identitete (2) i jer D i D_{ik} imaju iste elemente (samo na različitim mjestima), onda zaključujemo

$$\alpha_{ik}A_{ik} = (-1)^{i+k}\alpha_{ik}\Delta_{ik} ,$$

dakle

$$A_{ik} = (-1)^{i+k}\Delta_{ik}$$

i teorem je dokazan. ■

Kombinirajući Kor. 11 u 9.7. s Laplaceovim razvojem determinante, dolazimo do praktične metode za njihovo računanje. Naime, na taj način možemo postupno snižavati red determinante dok ne dođemo do determinante trećeg reda, koju možemo izračunati elementarno (npr. pomoću Sarrusova pravila). Na primjer,

$$\begin{vmatrix} 2 & 2 & 4 & 12 \\ 3 & 1 & 5 & 0 \\ 1 & 2 & 3 & 1 \\ 1 & 4 & 1 & 0 \end{vmatrix} = \begin{vmatrix} 2 & 0 & 0 & 0 \\ 3 & -2 & -1 & -18 \\ 1 & 1 & 1 & -5 \\ 1 & 3 & -1 & -6 \end{vmatrix} = 2\cdot \begin{vmatrix} -2 & -1 & -18 \\ 1 & 1 & -5 \\ 3 & -1 & -6 \end{vmatrix} = 2\cdot 103 = 206 .$$

PROPOZICIJA 3

Za matricu $A = [\alpha_{ik}]$ *je, uz* $i \neq j$,

$$\sum_k \alpha_{ik} A_{jk} = 0 \,,$$

tj. suma produkata elemenata bilo kojeg retka matrice s algebarskim komplementima korespondentnih elemenata nekog drugog retka jednaka je nuli.

Dokaz

Neka je $B = [\beta_{rk}]$ definirana s

$$\beta_{rk} = \begin{cases} \alpha_{rk} & , \ r \neq j \\ \alpha_{ik} & , \ r = j \end{cases} \,,$$

za svaki k. Onda po Prop. 1 razvijanjem po j-tom retku imamo

$$\det B = \sum_k \beta_{jk} B_{jk} = \sum_k \alpha_{ik} A_{jk} \,.$$

Kako B ima dva jednaka retka, i-ti i j-ti, odmah je $\det B = 0$ pa imamo tvrdnju. ■

Analogna tvrdnja vrijedi i za stupce. Prema tome, možemo rezimirati:

KOROLAR 4

Za bilo koju kvadratnu matricu $A = [\alpha_{ik}]$ *je*

(1) $\sum_k \alpha_{ik} A_{jk} = \delta_{ij} \cdot \det A;$

(2) $\sum_i \alpha_{ik} A_{il} = \delta_{kl} \cdot \det A.$ ■

Neka je sada $A = [\alpha_{ik}]$ bilo koja kvadratna matrica, a $[A_{ik}]$ matrica algebarskih komplemenata elemenata matrice A. Transponiranu matricu te matrice, tj. matricu

$$\tilde{A} = [A_{ik}]' = [A_{ki}] \,,$$

nazivamo **adjunkta** matrice A.

PROPOZICIJA 5

Za svaku je matricu

$$A\tilde{A} = \tilde{A}A = (\det A) \cdot E \,,$$

gdje je E *jedinična matrica.*

Dokaz

Neka je $A\tilde{A} = C$, gdje je $C = [\gamma_{ik}]$. Onda je zbog Kor. 4

$$\gamma_{ik} = \sum_j \alpha_{ij} A_{kj} = \delta_{ik} \cdot \det A \,,$$

pa je

$$C = [\gamma_{ik}] = [\delta_{ik} \det A] = \det A \cdot [\delta_{ik}] = (\det A) E \,. \qquad \blacksquare$$

KOROLAR 6

Za svaku matricu reda n je

$$\det A \cdot \det \tilde{A} = (\det A)^n \,.$$

Dokaz

Tvrdnja izlazi primjenom Binet-Cauchyjeva teorema na jednakost $A\tilde{A} = (\det A)E$. $\blacksquare$

ZADACI

1. Koji put je potrebno povisiti red determinante, zadržavajući pritom njezinu vrijednost. To postižemo umetanjem jednog retka i jednog stupca, stavljajući na njihov presjek ± 1, u ovisnosti o parnosti sume rednog broja tog stupca i retka, dok za ostale elemente u retku stavimo nule, a za ostale elemente u stupcu **bilo što**. Kažemo da smo polaznu determinantu **obrubili**. Imamo npr.

$$\begin{vmatrix} \alpha & \beta \\ \gamma & \delta \end{vmatrix} = \begin{vmatrix} \alpha & \beta & x \\ \gamma & \delta & y \\ 0 & 0 & 1 \end{vmatrix} \,.$$

Obrubljivanjem pokaži da se jednadžba ravnine u E^3 kroz tri dane točke može pisati i kao

$$\begin{vmatrix} x & y & z & 1 \\ x_1 & y_1 & z_1 & 1 \\ x_2 & y_2 & z_2 & 1 \\ x_3 & y_3 & z_3 & 1 \end{vmatrix} = 0 \,,$$

kako smo najavili u 6.3.

2. Pokaži: Ako je matrica $A = [\alpha_{ik}]$ ortogonalna, onda je $A_{ik} = \pm \alpha_{ik}$, za svaki i, k. Obrat ne vrijedi.

3. Dokaži ova svojstva adjunkte matrice A:

   (a) $(\tilde{A}') = (\tilde{A})'$;

   (b) $(\widetilde{\lambda A}) = \lambda^{n-1} \cdot \tilde{A}$;

   (c) $(\widetilde{AB}) = \tilde{B}\tilde{A}$;

   (d) $(\tilde{\tilde{A}}) = (\det A)^{n-2} \cdot A$.

9.10. Još o rangu i inverzu matrice

Determinante su pogodno sredstvo za utvrđivanje regularnosti matrice i određivanje njezina inverza, odnosno ranga.

TEOREM 1

Kvadratna matrica A je regularna onda i samo onda ako je $\det A \neq 0$.

Dokaz

Neka je A regularna matrica, a A^{-1} njezin inverz. Kad bi bilo $\det A = 0$, iz $AA^{-1} = E$ bismo primjenom Binet-Cauchyjeva teorema dobili

$$\det A \cdot \det A^{-1} = \det E = 1 ,$$

dakle $0 \cdot \det A^{-1} = 1$, što je kontradikcija. Dakle je $\det A \neq 0$.

Obratno, neka je $\det A \neq 0$. Onda iz

$$A\tilde{A} = \tilde{A}A = (\det A) \cdot E$$

(Prop. 5 u 9.9.), množenjem sa skalarom $(\det A)^{-1}$ dobivamo

$$A\left[(\det A)^{-1}\,\tilde{A}\right] = \left[(\det A)^{-1}\,\tilde{A}\right] A = E ,$$

što pokazuje da jednadžba $AX = XA = E$ ima rješenje, pa je A regularna matrica. ■

KOROLAR 2

Ako je A regularna matrica, njezin je inverz dan formulom

$$A^{-1} = (\det A)^{-1} \cdot \tilde{A} ,$$

gdje je $\tilde{A}$ adjunkta matrice A.

Dokaz

Neposredno iz drugog dijela dokaza Tm. 1. ■

Time smo dobili eksplicitnu formulu za računanje inverza matrice.
Iz Zad. 7. u 9.6. te Tm. 1 slijedi neposredno

KOROLAR 3

Neka je A kvadratna matrica. Onda je

(1) $\det A \neq 0$ *ako i samo ako je skup njezinih redaka (stupaca) linearno nezavisan;*

(2) $\det A = 0$ *ako i samo ako je skup njezinih redaka (stupaca) linearno zavisan.* ■

Druga tvrdnja je dakako posljedica prve, ali ju je dobro imati zapisanu eksplicitno.

U 8.9. smo definirali pojam minore kvadratne matrice A, određene nekim njezinim elementom, i ta je minora bila determinanta $(n-1)$-og reda. Sada taj pojam generaliziramo. Neka je A bilo koja matrica tipa (m,n) i $k \leq \min\{m,n\}$. Pod **minorom reda** k matrice A podrazumijevamo determinantu bilo koje kvadratne submatrice (vidi Zad. 3. u 9.6.) od A koja je reda k, tj. koja se dobiva iz A uklanjanjem $m-k$ redaka i $n-k$ stupaca. Na primjer, u matrici tipa (3,4) imamo 4 minore reda 3, 18 minora reda 2 i, dakako, 12 minora reda 1 (to su elementi te matrice).

TEOREM 4

Matrica A će imati različitu od nule minoru reda r ako i samo ako je rang matrice bar r.

Dokaz

Pretpostavimo da postoji minora matrice A koja je različita od nule i koja je reda r. Kad bi rang matrice A bio manji od r, svakih r njezinih stupaca bilo bi linearno zavisno. Posebno dakle, u svakoj submatrici od A reda r njezini bi stupci bili linearno zavisni, pa bi determinanta te submatrice po Kor. 3 bila jednaka nuli. Prema tome bi svaka minora od A reda r bila jednaka nuli, što se protivi pretpostavci.

Obratno, pretpostavimo da je matrica A tipa (m,n) i da je njezin rang bar r. Onda A sigurno ima r linearno nezavisnih stupaca. Neka je B submatrica od A tipa (m,r), u kojoj stupci čine linearno nezavisan skup. Njezin je rang dakako r. Nadalje, u matrici B ima točno r linearno nezavisnih redaka (Tm. 2 u 9.6.). Neka je C submatrica od B određena tim redcima. Onda je C kvadratna submatrica od A reda r, i prema Kor. 3 je $\det C \neq 0$, pa je $\det C$ tražena minora i tvrdnja je dokazana. ■

KOROLAR 5

Matrica A je ranga r onda i samo onda ako postoji bar jedna minora reda r te matrice, koja je različita od nule, dok su sve minore reda većeg od r jednake nuli.

Dokaz

Ako je rang matrice A jednak r, onda po Tm. 4 postoji minora reda r koja je različita od nule. Kad bi u A postojala minora većeg reda koja je različita od nule, bio bi opet po Tm. 4 i rang od A veći od r, protivno pretpostavci. Slično se pokazuje i obrat. ■

Iz Kor. 5 zaključujemo da **rang matrice možemo alternativno definirati** kao red najobuhvatnije minore te matrice, koja je različita od nule.

ZADACI

1. Dokaži: Matrica A je regularna onda i samo onda ako je $\tilde{A}$ regularna. Prema tome je uvijek (vidi Kor. 6 u 9.9.)

$$\det \tilde{A} = (\det A)^{n-1} ,$$

gdje je n red matrice A.

2. Dokaži: $\tilde{A} = O$ ako i samo ako je $r(A) \leq n - 2$.

3. Ako je A regularna matrica, onda je

$$\det A^{-1} = (\det A)^{-1} .$$

Vrijedi i općenitije, tj.

$$\det A^k = (\det A)^k ,$$

za svaki $k \in \mathbb{Z}$. Dokaži!

4. Iz Tm. 1 slijedi da opću linearnu grupu (vidi 9.5.) možemo definirati kao

$$GL(n, F) = \{A \in M_n \mid \det A \neq 0\} .$$

Neka je

$$UM(n, F) = \{A \in M_n \mid \det A = \pm 1\} .$$

Pokaži da je $UM(n, F)$ podgrupa od $GL(n, F)$. Grupu $UM(n, F)$ nazivamo **unimodularna grupa**. Neka je, nadalje,

$$SL(n, F) = \{A \in M_n \mid \det A = 1\} .$$

Pokaži da je $SL(n, F)$ podgrupa od $UM(n, F)$. Tu grupu zovemo **specijalna linearna grupa**. Konačno, ako je $O(n, F) < UM(n, F)$ ortogonalna grupa, onda definiramo

$$SO(n, F) = O(n, F) \cap SL(n, F) ,$$

i tu grupu nazivamo **specijalna ortogonalna grupa**. Ako $\rightarrow$ označava relaciju "biti podgrupa", odnose između navedenih grupa možemo shematski prikazati ovako:

$$SO \begin{array}{c} \nearrow \\ \searrow \end{array} \begin{array}{c} O \\ \\ SL \end{array} \begin{array}{c} \searrow \\ \nearrow \end{array} UM \rightarrow GL \ .$$

Te grupe imaju važnu ulogu u geometriji euklidskog prostora, a i drugdje.

5. Dokaži ovu strožu formu Kor. 5: Matrica ima rang r ako i samo ako ima bar jednu od nule različitu minoru reda r, dok su sve minore reda $r+1$ jednake nuli.

6. Neka je $A \in M_n$ bilo koja kvadratna matrica. Onda se pomoću tragova može utvrditi je li ta matrica regularna, i ako jest, odrediti njezin inverz. Radi se po ovoj shemi:

$$\begin{array}{lllllllll} A_1 & = & A\,, & \operatorname{tr} A_1 & = & s_1\,, & B_1 & = & A_1 - s_1 E \\ A_2 & = & AB_1\,, & 1/2 \operatorname{tr} A_2 & = & s_2\,, & B_2 & = & A_2 - s_2 E \\ & \vdots & & & \vdots & & & \vdots & \\ A_n & = & AB_{n-1}\,, & 1/n \operatorname{tr} A_n & = & s_n\,, & B_n & = & A_n - s_n E\ . \end{array}$$

Pokaži da je uvijek $B_n = 0$. Pokaži, nadalje, da je matrica A regularna ako i samo ako je $s_n \neq 0$, i da je u tom slučaju

$$A^{-1} = \frac{B_{n-1}}{s_n}\ .$$

Taj postupak se zove **Frame-Fadejevljev algoritam**.

10

INVARIJANTE LINEARNOG OPERATORA

U ovom poglavlju nastavljamo s ispitivanjem svojstava linearnih operatora. Pritom se, bitno i u znatnoj mjeri, koristimo upravo zaokruženom teorijom determinanata i matrica, što dokazuje važnost te teorije u linearnoj algebri.

10.1. Koordinatizacija

Neka je V linearni prostor nad poljem F i neka je $\dim V = n$. Neka je

$$B = (a_1, ..., a_n)$$

bilo koja njegova (uređena) baza. Tu bazu nazivamo još i **koordinatna baza** ili **koordinatni sustav** u prostoru V. Neka je sada $a \in V$ bilo koji vektor. Onda on ima jednoznačan prikaz oblika

$$a = \sum_{i=1}^{n} \alpha_i a_i \ .$$

Koeficijente $\alpha_i \in F$ nazivamo **koordinatama**, njihovu uređenu n–torku

$$(\alpha_1, ..., \alpha_n) = \text{kraće} = (\alpha_i)$$

koordinatnim slogom, a matricu

$$X = \begin{bmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{bmatrix} = \text{kraće} = [\alpha_i]$$

koordinatnom matricom vektora a u bazi B. Neka je

$$k : V \to F^n$$

operator definiran kao $k(a) = (\alpha_i)$, a

$$h : V \to M_{n1}$$

operator dan s $h(a) = [\alpha_i]$.

PROPOZICIJA 1

Operatori k i h su izomorfizmi linearnih prostora.

Dokaz

Trivijalan. ■

Svaki od tih operatora nazivamo **koordinatizacija prostora** V, s obzirom na danu bazu B. Pomoću tih izomorfizama provodimo identifikaciju

$$a = k(a) = h(a) ,$$

i pišemo kraće

$$a = (\alpha_i) , \quad \text{odnosno} \quad a = [\alpha_i] .$$

Neka je sada $S = (x_1, ..., x_s) \subset V$ uređeni skup vektora iz V. Neka je za $k = 1, ..., s$

$$x_k = \begin{bmatrix} \alpha_{1k} \\ \vdots \\ \alpha_{nk} \end{bmatrix}$$

koordinatna matrica vektora $x_k \in S$ u bazi B. Onda skupu S možemo pridružiti matricu

$$M(S) = \begin{bmatrix} \alpha_{11} & \alpha_{12} & \cdots & \alpha_{1s} \\ \vdots & \vdots & & \vdots \\ \alpha_{n1} & \alpha_{n2} & \cdots & \alpha_{ns} \end{bmatrix}$$

tipa (n, s), kojoj se stupci podudaraju s koordinatnim matricama vektora x_k, $k = 1, \ldots, s$. Kažemo da je $M(S)$ **matrica skupa vektora** S s obzirom na bazu B. Sada imamo jednostavan kriterij za utvrđivanje linearne nezavisnosti vektora.

PROPOZICIJA 2

Maksimalni linearno nezavisni podskup skupa S sadrži r vektora ako i samo ako je rang matrice $M(S)$ jednak r.

Dokaz

Neposredno iz činjenice da je koordinatizacija h izomorfizam i definicije ranga matrice. ■

Specijalno, kad je $s = n = \dim V$ imamo

KOROLAR 3

Skup $S = (x_1, ..., x_n)$ od n vektora iz V bit će baza prostora V onda i samo onda ako je matrica $M(S)$ toga skupa regularna, tj. ako i samo ako je

$$\det M(S) \neq 0 .$$ ■

ZADACI

1. Pokaži da vektori $(1,1,1), (1,2,2), (1,2,3)$ čine bazu za $\mathbb{R}^3$.
2. Jesu li polinomi $t^3 + t^2 + t$, $t^2 + t + 1$, $t^3 + t^2 + t + 1 \in P_4$ linearno nezavisni?

10.2. Transformacija koordinata

Neka su $B = (a_i)$ i $B' = (a'_k)$ dvije koordinatne baze linearnog prostora V. Ako je $a \in V$ bilo koji vektor, on će imati svoju koordinatnu matricu $X = [\alpha_i]$ u bazi B, i koordinatnu matricu $X' = [\alpha'_i]$ s obzirom na bazu B'. Postavlja se pitanje u kakvom su odnosu te matrice, tj. po kakvom se zakonu mijenjaju koordinate vektora a pri prijelazu iz jednoga koordinatnog sustava u drugi.

To će očito ovisiti o međusobnom relativnom položaju koordinatnih sustava. Taj će položaj biti fiksiran ako su zadane koordinate vektora baze B' u bazi B, tj. ako znamo

$$a'_k = \begin{bmatrix} \beta_{1k} \\ \vdots \\ \beta_{nk} \end{bmatrix} ,$$

gdje je $k = 1, ..., n$. Matricu

$$T = M(B') = \begin{bmatrix} \beta_{11} & \cdots & \beta_{1n} \\ \vdots & & \vdots \\ \beta_{n1} & \cdots & \beta_{nn} \end{bmatrix}$$

skupa B' u bazi B nazivamo **matrica prijelaza** ili **matrica transformacije** baze B u bazu B'. Pišemo $B \xrightarrow{T} B'$. Kako je B' također baza, prema Kor. 3 u 10.1. zaključujemo da je matrica T uvijek regularna, dakle

$$\det T \neq 0 .$$

TEOREM 1

Neka su X i X' koordinatne matrice vektora $a \in V$ u bazama B, odnosno B', a T neka je matrica prijelaza iz prve baze u drugu. Onda je

$$X = TX' ,$$

odnosno

$$X' = T^{-1}X .$$

Dokaz

U bazi B vektor a ima prikaz

$$a = \sum_{i=1}^{n} \alpha_i a_i , \tag{1}$$

a u bazi B' imamo

$$a = \sum_{k=1}^{n} \alpha'_k a'_k = \sum_{k=1}^{n} \alpha'_k \left(\sum_{i=1}^{n} \beta_{ik} a_i \right) = \sum_{i=1}^{n} \left(\sum_{k=1}^{n} \beta_{ik} \alpha'_k \right) a_i . \tag{2}$$

Uspoređivanjem (1) i (2) dobivamo

$$\alpha_i = \sum_{k=1}^{n} \beta_{ik} \alpha'_k ,$$

za svaki $i = 1, ..., n$, dakle $X = TX'$, i teorem je dokazan. ■

Relacije

$$\alpha_i = \sum_{k=1}^{n} \beta_{ik} \alpha'_k , \quad i = 1, \ldots, n ,$$

i njima inverzne

$$\alpha'_i = \sum_{k=1}^{n} \gamma_{ik} \alpha_k , \quad i = 1, \ldots, n ,$$

gdje je $[\gamma_{ik}] = T^{-1}$, nazivamo **jednadžbama transformacije koordinata**. Prvima su eksplicitno izražene koordinate vektora u bazi B pomoću onih u bazi B', a drugima obratno.

ZADACI

1. Kako smo vidjeli, matrica transformacije je uvijek regularna. Dokaži obratno: Svaka regularna matrica reda n nad poljem F je matrica neke transformacije koordinatnih sustava u n–dimenzionalnom prostoru nad poljem F.

2. Pokaži: Ako je T matrica prijelaza $B \to B'$, onda je T^{-1} matrica prijelaza $B' \to B$. [Uputa: Rabi Lemu 1 u 10.4.]

3. Dokaži: Ako je prijelaz $B \to B'$ opisan matricom T_1, a prijelaz $B' \to B''$ matricom T_2, onda je matrica prijelaza iz baze B u bazu B'' dana s $T = T_1 \cdot T_2$.

4. Neka su $\{0; (\vec{i}, \vec{j})\}$ i $\{0; (\vec{i}', \vec{j}')\}$ dva pravokutna sustava u E^2 i neka je

$$\sphericalangle(\vec{i}, \vec{i}') = \sphericalangle(\vec{j}, \vec{j}') = \varphi \, .$$

Pokaži da je matrica prijelaza iz prvog sustava u drugi dana s

$$R = \begin{bmatrix} \cos\varphi & -\sin\varphi \\ \sin\varphi & \cos\varphi \end{bmatrix} .$$

Ta se transformacija naziva **rotacija koordinatnog sustava** za kut φ. Uoči da je matrica R ortogonalna. Uvjeri se, nadalje, da su jednadžbe transformacije koordinata (nove koordinate pomoću starih)

$$\begin{aligned} x' &= x\cos\varphi + y\sin\varphi \\ y' &= -x\sin\varphi + y\cos\varphi \, . \end{aligned}$$

5. Neka su $B = \{0; (\vec{i}, \vec{j}, \vec{k})\}$ i $B' = \{0; (\vec{i}', \vec{j}', \vec{k}')\}$ dva jednako orijentirana, npr. desna pravokutna koordinatna sustava u E^3, s istim ishodištem. Onda se prijelaz iz B u B' može uvijek realizirati pomoću tri "rotacije", tj. uzastopnim prijelazom

$$B \to B_1 \to B_2 \to B' \, ,$$

gdje su $B_s = \{0; (\vec{i}_s, \vec{j}_s, \vec{k}_s)\}$, $s = 1, 2$ pomoćni međusustavi koje ćemo sada opisati. Neka je $\vec{e} \in [\{\vec{i}, \vec{j}\}] \cap [\{\vec{i}', \vec{j}'\}]$ vektor iz presjeka ravnina razapetih vektorima $\vec{i}$ i $\vec{j}$, odnosno $\vec{i}'$ i $\vec{j}'$, i neka je

$$\varphi = \sphericalangle(\vec{i}, \vec{e}) \, .$$

Nadalje, neka je

$$\chi = \sphericalangle(\vec{k}, \vec{k}') \, ,$$

i konačno,

$$\psi = \sphericalangle(\vec{e}, \vec{i}') \, .$$

Onda prijelaze iz sustava u sustav definiramo ovako:

(1) $B \to B_1$, s $\sphericalangle(\vec{i}, \vec{i}_1) = \sphericalangle(\vec{j}, \vec{j}_1) = \varphi$, $\sphericalangle(\vec{k}, \vec{k}_1) = 0$,

tj. kao rotaciju oko $\vec{k}$ za kut φ, dakle matricom

$$R_1 = \begin{bmatrix} \cos\varphi & -\sin\varphi & 0 \\ \sin\varphi & \cos\varphi & 0 \\ 0 & 0 & 1 \end{bmatrix} ;$$

(2) $B_1 \to B_2$ s $\sphericalangle(\vec{\imath}_1, \vec{\imath}_2) = 0$, $\sphericalangle(\vec{\jmath}_1, \vec{\jmath}_2) = \sphericalangle(\vec{k}_1, \vec{k}_2) = \chi$,

tj. kao rotaciju oko $\vec{\imath}_1$ za kut χ, dakle matricom

$$R_2 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & \cos\chi & -\sin\chi \\ 0 & \sin\chi & \cos\chi \end{bmatrix} , \text{ i}$$

(3) $B_2 \to B'$, s $\sphericalangle(\vec{\imath}_2, \vec{\imath}') = \sphericalangle(\vec{\jmath}_2, \vec{\jmath}') = \psi$, $\sphericalangle(\vec{k}_2, \vec{k}') = 0$,

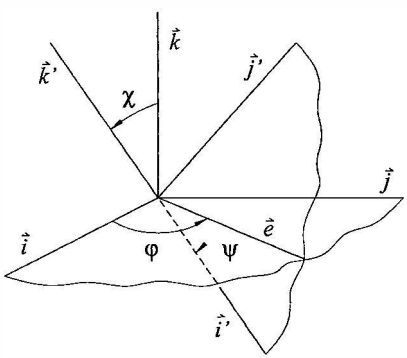
tj. kao rotaciju oko $\vec{k}_2$ za kut ψ, dakle matricom

$$R_3 = \begin{bmatrix} \cos\psi & -\sin\psi & 0 \\ \sin\psi & \cos\psi & 0 \\ 0 & 0 & 1 \end{bmatrix} .$$

Prema tome je prijelaz iz sustava B u B' opisan matricom

$$R = R_1 \, R_2 \, R_3 .$$

Nacrtaj sliku i uvjeri se u ispravnost navedene konstrukcije.



Napiši matricu R eksplicitno. Isto tako, napiši jednadžbe transformacije koordinata, starih pomoću novih i obratno. Nadalje, pokaži da je svaka od matrica R_i, pa onda i matrica R, ortogonalna. Kutovi φ, χ i ψ nazivaju se **Eulerovi kutovi**, i to redom: **kut vlastite rotacije**, **kut nutacije** i **kut precesije**. Ti kutovi igraju važnu ulogu i u geometriji, i u mehanici.

10.3. Matrični zapis linearnog operatora

Kako smo već napomenuli u točki 9.1., linearni se operatori mogu reprezentirati matricama. Ponovimo:

Neka su U, V linearni prostori nad istim poljem, dimenzije n, odnosno m, a

$$f : U \to V$$

neka je linearni operator. Neka je $A = (a_1, \ldots, a_n)$ baza za U, a $B = (b_1, ..., b_m)$ baza za V. Neka je

$$f(a_k) = \sum_{i=1}^{m} \alpha_{ik} b_i \, .$$

Kako je operator jednoznačno zadan svojim djelovanjem na bazi A, on je jednoznačno određen matricom

$$F = F_{(A,B)} = M(\,(f(a_1), \ldots, f(a_n))\,) = \begin{bmatrix} \alpha_{11} & \cdots & \alpha_{1n} \\ \vdots & & \vdots \\ \alpha_{m1} & \cdots & \alpha_{mn} \end{bmatrix}$$

tipa (m, n), u kojoj su stupci koordinatne matrice slika $f(a_k)$ vektora baze A u bazi B. Matricu F nazivamo **matrični zapis**, odnosno **matrični prikaz**, **matrična reprezentacija** ili, kratko, **matrica** operatora F u paru baza (A, B). Ako je $U = V$, standardno uzimamo $A = B$, i govorimo o matrici operatora f u bazi A.

Primijetimo odmah da vrijedi

PROPOZICIJA 1

Rang linearnog operatora jednak je rangu matrice tog operatora.

Dokaz

Kako je rang r operatora $f : U \to V$ po definiciji jednak

$$r = \dim\,[\{f(a_1), \ldots, f(a_n)\}]\,,$$

dakle dimenzija maksimalnog linearno nezavisnog podskupa od $\{f(a_1), \ldots, f(a_n)\}$, to je po Prop. 2 u 10.1. taj rang jednak rangu matrice

$$M(\{f(a_1), \ldots, f(a_n)\}) = F\,,$$

pa je $r(F) = r$. ■

KOROLAR 2

Linearni operator je izomorfizam linearnih prostora ako i samo ako je matrica tog operatora regularna. ■

PRIMJERI

1. Projektor $p : F^3 \to F^2$, $p(\alpha, \beta, \gamma) = (\alpha, \beta)$, u paru kanonskih baza zapisan je matricom
$$P = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix} .$$

2. Operator deriviranja $d : P_n \to P_{n-1}$ u paru standardnih baza zapisan je matricom
$$D = \begin{bmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 2 & \cdots & 0 \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & \cdots & n-1 \end{bmatrix}$$
tipa $(n-1, n)$.

3. Nuloperator očito ima nulmatricu O za matrični zapis, a jedinični operator jediničnu matricu E.

Neka je sada $f : U \to V$ linearni operator, a $F = [\alpha_{ik}]$ njegov matrični zapis u danom paru baza (A, B). Neka je, nadalje, $a \in U$ bilo koji vektor, a $X = [\alpha_i]$ njegova koordinatna matrica u bazi A. Ako je $Y = [\beta_i]$ koordinatna matrica slike $f(a) \in V$ tog vektora u bazi B, postavlja se pitanje kako odrediti tu matricu pomoću matrica X i F. Odgovor daje

PROPOZICIJA 3

Koordinate slike dane su relacijom

$$Y = FX .$$

Dokaz

Po pretpostavci je

$$a = \sum_{k=1}^{n} \alpha_k a_k .$$

Zato je

$$f(a) = f(\sum_{k=1}^{n} \alpha_k a_k) = \sum_{k=1}^{n} \alpha_k f(a_k) = \sum_{k=1}^{n} \alpha_k (\sum_{i=1}^{m} \alpha_{ik} b_i) =$$

$$= \sum_{i=1}^{m} (\sum_{k=1}^{n} \alpha_{ik}\alpha_k) b_i \ . \tag{1}$$

No, u drugu ruku je

$$f(a) = \sum_{i=1}^{m} \beta_i b_i \ , \tag{2}$$

pa uspoređivanjem (1) i (2) dobivamo

$$\beta_i = \sum_{k=1}^{n} \alpha_{ik}\alpha_k \ ,$$

za svaki $i = 1, \ldots, m$. Dakle, zaista je

$$Y = FX \ .$$

■

ZADACI

1. Nađi matrični zapis operatora integriranja $s : P_n \to P_{n+1}$, u standardnom paru baza.

2. U prostoru V^3 dan je vektor $a = (1, 1, 1)$. Nađi koordinate njegove slike pri zrcaljenju na ravnini $[\vec{j}, \vec{k}]$, pravcu $[\vec{i}]$, odnosno pri rotaciji za kut $\varphi = \pi/4$ oko $[\vec{k}]$ (vidi 5.14.).

10.4. Izomorfizam prostora Hom (U, V) i M_{mn}

Dokažimo najprije ovaj rezultat:

LEMA 1

Neka su $A = [\alpha_{ik}]$ i $B = [\beta_{ik}]$ matrice tipa (m, n). Ako je

$$AX = BX \ ,$$

za svaku stupčanu matricu $X \in M_{n1}$, onda je

$$A = B \ .$$

Dokaz

Odaberimo za svaki $k = 1, ..., n$ specijalni stupac $E_k = [\lambda_i] = [\delta_{ik}]$, koji, dakle, u k-tom retku ima 1, a svi ostali elementi su mu nule. Onda iz $AE_k = BE_k$ izlazi

$$\begin{bmatrix} \alpha_{1k} \\ \vdots \\ \alpha_{mk} \end{bmatrix} = \begin{bmatrix} \beta_{1k} \\ \vdots \\ \beta_{mk} \end{bmatrix},$$

tj.

$$\alpha_{ik} = \beta_{ik},$$

za svaki i i za svaki k, pa je $A = B$. ■

Imamo sada

TEOREM 2

Neka su $A = (a_1, \ldots, a_n)$ *i* $B = (b_1, \ldots, b_m)$ *baze za prostore* U, *odnosno* V. *Neka je*

$$\Phi : \mathrm{Hom}\,(U, V) \to M_{mn}$$

operator definiran s

$$\Phi(f) = F,$$

gdje je F *matrični zapis operatora* f *u paru baza* (A, B). *Onda je* Φ *izomorfizam linearnih prostora. Specijalno, ako je* $U = V$,

$$\Phi : \mathrm{Hom}\, V \to M_n$$

jest izomorfizam algebri.

Dokaz

Prije svega, Φ je bijekcija. Zaista, iz

$$\Phi(f) = \Phi(g)$$

slijedi

$$F = G,$$

a onda je, prema definiciji matrice operatora,

$$f(a_k) = g(a_k),$$

za svaki $k = 1, \ldots, n$, i prema tome je

$$f = g,$$

jer je linearni operator jednoznačno određen svojim djelovanjem na bazi prostora.

Pokažimo da vrijedi

$$\Phi(f+g) = \Phi(f) + \Phi(g). \tag{1}$$

Neka je $\Phi(f) = F$, $\Phi(g) = G$ i $\Phi(f+g) = H$. Neka je $a \in U$ bilo koji vektor, a X njegova koordinatna matrica u bazi A. Nadalje, neka su Y i Z koordinatne matrice slika $f(a)$ i $g(a)$ tog vektora, u odnosu na bazu B. Dakako, budući da je koordinatizacija izomorfizam, slici $(f+g)(a) = f(a) + g(a)$ odgovarat će koordinatna matrica $Y + Z$. Prema Prop. 3 u 10.3. onda je

$$Y = FX \quad , \quad Z = GX \quad , \quad Y + Z = HX \ ,$$

tj.

$$HX = Y + Z = FX + GX = (F+G)X \ ,$$

i to je istina za svaku matricu $X \in M_{n1}$. Po Lemi 1. je zato

$$H = F + G$$

i (1) je dokazana. Posve analogno vidi se da je

$$\Phi(\alpha f) = \alpha \Phi(f) \ , \tag{2}$$

i prema tome je Φ zaista izomorfizam linearnih prostora.

Pokažimo još da u slučaju $U = V$ vrijedi i

$$\Phi(g \circ f) = \Phi(g) \cdot \Phi(f) \ , \tag{3}$$

tj. da je Φ izomorfizam algebri. Neka su opet $\Phi(f) = F$, $\Phi(g) = G$ i $\Phi(g \circ f) = K$ matrični zapisi promatranih operatora, s obzirom na bazu B. Nadalje, za $a \in V$ neka su X, Y i Z redom koordinatne matrice tog vektora a, te vektora $f(a)$ i vektora $(g \circ f)(a) = g[f(a)]$ u danoj bazi B prostora V. Prop. 3 iz 10.3. onda kaže da je

$$Z = KX \ , \tag{4}$$

a u drugu ruku je

$$Y = FX \quad \text{i} \quad Z = GY \ . \tag{5}$$

Zbog (4) i (5) onda je

$$KX = Z = GY = G(FX) = (GF)X$$

i odatle, zbog Leme 1,

$$K = GF\,,$$

pa je verificirana relacija (3) i teorem je dokazan. ■

Primijetimo da izomorfizam Φ ovisi o izboru baza, pa bi bilo korektnije pisati $\Phi_{(A,B)}$. Pomoću tog izomorfizma je u danim bazama uspostavljena korespondencija

$$\begin{aligned} f+g &\mapsto F+G\,,\\ \lambda f &\mapsto \lambda F\,,\\ fg &\mapsto FG\,, \end{aligned}$$

koja potpunije objašnjava izreku da su linearni operatori reprezentirani svojim matricama.

Kako smo vidjeli (Kor. 2 u 10.3.), izomorfizam linearnih prostora ima za matrični zapis regularnu matricu. Zato se automorfizam $f : V \to V$ zove i regularni operator. Kako znamo (Zad. 8. u 8.4.), skup

$$\operatorname{Aut} V$$

svih regularnih operatora čini multiplikativnu grupu. Iz te činjenice i Tm. 2 slijedi

PROPOZICIJA 3

Grupa $\operatorname{Aut} V$ *je izomorfna s* $GL(n, F)$. ■

Zbog toga identificiramo $\operatorname{Aut} V = GL(n, F)$, pa i grupu regularnih operatora često zovemo opća linearna grupa.

ZADACI

1. Dokaži: Ako je F matrični zapis regularnog operatora f, onda je F^{-1} matrica njegova inverza f^{-1}. Je li tvrdnja istinita ako je f izomorfizam $f : U \to V$?

2. Neka su $f : U \to V$ i $g : V \to W$ linearni operatori, F matrica od f u paru baza (A, B), a G matrica od g u paru baza (B, C). Pokaži da je GF matrica operatora gf u paru baza (A, C).

3. Putem izomorfizma Φ se pojmovi iz teorije linearnih operatora prevode u teoriju matrica i obratno. Ilustriraj to primjerima! Što su npr. slični operatori?

10.5. Odnos matričnih zapisa istog operatora

Neka je

$$f : U \to V$$

linearni operator, F matrica tog operatora u paru baza (A, B), a F' matrica istog operatora u paru baza (A', B'). Pitamo se u kojem su odnosu matrice F i F', tj. u kojoj su relaciji matrični zapisi istog linearnog operatora u različitim parovima baza. Odgovor daje ovaj

TEOREM 1

Neka su F i F' matrice operatora f u paru baza (A, B), odnosno (A', B'). Onda je

$$F' = T^{-1}FS\,,$$

gdje je S matrica prijelaza $A \to A'$, a T matrica prijelaza $B \to B'$.

Dokaz

Neka je $a \in U$ bilo koji vektor, X i X' koordinatne matrice tog vektora u bazama A, odnosno A' prostora U, a Y i Y' koordinatne matrice njegove slike $f(a) \in V$ u bazama B, odnosno B' prostora V. Onda je prema Prop. 3 iz 10.3.

$$Y = FX, \tag{1}$$

odnosno

$$Y' = F'X'. \tag{2}$$

Nadalje, kako je S matrica transformacije baza u prostoru U, prema Tm. 1 u 10.2. imamo

$$X = SX', \tag{3}$$

a jer je T matrica transformacije baza u prostoru V, vrijedi i

$$Y = TY'. \tag{4}$$

Primjenjujući redom relacije (2), (4), (1), odnosno (3), onda imamo

$$F'X' = Y' = T^{-1}Y = T^{-1}FX = T^{-1}FSX' = (T^{-1}FS)X'.$$

Kako je to istina za svaki $X' \in M_{n1}$, na temelju Leme 1 u 10.4. zaključujemo da je

$$F' = T^{-1}FS,$$

što je trebalo dokazati. ■

Ako sada pogledamo Zad. 10. u 9.6., u kojem je dana alternativna definicija ekvivalencije matrica, iz Tm. 1 odmah razabiremo

KOROLAR 2

Matrični zapisi F i F' istog linearnog operatora u različitim parovima baza su ekvivalentne matrice, $F' \sim F$. ■

Razmotrimo još specijalni slučaj kad je $U = V$, dakle $f : V \to V$. Prema Tm. 1 će onda matrice F i F' tog operatora u bazama B, odnosno B', biti vezane relacijom

$$F' = T^{-1}FT. \tag{5}$$

Neka su sada $A, B \in M_n$ kvadratne matrice istog reda. Kažemo da je matrica A **slična** matrici B, i pišemo $A \simeq B$, ako postoji regularna matrica $T \in M_n$ takva da je $B = T^{-1}AT$. U tom slučaju kažemo da T provodi **sprezanje** matrica A i B. Sličnost matrica je relacija ekvivalencije na skupu M_n (vidi Zad. 16. u 9.5.).

Kako je matrica prijelaza jedne baze u drugu uvijek regularna, iz (5) čitamo

KOROLAR 3

Matrični zapisi F i F' istog linearnog operatora $f : V \to V$ u različitim bazama prostora V su slične matrice, $F' \simeq F$. ■

ZADACI

1. Uz koji će uvjet operator $f : V \to V$ imati isti zapis u različitim bazama?

2. Neka su F i F' slične matrice. Postoji li nužno linearni operator za koji su F i F' matrični prikazi (u raznim bazama)?

10.6. Karakteristični polinom. Hamilton–Cayleyjev teorem

Već smo se sreli s nekim karakteristikama linearnog operatora, kao što su njegov rang i defekt. Sada ćemo upoznati neke daljnje **invarijante linearnog operatora**, tj. svojstva koja se mogu pročitati iz matričnog prikaza operatora, ali o tom prikazu (tj. o izboru koordinatnog sustava) zapravo ne ovise. Zbog Kor. 3 u 10.5. problem gledamo matrično, što znači da će nas interesirati zajednička svojstva neke klase sličnih matrica, tzv. **invarijante sličnosti**.

Neka je A kvadratna matrica reda n nad poljem F. Onda matricu

$$C = A - \lambda E\,,$$

gdje je λ varijabilni parametar, a E jedinična matrica, nazivamo **karakteristična matrica** ili, također, **svojstvena matrica** za matricu A. Ako je $A = [\alpha_{ik}]$, njezina karakteristična matrica je oblika

$$C = \begin{bmatrix} \alpha_{11} - \lambda & \alpha_{12} & \cdots & \alpha_{1n} \\ \alpha_{21} & \alpha_{22} - \lambda & \cdots & \alpha_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_{n1} & \alpha_{n2} & \cdots & \alpha_{nn} - \lambda \end{bmatrix} .$$

Determinanta matrice C,

$$\det C = \det(A - \lambda E) = |A - \lambda E| ,$$

očito je polinom n-tog stupnja u varijabli λ, s koeficijentima iz polja F,

$$k_A(\lambda) = k_n\lambda^n + k_{n-1}\lambda^{n-1} + \cdots + k_0 , \quad k_i \in F ,$$

koji nazivamo **karakteristični** ili **svojstveni polinom** matrice A. Konačno, pripadnu jednadžbu

$$k_A(\lambda) = 0$$

nazivamo **karakteristična** ili **svojstvena jednadžba** za matricu A. Na primjer, za matricu $A = \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}$ je njezin karakteristični polinom

$$k_A(\lambda) = \begin{vmatrix} 1 - \lambda & 2 \\ 3 & 4 - \lambda \end{vmatrix} = \lambda^2 - 5\lambda - 2 .$$

Razvijanjem $\det C$ lako se provjeri da vrijedi

PROPOZICIJA 1

U karakterističnom polinomu matrice A su koeficijenti:

$$k_n = (-1)^n , \quad k_{n-1} = (-1)^{n-1}\mathrm{tr}\ A , \quad k_0 = \det A .$$

■

Karakteristični polinom je invarijantni pojam za slične matrice.

PROPOZICIJA 2

Slične matrice imaju isti karakteristični polinom.

Dokaz

Neka su A i B slične matrice, a T regularna matrica koja provodi njihovo sprezanje, $B = T^{-1}AT$. Onda imamo, koristeći se Binet–Cauchyjevim teoremom,

$$\begin{aligned} k_B(\lambda) &= \det(B - \lambda E) = \det[T^{-1}AT - \lambda(T^{-1}T)] = \\ &= \det[T^{-1}AT - T^{-1}(\lambda E)T] = \det[T^{-1}(A - \lambda E)T] = \\ &= \det T^{-1} \cdot \det(A - \lambda E) \cdot \det T = \det T^{-1} \cdot \det T \cdot \det(A - \lambda E) = \\ &= \det(T^{-1}T) \cdot \det(A - \lambda E) = \det E \cdot \det(A - \lambda E) = \\ &= \det(A - \lambda E) = k_A(\lambda) , \end{aligned}$$

i tvrdnja je dokazana. ■

Neka je sada $f : V \to V$ bilo koji linearni operator koji djeluje na prostoru V. Onda definiramo **karakteristični** ili **svojstveni polinom** k_f tog **operatora** s

$$k_f(\lambda) = k_F(\lambda) ,$$

gdje je F bilo koji matrični prikaz operatora f. Na osnovi Kor. 3 iz 10.5. i Prop. 2 odmah zaključujemo da je karakteristični polinom operatora dobro definiran pojam, tj. neovisan o matričnoj reprezentaciji tog operatora (o izboru koordinatnog sustava).

Isto tako, za operator f definiramo njegov **trag** $\operatorname{tr} f$ i **determinantu** $\det f$ s

$$\operatorname{tr} f = \operatorname{tr} F ,$$

$$\det f = \det F ,$$

gdje je opet F neka matrica operatora f. Kako su trag i determinanta matrice F koeficijenti u njezinu karakterističnom polinomu (Prop. 1), a time i u karakterističnom polinomu operatora f, $\operatorname{tr} f$ i $\det f$ su dobro definirane karakteristike operatora, tj. neovisne o njegovu matričnom prikazu.

Osim ranga i defekta, karakteristični polinom k_f, te skalari $\operatorname{tr} f$ i $\det f$ su važne invarijante operatora, koje nam daju bitne informacije o njegovoj naravi.

Pokazat ćemo, na kraju, interesantnu vezu koja postoji između matrice (operatora) i njezina (njegova) karakterističnog polinoma. Najprije nekoliko napomena. Neka je

$$p(\lambda) = \alpha_n\lambda^n + \alpha_{n-1}\lambda^{n-1} + \cdots + \alpha_0$$

bilo koji polinom u varijabli λ, s koeficijentima iz polja F. Ako je A kvadratna matrica s elementima iz polja F, onda pod $p(A)$ podrazumijevamo **matricu**

$$p(A) = \alpha_n A^n + \alpha_{n-1} A^{n-1} + \cdots + \alpha_0 E \, .$$

Primijetimo da smo slobodni član α_0 u polinomu zamijenili s $\alpha_0 E$, kako bi svaki član u $p(A)$ bio matrica. S **matričnim polinomima** tog tipa nema posebnih problema jer potencije dane matrice komutiraju međusobno. Takvi se polinomi npr. zbrajaju i množe na uobičajeni način. Nadalje, svaki identitet koji vrijedi za polinome u jednoj varijabli ostaje istinit ako varijablu zamijenimo matricom. Na primjer, iz $\lambda^2 - 1 = (\lambda + 1)(\lambda - 1)$ slijedi da je

$$A^2 - E = (A + E)(A - E) \, ,$$

za svaku kvadratnu matricu A. Poteškoće, međutim, nastupaju kod matričnih polinoma u više varijabli (jer množenje matrica nije komutativno).

Ako je $A \in M_n(F)$ bilo koja matrica, onda uvijek postoji polinom $p(\lambda)$, s koeficijentima iz polja F, koji matrica A poništava, tj. za koji vrijedi

$$p(A) = O \, ,$$

gdje je na desnoj strani, naravno, nulmatrica. Kako, naime, znamo, M_n je linearni prostor nad poljem F i $\dim M_n = n^2$. Promatrajmo $n^2 + 1$ vektora u tom prostoru:

$$E, A, A^2, \ldots, A^n, \ldots, A^{n^2} \, .$$

Oni su, dakako, linearno zavisni (jer ih ima $n^2 + 1$) pa postoje skalari $\lambda_i \in F$ koji nisu svi jednaki nuli, tako da vrijedi

$$\alpha_0 E + \alpha_1 A + \cdots + \alpha_n A^n + \cdots + \alpha_{n^2} A^{n^2} = O \, .$$

No, ta relacija upravo pokazuje da matrica A poništava polinom

$$p(\lambda) = \alpha_0 + \alpha_1 \lambda + \cdots + \alpha_{n^2} \lambda^{n^2} \, ,$$

s koeficijentima iz polja F.

Interesantno je, međutim, da se stupanj polinoma kojeg poništava dana matrica može znatno sniziti. Vrijedi, naime, ovaj čuveni

TEOREM 3 (Hamilton-Cayley)

Svaka kvadratna matrica A poništava svoj karakteristični polinom, tj. vrijedi

$$k_A(A) = O \, .$$

Dokaz

Primijetimo najprije da treba biti vrlo oprezan u zaključivanju, da ne bismo upali u sljedeću standardnu grešku: kako je $k_A(\lambda) = \det(A - \lambda E)$, to je $k_A(A) = \det(A - AE) = \det(A - A) = \det O = 0$ i dokaz je gotov. Naravno, argumentacija nije ispravna jer se u računanju determinante, λ mora shvaćati kao skalar, a ne kao matrica.

Prijeđimo sada na dokaz teorema. Neka je $A = [\alpha_{ik}]$ bilo koja kvadratna matrica reda n, nad poljem F. Treba dokazati da je

$$k_n A^n + k_{n-1} A^{n-1} + \cdots + k_0 E = O \,,$$

gdje su, dakako, k_i koeficijenti iz karakterističnog polinoma matrice A. Za karakterističnu matricu $C = A - \lambda E$ od A promatrajmo njezinu adjunktu $\tilde{C} = [C_{ki}]$. Njezini će elementi biti polinomi u λ, čiji stupanj ne premašuje $n - 1$, jer npr. imamo

$$C_{11} = \begin{vmatrix} \alpha_{22} - \lambda & \cdots & \alpha_{2n} \\ \vdots & & \vdots \\ \alpha_{n2} & \cdots & \alpha_{nn} - \lambda \end{vmatrix} = \gamma_{n-1}\lambda^{n-1} + \cdots + \gamma_0 = p_{11}(\lambda) \,.$$

Prema tome je adjunkta oblika

$$\tilde{C} = \begin{bmatrix} p_{11}(\lambda) & \cdots & p_{n1}(\lambda) \\ \vdots & \ddots & \vdots \\ p_{1n}(\lambda) & \cdots & p_{nn}(\lambda) \end{bmatrix} \,,$$

gdje su elementi $p_{ik}(\lambda)$ polinomi, i $\operatorname{st} p_{ik} \leq n - 1$. Nije se teško uvjeriti da je takvu matricu moguće prikazati kao polinom u λ s matričnim koeficijentima, čiji je stupanj najviše $n - 1$ (vidi Zad. 6.), tj. u obliku

$$\tilde{C} = C_{n-1}\lambda^{n-1} + C_{n-2}\lambda^{n-2} + \cdots + C_1\lambda + C_0 \,, \tag{1}$$

gdje su C_i, $i = n - 1, ..., 0$, matrice reda n, s elementima iz polja F. Imamo sada

$$C\tilde{C} = (A - \lambda E)\tilde{C} = A\tilde{C} - \lambda\tilde{C} \,, \tag{2}$$

a u drugu ruku, zbog Prop. 5 u 9.9.,

$$C\tilde{C} = (\det C)E = k_A(\lambda)E \,, \tag{3}$$

pa uspoređivanjem (2) i (3) dolazimo do relacije

$$k_A(\lambda)E = A\tilde{C} - \lambda\tilde{C} \,. \tag{4}$$

Ako sada u (4) uzmemo u obzir eksplicitni prikaz karakterističnog polinoma, kao i relaciju (1), imamo

$$\begin{aligned} & k_n E\lambda^n + k_{n-1}E\lambda^{n-1} + \cdots + k_1 E\lambda + k_0 E = \\ & = AC_{n-1}\lambda^{n-1} + AC_{n-2}\lambda^{n-2} + \cdots + AC_1\lambda + AC_0 - \\ & -C_{n-1}\lambda^n - C_{n-2}\lambda^{n-1} - \cdots - C_1\lambda^2 - C_0\lambda \ . \end{aligned} \tag{5}$$

No, izrazi na obje strane ove jednakosti su polinomi u λ s matricama kao koeficijentima, a takvi su polinomi jednaki onda i samo onda ako su im korespondentni koeficijenti jednaki. Prema tome je (5) ekvivalentno sa sljedećim nizom matričnih jednakosti:

$$\left.\begin{array}{rcr} k_n E & = & -C_{n-1} \\ k_{n-1}E & = & AC_{n-1} - C_{n-2} \\ \vdots & & \\ k_1 E & = & AC_1 - C_0 \\ k_0 E & = & AC_0 \end{array}\right\} \ . \tag{6}$$

Ako prvu od jednadžbi (6) pomnožimo slijeva s A^n , drugu s A^{n-1}, itd. i konačno predzadnju s A i zadnju s E, dobivamo (zbog $A^j(k_j E) = k_j A^j$, jer je k_j skalar)

$$\left.\begin{array}{rcr} k_n A^n & = & -A^n C_{n-1} \\ k_{n-1}A^{n-1} & = & A^n C_{n-1} - A^{n-1}C_{n-2} \\ \vdots & & \\ k_1 A & = & A^2 C_1 - AC_0 \\ k_0 E & = & AC_0 \end{array}\right\} \ . \tag{7}$$

Sada sve jednadžbe u (7) zbrojimo. Odmah razabiremo da će se članovi na desnoj strani ukinuti, pa ostaje

$$k_n A^n + k_{n-1}A^{n-1} + \cdots + k_1 A + k_0 E = O \ ,$$

dakle

$$k_A(A) = O \ ,$$

i teorem je dokazan. ■

ZADACI

1. Dokaži direktno: Slične matrice imaju isti trag i istu determinantu. [Uputa: Koristi se činjenicom da je $\operatorname{tr} AB = \operatorname{tr} BA$, odnosno Binet–Cauchyjevim teoremom.]

2. Dokaži: Za skalarnu matricu $A = \alpha E$ je karakteristični polinom

$$k_A(\lambda) = (\alpha - \lambda)^n ,$$

gdje je n red od A.

3. Za matricu $A = \begin{bmatrix} 1 & -1 \\ 2 & -1 \end{bmatrix}$ nađi karakterističnu jednadžbu, pa pokaži direktnim računom da je matrica A zadovoljava.

4. **Polinomi s matričnim koeficijentima** su izrazi oblika

$$A_m\lambda^m + A_{m-1}\lambda^{m-1} + \cdots + A_0 ,$$

gdje su koeficijenti A_i matrice istog reda, s elementima iz danog polja, a varijabla λ se ponaša kao skalar (tj. njezine potencije komutiraju s koeficijentima). Takvi se polinomi mogu zbrajati i množiti na uobičajen način, s tim da je važan poredak faktora pri množenju, jer koeficijenti ne moraju komutirati. Pokaži, da polinomi tog tipa čine algebru. Pokaži nadalje, da su dva polinoma s matričnim koeficijentima jednaka onda i samo onda, ako su im korespondentni koeficijenti jednaki.

5. Pod **polinomskom matricom** podrazumijevamo matricu

$$[p_{ik}(\lambda)]$$

u kojoj su elementi polinomi u varijabli λ, s koeficijentima iz polja F. Neka je K skup svih racionalnih funkcija u λ, tj. skup svih dopustivih kvocijenata polinoma u varijabli λ, s koeficijentima iz polja F. Pokaži da je K također polje. Prema tome je polinomska matrica dobro definiran pojam, kao specijalni slučaj matrice nad poljem K.

6. Pokaži da se svaki polinom s matričnim koeficijentima može prikazati kao jedna jedina polinomska matrica, i obratno, da se svaka polinomska matrica može razviti u polinom s matričnim koeficijentima. Na primjer,

$$\begin{bmatrix} 1 & 2 \\ 2 & 1 \end{bmatrix}\lambda^2 + \begin{bmatrix} 0 & 1 \\ -1 & 2 \end{bmatrix}\lambda + \begin{bmatrix} 3 & 1 \\ 1 & 3 \end{bmatrix} = \begin{bmatrix} \lambda^2+3 & 2\lambda^2+\lambda+1 \\ 2\lambda^2-\lambda+1 & \lambda^2+2\lambda+3 \end{bmatrix} .$$

10.7. Minimalni polinom

Sada ćemo definirati još jednu važnu invarijantu linearnih operatora. Neka je A kvadratna matrica nad poljem F. Neka je

$$m_A(\lambda)$$

polinom najnižeg stupnja u varijabli λ, s koeficijentima iz polja F, koji matrica A poništava, tj. za koji vrijedi

$$m_A(A) = O\,.$$

Onda kažemo da je m_A jedan **minimalni polinom** za matricu A, a pripadnu jednadžbu

$$m_A(\lambda) = 0$$

nazivamo **minimalna jednadžba** matrice A.

Kako prema Hamilton–Cayleyjevu teoremu matrica A poništava svoj karakteristični polinom, to stupanj minimalnog polinoma nije veći od reda n matrice A,

$$\operatorname{st} m_A \leq n = \operatorname{st} k_A\,.$$

Ako je npr. $A = \alpha E$, onda je $k_A(\lambda) = (\alpha - \lambda)^n$, a $m_A(\lambda) = \alpha - \lambda$.

Neka je $p(\lambda)$ bilo koji polinom s koeficijentima iz polja F, koji matrica A poništava, tj.

$$p(A) = O\,.$$

Onda vrijedi

PROPOZICIJA 1

Polinom $p(\lambda)$ je djeljiv sa svakim minimalnim polinomom $m(\lambda)$ matrice A.

Dokaz

Dijeleći polinom $p(\lambda)$ polinomom $m(\lambda)$, jer je po definiciji minimalnog polinoma $\operatorname{st} p \geq \operatorname{st} m$, vidimo da $p(\lambda)$ možemo prikazati kao

$$p(\lambda) = m(\lambda) \cdot q(\lambda) + r(\lambda)\,,$$

gdje je $q(\lambda)$ kvocijentni polinom, a $r(\lambda)$ ostatak koji je ili identički jednak nuli ili je polinom čiji je stupanj manji od stupnja polinoma $m(\lambda)$.

Kako je po pretpostavci $p(A) = O$, imamo

$$p(A) = O = m(A) \cdot q(A) + r(A)\,,$$

a odatle zbog $m(A) = O$ slijedi da je $r(A) = O$. No, to je u kontradikciji s minimalnošću polinoma $m(\lambda)$, osim u slučaju kad je $r(\lambda) \equiv 0$, čime je tvrdnja dokazana. ■

KOROLAR 2

Karakteristični polinom matrice djeljiv je njezinim minimalnim polinomom. ■

Ako je $m_A(\lambda)$ minimalni polinom od A, onda je jasno da je i $\alpha m_A(\lambda)$, $\alpha \neq 0$, minimalni polinom za tu matricu. Vrijedi, međutim i više.

KOROLAR 3

Minimalni polinom dane matrice je jedinstven do na skalarni faktor različit od nule. Drugim riječima, ako su $m_1(\lambda)$ i $m_2(\lambda)$ minimalni polinomi iste matrice, onda postoji $\alpha \in F$, $\alpha \neq 0$, takav da je

$$m_2(\lambda) = \alpha m_1(\lambda) .$$

Dokaz

Neposredno iz činjenice da je $\operatorname{st} m_1 = \operatorname{st} m_2$ i Prop. 1. ■

Pokažimo sada invarijantnost minimalnog polinoma.

PROPOZICIJA 4

Slične matrice imaju iste minimalne polinome.

Dokaz

Neka su A i B slične matrice, $B = T^{-1}AT$. Neka su $m_A(\lambda)$ i $m_B(\lambda)$ minimalni polinomi za te matrice i neka je

$$m_A(\lambda) = \alpha_m \lambda^m + \alpha_{m-1}\lambda^{m-1} + \cdots + \alpha_0 .$$

Lako se vidi da vrijedi

$$B^j = (T^{-1}AT)^j = T^{-1}A^jT ,$$

za svaki $j = 0, ..., m$. Onda imamo

$$\begin{aligned} m_A(B) &= \alpha_m(T^{-1}AT)^m + \alpha_{m-1}(T^{-1}AT)^{m-1} + \cdots + \alpha_0 E = \\ &= T^{-1}(\alpha_m A^m)T + T^{-1}(\alpha_{m-1}A^{m-1})T + \cdots + T^{-1}(\alpha_0 E)T = \\ &= T^{-1}(\alpha_m A^m + \cdots + \alpha_0 E)T = T^{-1}\underbrace{m_A(A)}_{=O}T = O , \end{aligned}$$

tj. B poništava minimalni polinom od A. Odatle slijedi da je

$$\operatorname{st} m_B \leq \operatorname{st} m_A .$$

Posve analogno, polazeći od $A = TBT^{-1}$, vidimo da je

$$\operatorname{st} m_A \leq \operatorname{st} m_B ,$$

pa zaključujemo da je

$$\operatorname{st} m_B = \operatorname{st} m_A .$$

U drugu ruku, jer je $m_A(B) = O$, po Prop. 1 slijedi da je

$$\frac{m_A(\lambda)}{m_B(\lambda)} = q(\lambda) ,$$

a kako su polinomi $m_A(\lambda)$ i $m_B(\lambda)$ istog stupnja, mora biti

$$q(\lambda) = \text{konst.} = \alpha \neq 0$$

pa je

$$m_A(\lambda) = \alpha m_B(\lambda) ,$$

što se i tvrdilo. ■

Propozicija nam omogućuje uvođenje pojma minimalnog polinoma na razini operatora. Za linearni operator $f : V \to V$ definiramo **minimalni polinom** m_f tog **operatora** s

$$m_f(\lambda) = m_F(\lambda) ,$$

gdje je F bilo koji matrični zapis operatora f. Zbog Prop. 4, to je dobro definiran pojam, neovisan o izboru koordinatnog sustava (tj. matrice operatora).

Postavlja se pitanje kako efektivno izračunati minimalni polinom za danu matricu (operator). Kako smo vidjeli (dokaz Tm. 3. u 10.6.), adjunkta karakteristične matrice $C = A - \lambda E$ je oblika

$$\tilde{C} = [p_{ki}(\lambda)] ,$$

tj. njezini su elementi polinomi u λ, čiji stupanj ne premašuje $n-1$, $\text{st} p_{ik} \leq n-1$. Neka je s

$$q_A(\lambda)$$

označen polinom koji je najveći zajednički divizor svih elemenata (polinoma!) matrice $\tilde{C}$. Jasno je da je

$$\text{st}\, q_A(\lambda) \leq n - 1 ,$$

gdje je n red matrice A.

PROPOZICIJA 5

Polinom $q_A(\lambda)$ dijeli karakteristični polinom $k_A(\lambda)$.

Dokaz

Neka je $\tilde{C} = q_A(\lambda) \cdot B$. Onda iz $\tilde{C}C = k_A(\lambda)E$ slijedi

$$BC = \frac{k_A(\lambda)}{q_A(\lambda)} \cdot E \,,$$

pa kako je lijeva strana u toj jednakosti polinomska matrica, kao produkt polinomskih matrica B i C, takva mora biti i desna strana, pa polinom $k_A(\lambda)$ mora biti djeljiv sa $q_A(\lambda)$. ■

Sada smo u mogućnosti dokazati ovaj

TEOREM 6

Polinom $h(\lambda) = k_A(\lambda)/q_A(\lambda)$ je minimalni polinom za matricu A.

Dokaz

Već znamo da možemo pisati $\tilde{C} = q_A(\lambda) \cdot B$, gdje u matrici B elementi (polinomi!) nemaju više zajednički divizor, pa imamo

$$BC = h(\lambda)E \,.$$

Promatrajući matricu B umjesto $\tilde{C}$ i koristeći se potpuno istom argumentacijom kao u dokazu Hamilton – Cayleyjeva teorema, lako se provjeri da vrijedi

$$h(A) = O \,.$$

U drugu ruku, neka je

$$m_A(\lambda) = \alpha_m \lambda^m + \alpha_{m-1}\lambda^{m-1} + \cdots + \alpha_1 \lambda + \alpha_0$$

minimalni polinom matrice A. Promatrajmo polinom

$$m_A(\lambda) - m_A(\mu) = \alpha_m(\lambda^m - \mu^m) + \cdots + \alpha_1(\lambda - \mu) \,.$$

Kako su članovi u tom polinomu oblika

$$\alpha_j(\lambda^j - \mu^j) \,,$$

svaki od njih je djeljiv s $\mu - \lambda$ pa možemo pisati

$$m_A(\lambda) - m_A(\mu) = (\mu - \lambda)\, p(\lambda, \mu) \,,$$

gdje je $p(\lambda, \mu)$ neki polinom u λ i μ. Ako zamijenimo λ matricom λE, a μ matricom A, dobivamo

$$m_A(\lambda E) - m_A(A) = (A - \lambda E)\, p(\lambda E, A) \,,$$

odnosno, jer je $m_A(A) = O$ i $m_A(\lambda E) = m_A(\lambda)E$,

$$m_A(\lambda) \cdot E = C\, p(\lambda E, A) \,.$$

Množeći tu jednakost slijeva s $\tilde{C}$, onda imamo

$$m_A(\lambda)\tilde{C} = \tilde{C}C\, p(\lambda E, A) = k_A(\lambda)\, p(\lambda E, A) \,.$$

Kako je $\tilde{C} = q_A(\lambda)B$, a $k_A(\lambda) = q_A(\lambda)\, h(\lambda)$, iz prethodne relacije slijedi

$$m_A(\lambda)q_A(\lambda)B = q_A(\lambda)\, h(\lambda)\, p(\lambda E, A) \,,$$

ili, nakon skraćivanja,

$$m_A(\lambda)B = h(\lambda)\, p(\lambda E, A) \,.$$

Konačno, jer je $p(\lambda E, A)$ polinomska matrica, $h(\lambda)$ mora dijeliti svaki element matrice $m_A(\lambda)B$. Međutim, po pretpostavci elementi od B nemaju zajednički divizor. Odavde slijedi da $h(\lambda)$ dijeli $m_A(\lambda)$, pa je $\operatorname{st} h \leq \operatorname{st} m_A$. Pokazali smo, međutim, da je $h(A) = O$, odakle zaključujemo da je $h(\lambda)$ također minimalni polinom za A i da je (Kor. 3)

$$h(\lambda) = \alpha m_A(\lambda) \,. \qquad \blacksquare$$

PRIMJER

Nađimo minimalni polinom za matricu

$$A = \begin{bmatrix} 7 & 4 & -4 \\ 4 & -8 & -1 \\ -4 & -1 & -8 \end{bmatrix} \,.$$

Imamo

$$\begin{aligned} k_A(\lambda) &= \det C = \det \begin{bmatrix} 7-\lambda & 4 & -4 \\ 4 & -8-\lambda & -1 \\ -4 & -1 & -8-\lambda \end{bmatrix} = \\ &= -\lambda^3 - 9\lambda^2 + 81\lambda + 729 \,. \end{aligned}$$

Nadalje,

$$\begin{aligned} \tilde{C} &= \begin{bmatrix} (\lambda+7)(\lambda+9) & 4(\lambda+9) & -4(\lambda+9) \\ 4(\lambda+9) & (\lambda-8)(\lambda+9) & -(\lambda+9) \\ -4(\lambda+9) & -(\lambda+9) & (\lambda-8)(\lambda+9) \end{bmatrix} = \\ &= (\lambda+9) \begin{bmatrix} \lambda+7 & 4 & -4 \\ 4 & \lambda-8 & -1 \\ -4 & -1 & \lambda-8 \end{bmatrix} \,, \end{aligned}$$

pa je $q_A(\lambda) = \lambda + 9$. Odatle je

$$m_A(\lambda) = \frac{k_A(\lambda)}{q_A(\lambda)} = \frac{-\lambda^2(\lambda+9) + 81(\lambda+9)}{\lambda+9} = -\lambda^2 + 81 \ .$$

Za polinom $p(\lambda)$, s koeficijentima iz polja F, kažemo da je **reducibilan** s obzirom na to polje ako ga je moguće prikazati u obliku

$$p(\lambda) = a(\lambda)\, b(\lambda) \ ,$$

gdje su $a(\lambda)$ i $b(\lambda)$ polinomi s koeficijentima iz F, i svaki od njih je stupnja manjeg nego što je stupanj od $p(\lambda)$. Za polinom koji nije reducibilan kažemo da je **ireducibilan** s obzirom na dano polje. Na primjer, svaki je linearni polinom ireducibilan. Polinom $\lambda^2 + 1$ je ireducibilan u odnosu na polje realnih brojeva, ali je reducibilan s obzirom na polje kompleksnih brojeva. Polinomi $\lambda^2 - 1$ i $(\lambda - 1)^3$ su, dakako, reducibilni. Vrijedi

PROPOZICIJA 7

Svaki ireducibilni faktor karakterističnog polinoma neke matrice je također ireducibilni faktor minimalnog polinoma te matrice.

Dokaz

U dokazu Tm. 6 smo za matricu A imali relaciju

$$m_A(\lambda) \cdot E = C \cdot p(\lambda E, A) \ .$$

Uzimanjem determinante, zbog Binet–Cauchyjeva teorema dobivamo

$$\det\,[m_A(\lambda)E] = \det C \det p(\lambda E, A) \ ,$$

odnosno

$$[m_A(\lambda)]^n = k_A(\lambda) \det p(\lambda E, A) \ ,$$

gdje je n red matrice A. Odatle je

$$\frac{[m_A(\lambda)]^n}{k_A(\lambda)} = \det p(\lambda E, A) \ ,$$

i pritom je $\det p(\lambda E, A)$ polinom, iz čega zaključujemo da svaki ireducibilni faktor od $k_A(\lambda)$ mora dijeliti $[m_A(\lambda)]^n$, pa onda i $m_A(\lambda)$. ■

Na primjer, u našem primjeru smo imali

$$\begin{aligned} k_A(\lambda) &= -(\lambda+9)^2(\lambda-9) \ , \\ m_A(\lambda) &= -(\lambda+9)(\lambda-9) \ . \end{aligned}$$

KOROLAR 8

Ako u karakterističnom polinomu nema istih (ireducibilnih) faktora, taj se polinom podudara s minimalnim polinomom matrice.

Dokaz

Neposredno iz Prop. 7 i minimalnosti. ■

Pokazuje se da upravo slučaj u kojemu karakteristični polinom ima više istih faktora izaziva poteškoće.

ZADACI

1. Pokaži da nema realne matrice reda 3 koja bi zadovoljavala jednadžbu $\lambda^2 + 1 = 0$, ali postoje kompleksne matrice s tim svojstvom. Pokaži, također, da postoje realne matrice reda 2 koje zadovoljavaju navedenu jednadžbu.

2. Nađi matricu drugog reda s cjelobrojnim elementima koja zadovoljava jednadžbu $\lambda^3 - 1 = 0$, ali ne zadovoljava jednadžbu $\lambda - 1 = 0$.

3. Neka je
$$p(\lambda) = (-1)^n \lambda^n + \alpha_{n-1}\lambda^{n-1} + \cdots + \alpha_0$$
bilo koji polinom s koeficijentima iz polja F. Pokaži da uvijek postoji matrica A reda n nad poljem F, za koju je $p(\lambda)$ minimalni polinom, i da je to matrica
$$A = \begin{bmatrix} 0 & 0 & \dots & 0 & -(-1)^n\alpha_0 \\ 1 & 0 & \cdots & 0 & -(-1)^n\alpha_1 \\ 0 & 1 & \cdots & 0 & -(-1)^n\alpha_2 \\ \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & -(-1)^n\alpha_{n-1} \end{bmatrix}.$$
Nađi matricu za koju je $p(\lambda) = \lambda^4 + 3\lambda^3 + 2\lambda^2 - \lambda + 6 = 0$ minimalna jednadžba.

4. Pokaži da se karakteristična matrica matrice A može elementarnim transformacijama (vidi 9.6) prevesti u oblik
$$\begin{bmatrix} p_1(\lambda) & 0 & \cdots & 0 \\ 0 & p_2(\lambda) & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & p_n(\lambda) \end{bmatrix},$$

gdje su $p_i(\lambda)$ polinomi sa svojstvom da $p_i(\lambda)$ dijeli $p_{i+1}(\lambda)$, za svaki $i = 1, ..., n-1$. Pokaži, nadalje, da je onda

$$k_A(\lambda) = \pm p_1(\lambda) \cdot p_2(\lambda) \cdot \ldots \cdot p_n(\lambda)$$

i da je

$$m_A(\lambda) = p_n(\lambda) .$$

Služeći se tim algoritmom, nađi ponovno minimalni i karakteristični polinom za matricu iz primjera u tekstu.

5. Ako su A i B kvadratne matrice istog reda, pokaži da matrice AB i BA imaju isti karakteristični polinom.

6. Za operator $f : V \dashrightarrow V$ kažemo da je **nilpotentan**, ako je njegov minimalni polinom oblika $m_f(\lambda) = \lambda^k$, gdje je $k \in \mathbb{N}$ tzv. **indeks operatora** f. Dokaži da je onda $f^k = n =$ nuloperator, a $f^{k-1} \neq n$. Dokaži, nadalje, da je za takav operator

$$k_f(\lambda) = \lambda^m ,$$

gdje je $m = \dim V$.

7. Dokaži: Neka su $f, g : V \to V$ nilpotentni operatori i $fg = gf$. Onda su $f + g$ i fg nilpotentni.

8. Dokaži da je trag nilpotentnog operatora uvijek jednak 0.

10.8. Invarijantni potprostori

Neka je $f : V \dashrightarrow V$ linearni operator, i $L < V$ potprostor od V sa svojstvom da je

$$f(a) \in L ,$$

za svaki vektor $a \in L$, tj. da vrijedi

$$f(L) \subset L .$$

Onda kažemo da je L **invarijantni potprostor** s obzirom na operator f ili, kraće, da je L **f-invarijantan** potprostor od V. Restrikcija

$$\bar{f} = f/L$$

je u tom slučaju linearni operator

$$\bar{f} : L \dashrightarrow L$$

koji djeluje na prostoru L i za koji kažemo da je **induciran** operatorom f.

Očigledno, za svaki linearni operator postoje invarijantni potprostori. Trivijalni su $L = V$ i $L = \{\Theta\}$. Ako operator posjeduje i netrivijalne invarijantne potprostore, za njega kažemo da je **reducibilan**.

Može se dogoditi da operator f dopušta više invarijantnih potprostora. Posebno je interesantan slučaj kad su $L, M < V$ invarijantni potprostori za operator f i pritom vrijedi

$$L \oplus M = V .$$

U tom slučaju vrijedi

PROPOZICIJA 1

Linearni operator je potpuno određen operatorima koje inducira na direktnim sumandima prostora V.

Dokaz

Neka su $f_1 = f/L$ i $f_2 = f/M$ operatori na invarijantnim potprostorima L i M, inducirani operatorom f. Kako je $V = L \oplus M$, za bilo koji $x \in V$ imamo jedinstveni prikaz

$$x = a + b , \quad a \in L , b \in M .$$

Onda je

$$f(x) = f(a+b) = f(a) + f(b) = f_1(a) + f_2(b)$$

i tvrdnja je dokazana. ■

Prema tome, ako su f_1 i f_2 ma koji linearni operatori koji djeluju na direktnim sumandima L, odnosno M, prostora V, onda je jednoznačno određen linearni operator $f : V \to V$, sa svojstvom da je $f/L = f_1$ i $f/M = f_2$. U tom slučaju kažemo da je operator f **direktna suma operatora** f_1 i f_2 (s obzirom na rastav $V = L \oplus M$), i pišemo

$$f = f_1 \oplus f_2 .$$

Operator f koji posjeduje netrivijalne invarijantne potprostore čija je suma cijeli prostor, naziva se **potpuno reducibilan**.

Pogledajmo sada kako se reducibilnost i potpuna reducibilnost operatora odražavaju u njegovu matričnom prikazu.

Neka je $L < V$ invarijantan potprostor s obzirom na operator f, i neka je $\dim L = r$, $1 \leq r \leq n-1$. Neka je

$$(a_1, a_2, ..., a_r)$$

baza za prostor L, a

$$B = (a_1, a_2, ..., a_r, a_{r+1}, ..., a_n)$$

baza za prostor V, dobivena dopunjavanjem linearno nezavisnog skupa

$$(a_1, a_2, ..., a_r).$$

Kako je L f-invarijantan potprostor, za svaki $i = 1, ..., r$ je $f(a_i) \in L$, pa je

$$f(a_i) = \alpha_{1i}a_1 + \cdots + \alpha_{ri}a_r + 0 \cdot a_{r+1} + \cdots + 0 \cdot a_n \ ,$$

za $i = 1, ..., r$. Prema tome matrični zapis operatora f u bazi B ima oblik

$$F = \begin{bmatrix} \alpha_{11} & \cdots & \alpha_{1r} & \alpha_{1r+1} & \cdots & \alpha_{1n} \\ \vdots & & \vdots & \vdots & & \vdots \\ \alpha_{r1} & \cdots & \alpha_{rr} & \alpha_{rr+1} & \cdots & \alpha_{rn} \\ 0 & \cdots & 0 & \alpha_{r+1r+1} & \cdots & \alpha_{r+1n} \\ \vdots & & \vdots & \vdots & & \vdots \\ 0 & \cdots & 0 & \alpha_{nr+1} & \cdots & \alpha_{nn} \end{bmatrix} , \qquad (1)$$

tj. matrica F ima u donjem lijevom kutu nulmatricu tipa $(n - r, r)$, dok je u gornjem lijevom kutu kvadratna matrica reda r, koja je matrični zapis induciranog operatora f/L u bazi $(a_1, a_2, ..., a_r)$.

Slično, neka je $f : V \to V$ potpuno reducibilan operator, a L i M njegovi invarijantni potprostori sa svojstvom da je $L \oplus M = V$. Neka je

$$B_1 = (a_1, ..., a_r)$$

baza za L, a

$$B_2 = (a_{r+1}, ..., a_n)$$

baza za M. Onda je

$$B = B_1 \cup B_2 = (a_1, ..., a_r, a_{r+1}, ..., a_n)$$

baza za B i vrijedi

$$f(a_i) = \alpha_{1i}a_1 + \cdots + \alpha_{ri}a_r + 0 \cdot a_{r+1} + \cdots + 0 \cdot a_n \ ,$$

za $1 \leq i \leq r$, odnosno

$$f(a_j) = 0 \cdot a_1 + \cdots + 0 \cdot a_r + \alpha_{r+1\,j}a_{r+1} + \cdots + \alpha_{nj}a_n \ ,$$

za $r+1 \leq j \leq n$. Prema tome operator f ima u bazi B matrični zapis

$$F = \begin{bmatrix} \alpha_{11} & \cdots & \alpha_{1r} & 0 & \cdots & 0 \\ \vdots & & \vdots & \vdots & & \vdots \\ \alpha_{r1} & \cdots & \alpha_{rr} & 0 & \cdots & 0 \\ 0 & \cdots & 0 & \alpha_{r+1\,r+1} & \cdots & \alpha_{r+1\,n} \\ \vdots & & \vdots & \vdots & & \vdots \\ 0 & \cdots & 0 & \alpha_{n\,r+1} & \cdots & \alpha_{nn} \end{bmatrix}, \tag{2}$$

u kojemu su u gornjem lijevom kutu i donjem desnom kutu matrice induciranih operatora $f_1 = f/L$, odnosno $f_2 = f/M$ (u bazama B_1, odnosno B_2), a na ostalim mjestima matrice su nule. Ako matrični zapis operatora f_i u bazi B_i označimo s F_i, $i = 1, 2$, matricu F možemo preglednije pisati u obliku tzv. **blokmatrice** kao

$$F = \begin{bmatrix} F_1 & O \\ O & F_2 \end{bmatrix}, \tag{3}$$

gdje su s O označene nulmatrice, i to tipa $(n-r, r)$, odnosno $(r, n-r)$, uz $r = \dim L$. Matricu oblika (2), odnosno (3), nazivamo **kvazidijagonalna matrica**, jer je ona dijagonalna, shvaćena kao blokmatrica. Imamo, dakle, zaključak:

PROPOZICIJA 2

Linearni operator $f : V \to V$ je reducibilan ili potpuno reducibilan ako i samo ako dopušta matrični zapis oblika (1)*, odnosno oblika* (2). ■

Prema tome, operator f je reducibilan ako i samo ako je svaka njegova matrica slična matrici oblika (1), a potpuno reducibilan ako i samo ako je bilo koji njegov matrični prikaz sličan kvazidijagonalnoj matrici.

Osnovni je problem naći bazu za prostor V, u kojoj će matrica operatora f imati najjednostavniji oblik, ili, što je isto, u klasi sličnih matrica naći onu koja je najjednostavnija za računanje (ima najviše nula). Na taj ćemo se problem još vratiti.

Opisana situacija se lako generalizira. Neka su $L_1, L_2, \ldots, L_m < V$ netrivijalni invarijantni potprostori za operator f, sa svojstvom da je

$$V = L_1 \oplus L_2 \oplus \cdots \oplus L_m .$$

Ako su $f_i = f/L_i$, $i = 1, \ldots, m$, inducirani operatori, kažemo da je f njihova direktna suma i pišemo

$$f = f_1 \oplus f_2 \oplus \cdots \oplus f_m .$$

Nadalje, ako je F_i matrični zapis operatora f_i u nekoj bazi B_i prostora L_i, onda je

$$B = B_1 \cup B_2 \cup \cdots \cup B_m$$

baza za prostor V, i u toj bazi operator f ima matrični prikaz

$$F = \begin{bmatrix} F_1 & & & O \\ & F_2 & & \\ & & \ddots & \\ O & & & F_m \end{bmatrix}, \tag{4}$$

tj. operator f je reprezentiran kvazidijagonalnom matricom, u kojoj na glavnoj dijagonali stoje matrice operatora f_i, $i = 1, \ldots, m$, a svi ostali elementi su nule.

Posebno je važan slučaj kad su invarijantni potprostori L_i operatora f jednodimenzionalni. U tom slučaju su blokovi F_i u matrici (4) matrice reda 1, dakle skalari, pa se ta kvazidijagonalna matrica reducira na **običnu dijagonalnu matricu**.

Ostaje otvoreno pitanje egzistencije reducibilnih i potpuno reducibilnih operatora, posebno takvih koji se mogu reprezentirati pomoću dijagonalne matrice. Na to pitanje odgovorit ćemo u sljedećim točkama.

ZADACI

1. Dokaži: Neka su $L, M < V$ f-invarijantni potprostori. Onda su i potprostori $L + M$, odnosno $L \cap M$, f-invarijantni.

2. Dokaži: Neka je

$$A = \begin{bmatrix} A_1 & & & O \\ & A_2 & & \\ & & \ddots & \\ O & & & A_m \end{bmatrix}$$

kvazidijagonalna matrica. Onda je

$$\det A = \det A_1 \det A_2 \cdots \det A_m .$$

Kako su blokovi A_i matrice nižeg reda, ova formula znatno olakšava računanje determinante matrice A.

3. Ako matricu rastavimo pravcima paralelnim njezinim stupcima i redcima u manje matrice, kažemo da smo je razbili u **blokove**. Matrica kojoj su elementi ti blokovi zove se **blokmatrica**. Pokaži da se blokmatrice zbrajaju, množe skalarom i množe na isti način, kao i obične matrice (ako su blokovi takvi da su potrebne operacije s njima definirane).

4. Neka su $P = \begin{bmatrix} E & O \\ A & O \end{bmatrix}$ i $Q = \begin{bmatrix} E & B \\ O & O \end{bmatrix}$ kvadratne blokmatrice. Pokaži da su idempotentne, tj. da vrijedi $P^2 = P$, odnosno $Q^2 = Q$.

5. Neka je $f : V \to V$ linearni operator. Dokaži da su slika $S(f) < V$ i jezgra $J(f) < V$ invarijantni potprostori s obzirom na f.

10.9. Svojstvene vrijednosti linearnog operatora

Sada ćemo se pozabaviti pitanjem egzistencije invarijantnih potprostora za dani linearni operator, posebno jednodimenzionalnih.

Neka je V n-dimenzionalni linearni prostor nad poljem F, $f : V \to V$ linearni operator, a $L < V$ invarijantni potprostor za taj operator, takav da je $\dim L = 1$. Neka je $\{a\}$ jedna baza za L. Kako je L invarijantan, to je $f(a) \in L$, pa postoji skalar $\lambda \in F$ takav da je $f(a) = \lambda a$. Ako je sada $x \in L$ bilo koji vektor, sigurno je $x = \alpha a$, pa imamo

$$f(x) = f(\alpha a) = \alpha f(a) = \alpha(\lambda a) = \lambda(\alpha a) = \lambda x\,.$$

Prema tome je skalar λ na neki način karakterističan za potprostor L. Operator f svaki vektor iz tog potprostora "produžuje", odnosno "skraćuje" za isti faktor λ.

Općenito, problem određivanja skalara $\lambda \in F$ i vektora $x \in V$, za koje je

$$f(x) = \lambda x\,, \tag{1}$$

naziva se **problem svojstvenih vrijednosti** za operator $f : V \to V$. Uočimo da je (1) jednadžba s dvije nepoznanice: jedna od njih je skalar, a druga vektor. Naravno, $x = \Theta$ zadovoljava svaku jednadžbu (1), ali tu mogućnost ignoriramo kao trivijalnu. Imamo sada ovaj niz definicija:

Skalar $\lambda \in F$ nazivamo **svojstvena vrijednost** operatora f ako postoji vektor $a \in V$, različit od nulvektora, takav da vrijedi

$$f(a) = \lambda a\,.$$

Svaki vektor a, različit od nulvektora, koji zadovoljava navedeni uvjet, naziva se **svojstveni vektor** operatora f pridružen svojstvenoj vrijednosti λ.

NAPOMENA 1

U literaturi su za svojstvenu vrijednost operatora uobičajeni nazivi još i karakteristična vrijednost, vlastita vrijednost ili latentna vrijednost operatora. Analogni se sinonimi upotrebljavaju i za svojstveni vektor.

Neka je sa $S(\lambda)$ označen skup **svih** svojstvenih vektora pridruženih svojstvenoj vrijednosti λ, zajedno s nulvektorom Θ,

$$S(\lambda) = \{a \in V \mid f(a) = \lambda a\} .$$

Onda vrijedi

PROPOZICIJA 2

Skup $S(\lambda) \subset V$ je potprostor od V.

Dokaz

Neka su $a, b \in S(\lambda)$ svojstveni vektori, a $\alpha, \beta \in F$ bilo koji skalari. Onda je

$$\begin{aligned} f(\alpha a + \beta b) &= \alpha f(a) + \beta f(b) = \alpha(\lambda a) + \beta(\lambda b) = \\ &= \lambda(\alpha a) + \lambda(\beta b) = \lambda(\alpha a + \beta b) , \end{aligned}$$

zbog čega je $\alpha a + \beta b \in S(\lambda)$ i tvrdnja je dokazana. ■

Potprostor $S(\lambda)$ nazivamo **svojstveni potprostor** operatora f pridružen svojstvenoj vrijednosti λ, a njegovu dimenziju **geometrijska kratnost** od λ.

Skup $\sigma(f)$ **svih** svojstvenih vrijednosti operatora f obično se naziva **spektar** operatora f. Sljedeći teorem pokazuje kako se računaju svojstvene vrijednosti operatora, tj. određuje njegov spektar.

TEOREM 3

Skalar $\lambda_0 \in F$ je svojstvena vrijednost operatora f ako i samo ako je λ_0 korijen karakteristične jednadžbe $k_f(\lambda) = 0$ tog operatora.

Dokaz

Neka je F matrični zapis*) operatora f. Treba vidjeti da je λ_0 svojstvena vrijednost operatora f ako i samo ako je $k_F(\lambda_0) = 0$.

Najprije, neka je λ_0 svojstvena vrijednost. Po definiciji, to znači da postoji vektor $a \neq \Theta$ takav da je $f(a) = \lambda_0 a$. No, tu relaciju možemo pisati u obliku

$$(f - \lambda_0 e)(a) = \Theta$$

gdje je $e : V \to V$ jedinični operator. Iz te relacije razabiremo da linearni operator

$$c = f - \lambda_0 e$$

*) Oprez: Ne brkaj matricu F s poljem F nad kojim je definiran prostor V!

ima netrivijalnu jezgru $J(c) \neq \{\Theta\}$, pa prema tome nije bijektivan. Odatle slijedi da taj operator nije regularan. Kako je očito matrični zapis operatora c matrica $C = F - \lambda_0 E$, zbog Kor. 2 u 10.3. mora biti

$$\det C = \det (F - \lambda_0 E) = 0 ,$$

što pokazuje da je λ_0 korijen karakteristične jednadžbe

$$k_F(\lambda) = \det (F - \lambda E) = 0$$

matrice F.

Obratno, neka je $\lambda_0 \in F$ takav da je $k_F(\lambda_0) = 0$, tj. $\det (F - \lambda_0 E) = 0$. To, međutim, znači da operator $c = f - \lambda_0 e$ nije regularan pa postoji vektor $a \neq \Theta$ takav da je

$$c(a) = (f - \lambda_0 e)(a) = 0 ,$$

dakle $f(a) = \lambda_0 a$, što pokazuje da je λ_0 svojstvena vrijednost operatora f. ■

Problem određivanja svojstvenih vrijednosti se, dakle, svodi na problem rješavanja karakteristične jednadžbe. No, pri tome valja biti oprezan. Neka je npr.

$$f : V \to V$$

linearni operator, a

$$F = \begin{bmatrix} -1 & 5 \\ -1 & 1 \end{bmatrix}$$

njegov matrični prikaz. Onda je karakteristična jednadžba operatora f

$$k_f(\lambda) = \det (F - \lambda E) = \lambda^2 + 4 = 0 .$$

Ako je V prostor nad poljem $\mathbb{C}$ kompleksnih brojeva, operator f ima svojstvene vrijednosti $\lambda = 2i$ i $\lambda = -2i$. Međutim, ako je V prostor nad poljem $\mathbb{R}$ realnih brojeva, operator f **nema svojstvenih vrijednosti** jer nema **realnih brojeva** koji bi zadovoljavali njegovu karakterističnu jednadžbu.

Linearni operator, koji djeluje na n-dimenzionalnom prostoru, imat će najviše n svojstvenih vrijednosti, ali i manje (možda čak nijednu), u ovisnosti o tome koliko rješenja karakteristične jednadžbe pripada polju nad kojim je linearni operator definiran. Tih teškoća nema ako se promatraju "dobra" polja. Za polje F kažemo da je **algebarski zatvoreno** ako svaki polinom $p(\lambda)$, s koeficijentima iz tog polja, dopušta faktorizaciju u linearne faktore (s koeficijentima iz tog polja), tj. ako se može prikazati kao

$$p(\lambda) = \alpha_m(\lambda - \lambda_1)(\lambda - \lambda_2) \cdots (\lambda - \lambda_m) ,$$

gdje su $\alpha_m, \lambda_1, ..., \lambda_m \in F$. Polje $\mathbb{C}$ kompleksnih brojeva je primjer takvog polja (iako to nije sasvim jednostavno dokazati). Problem bi se znatno pojednostavnio, kad bismo teoriju ograničili na algebarski zatvorena polja. Nažalost, važna polja, kao što su polje $\mathbb{Q}$ racionalnih brojeva i polje $\mathbb{R}$ realnih brojeva, koja se pojavljuju u raznim primjenama, nisu algebarski zatvorena. O njima treba voditi računa, a to komplicira teoriju. Zabilježimo:

PROPOZICIJA 4

Linearni operator, koji djeluje na n-dimenzionalnom prostoru nad algebarski zatvorenim poljem, ima točno n svojstvenih vrijednosti (među kojima može, dakako, biti i jednakih). ■

Pogledajmo sada kako odrediti svojstvene vektore koji su pridruženi svojstvenoj vrijednosti λ operatora f. Za $\lambda = \lambda_0$ to je svaki vektor $a \neq \Theta$, za koji je

$$f(a) = \lambda_0 \cdot a \, .$$

Ako je F matrični zapis operatora f u nekoj bazi B, a $X = [\alpha_i]$ koordinatna matrica traženog vektora a u toj istoj bazi, onda navedenu jednakost možemo zapisati matrično kao

$$FX = \lambda_0 X \, ,$$

ili

$$(F - \lambda_0 E)X = O \, ,$$

dakle kao

$$C(\lambda_0)X = O \, ,$$

tj. $C(\lambda_0) \cdot [\alpha_i] = O$, gdje je $C(\lambda_0) = F - \lambda_0 E$ karakteristična matrica operatora, u koju je uvršteno $\lambda = \lambda_0$. No, ova matrična jednadžba je očito ekvivalentna s homogenim sustavom od n linearnih jednadžbi u nepoznanicama $\alpha_1, ..., \alpha_n$, i koeficijentima iz matrice $C(\lambda_0)$. Kako je $\det C(\lambda_0) = 0$, taj će sustav uvijek imati i netrivijalnih rješenja (vidi Kor. 3 u 11.5., tj. Roucheov teorem), i svako takvo rješenje predstavlja koordinate nekog svojstvenog vektora (u bazi B), pridruženog svojstvenoj vrijednosti λ_0.

Ilustrirajmo taj postupak jednim primjerom. Neka je linearni operator reprezentiran matricom

$$F = \begin{bmatrix} -1 & 2 & 2 \\ 2 & 2 & 2 \\ -3 & -6 & -6 \end{bmatrix} \, .$$

Pripadna karakteristična matrica je

$$C(\lambda) = \begin{bmatrix} -1-\lambda & 2 & 2 \\ 2 & 2-\lambda & 2 \\ -3 & -6 & -6-\lambda \end{bmatrix},$$

pa je karakteristični polinom

$$k_F(\lambda) = \det C(\lambda) = -\lambda(\lambda+2)(\lambda+3)\,.$$

Prema tome, svojstvene vrijednosti operatora su $\lambda_1 = 0$, $\lambda_2 = -2$, $\lambda_3 = -3$. Sada ćemo računati pridružene svojstvene vektore. Za $\lambda_1 = 0$ je

$$C(0) = \begin{bmatrix} -1 & 2 & 2 \\ 2 & 2 & 2 \\ -3 & -6 & -6 \end{bmatrix} = F$$

i onda

$$C(0)[\alpha_i] = O\,,$$

dakle

$$\begin{bmatrix} -1 & 2 & 2 \\ 2 & 2 & 2 \\ -3 & -6 & -6 \end{bmatrix} \begin{bmatrix} \alpha_1 \\ \alpha_2 \\ \alpha_3 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix},$$

što se svodi na sustav

$$\begin{aligned} -\alpha_1 \;+\; & 2\alpha_2 + 2\alpha_3 = 0 \\ 2\alpha_1 \;+\; & 2\alpha_2 + 2\alpha_3 = 0 \\ -3\alpha_1 \;-\; & 6\alpha_2 - 6\alpha_3 = 0\,. \end{aligned}$$

Lako se vidi da taj sustav ima netrivijalno rješenje

$$\alpha_1 = 0,\ \alpha_2 = 1,\ \alpha_3 = -1\,,$$

pa onda i familiju rješenja

$$\alpha_1 = 0,\ \alpha_2 = \alpha,\ \alpha_3 = -\alpha, \qquad \text{za svaki } \alpha \in \mathbb{R}\,.$$

Prema tome je

$$a_1 = \begin{bmatrix} 0 \\ 1 \\ -1 \end{bmatrix},$$

i, uopće, svaki vektor oblika

$$\alpha a_1 = \begin{bmatrix} 0 \\ \alpha \\ -\alpha \end{bmatrix}, \quad \alpha \neq 0\,,$$

svojstveni je vektor za svojstvenu vrijednost λ_1. Dakako,

$$S(\lambda_1) = \{\alpha a_1 \mid \alpha \in \mathbb{R}\}$$

jest onda svojstveni potprostor pridružen λ_1. Za $\lambda_2 = -2$ imamo

$$C(-2) = \begin{bmatrix} 1 & 2 & 2 \\ 2 & 4 & 2 \\ -3 & -6 & -4 \end{bmatrix},$$

i u tom slučaju sustav

$$C(-2)[\alpha_i] = O$$

ima netrivijalno rješenje

$$\alpha_1 = 2\,, \quad \alpha_2 = -1\,, \quad \alpha_3 = 0\,,$$

pa je

$$a_2 = \begin{bmatrix} 2 \\ -1 \\ 0 \end{bmatrix}$$

svojstveni vektor pridružen svojstvenoj vrijednosti λ_2. Takvi su i svi vektori βa_2, $\beta \neq 0$, pa je

$$S(\lambda_2) = \{\beta a_2 \mid \beta \in \mathbb{R}\}$$

pripadni svojstveni potprostor. Konačno, za $\lambda_3 = -3$ je

$$C(-3) = \begin{bmatrix} 2 & 2 & 2 \\ 2 & 5 & 2 \\ -3 & -6 & -3 \end{bmatrix},$$

i ta nas matrica vodi na sustav s netrivijalnim rješenjem

$$\alpha_1 = 1\,, \quad \alpha_2 = 0\,, \quad \alpha_3 = -1\,.$$

Dakle je

$$a_3 = \begin{bmatrix} 1 \\ 0 \\ -1 \end{bmatrix},$$

i svaki vektor oblika γa_3, $\gamma \neq 0$, svojstven za λ_3, a

$$S(\lambda_3) = \{\gamma a_3 \mid \gamma \in \mathbb{R}\}$$

svojstveni potprostor za tu svojstvenu vrijednost.

Navedimo na kraju još i ovu važnu značajku svojstvenih vektora:

TEOREM 5

Neka su $\lambda_1, ..., \lambda_s$ međusobno različite svojstvene vrijednosti operatora $f : V \to V$ i neka su $a_1, ..., a_s \in V$ svojstveni vektori tog operatora, odabrani tako da je vektor a_i pridružen svojstvenoj vrijednosti λ_i, za svaki $i = 1, ..., s$. Onda je skup $S = \{a_1, ..., a_s\}$ linearno nezavisan u V.

Dokaz

Pretpostavimo, protivno tvrdnji, da je skup S linearno zavisan. Pretpostavimo nadalje, da su vektori u S numerirani tako da prvih k, $k < s$, vektora predstavlja maksimalni linearno nezavisan podskup od S. Prema tome, preostali vektori u S su linearne kombinacije vektora $a_1, \ldots, a_k$. Onda npr. posljednji vektor a_s možemo na **jednoznačan** način (Tm. 8 u 7.5.) prikazati u obliku

$$a_s = \sum_{i=1}^{k} \alpha_i a_i \, . \tag{2}$$

Pritom je bar jedan $\alpha_i \neq 0$, jer bi u protivnom bilo $a_s = \Theta$, suprotno definiciji svojstvenog vektora. Primjenom operatora f na relaciju (2) dobivamo

$$f(a_s) = \sum_{i=1}^{k} \alpha_i f(a_i) \, ,$$

odnosno, zbog $f(a_i) = \lambda_i a_i$,

$$\lambda_s a_s = \sum_{i=1}^{k} \alpha_i \lambda_i a_i \, .$$

Razlikujemo dva slučaja. Ako je $\lambda_s = 0$, nijedan od λ_i, $i \leq k$, ne može biti nula jer su svojstvene vrijednosti $\lambda_1, \ldots, \lambda_s$ po pretpostavci različite. Kako ni svi α_i nisu nula, u prikazu

$$\Theta = \sum_{i=1}^{k} \alpha_i \lambda_i a_i$$

bar je jedan od koeficijenata različit od 0, što povlači da je skup $\{a_1, ..., a_k\}$ linearno zavisan, protivno pretpostavci. Ako je pak $\lambda_s \neq 0$, imamo

$$a_s = \sum_{i=1}^{k} \alpha_i \, \lambda_i \lambda_s^{-1} \, a_i \, . \tag{3}$$

Kako je $\lambda_i \lambda_s^{-1} \neq 1$ za svaki $i \leq k$, i kako svi α_i nisu 0, (3) je prikaz od a_s različit od (2), što je kontradikcija s jednoznačnošću prikaza. U svakom smo,

dakle, slučaju dobili kontradikciju, pa skup S mora biti linearno nezavisan. ■

ZADACI

1. Dokaži neposredno: Ako je $f = \lambda e$, gdje je e jedinični operator, a $\lambda \in F$ bilo koji skalar, onda je λ jedina svojstvena vrijednost operatora f.

2. Dokaži: dim $S(\lambda)$ jednaka je defektu operatora $f - \lambda e$, za svaku svojstvenu vrijednost λ operatora f.

3. Kako smo rekli, dim $S(\lambda_0)$ nazivamo geometrijska kratnost za svojstvenu vrijednost λ_0. Nadalje, $\lambda - \lambda_0$ je očito faktor od $k_f(\lambda)$. Ako je $(\lambda - \lambda_0)^k$ faktor karakterističnog polinoma, a $(\lambda - \lambda_0)^{k+1}$ to nije, kažemo da je λ_0 svojstvena vrijednost **algebarske kratnosti** k. Dokaži da geometrijska kratnost od λ_0 ne može biti veća od njezine algebarske kratnosti.

4. Nađi svojstvene vrijednosti za operator dan matricom

$$F = \begin{bmatrix} 1 & 1 & -1 \\ -1 & 3 & -1 \\ -1 & 2 & 0 \end{bmatrix} .$$

   Uvjeri se, na tom primjeru, da geometrijska kratnost svojstvene vrijednosti može zaista biti manja od algebarske kratnosti.

5. Definiraj pojam svojstvenih vrijednosti i svojstvenih vektora za kvadratnu matricu A, shvaćajući tu matricu kao operator $F^n \to F^n$. Uoči da će skalar $\lambda_0 \in F$ iz **polja** F biti (zbog Tm. 3) **svojstvena** (ili **karakteristična**) **vrijednost matrice** A ako i samo ako je λ_0 nula karakterističnog polinoma te matrice, dakle rješenje jednadžbe $k_A(\lambda) = 0$. To se obično uzima kao (alternativna) definicija svojstvene vrijednosti matrice. Primijetimo da će zbog Prop. 2 iz 10.6., slične matrice imati isti skup svojstvenih vrijednosti, tj. isti spektar. Okrećući red stvari, mogli bismo svojstvenu vrijednost operatora definirati i kao svojstvenu vrijednost (bilo koje) matrice tog operatora.

6. Pokaži: Ako je λ svojstvena vrijednost operatora f, onda je λ^2 svojstvena vrijednost od f^2. Što možeš reći o višim potencijama?

7. Ako su a_1 i a_2 svojstveni vektori od f, pridruženi različitim svojstvenim vrijednostima, uvjeri se da $a_1 + a_2$ nije svojstveni vektor od f.

8. Ako su svi vektori prostora, različiti od nulvektora, svojstveni vektori za neki operator f, onda je taj operator skalarni operator, tj. oblika $f = \lambda e$. Dokaži!

9. Neka je $V = [\{\sin t, \cos t\}]$ prostor nad poljem $\mathbb{C}$, razapet funkcijama $\sin t$ i $\cos t$. Te su funkcije onda baza za V i $\dim V = 2$. Promatraj operator deriviranja $d : V \to V$, te nađi njegove svojstvene vrijednosti i svojstvene vektore. Nađi matrični zapis operatora u bazi, koju čini par linearno nezavisnih svojstvenih vektora.

10. Pokaži da je $\lambda = 0$ svojstvena vrijednost operatora ako i samo ako je taj operator singularan.

11. Dokaži: Ako je a svojstveni vektor od f, onda je a svojstveni vektor i za f^k, za svaki $k \geq 0$.

12. Ako je a svojstveni vektor operatora f i g, onda je a svojstveni vektor i za operatore αf i $f + g$. Dokaži!

13. Ako je λ_i svojstvena vrijednost za $f_i, i = 1, 2$, onda $\lambda_1 + \lambda_2$ nije općenito svojstvena vrijednost za $f_1 + f_2$. Nađi primjer.

14. Dokaži: Ako je f regularan operator i λ svojstvena vrijednost za f, onda je λ^{-1} svojstvena vrijednost za f^{-1}. U kakvom su odnosu pripadni svojstveni vektori?

15. Neka su $f, g : V \to V$ operatori koji komutiraju, a V prostor nad algebarski zatvorenim poljem. Ako je $L < V$ svojstveni potprostor od f, onda je L invarijantan s obzirom na g; dokaži.

10.10. Dijagonalizacija. Jordanova forma matrice

Neka je $f : V \to V$ linearni operator. Želimo naći bazu za prostor V u kojoj bi f imao što je moguće jednostavniji matrični zapis. Dakako, najjednostavniji takav zapis bila bi dijagonalna matrica (vidi Zad. 11. u 9.4.). Nažalost, nije moguće svaki linearni operator reprezentirati pomoću dijagonalne matrice, ali se to može postići za relativno široku klasu operatora.

Za operator f kažemo da **dopušta dijagonalizaciju** ako postoji baza u kojoj je operator reprezentiran dijagonalnom matricom. Drugim riječima, to je operator kojem je (svaki) matrični prikaz sličan dijagonalnoj matrici (tj., kako se to kaže, može se dijagonalizirati). Za operatore (matrice) koji dopuštaju dijagonalizaciju, u literaturi je još uobičajen i naziv **polujednostavni** ili **poluprosti operatori**. Postavljamo si zadatak da nađemo uvjete uz koje će operator dopuštati dijagonalizaciju.

TEOREM 1

Linearni operator $f : V \to V$ dopušta dijagonalizaciju ako i samo ako u prostoru V postoji baza koja se sastoji od svojstvenih vektora tog operatora.

Dokaz

Neka je $B = (a_1, ..., a_n)$ baza od V, u kojoj je svaki a_i svojstveni vektor operatora f. Neka je za svaki $i = 1, \ldots, n$ vektor a_i pridružen svojstvenoj vrijednosti λ_i (koje ne moraju biti sve različite). Onda je $f(a_i) = \lambda_i a_i$, pa f u toj bazi ima zapis

$$D = \begin{bmatrix} \lambda_1 & 0 & \cdots & 0 \\ 0 & \lambda_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \lambda_n \end{bmatrix},$$

tj. reprezentiran je dijagonalnom matricom. Obratno, ako za operator f postoji baza $B = (a_1, ..., a_n)$ od V, u kojoj je reprezentiran dijagonalnom matricom

$$\begin{bmatrix} \alpha_1 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & \alpha_n \end{bmatrix},$$

onda je, dakako, $f(a_i) = \alpha_i a_i$, za $i = 1, \ldots, n$, što pokazuje da su vektori baze B svojstveni vektori od f (a skalari α_i svojstvene vrijednosti). ■

Iz dokaza Tm. 1 neposredno slijedi

KOROLAR 2

Ako operator f dopušta dijagonalizaciju, onda je njegov dijagonalni matrični zapis u bazi koja se sastoji od njegovih svojstvenih vektora, a elementi na glavnoj dijagonali matrice su svojstvene vrijednosti tog operatora. ■

KOROLAR 3

Ako operator $f : V \to V$ ima n različitih svojstvenih vrijednosti, gdje je $n = \dim V$, onda operator f dopušta dijagonalizaciju.

Dokaz

Prema Tm. 5 u 10.9., različitim svojstvenim vrijednostima pridruženi su linearno nezavisni svojstveni vektori, a jer ih ima n, oni čine bazu za V, pa tvrdnja slijedi iz Tm. 1. ■

Kor. 3 daje praktičan dovoljan uvjet za prepoznavanje operatora koji se mogu dijagonalizirati. On ujedno pokazuje da je klasa takvih operatora vrlo široka, jer za po volji odabran operator možemo s velikom vjerojatnošću očekivati da će sve njegove svojstvene vrijednosti biti različite. Postoje ipak okolnosti kad se taj kriterij ne može primijeniti. To je npr. slučaj kad je pojedina svojstvena vrijednost algebarske kratnosti veće od jedan ili, pak,

kada karakteristična jednadžba nema sve korijene iz pripadnog polja. U nekim od tih slučajeva operator se ipak može dijagonalizirati (Kor. 3 daje samo dovoljan, a ne i nuždan uvjet). Najopćenitiju tvrdnju u tom smjeru koju ovdje ne dokazujemo, a kojom se karakteriziraju operatori koji se mogu dijagonalizirati, daje

TEOREM 4

Da bi linearni operator dopuštao dijagonalizaciju, nužno je i dovoljno da se njegov minimalni polinom može prikazati kao produkt međusobno različitih linearnih faktora s koeficijentima iz pripadnog polja. ■

Dakako, teorem karakterizira i matrice koje su slične dijagonalnim matricama. Primijetimo da je teorem egzistencijalne prirode, tj. na temelju njega možemo samo zaključiti postoji li baza svojstvenih vektora za promatrani operator. Onda tek treba naći te svojstvene vektore, i time dijagonalnu formu matrice operatora (Kor. 2).

Često linearni operator f nije zadan direktno, nego svojom matricom F, u nekoj nespecificiranoj bazi B. Ako su

$$a_k = \begin{bmatrix} t_{1k} \\ \vdots \\ t_{nk} \end{bmatrix}$$

linearno nezavisni svojstveni vektori operatora f, dani svojim koordinatnim matricama u toj istoj bazi B, i ako ih ima n, onda oni čine bazu $A = (a_1, ..., a_n)$. Prijelaz iz baze B u bazu A opisan je matricom transformacije (vidi 10.2.)

$$T = \begin{bmatrix} t_{11} & \cdots & t_{1n} \\ \vdots & \ddots & \vdots \\ t_{n1} & \cdots & t_{nn} \end{bmatrix} .$$

No, u bazi A matrica operatora ima dijagonalnu formu D (Tm. 1), i do nje dolazimo (vidi relaciju (5) u 10.5) na ovaj način:

$$D = T^{-1} F T .$$

Prema tome, vrijedi

PROPOZICIJA 5

Ako je matrica F operatora slična dijagonalnoj matrici, onda sprezanje obavlja matrica T koordinata svojstvenih vektora operatora (u istoj bazi u kojoj je F matrični zapis operatora). ■

Na primjer, za matricu

$$F = \begin{bmatrix} -1 & 2 & 2 \\ 2 & 2 & 2 \\ -3 & -6 & -6 \end{bmatrix}$$

vidjeli smo u 10.9. da ima tri linearno nezavisna svojstvena vektora

$$a_1 = \begin{bmatrix} 0 \\ 1 \\ -1 \end{bmatrix}, \quad a_2 = \begin{bmatrix} 2 \\ -1 \\ 0 \end{bmatrix}, \quad a_3 = \begin{bmatrix} 1 \\ 0 \\ -1 \end{bmatrix},$$

pa dijagonalizaciju provodi matrica sprezanja

$$T = \begin{bmatrix} 0 & 2 & 1 \\ 1 & -1 & 0 \\ -1 & 0 & -1 \end{bmatrix}.$$

Zaista, nalazimo da je

$$T^{-1} = \begin{bmatrix} 1 & 2 & 1 \\ 1 & 1 & 1 \\ -1 & -2 & -2 \end{bmatrix}$$

i onda

$$D = T^{-1}FT = \begin{bmatrix} 0 & 0 & 0 \\ 0 & -2 & 0 \\ 0 & 0 & -3 \end{bmatrix}.$$

Na glavnoj dijagonali čitamo svojstvene vrijednosti $\lambda_1 = 0$, $\lambda_2 = -2$, $\lambda_3 = -3$, koje smo i prije dobili.

U drugu ruku, za matricu

$$F = \begin{bmatrix} 1 & 1 & -1 \\ -1 & 3 & -1 \\ -1 & 2 & 0 \end{bmatrix}$$

iz Zad. 4. u 10.9. nalaze se svojstvene vrijednosti $\lambda_1 = \lambda_2 = 1$, $\lambda_3 = 2$, kojima su pridružena samo dva linearno nezavisna svojstvena vektora $a = (1, 1, 1)$ i $b = (0, 1, 1)$. U tom, dakle, slučaju ne postoji skup od tri linearno nezavisna svojstvena vektora. Prema tome, operator predočen tom matricom ne dopušta dijagonalizaciju. Matrica F nije slična dijagonalnoj matrici.

Ima i vrlo jednostavnih matrica koje se ne daju dijagonalizirati. Na primjer, matrica

$$A = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}$$

ne dopušta dijagonalizaciju ni nad kojim poljem. Naime, obje su njezine svojstvene vrijednosti jednake 0, pa bi morala biti slična nulmatrici, a to nije moguće (jer nemaju isti rang).

Matricu koja se ne može dijagonalizirati nastojimo pojednostavniti tako da je **kvazidijagonaliziramo**, tj. prikažemo kao dijagonalnu blokmatricu (vidi točku 10.8.), i to tako da blokovi budu što je moguće jednostavnije strukture. Taj problem nas vodi na pojam tzv. **Jordanove forme** (ili **Jordanova normalnog oblika**) **matrice**. Opišimo najprije što pod tim pojmom podrazumijevamo.

Temeljni Jordanov blok (ili **Jordanova klijetka**) pridružen skalaru $\lambda \in F$ je kvadratna matrica oblika

$$B = \begin{bmatrix} \lambda & 1 & 0 & \cdots & 0 & 0 \\ 0 & \lambda & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & \lambda & 1 \\ 0 & 0 & 0 & \cdots & 0 & \lambda \end{bmatrix},$$

tj. matrica kojoj je na glavnoj dijagonali raspoređen taj skalar λ, točno iznad dijagonale su jedinice, a svi ostali elementi jednaki su nuli. Nadalje, **Jordanov blok** pridružen skalaru $\lambda \in F$ je dijagonalna blokmatrica

$$C = \begin{bmatrix} B_1 & & & O \\ & B_2 & & \\ & & \ddots & \\ O & & & B_s \end{bmatrix},$$

gdje su B_i, $i = 1, ..., s$, temeljni Jordanovi blokovi, možda različitih redova, ali pridruženi istom skalaru λ. Konačno, **Jordanova matrica** je dijagonalna blokmatrica

$$J = \begin{bmatrix} C_1 & & & O \\ & C_2 & & \\ & & \ddots & \\ O & & & C_r \end{bmatrix},$$

gdje su blokovi C_j, $j = 1, ..., r$, Jordanovi blokovi koji pripadaju međusobno **različitim** skalarima λ_j.

Na primjer,

$$B = \begin{bmatrix} 3 & 1 & 0 \\ 0 & 3 & 1 \\ 0 & 0 & 3 \end{bmatrix}$$

jest jedan temeljni Jordanov blok, zatim

$$C = \begin{bmatrix} 3 & 1 & 0 & 0 & 0 \\ 0 & 3 & 1 & 0 & 0 \\ 0 & 0 & 3 & 0 & 0 \\ 0 & 0 & 0 & 3 & 1 \\ 0 & 0 & 0 & 0 & 3 \end{bmatrix}$$

jest primjer Jordanovog bloka, a

$$J = \begin{bmatrix} 3 & 1 & 0 & & & & & O \\ 0 & 3 & 1 & & & & & \\ 0 & 0 & 3 & & & & & \\ & & & 3 & 1 & & & \\ & & & 0 & 3 & & & \\ & & & & & -2 & 1 & \\ & & & & & 0 & -2 & \\ O & & & & & & & -2 \end{bmatrix}$$

jedna je Jordanova matrica. Uočimo da je svaka Jordanova matrica specijalan tip (gornje) trokutaste matrice. Naravno, svaka je dijagonalna matrica specijalan slučaj Jordanove matrice (gdje su temeljni Jordanovi blokovi reda 1, tj. oblika $[\lambda] = \lambda$). Prema tome Jordanova matrica je generalizacija dijagonalne matrice.

Osnovni rezultat onda kaže

TEOREM 6

Svaka je kvadratna matrica nad algebarski zatvorenim poljem (specijalno, nad poljem $\mathbb{C}$ kompleksnih brojeva) slična nekoj Jordanovoj matrici nad tim istim poljem. Nadalje, ta je Jordanova matrica jedinstvena, do na poredak blokova duž dijagonale. ■

Popularno rečeno, teorem kaže da se svaka kvadratna matrica može svesti na Jordanovu formu, i to u biti na jedan jedini način. Posebno, ako se matrica može dijagonalizirati, njezina se Jordanova forma podudara s dijagonalnom formom.

Prevedeno na jezik operatora, Tm. 6 se svodi na

TEOREM 7

Neka je $f : V \to V$ linearni operator koji djeluje na prostoru V nad algebarski zatvorenim poljem. Onda u prostoru V postoji baza u kojoj je operator f reprezentiran Jordanovom matricom. ■

U preciznijoj formulaciji (korištenjem pojma svojstvene vrijednosti matrice, kao u Zad. 5. iz 10.9.), Tm. 6 glasi ovako:

TEOREM 8

Neka je A kvadratna matrica nad algebarski zatvorenim poljem. Neka je

$$k_A(\lambda) = (\lambda - \lambda_1)^{r_1} \dots (\lambda - \lambda_k)^{r_k}$$

karakteristični polinom, a

$$m_A(\lambda) = (\lambda - \lambda_1)^{s_1} \dots (\lambda - \lambda_k)^{s_k}$$

minimalni polinom matrice A. Onda je matrica A slična Jordanovoj matrici

$$J = \begin{bmatrix} C_1 & & O \\ & \ddots & \\ O & & C_k \end{bmatrix},$$

gdje Jordanov blok C_i odgovara svojstvenoj vrijednosti λ_i, za svaki $i = 1, 2, \dots, k$. Pritom je u matrici C_i bar jedan od temeljnih Jordanovih blokova reda s_i, dok red ostalih blokova u toj matrici ne prelazi s_i. Broj blokova u matrici C_i podudara se s geometrijskom kratnošću svojstvene vrijednosti λ_i. Nadalje, suma redova svih blokova u matrici C_i jednaka je broju r_i (tj. algebarskoj kratnosti svojstvene vrijednosti λ_i). Konačno, broj temeljnih Jordanovih blokova svakog mogućeg reda, koji se pojavljuju u matrici J, jednoznačno je određen matricom A. Matrica J je određena jednoznačno, do na raspored (temeljnih Jordanovih) blokova duž glavne dijagonale. ■

Za razliku od Tm. 6, koji nam osigurava samo egzistenciju Jordanove forme matrice, Tm. 8 je konstruktivnog karaktera, tj. daje nam i postupak, pomoću kojeg možemo doći do Jordanove forme dane matrice. Dokaz Tm. 8 je dosta dug i složen, i mi ga ovdje nećemo provoditi.

Za ilustraciju uzmimo matricu

$$A = \begin{bmatrix} 3 & 1 & -3 \\ -7 & -2 & 9 \\ -2 & -1 & -4 \end{bmatrix}.$$

Njezin je karakteristični polinom $k_A(\lambda) = -(\lambda-1)(\lambda-2)^2$, pa se primjenom Tm. 8 lako utvrdi da je Jordanova forma te matrice

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 2 & 1 \\ 0 & 0 & 2 \end{bmatrix}.$$

Spomenimo na kraju da slična teorija postoji i za slučaj kad matrica nije nad algebarski zatvorenim poljem. I takva se matrica (operator) može uvijek prevesti na standardnu, relativno jednostavnu matricu, tzv. **normalnu formu.**

ZADACI

1. Dokaži da se matrica
$$\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$$
ne može dijagonalizirati nad poljem $\mathbb{R}$, ali dopušta dijagonalizaciju nad poljem $\mathbb{C}$.

2. Dokaži: Neka je V prostor s bazom koja se sastoji od svojstvenih vektora operatora f. Ako je $L < V$ bilo koji f-invarijantan potprostor, onda L također ima bazu koja se sastoji od svojstvenih vektora operatora f.

3. Dokaži: Neka je V linearni prostor nad algebarski zatvorenim poljem. Operator $f : V \to V$ dopušta dijagonalizaciju ako i samo ako za svaki f-invarijantan potprostor $L < V$ postoji f-invarijantan potprostor $M < V$ takav da je $L \oplus M = V$.

4. Dokaži: Ako su $\lambda_1, \ldots, \lambda_n$ različite svojstvene vrijednosti operatora $f : V \to V$, $n = \dim V$, onda je
$$V = S(\lambda_1) \oplus \cdots \oplus S(\lambda_n) ,$$
gdje je $S(\lambda_i)$ svojstveni potprostor pridružen svojstvenoj vrijednosti λ_i.

5. Dokaži: Svaka realna simetrična matrica se može dijagonalizirati.

6. Temeljni Jordanov blok ima karakteristični polinom $(\lambda - \lambda_0)^n$, gdje je n red matrice. Prema tome, za tu matricu jedina svojstvena vrijednost je $\lambda = \lambda_0$, i to kratnosti n. Dokaži!

7. Svedi na Jordanovu formu sljedeće matrice:
$$\begin{bmatrix} 1 & 0 & -1 & 1 & 0 \\ -4 & 1 & -3 & 2 & 1 \\ -2 & -1 & 0 & 1 & 1 \\ -3 & -1 & -3 & 4 & 1 \\ -8 & -2 & -7 & 5 & 4 \end{bmatrix} , \quad \begin{bmatrix} 5 & -1 & -3 & 2 & -5 \\ 0 & 2 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & -2 \\ 0 & -1 & 0 & 3 & 1 \\ 1 & -1 & -1 & 1 & 1 \end{bmatrix} .$$

[Za provjeru: Karakteristični polinomi su $-(\lambda-2)^5$, odnosno $-(\lambda-2)^3(\lambda-3)^2$.]

8. Dokaži: Svaka je idempotentna matrica A slična matrici

$$\begin{bmatrix} E & O \\ O & O \end{bmatrix}.$$

Nadalje, ako je to matrica nad poljem karakteristike 0, rang od A je jednak $\operatorname{tr} A$.

9. Pretpostavimo da se matrica A može dijagonalizirati. Mogu li se dijagonalizirati i njezine potencije A^k? Obratno, ako A^k dopušta dijagonalizaciju za neki k, može li se A svesti na dijagonalnu formu?

11

SUSTAVI LINEARNIH JEDNADŽBI

Na potrebu izučavanja sustava linearnih jednadžbi, kao najjednostavnijeg tipa algebarskih jednadžbi, upućuju mnogi problemi teorije i prakse. Kako ćemo vidjeti, u sažetom i jasnom prikazu te teorije važnu ulogu imaju linearni operatori, matrice i determinante. To je glavni razlog da se o linearnim sustavima govori tek sada.

11.1. Notacija i formulacija problema

Neka je F dano polje. **Linearna jednadžba nad poljem F, u nepoznanicama**

$$x_1, x_2, \ldots, x_n \ ,$$

jest izraz oblika

$$\alpha_1 x_1 + \alpha_2 x_2 + \cdots + \alpha_n x_n = \beta \ , \tag{1}$$

gdje su $\alpha_i, \beta \in F$ bilo koji skalari iz danog polja. Skalare α_i nazivamo **koeficijentima**, a β **slobodnim članom** jednadžbe (1).

Mi ćemo izučavati **konačne** kolekcije takvih jednadžbi, tzv. **sustave linearnih jednadžbi nad poljem** F. Opći takav sustav je oblika

$$\left.\begin{array}{ccccccc} \alpha_{11}x_1 & + & \cdots & + & \alpha_{1n}x_n & = & \beta_1 \\ \alpha_{21}x_1 & + & \cdots & + & \alpha_{2n}x_n & = & \beta_2 \\ \vdots & & & & & & \vdots \\ \alpha_{i1}x_1 & + & \cdots & + & \alpha_{in}x_n & = & \beta_i \\ \vdots & & & & & & \vdots \\ \alpha_{m1}x_1 & + & \cdots & + & \alpha_{mn}x_n & = & \beta_m \end{array}\right\} \ , \tag{2}$$

tj. sastoji se od m linearnih jednadžbi, od kojih je svaka s n nepoznanica (bez narušavanja općenitosti, možemo uvijek pretpostaviti da je broj nepoznanica u svakoj jednadžbi sustava isti). Pritom se, općenito govoreći, broj jednadžbi i broj nepoznanica ne moraju podudarati.
Sustav (2) u kompaktnom obliku pišemo kao

$$\sum_{k=1}^{n} \alpha_{ik}\, x_k = \beta_i \quad , \quad i = 1, \ldots, m \, . \tag{3}$$

Naš je problem, dakako, **riješiti** sustav (2), tj. naći **sva njegova rješenja**. Pritom **rješenjem sustava** smatramo svaku uređenu n-torku

$$(\gamma_1, \gamma_2, \ldots, \gamma_n) \tag{4}$$

skalara iz polja F, koja supstitucijom $x_k = \gamma_k$, $k = 1, \ldots, n$, u sve jednadžbe (2), prevodi te jednadžbe u numeričke identitete, tj. u trivijalne jednakosti među elementima polja. Popularno kažemo da će (4) biti rješenje sustava (2) ako i samo ako **zadovoljava** sve jednadžbe tog sustava. Uočimo da (4) predstavlja **jedno**, a ne n rješenja danog sustava.

Uz sustav (2) na prirodan način vežemo neke matrice. Prije svega, koeficijente u sustavu možemo shvatiti kao elemente jednoznačno određene matrice

$$A = [\alpha_{ik}] = \begin{bmatrix} \alpha_{11} & \cdots & \alpha_{1n} \\ \vdots & & \vdots \\ \alpha_{m1} & \cdots & \alpha_{mn} \end{bmatrix} \tag{5}$$

tipa (m, n), u kojoj skalari α_{ik} zadržavaju istu poziciju koju imaju u sustavu (2). Tu matricu nazivamo **osnovna matrica sustava**, ili kraće, **matrica sustava** (2). Nadalje, bit će nam potrebna i matrica

$$A_p = \left[\begin{array}{c|c} \alpha_{ik} & \beta_i \end{array}\right] = \left[\begin{array}{ccc|c} \alpha_{11} & \cdots & \alpha_{1n} & \beta_1 \\ \vdots & & \vdots & \vdots \\ \alpha_{m1} & \cdots & \alpha_{mn} & \beta_m \end{array}\right] \tag{6}$$

tipa $(m, n+1)$, koja se dobiva iz matrice A dodavanjem stupca slobodnih članova, i koju nazivamo **proširena matrica sustava** (2). Slobodne članove sustava možemo shvatiti kao elemente stupčane matrice

$$B = [\beta_i] = \begin{bmatrix} \beta_1 \\ \vdots \\ \beta_m \end{bmatrix} \tag{7}$$

tipa $(m, 1)$. Ako i nepoznanice $x_1, \ldots, x_n$ zapišemo pomoću stupčane matrice

$$X = [x_k] = \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} , \tag{8}$$

naravno, tipa $(n, 1)$, odmah vidimo da se sustav (2) može zapisati u obliku **matrične jednadžbe**

$$AX = B , \tag{9}$$

u kojoj je X nepoznata matrica (matrica nepoznanica). Sustav (2) i jednadžba (9) su različiti zapisi iste činjenice. U (9) se, naime, tvrdi da su matrice AX i B međusobno jednake, a to će biti ako i samo ako je ispunjeno

$$\sum_{k=1}^{n} \alpha_{ik} x_k = \beta_i ,$$

za svaki $i = 1, 2, \ldots, m$, što je upravo sustav (2).

Naravno, rješenje matrične jednadžbe (9) bit će stupčana matrica

$$C = [\gamma_k] = \begin{bmatrix} \gamma_1 \\ \vdots \\ \gamma_n \end{bmatrix} , \tag{10}$$

za koju supstitucija $X = C$ u jednadžbu (9) daje matričnu jednakost

$$AC = B .$$

Prema tome, svako rješenje (4) sustava (2) određuje matricu (10), koja je rješenje jednadžbe (9), a vrijedi i obratno, tj. problem rješenja sustava (2) je ekvivalentan s problemom rješenja matrične jednadžbe (9).

Kako smo rekli, naša je želja riješiti dani sustav. Prema tome, jasno je da se teorija linearnih sustava u suštini svodi na razmatranje ovih osnovnih problema:

1. Problem egzistencije rješenja.

Postavlja se pitanje koji su nužni i dovoljni uvjeti da bi sustav (2) imao bar jedno rješenje. Ako takvo rješenje postoji, kažemo da je sustav **rješiv**, **moguć** ili **kompatibilan**. Naprotiv, ako sustav ne dopušta nijedno rješenje, kažemo da je takav sustav **nerješiv**, **nemoguć**, odnosno, **inkompatibilan**. Na primjer, sustav

$$\left.\begin{aligned} x + 2y &= 9 \\ 2x - 3y &= 4 \end{aligned}\right\} \tag{11}$$

je rješiv, dok sustav

$$\left.\begin{array}{rl} x+2y & =5 \\ x+2y & =15 \end{array}\right\} \tag{12}$$

nije rješiv. Problem, dakle, možemo formulirati ovako: Treba naći kriterije za egzistenciju rješenja sustava (2).

2. Problem jedinstvenosti rješenja.

Ako je sustav rješiv, postavlja se pitanje uz koje će uvjete imati jedno jedino rješenje, tj. koji je kriterij za jedinstvenost rješenja. Na primjer, sustav (11) ima samo jedno rješenje $x = 5$, $y = 2$.

3. Problem strukture skupa rješenja.

Ako sustav ima više rješenja, pitanje je koliko ih ima i u kakvoj su vezi? Drugim riječima, kakva je struktura skupa svih rješenja? Na primjer, sustav

$$\left.\begin{array}{rl} x+2y & =4 \\ 3x+6y & =12 \end{array}\right\} \tag{13}$$

ima beskonačno mnogo rješenja, i ona su oblika $x = 4-2t$, $y = t$, gdje je t bilo koji realan broj. Kako ćemo vidjeti (točka 11.2.), rješenja sustava se mogu interpretirati kao vektori, pa se postavlja pitanje koliko je među njima linearno nezavisnih.

4. Problem efektivnog rješavanja sustava.

Radi se o problemu nalaženja jednog razumnog numeričkog postupka, algoritma, koji će omogućiti da se stvarno nađu **sva** rješenja danog sustava. Na primjer, lako se vidi da se sustav (11) može zamijeniti ekvivalentnim sustavom

$$\left.\begin{array}{rl} x+2y & =9 \\ -7y & =-14 \end{array}\right\}, \tag{14}$$

iz kojeg se rješenje lako pročita. Postoje, dakako, razne metode rješavanja sustava. Neke od njih prikazujemo i ovdje.

11.2. Geometrijska interpretacija

Matrična jednadžba (9) u točki 11.1. sugerira da problemima u teoriji linearnih sustava damo geometrijsku interpretaciju, koristeći se pojmovima i činjenicama iz teorije linearnih prostora i linearnih operatora, koju smo upoznali u prethodnim poglavljima. To će često znatno pojednostavniti naša razmatranja i zaključivanja.

Uvodno, uočimo jednostavno svojstvo prostora stupaca, koje izlazi neposredno iz opće teorije. Neka je

$$M_{n1} = M_{n1}(F) = \{ \begin{bmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{bmatrix} \mid \alpha_i \in F \}$$

linearni prostor stupčanih matrica, $\dim M_{n1} = n$. Neka je

$$E = (e_1, \ldots, e_n)$$

kanonska ili **standardna baza** za taj prostor, gdje je

$$e_i = \begin{bmatrix} 0 \\ \vdots \\ 1 \\ \vdots \\ 0 \end{bmatrix} \leftarrow i\text{-ti redak} \quad ,$$

za $i = 1, \ldots, n$.

Neka je sada $x \in M_{n1}$ bilo koji vektor, a X njegova koordinatna matrica u bazi E. Onda imamo redom

$$x = \begin{bmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{bmatrix} = \alpha_1 \begin{bmatrix} 1 \\ \vdots \\ 0 \end{bmatrix} + \cdots + \alpha_n \begin{bmatrix} 0 \\ \vdots \\ 1 \end{bmatrix} = \alpha_1 e_1 + \cdots + \alpha_n a_n \ ,$$

pa je koordinatna matrica tog vektora baš

$$X = \begin{bmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{bmatrix} .$$

Zaključujemo da je

$$x = X \ ,$$

tj. **vektor** iz prostora M_{n1} **podudara se sa svojom koordinatnom matricom**.

Vratimo se sada problemu geometrijske interpretacije linearnog sustava. Neka je, dakle, $M_{m1} = M_{m1}(F)$ drugi prostor stupčanih matrica, $\dim M_{m1} = m$, i neka je

$$F = (f_1, \ldots, f_m)$$

kanonska baza za taj prostor.

Ako sada, kao u točki 11.1., promatramo sustav od m linearnih jednadžbi s n nepoznanica, onda matricu

$$A = [\alpha_{ik}]$$

tog sustava, koja je tipa (m, n), možemo (zbog Tm. 2 u 10.4.), interpretirati kao matrični zapis jednoznačno određenog linearnog operatora

$$f : M_{n1} \to M_{m1} ,$$

$$f(e_k) = f\left(\begin{bmatrix} 0 \\ \vdots \\ 1 \\ \vdots \\ 0 \end{bmatrix}\right)^{\swarrow k} = \sum_{i=1}^{m} \alpha_{ik} f_i = \sum_{i=1}^{m} \alpha_{ik} \begin{bmatrix} 0 \\ \vdots \\ 1 \\ \vdots \\ 0 \end{bmatrix}^{\swarrow i} = \begin{bmatrix} \alpha_{1k} \\ \vdots \\ \alpha_{mk} \end{bmatrix} \in M_{m1} ,$$

u fiksiranom paru (kanonskih) baza. Nadalje, stupčanu matricu

$$B = [\beta_i]$$

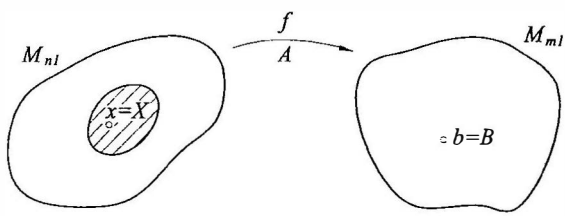
slobodnih članova sustava možemo shvatiti kao koordinatnu matricu nekog vektora $b \in M_{m1}$ u bazi F, a jer je to kanonska baza, vrijedi dakako $b = B$.

Sada je jasno da **matričnu jednadžbu**

$$AX = B , \tag{1}$$

za koju smo u 11.1. utvrdili da je ekvivalentna sustavu linearnih jednadžbi (2) iz 11.1., možemo uz navedenu geometrijsku interpretaciju matrica, a zbog Prop. 3 iz 10.3., zapisati kao **operatorsku jednadžbu**

$$f(x) = b , \tag{2}$$



odnosno (kanonske baze!) kao jednadžbu

$$f(X) = B . \tag{3}$$

Prema tome, stupčana matrica $X = [x_k]$ bit će rješenje jednadžbe (1) ako i samo ako vektor $X \in M_{n1}$ zadovoljava operatorsku jednadžbu (3). Drugim riječima, skup R svih rješenja jednadžbe (1), odnosno (3), dakle našeg linearnog sustava, jednoznačno je određen kao

$$R = f^{-1}(B)\,, \tag{4}$$

tj. kao skup svih praslika vektora B.

U točkama koje slijede nastojat ćemo odgovoriti, djelomično i pomoću upravo opisane geometrijske interpretacije, na osnovna pitanja teorije linearnih sustava, formulirana u 11.1.

ZADACI

1. Uoči da za geometrijsku interpretaciju nije bitno promatrati baš prostore stupaca. Umjesto njih možemo promatrati bilo koje linearne prostore U i V nad F, dimenzije n, odnosno m.

2. Uvjeri se da se za svaki linearni operator $f : U \to V$ i svaki vektor $b \in V$ problem određivanja **svih** vektora $x \in U$, koji zadovoljavaju operatorsku jednadžbu $f(x) = b$, svodi na rješavanje sustava linearnih jednadžbi.

11.3. Egzistencija rješenja

U ovoj točki odgovaramo na prvo od pitanja koja smo postavili u 11.1. Kako smo primijetili u prethodnoj točki, u geometrijskoj interpretaciji je skup rješenja linearnog sustava dan relacijom

$$R = f^{-1}(B)\,,$$

i prema tome sustav će biti rješiv ako i samo ako taj skup nije prazan, dakle ako i samo ako je

$$B \in f(M_{n1}) = S(f)\,, \tag{1}$$

tj. $B \in M_{m1}$ je u slici operatora f. Iako jasan i elegantan, uvjet (1) nije prikladan za praktičnu upotrebu. Zato ćemo ga razraditi, kako bismo dobili kriterij za rješivost sustava na razini matrica, s kojima znamo računati.

Neka je, dakle, $E = (e_1, \ldots, e_n)$ kanonska baza prostora M_{n1}. Sliku $S(f) < M_{m1}$ operatora f onda će razapinjati vektori

$$(f(e_1), \ldots, f(e_n))\,.$$

Prema tome, vektor B će biti u slici od f ako i samo ako ga možemo prikazati kao

$$B = \sum_{k=1}^{n} \gamma_k f(e_k) = \sum_{k=1}^{n} \gamma_k \begin{bmatrix} \alpha_{1k} \\ \vdots \\ \alpha_{mk} \end{bmatrix} , \tag{2}$$

tj. ako i samo ako je posljednji stupac proširene matrice sustava,

$$A_p = \left[\begin{array}{c|c} A & B \end{array} \right] ,$$

linearna kombinacija prethodnih stupaca te matrice, dakle stupaca matrice A. Odatle slijedi da će, u tom slučaju, biti moguće izabrati jedan te isti maksimalni linearno nezavisni podskup skupova stupaca matrica A_p i A. Kao zaključak imamo ovaj klasični

TEOREM 1 (Kronecker–Capelli)

Da bi sustav linearnih jednadžbi bio rješiv, nužno je i dovoljno da matrica tog sustava i njegova proširena matrica imaju isti rang, tj. da je

$$r(A_p) = r(A) .$$

Dokaz

Neposredno iz prethodnog razmatranja i definicije ranga matrice. ■

Primijetimo da je relacija (2) ekvivalentna s

$$\beta_i = \sum_{k=1}^{n} \alpha_{ik} \gamma_k , \tag{3}$$

za $i = 1, \ldots, m$, što pokazuje da su koeficijenti

$$(\gamma_1, \ldots, \gamma_n)$$

u prikazu (2) jedno rješenje promatranog linearnog sustava. To rješenje ne mora biti jedinstveno, jer prikaz (2) općenito nije jednoznačan.

Neposredna posljedica Tm. 1 je ovaj

KOROLAR 2

Ako je rang matrice sustava jednak broju jednadžbi, tj.

$$r(A) = m ,$$

onda je takav sustav sigurno rješiv.

Dokaz

Ako je $r(A) = m$, tada je nužno $r(A_p) = r(A)$, jer je taj rang već maksimalan za obje matrice, pa tvrdnja slijedi iz Tm. 1. ■

Rezultat koji daje Kor. 2 geometrijski je očigledan. Naime,

$$r(A) = r(f) = \dim S(f) = m$$

povlači da je

$$S(f) = M_{m1} ,$$

tj. f je surjektivan, pa je jasno da je $f^{-1}(B) \neq \emptyset$.

ZADACI

1. Dokaži Tm. 1 ne koristeći se geometrijskim argumentima, nego samo svojstvima matrica.

2. Utvrdi je li rješiv sustav

$$\begin{array}{rcrcrcrcl} 3x_1 & + & x_2 & - & 2x_3 & + & x_4 & - & x_5 = 1 \\ 2x_1 & - & x_2 & + & 7x_3 & - & 3x_4 & + & 5x_5 = 2 \\ x_1 & + & 3x_2 & - & 2x_3 & + & 5x_4 & - & x_5 = 3 \\ 3x_1 & - & 2x_2 & + & 7x_3 & - & 5x_4 & + & 8x_5 = 3. \end{array}$$

   [Rješenje: Nije rješiv.]

3. Odredi λ tako da sustav

$$\begin{array}{rcrcrcrcrcl} x_1 & + & 3x_2 & - & x_3 & - & 5x_4 & + & x_5 & = & -2 \\ 2x_1 & + & x_2 & + & x_3 & - & 5x_4 & - & 2x_5 & = & 2 \\ 3x_1 & - & 9x_2 & + & x_3 & + & 3x_4 & + & 9x_5 & = & 2 \\ 5x_1 & - & 8x_2 & + & 2x_3 & - & 2x_4 & + & 7x_5 & = & \lambda \end{array}$$

   bude rješiv. [Rješenje: $\lambda = 4$.]

11.4. Cramerov sustav

Pretpostavimo sada da imamo rješiv sustav linearnih jednadžbi, tj. da je

$$R = f^{-1}(B) \neq \emptyset .$$

Sljedeći je problem utvrditi uz koje će uvjete rješenje tog sustava biti jedinstveno. Imamo odmah i jednostavan odgovor

PROPOZICIJA 1

Neka je sustav linearnih jednadžbi rješiv. Rješenje sustava je jedinstveno ako i samo ako je operator f injektivan.

Dokaz

Neka je $C \in M_{n1}$ jedinstveno rješenje sustava $AX = B$, tj. operatorske jednadžbe

$$f(X) = B\,.$$

Tada je sigurno

$$f(C) = B\,. \tag{1}$$

Kad operator f ne bi bio injektivan, njegova jezgra ne bi bila trivijalna (vidi Zad. 1. u 8.5.), tj. postojao bi vektor $C_0 \in M_{n1}$, $C_0 \neq O$, takav da je

$$f(C_0) = O\,. \tag{2}$$

No onda bismo, zbrajanjem (1) i (2), zbog linearnosti od f imali

$$f(C + C_0) = f(C) + f(C_0) = B\,,$$

pa bi i $C + C_0 \neq C$ bilo rješenje našeg sustava, protivno pretpostavci da je rješenje jedinstveno. Prema tome, f je injektivan.

Obratno, ako je operator f injektivan, operatorska jednadžba

$$f(X) = B$$

imat će za **svaki** $B \in M_{m1}$ najviše jedno rješenje. Jer je po pretpostavci sustav rješiv, tvrdnja je dokazana. ■

Kao specijalan slučaj imamo

KOROLAR 2

Rješivi sustav, u kojem se broj jednadžbi podudara s brojem nepoznanica, imat će jedinstveno rješenje ako i samo ako je operator f regularan.

Dokaz

Neposredno iz Prop. 1, uzimajući u obzir činjenicu da je sada injektivni operator

$$f : M_{n1} \to M_{n1}$$

i surjektivan, dakle bijektivan, tj. regularan. ■

Za tako "lijepe" i tradicionalno najvažnije sustave imamo onda i posebno ime. Za sustav linearnih jednadžbi kažemo da je **Cramerov**, ako je

(1) $m = n$, tj. broj jednadžbi je jednak broju nepoznanica, i

(2) $r(A) = n$, tj. rang matrice sustava je maksimalan, odnosno matrica je regularna.

Uočimo da je tu bitan uvjet (2), jer se (1) uvijek može postići na umjetni način. Dakako, uvjet (2) možemo zapisati i kao

$$\det A \neq 0 \,. \tag{3}$$

Imamo odmah i zaključak

KOROLAR 3

Cramerov sustav ima uvijek jedno i samo jedno rješenje.

Dokaz

Kako je u Cramerovu sustavu

$$r(A) = n = m = \text{ broj jednadžbi} \,,$$

sustav ima bar jedno rješenje, po Kor. 2 iz 11.3. Rješenje je jedinstveno po Kor. 2: zbog $\det f = \det A \neq 0$ operator $f : M_{n1} \to M_{n1}$ je regularan. ■

Kor. 3 nam osigurava egzistenciju rješenja Cramerova sustava samo teorijski. Naravno, sljedeće je pitanje kako to rješenje izgleda, tj. kako se može izračunati. Neka je

$$D = \det A \,,$$

a D_k neka je determinanta koja se iz determinante D dobiva tako da se njezin k-ti stupac zamijeni stupcem slobodnih članova, tj.

$$D_k = \begin{vmatrix} \alpha_{11} & \cdots & \alpha_{1\,k-1} & \beta_1 & \alpha_{1\,k+1} & \cdots & \alpha_{1n} \\ \vdots & & \vdots & \vdots & \vdots & & \vdots \\ \alpha_{n1} & \cdots & \alpha_{n\,k-1} & \beta_n & \alpha_{n\,k+1} & \cdots & \alpha_{nn} \end{vmatrix} .$$

Onda imamo

TEOREM 4

Jedinstveno rješenje Cramerova sustava je oblika

$$\gamma_k = D_k \cdot D^{-1} \,, \quad k = 1, \ldots, n \,.$$

Dokaz

Treba vidjeti da to rješenje zadovoljava sve jednadžbe sustava (2) iz 11.1. Pokažimo da zadovoljava i-tu jednadžbu, za bilo koji $i = 1, \ldots, n$. Polazeći od lijeve strane i koristeći se Prop. 1 te Kor. 4 u 9.9. imamo

$$\sum_{k=1}^{n} \alpha_{ik}\,\gamma_k = \sum_{k=1}^{n} \alpha_{ik}\,D_k \cdot D^{-1} = D^{-1} \sum_{k=1}^{n} \alpha_{ik}\,D_k =$$

$$= D^{-1} \sum_{k=1}^{n} \alpha_{ik} \left(\sum_{j=1}^{n} \beta_j\,A_{jk}\right) = D^{-1} \sum_{j=1}^{n} \beta_j \left(\sum_{k=1}^{n} \alpha_{ik}\,A_{jk}\right) =$$

$$= D^{-1} \left(\sum_{j=1}^{n} \beta_j \cdot \delta_{ij}\,D\right) = D^{-1} \cdot \beta_i \cdot D = \beta_i \ .$$

Tu je, dakako, s A_{jk} bio označen algebarski komplement elementa α_{jk} u matrici sustava A. Razabiremo kako smo pokazali da uređena n-torka

$$(\gamma_1, \cdots, \gamma_n)$$

zadovoljava jednadžbe

$$\sum_{k=1}^{n} \alpha_{ik}\,x_k = \beta_i \ , \qquad i = 1, \ldots, n \ ,$$

pa je teorem dokazan. ■

Napomenimo da navedeni postupak rješavanja Cramerova sustava ima više teorijsko značenje i da u praksi nije upotrebljiv u slučaju kad je n velik.

ZADACI

1. Kao primjenu Cramerova sustava, dokaži ovaj teorem: U ortogonalnoj matrici se svaki element do na predznak podudara sa svojim algebarskim komplementom. Točnije, ako je $A = [\alpha_{ik}]$ ortogonalna matrica, onda je

$$\begin{aligned} \alpha_{ik} &= \ \ A_{ik} \ , \ \text{ako je} \ \ \det A = \ \ 1 \ , \\ \alpha_{ik} &= -A_{ik} \ , \ \text{ako je} \ \ \det A = -1 \ . \end{aligned}$$

2. Pokaži da je sustav

$$\begin{aligned} 2x \ - \ 3y \ + \ 5z \ &= 1 \\ x \ + \ 2y \ - \ 2z \ &= 2 \\ 3x \ - \ \ y \ - \ \ z \ &= 3 \end{aligned}$$

Cramerov i nađi njegovo rješenje.

11.5. Homogeni sustav

U točkama koje slijede rješavamo treći osnovni problem u našem programu iz točke 11.1., tj. odgovaramo na pitanje o strukturi skupa svih rješenja linearnog sustava. Najprije ćemo nešto reći o jednom specijalnom slučaju problema.

Za linearni sustav kažemo da je **homogen** ako su svi slobodni članovi jednaki nuli,

$$\beta_i = 0 \quad , \quad i = 1, \ldots, m \, ,$$

tj. ako je oblika

$$\sum_{k=1}^{n} \alpha_{ik} \, x_k = 0 \, , \quad i = 1, \ldots, m \, , \tag{1}$$

ili, u matričnoj formi,

$$AX = O \, , \tag{2}$$

gdje je $O \in M_{m1}$, dakako, nulmatrica.

Jasno je da je takav sustav uvijek rješiv, jer ima bar jedno rješenje,

$$x_1 = x_2 = \cdots = x_n = 0 \, , \tag{3}$$

ili kraće

$$X = O \, ,$$

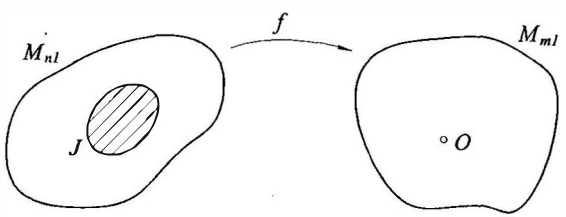
koje nazivamo **trivijalnim rješenjem** homogenog sustava. Od interesa su eventualna rješenja različita od (3), tzv. **netrivijalna rješenja sustava**.

U geometrijskoj interpretaciji, danom homogenom sustavu je, uz operator $f : M_{n1} \to M_{m1}$, pridružen i vektor $B = O$, nulvektor iz prostora M_{m1}, pa je skup rješenja jednak

$$R = f^{-1}(O) = J(f) = J \, ,$$

tj. podudara se s jezgrom operatora f.

Prema tome, $C \in M_{n1}$ je rješenje homogenog sustava (2) ako i samo ako je C vektor iz jezgre operatora f. Međutim, kako znamo, jezgra je



potprostor od M_{n1} i njezina je dimenzija defekt $d(f)$ operatora f. Kako je, prema teoremu o rangu i defektu,

$$d(f) = n - r(f) \,, \tag{4}$$

i jer je $r(f) = r(A)$, imamo ovaj zaključak:

PROPOZICIJA 1

Homogeni sustav ima

(1) *samo trivijalno rješenje, ako i samo ako je* $r(A) = n$;

(2) *i netrivijalna rješenja, ako i samo ako je* $r(A) < n$. ■

Odatle odmah slijedi

KOROLAR 2

Homogeni sustav, u kojem je broj jednadžbi manji od broja nepoznanica, uvijek ima i netrivijalna rješenja.

Dokaz

Onda je $r(A) \leq m < n$, pa zaključak slijedi iz Prop. 1. ■

KOROLAR 3 (Roucheov teorem)

Homogeni sustav, u kojem se broj jednadžbi podudara s brojem nepoznanica, ima i netrivijalna rješenja ako i samo ako je $\det A = 0$.

Dokaz

Kad bi bilo $\det A \neq 0$, imali bismo $r(A) = m = n$ pa bi sustav imao samo trivijalno rješenje, po Prop. 1. ■

Kažimo nešto o strukturi skupa svih rješenja homogenog sustava, u slučaju kad je $r(A) < n$. Kako smo vidjeli, vektori tog skupa određuju potprostor $J < M_{n1}$, koji nazivamo **prostor rješenja sustava** (1). Taj je prostor dimenzije

$$\dim J = d = n - r \neq 0 \,,$$

gdje je $r = r(A)$. Prema tome, u prostoru J postoji točno d linearno nezavisnih vektora

$$C_1, C_2, \cdots, C_d \in J \,, \tag{5}$$

koji čine bazu tog prostora, pa se svaki vektor $C \in J$ može dobiti kao njihova linearna kombinacija,

$$C = \lambda_1 C_1 + \cdots + \lambda_d C_d \,, \quad \lambda_i \in F \,. \tag{6}$$

Vektori C_i iz baze su rješenja sustava (1), koja zovemo **fundamentalnim rješenjima** tog sustava, pa kažemo da je (5) **fundamentalni skup rješenja** sustava (1). Primijetimo da baza od J (pa onda ni fundamentalni skup rješenja) nije određena jednoznačno danim sustavom.

Iz (6) razabiremo da se svako rješenje sustava (1) može dobiti kao linearna kombinacija fundamentalnih rješenja. Ako u (6) pustimo da koeficijenti $\lambda_i \in F$ slobodno variraju, na taj način dobit ćemo sva moguća rješenja homogenog sustava. Zato kažemo da je sa (6), uz varijabilne λ_i, dano **opće rješenje sustava** (1). Prema tome, dokazali smo ovaj

TEOREM 4

Homogeni sustav, za koji je $d = n - r \neq 0$, ima točno d fundamentalnih rješenja, i svako rješenje sustava je linearna kombinacija tih rješenja. ■

ZADACI

1. Uvjeri se da homogeni sustav, u kojem se broj nepoznanica podudara s brojem jednadžbi, ima samo trivijalno rješenje ako i samo ako je $\det A \neq 0$, tj. ako i samo ako je taj sustav Cramerov.

2. Za sustav

$$\begin{aligned} x+ \quad & y \quad +z \quad = 0 \\ 3x+ \quad & y \quad -z \quad = 0 \\ 2x+ \quad & y \quad\quad = 0 \end{aligned}$$

nađi fundamentalni skup rješenja i opće rješenje.

[Jedno fundamentalno rješenje je npr. $C_1 = \begin{bmatrix} 1 \\ -2 \\ 1 \end{bmatrix}$.]

11.6. Nehomogeni sustav

Za sustav

$$\sum_{k=1}^{n} \alpha_{ik} x_k = \beta_i \ , \quad i = 1, \ldots, m \ , \tag{1}$$

kažemo da je **nehomogen** ako je bar jedan od slobodnih članova u tom sustavu različit od nule. U matričnom zapisu to je sustav

$$AX = B$$

u kojem je

$$B \neq O \ . \tag{2}$$

Svakom nehomogenom sustavu jednoznačno je pridružen homogeni sustav

$$\sum_{k=1}^{n} \alpha_{ik} x_k = 0 \ , \quad i = 1, \ldots, m \ , \tag{3}$$

odnosno

$$AX = O \ , \tag{4}$$

koji nazivamo **pripadni homogeni sustav** sustava (1).

Pretpostavimo da je sustav (1) rješiv, tj. da je

$$r(A_p) = r(A) = r \ .$$

Za broj r onda kažemo da je **rang sustava**. Željeli bismo naći sva rješenja sustava (1), koristeći se pritom općim rješenjem pripadnog homogenog sustava.

Pogledajmo geometrijski aspekt našeg problema. Neka je $f : M_{n1} \to M_{m1}$ linearni operator pridružen sustavu (1). Kako je sustav rješiv po pretpostavci, to je skup rješenja

$$R = f^{-1}(B) \neq \emptyset \ .$$

Neka je C_0 bilo koji vektor iz R, tj. neka je

$$f(C_0) = B \ . \tag{5}$$

Tada kažemo da je C_0 jedno **partikularno rješenje** nehomogenog sustava (1). Ako je $C \in R$ bilo koje drugo rješenje sustava (1),

$$f(C) = B \ , \tag{6}$$

iz (5) i (6) imamo

$$f(C - C_0) = f(C) - f(C_0) = B - B = O \ . \tag{7}$$

No, iz (7) čitamo da je

$$C - C_0 \in J \ ,$$

gdje je $J = J(f)$ jezgra operatora f. Odatle slijedi da je

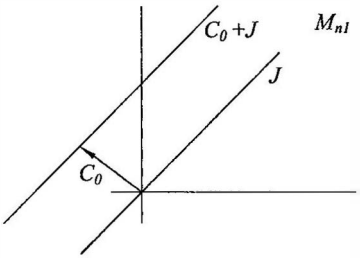
$$C \in C_0 + J \ ,$$

tj. svako rješenje sustava (1) pripada skupu $C_0 + J$. Lako se pokaže da vrijedi i obrnuto, i prema tome je

$$R = C_0 + J \ . \tag{8}$$

No, kako smo vidjeli u točki 7.8., skupovi oblika (8) su elementi kvocijentnog

prostora, tj. linearne mnogostrukosti. U našem slučaju, skup (8) je vektor



u prostoru M_{n1}/J. Prema tome, vrijedi

PROPOZICIJA 1

Skup $R \subset M_{n1}$ svih rješenja nehomogenog sustava je linearna mnogostrukost u prostoru M_{n1}, generirana bilo kojim rješenjem C_0 tog sustava i "paralelna" s jezgrom J linearnog operatora pridruženog sustavu. ■

Ta mnogostrukost je, dakako, dimenzije (vidi 7.8.)

$$\dim R = \dim J = d = n - r \, .$$

Prevedimo sada ovaj rezultat na razumljiviji i operativniji jezik matrica. Primijetimo da jednakost (7) možemo zapisati kao matričnu jednakost

$$A(C - C_0) = O \, ,$$

koja pokazuje da $C - C_0$ zadovoljava matričnu jednadžbu (4). Na temelju toga zaključujemo:

PROPOZICIJA 2

Razlika bilo kojih dvaju rješenja nehomogenog sustava je jedno rješenje pripadnog homogenog sustava. ■

Ako je, dakle,

$$(C_1, \ldots, C_d)$$

fundamentalni skup rješenja homogenog sustava (3), onda postoje skalari $\lambda_i \in F$ takvi da je

$$C - C_0 = \sum_{i=1}^{d} \lambda_i C_i \, ,$$

i prema tome je

$$C = C_0 + \lambda_1 C_1 + \cdots + \lambda_d C_d \, . \tag{9}$$

Svako se, dakle, rješenje nehomogenog sustava može, za neki izbor skalara λ_i, napisati u obliku (9). Lako se provjeri da vrijedi i obratno, tj. da je za svaki izbor $\lambda_i \in F$ s (9) dano neko rješenje sustava (1). Prema tome, s (9), uz varijabilne λ_i, opisano je **opće rješenje nehomogenog sustava**. Dokazali smo, dakle,

TEOREM 3

Opće rješenje rješivog nehomogenog sustava jednako je sumi bilo kojeg partikularnog rješenja tog sustava i općeg rješenja pripadnog homogenog sustava. ■

ZADACI

1. Uoči da u slučaju kad pripadni homogeni sustav ima samo trivijalno rješenje, Tm. 3 tvrdi da je partikularno rješenje nehomogenog sustava ujedno i jedino rješenje tog sustava. To je npr. slučaj kad je nehomogeni sustav Cramerov (ali ne samo onda).

11.7. Gauss–Jordanova metoda eliminacije

Na kraju smo došli do problema efektivnog algoritma za rješavanje svakog rješivog sustava. Navest ćemo najprije Gauss–Jordanov postupak koji je generalizacija uobičajenog postupka obrađenog u srednjoj školi pri rješavanju sustava s dvije ili tri nepoznanice. Ta je metoda prikladna iz više razloga. Njome se može istodobno odrediti je li sustav rješiv ili nije, pa ako jest, efektivno naći sva njegova rješenja. Spomenimo da je algoritam u toj metodi prikladan i za primjenu računala.

Definirajmo najprije pojam ekvivalentnih sustava. Za dva sustava nad istim poljem F i s istim brojem nepoznanica (ne nužno istim brojem jednadžbi) kažemo da su **ekvivalentni**, ako imaju isti skup rješenja, tj. ako je svako rješenje prvog sustava ujedno i rješenje drugog sustava, i obratno, svako rješenje drugog sustava je i rješenje prvog.

Pogledajmo sada pod kojim uvjetima dani sustav prelazi u ekvivalentan. Kažemo da smo proveli **elementarnu transformaciju** nad sustavom ako smo obavili neki od sljedećih zahvata:

I. Zamijenili poredak dviju jednadžbi u sustavu;

II. Pomnožili neku jednadžbu sustava skalarom različitim od nule;

III. Nekoj od jednadžbi sustava pribrojili neku drugu jednadžbu sustava.

Onda vrijedi

PROPOZICIJA 1

Konačnim brojem elementarnih transformacija linearni sustav prelazi u sustav koji mu je ekvivalentan.

Dokaz

Jasno je da transformacijama I. i II. tipa sustav prelazi u ekvivalentan. Pokažimo da je tako i u III. slučaju. Neka je, dakle, u sustavu

$$\sum_{k=1}^{n} \alpha_{ik}\, x_k = \beta_i\,, \quad i = 1, \ldots, m\,, \tag{1}$$

i-toj jednadžbi dodana j-ta jednadžba, uz $i \neq j$. Na taj način dolazimo do novog sustava

$$\sum_{k=1}^{n} \alpha'_{ik}\, x_k = \beta'_i\,, \quad i = 1, \ldots, m\,, \tag{2}$$

u kojem su sve jednadžbe iste kao i u polaznom sustavu, osim i-te jednadžbe, koja sada glasi

$$\sum_{k=1}^{n} (\alpha_{ik} + \alpha_{jk})\, x_k = \beta_i + \beta_j\,.$$

Ako je $(\gamma_1, \ldots, \gamma_n) = (\gamma_k)$ bilo koje rješenje sustava (1), imamo posebno

$$\sum_{k=1}^{n} \alpha_{ik}\, \gamma_k = \beta_i \qquad \text{i} \qquad \sum_{k=1}^{n} \alpha_{jk}\, \gamma_k = \beta_j\,,$$

pa je

$$\begin{aligned} \sum_{k=1}^{n} \alpha'_{ik}\, \gamma_k &= \sum_{k=1}^{n} (\alpha_{ik} + \alpha_{jk})\, \gamma_k = \\ &= \sum_{k=1}^{n} \alpha_{ik}\, \gamma_k + \sum_{k=1}^{n} \alpha_{jk}\, \gamma_k = \beta_i + \beta_j = \beta'_i\,, \end{aligned}$$

što pokazuje da je (γ_k) rješenje sustava (2) jer su ostale jednadžbe sustava (2) zadovoljene trivijalno. Obratno, ako je $(\gamma'_1, \ldots, \gamma'_n) = (\gamma'_k)$ rješenje sustava (2), posebno za njegovu i-tu i j-tu jednadžbu, vrijedi

$$\sum_{k=1}^{n} (\alpha_{ik} + \alpha_{jk})\, \gamma'_k = \beta_i + \beta_j$$

i

$$\sum_{k=1}^{n} \alpha_{jk}\, \gamma'_k = \beta_j\,,$$

pa oduzimanjem dobivamo

$$\sum_{k=1}^{n} \alpha_{ik}\,\gamma'_k = \beta_i\,,$$

što pokazuje da (γ'_k) zadovoljava i-tu jednadžbu sustava (1). Kako su sve ostale jednadžbe tog sustava iste kao one u (2), to je (γ'_k) rješenje i sustava (1), dakle, sustavi (1) i (2) su ekvivalentni. ■

Može se pokazati da vrijedi i obrnuto: Ako su dva sustava ekvivalentna, jedan od njih može se dobiti iz drugoga konačnim brojem elementarnih transformacija.

Važno je sada uočiti da svaka elementarna transformacija danog sustava ima za posljedicu odgovarajuću elementarnu transformaciju provedenu **nad redcima** proširene matrice

$$A_p = \begin{bmatrix} \alpha_{11} & \cdots & \alpha_{1n} & \beta_1 \\ \vdots & & \vdots & \vdots \\ \alpha_{m1} & \cdots & \alpha_{mn} & \beta_m \end{bmatrix}$$

tog sustava. Vrijedi i obrnuto: svaka elementarna transformacija provedena nad redcima proširene matrice A_p sustava povlači odgovarajući zahvat, elementarnu transformaciju nad našim sustavom. Zapišimo, dakle, zajedno

PROPOZICIJA 2

Dva su linearna sustava ekvivalentna onda i samo onda ako su proširene matrice tih sustava ekvivalentne, i to putem niza elementarnih transformacija redaka. ■

Neka je sada

$$\sum_{k=1}^{n} \alpha_{ik}\,x_k = \beta_i\,, \quad i = 1, \ldots, m\,, \tag{3}$$

bilo koji linearni sustav i neka je $r = r(A)$ rang matrice A tog sustava. U osnovi Gauss–Jordanove metode je ideja da se taj sustav zamijeni ekvivalentnim sustavom

$$\sum_{k=1}^{n} \alpha'_{ik}\,x_k = \beta'_i\,, \quad i = 1, \ldots, r\,, \tag{4}$$

koji je moguće riješiti na posebno jednostavan način.

Postupak se sastoji u sljedećem: Polazimo od proširene matrice sustava (3),

$$A_p = \left[\begin{array}{c|c} A & B \end{array}\right],$$

u kojoj je matrica A ranga r. Elementarnim transformacijama **nad redcima** matrice A_p i eventualnim zamjenama mjesta **prvih** n **stupaca** te matrice (zadnji se stupac ne smije dirati), što odgovara prenumeraciji nepoznanica u sustavu, može se, postupkom sličnim kao pri svođenju matrice na kanonski oblik (vidi točku 9.6.), matrica A_p prevesti u matricu

$$A'_p = \begin{bmatrix} 1 & 0 & \cdots & 0 & \alpha'_{1\,r+1} & \cdots & \alpha'_{1\,n} & \beta'_1 \\ 0 & 1 & \cdots & 0 & \alpha'_{2\,r+1} & \cdots & \alpha'_{2\,n} & \beta'_2 \\ \vdots & \vdots & & \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & \alpha'_{r\,r+1} & \cdots & \alpha'_{r\,n} & \beta'_r \\ 0 & 0 & \cdots & 0 & 0 & \cdots & 0 & \beta'_{r+1} \\ \vdots & \vdots & & \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & \cdots & 0 & 0 & \cdots & 0 & \beta'_m \end{bmatrix}, \tag{5}$$

koja je očito ekvivalentna polaznoj matrici,

$$A'_p \sim A_p\,,$$

i to putem elementarnih transformacija (u biti) nad redcima. No, toj matrici odgovara posebno jednostavan sustav

$$\left.\begin{array}{rrrrrrrrr} x_1+ & & & & \alpha'_{1r+1}x_{r+1} & +\cdots+ & \alpha'_{1n}x_n = & \beta'_1 \\ & x_2+ & & & \alpha'_{2r+1}x_{r+1} & +\cdots+ & \alpha'_{2n}x_n = & \beta'_2 \\ & & & & \cdots & \cdots & \cdots & \cdots \\ & & & x_r+ & \alpha'_{rr+1}x_{r+1} & +\cdots+ & \alpha'_{rn}x_n = & \beta'_r \\ 0\cdot x_1+ & \cdots\cdots+ & & 0\cdot x_r+ & 0\cdot x_{r+1} & +\cdots+ & 0\cdot x_n = & \beta'_{r+1} \\ \cdots & \cdots\cdots & & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0\cdot x_1+ & \cdots\cdots+ & & 0\cdot x_r+ & 0\cdot x_{r+1} & +\cdots+ & 0\cdot x_n = & \beta'_m \end{array}\right\} \tag{6}$$

Na osnovi Prop. 2 zaključujemo da je taj sustav ekvivalentan sustavu (3). No, iz njega se mogu dobiti sve informacije koje želimo. Prije svega, ako je makar i jedan od slobodnih članova

$$\beta'_{r+1}, \ldots, \beta'_m$$

različit od nule, odmah zaključujemo da sustav (6), a time i polazni sustav (3), **nije rješiv**. Zaista, kad bi npr. bilo $\beta'_{r+1} \neq 0$, u sustavu bismo imali jednadžbu

$$0\cdot x_1 + \cdots + 0\cdot x_n = \beta'_{r+1}\,,$$

koju očito ne zadovoljava nijedna uređena n-torka skalara iz polja F.

Ako su pak svi $\beta'_j = 0$, za $j = r+1, \ldots, m$, sustav (6) je rješiv i može se reducirati na ekvivalentni sustav

$$\left.\begin{array}{rrrcl} x_1+ & & \alpha'_{1r+1}x_{r+1}+\cdots+\alpha'_{1n}x_n & = & \beta'_1 \\ & x_2+ & \alpha'_{2r+1}x_{r+1}+\cdots+\alpha'_{2n}x_n & = & \beta'_2 \\ & & \cdots\cdots\cdots\cdots\cdots & & \cdots \\ & x_r + & \alpha'_{rr+1}x_{r+1}+\cdots+\alpha'_{rn}x_n & = & \beta'_r \end{array}\right\}, \qquad (7)$$

koji ima samo r jednadžbi, jer su preostale jednadžbe, njih $m-r$, trivijalni identiteti $0 = 0$. Naravno, i taj je sustav ekvivalentan polaznom sustavu (3), i to je sustav (4) koji smo tražili. Naime, iz sustava (7) rješenja se mogu pročitati neposredno:

$$\left.\begin{array}{rcl} x_1 & = & \beta'_1 - \alpha'_{1\,r+1}\,t_1 - \cdots - \alpha'_{1n}\,t_d \\ x_2 & = & \beta'_2 - \alpha'_{2\,r+1}\,t_1 - \cdots - \alpha'_{2n}\,t_d \\ \cdots & & \cdots\cdots\cdots\cdots \\ x_r & = & \beta'_r - \alpha'_{r\,r+1}\,t_1 - \cdots - \alpha'_{rn}\,t_d \\ x_{r+1} & = & t_1 \\ \cdots & & \cdots \\ x_n & = & t_d \end{array}\right\}, \qquad (8)$$

gdje je $d = n - r$, a $t_1, t_2, \ldots, t_d \in F$ su bilo koji elementi polja, tzv. **slobodni parametri**.

Lako se provjeri da je s (8) dano opće rješenje sustava (7), tj. da ga je moguće napisati u obliku

$$X = C_0 + H\,,$$

gdje je C_0 jedno partikularno rješenje sustava, a H opće rješenje pripadnog homogenog sustava (Tm. 3 u 11.6.). Zaista, za $t_1 = \cdots = t_d = 0$ dobivamo partikularno rješenje

$$C_0 = \begin{bmatrix} \beta'_1 \\ \vdots \\ \beta'_r \\ 0 \\ \vdots \\ 0 \end{bmatrix}$$

sustava (7), što se odmah vidi. Nadalje, odaberimo $d = n - r$ rješenja pripadnog homogenog sustava stavljajući za parametre redom:

za prvo rješenje: $t_1 = 1, t_2 = 0, \ldots, t_d = 0$;
za drugo rješenje: $t_1 = 0, t_2 = 1, \ldots, t_d = 0$;
$\vdots$
za d-to rješenje: $t_1 = 0, t_2 = 0, \ldots, t_d = 1$.

Ta su rješenja oblika

$$C_1 = \begin{bmatrix} -\alpha'_{1\,r+1} \\ \vdots \\ -\alpha'_{r\,r+1} \\ 1 \\ \vdots \\ 0 \end{bmatrix}, \cdots, \quad C_d = \begin{bmatrix} cc - \alpha'_{1\,n} \\ \vdots \\ -\alpha'_{r\,n} \\ 0 \\ \vdots \\ 1 \end{bmatrix},$$

i za njih se odmah vidi da su linearno nezavisna jer je njihova matrica tipa (n, d), gdje je $d \leq n$, i oblika

$$M(\{C_1, \ldots, C_d\}) = \left.\begin{bmatrix} -\alpha'_{1\,r+1} & \cdots & -\alpha'_{1n} \\ \vdots & & \vdots \\ -\alpha'_{r\,r+1} & \cdots & -\alpha'_{rn} \\ 1 & & 0 \\ \vdots & \ddots & \vdots \\ 0 & & 1 \end{bmatrix}\right\} n - r = d,$$

za koju je očito da je maksimalnog ranga d. Kako je tih rješenja baš $d = n-r$, jasno je da čine jedan fundamentalni skup rješenja za pripadni homogeni sustav sustava (7). Prema tome je

$$X = C_0 + t_1 C_1 + \cdots + t_d C_d,$$

uz varijabilne $t_i \in F$, opće rješenje sustava (7). No, odmah se vidi da je to upravo rješenje (8), zapisano u matričnoj formi. Dakle, zaista je (8) opće rješenje sustava (7).

Konačno, jer je sustav (7) ekvivalentan sa sustavom (6), a taj sa sustavom (3), to je (8) i opće rješenje sustava (3), koje smo tražili.

Za ilustraciju tog postupka riješimo npr. sustav

$$\begin{array}{rcrcrcrcrcr} x_1 & + & 2x_2 & + & 2x_3 & + & 3x_4 & + & x_5 & = & 3 \\ 2x_1 & & & - & x_3 & - & x_4 & + & 5x_5 & = & 2 \\ x_1 & + & 2x_2 & + & 6x_3 & - & x_4 & + & 5x_5 & = & 3 \\ x_1 & - & 2x_2 & + & 5x_3 & - & 12x_4 & + & 12x_5 & = & -1 \end{array}.$$

Imamo

$$A_p = \begin{bmatrix} 1 & 2 & 2 & 3 & 1 & 3 \\ 2 & 0 & -1 & -1 & 5 & 2 \\ 1 & 2 & 6 & -1 & 5 & 3 \\ 1 & -2 & 5 & -12 & 12 & -1 \end{bmatrix} \sim \begin{bmatrix} 1 & 2 & 2 & 3 & 1 & 3 \\ 0 & -4 & -5 & -7 & 3 & -4 \\ 0 & 0 & 4 & -4 & 4 & 0 \\ 0 & -4 & 3 & -15 & 11 & -4 \end{bmatrix} \sim$$

$$\sim \begin{bmatrix} 1 & 2 & 2 & 3 & 1 & 3 \\ 0 & 1 & 5/4 & 7/4 & -3/4 & 1 \\ 0 & 0 & 1 & -1 & 1 & 0 \\ 0 & -4 & 3 & -15 & 11 & -4 \end{bmatrix} \sim \begin{bmatrix} 1 & 0 & -1/2 & -1/2 & 5/2 & 1 \\ 0 & 1 & 5/4 & 7/4 & -3/4 & 1 \\ 0 & 0 & 1 & -1 & 1 & 0 \\ 0 & 0 & 8 & -8 & 8 & 0 \end{bmatrix} \sim$$

$$\sim \begin{bmatrix} 1 & 0 & 0 & -1 & 3 & 1 \\ 0 & 1 & 0 & 3 & -2 & 1 \\ 0 & 0 & 1 & -1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} .$$

Kako se u donjem desnom kutu posljednje matrice nalazi 0, odmah zaključujemo da je sustav rješiv. Nadalje, vidimo da je $r(A) = 3$, i polazni se sustav svodi na ekvivalentni

$$\begin{aligned} x_1 \quad\quad\quad - \; x_4 + 3x_5 &= 1 \\ x_2 \quad + \; 3x_4 - 2x_5 &= 1 \\ x_3 - \; x_4 + \; x_5 &= 0 , \end{aligned}$$

koji ima opće rješenje

$$\begin{aligned} x_1 &= 1 + u - 3v \\ x_2 &= 1 - 3u + 2v \\ x_3 &= \quad u - v \\ x_4 &= \quad u \\ x_5 &= \quad\quad v , \end{aligned}$$

gdje su $u, v \in \mathbb{R}$ slobodni parametri. Zapisano matrično, rješenje je

$$\begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} + u \begin{bmatrix} 1 \\ -3 \\ 1 \\ 1 \\ 0 \end{bmatrix} + v \begin{bmatrix} -3 \\ 2 \\ -1 \\ 0 \\ 1 \end{bmatrix} ,$$

gdje je prva matrica s desne strane jednakosti jedno partikularno rješenje sustava, a ostale dvije formiraju fundamentalni skup rješenja pripadnog homogenog sustava (tj. gledano geometrijski, bazu jezgre pridruženog operatora u M_{51}).

ZADACI

1. Uvjeri se da je Gauss–Jordanov postupak primjenjiv i kad se radi o homogenom sustavu.

2. Riješi sljedeće sustave:

(a)
$$\begin{array}{rcrcrcr} x_1 & + & 2x_2 & + & 3x_3 & = & 3 \\ -2x_1 & & & + & x_3 & = & -2 \\ x_1 & + & 2x_2 & - & x_3 & = & 3 \\ -x_1 & + & 2x_2 & + & 12x_3 & = & 1 \end{array} .$$
[Rješenje: $x_1 = x_2 = 1$, $x_3 = 0$.]

(b)
$$\begin{array}{rcrcrcrcr} 2x_1 & + & 3x_2 & + & x_3 & + & 4x_4 & = & 1 \\ 2x_1 & + & 3x_2 & + & 4x_3 & + & x_4 & = & 0 \\ 2x_1 & + & 3x_2 & - & 2x_3 & + & 7x_4 & = & 2 \\ 2x_1 & + & 3x_2 & + & 7x_3 & - & 2x_4 & = & -1 \end{array} .$$
[Rješenje: $x_1 = 2/3 - 3/2\,u - 5/2\,v$, $x_2 = u$, $x_3 = -1/3 + v$, $x_4 = v$.]

(c)
$$\begin{array}{rcrcrcrcrcr} x_1 & + & x_2 & - & x_3 & - & 3x_4 & + & 4x_5 & = & 2 \\ 3x_1 & + & x_2 & - & x_3 & - & x_4 & & & = & 2 \\ 9x_1 & + & x_2 & - & 2x_3 & - & x_4 & - & 2x_5 & = & 5 \\ x_1 & - & x_2 & & & - & x_4 & + & 2x_5 & = & 1 \end{array} .$$
[Rješenje: $x_1 = -u + 2v$, $x_2 = -1 - 2u + 4v$, $x_3 = -3 - 6u + 10v$, $x_4 = u$, $x_5 = v$.]

3. Pod **Gaussovom metodom** podrazumijeva se svođenje matrice na gornju trokutastu, i onda rješavanje sustava postupnim supstitucijama "odozdo". Razradi tu ideju.

11.8. Metoda redukcije na Cramerov sustav

Metoda je praktično primjenjiva kad sustav nema velik broj nepoznanica. Neka je

$$\sum_{k=1}^{n} \alpha_{ik}\, x_k = \beta_i\,, \quad i = 1, \ldots, m\,, \tag{1}$$

rješiv sustav, a r njegov rang, tj.

$$r(A_p) = r(A) = r\,.$$

Bez narušavanja općenitosti, možemo pretpostaviti da je **osnovna submatrica** proširene matrice sustava A_p (tj. maksimalna submatrica čija je determinanta različita od nule) smještena u gornjem lijevom kutu matrice

A_p. To se uvijek može postići zamjenom redaka (tj. poretka jednadžbi u sustavu) i zamjenom stupaca (permutacijom nepoznanica) u A_p, ne dirajući zadnji stupac. Tako dobivamo

$$A_p = \begin{bmatrix} \alpha_{11} & \cdots & \alpha_{1r} & \alpha_{1r+1} & \cdots & \alpha_{1n} & \beta_1 \\ \vdots & & \vdots & \vdots & & \vdots & \vdots \\ \alpha_{r1} & \cdots & \alpha_{rr} & \alpha_{rr+1} & \cdots & \alpha_{rn} & \beta_r \\ \vdots & & \vdots & \vdots & & \vdots & \vdots \\ \alpha_{m1} & \cdots & \alpha_{mr} & \alpha_{mr+1} & \cdots & \alpha_{mn} & \beta_m \end{bmatrix} .$$

Jednadžbe koje odgovaraju redcima osnovne submatrice nazivamo **osnovne jednadžbe sustava** (1), i one čine tzv. **osnovni sustav** pridružen sustavu (1). Nadalje, nepoznanice koje odgovaraju stupcima osnovne submatrice nazivamo **glavnima**, a ostale nepoznanice nazivamo **slobodnima**. Prema tome, osnovni je sustav oblika

$$\begin{aligned} \alpha_{11}x_1 + \quad & \cdots + \alpha_{1r}x_r + \cdots + \alpha_{1n}x_n \quad = \beta_1 \\ \vdots \qquad & \qquad\qquad\qquad\qquad\quad \vdots \qquad\quad \vdots \\ \alpha_{r1}x_1 + \quad & \cdots + \alpha_{rr}x_r + \cdots + \alpha_{rn}x_n \quad = \beta_r \end{aligned} \tag{2}$$

i pritom su $x_1, \ldots, x_r$ glavne, a $x_{r+1}, \ldots, x_n$ slobodne nepoznanice.

PROPOZICIJA 1

Sustav (1) *je ekvivalentan s pripadnim osnovnim sustavom* (2).

Dokaz

Matrica A_p ima točno r linearno nezavisnih redaka pa je svaki redak u A_p linearna kombinacija tih r redaka. Odatle slijedi da se svaka jednadžba sustava (1) može dobiti kao linearna kombinacija jednadžbi osnovnog sustava (2). To povlači da se sustav (1) može elementarnim transformacijama prevesti na sustav (2), tj. da je ekvivalentan tom sustavu. ■

Prema tome, sustavi (1) i (2) imaju isti skup rješenja. Kako je uvijek $r(A) \leq n$, sustav (2) možemo pisati kao

$$\begin{aligned} \alpha_{11}x_1 + \cdots + \alpha_{1r}x_r = \quad & \beta_1 - \alpha_{1r+1}x_{r+1} - \cdots - \alpha_{1n}x_n \\ \vdots \qquad\qquad\qquad\qquad & \qquad\qquad\qquad\qquad\qquad \vdots \\ \alpha_{r1}x_1 + \cdots + \alpha_{rr}x_r = \quad & \beta_r - \alpha_{rr+1}x_{r+1} - \cdots - \alpha_{rn}x_n \, , \end{aligned} \tag{3}$$

i shvatiti ga kao sustav u glavnim nepoznanicama $x_1, \ldots, x_r$. Budući da je po pretpostavci

$$\begin{vmatrix} \alpha_{11} & \cdots & \alpha_{1r} \\ \vdots & & \vdots \\ \alpha_{r1} & \cdots & \alpha_{rr} \end{vmatrix} \neq 0 \ ,$$

taj je sustav za **svaki** izbor skalara

$$x_{r+1} = \gamma_{r+1}\,,\ \ldots\ ,\ x_n = \gamma_n$$

Cramerov sustav, pa ima jedinstveno rješenje

$$x_1 = \gamma_1\,,\ \ldots\ ,\ x_r = \gamma_r\,.$$

To znači da opće rješenje sustava (1) ovisi o $n-r = d$ slobodnih parametara. Metoda je primjenjiva i u nehomogenom i u homogenom slučaju.

Riješimo npr. sustav

$$\begin{array}{rcrcrcl} x & - & 2y & + & z & = & 3 \\ x & + & 3y & - & z & = & 1 \\ 3x & + & 4y & - & z & = & 5 \end{array}\ .$$

Lako se provjeri da je $r(A_p) = r(A) = 2$. U matrici

$$\begin{bmatrix} 1 & -2 & 1 & 3 \\ 1 & 3 & -1 & 1 \\ 3 & 4 & -1 & 5 \end{bmatrix}$$

je, naime, treći redak linearna kombinacija prva dva. Imamo osnovni sustav

$$\begin{array}{rcrcrcl} x & - & 2y & + & z & = & 3 \\ x & + & 3y & - & z & = & 1 \end{array}\ ,$$

koji pišemo kao

$$\begin{array}{rcrcrcl} x & - & 2y & = & 3 & - & z \\ x & + & 3y & = & 1 & + & z \end{array}\ .$$

Taj sustav ima rješenje $x = 1/5(11 - z)$, $y = -2/5(1 - z)$, gdje je $z = t$ slobodni parametar. Dakle,

$$\begin{array}{rcr} x & = & 11/5 - 1/5t \\ y & = & -2/5 + 2/5t \\ z & = & t \end{array}$$

je, uz varijabilni $t \in \mathbb{R}$, opće rješenje sustava. Možemo ga zapisati i matrično kao

$$\begin{bmatrix} x \\ y \\ z \end{bmatrix} = \begin{bmatrix} 11/5 \\ -2/5 \\ 0 \end{bmatrix} + t \begin{bmatrix} -1/5 \\ 2/5 \\ 1 \end{bmatrix}\ ,$$

gdje je, kako znamo, prva matrica s desne strane jednakosti jedno partikularno rješenje sustava, a druga fundamentalno rješenje pripadnog homogenog sustava.

ZADACI

1. Ako je u rješivom sustavu rang manji od broja nepoznanica, taj sustav ima beskonačno mnogo rješenja (dakako, kad je polje F beskonačno!). Pritom se glavne nepoznanice linearno izražavaju pomoću slobodnih nepoznanica, tj. parametara. Dokaži!

2. Ponovimo i zapamtimo! Rješiv sustav (homogen ili nehomogen) ima:

   (a) jedinstveno rješenje ako i samo ako je $r(A) = n$;

   (b) beskonačno mnogo rješenja ako i samo ako je $r(A) < n$.

   Kriteriji za rješivost su npr. $r(A) = m$, homogenost, itd.

11.9. Matrične jednadžbe

Kažimo nekoliko riječi o **linearnim matričnim jednadžbama**. To su jednadžbe oblika

$$AX = B\,, \tag{1}$$

odnosno

$$YA = B\,, \tag{2}$$

gdje su A i B dane kvadratne matrice n-tog reda nad poljem F, a X, odnosno Y je nepoznanica, tj. tražena matrica istog reda.

Rješenje takve jednadžbe je svaka matrica C nad poljem F, koja uvrštena umjesto X, odnosno Y prevodi jednadžbe (1) i (2) u identitete.

Ako je matrica A regularna, jednadžba (1) ima jedinstveno rješenje. Zaista, postoji A^{-1} i rješenje je

$$X = A^{-1}B\,.$$

Slično, $Y = BA^{-1}$ je rješenje za (2).

Na primjer, za jednadžbu

$$\begin{bmatrix} 3 & 4 \\ 1 & 1 \end{bmatrix} X = \begin{bmatrix} 2 & 9 \\ 1 & 3 \end{bmatrix}$$

jest $\det A = -1$, pa je

$$A^{-1} = \begin{bmatrix} -1 & 4 \\ 1 & -3 \end{bmatrix},$$

i rješenje je

$$X = A^{-1}B = \begin{bmatrix} 2 & 3 \\ -1 & 0 \end{bmatrix} .$$

Ako je, međutim, matrica A singularna, opisana se metoda ne može primijeniti (jer ne postoji A^{-1}). U tom se slučaju rješavanje svodi na rješavanje pridruženog linearnog sustava jednadžbi (1). Lako se može zaključiti da je taj sustav, pa onda i polazna matrična jednadžba, ili neriješiva ili ima beskonačno mnogo rješenja (uz uvjet da je polje F beskonačno).

Imamo npr. jednadžbu

$$\begin{bmatrix} 2 & 3 \\ 4 & 6 \end{bmatrix} X = \begin{bmatrix} 1 & 2 \\ 2 & 4 \end{bmatrix} .$$

Ovdje je $\det A = 0$. Stavimo li $X = \begin{bmatrix} x_1 & x_2 \\ x_3 & x_4 \end{bmatrix}$, dobivamo

$$\begin{bmatrix} 2x_1 + 3x_3 & 2x_2 + 3x_4 \\ 4x_1 + 6x_3 & 4x_2 + 6x_4 \end{bmatrix} = \begin{bmatrix} 1 & 2 \\ 2 & 4 \end{bmatrix} .$$

No, ta je jednadžba ekvivalentna sa sustavom

$$\begin{aligned} 2x_1 + 3x_3 &= 1 \\ 4x_1 + 6x_3 &= 2 \\ 2x_2 + 3x_4 &= 2 \\ 4x_2 + 6x_4 &= 4 \end{aligned} ,$$

koji se raspada u dva podsustava, sa po dvije nepoznanice (uvijek je tako!), koji su rješivi. Imamo

$$\begin{aligned} x_1 &= 1 - 3u/2 \\ x_3 &= u \\ x_2 &= 2 - 3v/2 \\ x_4 &= v \end{aligned} ,$$

pa je rješenje matrične jednadžbe

$$X = \frac{1}{2} \begin{bmatrix} 1 - 3u & 2 - 3v \\ 2u & 2v \end{bmatrix} ,$$

gdje su $u, v \in \mathbb{R}$ bilo koji brojevi. Imamo, dakle, dvoparametarsku familiju rješenja.

ZADACI

1. Diskutiraj sustav

$$A_1X + B_1Y = C_1$$
$$A_2X + B_2Y = C_2$$

linearnih matričnih jednadžbi u nepoznatim matricama X i Y. Generaliziraj!

2. Odredi sve matrice drugog reda koje su involutorne, tj. riješi jednadžbu
$$X^2 = E\,.$$

3. Među kvadratima matrica drugog reda odredi djelitelje nule, tj. riješi jednadžbu
$$X^2 = 0\,.$$

4. Nađi sve matrice koje komutiraju s matricom $A = \begin{bmatrix} 3 & 7 \\ 4 & 3 \end{bmatrix}$, tj. riješi jednadžbu
$$AX = XA\,.$$

5. Riješi matričnu jednadžbu
$$A^{-1}X^2A = B\,,$$
gdje je
$$A = \begin{bmatrix} 1 & 1 & 1 \\ 1 & -1 & -1 \\ 1 & 1 & -1 \end{bmatrix}, \quad B = \begin{bmatrix} 4 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 9 \end{bmatrix}.$$

12

UNITARNI PROSTOR

U ovom poglavlju u opće linearne prostore nad poljem realnih, odnosno kompleksnih brojeva, aksiomatski uvodimo dodatnu, tzv. unitarnu strukturu koja omogućuje da u tim prostorima definiramo metričke pojmove i onda izučavamo njihova svojstva, tj. razvijamo geometriju linearnog prostora.

12.1. Uvodne napomene

Dosta detaljno izučavali smo svojstva apstraktnog linearnog prostora. Lako je zapaziti da takvi prostori imaju siromašniju strukturu od standardnog prototipa, prostora V^3 (geometrijskih vektora, klasa orijentiranih dužina). Naime, oslanjajući se samo na aksiome linearnog prostora, nije moguće definirati pojmove kao što su dužina vektora, kut među vektorima, okomitost vektora i sl. (kojima smo operirali u V^3), tj. ispitivati **metrička svojstva** prostora koja su toliko važna za izgradnju njegove geometrije. Taj se nedostatak može ukloniti tako da na linearnom prostoru definiramo jednu dodatnu strukturu, tj. aksiomatski uvedemo pojam **skalarnog produkta**. Pokazat ćemo, naime, da pomoću skalarnog produkta navedene pojmove nije teško rekonstruirati, tj. definirati **linearnu i angularnu metriku**. To nas vodi pojmu tzv. **unitarnog prostora**.

Postavlja se pitanje kako na razuman način aksiomatski fundirati pojam skalarnog produkta. Podsjetimo se, u prostoru V^3 smo (imajući već geometrijski definirane duljinu vektora i kut među njima) skalarni produkt vektora $\vec{a}$ i $\vec{b}$ definirali kao broj

$$\vec{a} \cdot \vec{b} = |\vec{a}| \cdot |\vec{b}| \cdot \cos(\vec{a}, \vec{b}) \,,$$

koji se u pravokutnim koordinatama vektora mogao zapisati u obliku

$$\vec{a} \cdot \vec{b} = \alpha_1\beta_1 + \alpha_2\beta_2 + \alpha_3\beta_3 \,.$$

Ta se formula često uzima i kao definicija skalarnog produkta. Utvrdili smo, nadalje (vidi točku 5.9.), da to množenje ima ova karakteristična svojstva:

(1) $\vec{b}\cdot\vec{a}=\vec{a}\cdot\vec{b}$;

(2) $(\alpha\vec{a})\cdot\vec{b}=\alpha(\vec{a}\cdot\vec{b})$;

(3) $(\vec{a}+\vec{b})\cdot\vec{c}=\vec{a}\cdot\vec{c}+\vec{b}\cdot\vec{c}$;

(4) $\vec{a}^2\geq 0$; $\vec{a}^2=0\Leftrightarrow\vec{a}=\vec{0}$.

Tom smo prilikom kratko napomenuli da ćemo i u općenitijem slučaju, uzimajući, kao i obično, konkretno utvrđena svojstva za definiciju, svako preslikavanje

$$V\times V\to\mathbb{R}\,,$$

koje ima svojstva (1)–(4), zvati skalarnim množenjem u linearnom prostoru V (a sam taj prostor unitarnim prostorom).

Generalizacija je dobra za prostore nad poljem realnih brojeva, tzv. realne prostore. Ona će, međutim, zatajiti ako promatramo prostore nad bilo kojim poljem F, jer tamo npr. zahtjev (4), $\vec{a}^2\geq 0$, nema smisla (jer polje F ne mora biti uređeno!). U drugu ruku, u mnogim se primjenama operira s kompleksnim brojevima pa nam je važno proširiti pojam skalarnog produkta makar na linearne prostore nad poljem $\mathbb{C}$ kompleksnih brojeva.

Tu, međutim, nastupaju neke teškoće. Ako prostor V^3 zamislimo nad poljem $\mathbb{C}$, tj. ako dopustimo da vektori imaju za svoje koordinate i kompleksne brojeve, a zadržavamo standardnu (koordinatnu) definiciju skalarnog produkta u V^3, imat ćemo, primjerice, da je za vektor

$$\vec{a}=3\vec{\imath}+4\vec{\jmath}+5i\vec{k}$$

njegov skalarni kvadrat

$$\vec{a}^2=9+16-25=0\,,$$

što je u proturječnosti sa svojstvom (4).

Kako bismo tome doskočili, definiciju skalarnog produkta modificiramo stavljajući

$$\vec{a}\cdot\vec{b}=\alpha_1\overline{\beta}_1+\alpha_2\overline{\beta}_2+\alpha_3\overline{\beta}_3\,,$$

tj. uvodeći tzv. **hermitsko množenje** (ovdje je, dakako, $\overline{\beta}_i$ kompleksni broj konjugiran broju β_i). Prije svega, odmah se vidi da je to dobro proširenje definicije skalarnog produkta, jer je u realnom slučaju $\overline{\beta}_i=\beta_i$, pa se navedena formula svodi na standardnu. Nadalje, i uz tu su definiciju sačuvana svojstva (2),(3) i (4) skalarnog produkta. Tako je npr.

$$\vec{a}^2=\alpha_1\overline{\alpha}_1+\alpha_2\overline{\alpha}_2+\alpha_3\overline{\alpha}_3=|\alpha_1|^2+|\alpha_2|^2+|\alpha_3|^2\geq 0\,,$$

gdje je $|\alpha| \in \mathbb{R}$ modul kompleksnog broja, i pritom je $\vec{a}^2 = 0$ ako i samo ako je $\vec{a} = \vec{0}$, što pokazuje da je ispunjen zahtjev (4), posebno važan za uvođenje metrike. Ostaje upitan zahtjev (1). Odmah se vidi da uz novu definiciju vrijedi

$$\vec{b} \cdot \vec{a} = \beta_1\overline{\alpha_1} + \beta_2\overline{\alpha_2} + \beta_3\overline{\alpha_3} = \overline{\alpha_1\overline{\beta_1} + \alpha_2\overline{\beta_2} + \alpha_3\overline{\beta_3}} = \overline{\vec{a} \cdot \vec{b}}\,,$$

tj. da komutaciju prati konjugiranje, što se, dakako, u realnom slučaju svodi na obično komutiranje, tj. na svojstvo (1).

Prema tome, hermitsko množenje u V^3 ima sva bitna svojstva skalarnog množenja, s time da običnu komutaciju treba zamijeniti s tzv. hermitskom. Prirodna je, dakle, ideja da se upravo ta svojstva uzmu za aksiome u pokušaju da se u opći linearni prostor (bilo koje dimenzije) **nad poljem kompleksnih brojeva** uvede skalarni produkt, i preko njega struktura unitarnog prostora. Tu ćemo ideju precizno formulirati u sljedećoj točki.

12.2. Definicija i osnovna svojstva

Do sada smo promatrali linearne prostore nad bilo kojim poljem. Razmatranja o unitarnosti imaju, međutim, smisla ako se ograničimo na **prostore nad poljem kompleksnih ili realnih brojeva** (vidi i Zad. 2). To je zapravo najvažnija klasa linearnih prostora; takvi se prostori pojavljuju u većini primjena.

Neka je, dakle, F polje kompleksnih ili polje realnih brojeva. Neka je U linearni prostor nad poljem F, a

$$s : U \times U \to F$$

preslikavanje s ovim svojstvima:

(1) hermitska komutativnost:

$$s(b, a) = \overline{s(a, b)}\,,$$

(2) kvaziasocijativnost:

$$s(\alpha a, b) = \alpha\, s(a, b)\,,$$

(3) distributivnost:

$$s(a + b, c) = s(a, c) + s(b, c)\,,$$

(4) pozitivna definitnost:

$$a \neq \Theta \Rightarrow s(a,a) > 0 ,$$

za svaki izbor vektora $a, b, c \in U$ i skalara $\alpha \in F$, gdje je u (1) potezom označena operacija konjugiranja. Onda preslikavanje s nazivamo **skalarnim množenjem** u prostoru U, a skalar $s(a,b) \in F$ **skalarnim produktom vektora** $a, b \in U$.

Nadalje, uređeni par (U, s), koji se sastoji od linearnog prostora U i jednog skalarnog množenja na tom prostoru, nazivamo unitarni linearni prostor, ili kraće **unitarni prostor nad poljem** F. **Dimenzija unitarnog prostora** je po definiciji jednaka dimenziji pripadnog linearnog prostora U.

Ako je prostor U nad poljem $F = \mathbb{C}$ kompleksnih brojeva, govorimo o **kompleksnom unitarnom prostoru**, a ako je taj prostor nad poljem $F = \mathbb{R}$ realnih brojeva, nazivamo ga **realni unitarni prostor**. Naravno, u slučaju realnog prostora zahtjev (1) reducira se na

(1') komutativnost:

$$s(b,a) = s(a,b) .$$

Skalarni produkt dvaju vektora kraće ćemo označivati kao

$$s(a,b) = (a,b) ,$$

što ne treba miješati s uređenim parom. U literaturi se može naići i na oznake $\langle a, b\rangle$, $(a \mid b)$ i $\langle a \mid b\rangle$.

Zahtjevi (1)–(4) u definiciji unitarnog prostora nazivaju se **aksiomi unitarnog prostora**. Njima se, među ostalim, postulira kvaziasocijativnost i distributivnost za prve faktore u skalarnom produktu. Analogne se tvrdnje za druge faktore mogu dokazati. Vrijedi

PROPOZICIJA 1

U unitarnom je prostoru

(5) $(a, \beta b) = \overline{\beta}(a,b)$,

(6) $(a, b+c) = (a,b) + (a,c)$,

za svaki izbor vektora $a, b, c \in U$ *i skalara* $\beta \in F$.

Dokaz

Dokažimo npr. (5). Imamo redom, koristeći se aksiomima unitarnog prostora i svojstvima kompleksnih brojeva,

$$(a, \beta b) = (\overline{\beta b, a}) = \overline{\beta(b,a)} = \overline{\beta}\,\overline{(b,a)} = \overline{\beta}(a,b) .$$

Analogno se dokazuje i (6). ■

Primijetimo da aksiom (4) implicitno sadrži dva svojstva. Naime vrijedi

PROPOZICIJA 2

Za svaki vektor $a \in U$ je

(7) $(a, a) \geq 0$,

(8) $(a, a) = 0 \quad \Leftrightarrow \quad a = \Theta$.

Dokaz

Iz $(a, a) = 0$ slijedi $a = \Theta$, jer bi $a \neq \Theta$ zbog (4) povlačilo $(a, a) > 0$. Obratno, ako je $a = \Theta$ imamo

$$(a, a) = (\Theta, \Theta) = (0 \cdot a, \Theta) = 0 \cdot (a, \Theta) = 0 ,$$

pa je (8) dokazano. Relacija (7) je posljedica relacija (4) i (8). ■

Na osnovi Prop. 2 zaključujemo da će skalarni kvadrat (a, a) vektora uvijek biti realan broj, neovisno o tome promatramo li unitarni prostor nad poljem kompleksnih ili realnih brojeva. Konačno, posve analogno kao (8) dokazuje se i

PROPOZICIJA 3

Za bilo koji vektor $a \in U$ je

$$(\Theta, a) = (a, \Theta) = 0 .$$

■

Napomenimo na kraju da ćemo se, iako je naša definicija unitarnog prostora općenita, kao i u teoriji linearnih prostora, gotovo isključivo baviti **konačnodimenzionalnim** unitarnim prostorima. Beskonačnodimenzionalni slučaj ima mnoge specifičnosti i njega obrađuje funkcionalna analiza.

ZADACI

1. Generaliziraj (2), (3), (5) i (6), tj. pokaži da u unitarnom prostoru vrijedi
$$(\sum_{i=1}^{m} \alpha_i a_i, \sum_{k=1}^{n} \beta_k b_k) = \sum_{i=1}^{m} \sum_{k=1}^{n} \alpha_i \overline{\beta}_k (a_i, b_k) ,$$
za svaki izbor $a_i, b_k \in U$, $\alpha_i, \beta_k \in F$.

2. U definiciji unitarnog prostora ne moramo nužno biti toliko restriktivni u izboru polja. Neka je $F < \mathbb{C}$ potpolje od $\mathbb{C}$ sa svojstvom da je za svaki $\alpha \in F$ i $\overline{\alpha} \in F$. Kažemo, u tom slučaju, da je F **normalno iznad svog realnog potpolja**. Osim polja realnih i kompleksnih brojeva, i mnoga druga polja imaju to svojstvo. Uvjeri se da se naša definicija unitarnog prostora može primijeniti i u slučaju kad je U linearni prostor nad bilo kojim poljem F, koje je normalno nad svojim realnim potpoljem.

12.3. Primjeri unitarnih prostora

Navedimo nekoliko tipičnih primjera unitarnih struktura.

1. U prostoru V^3 geometrijskih vektora (klasa orijentiranih dužina) definiramo
$$(\vec{a}, \vec{b}) = |\vec{a}| \cdot |\vec{b}| \cdot \cos(\vec{a}, \vec{b}) \in \mathbb{R} ,$$
kao u točki 5.9. Kako smo tamo vidjeli, to množenje ima tražena svojstva pa na V^3 definira strukturu realnog unitarnog prostora.

2. Neka je $\mathbb{R}^n$ prostor uređenih n-torki realnih brojeva. Za $a = (\alpha_i)$ i $b = (\beta_i)$ iz $\mathbb{R}^n$ definiramo
$$(a, b) = ((\alpha_1, \ldots, \alpha_n), (\beta_1, \ldots, \beta_n)) = \alpha_1\beta_1 + \cdots + \alpha_n\beta_n \in \mathbb{R} .$$
Aksiomi (1)–(4) lako se provjere. Na primjer, iz definicije imamo
$$(a, a) = \alpha_1^2 + \cdots + \alpha_n^2 ,$$
odakle odmah razabiremo da $a \neq \Theta$ povlači $(a, a) > 0$, tj. da je ispunjen uvjet (4). To množenje nazivamo **standardni skalarni produkt** na $\mathbb{R}^n$, i preko njega $\mathbb{R}^n$ postaje n-dimenzionalni realni unitarni prostor. Taj se prostor obično zove **euklidski prostor**.

3. Neka su $\lambda_1, ..., \lambda_n \in \mathbb{R}$, $\lambda_i > 0$, $i = 1, .., n$, dani brojevi. Onda u prostoru $\mathbb{R}^n$ množenje možemo definirati formulom
$$(a, b) = \lambda_1\alpha_1\beta_1 + \cdots + \lambda_n\alpha_n\beta_n \in \mathbb{R} ,$$
za svaki $a = (\alpha_i)$, $b = (\beta_i) \in \mathbb{R}^n$. I to je dobro definiran skalarni produkt, pa preko njega $\mathbb{R}^n$ također postaje unitarni prostor. Primjer pokazuje da na **istom** linearnom prostoru možemo definirati različite unitarne strukture, pa dobivamo **različite** unitarne prostore.

4. U prostoru $\mathbb{C}^n$ svih uređenih n-torki kompleksnih brojeva definiramo standardni skalarni produkt formulom
$$(a, b) = \sum_{i=1}^{n} \alpha_i\overline{\beta}_i \in \mathbb{C} ,$$
za svaki $a = (\alpha_i)$, $b = (\beta_i) \in \mathbb{C}^n$. Lako se vidi da je riječ o dobro definiranom skalarnom množenju, pa uz njega $\mathbb{C}^n$ postaje n-dimenzionalni kompleksni unitarni prostor, **standardni kompleksni prostor** dimenzije n.

5. Neka je s $\mathbb{R}_{[0,1]}$ označen linearni prostor svih neprekidnih realnih funkcija definiranih na segmentu $[0,1]$. Za takve funkcije $f, g \in \mathbb{R}_{[0,1]}$, definiramo njihov produkt s

$$(f,g) = \int_0^1 f(t)g(t)dt \quad \in \mathbb{R}\,.$$

Iz osnovnih svojstava integrala odmah se vidi da su ispunjeni aksiomi (1)–(3) skalarnog produkta. Aksiom (4) slijedi iz teorema koji kaže da je

$$\int_0^1 f(t)^2 \mathrm{d}t > 0\,,$$

ako funkcija f nije identički jednaka nuli. Na taj način $\mathbb{R}_{[0,1]}$ postaje realni unitarni prostor. To je primjer beskonačnodimenzionalnog unitarnog prostora.

ZADACI

1. U prostoru $M_n(\mathbb{C})$ kvadratnih kompleksnih matrica definiramo

$$(A,B) = \mathrm{tr}(AB^*)\,.$$

Pokaži da je uz to množenje $M_n(\mathbb{C})$ kompleksni unitarni prostor. Analogno se i $M_n(\mathbb{R})$ organizira u realni unitarni prostor.

2. Neka je

$$U = \left\{(\alpha_1, \ldots, \alpha_n, \ldots) \mid \alpha_i \in \mathbb{R},\ \sum_{i=1}^{\infty} |\alpha_i|^2 < \infty\right\} \subset \mathbb{R}^\infty$$

skup svih kvadratnih sumabilnih nizova iz $\mathbb{R}^\infty$. Pokaži da je U linearni prostor. Uvjeri se da za bilo koje nizove $(\alpha_i), (\beta_i) \in U$ suma

$$\sum_{i=1}^{\infty} \alpha_i \beta_i$$

uvijek konvergira, pa tu sumu uzmi za produkt nizova. Dokaži da je uz takvo množenje U (beskonačnodimenzionalni) unitarni prostor.

3. Na prostoru $\mathbb{C}_{[0,1]}$ neprekidnih funkcija $[0,1] \to \mathbb{C}$ definiramo produkt funkcija $f, g \in C_{[0,1]}$ s

$$(f,g) = \int_0^1 f(t)\overline{g(t)}dt \quad \in \mathbb{C}\,.$$

Pokaži da je $\mathbb{C}_{[0,1]}$ uz to množenje kompleksni unitarni prostor.

4. Neka je $\varrho \in \mathbb{C}_{[0,1]}$ funkcija sa svojstvom da je $\varrho(t) \geq 0$, za svaki $t \in [0,1]$ i $\varrho(t) = 0$, za najviše konačno mnogo t-ova. Onda je $\mathbb{C}_{[0,1]}$, uz množenje

$$(f,g) = \int_0^1 \varrho(t) f(t) \overline{g(t)}\, \mathrm{d}t \in \mathbb{C}\,,$$

također kompleksni unitarni prostor, različit od onog opisanog u Zad. 3. Dokaži!

5. Neka su U_1 i U_2 unitarni prostori nad istim poljem. Onda je direktni produkt $U_1 \times U_2$ linearnih prostora U_1 i U_2 također unitarni prostor uz skalarno množenje

$$((a_1,a_2),(b_1,b_2)) = (a_1,b_1) + (a_2,b_2)\,,$$

i taj prostor nazivamo **direktni produkt unitarnih prostora** U_1 i U_2. Dokaži i generaliziraj za konačno mnogo faktora. Na taj način se euklidski prostor $\mathbb{R}^n$ može interpretirati kao produkt od n kopija unitarnog prostora $\mathbb{R}$.

12.4. Nejednakost Schwarz-Cauchy-Bunjakovskog

Sada ćemo dokazati jednu važnu nejednakost koja vrijedi u unitarnim prostorima. Imamo

TEOREM 1

Neka je U unitarni prostor, te $a, b \in U$ bilo koji njegovi vektori. Onda vrijedi

$$|(a,b)|^2 \leq (a,a)(b,b)\,. \tag{1}$$

Pritom znak jednakosti vrijedi ako i samo ako su vektori a i b linearno zavisni.

Dokaz

Ako je $b = \Theta$, relacija (1) zbog Prop. 3 u 12.2. postaje trivijalna jednakost. Pretpostavimo zato da je $b \neq \Theta$.

Neka je $\lambda \in F$ bilo koji skalar. Promatrajmo vektor $a - \lambda b \in U$. Za njega vrijedi

$$(a - \lambda b, a - \lambda b) \geq 0\,. \tag{2}$$

Primjenom distribucije i kvaziasocijativnosti iz (2) slijedi

$$(a,a) - \lambda(b,a) - \overline{\lambda}(a,b) + \lambda\overline{\lambda}(b,b) \geq 0\,. \tag{3}$$

Uzmimo sada specijalno

$$\lambda = \frac{(a,b)}{(b,b)} . \tag{4}$$

Kako je $b \neq \Theta$, to je dobro definiran broj. Nakon uvrštavanja λ iz relacije (4) i množenja nazivnikom $(b,b) > 0$, iz (3) dobivamo

$$(a,a)(b,b) - (a,b)(b,a) - \overline{(a,b)}(a,b) + (a,b)\overline{(a,b)} \geq 0 ,$$

dakle

$$(a,b)(b,a) \leq (a,a)(b,b) ,$$

odnosno, zbog hermitske komutativnosti,

$$(a,b)\overline{(a,b)} \leq (a,a)(b,b) .$$

Iz svojstva modula kompleksnog broja odmah slijedi

$$|(a,b)|^2 \leq (a,a)(b,b) ,$$

pa je tvrdnja (1) dokazana.

Dokažimo drugi dio teorema. Neka su vektori a i b linearno zavisni, tj. $a = \lambda b$, uz $b \neq \Theta$ (slučaj $b = \Theta$ spomenuli smo uvodno). Onda je

$$\begin{aligned} |(a,b)|^2 &= |(\lambda b, b)|^2 = |\lambda (b,b)|^2 = |\lambda|^2 \cdot |(b,b)|^2 = \\ &= \lambda\overline{\lambda}(b,b)(b,b) = (\lambda b, \lambda b)(b,b) = (a,a)(b,b) , \end{aligned}$$

tj. u (1) vrijedi jednakost. Obratno, iz jednakosti

$$|(a,b)|^2 = (a,a)(b,b) ,$$

zaključujući unatrag, i uz λ kao u (4), dolazimo do jednakosti

$$(a - \lambda b, a - \lambda b) = 0 ,$$

što povlači (vidi Prop. 2 u 12.2.) da je

$$a - \lambda b = \Theta ,$$

dakle $a = \lambda b$, i dokaz je gotov. ■

Uočimo da u slučaju realnog unitarnog prostora nejednakost (1) ima oblik

$$(a,b)^2 \leq (a,a)(b,b) .$$

Relacija (1) obično se naziva **nejednakost Schwarz – Cauchy – Bunjakovskog**. Dokazana je odavno. Prvi ju je dokazao Lagrange (1773.) za prostor $\mathbb{R}^3$, zatim Cauchy (1821.) za prostore $\mathbb{R}^n$, odnosno $\mathbb{C}^n$, i konačno Bunjakovski (1859.) i Schwarz (1885.) za unitarne prostore funkcija.

ZADACI

1. Uvjeri se da nejednakost (1) u euklidskom prostoru $\mathbb{R}^n$ ima oblik

$$(\sum_{i=1}^{n} \alpha_i \beta_i)^2 \leq (\sum_{i=1}^{n} \alpha_i^2)(\sum_{i=1}^{n} \beta_i^2) ,$$

a u standardnom kompleksnom prostoru $\mathbb{C}^n$, slično

$$\left| \sum_{i=1}^{n} \alpha_i \overline{\beta}_i \right|^2 \leq (\sum_{i=1}^{n} |\alpha_i|^2)(\sum_{i=1}^{n} |\beta_i|^2) .$$

To su tzv. **Cauchyjeve nejednakosti**.

2. U prostoru $\mathbb{R}_{[0,1]}$ relacija (1) poprima oblik

$$\left(\int_0^1 f(t)g(t)\,\mathrm{d}t \right)^2 \leq \int_0^1 f(t)^2 \mathrm{d}t \cdot \int_0^1 g(t)^2 \mathrm{d}t$$

i to je tzv. **Schwarzova nejednakost**. Napiši odgovarajuću nejednakost u prostoru $\mathbb{C}_{[0,1]}$.

12.5. Norma vektora. Kut

Ovdje ćemo vidjeti kako struktura unitarnog prostora omogućuje mjerenje duljine vektora.

Neka je U bilo koji unitarni prostor (realni ili kompleksni). Za svaki vektor $a \in U$ je njegov skalarni kvadrat nenegativan, $(a, a) \geq 0$. Zato je dobro definiran realni broj

$$\|a\| = \sqrt{(a, a)} ,$$

gdje treba uzeti pozitivnu determinaciju drugog korijena. Taj broj nazivamo **duljina**, **modul** ili, također, **norma** vektora a.

Na primjer, prema toj definiciji je norma u V^3 dana s

$$\|\vec{a}\| = \sqrt{\vec{a}^2} = |\vec{a}| ,$$

tj. poklapa se s modulom vektora $\vec{a}$, definiranim prije (vidi točku 5.4.). Nadalje,

$$\|a\| = \sqrt{\sum_{i=1}^{n} \alpha_i^2} , \quad \|a\| = \sqrt{\sum_{i=1}^{n} |\alpha_i|^2} , \quad \|f\| = \sqrt{\int_0^1 f(t)^2 \mathrm{d}t}$$

jesu norme u unitarnim prostorima $\mathbb{R}^n$, $\mathbb{C}^n$, odnosno $\mathbb{R}_{[0,1]}$.

Odmah vidimo da se nejednakost Schwarz-Cauchy-Bunjakovskog može jednostavno zapisati pomoću norme, što precizira

PROPOZICIJA 1

Za svaki izbor $a, b \in U$ vrijedi

$$|(a,b)| \leq \|a\| \cdot \|b\| ,$$

s tim da jednakost nastupa ako i samo ako su vektori linearno zavisni. ■

Navedimo osnovna svojstva norme.

TEOREM 2

Norma vektora u unitarnom prostoru ima ova svojstva:

(1) *pozitivna definitnost:* $\|a\| \geq 0$,

(2) *strogost:* $\|a\| = 0 \Leftrightarrow a = \Theta$,

(3) *homogenost:* $\|\alpha a\| = |\alpha| \cdot \|a\|$, *i*

(4) *nejednakost trokuta:* $\|a + b\| \leq \|a\| + \|b\|$,

za svaki izbor $a, b \in U$ i $\alpha \in F$.

Dokaz

Svojstva (1) i (2) su očigledna. Svojstvo (3) izlazi neposredno iz definicije jer imamo

$$\begin{aligned} \|\alpha a\| &= \sqrt{(\alpha a, \alpha a)} = \sqrt{\alpha\overline{\alpha}(a,a)} = \sqrt{|\alpha|^2(a,a)} = \\ &= |\alpha|\sqrt{(a,a)} = |\alpha| \cdot \|a\| . \end{aligned}$$

Dokažimo još relaciju trokuta (4). Sjetimo se da je za svaki kompleksni broj z, $\mathrm{Re}(z) \leq |z|$, gdje $\mathrm{Re}(z)$ označava realni dio od z, a $|z|$ njegov modul. Onda imamo, koristeći Prop. 1,

$$\begin{aligned} \|a+b\|^2 &= (a+b, a+b) = (a,a) + (a,b) + (b,a) + (b,b) = \\ &= (a,a) + (b,b) + (a,b) + \overline{(a,b)} = (a,a) + (b,b) + 2\mathrm{Re}\,(a,b) \leq \\ &\leq (a,a) + (b,b) + 2|(a,b)| \leq \|a\|^2 + \|b\|^2 + 2\|a\| \cdot \|b\| = \\ &= (\|a\| + \|b\|)^2 , \end{aligned}$$

dakle

$$\|a + b\| \leq \|a\| + \|b\| ,$$

i relacija (4) je dokazana. ■

Primijetimo ovdje da se pojam norme može definirati i općenitije, neovisno o skalarnom produktu. Neka je V bilo koji linearni prostor nad poljem F (realnih ili kompleksnih brojeva). Svako preslikavanje

$$\|\cdot\| : V \to \mathbb{R}$$

koje ima svojstva od (1) do (4) iz Tm. 2, nazivamo **norma** na prostoru V. Uređeni par $(V, \|\cdot\|)$ nazivamo normirani linearni prostor ili, kratko, **normirani prostor**. Kako smo vidjeli, svaki unitarni prostor pomoću **norme** $\|a\| = \sqrt{(a,a)}$, **inducirane skalarnim produktom**, postaje normirani prostor. Obrat, međutim, ne vrijedi. Normirani prostor V nije nužno unitaran, tj. na V ne mora postojati skalarni produkt sa svojstvom da se norma inducirana tim produktom podudara s polaznom normom na prostoru V (vidi Zad. 4., 5. i 6.). Klasa normiranih prostora je šira od klase unitarnih prostora.

Vratimo se unitarnim prostorima. Za vektor $a \in U$, za koji je

$$\|a\| = 1 ,$$

kažemo da je **jedinični** ili **normirani** vektor. Svakom vektoru $a \neq \Theta$ možemo pridružiti jednoznačno određen vektor

$$a_0 = \frac{1}{\|a\|} \cdot a ,$$

koji je zbog aksioma (3) jediničan. U tom slučaju kažemo da smo vektor a normirali.

Neka su $a, b \in U$ bilo koji vektori različiti od nulvektora. Iz Prop. 1 slijedi da je

$$\frac{|(a,b)|}{\|a\| \cdot \|b\|} \leq 1 .$$

Ako je U realan prostor, onda je $(a,b) = \pm|(a,b)|$, tj.

$$-1 \leq \frac{(a,b)}{\|a\| \cdot \|b\|} \leq 1 .$$

Postoji, dakle, jedinstveni broj φ iz intervala $[0, \pi]$ takav da je

$$\cos\varphi = \frac{(a,b)}{\|a\| \cdot \|b\|} .$$

Po definiciji onda kažemo da je φ **kut između vektora** a **i** b, $\varphi = \sphericalangle(a, b)$. Napomenimo na kraju, da iz definicije kuta slijedi relacija

$$(a, b) = \|a\| \cdot \|b\| \cos\varphi \,,$$

u kojoj prepoznajemo tradicionalnu formulu za skalarni produkt.

ZADACI

1. Zahtjevi (1)–(4), tzv. **aksiomi norme**, nisu nezavisni. Na primjer, (1) se može dokazati pomoću ostalih aksioma, pa bi se u definiciji norme mogao i ispustiti. Dokaži!

2. U realnom unitarnom prostoru vrijedi

$$2(a, b) = \|a + b\|^2 - \|a\|^2 - \|b\|^2 \,.$$

   Koji se poučak iz elementarne geometrije krije u toj formuli?

3. U kompleksnom unitarnom prostoru vrijedi

$$2(a, b) = \|a + b\|^2 + i\|a + ib\|^2 - 2(\|a\|^2 - \|b\|^2) \,.$$

   Dokaži!

4. Za normu u unitarnom prostoru istinita je i ova jednakost

$$\|a + b\|^2 + \|a - b\|^2 = 2\|a\|^2 + 2\|b\|^2 \,,$$

   tzv. **relacija paralelograma**. Dokaži i interpretiraj geometrijski!

5. Na normiranom prostoru V moguće je definirati strukturu unitarnog prostora, koja inducira normu jednaku polaznoj, ako i samo ako ta norma zadovoljava relaciju paralelograma. Dokaži! [Uputa: Ako je V realni prostor, definiraj

$$(a, b) = \frac{1}{4}(\|a + b\|^2 - \|a - b\|^2) \,,$$

   a ako je kompleksan, uzmi

$$(a, b) = \frac{1}{4}(\|a + b\|^2 - \|a - b\|^2) + \frac{1}{4}\, i\, (\|a + ib\|^2 - \|a - ib\|^2) \,.]$$

6. Uvjeri se da linearni prostor $\mathbb{R}_{[0,1]}$, uz

$$\|f\| = \max_t |f(t)| ,$$

postaje normirani prostor. Promatraj funkcije

$$f(t) = \begin{cases} t - 1/2 & , \quad 1/2 \leq t \leq 1 \\ 0 & , \quad 0 \leq t \leq 1/2 \end{cases}$$

i

$$g(t) = \begin{cases} 0 & , \quad 1/2 \leq t \leq 1 \\ -t + 1/2 & , \quad 0 \leq t \leq 1/2 \end{cases}$$

iz $\mathbb{R}_{[0,1]}$ pa dokaži da za njih ne vrijedi relacija paralelograma. Prema tome, $\mathbb{R}_{[0,1]}$ ne dopušta unitarnu strukturu koja bi bila kompatibilna s danom strukturom normiranog prostora (vidi Zad. 5.), tj. na $\mathbb{R}_{[0,1]}$ nema skalarnog produkta za koji bi vrijedilo

$$\sqrt{(f,f)} = \max_t |f(t)| .$$

7. Dokaži: U normiranom prostoru uvijek vrijedi

$$\|a+b\| + \|a-b\| \leq 2\|a\| + 2\|b\| .$$

Kada u toj relaciji vrijedi znak jednakosti?

8. U prostoru $\mathbb{R}^n$ za svaki $a = (\alpha_i)$ definiramo

(a) $\|a\|_\infty = \max_i |\alpha_i|$;

(b) $\|a\|_1 = |\alpha_1| + \cdots + |\alpha_n|$;

(c) $\|a\|_2 = \sqrt{\alpha_1^2 + \cdots + \alpha_n^2}$.

Pokaži da je svakim od izraza (a)–(c) dobro definirana norma na $\mathbb{R}^n$.

9. Neka je p dani prirodni broj. Na $\mathbb{R}^n$ definiramo

$$\|a\| = \left[\sum_{i=1}^n |\alpha_i|^p \right]^{1/p} ,$$

za svaki $a = (\alpha_i)$. Pokaži da je to norma na $\mathbb{R}^n$, i da u toj normi nejednakost trokuta ima oblik

$$\left[\sum_{i=1}^n |\alpha_i + \beta_i|^p \right]^{1/p} \leq \left[\sum_{i=1}^n |\alpha_i|^p \right]^{1/p} + \left[\sum_{i=1}^n |\beta_i|^p \right]^{1/p} ,$$

i to je tzv. **nejednakost Minkowskog**. Dokaži da će, uz $n \geq 2$, tako definiran normirani prostor $(\mathbb{R}^n, \|\cdot\|)$ biti unitaran jedino u slučaju kada je $p = 2$ (vidi Zad. 5.).

10. Vektori $a, b \in U$ su linearno zavisni ako i samo ako je jedan od njih nulvektor ili je $\sphericalangle(a, b) = 0, \pi$. Dokaži!

11. Dokaži: $\sphericalangle(a, b) = \sphericalangle(b, a)$. Nadalje, ako je $\sphericalangle(a, b) = \varphi$, uvjeri se da je

$$\sphericalangle(-a, b) = \sphericalangle(a, -b) = \pi - \varphi \, .$$

12.6. Metrika

Pomoću norme jednostavno je definirati udaljenost dvaju vektora, tj. unitarni prostor opremiti metrikom.

U V^3 udaljenošću dvaju vektora smatramo modul razlike tih vektora, a u E^3 duljinu segmenta određenog danim točkama. To sada generaliziramo.

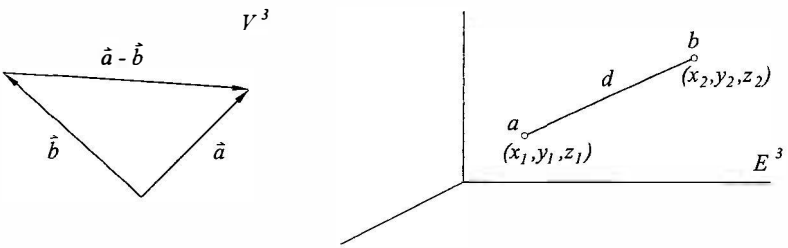
Neka je U unitarni prostor, a $a, b \in U$ bilo koji vektori. Onda realni broj

$$d(a, b) = \|a - b\|$$

nazivamo **udaljenost** vektora a od vektora b.

Tako je u V^3

$$(\vec{a}, \vec{b}) = \|\vec{a} - \vec{b}\| = |\vec{a} - \vec{b}| \, ,$$



a u $\mathbb{R}^3$ je

$$d(a, b) = \sqrt{(x_2 - x_1)^2 + (y_2 - y_1)^2 + (z_2 - z_1)^2} \, ,$$

kako smo i željeli. U $\mathbb{R}^n$, odnosno $\mathbb{R}_{[0,1]}$ udaljenost je dana s

$$d(a, b) = \left[\sum_{i=1}^{n} (\alpha_i - \beta_i)^2 \right]^{1/2} \, ,$$

i

$$d(f, g) = \left[\int_0^1 [f(t) - g(t)]^2 dt \right]^{1/2} \, .$$

TEOREM 1

Funkcija $d : U \times U \to \mathbb{R}$ udaljenosti ima ova svojstva:

(1) *pozitivna definitnost:* $d(a,b) \geq 0$,

(2) *strogost:* $d(a,b) = 0 \Leftrightarrow a = b$,

(3) *simetričnost:* $d(b,a) = d(a,b)$,

(4) *nejednakost trokuta:* $d(a,b) \leq d(a,c) + d(c,b)$,

za svaki izbor $a, b, c \in U$.

Dokaz

Iz svojstava norme. (1) i (2) je očigledno. Nadalje

$$d(b,a) = \|b-a\| = \|(-1)(a-b)\| = |-1| \cdot \|a-b\| = \|a-b\| = d(a,b) ,$$

tj. vrijedi (3). Konačno, (4) izlazi iz nejednakosti trokuta za normu, jer imamo

$$\begin{aligned} d(a,b) &= \|a-b\| = \|(a-c)+(c-b)\| \leq \\ &\leq \|a-c\| + \|c-b\| = d(a,c) + d(c,b) . \end{aligned}$$

■

Primijetimo da se u dokazu nismo služili strukturom unitarnog prostora, nego samo aksiomima norme. Prema tome, teorem je istinit i u normiranom prostoru, tj. u svakom se takvom prostoru može pomoću norme definirati udaljenost vektora s navedenim svojstvima.

U matematici se pojam udaljenosti definira još mnogo općenitije, neovisno o normi i linearnoj strukturi. Neka je X bilo koji **skup**, a

$$d : X \times X \to \mathbb{R}$$

preslikavanje sa svojstvima (1)–(4) iz Tm 1. Onda kažemo da je d jedna **funkcija udaljenosti**, **metrička funkcija**, ili kraće, **metrika** na skupu X, a par (X,d) nazivamo **metrički prostor**.

Svaki unitarni prostor, i općenitije, svaki normirani prostor postaje, dakle, preko metrike inducirane normom, jedan metrički prostor. Obrat dakako ne vrijedi jer metrički prostor ne mora biti niti linearan.

ZADACI

1. Aksiomi metrike nisu nezavisni. Uvjeri se da se npr. (1) može dokazati pomoću ostalih aksioma.

2. Uvjeri se da je na prostoru $\mathbb{R}^n$ svakom od funkcija

   (a) $d(a,b) = \sum_{i=1}^{n} |\alpha_i - \beta_i|$;

(b) $d(a,b) = [\sum_{i=1}^{n} |\alpha_i - \beta_i|^p]^{1/p}$, gdje je p dani prirodni broj;

(c) $d(a,b) = \max\{|\alpha_1 - \beta_1|, \ldots, |\alpha_n - \beta_n|\}$;

(d) $d(a,b) = \begin{cases} 1, & a \neq b \\ 0, & a = b \end{cases}$

dobro definirana metrika. Ova posljednja (koja se, uostalom, može definirati na svakom skupu) zove se **diskretna metrika**.

3. Nađi nekoliko metrika na skupu $\mathbb{R}$ realnih brojeva. Pokaži da je

$$d(a,b) = \operatorname{arctg} |a - b|$$

jedna metrika na $\mathbb{R}$.

4. Neka je d metrika na skupu X. Onda su:

(a) $d'(a,b) = \dfrac{d(a,b)}{1 + d(a,b)}$;

(b) $d''(a,b) = \min\{1, d(a,b)\}$,

također metrike na skupu X. Dokaži!

5. Ako u definiciji metrike zamijenimo aksiom (2) blažim zahtjevom

(2') $a = b \Rightarrow d(a,b) = 0$,

dobivamo tzv. **pseudometriku** na skupu X. Pokaži da je za (x_1, y_1) i (x_2, y_2) iz $\mathbb{R}^2$ formulom

$$d\,[(x_1, y_1), (x_2, y_2)] = |x_1 - x_2|$$

dana jedna pseudometrika u ravnini. Je li d metrika?

6. Dokaži indukcijom da u svakom metričkom prostoru X vrijedi i ova **nejednakost mnogokuta**:

$$d(a_1, a_n) \leq d(a_1, a_2) + d(a_2, a_3) + \cdots + d(a_{n-1}, a_n) ,$$

za svaki izbor točaka $a_1, a_2, \ldots, a_n \in X$.

7. Za danu metriku na linearnom prostoru V ne mora postojati norma na V, koja bi tu metriku inducirala. Prema tome, klasa metričkih linearnih prostora je šira od klase normiranih prostora. Dokaži! [Uputa: Uoči da bi za takvu normu moralo vrijediti $\|a\| = d(a, \Theta)$, gdje je d polazna metrika.]

8. U metričkom prostoru (X, d) možemo definirati pojam (otvorene) **kugle**, sa središtem u $x_0 \in X$ i radijusa r. To je skup

$$K(x_0, r) = \{x \in X \mid d(x, x_0) < r\} .$$

Za podskup $U \subset X$ kažemo da je **otvoren**, ako se može prikazati kao unija neke familije kugala iz X. Pokaži da kolekcija $\mathcal{U}$ svih otvorenih skupova iz X ima ova svojstva:

(1) unija bilo koje familije elemenata iz $\mathcal{U}$ je opet element iz $\mathcal{U}$,

(2) presjek konačno mnogo elemenata iz $\mathcal{U}$ je element iz $\mathcal{U}$, i

(3) X i $\emptyset$ su elementi iz $\mathcal{U}$.

Kolekciju $\mathcal{U}$ nazivamo **topološka struktura** ili **topologija** na prostoru X. Iz svega rečenog, zaključujemo da su unitarni i uopće normirani prostori prirodno snabdjeveni topološkom strukturom, koja ih čini **topološkim prostorima**[*]. Topološka baza (vidi točku 7.4.) ili **baza topologije** je podskup $\mathcal{B} \subset \mathcal{U}$ sa svojstvom, da se svaki element iz $\mathcal{U}$ može dobiti kao unija elemenata iz $\mathcal{B}$. Očito, baza nije jednoznačno određena topologijom $\mathcal{U}$. U metričkom prostoru jednu bazu čine npr. sve kugle, a drugu, racionalniju, kugle polumjera $r = 1/n$, $n \in \mathbb{N}$.

12.7. Gramova matrica

U unitarnom prostoru možemo na jednostavan način doći do kriterija za utvrđivanje linearne zavisnosti, odnosno nezavisnosti skupa vektora iz tog prostora, i to bez upotrebe koordinata.

Neka je

$$S = \{a_1, ..., a_k\}$$

konačan skup vektora iz unitarnog prostora U. Kako znamo, taj će skup biti linearno zavisan, odnosno nezavisan, već prema tome može li relacija

$$\lambda_1 a_1 + \cdots + \lambda_k a_k = \Theta \tag{1}$$

biti ispunjena i netrivijalno, ili samo trivijalno.

[*] Sasvim općenito, **topološki prostor** se definira kao par $(X, \mathcal{U})$, koji se sastoji od skupa X i kolekcije

$$\mathcal{U} = \{\mathcal{U}_\alpha \subset X \mid \alpha \in A\}$$

podskupova od X, koja zadovoljava uvjete (1)–(3) propisane u Zad. 8., tzv. **aksiome topologije**. Elemente iz $\mathcal{U}$ nazivamo **otvoreni skupovi** u X. Razabiremo da je, prema toj definiciji, metrički prostor specijalni slučaj topološkog prostora.

Pomnožimo (1) skalarno vektorom a_i zdesna. Imamo

$$(\sum_{j=1}^{n} \lambda_j a_j, a_i) = (\Theta, a_i) ,$$

odnosno

$$\sum_{j=1}^{n} \lambda_j (a_j, a_i) = 0 .$$

Ako to ponovimo sa svakim a_i, $i = 1, ..., k$, dolazimo do skupa relacija

$$\begin{aligned}
(a_1, a_1)\lambda_1 + (a_2, a_1)\lambda_2 + \cdots + (a_k, a_1)\lambda_k &= 0 \\
(a_1, a_2)\lambda_1 + (a_2, a_2)\lambda_2 + \cdots + (a_k, a_2)\lambda_k &= 0 \\
\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots & \\
(a_1, a_i)\lambda_1 + (a_2, a_i)\lambda_2 + \cdots + (a_k, a_i)\lambda_k &= 0 \\
\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots & \\
(a_1, a_k)\lambda_1 + (a_2, a_k)\lambda_2 + \cdots + (a_k, a_k)\lambda_k &= 0 ,
\end{aligned} \tag{2}$$

koje možemo shvatiti kao homogeni sustav linearnih jednadžbi u nepoznanicama $\lambda_1, ..., \lambda_k$, s koeficijentima iz polja F.

PROPOZICIJA 1

Uređena k–torka $(\lambda_1^0, \cdots, \lambda_k^0)$ *skalara iz polja* F *će zadovoljavati relaciju* (1) *ako i samo ako je ona jedno od rješenja homogenog sustava* (2).

Dokaz

Nužnost je očigledna. Dokažimo dovoljnost. Ako je (λ_j^0) rješenje od (2), i–ta jednadžba postaje

$$\sum_{j=1}^{k} \lambda_j^0 (a_j, a_i) = 0 .$$

Ako tu jednakost pomnožimo s $\overline{\lambda_i^0}$, $i = 1, \ldots, k$, i sve jednakosti zbrojimo, dobivamo

$$\sum_{i=1}^{k} \overline{\lambda_i^0} \left(\sum_{j=1}^{k} \lambda_j^0 (a_j, a_i) \right) = 0 ,$$

odnosno

$$\sum_{i=1}^{k} \sum_{j=1}^{k} \lambda_j^0 \overline{\lambda_i^0} (a_j, a_i) = 0 .$$

No, to se prema Zad. 1. u 12.2. može pisati kao

$$\left(\sum_{j=1}^{k} \lambda_j^0 a_j , \sum_{i=1}^{k} \lambda_i^0 a_i \right) = 0 .$$

Pritom su faktori u skalarnom produktu jednaki (imamo samo različito označene indekse sumacije), pa zaključujemo da mora biti

$$\sum_{i=1}^{k} \lambda_i^0 a_i = \Theta \,,$$

što pokazuje da $(\lambda_1^0, \cdots, \lambda_k^0)$ zadovoljava relaciju (1). ■

Prema tome, karakter skupa S će ovisiti o rješenjima sustava (2). Ta rješenja ovise o matrici sustava, odnosno njezinoj determinanti. Matricu

$$G(S) = \begin{bmatrix} (a_1, a_1) & (a_2, a_1) & \cdots & (a_k, a_1) \\ (a_1, a_2) & (a_2, a_2) & \cdots & (a_k, a_2) \\ \vdots & \vdots & \ddots & \vdots \\ (a_1, a_k) & (a_2, a_k) & \cdots & (a_k, a_k) \end{bmatrix} = [(a_j, a_i)]$$

sustava (2) nazivamo **Gramova matrica** skupa vektora $S \subset U$. Primijetimo da iz svojstva hermitske komutativnosti skalarnog produkta slijedi da je ta matrica hermitska, odnosno simetrična, već prema tome je li U kompleksan ili realan unitarni prostor (vidi Zad. 4., odnosno 1. u 9.3.). Nadalje, determinantu te matrice označavamo s

$$\Gamma(S) = \det G(S) = \begin{vmatrix} (a_1, a_1) & \cdots & (a_k, a_1) \\ \vdots & & \vdots \\ (a_1, a_k) & \cdots & (a_k, a_k) \end{vmatrix}$$

i zovemo **Gramova determinanta** skupa S. Na osnovi Kor. 3 iz 11.5. (Roucheov teorem), odmah zaključujemo da će homogeni sustav (2) imati i netrivijalnih rješenja ako i samo ako je determinanta matrice tog sustava jednaka nuli, tj. ako vrijedi

$$\Gamma(S) = 0 \,.$$

Kombiniranjem tog rezultata s Prop. 1 dokazali smo ovaj teorem:

TEOREM 2

Neka je S konačan skup vektora iz unitarnog prostora U. Taj je skup

(1) *linearno nezavisan ako i samo ako je*

$$\Gamma(S) \neq 0 \,;$$

(2) *linearno zavisan ako i samo ako je*

$$\Gamma(S) = 0 \,.$$ ■

Nekoliko riječi o geometrijskoj interpretaciji Gramove determinante. U prostoru V^3 je $\Gamma(\vec{a}) = \vec{a} \cdot \vec{a} = \vec{a}^2$, pa je $\sqrt{\Gamma(\vec{a})} = |\vec{a}|$, tj. korijen Gramove determinante vektora $\vec{a}$ jednak je duljini tog vektora. Za vektore $\vec{a}, \vec{b} \in V^3$, rabeći Lagrangeov identitet (Zad. 2. u 5.11.) imamo

$$\Gamma(\vec{a}, \vec{b}) = \begin{vmatrix} \vec{a}^2 & \vec{b}\vec{a} \\ \vec{a}\vec{b} & \vec{b}^2 \end{vmatrix} = \vec{a}^2\vec{b}^2 - (\vec{a}\vec{b})^2 = (\vec{a} \times \vec{b})^2 ,$$

dakle

$$\sqrt{\Gamma(\vec{a}, \vec{b})} = |\vec{a} \times \vec{b}| ,$$

tj. kvadratni korijen Gramove determinante vektora $\vec{a}$ i $\vec{b}$ jednak je površini paralelograma što ga ti vektori razapinju. Posve se analogno pokazuje da je

$$\sqrt{\Gamma(\vec{a}, \vec{b}, \vec{c})} = |(\vec{a}, \vec{b}, \vec{c})| ,$$

tj. da je korijen Gramove determinante tri vektora $\vec{a}, \vec{b}, \vec{c} \in V^3$ jednak apsolutnoj vrijednosti mješovitog produkta, tj. volumenu paralelepipeda (Tm. 6 u 5.13.) što ga ti vektori razapinju u prostoru.

Navedeni primjeri nas motiviraju za sljedeću generalizaciju: Neka je $\{a_1, \ldots, a_k\} \subset U$ linearno nezavisan skup vektora u realnom unitarnom prostoru U. Onda skup

$$P = \left\{a \in U \mid a = \sum_{i=1}^{k} \lambda_i a_i,\ 0 \leq \lambda_i \leq 1,\ i = 1, \ldots, k\right\}$$

zovemo k-dimenzionalni **paralelotop** razapet skupom vektora $\{a_1, \ldots, a_k\}$ u prostoru U. Po analogiji s prethodnim, **volumen paralelotopa** P definiramo kao broj

$$V = \sqrt{\Gamma(a_1, \ldots, a_k)} .$$

Volumen je dobro definiran realni broj jer se pokazuje da je Gramova determinanta uvijek nenegativna (vidi Kor. 8 u 12.8.).

ZADACI

1. Dokaži da je $V = \sqrt{\Gamma(\vec{a}, \vec{b}, \vec{c})}$ volumen paralelepipeda razapetog vektorima $\vec{a}, \vec{b}, \vec{c} \in V^3$.

2. Neka je B bilo koja baza za U, a $a = (\alpha_i)$ i $b = (\beta_i)$ vektori dani svojim koordinatama u toj bazi. Onda je

$$(a, b) = \sum_{i=1}^{n} \sum_{k=1}^{n} a_{ik} \alpha_i \overline{\beta}_k ,$$

i specijalno

$$\|a\| = \left(\sum_{i=1}^{n} \sum_{k=1}^{n} a_{ik} \alpha_i \overline{\alpha}_k \right)^{1/2} ,$$

gdje su a_{ik} elementi Gramove matrice $\Gamma(B)$. Dokaži!

3. Neka su $a_1, ..., a_k, a_{k+1}, ..., a_m \in U$ bilo koji vektori. Onda vrijedi

$$\Gamma(a_1, ..., a_k, a_{k+1}, ..., a_m) \leq \Gamma(a_1, ..., a_k) \cdot \Gamma(a_{k+1}, ..., a_m) .$$

Dokaži! Kada u toj relaciji vrijedi znak jednakosti?

4. Neka je $f : U \to U$ linearni operator koji djeluje na n-dimenzionalnom unitarnom prostoru U. Neka su $a_1, ..., a_n \in U$ bilo koji vektori, a $b_i = f(a_i)$ njihove slike. Dokaži da je

$$\Gamma(b_1, ..., b_n) = (\det F)^2 \cdot \Gamma(a_1, ..., a_n) ,$$

gdje je F (bilo koji) matrični zapis operatora f.

12.8. Ortonormirani skupovi vektora

Neka su $a, b \in U$ vektori u unitarnom prostoru. Kažemo da je a **ortogonalan** na b, i pišemo

$$a \perp b ,$$

ako i samo ako je

$$(a, b) = 0 .$$

Kako $(a, b) = 0$ povlači $\overline{(b, a)} = 0$, a ovo opet $(b, a) = 0$, "biti ortogonalan" je simetrična relacija pa govorimo o **paru ortogonalnih vektora**. Nadalje, jer je $(\Theta, a) = (a, \Theta) = 0$, za svaki a iz U, nulvektor je ortogonalan na svaki vektor prostora, i to je očito jedini vektor s tim svojstvom.

U prostorima $\mathbb{R}^n$ i $\mathbb{R}_{[0,1]}$ ortogonalnost se izražava formulama

$$\sum_{i=1}^{n} \alpha_i \beta_i = 0 \quad i \quad \int_0^1 f(t) g(t) dt = 0 .$$

Primijetimo da je ortogonalnost dobra generalizacija pojma okomitosti, jer će u V^3 ili, općenitije, u bilo kojem realnom unitarnom prostoru U dva vektora biti ortogonalna ako i samo ako je bar jedan od njih nulvektor, ili su okomiti u geometrijskom smislu, tj. zatvaraju kut od $\pi/2$ (vidi točke 5.9. i 12.5.).

Neka je $S = \{a_1, ..., a_s\}$ skup vektora iz unitarnog prostora U, u kojem je svaki vektor **različit** od nulvektora. Kažemo da je S **ortogonalan skup vektora** ako su svaka dva međusobno različita vektora iz S ortogonalna, tj.

$$a_i \perp a_k ,$$

za $i \neq k$. Po definiciji, smatramo da je ortogonalan skup i onaj koji se sastoji od jednog jedinog vektora različitog od nulvektora. Ako je uz to svaki od vektora iz S i normiran, tj.

$$\|a_i\| = 1 ,$$

za svaki i, kažemo da je S **ortonormiran skup vektora**. To će, dakako, biti slučaj ako i samo ako za vektore iz S vrijedi

$$(a_i, a_k) = \delta_{ik} .$$

U specijalnom slučaju, kada je S i baza prostora U, govorimo o **ortogonalnoj**, odnosno **ortonormiranoj bazi**. Takvu uređenu bazu često zovemo i **ortonormirani koordinatni sustav** u U.

Ove definicije imaju, naravno, smisla i kada je skup S beskonačan.

TEOREM 1

Svaki ortogonalan skup vektora iz unitarnog prostora je linearno nezavisan.

Dokaz

Neka je $S = \{a_1, ..., a_s\} \subset U$ ortogonalan skup vektora. Promatrajmo relaciju

$$\alpha_1 a_1 + \cdots + \alpha_s a_s = \Theta . \tag{1}$$

Množeći u (1) obje strane skalarno sa a_i, za bilo koji $i = 1, ..., s$, imamo

$$(\alpha_1 a_1 + \cdots + \alpha_s a_s, a_i) = (\Theta, a_i) = 0 ,$$

odnosno

$$\alpha_1 (a_1, a_i) + \cdots + \alpha_i (a_i, a_i) + \cdots + \alpha_s (a_s, a_i) = 0 ,$$

a ta se relacija zbog ortogonalnosti reducira na

$$\alpha_i \cdot \|a_i\|^2 = 0 .$$

Kako je po definiciji $\|a_i\| \neq 0$, zaključujemo da je

$$\alpha_i = 0 .$$

To vrijedi za svaki $i = 1, ..., s$, pa iz (1) slijedi da je skup S linearno nezavisan. ■

KOROLAR 2

Neka je U unitarni prostor dimenzije n. Onda ortogonalni skup vektora iz U ne može imati više od n vektora. ■

Za ortogonalni skup $M = \{a_1, ..., a_m\} \subset U$ kažemo da je **maksimalan**, ako iz $a \in U$ i $a \perp a_i$, za svaki $i = 1, ..., m$, slijedi da je nužno $a = \Theta$.

TEOREM 3

Svaki se ortogonalni skup vektora u (konačnodimenzionalnom) unitarnom prostoru U može dopuniti do ortogonalne baze prostora.

Dokaz

Neka je $S = \{a_1, ..., a_s\} \subset U$ bilo koji ortogonalan skup. Neka je, nadalje,

$$M = \{a_1, ..., a_s, a_{s+1}, ..., a_m\} \subset U \tag{2}$$

jedan maksimalan ortogonalni skup u U, koji sadrži polazni skup S. Zbog Kor. 2 takav skup uvijek postoji, i vrijedi

$$m \leq n = \dim U \ .$$

Skup (2) je linearno nezavisan po Tm. 1. Da bi predstavljao bazu, treba još pokazati da je to skup izvodnica za U. Neka je $x \in U$ bilo koji vektor. Promatrajmo skalare

$$\alpha_i = \frac{(x, a_i)}{(a_i, a_i)} \ , \tag{3}$$

za svaki $i = 1, ..., m$, i zatim vektor

$$y = \alpha_1 a_1 + \cdots + \alpha_i a_i + \cdots + \alpha_m a_m \ .$$

Skalarnim množenjem ove relacije s a_i, zbog ortogonalnosti i (3) imamo

$$(y, a_i) = \alpha_i (a_i, a_i) = (x, a_i) \ .$$

Odatle slijedi da je

$$(y - x, a_i) = 0 \ , \tag{4}$$

za svaki $i = 1, ..., m$. Kako je skup (2) maksimalan, iz (4) slijedi da je

$$y - x = \Theta \ ,$$

dakle

$$x = y = \sum_{i=1}^{m} \alpha_i a_i \ ,$$

što pokazuje da je (2) skup izvodnica, dakle i baza za U. Zaključujemo, također, da je nužno $m = n$. ■

KOROLAR 4

Svaki netrivijalni unitarni prostor ima bar jednu ortonormiranu bazu.

Dokaz

Ako je $U \neq \{\Theta\}$, vektor $a \neq \Theta$ iz U (koji po definiciji predstavlja ortogonalni skup) možemo po Tm. 3 dopuniti do ortogonalne baze prostora, koju je onda lako normirati. ■

PROPOZICIJA 5

Neka je $E = (e_1, ..., e_n)$ ortonormirana baza prostora U, $a \in U$ bilo koji vektor i $(\alpha_1, ..., \alpha_n)$ koordinatni slog tog vektora u odnosu na bazu E. Onda je

$$\alpha_i = (a, e_i) ,$$

za svaki $i = 1, ..., n$.

Dokaz

Kako je

$$a = \alpha_1 e_1 + \cdots + \alpha_n e_n ,$$

skalarnim množenjem s e_i, zbog ortogonalnosti, dobivamo

$$(a, e_i) = \alpha_i \|e_i\|^2 = \alpha_i ,$$

a to se i tvrdilo. ■

Brojevi (a, e_i) zovu se **Fourierovi koeficijenti** vektora a.

PROPOZICIJA 6

Neka je $E = (e_1, ..., e_n) \subset U$ ortonormirana baza, a $a = (\alpha_i)$, $b = (\beta_i)$ vektori iz U, dani svojim koordinatama u toj bazi. Onda je njihov skalarni produkt dan formulom

$$(a, b) = \alpha_1 \overline{\beta}_1 + \cdots + \alpha_n \overline{\beta}_n .$$

Dokaz

Kako je $a = \sum_{i=1}^{n} \alpha_i e_i$ i $b = \sum_{k=1}^{n} \beta_k e_k$, imamo

$$\begin{aligned} (a, b) &= (\sum_{i=1}^{n} \alpha_i e_i, \sum_{k=1}^{n} \beta_k e_k) = \sum_{i=1}^{n} \sum_{k=1}^{n} \alpha_i \overline{\beta}_k (e_i, e_k) = \\ &= \sum_{i=1}^{n} \sum_{k=1}^{n} \alpha_i \overline{\beta}_k \delta_{ik} = \sum_{i=1}^{n} \alpha_i \overline{\beta}_i , \end{aligned}$$

i tvrdnja je dokazana. ■

PROPOZICIJA 7

Neka je $E = (e_1, ..., e_n)$ *ortonormirana baza za prostor* U, *a* $S = \{a_1, ..., a_s\} \subset U$ *bilo koji skup vektora. Neka je* $M = M(S)$ *matrica tog skupa vektora u bazi* E. *Onda je Gramova matrica skupa* S

$$G(S) = M^*M \, .$$

Dokaz

Ako je $a_k = (\alpha_{1k}, ..., \alpha_{nk})$ koordinatni slog vektora a_k u bazi E, $k = 1, ..., s$, onda je zbog Prop. 6

$$\begin{aligned} M^*M &= \begin{bmatrix} \overline{\alpha}_{11} & \cdots & \overline{\alpha}_{n1} \\ \vdots & & \vdots \\ \overline{\alpha}_{1s} & \cdots & \overline{\alpha}_{ns} \end{bmatrix} \cdot \begin{bmatrix} \alpha_{11} & \cdots & \alpha_{1s} \\ \vdots & & \vdots \\ \alpha_{n1} & \cdots & \alpha_{ns} \end{bmatrix} = \\ &= \left[\sum_{j=1}^{n} \overline{\alpha}_{ji} \alpha_{jk} \right] = \left[\sum_{j=1}^{n} \alpha_{jk} \overline{\alpha}_{ji} \right] = [(a_k, a_i)] = G(S). \end{aligned}$$

■

KOROLAR 8

Za bilo koji konačni skup vektora $S \subset U$ *je*

$$\Gamma(S) \geq 0 \, .$$

Dokaz

Pretpostavimo najprije da je $\operatorname{card} S = n = \dim U$. Onda je M kvadratna matrica pa, iz Prop. 7, primjenom Binet-Cauchyjeva teorema imamo

$$\begin{aligned} \Gamma(S) &= \det G(S) = \det M^*M = \det M^* \det M = \det \overline{M} \det M = \\ &= \overline{\det M} \det M = |\det M|^2 \geq 0 \, . \end{aligned}$$

Kad je $\operatorname{card} S \neq n$, dokaz je nešto složeniji (vidi Zad. 8.). ■

ZADACI

1. Dokaži: Matrica prijelaza iz jedne ortonormirane baze u drugu ortonormiranu bazu uvijek je unitarna matrica (vidi Zad. 8. i 9. u 9.5. ili točku 13.3.).

2. Obratno: Neka je $S = \{a_1, ..., a_n\} \subset U$, $n = \dim U$, skup vektora sa svojstvom da je matrica tog skupa u odnosu na neku ortonormiranu bazu unitarna. Onda je S ortonormirana baza prostora U. Dokaži!

3. Neka je $E = (e_1, ..., e_m) \subset U$ ortonormirani skup vektora, a $a \in U$ bilo koji vektor. Onda, uz oznake

$$\alpha_i = (a, e_i) ,$$

vrijedi sljedeća nejednakost:

$$(a, a) \geq |\alpha_1|^2 + \cdots + |\alpha_m|^2 ,$$

tzv. **Besselova nejednakost**. Nadalje, ako je polazni skup E baza za prostor U, nejednakost postaje jednakost, i to je tzv. **Parsevalova jednakost** . Dokaži!

4. Parsevalova jednakost karakterizira ortonormirane baze: Ortonormirani skup $E = (e_1, ..., e_m) \subset U$ je baza za U ako i samo ako za svaki $a \in U$ vrijedi

$$(a, a) = |\alpha_1|^2 + \cdots + |\alpha_m|^2 ,$$

gdje je $\alpha_i = (a, e_i)$, $i = 1, ..., m$. Dokaži!

5. Dokaži: Ortonormirani skup $E = (e_1, ..., e_m)$ jest baza za U ako i samo ako je ispunjeno

$$(a, b) = \sum_{i=1}^{m} (a, e_i)(e_i, b) ,$$

za svaki $a, b \in U$. To je neka vrsta obrata Prop. 6.

6. Neka je $S = \{a_1, ..., a_s\} \subset U$ ortogonalan skup vektora. Uvjeri se da za te vektore vrijedi

$$\|a_1 + \cdots + a_s\|^2 = \|a_1\|^2 + \cdots + \|a_s\|^2 .$$

To je generalizirani **Pitagorin teorem**.

7. Uvjeri se da je skup

$$\{e^{int}/\sqrt{2\pi} \mid n = 0, 1, 2, ...\}$$

funkcija iz $\mathbb{C}_{[-\pi,\pi]}$ ortonormiran (uz standardni skalarni produkt u $\mathbb{C}_{[-\pi,\pi]}$). To je primjer beskonačnog ortonormiranog skupa.

8. Dokaži Kor. 8 u općem slučaju! [Uputa: Neka je $M \in M_{ns}$ kao u Prop. 7. Neka je λ bilo koja svojstvena vrijednost matrice $M^*M \in M_s$ (vidi Zad. 5. u 10.9.), a $X \in M_{s1}$ pripadni svojstveni vektor, $X \neq O$. Uvjeri se da je onda $(MX)^*MX \geq 0$, odakle odmah slijedi da je nužno $\lambda \geq 0$, pa je tvrdnja posljedica rezultata u točki 10.10.]

12.9. Gram-Schmidtov postupak ortogonalizacije

U prošloj smo točki dokazali egzistenciju ortonormirane baze u unitarnom prostoru. Sada ćemo opisati efektivni postupak koji nam omogućuje, da dođemo do takve baze. Konstrukcija polazi od bilo koje baze prostora, koju onda postupnom zamjenom vektora prevodimo u ortonormiranu bazu prostora, tijesno vezanu uz polaznu bazu. To je tzv. Gram–Schmidtov postupak ortogonalizacije.

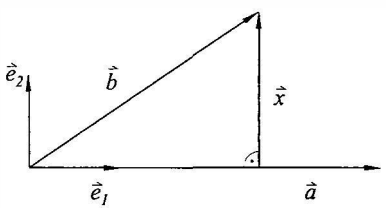
Razmotrimo najprije tu ideju na jednom primjeru. Neka je $(\vec{a}, \vec{b}) \subset V^3$ linearno nezavisan skup vektora u V^3. Želimo ga nadomjestiti ortonormiranim skupom $(\vec{e}_1, \vec{e}_2) \subset V^3$, ali tako da $\vec{e}_1$ bude kolinearan s $\vec{a}$, a $\vec{e}_2$ komplanaran s $\vec{a}$ i $\vec{b}$. To će onda značiti da vektori $\vec{e}_1$ i $\vec{e}_2$ razapinju u V^3 istu ravninu kao i vektori $\vec{a}$ i $\vec{b}$. Definirajmo najprije

$$\vec{e}_1 = \frac{1}{|\vec{a}|} \cdot \vec{a} \, .$$

Zatim konstruirajmo vektor $\vec{x}$, stavljajući

$$\vec{x} = \vec{b} - (\vec{b}\vec{e}_1)\vec{e}_1 = \vec{b} - \frac{(\vec{b}\vec{a})\vec{a}}{|\vec{a}|^2} \, ,$$

tj. oduzimajući od $\vec{b}$ njegovu ortogonalnu projekciju na vektor $\vec{a}$. Jasno je



da je $\vec{x}$ okomit na $\vec{e}_1$. Stavljajući

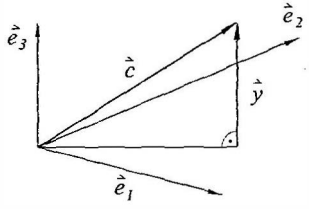
$$\vec{e}_2 = \frac{1}{|\vec{x}|} \cdot \vec{x} \, ,$$

dolazimo do traženog sustava $(\vec{e}_1, \vec{e}_2)$.

Posve analogno, polazeći od linearno nezavisnog skupa $(\vec{a}, \vec{b}, \vec{c}) \subset V^3$, dakle baze u V^3, možemo konstruirati ortonormiranu bazu $(\vec{e}_1, \vec{e}_2, \vec{e}_3)$ sa svojstvom da je $\vec{e}_1$ kolinearan s $\vec{a}$, $\vec{e}_2$ komplanaran s $\vec{a}$ i $\vec{b}$, a $\vec{e}_3$ linearno zavisan s $\vec{a}, \vec{b}, \vec{c}$ (to je u ovom slučaju jasno, jer se sve odigrava u V^3). Postupak ide ovako: odaberemo $\vec{e}_1$ i $\vec{e}_2$ kao prije, a zatim definiramo vektor $\vec{y}$ s

$$\vec{y} = \vec{c} - [(\vec{c}\vec{e}_1)\vec{e}_1 + (\vec{c}\vec{e}_2)\vec{e}_2] \, ,$$

tj. oduzimajući od $\vec{c}$ njegovu ortogonalnu projekciju na ravninu razapetu vektorima $\vec{e}_1$ i $\vec{e}_2$ (vidi sliku).



Iz definicije od $\vec{y}$ slijedi da je

$$(\vec{y}, \vec{e}_1) = 0 \quad i \quad (\vec{y}, \vec{e}_2) = 0 \,,$$

tj. da je $\vec{y}$ okomit na vektore $\vec{e}_1$ i $\vec{e}_2$. Normiranjem dobivamo

$$\vec{e}_3 = \frac{1}{|\vec{y}|} \cdot \vec{y} \,,$$

i tako dolazimo do ortonormirane baze $(\vec{e}_1, \vec{e}_2, \vec{e}_3)$, koja ima tražena svojstva.

Opisani postupak nije teško generalizirati. Imamo

TEOREM 1 (Gram-Schmidt)

Neka je

$$S = (a_1, \ldots, a_m)$$

uređeni linearno nezavisni skup vektora iz unitarnog prostora U. Taj se skup može **ortonormirati**, *tj. zamijeniti novim skupom*

$$T = (e_1, \ldots, e_m) \subset U \,,$$

tako da vrijedi:

(1) *T je ortonormirani skup, i*

(2) *$[\{e_1, \ldots, e_j\}] = [\{a_1, \ldots, a_j\}]$, tj. prvih j vektora od T razapinju isti potprostor od U kao i prvih j vektora od S, za svaki $j = 1, \ldots, m$.*

Dokaz

Skup T gradimo korak po korak, induktivno. Stavimo najprije

$$e_1 = \frac{a_1}{\|a_1\|} \,,$$

čime su očito ispunjeni (1) i (2). Pretpostavimo da smo konstruirali skup

$$(e_1, \ldots, e_k) \tag{3}$$

koji ima svojstva (1) i (2), tj. koji je ortonormiran i razapinje isti potprostor kao vektori $(a_1, \ldots, a_k)$. Želimo definirati vektor e_{k+1}. Promatrajmo vektor

$$b_{k+1} = a_{k+1} - \sum_{j=1}^{k} (a_{k+1}, e_j) e_j \,. \tag{4}$$

Po pretpostavci indukcije imamo

$$a_{k+1} \notin [\{a_1, \ldots, a_k\}] = [\{e_1, \ldots, e_k\}] \,,$$

pa je $(a_{k+1}, e_1, \ldots, e_k)$ linearno nezavisan skup. Odatle slijedi da vrijedi $b_{k+1} \neq \Theta$, pa ga možemo normirati. Definiramo

$$e_{k+1} = \frac{b_{k+1}}{\|b_{k+1}\|} \,. \tag{5}$$

Tvrdimo da skup vektora

$$(e_1, \ldots, e_k, e_{k+1}) \tag{6}$$

ima svojstva (1) i (2). Pokažimo najprije da je ortonormiran. Kako je (3) već ortonormiran po pretpostavci indukcije, a iz (5) je očito $\|e_{k+1}\| = 1$. Ostaje pokazati da vrijedi

$$(e_{k+1}, e_i) = 0 \,,$$

za svaki $i = 1, \ldots, k$. No, zbog (4) i (5) imamo

$$\begin{aligned}
(e_{k+1}, e_i) &= \frac{1}{\|b_{k+1}\|}(b_{k+1}, e_i) = \frac{1}{\|b_{k+1}\|}(a_{k+1} - \sum_{j=1}^{k}(a_{k+1}, e_j)e_j, e_i) = \\
&= \frac{1}{\|b_{k+1}\|}\left[(a_{k+1}, e_i) - \sum_{j=1}^{k}(a_{k+1}, e_j)\underbrace{(e_j, e_i)}_{\delta_{ji}}\right] = \\
&= \frac{1}{\|b_{k+1}\|}[(a_{k+1}, e_i) - (a_{k+1}, e_i)] = 0 \,,
\end{aligned}$$

i tvrdnja je dokazana.

Nadalje, zbog pretpostavke indukcije, te (4) i (5) je

$$e_1, \ldots, e_k,\ e_{k+1} \in [\{a_1, .., a_k,\ a_{k+1}\}] \,,$$

a jer su ti vektori i linearno nezavisni (ortonormirani skup), to je

$$[\{e_1, \ldots, e_{k+1}\}] = [\{a_1, .., a_{k+1}\}] \,,$$

kako se i tvrdilo. Indukcija svršava s $k = m$ i teorem je dokazan. ■

KOROLAR 2

Svaka se baza unitarnog prostora može ortonormirati, tj. zamijeniti ortonormiranom bazom (koja ima i svojstvo (2)*). Prema tome, u netrivijalnom unitarnom prostoru uvijek postoje ortonormirane baze.*

Dokaz

Neposredno iz Tm. 1. ■

Time smo ponovno dokazali egzistenciju ortonormiranih baza.

Neka je $B = (a_1, \ldots, a_n)$ bilo koja baza prostora U, a $E = (e_1, \ldots, e_n)$ ortonormirana baza koja joj je pridružena Gram-Schmidtovim postupkom. Onda je iz konstrukcije u Tm. 1 jasno da je

$$\begin{aligned} e_1 &= \alpha_{11} a_1 \\ e_2 &= \alpha_{21} a_1 + \alpha_{22} a_2 \\ \cdots &\quad \cdots\cdots\cdots\cdots \\ e_n &= \alpha_{n1} a_1 + \alpha_{n2} a_2 + \cdots + \alpha_{nn} a_n \end{aligned}$$

i pritom je

$$\alpha_{ii} = \frac{1}{\|b_i\|} ,$$

za svaki i, gdje je b_i definiran formulom (4). Imamo, dakle,

KOROLAR 3

Matrica $T = [\alpha_{ik}]$ prijelaza iz baze B u (Gram–Schmidtovim postupkom) pridruženu ortonormiranu bazu E je uvijek gornja trokutasta matrica, pa za njezinu determinantu vrijedi

$$\det T = \frac{1}{\|b_1\| \cdots \|b_n\|} > 0 . \quad ■$$

ZADACI

1. Još nekoliko riječi o Tm. 1. Primijetimo da će postojati razni skupovi T, koji će imati tražena svojstva (1) i (2) (mogli smo npr. definirati $e_1 = -\frac{a_1}{\|a_1\|}$). Ako, međutim, zahtijevamo još
   (3) $(a_i, e_i) > 0$, za svaki $i = 1, ..., m$,
   onda je skup T određen jednoznačno. Dokaži! Uvjeri se, nadalje, da upravo skup T konstruiran u dokazu Tm. 1 ima i to dodatno svojstvo.

[Uputa: Zbog (4) i (5) imamo

$$\begin{aligned}(a_{k+1}, e_{k+1}) &= (b_{k+1} + \sum_{j=1}^{k}(a_{k+1}, e_j)e_j, e_{k+1}) = \\ &= \|b_{k+1}\| \underbrace{(e_{k+1}, e_{k+1})}_{=1} + \sum_{j=1}^{k}(a_{k+1}, e_j)\underbrace{(e_j, e_{k+1})}_{=0} = \\ &= \|b_{k+1}\| > 0\,,\end{aligned}$$

a to se i tvrdilo.]

2. Pokaži da se ortonormirani skup $(\vec{e}_1, \vec{e}_2, \vec{e}_3)$, pridružen bazi $(\vec{a}, \vec{b}, \vec{c})$ prostora V^3 u uvodnim razmatranjima, može eksplicitno napisati ovako:

$$\vec{e}_1 = \frac{\vec{a}}{\sqrt{\Gamma(\vec{a})}}\,, \qquad \vec{e}_2 = \frac{\begin{vmatrix} \vec{a}\vec{a} & \vec{b}\vec{a} \\ \vec{a} & \vec{b} \end{vmatrix}}{\sqrt{\Gamma(\vec{a})\Gamma(\vec{a}, \vec{b})}}\,,$$

$$\vec{e}_3 = \frac{\begin{vmatrix} \vec{a}\vec{a} & \vec{b}\vec{a} & \vec{c}\vec{a} \\ \vec{a}\vec{b} & \vec{b}\vec{b} & \vec{c}\vec{b} \\ \vec{a} & \vec{b} & \vec{c} \end{vmatrix}}{\sqrt{\Gamma(\vec{a}, \vec{b})\Gamma(\vec{a}, \vec{b}, \vec{c})}}\,.$$

3. Generalizirajući Zad. 2. pokaži da je jedinstveni ortonormirani skup iz Zad. 1. dan eksplicitno ovim formulama:

$$e_1 = \frac{a_1}{\sqrt{\Gamma(a_1)}}$$

i

$$e_k = \frac{\begin{vmatrix} & & & \vdots & (a_k, a_1) \\ & G(a_1, ..., a_{k-1}) & & \vdots & \vdots \\ & & & \vdots & (a_k, a_{k-1}) \\ \cdots & \cdots & \cdots & \vdots & \\ a_1 & \cdots & a_{k-1} & \vdots & a_k \end{vmatrix}}{\sqrt{\Gamma(a_1, \ldots, a_{k-1})\Gamma(a_1, \ldots, a_k)}}\,,$$

za $k = 2, ..., m$.

4. Skup vektora $\{a_1, ..., a_m\}$ je ortonormiran ako i samo ako je

$$G(a_1, ..., a_m) = E\,,$$

tj. Gramova matrica tog skupa je jedinična. Dokaži!

5. Gram-Schmidtovim postupkom ortonormiraj skupove vektora:

(a) $a_1 = (1, 0, 1)$, $a_2 = (1, 2, 0)$, $a_3 = (0, 2, 3)$ u $\mathbb{R}^3$;
(b) $a_1 = (1, i)$, $a_2 = (-i, -1)$ u $\mathbb{C}^2$;
(c) $\vec{a}_1 = \vec{\imath} + \vec{\jmath} + \vec{k}$, $\vec{a}_2 = \vec{\imath} + \vec{\jmath} - \vec{k}$, $\vec{a}_3 = \vec{\imath} - \vec{\jmath} + \vec{k}$ u V^3 ;
(d) $f_1(t) = 1$, $f_2(t) = t$, $f_3(t) = t^2$ u prostoru $\mathbb{R}_{[0,1]}$.

6. Neka je P_4 linearni prostor polinoma čiji stupanj ne prelazi 3. Standardnu bazu $B = (1, t, t^2, t^3) \subset P_4$ ortonormiraj Gram - Schmidtovim postupkom s obzirom na skalarni produkt:

(a) $(p, q) = \int_{-1}^{1} p(t)q(t)\,dt$ (dobit ćeš tzv. **Legendreove polinome**);

(b) $(p, q) = \int_{-1}^{1} \frac{p(t)q(t)}{\sqrt{1-t^2}}\,dt$ (dobit ćeš tzv. **Čebiševljeve polinome**).

Generaliziraj!

12.10. Ortogonalni komplement. Projektor

Primijetimo da je svaki (linearni) potprostor $L < U$ unitarnog prostora U i sam unitarni prostor, u odnosu na restrikciju skalarnog množenja u U na $L \times L$. Prema tome, potprostori unitarnog prostora U se podudaraju s potprostorima linearnog prostora U.

Neka su $S, T \subset U$ podskupovi unitarnog prostora U. Kažemo da je skup S **ortogonalan** na skup T, i pišemo

$$S \perp T\,,$$

ako je svaki vektor prvog skupa ortogonalan na svaki vektor drugog skupa, tj. ako vrijedi

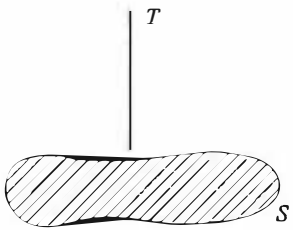
$$(a, b) = 0\,,$$

za svaki $a \in S$ i svaki $b \in T$. Iz definicije je jasno da je onda i

$$T \perp S\,,$$

tj. relacija "biti ortogonalan" je simetrična, pa govorimo o **paru ortogonalnih skupova** u U. Na primjer, je $U \perp \{\Theta\}$, jer vrijedi $(a, \Theta) = 0$, za

svaki $a \in U$.



PROPOZICIJA 1

Ako su skupovi $S, T \subset U$ ortogonalni, njihov je presjek prazan ili sadrži samo nulvektor.

Dokaz

Neka je $a \in S \cap T$. Onda je po definiciji $(a, a) = 0$, dakle $a = \Theta$. ■

Neka su $L, M < U$ potprostori od U. Kažemo da je suma $L + M$ tih potprostora **ortogonalna** ako su L i M ortogonalni skupovi, $L \perp M$.

PROPOZICIJA 2

Ortogonalna suma potprostora $L, M < U$ je uvijek direktna.

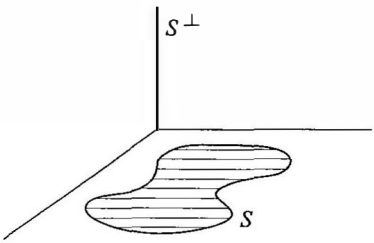
Dokaz

Neposredno iz Prop. 1, jer je $L \cap M = \{\Theta\}$. ■

Neka je sada $S \subset U$ bilo koji podskup. Onda skup

$$\{a \in U \mid \{a\} \perp S\}$$

svih vektora prostora U, koji su ortogonalni na skup S, nazivamo **ortogo-**



nalni komplement od S i standardno označavamo sa $S^\perp$. Očito je uvijek $S^\perp \perp S$.

PROPOZICIJA 3

Ortogonalni komplement bilo kojeg skupa $S \subset U$ je potprostor od U.

Dokaz

Neka su $a, b \in S^{\perp}$. Onda za bilo koji $x \in S$, te α, $\beta \in F$ vrijedi

$$(\alpha a + \beta b, x) = \alpha(a, x) + \beta(b, x) = \alpha \cdot 0 + \beta \cdot 0 = 0 \,,$$

pa je i

$$\alpha a + \beta b \in S^{\perp} \,,$$

što je i trebalo dokazati. ■

TEOREM 4

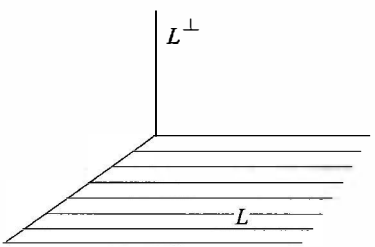
Neka je $L < U$ bilo koji potprostor. Onda se prostor U može prikazati kao direktna suma potprostora L i njegova ortogonalnog komplementa $L^{\perp}$,

$$U = L \oplus L^{\perp} \,.$$

Dokaz

Kako je $L \perp L^{\perp}$, dovoljno je pokazati da je U suma potprostora L i $L^{\perp}$, jer je onda direktna po Prop. 2.

Neka je $(e_1, ..., e_l) \subset L$ ortonormirana baza za L. Ona se, prema Tm. 3



iz 12.8., može dopuniti do ortonormirane baze

$$E = (e_1, ..., e_l, e_{l+1}, ..., e_n) \tag{1}$$

prostora U. Tvrdimo da je, za svaki $j = l+1, ..., n$, vektor $e_j \in L^{\perp}$. Neka je $a \in L$ bilo koji vektor. Onda možemo pisati

$$a = \alpha_1 e_1 + \cdots + \alpha_l e_l \,,$$

pa zbog ortogonalnosti baze E imamo

$$(a, e_j) = (\alpha_1 e_1 + \cdots + \alpha_l e_l, e_j) = \alpha_1(e_1, e_j) + \cdots + \alpha_l(e_l, e_j) = 0 \,,$$

dakle je zaista $e_j \in L^{\perp}$.

Ako je sada $x \in U$ bilo koji vektor, možemo ga u bazi (1) prikazati kao

$$x = \underbrace{\alpha_1 e_1 + \cdots + \alpha_l e_l}_{\in L} + \underbrace{\alpha_{l+1} e_{l+1} + \cdots + \alpha_n e_n}_{\in L^\perp} ,$$

dakle kao

$$x = a + a^\perp ,$$

gdje je $a \in L$, $a^\perp \in L^\perp$, što pokazuje da je

$$U \subset L + L^\perp ,$$

pa je prema tome

$$U = L + L^\perp ,$$

i dokaz je gotov. ■

KOROLAR 5

Neka je $L < U$ bilo koji potprostor. Onda je

$$(L^\perp)^\perp = L .$$

Dokaz

Inkluzija $L \subset (L^\perp)^\perp$ je očigledna. Dokažimo obratnu inkluziju. Neka je $x \in (L^\perp)^\perp \subset U$ bilo koji vektor. Prema Tm. 4 možemo ga pisati kao

$$x = a + a^\perp ,$$

gdje je $a \in L$, $a^\perp \in L^\perp$. Skalarnim množenjem s $a^\perp$ dobivamo

$$(x, a^\perp) = (a, a^\perp) + (a^\perp, a^\perp) .$$

No, $(x, a^\perp) = 0$, jer je $(L^\perp)^\perp \perp L^\perp$ po definiciji, a $(a, a^\perp) = 0$ jer je $L \perp L^\perp$. Zato je

$$(a^\perp, a^\perp) = 0 ,$$

dakle $a^\perp = \Theta$, pa je $x = a \in L$, tj.

$$(L^\perp)^\perp \subset L ,$$

što je i trebalo dokazati. ■

Primijetimo da Kor. 5 nije istinit za bilo koji skup $S \subset U$. U općem slučaju vrijedi samo

$$(S^\perp)^\perp \supset S ,$$

kako se vidi na slici iza Prop. 2.

Neka je sada $L < U$ bilo koji potprostor. Onda, zbog Tm. 4, svaki $x \in U$ ima **jednoznačan** prikaz

$$x = a + a^{\perp} ,$$

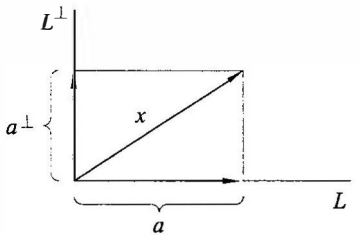
gdje je $a \in L$, $a^{\perp} \in L^{\perp}$. Zato je dobro definiran operator

$$p : U \to L$$

dan s

$$p(x) = p(a + a^{\perp}) = a ,$$

koji zovemo **ortogonalna projekcija**, ili **ortogonalni projektor**, prostora



U na potprostor L.

PROPOZICIJA 6

Ortogonalni projektor je linearni operator.

Dokaz

Dokažimo aditivnost. Neka su $x, y \in U$, $x = a + a^{\perp}$, $y = b + b^{\perp}$, gdje su $a, b \in L$, $a^{\perp}, b^{\perp} \in L^{\perp}$. Onda je

$$\begin{aligned} p(x+y) &= p[(a + a^{\perp}) + (b + b^{\perp})] = \\ &= p[\underbrace{(a+b)}_{\in L} + \underbrace{(a^{\perp} + b^{\perp})}_{\in L^{\perp}}] = a + b = p(x) + p(y) . \end{aligned}$$

Slično se vidi i homogenost. ■

Sljedeći teorem nam daje karakterizaciju ortogonalnog projektora.

TEOREM 7

Linearni operator $p : U \to U$ je ortogonalni projektor na potprostor

$$L = \{x \in U \mid p(x) = x\}$$

ako i samo ako ima ova svojstva:

(1) *idempotentnost, tj.* $p^2 = p$, *i*

(2) *hermitičnost, tj.* $(p(x), y) = (x, p(y))$.

Dokaz

Primijetimo najprije da je L zaista potprostor. Naime, iz $a, b \in L$, tj. $p(a) = a$, $p(b) = b$, zbog Prop. 6 slijedi

$$p(\alpha a + \beta b) = \alpha p(a) + \beta p(b) = \alpha a + \beta b \,,$$

pa je i $\alpha a + \beta b \in L$.

Neka je $p : U \to L$ ortogonalni projektor. Ako je $x \in U$ bilo koji vektor, možemo ga zapisati kao $x = a + a^\perp$, gdje je $a \in L$, $a^\perp \in L^\perp$, i tada je po definiciji $p(x) = a$. Zato imamo

$$p^2(x) = p[p(x)] = p(a) = a = p(x) \,,$$

za svaki $x \in U$, pa je $p^2 = p$ i (1) je provjerena. Ako je $y \in U$ drugi vektor i $y = b + b^\perp$, $b \in L$, $b^\perp \in L^\perp$ njegov prikaz, imamo

$$(p(x), y) = (a, b + b^\perp) = (a, b) + (a, b^\perp) = (a, b) \,,$$

i također,

$$(x, p(y)) = (a + a^\perp, b) = (a, b) + (a^\perp, b) = (a, b) \,,$$

pa je i (2) provjerena.

Obratno, pretpostavimo da je p linearni operator i da ima svojstva (1) i (2). Najprije, zbog (1) je očigledno da je $p : U \to L$, tj. da je slika $\mathcal{S}(p) \subset L$. Nadalje, za $x \in U$ promatrajmo rastav

$$x = p(x) + (x - p(x)) \,. \tag{3}$$

Ako uspijemo dokazati da je $p(x) \in L$, a $x - p(x) \in L^\perp$, onda smo gotovi, jer se eksplicitno vidi da je $p(x)$ jednak prvom sumandu u (3), kako definicija ortogonalne projekcije traži. Jasno je da je $p(x) \in L$. U drugu ruku, za bilo koji $a \in L$ imamo redom, uvažavajući uvjet (2),

$$\begin{aligned} (x - p(x), a) &= (x, a) - (p(x), a) = \\ &= (x, a) - (x, p(a)) = (x, a) - (x, a) = 0 \,, \end{aligned}$$

pa je zaista $x - p(x) \in L^\perp$, i dokaz je gotov. ∎

ZADACI

1. Neka su $L_1, ..., L_s < U$ potprostori od U. Suma

$$L_1 + \cdots + L_s$$

jest **ortogonalna** ako je $L_i \perp L_k$, za $i \neq k$. Pokaži da je ortogonalna suma direktna.

2. Neka je suma

$$L = L_1 + \cdots + L_s$$

ortogonalna i neka su $a, b \in L$. Ako je $a = a_1 + \cdots + a_s$, $b = b_1 + \cdots + b_s$, gdje su $a_i, b_i \in L_i$, $i = 1, ..., s$, onda je

$$(a, b) = (a_1, b_1) + \cdots + (a_s, b_s) .$$

Dokaži!

3. Neka su $L, M < U$ potprostori. Onda je

(a) $(L + M)^\perp = L^\perp \cap M^\perp$;

(b) $(L \cap M)^\perp = L^\perp + M^\perp$.

Dokaži!

4. Neka je $U = U_1 \times U_2$ direktni produkt unitarnih prostora U_1 i U_2 (vidi Zad. 5. u 12.3.). Onda su potprostori $U_1 \times \{\Theta_{U_2}\}$ i $\{\Theta_{U_1}\} \times U_2 < U$ ortogonalni. Dokaži!

5. Ako je $p : U \to L$ ortogonalni projektor, onda vrijedi

$$\|p(x)\| \leq \|x\| ,$$

za svaki $x \in U$. Nadalje, ako znak jednakosti vrijedi za svaki $x \in U$, p je jedinični operator. Dokaži!

6. Dokaži: Neka je $L < U$ potprostor, a $p : U \to L$ i $q : U \to L^\perp$ neka su ortogonalni projektori. Onda je

$$p + q = e ,$$

gdje je $e : U \to U$ jedinični operator.

13

OPERATORI NA UNITARNOM PROSTORU

Kao i uvijek, uz nove strukture definiramo specifična preslikavanja, organski vezana uz te strukture. U slučaju unitarnih prostora to su unitarni i hermitski operatori, tipični i zato, jer se pokazuje da se svaki linearni operator (koji djeluje na unitarnom prostoru) može reprezentirati pomoću tih operatora.

13.1. Unitarni operator

Neka su U i V unitarni prostori nad istim poljem F. Neka je

$$u : U \to V$$

linearni operator sa svojstvom da čuva skalarni produkt, tj. da vrijedi

$$(u(a), u(b)) = (a, b) \,, \tag{1}$$

za svaki izbor $a, b \in U$. Onda kažemo da je u **unitarni operator** iz prostora U u prostor V. Ako je F polje realnih brojeva, u se često naziva i **ortogonalni operator**.

Primijetimo da okrugle zagrade u definicijskoj relaciji (1) imaju različita značenja: one na lijevoj strani su oznaka za skalarni produkt u prostoru V, a one na desnoj strani za skalarni produkt u prostoru U.

PRIMJERI

1. Ako je $U < V$ potprostor, onda je inkluzija $i : U \to V$ unitarni operator. Specijalno, jedinični operator, identiteta, jest unitarni operator.

2. U ravnini $\mathbb{R}^2$ su

   (a) **centralna simetrija**, tj. operator

   $$(x, y) \mapsto (-x, -y) ,$$

   (b) **zrcaljenje**
   - na osi x: $(x, y) \mapsto (x, -y)$,
   - na osi y: $(x, y) \mapsto (-x, y)$,
   - na simetrali $x = y$: $(x, y) \mapsto (y, x)$,

   (c) **rotacija za dani kut** φ, tj. operator

   $$(x, y) \mapsto (x \cos\varphi - y \sin\varphi, x \sin\varphi + y \cos\varphi) ,$$

   unitarni (ortogonalni) operatori. To se lako provjeri i generalizira na prostor $\mathbb{R}^3$, odnosno $\mathbb{R}^n$.

3. Općenito, ako je U bilo koji unitarni prostor, operator $c : U \to U$, dan sa $c(a) = -a$, zovemo **centralna simetrija**. Lako se provjeri da je c unitarni operator.

4. Neka je U n-dimenzionalni kompleksni unitarni prostor, a $(e_1, \ldots, e_n)$ jedna ortonormirana baza za U. Neka je

   $$u : \mathbb{C}^n \to U$$

   operator dan s

   $$u(a) = u(\alpha_1, \ldots, \alpha_n) = \alpha_1 e_1 + \cdots + \alpha_n e_n ,$$

   za svaki $a = (\alpha_1, \ldots, \alpha_n) \in \mathbb{C}^n$. Onda je u, uz standardni skalarni produkt na $\mathbb{C}^n$, unitarni operator.

5. Za čvrsti $\lambda \in \mathbb{R}$ definiramo $u : \mathbb{C}^n \to \mathbb{C}^n$ sa $u(a) = e^{i\lambda} \cdot a$. Onda je operator u unitaran.

6. Neka je $L < U$ potprostor, a $p : U \to L$ ortogonalni projektor (vidi 12.10.). Ako je $L \neq U$, p nije unitarni operator. Zašto?

U definiciji unitarnog operatora izrekom se zahtijeva da taj operator bude linearan. Pokazuje se, međutim, da je uvjet čuvanja skalarnog produkta toliko jak da povlači linearnost, pa se taj zahtjev može u definiciji izostaviti. Imamo

TEOREM 1

Neka je $f : U \to V$ *operator sa svojstvom da je*

$$(f(a), f(b)) = (a, b) ,$$

za sve $a, b \in U$. *Onda je operator* f *nužno linearan, dakle i unitaran.*

Dokaz

Neka su $a, b \in U$ bilo koji vektori, a $\alpha, \beta \in F$ skalari. Treba vidjeti da je

$$f(\alpha a + \beta b) = \alpha f(a) + \beta f(b) . \tag{2}$$

Neka je $c \in V$ vektor definiran sa

$$c = f(\alpha a + \beta b) - \alpha f(a) - \beta f(b) . \tag{3}$$

Pokazat ćemo da je $c = \Theta_V$, čime će jednakost (2) biti verificirana.

Neka je $L = [f(U)] < V$ potprostor u V razapet slikom $f(U)$. Očito je $c \in L$. Neka je $L^{\perp} = [f(U)]^{\perp}$ ortogonalni komplement od L. Pokažimo da je također $c \in L^{\perp}$.

Neka je $y \in f(U)$ bilo koji vektor. Onda postoji $x \in U$ takav da je $f(x) = y$. Sada redom, uzimajući u obzir da f čuva skalarni produkt, imamo

$$\begin{aligned} (c, y) &= (f(\alpha a + \beta b) - \alpha f(a) - \beta f(b), f(x)) = \\ &= (f(\alpha a + \beta b), f(x)) - \alpha(f(a), f(x)) - \beta(f(b), f(x)) = \\ &= (\alpha a + \beta b, x) - \alpha(a, x) - \beta(b, x) = \\ &= \alpha(a, x) + \beta(b, x) - \alpha(a, x) - \beta(b, x) = 0 . \end{aligned}$$

Prema tome je $\{c\}$ ortogonalan na skup $f(U)$, pa onda očito i na potprostor $L = [f(U)]$, koji je njime generiran. Dakle je zaista $c \in L^{\perp}$. Kako je, međutim, $L \cap L^{\perp} = \{\Theta_V\}$ (vidi Tm. 4 u 12.10.), imamo zaključak da je $c = \Theta_V$ i tvrdnja je dokazana. ■

Navest ćemo neka osnovna svojstva unitarnog operatora.

PROPOZICIJA 2

Kompozicija unitarnih operatora je unitarni operator. Naprotiv, zbroj unitarnih operatora i produkt takvog operatora sa skalarom ne mora biti unitarni operator.

Dokaz

Neka su $u : U \to V$ i $v : V \to W$ unitarni operatori. Onda imamo

$$((u \circ v)(a), (u \circ v)(b)) = (u[v(a)], u[v(b)]) = (v(a), v(b)) = (a, b),$$

za svaki $a, b \in U$, pa kompozicija $u \circ v$ čuva skalarni produkt, odakle slijedi da je to unitarni operator po Tm. 1. ■

PROPOZICIJA 3

Unitarni operator čuva normu. Drugim riječima, ako je operator $u : U \to V$ unitaran, onda vrijedi

$$\|u(a)\| = \|a\| ,$$

za svaki $a \in U$. Posebno, dakle, unitarni operator čuva udaljenost vektora, a u slučaju realnih prostora i kut između vektora.

Dokaz

Za $a \in U$ je

$$\|u(a)\| = \sqrt{(u(a), u(a))} = \sqrt{(a, a)} = \|a\| ,$$

pa je prvi dio tvrdnje dokazan. Nadalje, za $a, b \in U$ je

$$\begin{aligned} d(u(a), u(b)) &= \|u(a) - u(b)\| = \|u(a - b)\| = \\ &= \|a - b\| = d(a, b) . \end{aligned}$$

Konačno,

$$\cos(u(a), u(b)) = \frac{(u(a), u(b))}{\|u(a)\| \cdot \|u(b)\|} = \frac{(a, b)}{\|a\| \cdot \|b\|} = \cos(a, b) ,$$

pa je $\sphericalangle(u(a), u(b)) = \sphericalangle(a, b)$. ■

Prema tome, unitarni operator čuva linearnu i angularnu metriku, pa ga zato često nazivamo i **izometrički operator** (vidi Zad. 2.).

Daljnje važno svojstvo unitarnih operatora sadrži

PROPOZICIJA 4

Unitarni operator je uvijek injektivan.

Dokaz

Neka je $u : U \to V$ unitarni operator, a $J = J(u)$ njegova jezgra. Neka je $a \in J$ bilo koji vektor. Kako je $u(a) = \Theta_V$, zbog Prop. 3 imamo

$$\|a\| = \|u(a)\| = \|\Theta_V\| = 0 ,$$

dakle je $a = \Theta_U$, tj. $J(u) = \{\Theta_U\}$, pa je u injekcija (vidi Zad. 1. u 8.5.). ■

Neka je $u : U \to V$ unitarni operator, koji je i surjektivan (dakle bijektivan, zbog Prop. 4). Onda kažemo da je u **izomorfizam unitarnih prostora**.

Za unitarne prostore U i V nad istim poljem kažemo da su **unitarno izomorfni**, i pišemo

$$U \underset{u}{\cong} V \ ,$$

ako postoji bar jedan izomorfizam unitarnih prostora s U u V. Lako se vidi da je $\underset{u}{\cong}$ relacija ekvivalencije koja, dakle, klasificira unitarne prostore nad istim poljem. Pojedine klase su karakterizirane dimenzijom prostora, jer vrijedi

TEOREM 5

Unitarni prostori U i V nad istim poljem F su unitarno izomorfni ako i samo ako imaju istu dimenziju, tj.

$$\dim U = \dim V \ .$$

Dokaz

Ako je $U \underset{u}{\cong} V$, prostori U i V su svakako izomorfni i kao linearni prostori, pa imaju istu dimenziju po Kor. 5 u 8.4. Obratno, pretpostavimo da je $\dim U = \dim V = n$, pa odaberimo ortonormirane baze $E = (e_1, \ldots, e_n)$ i $F = (f_1, \ldots, f_n)$ za prostore U i V redom. Definirajmo preslikavanje

$$u : U \to V$$

stavljajući $u(e_i) = f_i$, za svaki $i = 1, \ldots, n$, i proširujući linearno. Kako smo vidjeli (u dokazu Prop. 6 u 8.4.), u je izomorfizam linearnih prostora. Treba samo provjeriti da čuva skalarni produkt. Neka su $a, b \in U$ bilo koji vektori,

$$a = \sum_{i=1}^{n} \alpha_i e_i \quad , \quad b = \sum_{i=1}^{n} \beta_i e_i \ .$$

Onda je, dakako

$$u(a) = u(\sum_{i=1}^{n} \alpha_i e_i) = \sum_{i=1}^{n} \alpha_i u(e_i) = \sum_{i=1}^{n} \alpha_i f_i \ ,$$

i slično

$$u(b) = \sum_{i=1}^{n} \beta_i f_i \ ,$$

pa je, zbog Prop. 6 u 12.8.,

$$(u(a), u(b)) = \alpha_1\overline{\beta_1} + \cdots + \alpha_n\overline{\beta_n} = (a, b)$$

i teorem je dokazan. ∎

Prema tome, svi unitarni prostori iste dimenzije, i samo oni, imaju istu apstraktnu strukturu, i mogu se reprezentirati **standardnim modelom**, prostorom $\mathbb{C}^n$ u kompleksnom slučaju, odnosno prostorom $\mathbb{R}^n$ u realnom slučaju. Izomorfizam bilo kojeg prostora sa svojim standardnim modelom opisan je u Prim. 4.

ZADACI

1. Kako smo rekli, suma unitarnih operatora i produkt unitarnog operatora sa skalarom općenito nisu unitarni operatori. Uvjeri se u to primjerima!

2. Neka je U unitarni prostor. Svaki operator $f : U \to U$, ne nužno linearan, koji čuva udaljenosti, tj. za koji vrijedi

$$d(f(a), f(b)) = d(a, b) ,$$

za sve $a, b \in U$, nazivamo **kongruentni operator**, **izometrički operator** ili, kratko, **izometrija** prostora U. Naravno, svaki unitarni operator je jedna izometrija, ali osim njih ima i drugih izometrija. Na primjer, za čvrsti $a \in U$ je operator

$$t_a : U \to U ,$$

definiran s

$$t_a(x) = x + a ,$$

izometrija (iako nije linearni operator!). Dokaži! Taj se operator zove **translacija** za vektor a. Uvjeri se da skup $\mathcal{T}(U) = \{t_a \mid a \in U\}$ svih translacija u prostoru U čini grupu s obzirom na kompoziciju. To je tzv. **grupa translacija prostora** U.

3. Ako je s c označen operator centralne simetrije u U (vidi Prim. 3.), onda je očito i $\{e, c\}$ grupa, gdje je e jedinični operator. Pokaži da je i $\mathcal{T}(U) \cup \{e, c\}$ također grupa; to je tzv. **grupa translacija s centralnom simetrijom**.

4. Dokaži: Kompozicija izometrija prostora U je opet izometrija. Specijalno, $f = t_a \circ u$ je izometrija, za bilo koju translaciju t_a i bilo koji unitarni operator u.

5. Ako je U realni prostor, vrijedi i ovaj obrat: Neka je $f : U \to U$ bilo koja izometrija. Onda postoje ortogonalni operator u i translacija t_a takvi da je $f = t_a \circ u$, tj. da vrijedi $f(x) = u(x) + a$, za svaki $x \in U$. Dokaži!

6. Skup $I(U)$ svih izometrija prostora U čini grupu u odnosu na kompoziciju. Dokaži! To je **grupa izometrija** prostora U.

7. Neka je $p \in S_n$ bilo koja permutacija skupa $\{1, \ldots, n\}$, $p(i) = p_i$. Definiramo
$$f_p : \mathbb{R}^n \to \mathbb{R}^n$$
s
$$f_p(\alpha_1, \ldots, \alpha_n) = (\alpha_{p_1}, \ldots, \alpha_{p_n}) .$$
Pokaži da je f_p unitarni automorfizam prostora.

8. Neka je U unitarni prostor svih rješenja diferencijalne jednadžbe
$$y'' + y = 0 ,$$
uz skalarni produkt
$$(f, g) = \int_0^{2\pi} f(t)g(t)\, dt .$$
Za svaki $a \in \mathbb{R}$ definiramo preslikavanje
$$u_a : U \to U ,$$
stavljajući
$$u_a(f) = f(t - a) ,$$
za $f \in U$. Pokaži da je u_a unitarni operator, čak i automorfizam prostora U. Operator u_a zovemo **operator translacije** za a.

9. Operator $f : U \to U$ je **antilinearan** ako je aditivan i vrijedi
$$f(\alpha a) = \overline{\alpha} f(a) ,$$
za svaki $a \in U$, $\alpha \in F$. Operator $u : U \to U$ je **antiunitaran** ako je
$$(u(a), u(b)) = (b, a) ,$$
za sve $a, b \in U$. Dokaži da je antiunitaran operator u antilinearan.

13.2. Karakterizacije unitarnog operatora

Navest ćemo nekoliko nužnih i dovoljnih uvjeta za prepoznavanje unitarnih operatora. Svaki od njih može poslužiti kao (alternativna) definicija unitarnog operatora.

TEOREM 1

Linearni operator $f : U \to V$ je unitaran ako i samo ako čuva normu.

Dokaz

Nužnost smo dokazali u Prop. 3 u 13.1. Dokažimo dovoljnost. Po pretpostavci je $\|f(x)\| = \|x\|$, za svaki $x \in U$. Treba pokazati da za bilo koje $a, b \in U$ vrijedi $(f(a), f(b)) = (a, b)$.

Za vektor $a + \lambda b$ imamo

$$\|f(a + \lambda b)\| = \|a + \lambda b\| ,$$

dakle kvadriranjem,

$$(f(a + \lambda b), f(a + \lambda b)) = (a + \lambda b, a + \lambda b) ,$$

odnosno, zbog linearnosti od f,

$$(f(a) + \lambda f(b), f(a) + \lambda f(b)) = (a + \lambda b, a + \lambda b) ,$$

i odatle množenjem

$$\begin{aligned} (f(a), f(a)) \quad &+ \quad \lambda(f(b), f(a)) + \overline{\lambda}(f(a), f(b)) + \lambda\overline{\lambda}(f(b), f(b)) = \\ &= \quad (a, a) + \lambda(b, a) + \overline{\lambda}(a, b) + \lambda\overline{\lambda}(b, b) . \end{aligned}$$

Budući da f čuva normu, ta se relacija reducira na

$$\overline{\lambda}(f(a), f(b)) + \lambda\overline{(f(a), f(b))} = \overline{\lambda}(a, b) + \lambda\overline{(a, b)} . \tag{1}$$

Za $\lambda = 1$ iz (1) slijedi

$$(f(a), f(b)) + \overline{(f(a), f(b))} = (a, b) + \overline{(a, b)} ,$$

dakle

$$\mathrm{Re}[(f(a), f(b))] = \mathrm{Re}[(a, b)] , \tag{2}$$

gdje je s Re z označen realni dio kompleksnog broja z. U drugu ruku, ako uzmemo $\lambda = i$, iz (1) imamo

$$-i(f(a), f(b)) + i\overline{(f(a), f(b))} = -i(a, b) + i\overline{(a, b)} ,$$

odnosno

$$(f(a), f(b)) - \overline{(f(a), f(b))} = (a, b) - \overline{(a, b)} \,,$$

odakle slijedi da je

$$\mathrm{Im}[(f(a), f(b))] = \mathrm{Im}[(a, b)] \,, \tag{3}$$

gdje Im z označava imaginarni dio kompleksnog broja z. Iz (2) i (3) zaključujemo da je

$$(f(a), f(b)) = (a, b) \,,$$

i tvrdnja je dokazana. ■

TEOREM 2

Linearni operator $f : U \to V$ je unitaran ako i samo ako svaki jedinični vektor iz U preslikava u jedinični vektor iz V.

Dokaz

Nužnost je očigledna: Ako je f unitaran, prema Tm. 1 čuva normu, pa prema tome jedinični vektor prevodi u jedinični. Dokažimo dovoljnost. Neka je $a \in U$ bilo koji vektor. Ako je $a = \Theta_U$, imamo i $f(a) = \Theta_V$, pa je $\|f(a)\| = 0 = \|a\|$. Ako je $a \neq \Theta_U$, možemo pisati $a = \|a\| a_0$, gdje je očito a_0 jedinični vektor, $\|a_0\| = 1$. No, po pretpostavci je onda $\|f(a_0)\| = 1$, pa imamo redom

$$\|f(a)\| = \|f(\|a\| a_0)\| = \| \, \|a\| f(a_0)\| = \|a\| \, \|f(a_0)\| = \|a\| \,.$$

Operator f, dakle, čuva normu, pa je unitaran po Tm. 1. ■

TEOREM 3

Linearni operator $f : U \to V$ je unitaran ako i samo ako bar jednu ortonormiranu bazu prostora U preslikava u ortonormirani skup vektora iz prostora V.

Dokaz

Nužnost je trivijalna: Unitarni operator svaki ortonormirani skup vektora preslikava u ortonormirani skup (jer čuva skalarni produkt). Dokažimo dovoljnost. Neka je $E = (e_1, \ldots, e_n)$ ortonormirana baza za U, sa svojstvom da je

$$(f(e_1), \ldots, f(e_n))$$

ortonormirani skup u V. To znači da vrijedi

$$(f(e_i), f(e_k)) = \delta_{ik} = (e_i, e_k) \,.$$

Neka su $a, b \in U$ bilo koji vektori,

$$a = \sum_{i=1}^{n} \alpha_i e_i, \qquad b = \sum_{k=1}^{n} \beta_k e_k \, .$$

Onda redom imamo (koristeći se Prop. 6 iz 12.8.)

$$\begin{aligned}
(f(a), f(b)) &= (f(\sum_i \alpha_i e_i), f(\sum_k \beta_k e_k)) = \\
&= (\sum_i \alpha_i f(e_i), \sum_k \beta_k f(e_k)) = \\
&= \sum_i \sum_k \alpha_i \overline{\beta_k} (f(e_i), f(e_k)) = \\
&= \sum_i \sum_k \alpha_i \overline{\beta_k} \delta_{ik} = \sum_i \alpha_i \overline{\beta_i} = (a, b) \, ,
\end{aligned}$$

pa zaključujemo da je f unitaran. ■

Iz Tm. 3 razabiremo da je rang unitarnog operatora jednak dimenziji polaznog prostora U, pa je zbog toga njegova jezgra trivijalna ($\dim U = r + d$), tj. unitarni operator je injektivan, kako smo već dokazali. Ako je specijalno $\dim V = \dim U$, unitarni operator je nužno bijektivan, dakle izomorfizam unitarnih prostora.

ZADACI

1. Dokaži: Neka je $E = (e_1, \ldots, e_n) \subset U$ ortonormirana baza za U, a $(f_1, \ldots, f_n) \subset V$ bilo koji ortonormirani skup. Onda postoji jedan i samo jedan unitarni operator $u : U \to V$ tako da je $u(e_i) = f_i$, za svaki $i = 1, \ldots, n$.

2. Dokaži da vrijedi i općenitije: Neka su $\{a_1, \ldots, a_k\} \subset U$ i $\{b_1, \ldots, b_k\} \subset V$ skupovi vektora sa svojstvom da je $(a_i, a_j) = (b_i, b_j)$, za sve $i, j = 1, \ldots, k$. Onda postoji bar jedan unitarni operator $u : U \to V$ sa svojstvom da je $u(a_i) = b_i$, za svaki $i = 1, \ldots, k$. [Uputa: Odaberi linearno nezavisne vektore među vektorima a_i, pokaži da su korespondentni vektori b_i također linearno nezavisni, ortonormiraj svaki od tih skupova, dopuni do baze i primijeni Zad. 1.]

3. Nađi unitarni operator u prostoru V^3, koji prevodi:

   (a) $(\vec{i}, \vec{j}, \vec{k})$ na $(\vec{i}, \vec{j}, -\vec{k})$;

   (b) $\vec{i}$ u $1/3(2\vec{i} + 2\vec{j} + \vec{k})$.

   Ovaj posljednji, dakako, nije određen jednoznačno.

13.3. Matrica unitarnog operatora. Unitarna grupa

Usmjerimo sada pažnju na unitarne operatore koji preslikavaju (konačnodimenzionalni) unitarni prostor u **samog sebe**. Kako smo već primijetili, svaki takav operator je nužno surjektivan, dakle i bijektivan, tj. automorfizam unitarnog prostora. Drugim riječima, unitarni operatori s danog prostora u sebe su uvijek **regularni**.

PROPOZICIJA 1

Neka je $u : U \to U$ unitarni operator. Onda je i u^{-1} unitarni operator.

Dokaz

Kako je u regularan, u^{-1} uvijek postoji i to je linearni operator. Treba još vidjeti da čuva skalarni produkt. Neka su $a, b \in U$ bilo koji vektori. Onda imamo redom

$$(u^{-1}(a), u^{-1}(b)) = (u[u^{-1}(a)], u[u^{-1}(b)]) = (a, b)$$

i tvrdnja je dokazana. ■

Neka je s

$$\mathcal{U}(U) = \{u : U \to U \mid u \text{ je unitaran}\}$$

označen skup svih unitarnih operatora koji djeluju na prostoru U. Tada imamo

TEOREM 2

$\mathcal{U}(U)$ je grupa u odnosu na kompoziciju kao binarnu operaciju.

Dokaz

Neposredno iz Prop. 1 i činjenice da je jedinični operator unitaran, te da je kompozicija unitarnih operatora opet unitarni operator. ■

Grupu $\mathcal{U}(U)$ zovemo **grupa unitarnih operatora** prostora U. Ako je U realni unitarni prostor, tu grupu obično označavamo s $\mathcal{O}(U)$ i zovemo je **grupa ortogonalnih operatora**.

Kažimo nešto o matričnom zapisu unitarnog operatora. Kako smo već rekli (vidi Zad. 8. i 9. u 9.5.), kompleksna kvadratna matrica A je **unitarna** ako za nju vrijedi

$$AA^* = A^*A = E\,, \tag{1}$$

gdje $A^* = \overline{A}'$ označava hermitski konjugiranu (adjungiranu) matricu od A. Unitarna matrica je očito regularna i karakterizirana uvjetom $A^{-1} = A^*$.

Nadalje, primjenom Binet-Cauchyjeva teorema na definicijsku relaciju (1), odmah dobivamo da je

$$|\det A| = 1 .$$

Obrat ne vrijedi: Kompleksna matrica čija je determinanta po modulu jednaka 1 ne mora biti unitarna.

O strukturi unitarne matrice govori ova

PROPOZICIJA 3

Neka je $A = [\alpha_{ik}]$ *unitarna matrica reda* n. *Onda vrijedi:*

(1) $\sum_{j=1}^{n} \alpha_{ij}\overline{\alpha_{kj}} = \delta_{ik}$;

(2) $\sum_{j=1}^{n} \alpha_{ji}\overline{\alpha_{jk}} = \delta_{ik}$,

za sve $i, k = 1, \ldots, n$. *Obratno, ako je za matricu* A *ispunjen bilo koji od uvjeta* (1) *ili* (2), *ta je matrica unitarna.*

Dokaz

Neposredno iz definicije unitarne matrice. Naime, iz $AA^* = E$, zbog $E = [\delta_{ik}]$, imamo

$$\delta_{ik} = \sum_{j=1}^{n} \alpha_{ij}\beta_{jk} = \sum_{j=1}^{n} \alpha_{ij}\overline{\alpha_{kj}} ,$$

pa je (1) provjereno. Slično, iz $A^*A = E$ slijedi (2).

Obratno, pretpostavimo da za elemente matrice A vrijedi npr.

$$\sum_{j=1}^{n} \alpha_{ij}\overline{\alpha_{kj}} = \delta_{ik} ,$$

za sve $i, k = 1, \ldots, n$. To vodi na jednakost matrica

$$\left[\sum_{j=1}^{n} \alpha_{ij}\overline{\alpha_{kj}}\right] = [\delta_{ik}] \quad ,$$

što možemo pisati kao $AA^* = E$. Odatle je nužno i $A^*A = E$, pa zaključujemo da je matrica A unitarna. ■

Uvjetima (1) i (2) zapisanim u Prop. 3 iskazana je tzv. **hermitska ortonormiranost** redaka, odnosno stupaca matrice. Svaki od tih uvjeta karakterizira unitarnu matricu.

Neka je $U(n)$ skup svih unitarnih matrica reda n. Onda vrijedi

TEOREM 4

$U(n)$ je grupa u odnosu na množenje matrica.

Dokaz

Neka su $A, B \in U(n)$ bilo koje matrice, $A^{-1} = A^*$, $B^{-1} = B^*$. Onda imamo

$$(AB)^{-1} = B^{-1}A^{-1} = B^*A^* = (AB)^*$$

pa je $AB \in U(n)$. Slično,

$$(A^{-1})^{-1} = A = (A^*)^* = (A^{-1})^* ,$$

pa je i $A^{-1} \in U(n)$, pa je $U(n)$ zaista grupa, podgrupa opće linearne grupe $GL(n, \mathbb{C})$. ■

Grupu $U(n)$ nazivamo **unitarna grupa** (matrica reda n). Ako je matrica A realna, definicijska relacija (1) postaje

$$AA' = A'A = E ,$$

a matricu s tim svojstvom zvali smo **ortogonalna matrica**. Analogne tvrdnje o ortonormiranosti redaka i stupaca te o grupovnosti za ortogonalne matrice već smo dokazali (vidi Tm. 2, Prop. 3 i Prop. 4 u 9.5.), kada smo grupu svih ortogonalnih matrica reda n označili s $O(n)$ i nazvali **ortogonalna grupa**.

Vratimo se pitanju matrične reprezentacije unitarnog operatora. Vrijedi

PROPOZICIJA 5

Neka je $u : U \to U$ unitarni operator, a $E = (e_1, \ldots, e_n)$ bilo koja ortonormirana baza prostora U. Onda je matrični zapis operatora u u toj bazi unitarna matrica.

Dokaz

Neka je $A = [\alpha_{ik}]$ matrični zapis od u. Po definiciji to znači da je

$$u(e_i) = \sum_{j=1}^{n} \alpha_{ji} e_j ,$$

za svaki $i = 1, \ldots, n$. Kako je operator u unitaran, skup

$$\{u(e_1), \ldots, u(e_n)\}$$

je također ortonormiran, pa imamo

$$\delta_{ik} = (u(e_i), u(e_k)) = (\sum_{j=1}^{n} \alpha_{ji} e_j, \sum_{l=1}^{n} \alpha_{lk} e_l) =$$
$$= \sum_{j=1}^{n}\sum_{l=1}^{n} \alpha_{ji}\overline{\alpha_{lk}}(e_j, e_l) = \sum_{j=1}^{n}\sum_{l=1}^{n} \alpha_{ji}\overline{\alpha_{lk}}\delta_{jl} = \sum_{j=1}^{n} \alpha_{ji}\overline{\alpha_{jk}} \ ,$$

za svaki $i, k = 1, \ldots, n$ odakle, prema Prop. 3, zaključujemo da je matrica A unitarna. ■

Vrijedi međutim i obratno:

PROPOZICIJA 6

Neka je matrični zapis linearnog operatora $f : U \to U$ u nekoj ortonormiranoj bazi $E = (e_1, \ldots, e_n)$ unitarna matrica. Onda je operator f unitaran.

Dokaz

Neka je matrica $A = [\alpha_{ik}]$ operatora f u bazi E unitarna. Onda je, zbog Prop. 3,

$$(f(e_i), f(e_k)) = (\sum_{j=1}^{n} \alpha_{ji} e_j \ , \sum_{l=1}^{n} \alpha_{lk} e_l) =$$
$$= \sum_{j=1}^{n}\sum_{l=1}^{n} \alpha_{ji}\overline{\alpha_{lk}}(e_j, e_l) = \sum_{j=1}^{n} \alpha_{ji}\overline{\alpha_{jk}} = \delta_{ik} \ ,$$

za svaki $i, k = 1, \ldots, n$, pa tvrdnja izlazi iz Tm. 3 u 13.2. ■

Naravno, ako je linearni operator f reprezentiran u **nekoj** ortonormiranoj bazi unitarnom matricom, onda je on u **svakoj** ortonormiranoj bazi predočen takvom matricom. Zaista, veza matričnih zapisa u raznim bazama dana je relacijom

$$B = T^{-1}AT \ .$$

Pritom je matrica T prijelaza iz jednog ortonormiranog sustava u drugi unitarna (Zad. 1 u 12.8.), pa je B unitarna matrica, kao produkt unitarnih matrica (Tm. 4).

Imamo, dakle, još jednu karakterizaciju unitarnog operatora

TEOREM 7

Linearni operator $f : U \to U$ je unitaran ako i samo ako je u svakoj ortonormiranoj bazi prostora U reprezentiran unitarnom matricom. ■

Odatle i naziv za unitarne matrice. Naravno, ako je prostor U realan, ortogonalni operatori u tom prostoru bit će karakterizirani time da su im matrice u ortonormiranim bazama ortogonalne.

Sada je lako dokazati

TEOREM 8

Neka je U n-dimenzionalni unitarni prostor. Onda je grupa $\mathcal{U}(U)$ unitarnih operatora prostora U izomorfna s unitarnom grupom $U(n)$.

Dokaz

Neka je E ortonormirana baza za U. Kao u 10.4., promatramo operator

$$\Phi : \operatorname{Hom} U \to M_n ,$$

definiran s $\Phi(f) = A$, gdje je A matrica operatora f u bazi E. Prema Tm. 2 iz 10.4., Φ je izomorfizam algebri. Odatle, zbog Tm. 7 odmah slijedi da je restrikcija

$$\Psi = \Phi/_{\mathcal{U}(U)} : \mathcal{U}(U) \to U(n)$$

traženi izomorfizam grupa $\mathcal{U}(U)$ i $U(n)$. ■

Zato se i grupa unitarnih operatora (koju možemo reprezentirati s $\mathcal{U}(\mathbb{C}^n)$) obično naziva **unitarna grupa**.

Analogno, grupa $\mathcal{O}(U)$ je izomorfna s $O(n)$ i zovemo je **ortogonalna grupa**.

Navedimo još neka tipična svojstva unitarnih operatora.

PROPOZICIJA 9

Svojstvene vrijednosti unitarnog operatora su po modulu jednake 1. *Posebno, svojstvene vrijednosti ortogonalnog operatora su* ± 1.

Dokaz

Neka je u unitarni operator, a λ njegova svojstvena vrijednost. Tada postoji vektor $a \in U$, $a \neq \Theta$, takav da je $u(a) = \lambda a$. Za njega je

$$||a|| = ||u(a)|| = ||\lambda a|| = |\lambda| \cdot ||a||$$

i prema tome $|\lambda| = 1$. ■

PROPOZICIJA 10

Svojstveni vektori unitarnog operatora koji odgovaraju različitim svojstvenim vrijednostima međusobno su ortogonalni.

Dokaz

Neka su λ i μ međusobno različite svojstvene vrijednosti operatora u, te $a, b \in U$, $a, b \neq \Theta$ redom pripadni svojstveni vektori. Iz $u(a) = \lambda a$, $u(b) = \mu b$ slijedi

$$(a, b) = (u(a), u(b)) = (\lambda a, \mu b) = \lambda\overline{\mu}(a, b) .$$

Kad bi bilo $(a, b) \neq 0$, imali bismo $\lambda\overline{\mu} = 1$, dakle $\lambda(\overline{\mu}\mu) = \lambda|\mu|^2 = \mu$, odnosno, zbog Prop. 9,

$$\lambda = \mu \ ,$$

protivno pretpostavci. ■

Spomenimo još i ovo. Kako je polje kompleksnih brojeva algebarski zatvoreno, operator koji djeluje na kompleksnom unitarnom prostoru U uvijek će imati n svojstvenih vrijednosti, gdje je $n = \dim U$. Vrijedi nadalje

TEOREM 11

Neka je U kompleksni unitarni prostor, a $u : U \to U$ bilo koji unitarni operator. Onda u dopušta dijagonalizaciju. Točnije, postoji ortonormirana baza za U koja se sastoji od svojstvenih vektora operatora u, i u njoj u ima zapis

$$A = \begin{bmatrix} \lambda_1 & & 0 \\ & \ddots & \\ 0 & & \lambda_n \end{bmatrix} ,$$

gdje su λ_i, $i = 1, \ldots, n$, svojstvene vrijednosti od u.

Dokaz

Indukcijom po $n = \dim U$. Neka je λ_1 svojstvena vrijednost od u, a e_1 jedinični svojstveni vektor pridružen toj svojstvenoj vrijednosti, $u(e_1) = \lambda_1 e_1$. Onda je $L = [e_1]$ u-invarijantan potprostor od U (vidi 10.8.). Neka je $M = L^{\perp}$. Taj potprostor od U je također u-invarijantan, jer za $a \in M$ imamo $\{a\} \perp L$ i odatle, jer je operator u unitaran, $\{u(a)\} \perp u(L)$, pa je zbog $u(L) = L$ zaista $u(a) \in M$. Operator $u/_M : M \to M$ opet je unitaran. Kako je očito $\dim M = n - 1$, po pretpostavci indukcije postoji ortonormirana baza $(e_2, \ldots, e_n)$ za M koja se sastoji od svojstvenih vektora operatora $u/_M$. Onda je $(e_1, e_2, \ldots, e_n)$ ortonormirana baza za U, sastavljena od svojstvenih vektora operatora u, pa tvrdnja slijedi iz Tm. 1 i Kor. 2 u 10.10. ■

Ako je U prostor nad poljem realnih brojeva, nastupaju (poznate) teškoće. Unitarni (ortogonalni) operator, koji djeluje na takvom prostoru, ne mora se dati dijagonalizirati, ali se može dokazati da vrijedi

TEOREM 12

Neka je U realni unitarni prostor, a $u : U \to U$ ortogonalni operator. Onda postoji ortonormirana baza za U u kojoj u za matrični zapis ima dijagonalnu blok matricu

$$A = \begin{bmatrix} R_1 & & & & & & & O \\ & \ddots & & & & & & \\ & & R_{s_1} & & & & & \\ & & & 1 & & & & \\ & & & & \ddots & & & \\ & & & & & 1 & & \\ & & & & & & -1 & \\ & & & & & & & \ddots \\ O & & & & & & & -1 \end{bmatrix},$$

gdje su s R_i označeni blokovi oblika

$$R_i = \begin{bmatrix} \cos\varphi_i & -\sin\varphi_i \\ \sin\varphi_i & \cos\varphi_i \end{bmatrix},$$

za neki $0 \leq \varphi_i < 2\pi$. ■

To je najjednostavnija matrična reprezentacija ortogonalnog operatora, koja se općenito može postići. Primijetimo da se po dvije vrijednosti -1 na dijagonali od A mogu kombinirati u jedan blok R, s $\varphi = \pi$. Prema tome, možemo uvijek pretpostaviti da u A ili nema -1, ili se -1 pojavljuje točno jedanput. U prvom je slučaju $\det u = 1$ (vidi Zad. 2. u 10.8.) i u zovemo **specijalni ortogonalni operator** ili **rotacija**. U drugom slučaju je $\det u = -1$, i u se obično naziva **zrcaljenje** (**refleksija**). Razlog je očigledan. Naime, sa svakim R_i je opisana rotacija u ravnini za kut φ_i, pa se u slučaju $\det u = 1$ djelovanje operatora u može shvatiti kao niz uzastopnih rotacija u međusobno okomitim dvodimenzionalnim potprostorima od U (kombinirano s identitetom u preostalim smjerovima). Ako je pak $\det u = -1$, A možemo faktorizirati kao

$$A = A_1 A_2 ,$$

gdje je A_2 dobivena iz A zamjenom (jedinog) -1 u A s 1, a A_1 je matrica oblika

$$A_1 = \begin{bmatrix} 1 & & & 0 \\ & \ddots & & \\ & & 1 & \\ 0 & & & -1 \end{bmatrix} .$$

To znači da se djelovanje od u može shvatiti kao kompozicija rotacija i jednog zrcaljenja na $(n-1)$-dimenzionalnom potprostoru od U, tj. transformacije opisane u danoj bazi s

$$(\alpha_1, \ldots, \alpha_{n-1}, \alpha_n) \mapsto (\alpha_1, \ldots, \alpha_{n-1}, -\alpha_n) .$$

Matricu A u Tm. 11 (odnosno u Tm. 12) obično nazivamo **normalna forma** matrične reprezentacije unitarnog (ortogonalnog) operatora.

ZADACI

1. Pokaži da je, uz $\varphi \neq 0, \pi$,

$$A = \begin{bmatrix} \cos\varphi & -\sin\varphi \\ \sin\varphi & \cos\varphi \end{bmatrix}$$

matrični zapis ortogonalnog operatora $u : \mathbb{R}^2 \to \mathbb{R}^2$ koji ne dopušta dijagonalizaciju.

2. Dokaži Tm. 12. Uvjeri se da se 1, odnosno -1, pojavljuju u A točno toliko puta, kolika je njihova algebarska kratnost kao svojstvenih vrijednosti od u, dok su $\varphi_1, \ldots, \varphi_s$ takvi da $\cos\varphi_j \pm i\sin\varphi_j$, $j = 1, \ldots, s$, predstavljaju nule karakterističnog polinoma od u, različite od ± 1, i svaki se blok R_j u A ponavlja toliko puta, kolika je kratnost korijena $\cos\varphi_j + i\sin\varphi_j$.

3. Pokaži da je u realnom unitarnom prostoru $\mathbb{R}^3$ za svaki ortogonalni operator moguće naći ortonormiranu bazu (e_1, e_2, e_3) u kojoj taj operator ima jedan od sljedećih zapisa:

(a) $\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$, (b) $\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{bmatrix}$,

(c) $\begin{bmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{bmatrix}$, (d) $\begin{bmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{bmatrix}$,

(e) $\begin{bmatrix} \cos\varphi & -\sin\varphi & 0 \\ \sin\varphi & \cos\varphi & 0 \\ 0 & 0 & 1 \end{bmatrix}$, (f) $\begin{bmatrix} \cos\varphi & -\sin\varphi & 0 \\ \sin\varphi & \cos\varphi & 0 \\ 0 & 0 & -1 \end{bmatrix}$.

Geometrijski, (a) predstavlja jedinični operator, (b) zrcaljenje na ravnini $[e_1, e_2]$, (c) zrcaljenje na pravcu $[e_1]$, (d) centralnu simetriju, (e) rotaciju oko pravca $[e_3]$ za kut φ i (f) rotaciju oko pravca $[e_3]$ komponiranu sa zrcaljenjem na ravnini $[e_1, e_2]$. Prva četiri slučaja mogu se shvatiti kao specijalni slučajevi posljednja dva, za $\varphi = 0$ i $\varphi = \pi$.

4. Kako smo rekli (Zad. 20. u 9.5.), kompleksna kvadratna matrica A je **unitarno slična** (**kongruentna**) matrici B, ako postoji unitarna matrica T, tako da vrijedi $B = T^{-1}AT$. Pritom pišemo $A \underset{u}{\cong} B$, a radi se, dakako, o relaciji ekvivalencije. Analogno se definira (vidi Zad. 18. u 9.5.) **ortogonalna sličnost** za realne matrice. Pokaži da su unitarne (ortogonalne) matrice unitarno (ortogonalno) slične, ako i samo ako imaju isti karakteristični polinom.

5. Dokaži: Svaka je unitarna matrica unitarno slična dijagonalnoj matrici. Svaka je ortogonalna matrica ortogonalno slična svojoj normalnoj formi (vidi Tm. 12).

6. Neka su $f, g : U \to U$ linearni operatori. Kažemo da je operator f **unitarno sličan** s g, ako postoji unitarni operator u na U koji prevodi f u g, tj. takav da iz $f(a) = b$ slijedi $g[u(a)] = u(b)$, za svaki $a \in U$. Pokaži da je ta sličnost relacija ekvivalencije. Pokaži, nadalje, da su dva operatora f i g unitarno slična ako i samo ako je

$$g = u^{-1} \circ f \circ u \,,$$

tj. ako i samo ako su njihove matrice s obzirom na istu ortonormiranu bazu unitarno slične.

7. Linearni operatori f i g su unitarno slični ako i samo ako postoje dvije ortonormirane baze sa svojstvom da se matrica od f u jednoj od tih baza podudara s matricom od g u drugoj bazi. Dokaži!

8. Dokaži: A i B su matrični zapisi istog linearnog operatora u različitim ortogonalnim bazama ako i samo ako su A i B unitarno slične matrice.

9. Nađi centar unitarne grupe $U(n)$, posebno grupe $\mathcal{U}(\mathbb{C}^n)$, pa geometrijski interpretiraj rezultat.

10. Dokaži da skup

$$SU(n) = \{A \in U(n) \mid \det A = 1\}$$

tvori multiplikativnu grupu, koju zovemo **specijalna unitarna grupa**. Na primjer, je

$$\begin{bmatrix} \mathrm{e}^{it} & 0 \\ 0 & \mathrm{e}^{-it} \end{bmatrix} \in SU(2) ,$$

za svaki $t \in \mathbb{R}$. Analogno, prije smo definirali (Zad. 4. u 9.10.) **specijalnu ortogonalnu grupu** $SO(n) < O(n)$ i ona je bila podgrupa indeksa 2 u $O(n)$. Vrijedi li isto za $SU(n) \subset U(n)$?

11. Neka je $u : \mathbb{R}^3 \to \mathbb{R}^3$ specijalni ortogonalni operator, $\det u = 1$. Pokaži da u mora imati jednu svojstvenu vrijednost $\lambda = 1$. Zaključi odatle da u ima cijeli **pravac fiksnih točaka** (tj. takvih $a \in \mathbb{R}^3$ za koje je $u(a) = a$). Generaliziraj!

12. Pokaži da se **grupa** $I(\mathbb{R}^3)$ svih **izometrija prostora** $\mathbb{R}^3$ (zvana također i **euklidska grupa**) može dekomponirati u direktni produkt svojih podgrupa $\mathcal{T}(\mathbb{R}^3)$ i $\mathcal{O}(\mathbb{R}^3)$ (vidi Zad. 6. u 3.9.),

$$I(\mathbb{R}^3) = \mathcal{T}(\mathbb{R}^3) \otimes \mathcal{O}(\mathbb{R}^3) ,$$

gdje je $\mathcal{T}(\mathbb{R}^3)$ grupa translacija prostora $\mathbb{R}^3$ (Zad. 2. u 13.1.). Kako dalje dekomponirati ortogonalnu grupu $\mathcal{O}(\mathbb{R}^3)$? Imaj na umu rotacije i zrcaljenja!

13. Općenito, neka je U bilo koji **realni** unitarni prostor. Onda se grupa

$$\mathcal{G}(U) = \mathcal{T}(U) \otimes \mathcal{O}(U)$$

naziva **grupa gibanja** za U, i ona je izomorfna s grupom $I(U)$ svih izometrija prostora U (Zad. 6. u 13.1.). Dokaži!

14. Neka su $A = \{a_1, \ldots, a_k\}$ i $B = \{b_1, \ldots, b_k\}$ dva sustava vektora iz U. Da bi postojao unitarni operator $u : U \to U$ sa svojstvom $u(a_i) = b_i$, za svaki $i = 1, \ldots, k$, nužno je i dovoljno da bude

$$G(A) = G(B) ,$$

gdje je s G označena Gramova matrica. Dokaži!

13.4. Adjungirani operator

Posredovanjem strukture unitarnog prostora, svakom se linearnom operatoru, koji djeluje na tom prostoru, može prirodno pridružiti, adjungirati, jedan novi linearni operator.

Dokažimo najprije da vrijedi ova korisna

LEMA 1

Neka su $f, g : U \to U$ linearni operatori sa svojstvom da je

(1) $(f(a), b) = (g(a), b)$, *ili*

(2) $(a, f(b)) = (a, g(b))$,

za svaki izbor $a, b \in U$. Onda je $f = g$.

Dokaz

Dokažimo npr. (1). Iz pretpostavke imamo

$$(f(a), b) - (g(a), b) = (f(a) - g(a), b) = ((f - g)(a), b) = 0 ,$$

za sve $a, b \in U$. No, iz te relacije čitamo da je

$$f(a) - g(a) \perp b ,$$

za svaki $b \in U$, pa je nužno $f(a) - g(a) = \Theta$, dakle $f(a) = g(a)$, i to za svaki $a \in U$. Odatle slijedi da je $f = g$. ■

Za linearni operator $f : U \to U$ definiramo operator $g : U \to U$ zahtijevajući

$$(g(a), b) = (a, f(b)) , \tag{1}$$

za sve $a, b \in U$. Definicijski uvjet (1) možemo, dakako, pisati i kao

$$(g(b), a) = (b, f(a)) ,$$

odakle odmah slijedi i

$$(a, g(b)) = (f(a), b)) , \tag{2}$$

za svaki izbor $a, b \in U$, što pokazuje da smo g mogli alternativno definirati i relacijom (2).

PROPOZICIJA 2

Ako operator g postoji, on je linearan.

Dokaz

Iz (1) imamo redom

$$\begin{aligned}(g(\alpha_1 a_1 + \alpha_2 a_2), b) &= (\alpha_1 a_1 + \alpha_2 a_2, f(b)) = \alpha_1(a_1, f(b)) + \alpha_2(a_2, f(b)) = \\ &= \alpha_1(g(a_1), b) + \alpha_2(g(a_2), b) = (\alpha_1 g(a_1) + \alpha_2 g(a_2), b).\end{aligned}$$

Kako je to istina za svaki $b \in U$, imamo (kao u dokazu Leme 1)

$$g(\alpha_1 a_1 + \alpha_2 a_2) = \alpha_1 g(a_1) + \alpha_2 g(a_2) ,$$

tj. operator g je linearan. ■

PROPOZICIJA 3

Za svaki linearni operator $f : U \to U$ uvijek postoji i jednoznačno je određen operator $g : U \to U$ sa svojstvom (1).

Dokaz

Egzistenciju operatora g elegantno ćemo dokazati u 13.8. (Kor. 3), pomoću linearnih funkcionala (vidi i Zad. 2.). Dokažimo jedinstvenost. Neka su $g, g' : U \to U$ linearni operatori, takvi da vrijedi

$$(g(a), b) = (a, f(b)) \quad \text{i} \quad (g'(a), b) = (a, f(b)) ,$$

za sve $a, b \in U$. Onda imamo

$$(g(a), b) = (g'(a), b) ,$$

pa je $g' = g$, zbog Leme 1. ■

Jedinstveni linearni operator g pridružen operatoru f na opisani način, nazivamo **hermitski konjugiranim**, **hermitski adjungiranim** ili, kratko, **adjungiranim operatorom** od f i označavamo ga standardno s

$$g = f^* .$$

Ako je U realni prostor, f^* se često naziva i **transponirani** operator od f, iz razloga koji ćemo uskoro vidjeti.

Svojstva adjungiranog operatora popisana su u sljedećem teoremu:

TEOREM 4

Neka su $f, g : U \to U$ bilo koji linearni operatori. Onda je:

(1) $f^* = g^*$ *ako i samo ako je* $f = g$;

(2) $(f^*)^* = f$;

(3) $(f+g)^* = f^* + g^*$;

(4) $(\alpha f)^* = \overline{\alpha} f^*$;

(5) $(f \circ g)^* = g^* \circ f^*$.

Dokaz

Neposredno iz definicije i Leme 1. Imamo npr.

$$((f^*)^*(a), b) = (a, f^*(b)) = (f(a), b) ,$$

za svaki $a, b \in U$, odakle zbog Leme 1 slijedi da je $(f^*)^* = f$ i (2) je verificirano. Posve analogno dokazujemo (5):

$$\begin{aligned}((f \circ g)^*(a), b) &= (a, (f \circ g)(b)) = (a, f[g(b)]) = \\ &= (f^*(a), g(b)) = (g^*[f^*(a)], b) = ((g^* \circ f^*)(a), b),\end{aligned}$$

pa je zaista $(f \circ g)^* = g^* \circ f^*$. Slično se dokazuju i ostale tvrdnje. ■

KOROLAR 5

Operacija adjungiranja operatora je simetrična, tj. $f^* = g$ ako i samo ako je $g^* = f$.

Dokaz

Iz Tm. 4 vidimo da $f^* = g$ povlači $g^* = (f^*)^* = f$. ■

Zato govorimo o **paru** uzajamno **adjungiranih operatora**.

Sada postavljamo pitanje u kakvom su odnosu matrice međusobno adjungiranih operatora s obzirom na istu bazu. Neka je $E = (e_1, \ldots, e_n)$ **ortonormirana baza** za prostor U, a $A = [\alpha_{ik}]$ i $B = [\beta_{ik}]$ matrični zapisi operatora f i njemu adjungiranog operatora f^* u toj bazi. Onda je

$$f(e_k) = \sum_{j=1}^{n} \alpha_{jk} e_j \qquad \text{i} \qquad f^*(e_k) = \sum_{j=1}^{n} \beta_{jk} e_j ,$$

odnosno, zbog ortonormiranosti baze

$$(f(e_k), e_i) = \alpha_{ik} \qquad \text{i} \qquad (f^*(e_k), e_i) = \beta_{ik} .$$

Zato imamo redom

$$\beta_{ik} = (f^*(e_k), e_i) = (e_k, f(e_i)) = \overline{(f(e_i), e_k)} = \overline{\alpha_{ki}} .$$

Dakle je

$$B = [\beta_{ik}] = [\overline{\alpha_{ki}}] = A^* ,$$

tj. matrica B je **hermitski konjugirana** ili, kako smo još rekli, **adjungirana** matrici A (vidi Zad. 2. u 9.2.).

Prema tome, dokazali smo

TEOREM 6

Neka je A matrica linearnog operatora f u nekoj ortonormiranoj bazi. Onda njemu adjungirani operator f^* ima u toj istoj bazi matricu A^*, koja je adjungirana matrici A. ■

Ako je, dakle,

$$\Phi : \operatorname{Hom} U \to M_n$$

izomorfizam algebri iz Tm. 2 u 10.4., realiziran pomoću ortonormirane baze, imamo odmah ovaj zaključak:

KOROLAR 7

Izomorfizam Φ čuva operaciju adjungiranja, tj. vrijedi

$$\Phi(f^*) = [\Phi(f)]^* ,$$

gdje, dakako, zvjezdica na lijevoj strani označava adjungiranje operatora, a ona na desnoj strani adjungiranje matrice.

Dokaz

Ako je $\Phi(f) = A$, onda je, po Tm. 6, $\Phi(f^*) = A^*$, pa je

$$\Phi(f^*) = A^* = [\Phi(f)]^* .$$ ■

Pomoću tog izomorfizma lako se dokazuje da operacija adjungiranja za matrice ima ista svojstva (1)–(5), koja su u Tm. 4 utvrđena za operaciju adjungiranja operatora. Na primjer, ako je $A = \Phi(f)$ i $B = \Phi(g)$, imamo

$$\begin{aligned} (AB)^* &= [\Phi(f)\Phi(g)]^* = [\Phi(fg)]^* = \Phi[(fg)^*] = \\ &= \Phi(g^* f^*) = \Phi(g^*)\Phi(f^*) = [\Phi(g)]^*[\Phi(f)]^* = B^* A^* , \end{aligned}$$

što smo već utvrdili i direktno.

Ovu točku završit ćemo još jednom karakterizacijom unitarnog operatora, ovaj put pomoću adjungiranog operatora.

TEOREM 8

Linearni operator $f : U \to U$ je unitaran ako i samo ako vrijedi

$$f \circ f^* = f^* \circ f = e ,$$

gdje je $e : U \to U$ jedinični operator.

Dokaz

Ako je f unitaran, imamo

$$(a,b) = (f(a), f(b)) = (a, (f^* \circ f)(b)) ,$$

za sve $a, b \in U$, pa je, po Lemi 1, $f^* \circ f = e$. Slično je i $f \circ f^* = e$. Obratno, ako za f vrijedi $f \circ f^* = f^* \circ f = e$, zaključujemo da je

$$(f(a), f(b)) = (a, (f^* \circ f)(b)) = (a, e(b)) = (a, b) ,$$

tj. f je unitaran po definiciji. ■

Teorem se, dakako, mogao dokazati i posredovanjem izomorfizma Φ.

ZADACI

1. Neka je U kompleksni unitarni prostor, a $f, g : U \to U$ linearni operatori sa svojstvom da je $(f(a), a) = (g(a), a)$, za svaki $a \in U$. Onda je $f = g$. Dokaži! Uvjeri se na primjeru da zaključak nije točan ako je prostor U realan.

2. Dokaži egzistenciju adjungiranog operatora pomoću matrica. [Uputa: Ako je A matrica od f u nekoj ortonormiranoj bazi, promatraj operator g koji u toj bazi ima matricu A^*, pa dokaži da g ima željeno svojstvo.]

3. Jedinični operator i nuloperator su sami sebi adjungirani. Pokaži da isto svojstvo ima operator $f + f^*$, za bilo koji operator f.

4. Pokaži da f i f^* imaju isti rang.

5. Ako je λ svojstvena vrijednost operatora f, onda je $\overline{\lambda}$ svojstvena vrijednost njemu adjungiranog operatora f^*. Dokaži!

6. Ako je $L < U$ f-invarijantan potprostor, onda je potprostor $L^\perp < U$ f^*-invarijantan (vidi točku 10.8.). Dokaži!

7. Pokaži da je jezgra od f^* ortogonalni komplement slike od f, $J(f^*) = [S(f)]^\perp$.

8. Neka je $U = L \oplus M$. Ako je p projektor od U na L u smjeru M, onda je p^* projektor od U na $M^\perp$ u smjeru $L^\perp$. Dokaži!

9. Dokaži: Uvijek je $f(U) = (f \circ f^*)(U)$ i $f^*(U) = (f^* \circ f)(U)$.

10. Dokaži da $f^* \circ f = n$ povlači da je $f = n$ gdje je n nuloperator.

11. Neka je $f^* \circ f = f \circ f^*$. Onda f i f^* imaju iste jezgre i iste slike. Nadalje, u tom je slučaju $f^n(U) = f(U)$, za sve $n \geq 1$. Dokaži!

12. Dokaži Tm. 8 pomoću izomorfizma Φ.

13. Pokaži da je preslikavanje

$$\Psi : \operatorname{Hom} U \to \operatorname{Hom} U ,$$

dano s $\Psi(f) = f^*$, jedan antilinearni izomorfizam (vidi Zad. 9. u 13.1.).

13.5. Hermitski i antihermitski operatori

Neka je U unitarni prostor. Za linearni operator $h : U \to U$ kažemo da je **hermitski simetričan** ili, kratko, **hermitski** ako za njega vrijedi

$$h^* = h .$$

Operator $k : U \to U$ je **hermitski antisimetričan** ili **antihermitski** ako je ispunjeno

$$k^* = -k .$$

Iz očiglednih razloga hermitski operator često se naziva i **autoadjungirani** ili **samoadjungirani** operator. Ako je prostor U realan, za netom definirane operatore uobičajeni su nazivi **simetričan**, odnosno **antisimetričan** operator. Primijetimo da će hermitski operator sasvim iznimno biti unitaran, tj. onda i samo onda kada je **involutoran**, $h^2 = e$.

Odmah se vidi da je hermitski operator karakteriziran svojstvom

$$(h(a), b) = (a, h(b)) , \tag{1}$$

a antihermitski s

$$(k(a), b) = -(a, k(b)) , \tag{2}$$

za sve $a, b \in U$, i ta svojstva često služe za njihovu definiciju.

Ako je u ortonormiranoj bazi prostora operator f reprezentiran matricom A, njemu adjungirani operator f^* će biti reprezentiran matricom A^*. Zato iz definicije neposredno slijedi da je za matricu hermitskog operatora ispunjeno

$$A^* = A , \tag{3}$$

odnosno, na razini elemenata,

$$\alpha_{ik} = \overline{\alpha}_{ki} ,$$

što znači da je matrica A **hermitska** (vidi Zad. 4. u 9.3.). Ako je pak operator antihermitski, vrijedi

$$A^* = -A\,, \tag{4}$$

tj.

$$\alpha_{ik} = -\overline{\alpha}_{ki}\,,$$

i prema tome, njegova je matrica **antihermitska**. Vrijedi i obratno:

PROPOZICIJA 1

Linearni operator $f : U \to U$ je hermitski (antihermitski) ako i samo ako je njegov matrični zapis u ortonormiranoj bazi hermitska (antihermitska) matrica. ■

U realnom slučaju se (3) i (4) reduciraju na

$$A' = A \quad \text{i} \quad A' = -A\,,$$

odakle slijedi da su simetrični (antisimetrični) operatori karakterizirani činjenic da im je matrica u ortonormiranoj bazi simetrična (antisimetrična).

Na primjer, u ravnini $\mathbb{R}^2$ su matricama

$$\begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}, \begin{bmatrix} \lambda & 0 \\ 0 & \lambda \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \begin{bmatrix} \cos\varphi & \sin\varphi \\ \sin\varphi & \cos\varphi \end{bmatrix}$$

redom opisani centralna simetrija, homotetija (s koeficijentom λ i središtem u ishodištu), te zrcaljenje na osi x, odnosno na pravcu koji s osi x zatvara kut $\varphi/2$, i to su sve simetrični operatori. U drugu ruku, s

$$\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$$

je opisana rotacija ravnine za kut $\pi/2$, i to je antisimetrični operator.

Postavlja se pitanje kakvu strukturu čine hermitski, odnosno antihermitski operatori. Odmah se vidi da vrijedi

PROPOZICIJA 2

Skup hermitskih (antihermitskih) operatora definiranih na istom unitarnom prostoru je, s obzirom na zbrajanje, Abelova grupa. ■

Ako je prostor realan, imamo i više:

PROPOZICIJA 3

Simetrični (antisimetrični) operatori, koji djeluju na realnom prostoru U, čine linearni prostor, potprostor od $\operatorname{Hom} U$. *Dimenzija tog prostora je* $n(n+1)/2$ *(odnosno* $n(n-1)/2$*), gdje je* $n = \dim U$. ■

Naravno, analogne tvrdnje vrijede i za skupove hermitskih (antihermitskih), odnosno simetričnih (antisimetričnih) matrica reda n (vidi Zad. 15.).

Produkt, tj. kompozicija hermitskih (simetričnih) operatora općenito nije takav operator. To će zbog

$$(h_1 \circ h_2)^* = h_2^* \circ h_1^* = h_2 \circ h_1$$

biti ako i samo ako h_1 i h_2 komutiraju. Isto vrijedi i za matrice.

PROPOZICIJA 4

Svojstvene vrijednosti hermitskog operatora su uvijek realni brojevi. Svojstvene vrijednosti antihermitskog operatora su čisto imaginarni brojevi (uključujući $0 = 0 \cdot i$*).*

Dokaz

Neka je λ svojstvena vrijednost hermitskog operatora f, $f(a) = \lambda a$, $a \neq \Theta$. Onda je

$$(f(a), a) = (\lambda a, a) = \lambda (a, a) ,$$

a u drugu ruku

$$(a, f(a)) = (a, \lambda a) = \overline{\lambda} (a, a) ,$$

pa iz definicije (1) hermitskog operatora, zbog $(a, a) \neq 0$, slijedi $\overline{\lambda} = \lambda$, tj. λ je realan broj. Analogno bismo u slučaju antihermitskog operatora pomoću (2) zaključili da je $\overline{\lambda} = -\lambda$, tj. da je λ čisto imaginaran broj. ■

Primijetimo da iz Prop. 4 slijedi da antisimetrični operator ili uopće nema svojstvenih vrijednosti ili ima jednu jedinu, i to je $\lambda = 0$ (i tada je singularan, vidi Zad. 10. u 10.9.).

PROPOZICIJA 5

Svojstveni vektori hermitskog operatora, koji pripadaju različitim svojstvenim vrijednostima, međusobno su ortogonalni. Isto vrijedi i za svojstvene vektore antihermitskog operatora.

Dokaz

Neka je h hermitski operator te $h(a) = \lambda a$, $h(b) = \mu b$, $a \neq \Theta$, $b \neq \Theta$ i $\lambda \neq \mu$. Imamo

$$(h(a), b) = (\lambda a, b) = \lambda (a, b)$$

i, uzimajući u obzir Prop. 4,

$$(a, h(b)) = (a, \mu b) = \overline{\mu}(a, b) = \mu(a, b) ,$$

dakle zbog hermitičnosti,

$$(\lambda - \mu)(a, b) = 0 ,$$

odakle je $(a, b) = 0$. Slično se dokazuje i antihermitski slučaj. ■

Propozicija zapravo kaže da su svojstveni potprostori od h u parovima ortogonalni.

Posve analogno kao za unitarne operatore, dokazuje se teorem o dijagonalizaciji za hermitske operatore (vidi Tm. 11 u 13.3.).

TEOREM 6

Svaki se hermitski (simetrični) operator može dijagonalizirati, tj. postoji ortonormirana baza prostora u kojoj je operator reprezentiran realnom dijagonalnom matricom. ■

Naravno, ta se baza sastoji od svojstvenih vektora operatora, a skalari na dijagonali su njegove svojstvene vrijednosti. Drugim riječima, duž dijagonale je "razvučen" spektar operatora. Zato se ovaj teorem obično u literaturi naziva **spektralni teorem**; pokazao se osobito važnim u raznim primjenama u geometriji, fizici i drugdje. Samo ime spektar dolazi iz fizike, gdje se teorem rabi u opisu složenog titranja (svjetlosti), pomoću niza jednostavnih titranja, čije frekvencije (boje) čine spektar titranja.

Sličan teorem imamo i u antihermitskom slučaju:

TEOREM 7

Svaki antihermitski operator, definiran na kompleksnom prostoru, dopušta dijagonalizaciju. Za antisimetrični operator uvijek postoji ortonormirana baza u kojoj se može reprezentirati matricom

$$A = \begin{bmatrix} A_1 & & & & O \\ & \ddots & & & \\ & & A_s & & \\ & & & 0 & \\ & & & & \ddots \\ O & & & & 0 \end{bmatrix} ,$$

gdje su s A_i označene antisimetrične matrice drugog reda, dakle matrice oblika

$$A_i = \begin{bmatrix} 0 & \alpha_i \\ -\alpha_i & 0 \end{bmatrix} ,$$

za neki $\alpha_i \in \mathbb{R}$. ■

To je najjednostavniji, normalni oblik matrice antisimetričnog operatora.

Ako je h bilo koji hermitski operator, onda je

$$(h(a), a) = (a, h(a)) = \overline{(h(a), a)} ,$$

tj. taj je skalarni produkt realan. Zato ima smisla sljedeća definicija:

Za hermitski (simetrični) operator $h : U \to U$ kažemo da je **pozitivan** (ili **pozitivno semidefinitan**), i pišemo

$$h \geq 0 ,$$

ako je ispunjeno

$$(h(a), a) \geq 0 ,$$

za svaki $a \in U$. Ako pritom

$$(h(a), a) = 0$$

povlači da je $a = \Theta$, za h kažemo da je **strogo pozitivan** (ili **pozitivno definitan**), i pišemo

$$h > 0 .$$

Analogno se definiraju **negativni** i **strogo negativni** operatori. Za hermitski operator koji ne spada ni u jednu od tih kategorija kažemo, da je **indefinitan**.

PROPOZICIJA 8

Hermitski operator je pozitivan ako i samo ako su njegove svojstvene vrijednosti nenegativne.

Dokaz

Neka je $h \geq 0$ i λ svojstvena vrijednost od h, $h(a) = \lambda a$, $a \neq \Theta$. Onda je

$$0 \leq (h(a), a) = (\lambda a, a) = \lambda (a, a) ,$$

i odatle $\lambda \geq 0$. Obratno, pretpostavimo da su svojstvene vrijednosti od h nenegativne. Neka je $E = (e_1, \ldots, e_n)$ ortonormirana baza, koja se sastoji od svojstvenih vektora od h. Neka je $a \in U$ bilo koji vektor. Za njega je

$$a = \sum_{i=1}^{n} \alpha_i e_i \qquad \text{i} \qquad h(a) = \sum_{i=1}^{n} \alpha_i h(e_i) = \sum_{i=1}^{n} \alpha_i \lambda_i e_i ,$$

gdje su $\lambda_i \geq 0$, $i = 1, \ldots, n$, svojstvene vrijednosti opratora h. Imamo

$$(h(a), a) = \sum_{i=1}^{n} (\alpha_i \lambda_i) \overline{\alpha_i} = \sum_{i=1}^{n} \lambda_i \alpha_i \overline{\alpha_i} = \sum_{i=1}^{n} \lambda_i \cdot |\alpha_i|^2 \geq 0 ,$$

i tvrdnja je dokazana. ■

KOROLAR 9

Pozitivan operator je strogo pozitivan ako i samo ako je regularan.

Dokaz

Neka je h pozitivan operator. U dokazu Prop. 8 vidjeli smo da možemo pisati

$$(h(a), a) = \sum_{i=1}^{n} \lambda_i |\alpha_i|^2 \geq 0 \,, \tag{5}$$

gdje su $\lambda_i \geq 0$, $i = 1, \ldots, n$, svojstvene vrijednosti od h. U drugu ruku, h je regularan operator ako i samo ako je

$$\det h = \lambda_1 \cdot \cdots \cdot \lambda_n \neq 0 \,.$$

Ako je, dakle, $\det h \neq 0$, mora biti $\lambda_i > 0$ za $i = 1, \ldots, n$. Iz (5) zato slijedi da je $(h(a), a) = 0$ samo uz $\alpha_i = 0$ za sve i, tj. samo za $a = \Theta$, te je h strogo pozitivan. Obratno, neka je h strogo pozitivan. Uzmimo da je $\det h = 0$. To bi povlačilo da je $\lambda_i = 0$ za neki i, pa bismo imali $e_i \neq \Theta$ i $h(e_i) = 0 \cdot e_i = \Theta$, dakle

$$(h(e_i), e_i) = (\Theta, e_i) = 0 \,,$$

što je kontradikcija. ■

Pozitivni operatori su važni jer se iz njih može vaditi korijen.

Ako su f i g linearni operatori, kažemo da je f **kvadratni (drugi) korijen operatora** g, kad vrijedi

$$f^2 = f \circ f = g \,. \tag{6}$$

Operatorska jednadžba (6) ne mora imati rješenja, odnosno može imati jedno, više, čak i beskonačno mnogo rješenja, u ovisnosti o g. Lako se npr. vidi da operator predočen matricom

$$\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$$

nema kvadratni korijen. Međutim, u slučaju pozitivnih operatora situacija je potpuno određena. Imamo

TEOREM 10

Za svaki pozitivni operator postoji i jednoznačno je određen pozitivni kvadratni korijen.

Dokaz

Neka je $h : U \to U$ bilo koji pozitivni operator. Onda h, po Tm. 6, dopušta dijagonalizaciju, pa prema Tm. 1 iz 10.10. postoji ortonormirana baza $E = (e_1, \ldots, e_n)$ prostora U koja se sastoji od jediničnih svojstvenih vektora tog operatora. Neka su $\lambda_i \geq 0$ korespondentne svojstvene vrijednosti, $h(e_i) = \lambda_i e_i$, $i = 1, \ldots, n$.

Neka je sada f linearni operator, zadan na bazi E s

$$f(e_i) = \sqrt{\lambda_i}\, e_i \,,$$

za $i = 1, \ldots, n$, gdje uvijek uzimamo pozitivnu determinaciju korijena. Kako je E ortonormirana baza koja se sastoji od svojstvenih vektora operatora f, odmah se može provjeriti da za svaki izbor $a, b \in U$ vrijedi

$$(f(a), b) = (a, f(b)) \,,$$

tj. operator f je hermitski. Nadalje, zbog $\sqrt{\lambda_i} \geq 0$, za svaki $i = 1, \ldots, n$, iz Prop. 8 slijedi da je taj operator i pozitivan. Konačno, za svaki $i = 1, \ldots, n$ je

$$f^2(e_i) = f[f(e_i)] = f(\sqrt{\lambda_i}\, e_i) = \sqrt{\lambda_i}\, f(e_i) = \lambda_i e_i = h(e_i) \,,$$

odakle zaključujemo da je $f^2 = h$. Nije teško vidjeti da je operator f jedinstven (vidi Zad. 22.). Zato možemo pisati $f = \sqrt{h}$. ■

ZADACI

1. Dokaži: Neka je f bilo koji linearni operator na unitarnom prostoru. Onda su $f \circ f^*$ i $f^* \circ f$ hermitski operatori. Nadalje, ako je h hermitski operator, i operatori $f^* \circ h \circ f$ te $f \circ h \circ f^*$ su hermitski. Isto vrijedi i za matrice.

2. Svaki se linearni operator na unitarnom prostoru može predočiti kao suma jednog hermitskog i jednog antihermitskog operatora. Isto vrijedi i za matrice. Dokaži!

3. Svaki se linearni operator f, koji djeluje na unitarnom prostoru, može jednoznačno prikazati u obliku $f = h_1 + ih_2$, gdje su h_1 i h_2 hermitski operatori, a i imaginarna jedinica. Isto vrijedi i za matrice. Dokaži!

4. Neka je h hermitski operator. Ako je $L < U$ h-invarijantan, dokaži da je i $L^\perp < U$ također h-invarijantan. Isto vrijedi i za unitarne operatore.

5. Operator f je antihermitski ako i samo ako je if hermitski operator (i je imaginarna jedinica). Dokaži!

6. Neka je k antisimetrični operator. Onda je operator k^2 simetričan i njegove su svojstvene vrijednosti manje ili jednake nuli. Dokaži!

7. Neka su $h_1, \ldots, h_k$ simetrični operatori koji djeluju na istom prostoru. Ako je $h_1^2 + \cdots + h_k^2 = n$, onda je $h_1 = \cdots = h_k = n$, gdje je n nuloperator. Dokaži!

8. Neka je h simetrični operator. Onda se

$$\max\{(h(a), a) \mid \|a\| = 1\}$$

podudara s najvećom svojstvenom vrijednošću $\lambda_{\max}$ od h. Nadalje, $\lambda_{\max} = (h(a), a)$ ako i samo ako je a svojstveni vektor za $\lambda_{\max}$. Dokaži analogni rezultat za

$$\min\{(h(a), a) \mid \|a\| = 1\} .$$

9. Dokaži: Ako je h hermitski operator, skup

$$S = \{(h(a), a) \mid a \in U\}$$

je **konveksan** u kompleksnoj ravnini (tj. $\lambda x + (1 - \lambda)y \in S$, za sve $x, y \in S$, $\lambda \in [0, 1]$) i sadrži sve svojstvene vrijednosti od h.

10. Dokaži: Elementi na glavnoj dijagonali hermitske matrice su uvijek realni, a u antihermitskoj matrici čisto imaginarni brojevi (uključujući nulu). Posebno, dakle, dijagonala antisimetrične matrice se sastoji iz samih nula.

11. Dokaži: Svaka hermitska i svaka antihermitska matrica su unitarno slične dijagonalnoj matrici. Simetrična matrica je ortogonalno slična dijagonalnoj matrici, a antisimetrična matrica svojoj normalnoj formi (vidi Tm. 7).

12. Pokaži da je svaka antisimetrična matrica A ortogonalno slična matrici B sa svojstvom da je B^2 dijagonalna matrica.

13. Pokaži: Antisimetrična matrica pozitivnog ranga ne može biti ortogonalno slična dijagonalnoj matrici.

14. Ako su A i B hermitske matrice, dokaži da su matrice $AB + BA$ i $i(AB - BA)$ također hermitske.

15. Pokaži da hermitske (antihermitske) matrice reda n čine linearni prostor nad poljem $\mathbb{R}$ realnih brojeva. Koje dimenzije? Pokaži nadalje, da je u prostoru antihermitskih matrica s

$$(A, B) = -\mathrm{tr}\,(AB)$$

dobro definiran skalarni produkt (vidi Zad. 1. u 12.3.).

16. Dokaži da je u linearnom prostoru antisimetričnih matrica reda n s

$$(A, B) = -\mathrm{tr}\,(AB)$$

definiran skalarni produkt, koji ga čini realnim unitarnim prostorom.

17. Dokaži: Ako je A hermitska matrica, onda je $A + iE$ regularna, a

$$B = (A + iE)^{-1}(A - iE)$$

unitarna matrica. B se naziva **Cayleyjev transformat** od A.

18. Matrica A je **nilpotentna** ako postoji prirodni broj k takav da je $A^k = O$. Pokaži da je nulmatrica jedina nilpotentna hermitska matrica.

19. Hermitski, odnosno simetrični operator je strogo pozitivan (strogo negativan) ako i samo ako su sve njegove svojstvene vrijednosti pozitivne (negativne). Dokaži!

20. Dokaži: Linearna kombinacija pozitivnih operatora s nenegativnim koeficijentima je opet pozitivan operator.

21. Za bilo koji operator f je $f \circ f^*$ pozitivni operator. Obratno, ako je h bilo koji pozitivni operator, uvijek postoji operator f takav da je $f \circ f^* = h$. Dokaži!

22. Posebno, kvadrat hermitskog operatora je pozitivan operator. Obratno, ako je h pozitivan operator, onda postoji pozitivan operator f takav da je $f^2 = h$ (vidi Tm. 10). Dokaži da je f jedinstven. Dokaži, nadalje, da svaki linearni operator koji komutira s h, komutira i s f.

23. Neka je h pozitivan operator i n dani prirodni broj. Onda postoji (pozitivni) **n-ti korijen iz** h, tj. pozitivni operator f takav da je $f^n = h$. Je li f jedinstven?

24. Svaki pozitivni operator se može prikazati kao suma pozitivnih operatora ranga 1. Dokaži!

25. Za hermitsku matricu kažemo da je **pozitivna (negativna)** ako je ona matrica nekoga pozitivnog (negativnog) operatora u ortonormiranoj bazi. Analogno se definira **strogo pozitivna (strogo negativna) matrica**. Pokaži da je hermitska matrica pozitivna ako i samo ako koeficijenti u njezinu karakterističnom polinomu alterniraju predznak. Ako je jedan od koeficijenata nula, svi niži koeficijenti moraju također biti nula.

26. Ako su matrice $A = [\alpha_{ik}]$ i $B = [\beta_{ik}]$ pozitivne, dokaži da je i matrica $C = [\gamma_{ik}]$, gdje je $\gamma_{ik} = \alpha_{ik}\beta_{ik}$, $i, k = 1, \ldots, n$, pozitivna.

27. Ako je A simetrična matrica, dokaži da postoji cijeli broj m tako da je $A + mE$ strogo pozitivna matrica.

28. Ako je matrica A strogo pozitivna, postoji trokutasta matrica T takva da je $A = TT^*$ (to je tzv. **Toeplitzov prikaz** matrice). Dokaži!

29. Dokaži ovaj teorem o simultanoj dijagonalizaciji: Neka su A i B hermitske matrice od kojih je A strogo pozitivna. Onda postoji regularna matrica T takva da vrijedi

$$TAT^* = E\,, \qquad TBT^* = D\,,$$

gdje je D dijagonalna matrica kojoj su elementi na dijagonali korijeni jednadžbe

$$\det(B - \lambda A) = 0\,.$$

Ta se jednadžba često zove **sekularna jednadžba** (jer je u vezi s računanjem sekularnih perturbacija planetarnih orbita).

13.6. Normalni operatori

Mnoga dobra svojstva unitarnih i hermitskih operatora ima i šira klasa operatora na unitarnom prostoru, tzv. normalni operatori.

Neka je $f : U \to U$ linearni operator koji djeluje na unitarnom prostoru U. Kažemo da je taj operator **normalan** ako komutira sa svojim adjungiranim operatorom, tj. ako vrijedi

$$f \circ f^* = f^* \circ f\,. \tag{1}$$

Kako je unitarni operator karakteriziran svojstvom $f \circ f^* = f^* \circ f = e$ (Tm. 8 u 13.4.), a hermitski i antihermitski operator definirani relacijama $f^* = f$, odnosno $f^* = -f$, odmah razabiremo da su ti operatori specijalni slučajevi

normalnih operatora. Dakako, ako je U realni unitarni prostor, zaključujemo da su normalni i ortogonalni, simetrični te antisimetrični operatori.

Kompleksnu kvadratnu matricu A nazivamo **normalna matrica**, ako je $AA^* = A^*A$, gdje je A^* hermitski konjugirana (adjungirana) matrica matrici A. Kako se može očekivati, imamo ovu karakterizaciju normalnih operatora

PROPOZICIJA 1

Linearni operator $f : U \to U$ je normalan ako i samo ako je njegov matrični zapis u (nekoj, pa onda i svakoj) ortonormiranoj bazi normalna matrica.

Dokaz

Neka je $\Phi : \hom U \to M_n$ izomorfizam algebri iz Tm. 2 u 10.4., realiziran pomoću bilo koje ortonormirane baze prostora U, a A neka je matrica operatora f u toj bazi, $\Phi(f) = A$. Onda zbog Kor. 7 u 13.4. imamo

$$\begin{aligned} \Phi(f \circ f^*) &= \Phi(f)\Phi(f^*) = AA^* , \\ \Phi(f^* \circ f) &= \Phi(f^*)\Phi(f) = A^*A . \end{aligned}$$

Ako je, dakle, operator f normalan, tj. $f \circ f^* = f^* \circ f$, onda će vrijediti $AA^* = A^*A$, tj. matrica A tog operatora je normalna. Obratno, iz $AA^* = A^*A$ slijedi $\Phi(f \circ f^*) = \Phi(f^* \circ f)$, pa jer je Φ bijekcija, i $f \circ f^* = f^* \circ f$, tj. f je normalan operator. ■

Sada ćemo navesti neka osnovna svojstva normalnih operatora.

PROPOZICIJA 2

Linearni operator $f : U \to U$ je normalan ako i samo ako je

$$(f^*(a), f^*(b)) = (f(a), f(b)) , \tag{2}$$

za sve $a, b \in U$.

Dokaz

Ako je f normalan, imamo redom

$$(f^*(a), f^*(b)) = ((f \circ f^*)(a), b) = ((f^* \circ f)(a), b) = (f(a), f(b)) .$$

Obratno, ako vrijedi (2) imamo

$$(a, (f \circ f^*)(b)) = (f^*(a), f^*(b)) = (f(a), f(b)) = (a, (f^* \circ f)(b)) ,$$

pa je, prema Lemi 1 iz 13.4., $f \circ f^* = f^* \circ f$, tj. operator f je normalan. ■

KOROLAR 3

Ako je f normalni operator, onda je

$$\|f^*(a)\| = \|f(a)\| \,, \tag{3}$$

za svaki vektor a. ■

Vrijedi i obrat Kor. 3, tj. relacijom (3) su normalni operatori također karakterizirani (vidi Zad. 7.).

KOROLAR 4

Neka je $f : U \to U$ normalni operator i $a \in U$. Ako je $f^p(a) = \Theta$ za neki prirodni broj p, onda je također $f(a) = \Theta$.

Dokaz

Neka je p najmanji prirodni broj sa svojstvom da je $f^p(a) = \Theta$. Pretpostavimo da je $p > 1$. Ako označimo $b = f^{p-1}(a)$, onda je $b \neq \Theta$, ali $f(b) = f^p(a) = \Theta$, pa je po Kor. 3

$$\|f^*(b)\| = \|f(b)\| = 0 \,,$$

dakle i $f^*(b) = \Theta$. Prema tome je

$$0 = (f^*(b), f^{p-2}(a)) = (b, f^{p-1}(a)) = (b, b) \,,$$

odakle slijedi da je $b = \Theta$, što je protivno pretpostavci. Zato mora biti $p = 1$, dakle, $f(a) = \Theta$. ■

PROPOZICIJA 5

Neka je $f : U \to U$ normalni operator. Ako je $a \in U$ svojstveni vektor od f, pridružen svojstvenoj vrijednosti λ, onda je a svojstveni vektor i od f^*, ali pridružen svojstvenoj vrijednosti $\overline{\lambda}$.

Dokaz

Iz $f(a) = \lambda a$, korištenjem Prop. 2 slijedi

$$\begin{aligned} 0 &= \|f(a) - \lambda a\|^2 = (f(a) - \lambda a, f(a) - \lambda a) = \\ &= (f(a), f(a)) - \lambda(a, f(a)) - \overline{\lambda}(f(a), a) + \lambda\overline{\lambda}(a, a) = \\ &= (f^*(a), f^*(a)) - \lambda(f^*(a), a) - \overline{\lambda}(a, f^*(a)) + \lambda\overline{\lambda}(a, a) = \\ &= (f^*(a) - \overline{\lambda}a, f^*(a) - \overline{\lambda}a) = \|f^*(a) - \overline{\lambda}a\|^2 \,, \end{aligned}$$

pa je $f^*(a) - \overline{\lambda}a = \Theta$, tj. $f^*(a) = \overline{\lambda}a$. ■

PROPOZICIJA 6

Svojstveni vektori normalnog operatora, koji pripadaju različitim svojstvenim vrijednostima, međusobno su ortogonalni.

Dokaz

Neka je $f(a) = \lambda a$, $f(b) = \mu b$, $a, b \neq \Theta$ i $\lambda \neq \mu$. Onda imamo redom, koristeći Prop. 5,

$$\lambda(a,b) = (\lambda a, b) = (f(a), b) = (a, f^*(b)) = (a, \overline{\mu} b) = \mu(a,b) ,$$

dakle

$$(\lambda - \mu)(a,b) = 0 .$$

Kako je $\lambda - \mu \neq 0$, mora biti $(a,b) = 0$, što je i trebalo dokazati. ■

PROPOZICIJA 7

Neka je $f : U \to U$ linearni operator sa svojstvom da u U postoji ortonormirana baza koja se sastoji od njegovih svojstvenih vektora. Onda je f normalni operator.

Dokaz

Neka je $E = (e_1, \ldots, e_n)$ ortonormirana baza prostora U koja se sastoji od svojstvenih vektora operatora f. Neka su λ_i, $i = 1, \ldots, n$, pripadne svojstvene vrijednosti. Onda je

$$\begin{aligned} (e_i, f^*(e_j)) &= (f(e_i), e_j) = (\lambda_i e_i, e_j) = \lambda_i (e_i, e_j) = \\ &= \lambda_i \delta_{ij} = \lambda_j \delta_{ij} = \lambda_j (e_i, e_j) = (e_i, \overline{\lambda}_j e_j) . \end{aligned}$$

Uz čvrsti e_j, ta je relacija istinita za sve e_i, $i = 1, \ldots, n$, pa odmah zaključujemo da vrijedi

$$(a, f^*(e_j)) = (a, \overline{\lambda}_j e_j) , \tag{4}$$

za sve $a \in U$ i svaki e_j. Neka je sada $g : U \to U$ linearni operator definiran s

$$g(b) = g\left(\sum_{j=1}^{n} \alpha_j e_j\right) = \sum_{j=1}^{n} \overline{\lambda}_j \alpha_j e_j . \tag{5}$$

Zbog (4) i (5) imamo

$$\begin{aligned} (a, f^*(b)) &= (a, f^*\left(\sum_{j=1}^{n} \alpha_j e_j\right)) = \sum_{j=1}^{n} \overline{\alpha_j} (a, f^*(e_j)) = \\ &= \sum_{j=1}^{n} \overline{\alpha}_j (a, \overline{\lambda}_j e_j) = (a, \sum_{j=1}^{n} \overline{\lambda}_j \alpha_j e_j) = (a, g(b)) , \end{aligned}$$

pa na temelju Leme 1 iz 13.4. zaključujemo da je $f^* = g$. Tada je

$$\begin{aligned}(f \circ f^*)(b) &= (f \circ g)(b) = (f \circ g)\Big(\sum_{j=1}^{n} \alpha_j e_j\Big) = f\Big(\sum_{j=1}^{n} \overline{\lambda_j}\alpha_j e_j\Big) = \\ &= \sum_{j=1}^{n} \overline{\lambda_j}\alpha_j f(e_j) = \sum_{j=1}^{n} \overline{\lambda_j}\alpha_j \lambda_j e_j = \\ &= g\Big(\sum_{j=1}^{n} \alpha_j \lambda_j e_j\Big) = g\Big(\sum_{j=1}^{n} \alpha_j f(e_j)\Big) = \\ &= (g \circ f)\Big(\sum_{j=1}^{n} \alpha_j e_j\Big) = (g \circ f)(b) = (f^* \circ f)(b)\,,\end{aligned}$$

za svaki $b \in U$, pa je $f \circ f^* = f^* \circ f$ i tvrdnja je dokazana. ■

Zanimljivo je, da je, uz restrikciju na kompleksne prostore (koja osigurava dovoljno svojstvenih vektora), istinit i obrat Prop. 7:

PROPOZICIJA 8

Neka je U kompleksni unitarni prostor, a $f : U \to U$ normalni operator. Onda postoji ortonormirana baza u U koja se sastoji od svojstvenih vektora operatora f.

Dokaz

Dokaz je u suštini jednak dokazu Tm. 11 u 13.3. Tvrdnju dokazujemo indukcijom po dimenziji $n = \dim U$. Ako je $n = 1$ i $\{e\}$ ortonormirana baza od U, očito je $f(e) = \lambda e$, tj. tvrdnja je istinita. Pretpostavimo da je tvrdnja istinita za sve dimenzije manje od n i neka je prostor U n-dimenzionalan. Kako je U prostor nad poljem kompleksnih brojeva, postoji bar jedna svojstvena vrijednost λ_1 operatora f. Za pripadni svojstveni vektor $e_1 \neq \Theta$ možemo pretpostaviti da je normiran. Neka je $L = [e_1]$, a $M = L^{\perp}$. Očito je $\dim M = n - 1$. Neka je $a \in M$ bilo koji vektor. Onda je svakako $(a, e_1) = 0$ i nadalje, korištenjem Prop. 5, imamo

$$(f(a), e_1) = (a, f^*(e_1)) = (a, \overline{\lambda}_1 e_1) = \lambda_1 (a, e_1) = 0\,.$$

Odatle je $f(a) \in M$, dakle $f(M) \subset M$, tj. M je f-invarijantan. Prema tome je restrikcija $f/_M : M \to M$ normalni operator na M, pa po pretpostavci indukcije postoji ortonormirana baza

$$(e_2, \ldots, e_n)$$

za M, koja se sastoji od svojstvenih vektora operatora $f/_M$ tj. f. Tada je

$$(e_1, e_2, \ldots, e_n)$$

ortonormirana baza za prostor U, koju čine svojstveni vektori od f, i tvrdnja je dokazana. ■

Prop. 8 u uskoj je vezi s problemom dijagonalizacije. Kako smo vidjeli u 13.3. i 13.5., unitarni, hermitski i antihermitski operatori na kompleksnom prostoru uvijek dopuštaju dijagonalizaciju. Ima, međutim, i drugih operatora s tim svojstvom. Najširа klasa operatora koje je moguće dijagonalizirati (u ortonormiranoj bazi) upravo su normalni operatori, i to je svojstvo koje ih karakterizira.

TEOREM 9

Neka je U kompleksni unitarni prostor. Operator $f : U \to U$ je normalan ako i samo ako postoji ortonormirana baza za U u kojoj f ima dijagonalni matrični zapis.

Dokaz

Ako je operator f normalan, prema Prop. 8 u U postoji ortonormirana baza koju čine svojstveni vektori od f. Operator f u toj bazi ima dijagonalnu matricu, prema Tm. 1 iz 10.10.

Obratno, neka je D dijagonalna matrica, koja reprezentira operator f u nekoj ortonormiranoj bazi. Onda je, dakako, i D^* dijagonalna matrica. Budući da dijagonalne matrice očito komutiraju, imamo

$$DD^* = D^*D \ ,$$

pa iz Prop. 1 zaključujemo da je f normalni operator (tvrdnja slijedi također i iz Tm. 1 u 10.10. te Prop. 7). ■

Zapišimo i zapamtimo Tm. 9 i u ovom obliku:

TEOREM 10

Linearni operator na kompleksnom unitarnom prostoru dopušta dijagonalizaciju ako i samo ako je normalan. ■

Kao i uvijek, situacija je nešto složenija u slučaju realnog prostora. Tada vrijedi

TEOREM 11

Neka je U realni unitarni prostor. Operator $f : U \to U$ je normalan ako

i samo ako postoji ortonormirana baza za U u kojoj f ima matrični zapis

$$A = \begin{bmatrix} A_1 & & & & & O \\ & \ddots & & & & \\ & & A_s & & & \\ & & & \lambda_1 & & \\ & & & & \ddots & \\ O & & & & & \lambda_r \end{bmatrix},$$

gdje su s A_k označene (normalne) matrice drugog reda, oblika

$$A_k = \begin{bmatrix} \alpha_k & \beta_k \\ -\beta_k & \alpha_k \end{bmatrix},$$

za neke $\alpha_k, \beta_k \in \mathbb{R}$. Pritom bilo koji od brojeva s i r može biti i nula. ■

U A su, dakako, $\lambda_1, \ldots, \lambda_r$ svojstvene vrijednosti operatora f (koje se pojavljuju toliko puta, kolika im je algebarska kratnost). Nadalje, brojevi α_k, β_k, koji se pojavljuju u bloku A_k, imaju svojstvo da su $\alpha_k \pm i\beta_k$ (konjugirano kompleksne) nule karakterističnog polinoma k_f operatora f, i svaki se blok pojavljuje u matrici A toliko puta, kolika je kratnost tih nula.

Primijetimo da se blok A_k može pisati i u obliku

$$A_k = r_k \begin{bmatrix} \cos\varphi_k & \sin\varphi_k \\ -\sin\varphi_k & \cos\varphi_k \end{bmatrix},$$

za neke $r_k \in \mathbb{R}$ i $0 < \varphi_k < 2\pi$, što omogućuje geometrijsku interpretaciju normalnog operatora (vidi kraj točke 13.3.). S A_k je, naime, opisana rotacija u ravnini za kut φ_k, komponirana s homotetijom s koeficijentom r_k, pa se djelovanje normalnog operatora f može shvatiti kao niz uzastopnih transformacija tog tipa, u međusobno ortogonalnim dvodimenzionalnim potprostorima, kombiniranih s homotetijama (s koeficijentima λ_l) u preostalim smjerovima.

Tm. 9 i Tm. 11 nazivaju se **spektralni teoremi** (ili **teoremi o spektralnoj dekompoziciji**) za normalne operatore. Njima je dana najjednostavnija, **normalna forma** matrica tih operatora.

ZADACI

1. Unitarne, hermitske i antihermitske matrice su normalne. Nađi primjer normalne matrice koja nije te vrste.

2. Dokaži: Ako je A normalna matrica, onda je i matrica A^* normalna. Međutim, zbroj i produkt normalnih matrica nisu nužno normalne matrice. Zapravo, svaka se matrica može prikazati kao zbroj, odnosno produkt normalnih matrica (vidi točku 13.7.).

3. Neka su A i B unitarno slične matrice (vidi Zad. 4. u 13.3.). Ako je jedna od njih normalna, dokaži da je takva i druga.

4. Dokaži: Svaka kompleksna matrica je unitarno slična trokutastoj matrici. Takva matrica je unitarno slična dijagonalnoj matrici ako i samo ako je normalna.

5. Ako je p bilo koji polinom, a A normalna matrica, dokaži da je $p(A)$ također normalna matrica.

6. Neka su A i B hermitske matrice. Matrica $A + iB$ je normalna ako i samo ako je $AB = BA$. Dokaži!

7. Dokaži obrat Kor. 3: Ako je $\|f^*(a)\| = \|f(a)\|$ za svaki $a \in U$, onda je operator f normalan. [Uputa: Rabi formule iz Zad. 5. u 12.5.]

8. Neka je f normalni operator. Dokaži da je:

   (a) $J(f) = J(f^*)$;

   (b) $J(f) = [S(f)]^{\perp}$;

   (c) $S(f) = S(f^*)$,

   gdje su sa S i J označene slika, odnosno jezgra operatora.

9. Neka je $S \subset U$ bilo koji skup svojstvenih vektora normalnog operatora $f : U \to U$. Onda je $S^{\perp} < U$ f-invarijantan potprostor od U. Dokaži!

10. Ako je f normalni operator na U i $L < U$ f-invarijantan potprostor, onda je i $L^{\perp} < U$ f-invarijantan. Nadalje, ako je U kompleksni prostor, to svojstvo karakterizira normalne operatore. Dokaži!

11. Ako je f normalni operator, njegov minimalni polinom m_f može se rastaviti u produkt različitih linearnih faktora. Dokaži!

12. Dokaži ovu generalizaciju Prop. 7: Ako su $f, g : U \to U$ linearni operatori sa svojstvom da u U postoji baza (ne nužno ortogonalna) koju čine svojstveni vektori za oba operatora, onda je $f \circ g = g \circ f$, tj. operatori komutiraju.

13. Kao i u Prop. 8, obrat zahtijeva dodatne uvjete. Neka je U kompleksni unitarni prostor, a $f, g : U \to U$ normalni operatori. Ako je $f \circ g = g \circ f$, onda postoji ortonormirana baza za U koja se sastoji od vektora koji su svojstveni vektori i za f, i za g (ali ne nužno za iste svojstvene vrijednosti). Dokaži!

14. Dokaži: Ako postoji ortonormirana baza prostora u kojoj operatori f i g imaju dijagonalni zapis, onda je $f \circ g = g \circ f$.

15. Ako su f i g normalni operatori na kompleksnom prostoru i vrijedi $f \circ g = g \circ f$, onda se ti operatori mogu istodobno dijagonalizirati, tj. postoji ortonormirana baza prostora u kojoj oba operatora imaju dijagonalne matrične prikaze. Dokaži i generaliziraj!

16. Skup $\mathcal{F} \subset \hom U$ operatora definiranih na U nazivamo **Abelova familija operatora**, ako svaka dva operatora iz $\mathcal{F}$ komutiraju. Neka je U kompleksni unitarni prostor, a $\mathcal{F}$ Abelova familija normalnih operatora, koji djeluju na tom prostoru. Onda u U postoji ortonormirana baza, koju čine vektori svojstveni za svaki od operatora iz $\mathcal{F}$. Nadalje, u toj bazi svi operatori iz $\mathcal{F}$ imaju dijagonalni zapis. Prema tome, Abelova se familija normalnih operatora može istodobno dijagonalizirati.

17. Neka je f normalni operator na kompleksnom prostoru. Onda je f:

    (a) unitaran ako i samo ako su sve njegove svojstvene vrijednosti modula 1;

    (b) hermitski ako i samo ako su sve njegove svojstvene vrijednosti realne;

    (c) antihermitski ako i samo ako su sve njegove svojstvene vrijednosti čisto imaginarne (uključujući i 0 kao mogućnost);

    (d) nuloperator ako i samo ako su sve njegove svojstvene vrijednosti jednake 0.

18. Kao i kod matrica, za operator f kažemo da je **nilpotentan** ako postoji prirodni broj k takav da je $f^k = n$, gdje je n nuloperator. Pokaži da je nuloperator jedini normalni operator, koji je nilpotentan.

19. Neka je U realni unitarni prostor, a $f : U \to U$ normalni operator. Pokaži da se U može prikazati kao direktna suma jednodimenzionalnih i dvodimenzionalnih potprostora, invarijantnih u odnosu na f. Koristeći se tom činjenicom, dokaži Tm. 11.

20. Neka je f bilo koji normalni operator koji djeluje na kompleksnom unitarnom prostoru i neka je n bilo koji prirodni broj. Dokaži da postoji normalni operator g, takav da je $g^n = f$. Koji je maksimalni broj takvih operatora? Svaki operator g s tim svojstvom zovemo **n-ti normalni korijen** operatora f.

21. Normalni operatori su unitarno slični (vidi Zad. 6. u 13.3.) ako i samo ako imaju isti karakteristični polinom. Dokaži!

13.7. Dekompozicije linearnog operatora

Unitarni, hermitski i antihermitski operatori imaju mnogo dobrih svojstava i lako ih je geometrijski interpretirati. Zato se prirodno postavlja pitanje, je li možda moguće bilo koji linearni operator predočiti kao jednostavnu kombinaciju tih operatora. Odgovor je potvrdan (vidi Zad. 2. i 3. u 13.5.). Navest ćemo nekoliko rezultata te vrste.

PROPOZICIJA 1

Svaki se linearni operator $f : U \to U$, definiran na unitarnom prostoru U, može jednoznačno predočiti u obliku

$$f = h + k\,,$$

gdje je h hermitski, a k antihermitski operator.

Dokaz

Neka je

$$h = \frac{1}{2}(f + f^*)\,, \qquad k = \frac{1}{2}(f - f^*)\,.$$

Onda je

$$h^* = [\frac{1}{2}(f + f^*)]^* = \frac{1}{2}(f + f^*)^* = \frac{1}{2}(f^* + f) = \frac{1}{2}(f + f^*) = h\,,$$

pa je h hermitski operator, i

$$k^* = [\frac{1}{2}(f - f^*)]^* = \frac{1}{2}(f - f^*)^* = \frac{1}{2}(f^* - f) = -\frac{1}{2}(f - f^*) = -k\,,$$

tj. k je antihermitski operator. Očito vrijedi

$$f = h + k\,,$$

pa je egzistencija rastava dokazana. Kad bi postojao još jedan rastav

$$f = \tilde{h} + \tilde{k}$$

istog svojstva, nakon oduzimanja imali bismo

$$h - \tilde{h} = \tilde{k} - k \,,$$

gdje je lijeva strana jednakosti očito hermitski, a desna strana antihermitski operator (Prop. 2 u 13.5.). Međutim, operator je istodobno hermitski i antihermitski ako i samo ako je nuloperator, odakle zaključujemo da mora biti $\tilde{h} = h$ i $\tilde{k} = k$, čime je dokazana jednoznačnost rastava. ■

Operator h nazivamo **hermitski**, a operator k **antihermitski dio** operatora f.

Ako je prostor U realan, propozicija kaže da se svaki linearni operator na tom prostoru može jednoznačno predočiti kao suma simetričnog i antisimetričnog operatora.

PROPOZICIJA 2

Svaki linearni operator $f : U \to U$ na kompleksnom unitarnom prostoru U dopušta jedinstveni prikaz oblika

$$f = g + i\,h \,,$$

gdje su g i h hermitski operatori (a i imaginarna jedinica).

Dokaz

Prema Prop. 1 možemo pisati

$$f = g + k = g + i\,(-i\,k) \,,$$

gdje je g hermitski, a k antihermitski operator. Zato je dovoljno provjeriti da je $h = -i\,k$ hermitski operator. Imamo

$$h^* = (-ik)^* = ik^* = -ik = h \,,$$

pa je operator h zaista hermitski. Lako se vidi da je prikaz jednoznačan. ■

Eksplicitno, **hermitske komponente** operatora f dane su s

$$g = \frac{1}{2}(f + f^*) \,, \qquad h = -\frac{i}{2}(f - f^*) \,.$$

Razabiremo da prikaz nema smisla ako je U realni unitarni prostor.

Taj se prikaz obično naziva **Kartezijev rastav** (**dekompozicija**) linearnog operatora ili, također, **Kartezijeva forma** (**reprezentacija**) operatora.

Sada ćemo pokazati da se svaki operator može prikazati kao produkt jednog hermitskog i jednog unitarnog operatora.

Za linearne operatore $f, g : U \to U$ kažemo da su **ekvimetrični** (ili **izometrički jednaki**), ako je ispunjeno

$$\|f(a)\| = \|g(a)\| ,$$

za sve $a \in U$. Na primjer, svaki par unitarnih operatora je ekvimetričan, normalni operator je ekvimetričan sa svojim adjungiranim operatorom itd. Očito, ekvimetričnost je jedna relacija ekvivalencije na $\mathrm{Hom}\, U$.

LEMA 3

Neka su f i g ekvimetrični operatori koji djeluju na unitarnom prostoru U. Onda postoji unitarni operator u na tom prostoru tako da vrijedi

$$g = u \circ f .$$

Dokaz

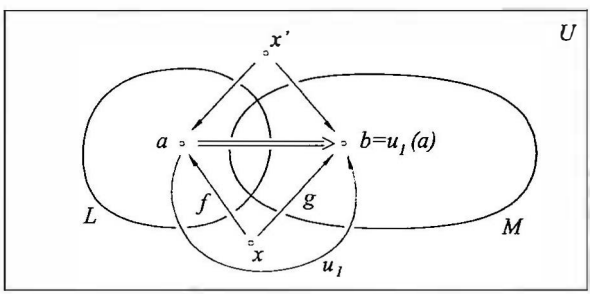
Neka su $L = f(U) < U$ i $M = g(U) < U$ slike operatora f, odnosno g. To su, dakako, potprostori od U. Definirajmo preslikavanje

$$u_1 : L \to M$$

na ovaj način: Za $a \in L$ odaberemo $x \in U$ takav da je $f(x) = a$. Onda označimo $b = g(x)$ i stavimo

$$u_1(a) = b . \tag{1}$$

Preslikavanje u_1 je dobro definirano, jer ako je $x' \in U$ drugi vektor sa svoj-



stvom da je $f(x') = a$, imamo $f(x') = f(x)$, tj. $f(x' - x) = \Theta$, i zbog ekvimetričnosti operatora

$$\|g(x' - x)\| = \|f(x' - x)\| = 0 .$$

Odatle slijedi $g(x'-x)=\Theta$, pa je $g(x')=g(x)=b$, što je i trebalo vidjeti. Primijetimo kako se iz (1) vidi da vrijedi

$$u_1(f(x))=g(x)\,, \tag{2}$$

za svaki $x\in U$.

Tvrdimo da je u_1 izomorfizam unitarnih prostora (vidi točku 13.1.). Najprije, u_1 je linearni operator jer, za bilo koje $a_1,a_2\in L$, zbog (2) imamo

$$\begin{aligned}
&u_1(\alpha_1a_1+\alpha_2a_2)=u_1(\alpha_1f(x_1)+\alpha_2f(x_2))=\\
&=(u_1\circ f)(\alpha_1x_1+\alpha_2x_2)=g(\alpha_1x_1+\alpha_2x_2)=\\
&=\alpha_1g(x_1)+\alpha_2g(x_2)=\alpha_1(u_1\circ f)(x_1)+\alpha_2(u_1\circ f)(x_2)=\\
&=\alpha_1u[f(x_1)]+\alpha_2u[f(x_2)]=\\
&=\alpha_1u_1(a_1)+\alpha_2u_1(a_2)\,.
\end{aligned}$$

Nadalje, u_1 čuva normu jer zbog (2) i ekvimetričnosti imamo

$$\|u_1(a)\|=\|(u_1\circ f)(x)\|=\|g(x)\|=\|f(x)\|=\|a\|\,,$$

pa je taj operator unitaran po Tm. 1 iz 13.2. Konačno, u_1 je surjektivan. Naime, za bilo koji $b\in M$ postoji $x\in U$ takav da je $g(x)=b$. Ako je sada $f(x)=a$, onda je

$$u_1(a)=(u_1\circ f)(x)=g(x)=b\,,$$

pa je dokazana i surjektivnost. Prema tome, u_1 je izomorfizam po definiciji, tj. L i M su unitarno izomorfni prostori.

Operator u_1 je bio definiran na $L<U$. Želimo ga proširiti do unitarnog operatora koji djeluje na čitavom prostoru U. Neka su s $L^{\perp}$ i $M^{\perp}$ označeni ortogonalni komplementi potprostora L, odnosno M. Tada je

$$U=L\oplus L^{\perp}=M\oplus M^{\perp}\,. \tag{3}$$

Kako su potprostori L i M izomorfni, to je $\dim L=\dim M$, pa je i $\dim L^{\perp}=\dim M^{\perp}$. Na temelju Tm. 5 iz 13.1. zaključujemo da su $L^{\perp}$ i $M^{\perp}$ unitarno izomorfni, tj. da postoji izomorfizam

$$u_2:L^{\perp}\to M^{\perp}\,.$$

Kako je $U=L\oplus L^{\perp}$, svaki vektor $x\in U$ ima jednoznačan prikaz $x=a+a^{\perp}$, gdje je $a\in L$, $a^{\perp}\in L^{\perp}$. Imajući to na umu, definiramo operator

$$u:U\to U\,,$$

stavljajući

$$u(x) = u(a + a^{\perp}) = u_1(a) + u_2(a^{\perp}) ,$$

za svaki $x \in U$. Lako se provjeri da je u linearni operator. Pokažimo da čuva normu. Zaista, zbog $M \perp M^{\perp}$ i $L \perp L^{\perp}$, te činjenice da su u_1 i u_2 unitarni operatori, imamo redom

$$\begin{aligned} \|u(x)\|^2 &= \|u_1(a) + u_2(a^{\perp})\|^2 = (u_1(a) + u_2(a^{\perp}),\ u_1(a) + u_2(a^{\perp})) = \\ &= (u_1(a), u_1(a)) + (u_1(a), u_2(a^{\perp})) + \\ &\quad + (u_2(a^{\perp}), u_1(a)) + (u_2(a^{\perp}), u_2(a^{\perp})) = \\ &= (u_1(a), u_1(a)) + (u_2(a^{\perp}), u_2(a^{\perp})) = (a, a) + (a^{\perp}, a^{\perp}) = \\ &= (a + a^{\perp}, a + a^{\perp}) = (x, x) = \|x\|^2 . \end{aligned}$$

Prema tome, u je unitarni operator koji očito proširuje u_1, $u/L = u_1$.

Ako je, dakle, $x \in U$ bilo koji vektor, bit će $f(x) \in L$, pa je

$$(u \circ f)(x) = (u_1 \circ f)(x) = g(x),$$

dakle $u \circ f = g$ i lema je dokazana. ■

TEOREM 4 (L. Autonne, 1902.)

Neka je $f : U \to U$ bilo koji linearni operator na (realnom ili kompleksnom) unitarnom prostoru U. Onda f dopušta prikaz

$$f = u \circ h ,$$

gdje je u unitarni, a h pozitivni hermitski operator. Pritom je h određen jednoznačno, a ako je f regularni operator, jednoznačno je određen i u.

Dokaz

Promatrajmo operator $f^* \circ f$. Kako je $(f^* \circ f)^* = f^* \circ f$ i vrijedi

$$((f^* \circ f)(a), a) = (f(a), f(a)) \geq 0 ,$$

za svako $a \in U$, zaključujemo da je $f^* \circ f$ pozitivni operator. Prema Tm. 10 iz 13.5. postoji kvadratni korijen tog operatora, tj. jednoznačno je određen pozitivni operator h tako da je

$$h^2 = f^* \circ f .$$

Ako je sada $x \in U$ bilo koji vektor, imamo

$$(f(x), f(x)) = (x, (f^* \circ f)(x)) = (x, h^2(x)) = (h(x), h(x)) ,$$

što pokazuje da su f i h ekvimetrični operatori. Prema Lemi 3 onda postoji unitarni operator u tako da je $f = u \circ h$, pa je egzistencija tražene faktorizacije dokazana.

Pokažimo jedinstvenost operatora h. Neka je $f = u \circ h$ bilo koja dekompozicija traženog tipa. Onda je, zbog Tm. 8 u 13.4.,

$$f^* = (u \circ h)^* = h^* \circ u^* = h \circ u^{-1}$$

i

$$f^* \circ f = (h \circ u^{-1}) \circ (u \circ h) = h^2 ,$$

pa je h kvadratni korijen pozitivnog operatora, a taj je, budući da je h nužno pozitivan, određen jednoznačno. Nadalje, ako je f regularan, i h mora biti regularan, pa iz promatrane dekompozicije imamo

$$u = f \circ h^{-1} ,$$

čime je dokazana i jednoznačnost za u. ■

Vrijedi i teorem o simetričnoj faktorizaciji. Imamo

TEOREM 5

Neka je $f : U \to U$ bilo koji linearni operator. Onda ga možemo prikazati kao

$$f = h \circ u ,$$

gdje je h pozitivni, a u unitarni operator. Operator h je pritom određen jednoznačno. Ako je f regularan, i u je jednoznačno određen.

Dokaz

Neka je

$$f^* = v \circ h$$

dekompozicija iz Tm. 4 za adjungirani operator f^* od f. Onda je

$$f = (f^*)^* = (v \circ h)^* = h^* \circ v^* = h \circ v^* = h \circ u ,$$

gdje je $u = v^*$ unitarni operator (kao adjungirani operator unitarnog operatora), i tvrdnja je dokazana. ■

Prikaz operatora iz Tm. 5, kao i onaj iz Tm. 4, nazivaju se **polarni rastav** (**faktorizacija**, **dekompozicija**) linearnog operatora ili, također, **polarna forma** (**reprezentacija**, **prikaz**) operatora.

Napomenimo da u slučaju kad je f singularan operator, tvrdnja o jednoznačnosti polarne dekompozicije ne stoji. Trivijalan je primjer kad je f

nuloperator. Onda, naime, i h mora biti nuloperator pa za u možemo uzeti bilo koji unitarni operator.

Općenito, operatori u i h u polarnom rastavu iz Tm. 5 neće biti jednaki onima koji se pojavljuju u rastavu iz Tm. 4. Malo je bolja situacija u slučaju normalnih operatora.

KOROLAR 6

Neka je f linearni operator, a

$$f = u_1 \circ h_1 \quad , \qquad f = h_2 \circ u_2$$

njegove polarne reprezentacije. Operator f je normalan ako i samo ako vrijedi

$$\left.\begin{array}{c} u_1 \circ h_1 = h_1 \circ u_1 \qquad , \qquad u_2 \circ h_2 = h_2 \circ u_2 \\ h_1 = h_2 \end{array}\right\} . \tag{4}$$

Dokaz

Neka je f normalni operator. Kako je $h_1^2 = f^* \circ f$ i $h_2^2 = f \circ f^*$, zbog normalnosti imamo

$$h_1^2 = f^* \circ f = f \circ f^* = h_2^2 ,$$

i odatle $h_1 = h_2$, zbog jednoznačnosti pozitivnoga kvadratnog korijena. Nadalje, iz $f \circ f^* = f^* \circ f$ slijedi

$$(u_1 \circ h_1) \circ (u_1 \circ h_1)^* = (u_1 \circ h_1)^* \circ (u_1 \circ h_1) ,$$

odnosno

$$(u_1 \circ h_1) \circ (h_1 \circ u_1^{-1}) = (h_1 \circ u_1^{-1}) \circ (u_1 \circ h_1) ,$$

dakle

$$u_1 \circ h_1^2 \circ u_1^{-1} = h_1^2 ,$$

tj.

$$u_1 \circ h_1^2 = h_1^2 \circ u_1 .$$

Kako je h_1 pozitivni kvadratni korijen iz h_1^2, svaki operator koji komutira s h_1^2 sigurno komutira i s h_1 (Zad. 22. u 13.5.), pa imamo

$$u_1 \circ h_1 = h_1 \circ u_1 ,$$

što se i tvrdilo. Analogno se dokaže i da je $u_2 \circ h_2 = h_2 \circ u_2$.

Obratno, pretpostavimo da su za operator f ispunjene relacije (4). Onda imamo

$$\begin{aligned} f^* \circ f - f \circ f^* &= (h_1 \circ u_1^{-1}) \circ (u_1 \circ h_1) - (h_2 \circ u_2) \circ (u_2^{-1} \circ h_2) = \\ &= h_1^2 - h_2^2 = h_1^2 - h_1^2 = n , \end{aligned}$$

pa je operator f normalan. ■

Primijetimo da i u ovom specijalnom slučaju u_1 može biti različit od u_2 (kao što pokazuje primjer nuloperatora, koji je normalan).

NAPOMENA 7

Nazivi Kartezijev te polarni prikaz operatora dolaze od očigledne analogije koja postoji između kompleksnih brojeva i linearnih operatora. Ako je u toj analogiji kompleksnom broju z pridružen operator f, prirodno je da konjugirano kompleksnom broju $\overline{z}$ pridružimo hermitski konjugirani, tj. adjungirani operator f^*. Prema toj korespondenciji, nekom će kompleksnom broju z modula 1, tj. takvom da je $z\overline{z} = |z|^2 = 1$, odgovarati operator sa svojstvom $f \circ f^* = e$, dakle unitarni operator. Nadalje, ako je $\overline{z} = z$, broj z je realan i njemu odgovara operator za koji je $f^* = f$, dakle hermitski operator. Slično, broj z za koji je $\overline{z} = -z$ čisto je imaginaran, i njemu je pridružen antihermitski operator, jer za njega vrijedi $f^* = -f$. Kartezijevu prikazu kompleksnog broja, $z = x + iy$, gdje su $x, y \in \mathbb{R}$, onda će korespondirati prikaz $f = g + ih$ operatora, gdje su g i h hermitski operatori, pa zato taj prikaz također zovemo Kartezijevim. U drugu ruku, polarnom prikazu kompleksnog broja, $z = re^{i\varphi}$, gdje je r nenegativni realni broj, a $e^{i\varphi}$ kompleksni broj modula 1, odgovara prikaz $f = h \circ u$ linearnog operatora, u kojem je h pozitivni, a u unitarni operator, i to je razlog da taj rastav nazivamo polarnim. Posebno, prikazu $0 = 0 \cdot e^{i\varphi}$, gdje φ nije jedinstven, odgovara prikaz $n = n \circ u$ nuloperatora, u kojem je operator u također neodređen. Nastavljajući tu analogiju, promatrajmo razlomljenu linearnu funkciju

$$z \mapsto w = \frac{z - i}{z + i} . \tag{5}$$

Lako se vidi da je u slučaju kad je z realni broj, $|w| = 1$. Na razini operatora, funkciji (5) odgovara operatorska funkcija

$$f \mapsto g = (f + ie)^{-1} \circ (f - ie) ,$$

gdje smo s e označili jedinični operator. Pritom očekujemo da će u slučaju kad je f hermitski, operator g biti unitaran. Pokazat ćemo da je ta hipoteza zaista točna.

TEOREM 8

Neka je U kompleksni unitarni prostor, a h hermitski operator definiran na tom prostoru. Onda je operator $h + ie$ regularan. Nadalje, operator u dan formulom

$$u = (h + ie)^{-1} \circ (h - ie) , \tag{6}$$

jest unitaran, sa svojstvenim vrijednostima različitim od 1.

Dokaz

Kako su svojstvene vrijednosti hermitskog operatora realne, $\lambda = -i$ ne može biti nula karakterističnog polinoma k_h operatora h. Prema tome je operator $h+ie$ regularan pa ima inverz, i u iz relacije (6) je dobro definirani operator. Pokažimo da je u unitaran. Primijetimo najprije da iz očigledne komutativnosti

$$(h - ie) \circ (h + ie) = (h + ie) \circ (h - ie)$$

odmah slijedi i komutativnost

$$(h - ie) \circ (h + ie)^{-1} = (h + ie)^{-1} \circ (h - ie) \,. \tag{7}$$

Nađimo operator u^* adjungiran operatoru u. Vrijedi

$$\begin{aligned} u^* &= (h - ie)^* \circ [(h + ie)^{-1}]^* = \\ &= (h - ie)^* \circ [(h + ie)^*]^{-1} = (h + ie) \circ (h - ie)^{-1} \,. \end{aligned}$$

Tada je zbog (7)

$$\begin{aligned} u^* \circ u &= (h + ie) \circ (h - ie)^{-1} \circ (h + ie)^{-1} \circ (h - ie) = \\ &= (h + ie) \circ (h - ie)^{-1} \circ (h - ie) \circ (h + ie)^{-1} = e \,, \end{aligned}$$

pa je u unitaran operator. Ako od obje strane u (6) oduzmemo operator e i novu relaciju slijeva pomnožimo s $h + ie$, dobivamo

$$(h + ie) \circ (u - e) = -2ie \,,$$

odakle slijedi da je

$$u - e = -2i(h + ie)^{-1} \,.$$

Prema tome je operator $u - e$ regularan,

$$(u - e)^{-1} = -\frac{1}{2i}(h + ie) \,,$$

pa $\lambda = 1$ ne može biti svojstvena vrijednost operatora u. ■

Posve analogno se dokazuje

TEOREM 9

Neka je U kompleksni unitarni prostor, a u bilo koji unitarni operator na U, koji nema $\lambda = 1$ kao svojstvenu vrijednost. Onda je $u - e$ regularni operator, a operator h dan formulom

$$h = -i(u - e)^{-1} \circ (u + e) \tag{8}$$

jest hermitski. ■

Nije teško uvjeriti se da su (6) i (8) različiti oblici iste formule: u (6) je u izražen pomoću h, a u (8) obratno. Prema tome, Tm. 9 je zapravo obrat Tm. 8.

Formulama (6) i (8) uspostavljena je bijektivna korespondencija između skupa svih hermitskih operatora na prostoru U i skupa svih unitarnih operatora na tom prostoru, koji nemaju $\lambda = 1$ u svom spektru. Analogno se vidi da je formulama

$$u = (ie - h)^{-1} \circ (ie + h) \,, \tag{9}$$

odnosno

$$h = i(u + e)^{-1} \circ (u - e) \,, \tag{10}$$

uspostavljena bijektivna korespondencija između skupa svih hermitskih operatora na U i skupa svih unitarnih operatora na U, koji nemaju $\lambda = -1$ u svom spektru.

Formule (6) i (8), odnosno (9) i (10), nazivaju se **Cayleyjeve transformacijske formule**.

U slučaju kad je U realni prostor, navedene se formule ne mogu primijeniti neposredno nego zahtijevaju modifikaciju (vidi Zad. 4.).

Na kraju navodimo još jednu mogućnost dekompozicije koja je primjenjiva samo na normalne operatore. U toj se dekompoziciji operator prikazuje kao linearna kombinacija posebno jednostavnih operatora, projektora.

Pojam ortogonalnog projektora $p : U \to L$ unitarnog prostora U na potprostor L definirali smo u točki 12.10. Tada smo utvrdili da je projektor hermitski operator, $p^* = p$, i da ima svojstvo idempotentnosti, $p^2 = p$. I više, dokazali smo da ta svojstva karakteriziraju projektore među linearnim operatorima (Tm. 7 u 12.10.).

Neka su $L, M < U$ potprostori od U, a $p : U \to L$, $q : U \to M$ pripadni projektori. Kažemo da je **projektor p ortogonalan na projektor q** ako je

$$p \circ q = n \,,$$

gdje je n nuloperator. Relacija "biti ortogonalan" je očito simetrična jer imamo

$$q \circ p = q^* \circ p^* = (p \circ q)^* = n^* = n \,,$$

pa govorimo o **paru međusobno ortogonalnih projektora**.

PROPOZICIJA 10

Projektori p i q su međusobno ortogonalni ako i samo ako su potprostori L i M ortogonalni.

Dokaz

Neka je $p \circ q = n$ i nadalje $a \in L$, $b \in M$ bilo koji vektori. Onda je

$$\begin{aligned}(a,b) &= (p(a), q(b)) = (a, (p^* \circ q)(b)) = \\ &= (a, (p \circ q)(b)) = (a, \Theta) = 0\,,\end{aligned}$$

pa je $L \perp M$. Obratno, ako su potprostori L i M ortogonalni, a $x \in U$ bilo koji vektor, onda je $q(x) \in M$ i $(p \circ q)(x) = p[q(x)] = \Theta$, dakle $p \circ q = n$. ■

Neka je $f : U \to U$ linearni operator, a

$$f = \lambda_1 p_1 + \cdots + \lambda_s p_s \tag{11}$$

prikaz tog operatora s ovim svojstvima:

(1) $\lambda_1, \ldots, \lambda_s$ su međusobno različiti skalari iz pripadnog polja;

(2) $p_1, \ldots, p_s$ su u parovima ortogonalni projektori definirani na U, različiti od nuloperatora;

(3) Vrijedi $p_1 + \cdots + p_s = e$, gdje je e jedinični operator.

Onda kažemo da je (11) jedan **spektralni rastav** (**dekompozicija**) operatora f ili, također, **spektralna forma** (**reprezentacija**, **prikaz**) tog operatora.

TEOREM 11

Operator $f : U \to U$, na kompleksnom unitarnom prostoru U, dopušta spektralnu dekompoziciju ako i samo ako je normalan.

Dokaz

Pretpostavimo da f dopušta prikaz (11). Kako su projektori hermitski operatori, adjungiranjem dobivamo

$$f^* = \overline{\lambda_1} p_1 + \cdots + \overline{\lambda_s} p_s\,.$$

Odatle je, uzimajući u obzir ortogonalnost projektora,

$$\begin{aligned}f \circ f^* &= \left(\sum_{i=1}^{s} \lambda_i p_i\right) \circ \left(\sum_{j=1}^{s} \overline{\lambda_j} p_j\right) = \sum_{i=1}^{s}\sum_{j=1}^{s} \lambda_i \overline{\lambda_j} p_i \circ p_j = \\ &= \sum_{i=1}^{s} \lambda_i \overline{\lambda_i} p_i^2 = \sum_{i=1}^{s} \overline{\lambda_i} \lambda_i p_i^2 = \sum_{j=1}^{s}\sum_{i=1}^{s} \overline{\lambda_j} \lambda_i p_j \circ p_i = \\ &= \left(\sum_{j=1}^{s} \overline{\lambda_j} p_j\right) \circ \left(\sum_{i=1}^{s} \lambda_i p_i\right) = f^* \circ f\,,\end{aligned}$$

i prema tome je f normalan.

Obratno, neka je f normalan operator. Kako je prostor U kompleksan, prema Prop. 8 iz 13.6. postoji ortonormirana baza $E = (e_1, \ldots, e_n)$ za U, koja se sastoji od svojstvenih vektora operatora f. Neka je s $L_i < U$, $i = 1, \ldots, s$, označen potprostor razapet onim vektorima baze koji su pridruženi istoj svojstvenoj vrijednosti λ_i operatora f. Očito, svi vektori iz L_i su onda svojstveni, pridruženi svojstvenoj vrijednosti λ_i. Kako isti svojstveni vektor ne može biti pridružen različitim svojstvenim vrijednostima, odmah zaključujemo da je

$$U = L_1 \oplus L_2 \oplus \cdots \oplus L_s \,,$$

i pritom je ta direktna suma ortogonalna, tj. potprostori $L_1, \ldots, L_s$ su u parovima ortogonalni. Neka je

$$p_i : U \to L_i$$

projektor na L_i, $i = 1, \ldots, s$. Prema Prop. 10 projektori $p_1, \ldots, p_s$ su u parovima ortogonalni. Ako je $a \in U$ bilo koji vektor, on dopušta jednoznačan prikaz $a = a_1 + \cdots + a_s$, gdje su $a_i \in L_i$. Onda je

$$(p_1 + \cdots + p_s)(a) = p_1(a) + \cdots + p_s(a) = a_1 + \cdots + a_s = a \,,$$

pa je

$$p_1 + \cdots + p_s = e \,.$$

Time smo provjerili da projektori p_i zadovoljavaju uvjete (2) i (3) iz definicije spektralnog prikaza. Treba još vidjeti da se f zaista može prikazati kao linearna kombinacija tih projektora. No, za $a \in U$ imamo

$$a = p_1(a) + \cdots + p_s(a) \,, \tag{12}$$

i pritom je $p_i(a) \in L_i$, $i = 1, \ldots, s$. Kako su svi vektori iz L_i svojstveni za f i pridruženi svojstvenoj vrijednosti λ_i, vrijedi

$$f[p_i(a)] = \lambda_i p_i(a) \,.$$

Iz (12) je onda

$$\begin{aligned} f(a) &= f[p_1(a) + \cdots + p_s(a)] = f[p_1(a)] + \cdots + f[p_s(a)] = \\ &= \lambda_1 p_1(a) + \cdots + \lambda_s p_s(a) = (\lambda_1 p_1 + \cdots + \lambda_s p_s)(a) \,, \end{aligned}$$

za svaki a, pa je

$$f = \lambda_1 p_1 + \cdots + \lambda_s p_s \,,$$

gdje su $\lambda_1, \ldots, \lambda_s$ međusobno različiti skalari (svojstvene vrijednosti operatora f). ■

Time je dokazana egzistencija spektralne dekompozicije za normalne operatore.

PROPOZICIJA 12

Neka je

$$f = \lambda_1 p_1 + \cdots + \lambda_s p_s$$

bilo koja spektralna dekompozicija operatora f. Onda je $\{\lambda_1, \ldots, \lambda_s\}$ skup svih različitih svojstvenih vrijednosti tog operatora (njegov spektar!).

Dokaz

Najprije ćemo pokazati da je svaki koeficijent λ_i svojstvena vrijednost operatora f. Kako je, po pretpostavci, projekcija p_i različita od nuloperatora, postoji $a \in U$, $a \neq \Theta$, takav da je $p_i(a) \neq \Theta$. Onda je, zbog ortogonalnosti i idempotentnosti projektora,

$$f[p_i(a)] = \lambda_1 p_1[p_i(a)] + \cdots + \lambda_i p_i[p_i(a)] + \cdots + \lambda_s p_s[p_i(a)] = \lambda_i p_i(a),$$

što pokazuje da je λ_i svojstvena vrijednost operatora f.

Obratno, neka je μ bilo koja svojstvena vrijednost od f, i $a \neq \Theta$ takav da je $f(a) = \mu a$. Iz svojstva (3) spektralnog prikaza imamo

$$a = p_1(a) + \cdots + p_s(a)\ . \tag{13}$$

Kako je

$$f(a) = \lambda_1 p_1(a) + \cdots + \lambda_s p_s(a)\ , \tag{14}$$

iz relacija (13) i (14) slijedi

$$\lambda_1 p_1(a) + \cdots + \lambda_s p_s(a) = \mu p_1(a) + \cdots + \mu p_s(a)\ .$$

Primijenimo p_i na obje strane te relacije. Zbog ortogonalnosti projektora i idempotentnosti dobivamo

$$\lambda_i p_i(a) = \mu p_i(a)\ ,$$

odnosno

$$(\lambda_i - \mu) p_i(a) = \Theta\ , \tag{15}$$

za svaki $i = 1, \ldots, s$. Budući da je $a \neq \Theta$, bar jedan od sumanada u (13) mora biti različit od nulvektora. Ako je $p_j(a) \neq \Theta$, za neki $j = 1, \ldots, s$, iz (15) slijedi da je $\lambda_j - \mu = 0$, dakle $\mu = \lambda_j$ i tvrdnja je dokazana. ■

Ostaje nam pokazati jedinstvenost spektralne dekompozicije. U tu svrhu potrebna nam je

LEMA 13

Neka je

$$f = \lambda_1 p_1 + \cdots + \lambda_s p_s$$

spektralna dekompozicija operatora f, a

$$\varphi(t) = \alpha_m t^m + \cdots + \alpha_1 t + \alpha_0$$

bilo koji polinom. Onda je

$$\varphi(f) = \varphi(\lambda_1)p_1 + \cdots + \varphi(\lambda_s)p_s.$$

Dokaz

Indukcijom imamo

$$\begin{aligned} e &= p_1 + \cdots + p_s \,, \\ f &= \lambda_1 p_1 + \cdots + \lambda_s p_s \,, \end{aligned}$$

$$\begin{aligned} f^2 &= (\sum_{i=1}^{s} \lambda_i p_i) \circ (\sum_{j=1}^{s} \lambda_j p_j) = \sum_{i=1}^{s}\sum_{j=1}^{s} \lambda_i \lambda_j p_i \circ p_j = \\ &= \lambda_1^2 p_1 + \cdots + \lambda_s^2 p_s \,, \end{aligned}$$

te

$$\begin{aligned} f^m &= f^{m-1} \circ f = (\sum_{i=1}^{s} \lambda_i^{m-1} p_i) \circ (\sum_{j=1}^{s} \lambda_j p_j) = \\ &= \sum_{i=1}^{s}\sum_{j=1}^{s} \lambda_i^{m-1} \lambda_j p_i \circ p_j = \lambda_1^m p_1 + \cdots + \lambda_s^m p_s \,. \end{aligned}$$

Ako te relacije pomnožimo redom s $\alpha_0, \ldots, \alpha_m$ i zatim zbrojimo, dobivamo traženi rezultat. ■

TEOREM 14

Normalni operator dopušta jednu i samo jednu spektralnu dekompoziciju. Pritom su koeficijenti u toj dekompoziciji sve međusobno različite svojstvene vrijednosti operatora.

Dokaz

Egzistenciju dekompozicije smo dokazali u Tm. 11, pa ostaje dokazati jedinstvenost. Neka je

$$f = \lambda_1 p_1 + \cdots + \lambda_s p_s \tag{16}$$

bilo koja spektralna dekompozicija normalnog operatora f. Prema Prop. 12, koeficijenti λ_i u toj dekompoziciji su elementi spektra od f i, prema tome, određeni su jednoznačno. Tvrdimo da je p_i u prikazu (16) nužno oblika

$$p_i = \frac{(f - \lambda_1 e) \circ \cdots \circ (f - \lambda_{i-1} e) \circ (f - \lambda_{i+1} e) \circ \cdots \circ (f - \lambda_s e)}{(\lambda_i - \lambda_1) \cdots (\lambda_i - \lambda_{i-1})(\lambda_i - \lambda_{i+1}) \cdots (\lambda_i - \lambda_s)} \,, \tag{17}$$

za svaki $i = 1, \ldots, s$. Ako to pokažemo, zbog jedinstvenosti koeficijenata λ_i, jedinstvenost spektralnog prikaza je dokazana.

Promatrajmo polinom

$$\varphi_i(t) = \frac{(t-\lambda_1)\cdots(t-\lambda_{i-1})(t-\lambda_{i+1})\cdots(t-\lambda_s)}{(\lambda_i-\lambda_1)\cdots(\lambda_i-\lambda_{i-1})(\lambda_i-\lambda_{i+1})\cdots(\lambda_i-\lambda_s)}\,, \qquad (18)$$

za $i = 1, \ldots, s$. Prema Lemi 13 je

$$\varphi_i(f) = \varphi_i(\lambda_1)p_1 + \cdots + \varphi_i(\lambda_i)p_i + \cdots + \varphi_i(\lambda_s)p_s\,.$$

No, iz (18) vidimo da je $\varphi_i(\lambda_j) = 0$ za $j \neq i$, a $\varphi_i(\lambda_i) = 1$, pa je

$$\varphi_i(f) = p_i\,,$$

i relacija (17) je verificirana. ■

Jasno je odakle dolazi naziv spektralna dekompozicija. Naime, koeficijenti u toj dekompoziciji su svojstvene vrijednosti operatora, koje čine njegov spektar.

Kao neposrednu posljedicu prethodnih teorema imamo (vidi i Zad. 17. u 13.6.)

KOROLAR 15

Normalni operator je:

(1) *hermitski ako i samo ako je njegov spektar realan;*

(2) *antihermitski ako i samo ako je njegov spektar čisto imaginaran;*

(3) *unitaran ako i samo ako se njegov spektar sastoji od brojeva modula jednakog* 1.

Dokaz

Dokažimo npr. (1). Neka je

$$f = \lambda_1 p_1 + \cdots + \lambda_s p_s$$

bilo koji normalni operator, a

$$f^* = \overline{\lambda_1} p_1 + \cdots + \overline{\lambda_s} p_s$$

njemu adjungirani operator. Iz jedinstvenosti spektralnog prikaza onda slijedi da će operator f biti hermitski, $f^* = f$, ako i samo ako je $\overline{\lambda_i} = \lambda_i$, za sve $i = 1, \ldots, s$, tj. ako i samo ako je njegov spektar realan. ■

ZADACI

1. Dokaži da svaka kompleksna kvadratna matrica A ima jedinstveni prikaz $A = G + iH$, gdje su G i H hermitske matrice.

2. Dokaži: Svaka se kompleksna (realna) kvadratna matrica A može faktorizirati u $A = HU$, gdje je H hermitska (simetrična), a U unitarna (ortogonalna) matrica. Pritom se može postići da H ima nenegativne svojstvene vrijednosti.

3. Uspostavi bijektivnu korespondenciju između unitarnih operatora koji nemaju $\lambda = 1$ u svom spektru i onih koji u svom spektru nemaju $\lambda = -1$. [Uputa: Eliminiraj h iz formula (6) i (9).]

4. Dokaži ovu modifikaciju Tm. 8 i Tm. 9, koja daje jedan tip Cayleyjevih formula, istinit i u realnom i u kompleksnom prostoru: Neka je k antihermitski operator. Onda su operatori $k \pm e$ regularni. Nadalje, operator
$$u = (k + e)^{-1} \circ (k - e) \tag{19}$$
jest unitaran, sa svojstvenim vrijednostima različitim od 1. Pritom je operator k izražen pomoću u formulom
$$k = -(u - e)^{-1} \circ (u + e)\,. \tag{20}$$
Obratno, ako je u unitarni operator sa svojstvenim vrijednostima različitim od 1, operator $u - e$ je regularan. Operator dan s (20) je antihermitski, a u je izražen pomoću k formulom (19).

5. Napiši i diskutiraj Cayleyjeve formule za matrice (vidi Zad. 17. u 13.5.).

6. Dokaži da je svaki ortogonalni projektor pozitivan operator.

7. Operator $f : U \to U$ je projektor ako i samo ako postoji ortonormirana baza U, u kojoj f ima zapis
$$\begin{bmatrix} 1 & & & & & O \\ & \ddots & & & & \\ & & 1 & & & \\ & & & 0 & & \\ & & & & \ddots & \\ O & & & & & 0 \end{bmatrix}.$$
Dokaži!

8. Neka su $p_L : U \to M$ i $p_L : U \to L$ projektori. Dokaži:
   (a) Suma $p_L + p_M$ je projektor ako i samo ako je $p_L \circ p_M = n$. U tom je slučaju $p_L + p_M = p_{L+M}$.
   (b) Produkt $p_L p_M$ je projektor ako i samo ako projektori komutiraju. U tom je slučaju $p_L \circ p_M = p_{L \cap M}$.
   (c) L je potprostor od M, $L < M$, ako i samo ako je $p_M \circ p_L = p_L$.
9. Dokaži da je za svaki $L < U$ ispunjeno
$$p_L + p_{L^\perp} = e \, .$$
10. $L < U$ je f-invarijantni potprostor ako i samo ako je $p_L \circ f \circ p_L = f \circ p_L$. Dokaži!
11. Neka su $\sum_i \lambda_i p_i$ i $\sum_j \mu_j q_j$ spektralni prikazi operatora f i g. Ako f i g komutiraju, dokaži da i svaki p_i komutira sa svakim q_j.
12. Ako normalni operator f komutira s linearnim operatorom g, onda on komutira i s g^*. Dokaži!

13.8. Funkcionali na unitarnom prostoru

Linearne funkcionale smo definirali i detaljno izučavali u točki 8.7. Sada ćemo reći nešto više o tim funkcionalima u slučaju kad im je domena unitarni prostor.

Neka je U unitarni prostor, a $a \in U$ bilo koji vektor. Onda definiramo funkcional
$$l_a : U \to F \, ,$$
stavljajući
$$l_a(x) = (x, a) \, ,$$
za svaki $x \in U$.

PROPOZICIJA 1

Za svaki $a \in U$ je funkcional l_a linearan. Nadalje, ako je $a \neq b$, onda su i funkcionali l_a i l_b različiti.

Dokaz

Iz svojstava skalarnog produkta imamo
$$\begin{aligned} l_a(\alpha x + \beta y) &= (\alpha x + \beta y, a) = \alpha(x, a) + \beta(y, a) = \\ &= \alpha l_a(x) + \beta l_a(y) \, , \end{aligned}$$

pa je l_a linearni funkcional. Kad bi, uz $a \neq b$, bilo $l_a = l_b$, imali bismo $(x, a) = (x, b)$, odnosno $(x, a-b) = 0$, za svaki $x \in U$. No, to odmah povlači $a - b = \Theta$, dakle $a = b$, što je kontradikcija. ■

Zanimljivo je, međutim, da vrijedi i obrat, tj. da se svaki linearni funkcional na unitarnom prostoru može dobiti na opisani način.

TEOREM 2

Neka je $l : U \to F$ bilo koji linearni funkcional. Onda postoji i jednoznačno je određen vektor $a \in U$ takav da je

$$l = l_a \, .$$

Dokaz

Neka je $N < U$ jezgra funkcionala l, a $M = N^{\perp}$ njezin ortogonalni komplement,

$$U = N \oplus M \, . \tag{1}$$

Kako je za funkcionale uvijek $\dim N \geq \dim U - 1$, to je $\dim M \leq 1$.

Ako je $\dim M = 0$, bit će $N = U$, pa je $l(x) = 0 = (x, \Theta)$ za sve $x \in U$, odakle slijedi da je $a = \Theta$ i $l = l_\Theta$. Pretpostavimo zato da je $\dim M = 1$. Neka je $\{e\}$ ortonormirana baza za M. Ako je $m \in M$ bilo koji vektor, možemo pisati $m = \lambda e$ i pritom je $\lambda = (m, e)$.

Iz (1) slijedi da svaki vektor $x \in U$ ima jednoznačan prikaz oblika

$$x = n + m \, ,$$

gdje je $n \in N$, a $m \in M$. Kako je $M \perp N$, imamo

$$(x, e) = (n + m, e) = (m, e) \, , \tag{2}$$

i onda redom, uzimajući u obzir prikaz od m i relaciju (2),

$$\begin{aligned} l(x) &= l(n+m) = l(n) + l(m) = l(m) = l[(m,e)e] = \\ &= (m,e)l(e) = (x,e)l(e) = (x, \overline{l(e)}e) = (x,a) = l_a(x) \, , \end{aligned}$$

za svaki $x \in U$, pa je $l = l_a$, gdje je $a = \overline{l(e)}e$.

Jednoznačnost slijedi iz Prop. 1, čime je teorem dokazan. ■

Kako smo već spomenuli i obećali (vidi Prop. 3 u 13.4.), sada ćemo pomoću Tm. 2 lako dokazati egzistenciju adjungiranog operatora.

KOROLAR 3

Za svaki linearni operator $f : U \to U$, na unitarnom prostoru U, postoji adjungirani operator f^*.

Dokaz

Neka je $y \in U$ bilo koji vektor. Definirajmo funkcional

$$l : U \to F$$

stavljajući

$$l(x) = (f(x), y) \ . \tag{3}$$

Kako je

$$\begin{aligned} l(\alpha x_1 + \beta x_2) &= (f(\alpha x_1 + \beta x_2), y) = (\alpha f(x_1) + \beta f(x_2), y) = \\ &= \alpha(f(x_1), y) + \beta(f(x_2), y) = \alpha l(x_1) + \beta l(x_2), \end{aligned}$$

funkcional l je linearan, pa prema Tm. 2 postoji $a \in U$ takav da je $l = l_a$, tj.

$$l(x) = l_a(x) = (x, a) \ . \tag{4}$$

Pritom je vektor a jednoznačno određen funkcionalom l, dakle operatorom f i vektorom y. Prema tome, uz fiksni f imamo dobro definirano preslikavanje

$$f^* : U \to U$$

dano s

$$f^*(y) = a \ , \tag{5}$$

za svaki $y \in U$. Uspoređujući (3) i (4), zbog (5) onda imamo

$$(f(x), y) = (x, a) = (x, f^*(y)) \ ,$$

pa je f^* adjungirani operator od f po definiciji. ■

Neka je sada U^* dualni prostor za prostor U (vidi točku 8.7.). Onda nam se prirodno nameće operator

$$\Psi : U \to U^*$$

definiran s

$$\Psi(a) = l_a \ .$$

PROPOZICIJA 4

Ako je U realni unitarni prostor, Ψ je izomorfizam linearnih prostora. Ako je pak U kompleksni unitarni prostor, Ψ je antiizomorfizam linearnih prostora.

Dokaz

Iz Prop. 1 i Tm. 2 slijedi da je Ψ bijektivno preslikavanje. Nadalje, za svaki $x \in U$ imamo

$$l_{a+b}(x) = (x, a+b) = (x, a) + (x, b) = l_a(x) + l_b(x) = (l_a + l_b)(x)$$

i

$$l_{\alpha a}(x) = (x, \alpha a) = \overline{\alpha}(x, a) = \overline{\alpha}\, l_a(x) .$$

Zato vrijedi

$$\Psi(a+b) = l_{a+b} = l_a + l_b = \Psi(a) + \Psi(b)$$

i

$$\Psi(\alpha a) = l_{\alpha a} = \overline{\alpha} l_a = \overline{\alpha}\, \Psi(a) ,$$

što pokazuje da je Ψ antilinearni operator (vidi Zad. 9. u 13.1.). Ako je U realni prostor, onda je $\overline{\alpha} = \alpha$, pa je Ψ linearan. Prema tome, Ψ je zaista izomorfizam, odnosno antiizomorfizam. ■

Pomoću preslikavanja Ψ možemo na dualnom prostoru definirati unitarnu strukturu. Za svaki izbor $l_a, l_b \in U^*$ definiramo

$$(l_a, l_b) = (\Psi^{-1}(l_b), \Psi^{-1}(l_a)) = (b, a) ,$$

i to množenje nazivamo **dualni skalarni produkt**.

PROPOZICIJA 5

Dualni prostor U^* je uz dualni skalarni produkt unitarni prostor.

Dokaz

Provjerimo npr. kvaziasocijativnost,

$$(\lambda l_a, l_b) = \lambda (l_a, l_b) .$$

Kako je Ψ^{-1} antiizomorfizam, imamo

$$\begin{aligned} \Psi^{-1}(\lambda l_a) &= \Psi^{-1}(\lambda \Psi(a)) = (\Psi^{-1} \circ \Psi)(\overline{\lambda} a) = \\ &= \overline{\lambda} a = \overline{\lambda} \Psi^{-1}(l_a) , \end{aligned}$$

pa je

$$\begin{aligned} (\lambda l_a, l_b) &= (\Psi^{-1}(l_b), \Psi^{-1}(\lambda l_a)) = (\Psi^{-1}(l_b), \overline{\lambda} \Psi^{-1}(l_a)) = \\ &= \lambda (\Psi^{-1}(l_b), \Psi^{-1}(l_a)) = \lambda (l_a, l_b) , \end{aligned}$$

što se i tvrdilo. ■

Prostor U^*, snabdjeven unitarnom strukturom pomoću dualnog skalarnog produkta, nazivamo **dualni unitarni prostor** prostora U.

Primijetimo da očito vrijedi

$$(\Psi(a), \Psi(b)) = (b, a) ,$$

tj. Ψ je **antiunitarni operator** (Zad. 9. u 13.1.) i prema tome **antiunitarni antiizomorfizam**. U realnom slučaju skalarno množenje je komutativno, pa je Ψ unitarni izomorfizam, izomorfizam unitarnih prostora.

Ako su

$$\Psi_1 : U \to U^* \quad , \quad \Psi_2 : U^* \to (U^*)^*$$

upravo spomenuti antiunitarni antiizomorfizmi, odmah vidimo da će vrijediti

KOROLAR 6

Kompozicija $\Phi = \Psi_2 \circ \Psi_1$ je unitarni izomorfizam između prostora U i njegova biduala U^{**}. ■

Kako su Ψ_i, $i = 1, 2$, definirani prirodno, tj. bez posredovanja baze, i $\Phi : U \to U^{**}$ je prirodni izomorfizam. Nije teško vidjeti da se taj izomorfizam podudara s prirodnim izomorfizmom definiranim u 8.7. (vidi i Zad. 3.).

Završno vrijedi još

PROPOZICIJA 7

Za svaku ortonormiranu bazu u U je dualna baza u U^* također ortonormirana.

Dokaz

Neka je $E = (e_1, \ldots, e_n)$ ortonormirana baza za U, a $E^* = (l_1, \ldots, l_n)$ njoj dualna baza u U^*. Po definiciji (vidi točku 8.7.), to znači da je

$$l_j(e_k) = \begin{cases} 1, & k = j \\ 0, & k \neq j \end{cases} ,$$

za svaki $j = 1, \ldots, n$. Onda imamo

$$l_j(e_k) = \delta_{jk} = \delta_{kj} = (e_k, e_j) = l_{e_j}(e_k) ,$$

za svaki k, odakle odmah slijedi da je $l_j = l_{e_j}$, za $j = 1, \ldots, n$. Tada je

$$(l_i, l_j) = (l_{e_i}, l_{e_j}) = (\Psi^{-1}(l_{e_j}), \Psi^{-1}(l_{e_i})) = (e_j, e_i) = \delta_{ji} ,$$

pa je dualna baza zaista ortonormirana. ■

ZADACI

1. Neka je $f : U \to U$ linearni operator, a $\widehat{f} : U^* \to U^*$ njemu **dualni operator**, definiran s $\widehat{f}(l) = l \circ f$, za svaki $l \in U^*$ (vidi Zad. 13. u 8.7.). Neka je $f^* : U \to U$ operator definiran s $f^* = \Psi^{-1} \circ \widehat{f} \circ \Psi$ (vidi dijagram).

$$\begin{array}{ccc} U & \underset{f^*}{\overset{f}{\rightleftarrows}} & U \\ {\scriptstyle\Psi}\downarrow & & \downarrow{\scriptstyle\Psi} \\ U^* & \overset{\widehat{f}}{\leftarrow} & U^* \end{array}$$

   Pokaži da je operator f^* linearan. Pokaži nadalje, da je f^* zapravo adjungirani operator od f. To je alternativna definicija tog operatora. [Uputa: Pokaži da je $[(\widehat{f} \circ \Psi)(b)](a) = (f(a), b)$ i $[(\Psi \circ f^*)(b)](a) = (a, f^*(b))$.]

2. Ako je $f : U \to U$ unitarni (hermitski, antihermitski, normalni) operator, je li takav i njemu dualni operator?

3. Pokaži da prirodni izomorfizam $\Phi : U \to U^{**}$ iz točke 8.7. čuva skalarni produkt. Uvjeri se, nadalje, da se taj Φ podudara s izomorfizmom $\Phi = \Psi_2 \circ \Psi_1$ iz Kor. 6. [Uputa: $[(\Psi_2 \circ \Psi_1)(a)](l_x) = [\Psi_2(l_a)](l_x) = (l_x, l_a) = (a, x) = l_x(a)$.]

4. Neka je V realni linearni prostor, a V^* njegov dual. Neka je $f : V \to V^*$ izomorfizam, koji preslikava bazu u V na njoj dualnu bazu. Pokaži da je s

$$(a, b) = [f(b)](a) ,$$

   za $a, b \in V$, definiran skalarni produkt na V. Formuliraj analognu tvrdnju za slučaj kad je V kompleksni linearni prostor.

14

BILINEARNI I KVADRATNI FUNKCIONALI. FORME

Ovo je završno poglavlje iz linearne algebre u kojem, zaokružujući tu teoriju, ukratko govorimo o raznim poopćenjima i primjeni prethodno definiranih pojmova i dokazanih rezultata. Najprije izučavamo bilinearne i kvadratne funkcionale te njihove prikaze u danoj bazi - bilinearne, odnosno kvadratne forme. Zatim, poopćujući pojam unitarnog prostora, definiramo pseudounitarni prostor i, još općenitije, prostor s hermitskom bilinearnom ili čak samo bilinearnom metrikom. Na kraju poglavlja dani su elementi geometrije linearnog prostora.

14.1. Bilinearni funkcionali

U ovom poglavlju ćemo radi jednostavnosti pretpostaviti da je s F označeno polje realnih ili kompleksnih brojeva. Većinu rezultata nije, međutim, teško modificirati i generalizirati na slučaj kad je F bilo koje polje čija karakteristika nije 2.

Neka su, dakle $V_1, \ldots, V_r$ linearni prostori nad istim poljem F realnih ili kompleksnih brojeva, a

$$\varphi : V_1 \times V_2 \times \cdots \times V_r \to F$$

funkcional koji je linearan u svakoj od varijabli zasebno, tj. pridruženje

$$(a_1, \ldots, a_{i-1}, x, a_{i+1}, \ldots, a_r) \mapsto \alpha \in F$$

koje je uz bilo koje, ali fiksne $a_j \in V_j$, $j = 1, \ldots, i-1, i+1, \ldots, r$, linearno u x, za svaki $i = 1, \ldots, r$. Onda kažemo da je φ **multilinearni** ili **r-linearni funkcional**.

U slučaju $r = 1$, φ je, dakako, linearni funkcional, kad je $r = 2$, govorimo o **bilinearnom funkcionalu**, kad je $r = 3$, o trilinearnom, itd. Primijetimo da za $r > 1$ φ nije linearni funkcional na prostoru $V_1 \times \cdots \times V_r$.

Nas će posebno zanimati slučaj kad je $r = 2$ i $V_1 = V_2 = V$, dakle **bilinearni funkcionali na** danom **prostoru** V. U skladu s općom definicijom, to je funkcional

$$\varphi : V \times V \to F$$

za koji vrijedi:

(1) biaditivnost, tj.

$$\varphi(x_1 + x_2, y) = \varphi(x_1, y) + \varphi(x_2, y)$$

$$\varphi(x, y_1 + y_2) = \varphi(x, y_1) + \varphi(x, y_2), \text{ i}$$

(2) bihomogenost, tj.

$$\varphi(\alpha x, y) = \alpha\, \varphi(x, y)$$

$$\varphi(x, \beta y) = \beta\, \varphi(x, y)\ ,$$

gdje su $x, y, x_i, y_i \in V$ bilo koji vektori, a $\alpha, \beta \in F$ skalari. Uvjete (1) i (2) možemo objediniti pa uzeti

$$\begin{aligned}&\varphi(\alpha_1 x_1 + \alpha_2 x_2, \beta_1 y_1 + \beta_2 y_2) = \\ &\quad = \alpha_1\beta_1\, \varphi(x_1, y_1) + \alpha_1\beta_2\, \varphi(x_1, y_2) + \alpha_2\beta_1\, \varphi(x_2, y_1) + \alpha_2\beta_2\, \varphi(x_2, y_2)\end{aligned} \tag{3}$$

kao definicijsku relaciju za bilinearni funkcional.

Ako je npr. $V = \mathbb{R}^n$, a $x = (\alpha_i)$ i $y = (\beta_i)$ bilo koji vektori iz $\mathbb{R}^n$, preslikavanje dano s

$$\varphi(x, y) = \sum_{i=1}^{n} \alpha_i \beta_i\ ,$$

tj. standardni skalarni produkt na $\mathbb{R}^n$ je bilinearni funkcional na $\mathbb{R}^n$. Slično, uz $V = \mathbb{R}_{[0,1]}$ je $\varphi : V \times V \to \mathbb{R}$,

$$\varphi(f, g) = \int_0^1 f(t)\, g(t)\, \mathrm{d}t\ ,$$

bilinearni funkcional na tom prostoru. Uopće, svaki je skalarni produkt na realnom prostoru primjer bilinearnog funkcionala.

Pokažimo egzistenciju i jedinstvenost bilinearnog funkcionala.

PROPOZICIJA 1

Neka je $(a_1, \ldots, a_n)$ *baza prostora* V, *a* $\alpha_{ij} \in F$, $i, j = 1, \ldots, n$, *bilo koji izbor od* n^2 *skalara. Onda postoji jedan i samo jedan bilinearni funkcional*

$$\varphi : V \times V \to F$$

za koji vrijedi

$$\varphi(a_i, a_j) = \alpha_{ij} \ ,$$

za sve $i, j = 1, \ldots, n$.

Dokaz

Neka su $x, y \in V$ bilo koji vektori, a $x = \sum_{i=1}^{n} x_i a_i$ i $y = \sum_{j=1}^{n} y_j a_j$ njihovi prikazi u danoj bazi. Onda definiramo

$$\varphi(x, y) = \sum_{i=1}^{n} \sum_{j=1}^{n} \alpha_{ij} \, x_i \, y_j \ .$$

Lako se provjeri da je φ bilinearni funkcional i da vrijedi $\varphi(a_i, a_j) = \alpha_{ij}$, pa je egzistencija dokazana. Ako je $\psi : V \times V \to F$ bilo koji bilinearni funkcional sa svojstvom $\psi(a_i, a_j) = \alpha_{ij}$, imamo redom

$$\psi(x, y) = \psi(\sum_{i=1}^{n} x_i a_i, \sum_{j=1}^{n} y_j a_j) = \sum_{i=1}^{n} \sum_{j=1}^{n} x_i y_j \, \psi(a_i, a_j) =$$

$$= \sum_{i=1}^{n} \sum_{j=1}^{n} x_i y_j \alpha_{ij} \ ,$$

pa je $\psi(x, y) = \varphi(x, y)$ za sve $x, y \in V$, čime je dokazana i jedinstvenost. ■

Prema tome, bilinearni funkcional je jednoznačno određen svojim djelovanjem na bazi prostora i u toj bazi ima prikaz

$$\varphi(x, y) = \sum_{i=1}^{n} \sum_{j=1}^{n} \alpha_{ij} x_i y_j \ , \tag{4}$$

gdje za koeficijente vrijedi $\alpha_{ij} = \varphi(a_i, a_j)$. Matricu koeficijenata

$$A = \begin{bmatrix} \alpha_{11} & \cdots & \alpha_{1n} \\ \vdots & & \vdots \\ \alpha_{n1} & \cdots & \alpha_{nn} \end{bmatrix} \tag{5}$$

nazivamo **matrični zapis** ili **matrica bilinearnog funkcionala** φ u danoj bazi. Ako s

$$X = \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} \quad , \quad Y = \begin{bmatrix} y_1 \\ \vdots \\ y_n \end{bmatrix} \tag{6}$$

označimo koordinatne matrice vektora $x, y \in V$ u zadanoj bazi, odmah vidimo da (4) možemo pregledno pisati kao

$$\varphi(x, y) = X' \, A \, Y \, . \tag{7}$$

Postavlja se pitanje kako se mijenja matrica bilinearnog funkcionala pri promjeni baze, tj. u kakvoj su vezi matrični prikazi istog funkcionala u raznim bazama.

PROPOZICIJA 2

Neka su A i B matrice bilinearnog funkcionala φ u bazama $(a_1, \ldots, a_n)$, odnosno $(b_1, \ldots, b_n)$, a T matrica prijelaza iz prve baze u drugu. Onda je

$$B = T' \cdot A \cdot T \ . \tag{8}$$

Dokaz

Označimo $A = [\alpha_{ij}]$, $B = [\beta_{ij}]$ i $T = [\tau_{ij}]$. Prema točki 10.2. je

$$b_k = \sum_{t=1}^{n} \tau_{tk} a_t$$

pa za $i, j = 1, \ldots, n$ imamo

$$\begin{aligned} \beta_{ij} &= \varphi(b_i, b_j) = \varphi(\sum_{r=1}^{n} \tau_{ri} a_r, \sum_{s=1}^{n} \tau_{sj} a_s) = \\ &= \sum_{r=1}^{n} \sum_{s=1}^{n} \tau_{ri} \tau_{sj} \, \varphi(a_r, a_s) = \sum_{r=1}^{n} \sum_{s=1}^{n} \tau_{ri} \, \alpha_{rs} \, \tau_{sj} \ , \end{aligned}$$

odakle odmah vidimo da vrijedi $B = T' \cdot A \cdot T$. ∎

Ako su X_1 i Y_1 koordinatne matrice vektorâ $x, y \in V$ u novoj bazi $(b_1, \ldots, b_n)$, veza s koordinatama u staroj bazi $(a_1, \ldots, a_n)$ je, prema Tm. 1 u 10.2., dana s

$$X = T \, X_1 \quad , \quad Y = T \, Y_1 \ , \tag{9}$$

pa uvažavajući Prop. 2 slijedi

$$\begin{aligned} \varphi(x, y) &= X' \, A \, Y = (T X_1)' \, A \, (T Y_1) = \\ &= X_1' (T' \, A \, T) Y_1 = X_1' \, B \, Y_1 \ , \end{aligned}$$

tj. dobivamo (ispravni) prikaz funkcionala φ u novoj bazi.

Neka su $A, B \in M_n$ kvadratne matrice istog reda. Kažemo da je matrica A **kongruentna** s matricom B, i pišemo $A \cong B$, ako postoji regularna matrica $T \in M_n$ takva da vrijedi $B = T' A T$. Lako se provjeri da je kongruencija matrica relacija ekvivalencije na M_n (vidi Zad. 17. u 9.5.). Prema tome, Prop. 2 možemo formulirati u

KOROLAR 3

Matrični zapisi istog bilinearnog funkcionala u raznim bazama su kongruentne matrice. ■

Kongruentne matrice imaju isti rang (vidi Zad. 12. u 9.6.). Zato možemo definirati **rang bilinearnog funkcionala** kao rang (bilo kojeg) njegova matričnog zapisa. Kažemo da je bilinearni funkcional **regularan**, ako je maksimalnog ranga, tj. ranga jednakog dimenziji prostora V. U protivnom, govorimo o **singularnom** bilinearnom funkcionalu.

Nas će posebno zanimati funkcionali s nekim dodatnim svojstvima. Bilinearni funkcional $\varphi : V \times V \to F$ je **simetričan** ako vrijedi

$$\varphi(y, x) = \varphi(x, y) ,$$

a **antisimetričan** ako je

$$\varphi(y, x) = -\varphi(x, y) ,$$

za sve $x, y \in V$.

PROPOZICIJA 4

Bilinearni funkcional je simetričan ako i samo ako je (svaki) njegov matrični zapis simetrična matrica.

Dokaz

Neka je φ simetrični funkcional, a $A = [\alpha_{ij}]$ njegova matrica u bazi $(a_1, \ldots, a_n)$. Onda je

$$\alpha_{ij} = \varphi(a_i, a_j) = \varphi(a_j, a_i) = \alpha_{ji} ,$$

za svako $i, j = 1, \ldots, n$, pa je $A = A'$, tj. matrica A je simetrična.

Obratno, iz $A = A'$ za $i, j = 1, \ldots, n$ slijedi

$$\varphi(a_i, a_j) = \alpha_{ij} = \alpha_{ji} = \varphi(a_j, a_i) ,$$

i za $x, y \in V$ onda

$$\begin{aligned}\varphi(x,y) &= \varphi(\sum_{i=1}^{n} x_i a_i, \sum_{j=1}^{n} y_j a_j) = \\ &= \sum_{i=1}^{n}\sum_{j=1}^{n} x_i y_j \varphi(a_i, a_j) = \sum_{j=1}^{n}\sum_{i=1}^{n} y_j x_i \varphi(a_j, a_i) = \\ &= \varphi(\sum_{j=1}^{n} y_j a_j, \sum_{i=1}^{n} x_i a_i) = \varphi(y,x)\ ,\end{aligned}$$

pa je funkcional φ simetričan. ■

Slično se dokazuje i

PROPOZICIJA 5

Bilinearni funkcional je antisimetričan ako i samo ako je (svaki) njegov matrični zapis antisimetrična matrica. ■

Imamo i ovu karakterizaciju antisimetričnih funkcionala:

PROPOZICIJA 6

Bilinearni funkcional φ je antisimetričan ako i samo ako je $\varphi(x,x) = 0$, za svaki $x \in V$.

Dokaz

Neka je funkcional φ antisimetričan. Tada je specijalno $\varphi(x,x) = -\varphi(x,x)$ dakle (jer polje F nije karakteristike 2) $\varphi(x,x) = 0$, za svaki $x \in V$.

Obratno, za svaki izbor $x, y \in V$ je po pretpostavci $\varphi(x+y, x+y) = 0$, odnosno

$$\varphi(x,x) + \varphi(x,y) + \varphi(y,x) + \varphi(y,y) = 0\ ,$$

tj.

$$\varphi(x,y) + \varphi(y,x) = 0\ ,$$

pa je funkcional φ zaista antisimetričan. ■

Važnost simetričnih i antisimetričnih funkcionala opravdava ovaj

TEOREM 7

Svaki se bilinearni funkcional može jednoznačno prikazati kao suma jednog simetričnog i jednog antisimetričnog bilinearnog funkcionala.

Dokaz

Neka je φ bilo koji bilinearni funkcional. Definiramo

$$\varphi_s(x,y) = \frac{1}{2}[\varphi(x,y) + \varphi(y,x)]$$

i

$$\varphi_a(x,y) = \frac{1}{2}[\varphi(x,y) - \varphi(y,x)] .$$

Odmah se vidi da je φ_s simetrični funkcional, a φ_a antisimetrični, i da je

$$\varphi = \varphi_s + \varphi_a .$$

Da bismo dokazali jednoznačnost, pretpostavimo da je $\varphi = \varphi_1 + \varphi_2$ bilo koji rastav funkcionala φ u sumu simetričnog (φ_1) i antisimetričnog (φ_2) funkcionala. Onda je

$$\begin{aligned} \varphi(x,y) + \varphi(y,x) &= \varphi_1(x,y) + \varphi_2(x,y) + \varphi_1(y,x) + \varphi_2(y,x) = \\ &= 2\varphi_1(x,y) , \end{aligned}$$

pa je

$$\varphi_1(x,y) = \frac{1}{2}[\varphi(x,y) + \varphi(y,x)] = \varphi_s(x,y) .$$

Analogno se vidi da mora biti i $\varphi_2(x,y) = \varphi_a(x,y)$, za svako $x, y \in V$, te je tvrdnja dokazana. ∎

Uočimo da smo u dokazu Tm. 7 implicitno rabili pretpostavku da polje F nije karakteristike 2, jer nam ona osigurava postojanje broja $1/2$.

ZADACI

1. Pokaži da skup $\mathrm{Bil}\, V$ svih bilinearnih funkcionala na prostoru V uz prirodne operacije zbrajanja i množenja skalarom tvori linearni prostor. Koje dimenzije?

2. Neka su U i V vektorski prostori nad istim poljem F, a $\varphi : U \times V \to F$ bilinearni funkcional, definiran na $U \times V$. Nađi njegov prikaz u paru baza za U i V i definiraj matricu funkcionala u tim bazama. Generalizirajući Prop. 2, pokaži da su matrični zapisi funkcionala φ u različitim parovima baza vezani relacijom

$$B = S' \cdot A \cdot T ,$$

gdje su S i T matrice prijelaza iz stare baze u novu u prostorima U i V redom.

3. Neka je $\varphi : U \times V \to F$ bilinearni funkcional i $a \in U$ dani vektor. Pokaži da je $l_a : V \to F$,

$$l_a(y) = \varphi(a, y) ,$$

linearni funkcional na V. Pokaži, nadalje, da je operator

$$F_\varphi : U \to V^* ,$$

dan s

$$F_\varphi(a) = l_a ,$$

linearan.

4. Neka je F_φ linearni operator iz Zad. 3. Pokaži da postoji vektor $a \in U$, $a \neq \Theta_U$, sa svojstvom da je l_a nulfunkcional, ako i samo ako jezgra od F_φ nije trivijalna.

5. Analogno kao u Zad. 3., za svaki $b \in V$ je $l_b : U \to F$,

$$l_b(x) = \varphi(x, b)$$

linearni funkcional na U, a

$$G_\varphi : V \to U^* ,$$

dan s

$$G_\varphi(b) = l_b ,$$

linearni operator. Pokaži da operatori F_φ i G_φ imaju isti rang.

6. Ako su prostori U i V različitih dimenzija, onda mora postojati vektor $a \in U$, $a \neq \Theta_U$, tako da je $\varphi(a, y) = 0$ za sve $y \in V$, ili vektor $b \in V$, $b \neq \Theta_V$, tako da je $\varphi(x, b) = 0$ za sve $x \in U$. Dokaži!

7. Neka je $\varphi : U \times V \to F$ bilinearni funkcional,

$$U_0 = \{a \in U \mid \varphi(a, y) = 0, \ \forall y \in V\} ,$$

i analogno

$$V_0 = \{b \in V \mid \varphi(x, b) = 0, \ \forall x \in U\} .$$

Pokaži da su $U_0 \subset U$ i $V_0 \subset V$ potprostori i da vrijedi

$$\dim U - \dim U_0 = \dim V - \dim V_0 .$$

8. Uvjeri se da sve tvrdnje u točki 14.1. (uključujući i ove u zadacima) vrijede i u općem slučaju, kad je F bilo koje polje karakteristike različite od 2.

9. Neka je φ bilinearni funkcional, a φ' funkcional definiran s

$$\varphi'(x, y) = \varphi(y, x) .$$

Onda φ' nazivamo **transponirani funkcional** od φ. Pokaži da je funkcional φ' također bilinearan i da je njegova matrica u bilo kojoj bazi transponirana matrica od φ u toj bazi. Nadalje, funkcional φ je simetričan ako i samo ako je $\varphi' = \varphi$, a antisimetričan ako i samo ako je $\varphi' = -\varphi$.

10. Neka je U realni unitarni prostor, a φ bilinearni funkcional na U. Dokaži da postoji i jednoznačno je određen linearni operator $f : U \to U$, takav da vrijedi

$$\varphi(x, y) = (f(x), y) ,$$

za svaki $x, y \in U$. [Uputa: Za svaki $a \in U$ je $y \mapsto \varphi(a, y)$ linearni funkcional, pa prema Tm. 2 u 13.8. postoji jedinstveni vektor $b \in U$ takav da je $\varphi(a, y) = (b, y)$; definiraj $f(a) = b$.]

11. Obratno, svaki linearni operator $f : U \to U$ generira bilinearni funkcional $\varphi(x, y) = (f(x), y)$. Na taj je način uspostavljena bijektivna korespondencija između prostora $\operatorname{Hom} U$ i $\operatorname{Bil} U$. Je li to izomorfizam?

12. Pokaži da su u korespondenciji iz Zad. 11. simetričnim (antisimetričnim) funkcionalima na unitarnom prostoru pridruženi simetrični (antisimetrični) operatori. Uopće, pomoću te korespondencije se teorija bilinearnih funkcionala prenosi u teoriju linearnih operatora, i obratno (pa se npr. definiraju svojstvene vrijednosti bilinearnog funkcionala kao one pripadnog operatora i sl.).

13. Pokaži: U unitarnom prostoru su bilinearni funkcional i pridruženi linearni operator u ortogonalnoj bazi reprezentirani istom matricom.

14. Ako je matrica A simetrična (antisimetrična), uvjeri se da je matrica $M'AM$ također simetrična (antisimetrična), za bilo koju matricu M.

15. Ako je A antisimetrična matrica, onda je matrica A^2 simetrična. Nadalje, ako je A antisimetrična, a B simetrična matrica, $AB - BA$ je simetrična matrica. Konačno, ako je A antisimetrična, a B simetrična matrica, AB je antisimetrična onda i samo onda ako matrice A i B komutiraju. Dokaži!

16. Dokaži: Antisimetrična matrica neparnog reda mora biti singularna.

17. Generalizirajući bilinearni funkcional, definiraj pojam **bilinearnog operatora** $V \times V \to W$ (V i W su linearni prostori) i ispitaj njegova svojstva (vidi Zad. 1. u 9.4.). Što su multilinearni operatori?

14.2. Kvadratni funkcionali

Neka je V linearni prostor nad poljem F realnih ili kompleksnih brojeva. Funkcional

$$q : V \to F ,$$

koji ima svojstvo

$$q(x+y) + q(x-y) = 2q(x) + 2q(y) , \tag{1}$$

za svaki $x, y \in V$, nazivamo **kvadratni funkcional** na prostoru V.

Svakom je bilinearnom funkcionalu $\varphi : V \times V \to F$ na prostoru V prirodno pridružen jedan kvadratni funkcional na V. Imamo, naime, pridruženja

$$V \xrightarrow{d} D \xrightarrow{\varphi/_D} F ,$$

gdje je $D \subset V \times V$ **dijagonala** od $V \times V$, a $d(x) = (x, x)$ **dijagonalna inkluzija**, pa definiramo funkcional q na prostoru V kao kompoziciju

$$q = \varphi \circ d ,$$

tj. s

$$q(x) = (\varphi \circ d)(x) = \varphi(x, x) , \tag{2}$$

za svaki $x \in V$.

PROPOZICIJA 1

Preslikavanje $q : V \to F$, definirano s (2), jest kvadratni funkcional na V.

Dokaz

Imamo

$$\begin{aligned} q(x+y) + q(x-y) &= \varphi(x+y, x+y) + \varphi(x-y, x-y) = \\ &= \varphi(x,x) + \varphi(x,y) + \varphi(y,x) + \varphi(y,y) + \\ &\quad + \varphi(x,x) - \varphi(x,y) - \varphi(y,x) + \varphi(y,y) = \\ &= 2\,\varphi(x,x) + 2\,\varphi(y,y) = 2\,q(x) + 2\,q(y) \end{aligned}$$

i tvrdnja je provjerena. ■

Nas će ovdje zanimati samo kvadratni funkcionali opisanog oblika, tj. ubuduće ćemo **pod kvadratnim funkcionalom podrazumijevati samo takav, koji je generiran bilinearnim funkcionalom.**

Kako smo vidjeli (Tm. 7 u 14.1.), svaki se bilinearni funkcional φ može prikazati u obliku $\varphi = \varphi_s + \varphi_a$, gdje je φ_s simetrični, a φ_a antisimetrični funkcional. Odatle slijedi (zbog Prop. 6 u 14.1.) da je za kvadratni funkcional q generiran s φ ispunjeno

$$q(x) = \varphi(x,x) = \varphi_s(x,x) + \varphi_a(x,x) = \varphi_s(x,x) ,$$

tj. q je potpuno određen samim simetričnim dijelom bilinearnog funkcionala φ. Prema tome, različiti bilinearni funkcionali s istim simetričnim dijelom generirat će isti kvadratni funkcional.

Ako je, dakle, q bilo koji kvadratni funkcional, neće biti moguće jednoznačno rekonstruirati bilinearni funkcional iz kojeg je dobiven. Najviše što možemo postići je da odredimo simetrični dio takvog bilinearnog funkcionala. Taj je, dakako, i sam bilinearni funkcional, i svaki će se eventualni bilinearni funkcional koji generira q razlikovati od tog funkcionala samo u antisimetričnom dijelu. Vrijedi

PROPOZICIJA 2

Neka je $q : V \to F$ bilo koji kvadratni funkcional (generiran bilinearnim funkcionalom). Onda postoji i jednoznačno je određen simetrični bilinearni funkcional φ_s koji generira q, i on je dan formulom

$$\varphi_s(x,y) = \frac{1}{2}\left[q(x+y) - q(x) - q(y)\right] . \tag{3}$$

Dokaz

Neka je q kao u iskazu propozicije. Uvrštavanjem $x = y = \Theta$ u (1), odmah slijedi da je $q(\Theta) = 0$, a za $x = y \in V$ iz (1) dobijemo

$$q(2x) = q(x+x) = 4q(x) .$$

Neka je $\varphi_s : V \times V \to F$ preslikavanje definirano relacijom (3). Tada je

$$\varphi_s(x,x) = \frac{1}{2}\left[q(x+x) - q(x) - q(x)\right] = q(x) ,$$

za svako $x \in V$, tj. φ_s generira q. Ako dokažemo da je φ_s simetrični bilinearni funkcional, dokazali smo egzistenciju traženoga funkcionala iz iskaza

propozicije. Neka je ψ bilo koji bilinearni funkcional koji generira q. Onda je

$$\begin{aligned}\varphi_s(x,y) &= \frac{1}{2}[q(x+y)-q(x)-q(y)] = \\ &= \frac{1}{2}[\psi(x+y,x+y)-\psi(x,x)-\psi(y,y)] = \\ &= \frac{1}{2}[\psi(x,x)+\psi(x,y)+\psi(y,x)+\psi(y,y)- \\ &\quad -\psi(x,x)-\psi(y,y)] = \frac{1}{2}[\psi(x,y)+\psi(y,x)] = \psi_s(x,y)\ ,\end{aligned}$$

gdje je ψ_s simetrični dio funkcionala ψ i tvrdnja je dokazana.

Za bilo koji simetrični bilinearni funkcional ψ_s koji generira q analogno imamo

$$\begin{aligned}\psi_s(x,y) &= \frac{1}{2}[\psi_s(x,y)+\psi_s(y,x)] = \\ &= \frac{1}{2}[q(x+y)-q(x)-q(y)] = \varphi_s(x,y)\ ,\end{aligned}$$

pa je dokazana i jednoznačnost. ■

Jedinstveni simetrični bilinearni funkcional određen kvadratnim funkcionalom q nazivamo **polarni funkcional** od q.

Dokazali smo, dakle,

TEOREM 3

Svakim je simetričnim bilinearnim funkcionalom jednoznačno određen jedan kvadratni funkcional, i on je dan formulom (2). *Obratno, svakim je kvadratnim funkcionalom jednoznačno određen jedan simetrični bilinearni funkcional, njegov polarni funkcional, i on je dan formulom* (3). ■

Prema tome, imamo bijektivnu korespondenciju između simetričnih bilinearnih funkcionala i kvadratnih funkcionala na danom linearnom prostoru, pomoću koje je uspostavljena veza između pripadnih teorija. Pojmovi i rezultati iz teorije simetričnih bilinearnih funkcionala lako se prenose u teoriju kvadratnih funkcionala, i obratno.

Odmah se npr. vidi da će u danoj bazi $(a_1,\ldots,a_n)$ prostora V kvadratni funkcional q imati prikaz

$$q(x) = \sum_{i=1}^{n}\sum_{j=1}^{n} \alpha_{ij}\, x_i x_j\ ,$$

odnosno, matrično pisano,

$$q(x) = X'\, A\, X\ ,$$

gdje za matricu $A = [\alpha_{ij}]$ možemo pretpostaviti da je simetrična i nazivamo je **matrica kvadratnog funkcionala** q. Njezin je rang, dakako, invarijantan i nazivamo ga **rang kvadratnog funkcionala**.

ZADACI

1. Pokaži da je polarni funkcional φ_s kvadratnog funkcionala q dan i formulom
$$\varphi_s(x, y) = \frac{1}{4}[q(x + y) - q(x - y)] .$$

2. Uvjeri se da tvrdnje o kvadratnom funkcionalu vrijede i u općem slučaju, kad je F bilo koje polje karakteristike različite od 2.

3. Neka je q kvadratni funkcional na prostoru $\mathbb{R}^2$. Dokaži da je s $q(x) = 1$ u standardnoj bazi dana **jednadžba** (nedegenerirane) **krivulje** k **drugog reda** u $\mathbb{R}^2$. Nadalje, ako je $\varphi(x, y)$ polarni funkcional od q, a $y^0 = (y_1^0, y_2^0)$ bilo koja točka, onda je $\varphi(x, y^0) = 1$ jednadžba pravca koji spaja dirališta tangenata, povučenih iz y^0 na krivulju k, tzv. **polara** točke y^0 s obzirom na k. Specijalno, ako je $y^0 \in k$, tako dobivamo jednadžbu **tangente** na krivulju u točki y^0.

14.3. Kvadratne forme. Lagrangeov algoritam

Homogeni polinomi nazivaju se forme. Točnije, polinom u varijablama $x_1, \ldots, x_n$, s koeficijentima iz polja F, naziva se **forma stupnja** p (u n varijabli x_i, $i = 1, \ldots, n$, nad poljem F), ako su svi njegovi članovi stupnja p. Forme prvog stupnja se nazivaju **linearne**, drugog **kvadratne**, trećeg **kubne** itd.

Nas će posebno zanimati kvadratne forme. One se pojavljuju u raznim situacijama u matematici i primjenama. Tako je npr.

$$x^2 + y^2 + z^2 - t^2$$

dobro poznata forma iz teorije relativnosti. U analizi se, kako znamo, pojavljuje kvadratna forma

$$\left(\frac{\partial^2 f}{\partial x^2}\right)_O x^2 + 2\left(\frac{\partial^2 f}{\partial x \partial y}\right)_O xy + \left(\frac{\partial^2 f}{\partial y^2}\right)_O y^2 ,$$

koja je vezana uz ispitivanje ekstrema funkcije $f(x, y)$ (u okolini ishodišta), i slično.

Općenito, **kvadratna forma** u n varijabli $x_1, \ldots, x_n$, tj. **reda** n, nad poljem F je oblika

$$Q(x) = \sum_{i=1}^{n} \sum_{j=1}^{n} \alpha_{ij} x_i x_j \,, \tag{1}$$

gdje su $\alpha_{ij} \in F$ dani skalari. Pritom smo kraće označili $x = (x_1, \ldots, x_n)$. Kako je za svaki $i, j = 1, \ldots, n$

$$\alpha_{ij} x_i x_j + \alpha_{ji} x_j x_i = \frac{\alpha_{ij} + \alpha_{ji}}{2} x_i x_j + \frac{\alpha_{ij} + \alpha_{ji}}{2} x_j x_i \,,$$

bez narušavanja općenitosti možemo pretpostaviti da je forma $Q(x)$ zapisana u simetričnom obliku, tj. da je **matrica forme**

$$A = [\alpha_{ij}]$$

simetrična. Rang te matrice naziva se **rang forme**. Posebno, forma je **regularna** ako je maksimalnog ranga, tj. ako je njezina matrica A regularna.

Ako s $X = [x_i]$ označimo (stupčanu) matricu varijabli, (1) možemo u sažetom obliku pisati kao

$$Q(x) = X' \, A \, X \,. \tag{2}$$

Iz (1) i razmatranja u točki 14.2. razabiremo da se kvadratne forme prirodno pojavljuju u teoriji kvadratnih funkcionala kao njihovi prikazi u danoj bazi ili, drugim riječima, kvadratni funkcionali čine geometrijsku interpretaciju formi u teoriji linearnih prostora.

Dvije kvadratne forme u istim varijablama su **jednake** ako za svaki izbor vrijednosti za varijable poprimaju istu vrijednost. To će, očito, biti slučaj ako i samo ako te forme imaju istu matricu*).

Osnovni problem teorije formi je danu formu zamjenom varijabli transformirati u novu, koja je jednostavnijeg oblika. Ako su s $y_1, \ldots, y_n$ označene nove varijable, **jednadžbe** (linearne) **transformacije** varijabli dane su s

$$x_i = \tau_{i1} y_1 + \cdots + \tau_{in} y_n \,, \tag{3}$$

$i = 1, \ldots, n$, gdje za matricu

$$T = [\tau_{ij}]$$

uvijek pretpostavljamo da je **regularna** (što nam omogućuje da nove varijable izrazimo uz pomoć starih, ako je potrebno) i nazivamo je **matrica**

*) Ne zaboravimo da su forme polinomi, a polinomi su (identički) jednaki ako i samo ako su im korespondentni koeficijenti jednaki.

transformacije (3). Odmah se vidi da transformaciju varijabli možemo matrično zapisati kao

$$X = T\,Y\,, \quad \text{odnosno} \quad Y = T^{-1}\,X\,, \tag{4}$$

gdje je $Y = [y_i]$ matrica novih varijabli. Ako je matrica T ortogonalna, govorimo o **ortogonalnoj transformaciji** varijabli.

Za kvadratnu formu $P(x)$ kažemo da je **kongruentna** s formom $Q(y)$ ako postoji transformacija varijabli (3) koja prevodi prvu formu u drugu. Očito se radi o dobro definiranoj relaciji ekvivalencije pa govorimo o **paru kongruentnih formi**. Dvije su forme **ortogonalno kongruentne** ako je pripadna transformacija varijabli ortogonalna.

Kako smo rekli u 14.1., matrice A i B su kongruentne ako postoji regularna matrica T tako da vrijedi

$$B = T'\,A\,T\,.$$

Ako je pritom matrica T ortogonalna, za matrice A i B kažemo da su **ortogonalno kongruentne**. Budući da ortogonalne matrice istog reda čine grupu, odmah možemo zaključiti da je i ortogonalna kongruencija matrica jedna relacija ekvivalencije (vidi Zad. 18. u 9.5.). Ortogonalno kongruentne matrice su slične, ali obrat, dakako, ne vrijedi općenito.

PROPOZICIJA 1

Dvije su forme (ortogonalno) kongruentne ako i samo ako su njihove matrice (ortogonalno) kongruentne.

Dokaz

Neka su $P(x)$ i $Q(y)$ kongruentne forme, a A, odnosno B, njihove matrice. Onda je, zbog (2) i (4),

$$\begin{aligned} P(x) &= X'\,A\,X = (TY)'\,A\,(TY) = \\ &= Y'\,(T'AT)\,Y = Y'\,B\,Y = Q(y)\,, \end{aligned}$$

pa zaključujemo da je $B = T'\,A\,T$, tj. da su matrice A i B kongruentne. Slično se vidi i obrat. ■

Kako kongruentne matrice imaju isti rang (Zad. 12. u 9.6.), evidentno i kongruentne forme imaju isti rang.

Na temelju Prop. 1 i Kor. 3 u 14.1. imamo i geometrijsku interpretaciju kongruentnih formi:

KOROLAR 2

Kvadratne forme su kongruentne ako i samo ako predstavljaju prikaze istog kvadratnog funkcionala (s obzirom na eventualno različite baze prostora).

■

Za kvadratnu formu kažemo da je **dijagonalna** ako je oblika

$$D(x) = \sum_{i=1}^{n} \alpha_i x_i^2 , \tag{5}$$

tj. ako je njezina matrica dijagonalna.

PROPOZICIJA 3

Svaka je kvadratna forma ortogonalno kongruentna s nekom dijagonalnom formom.

Dokaz

Neka je A matrica dane forme. Kako je A simetrična matrica, prema Zad. 11. u 13.5., ortogonalno je slična s nekom dijagonalnom matricom D, tj. postoji ortogonalna matrica T takva da je $D = T^{-1}AT$. No, zbog ortogonalnosti je $T^{-1} = T'$, pa je $D = T'AT$, što po našoj definiciji znači da je matrica D ortogonalno kongruentna s matricom A. Međutim, matricom D je očito na jednoznačan način određena neka dijagonalna forma koja je, prema Prop. 1, ortogonalno kongruentna s polaznom formom. ■

Dijagonalnu formu koja je kongruentna danoj formi (takva postoji zbog Prop. 3) nazivamo **dijagonalni** ili **kanonski oblik** polazne kvadratne forme. Jasno je da kanonski oblik neće danom formom biti jednoznačno određen.

Na razini funkcionala, zbog Kor. 2 imamo ovaj zaključak:

KOROLAR 4

Za svaki kvadratni funkcional postoji baza prostora u kojoj taj funkcional ima dijagonalni matrični zapis. ■

To je tzv. **kanonski prikaz** tog funkcionala, tj. prikaz u njegovoj **kanonskoj bazi**.

Postavlja se pitanje efektivnog prevođenja dane forme u njezin kanonski oblik. Za to postoje različite metode. Ako ne inzistiramo na ortogonalnosti matrice transformacije varijabli, najjednostavniji je tzv. **Lagrangeov algoritam**.

Neka je, dakle ,

$$Q(x) = \sum_{i,j=1}^{n} \alpha_{ij} x_i x_j \tag{6}$$

kvadratna forma koju želimo prevesti na kanonski oblik. Pretpostavimo najprije da je u (6) bar jedan od koeficijenata α_{ii} različit od nule, tj. da se

bar jedna od varijabli pojavljuje u kvadratu. Ako je npr. $\alpha_{11} \neq 0$, (6) ćemo pisati kao

$$\begin{aligned} Q(x) &= \alpha_{11}x_1^2 + 2\alpha_{12}x_1x_2 + \cdots + 2\alpha_{1n}x_1x_n + \sum_{i,j>1} \alpha_{ij}x_ix_j = \\ &= \alpha_{11}^{-1}(\alpha_{11}x_1 + \alpha_{12}x_2 + \cdots + \alpha_{1n}x_n)^2 - \\ &\quad -\alpha_{11}^{-1}(\alpha_{12}^2x_2^2 + \cdots + \alpha_{1n}^2x_n^2 + 2\alpha_{12}\alpha_{13}x_2x_3 + \cdots \\ &\quad +2\alpha_{12}\alpha_{1n}x_2x_n + \cdots + 2\alpha_{1n-1}\alpha_{1n}x_{n-1}x_n) + \sum_{i,j>1} \alpha_{ij}x_ix_j = \\ &= \alpha_{11}^{-1}(\alpha_{11}x_1 + \alpha_{12}x_2 + \cdots + \alpha_{1n}x_n)^2 + Q_1(x)\ , \end{aligned}$$

gdje je Q_1 kvadratna forma u varijablama $x_2, \ldots, x_n$. Primjenom transformacije

$$\left.\begin{aligned} y_1 &= \alpha_{11}x_1 + \cdots + \alpha_{1n}x_n \\ y_i &= x_i\ ,\quad i = 2, \ldots, n \end{aligned}\right\} \tag{7}$$

dolazimo do forme

$$Q(y) = \alpha_{11}^{-1}y_1^2 + Q_1(y)\ . \tag{8}$$

Kako je matrica transformacije (7) očito regularna, forma $Q(y)$ je kongruentna s polaznom formom $Q(x)$ i ima svojstvo da se u njoj varijabla y_1 pojavljuje samo u kvadratu te da je $Q_1(y)$ forma u varijablama $y_2, \ldots, y_n$.

Ako je pak u polaznoj formi $\alpha_{11} = \alpha_{22} = \cdots = \alpha_{nn} = 0$, pretpostavimo da je npr. $\alpha_{12} \neq 0$. Tada (6) pišemo kao

$$Q(x) = 2x_1(\alpha_{12}x_2 + \alpha_{13}x_3 + \cdots + \alpha_{1n}x_n) + Q_1(x)\ ,$$

gdje je $Q_1(x)$ opet kvadratna forma u varijablama $x_2, \ldots, x_n$, koje se ne pojavljuju u kvadratu. Zamjenom varijabli

$$\left.\begin{aligned} y_2 &= -x_1 + \alpha_{12}x_2 + \cdots + \alpha_{1n}x_n \\ y_i &= x_i\ ,\quad i = 1, 3, 4, \ldots, n \end{aligned}\right\} \tag{9}$$

onda dolazimo do kongruentne forme

$$\begin{aligned} Q(y) &= 2y_1(y_2 + y_1) + Q_1(y) = \\ &= 2y_1^2 + 2y_1y_2 + 2\alpha_{12}^{-1}\alpha_{23}y_1y_3 + \cdots\ , \end{aligned}$$

u kojoj se varijabla y_1 pojavljuje u kvadratu, pa smo u mogućnosti primijeniti prethodni algoritam koji nas vodi na (8).

Postupak nastavljamo primjenjujući opisanu metodu na formu $Q_1(y)$ u (8). Nakon najviše $2n - 2$ koraka tako dolazimo do dijagonalne forme koja je kongruentna polaznoj, dakle njezin kanonski oblik.

Navedimo jedan primjer. Polazimo od forme

$$\begin{aligned} Q(x) &= x_1^2 + 4x_2^2 + 8x_3^2 - x_4^2 - 4x_1x_2 + 6x_1x_3 - \\ &\quad -12x_2x_3 + 2x_3x_4 + x_2x_5 - x_4x_5 = \\ &= (x_1 - 2x_2 + 3x_3)^2 - 4x_2^2 - 9x_3^2 + 12x_2x_3 + 4x_2^2 + 8x_3^2 - x_4^2 - \\ &\quad -12x_2x_3 + 2x_3x_4 + x_2x_5 - x_4x_5 = \\ &= (x_1 - 2x_2 + 3x_3)^2 - x_3^2 - x_4^2 + 2x_3x_4 + x_2x_5 - x_4x_5 \quad . \end{aligned}$$

Transformacijom

$$\left.\begin{aligned} y_1 &= x_1 - 2x_2 + 3x_3 \\ y_i &= x_i \ , \quad i = 2,3,4,5 \end{aligned}\right\} \tag{10}$$

dolazimo do forme

$$\begin{aligned} Q(y) &= y_1^2 - y_3^2 - y_4^2 + 2y_3y_4 + y_2y_5 - y_4y_5 = \\ &= y_1^2 - (y_3 - y_4)^2 + y_2y_5 - y_4y_5 \quad . \end{aligned}$$

Daljnjom transformacijom

$$\left.\begin{aligned} z_3 &= y_3 - y_4 \\ z_i &= y_i \ , \quad i = 1,2,4,5 \end{aligned}\right\} \tag{11}$$

dobivamo formu

$$Q(z) = z_1^2 - z_3^2 + z_2z_5 - z_4z_5 = z_1^2 - z_3^2 + (z_2 - z_4)z_5 \ .$$

Kako u dijelu koji još treba transformirati nema kvadratnih članova, prema algoritmu (9) primijenimo supstituciju

$$\left.\begin{aligned} u_2 &= z_2 - z_4 - z_5 \\ u_i &= z_i \ , \quad i = 1,3,4,5 \end{aligned}\right\} \tag{12}$$

koja prethodnu formu prevodi u

$$Q(u) = u_1^2 - u_3^2 + (u_2 + u_5)u_5 = u_1^2 - u_3^2 + (\frac{1}{2}u_2 + u_5)^2 - \frac{1}{4}u_2^2 \ .$$

Konačno, transformacija

$$\left.\begin{aligned} v_4 &= \frac{1}{2}u_2 + u_5 \\ v_i &= u_i \ , \quad i = 1,2,3 \end{aligned}\right\} \tag{13}$$

daje

$$Q(v) = v_1^2 - \frac{1}{4}v_2^2 - v_3^2 + v_4^2 \ ,$$

i to je (jedan) kanonski oblik polazne forme $Q(x)$.

Navedeni postupak nije teško pratiti matrično. Neka su S_i, $i = 1, \ldots, 4$, matrice iskorištenih transformacija varijabli (opisanih sa (10), (11), (12) i (13); uvijek su nove varijable izražene pomoću starih!). Onda će

$$S = S_4 S_3 S_2 S_1$$

biti matrica transformacije kojom su varijable v_i u kanonskom obliku izražene pomoću polaznih varijabli x_j. Nadalje, matrica $T = S^{-1}$ provodi dijagonalizaciju forme, tj. vrijedi

$$B = T' A T ,$$

gdje je A matrica polazne forme $Q(x)$, a B matrica njezina kanonskog oblika $Q(v)$. Provjeri taj račun! Zaključak je općenit.

Analogno teoriji kvadratnih formi, može se razviti teorija bilinearnih i simetričnih bilinearnih formi (vidi Zad. 3.–12.).

ZADACI

1. Dvije kvadratne forme su ortogonalno kongruentne ako i samo ako njihove matrice imaju isti karakteristični polinom. Dokaži!

2. Lagrangeovim postupkom dijagonaliziraj forme:

   (a) $Q_1(x) = 9x_2^2 + 9x_3^2 + 12x_1x_2 + 12x_1x_3 - 6x_2x_3$;
   (b) $Q_2(x) = -3x_1^2 + 6x_2^2 - 12x_1x_2 + 12x_1x_3 + 6x_2x_3$;
   (c) $Q_3(x) = 11x_1^2 + 4x_2^2 + 11x_3^2 - 2x_1x_3 + 8x_2x_3$.

   Na temelju Zad. 1. utvrdi koje su od tih formi ortogonalno kongruentne, pa za njih nađi matricu transformacije varijabli koja prevodi jednu u drugu.

3. Umjesto polinoma u jednom sustavu varijabli, mogu se promatrati i polinomi u dva ili više sustava varijabli (ne nužno jednakobrojnih). Takav se polinom naziva **forma** ako je homogen u svakom sustavu varijabli posebno. Od posebnog su interesa forme koje su linearne u svakom sustavu varijabli. To su tzv. **multilinearne forme**. Tada imamo **linearne**, **bilinearne**, **trilinearne forme** itd. **Bilinearna forma** u sustavima varijabli $x_1, \ldots, x_n$ i $y_1, \ldots, y_n$ je, dakle, oblika

$$\Phi(x, y) = \sum_{i,j=1}^{n} \alpha_{ij} x_i y_j ,$$

gdje matricu $A = [\alpha_{ij}]$ nazivamo **matrica forme**, a rang te matrice je **rang forme**. Broj n varijabli u svakom sustavu nazivamo **red forme**. Forma je **regularna** ako je njezina matrica regularna, a inače je **singularna**. Uoči da se bilinearna forma može zapisati u obliku

$$\Phi(x, y) = X' A Y ,$$

gdje su $X = [x_i]$ i $Y = [y_j]$ (stupčane) matrice varijabli. Uvjeri se, nadalje (vidi 14.1.), da se bilinearne forme prirodno pojavljuju kao prikazi bilinearnih funkcionala u danoj bazi prostora.

4. Za bilinearnu formu $\Phi(x, y)$ kažemo da je **ekvivalentna** bilinearnoj formi $\Phi(x', y')$ ako postoje (općenito različite) transformacije obaju sustava varijabli, koje prevode prvu formu u drugu. Pokaži da se radi o dobro definiranoj relaciji ekvivalencije. Dokaži nadalje, da su dvije bilinearne forme ekvivalentne ako i samo ako za njihove matrice vrijedi

$$B = T' A S ,$$

gdje su T i S matrice transformacije prvog, odnosno drugog sustava varijabli (dakle regularne), tj. ako i samo ako su matrice formi ekvivalentne (vidi Zad. 10. u 9.6.).

5. Dokaži: Bilinearne forme nad istim poljem su ekvivalentne ako i samo ako su istog reda (tj. sadrže isti broj varijabli) i istog ranga. Posebno, sve su regularne forme istog reda ekvivalentne. Svaka je bilinearna forma ekvivalentna sa svojim **kanonskim oblikom**

$$x_1 y_1 + x_2 y_2 + \cdots + x_r y_r ,$$

gdje je r rang forme (vidi točku 9.6.).

6. Dvije bilinearne forme su **kongruentne** ako se druga može dobiti iz prve **istom** transformacijom varijabli za oba sustava. To je dobro definirana relacija klasifikacije. Kongruentne forme su, dakako, ekvivalentne, ali obrat ne vrijedi. Dokaži: Bilinearne forme su kongruentne ako i samo ako za njihove matrice vrijedi

$$B = T' A T ,$$

tj. ako su te matrice kongruentne. Prema tome (Kor. 3 u 14.1.), bilinearne forme su kongruentne onda i samo onda ako su to prikazi istog bilinearnog funkcionala.

7. Bilinearna forma je **simetrična** (**antisimetrična**) ako je njezina matrica simetrična (antisimetrična). Dokaži: Forma kongruentna simetričnoj (antisimetričnoj) formi i sama je simetrična (antisimetrična).

8. Bilinearne forme su **ortogonalno kongruentne** ako je matrica transformacije varijabli ortogonalna. To će biti onda i samo onda ako su njihove matrice ortogonalno kongruentne. Dokaži: Svaka simetrična bilinearna forma je ortogonalno kongruentna s formom

$$\alpha_1 x_1 y_1 + \alpha_2 x_2 y_2 + \cdots + \alpha_r x_r y_r \ , \tag{14}$$

gdje je r rang polazne forme. Forma (14) je **dijagonalni** ili **kanonski** oblik polazne forme (vidi Prop. 3).

9. Koeficijenti $\alpha_1, \ldots, \alpha_r$ u formi (13) jesu svojstvene vrijednosti matrice polazne forme, koje su različite od nule. Prema tome, simetrične bilinearne forme su ortogonalno kongruentne ako i samo ako njihove matrice imaju iste karakteristične polinome. Dokaži!

10. Svakoj simetričnoj bilinearnoj formi možemo prirodno pridružiti jednu kvadratnu formu, identificirajući prvi sustav varijabli s drugim:

$$\sum_{i,j} \alpha_{ij} x_i y_j \mapsto \sum_{i,j} \alpha_{ij} x_i x_j \ .$$

Obratno, uvodeći u kvadratnu formu novi sustav varijabli,

$$\sum_{i,j} \alpha_{ij} x_i x_j \mapsto \sum_{i,j} \alpha_{ij} x_i y_j \ ,$$

dolazimo do simetrične bilinearne forme, tzv. **polarne forme** polazne kvadratne forme. Na taj je način uspostavljena bijektivna korespondencija između simetričnih bilinearnih i kvadratnih formi, u kojoj pridružene forme imaju istu (simetričnu) matricu. Ta se korespondencija onda proširuje na pripadne teorije bilinearnih i kvadratnih formi.

Ako kvadratnu formu shvatimo kao prikaz kvadratnog funkcionala u nekoj bazi, dokaži da je njezina polarna forma prikaz kvadratnom funkcionalu pridruženog polarnog funkcionala u toj istoj bazi.

11. Koristeći se korespondencijom iz Zad. 10., opiši Lagrangeov postupak za dijagonalizaciju simetrične bilinearne forme. [Uputa: Zamijeni bilinearnu formu pripadnom kvadratnom, dijagonaliziraj kvadratnu formu algoritmom iz teksta i na kraju polariziraj rezultat.]

Kao primjer, dijagonaliziraj bilinearnu formu

$$\begin{aligned}\Phi(x,y) &= x_1y_1 + x_2y_2 + x_3y_3 + 2x_1y_3 + 2x_2y_1 + \\ &\quad +2x_2y_3 + 2x_3y_1 + 2x_3y_2 \ .\end{aligned}$$

12. Pokaži da je svaka antisimetrična bilinearna forma kongruentna s formom

$$x_1y_2 - x_2y_1 + x_3y_4 - x_4y_3 + \cdots + x_{2r-1}y_{2r} - x_{2r}y_{2r-1} \ ,$$

gdje je $2r$ rang polazne forme. Odavde (opet) slijedi da je rang antisimetrične matrice uvijek paran broj. Nađi odgovarajući algoritam koji realizira navedenu redukciju i primijeni ga na formu

$$\begin{aligned}\Phi(x,y) &= x_1y_2 - x_2y_1 + x_1y_3 - x_3y_1 + 2x_4y_1 - \\ &\quad -2x_1y_4 + 3x_2y_3 - 3x_3y_2 + x_2y_4 - x_4y_2 - 4x_3y_4 + 4x_4y_3 \ .\end{aligned}$$

14.4. Zakon inercije. Definitnost forme

Razmatranja u ovoj točki odnose se na kvadratne forme nad poljem realnih brojeva. Neka je

$$Q(x) = \sum_{i,j=1}^{n} \alpha_{ij} x_i x_j \tag{1}$$

realna kvadratna forma reda n i ranga r. Kako smo vidjeli, ta se forma može uvijek transformacijom varijabli (npr. Lagrangeovim algoritmom) svesti na kanonski oblik

$$Q(y) = \sum_{i=1}^{n} \beta_i y_i^2 = \beta_1 y_1^2 + \beta_2 y_2^2 + \cdots + \beta_n y_n^2 \ , \tag{2}$$

i nova je forma također ranga r. Bez narušavanja općenitosti (prenumeracija varijabli!) možemo pretpostaviti da je

$$\left.\begin{array}{llll} \beta_i > 0 & , & \text{za} & i = 1, \ldots, p \\ \beta_i < 0 & , & \text{za} & i = p+1, \ldots, p+q \\ \beta_i = 0 & , & \text{za} & i = p+q+1, \ldots, n \end{array}\right\} \ , \tag{3}$$

tj. da je u formi (2) prvih p koeficijenata pozitivno, sljedećih q koeficijenata negativno, a ostali koeficijenti su jednaki nuli. Pritom, dakako, vrijedi

$$p + q = r \ . \tag{4}$$

Ako sada u formi (2) provedemo transformaciju varijabli

$$\left.\begin{array}{rcccl} z_i & = & \sqrt{\beta_i}y_i & , & \text{za} \quad i = 1,\ldots,p \\ z_i & = & \sqrt{-\beta_i}y_i & , & \text{za} \quad i = p+1,\ldots,p+q \\ z_i & = & y_i & , & \text{za} \quad i = p+q+1,\ldots,n \end{array}\right\} , \tag{5}$$

dolazimo do forme

$$Q(z) = \sum_{i=1}^{n} \varepsilon_i z_i^2 = z_1^2 + \cdots + z_p^2 - z_{p+1}^2 - \cdots - z_{p+q}^2 , \tag{6}$$

gdje su $\varepsilon_i \in \{-1, 0, 1\}$, za $i = 1,\ldots,n$. Kako je matrica transformacije (5) očito regularna, forma (6) je kongruentna s formom (1), i tu formu nazivamo **normalni oblik** forme (1). Zapišimo ovaj rezultat:

PROPOZICIJA 1

Svaka je realna kvadratna forma kongruentna s nekom formom oblika

$$N(x) = \sum_i \varepsilon_i x_i^2 , \tag{7}$$

gdje su koeficijenti ε_i jednaki 1 ili -1, i to je njezin najjednostavniji, normalni oblik. ■

Primijetimo da ta kongruencija općenito nije ortogonalna jer transformacija (5) ne mora biti ortogonalna.

Dana kvadratna forma može se na razne načine svesti na kanonski, pa onda i na normalni oblik. Zanimljivo je, međutim, da dobivamo uvijek jedan te isti normalni oblik, tj. da on ne ovisi o upotrijebljenim transformacijama. Preciznije, vrijedi čuveni

TEOREM 2 (Zakon inercije, Sylvester)

Svi kanonski (normalni) oblici realne kvadratne forme imaju isti broj pozitivnih koeficijenata i isti broj negativnih koeficijenata.

Dokaz

Dovoljno je dokazati tvrdnju za pozitivne koeficijente jer jednakost broja negativnih koeficijenata onda slijedi iz invarijantnosti ranga i relacije (4).

Neka su, dakle,

$$Q(x) = x_1^2 + \cdots + x_p^2 - x_{p+1}^2 - \cdots - x_r^2 \tag{8}$$

i

$$Q(y) = y_1^2 + \cdots + y_t^2 - y_{t+1}^2 - \cdots - y_r^2 \tag{9}$$

normalni oblici iste kvadratne forme. Kako su te forme kongruentne s polaznom formom, one su kongruentne i međusobno pa postoji transformacija varijabli

$$x_i = \sum_{j=1}^{r} \tau_{ij} y_j \,, \quad i = 1, \ldots, r \,, \tag{10}$$

s regularnom matricom $T = [\tau_{ij}]$, koja formu $Q(x)$ prevodi u formu $Q(y)$. To znači da vrijedi jednakost

$$x_1^2 + \cdots + x_p^2 - x_{p+1}^2 - \cdots - x_r^2 = y_1^2 + \cdots + y_t^2 - y_{t+1}^2 - \cdots - y_r^2 \,, \tag{11}$$

u smislu da zamjenom varijabli x_i njihovim prikazima (10), relacija (11) postaje identitet u varijablama $y_1, \ldots, y_r$.

Pretpostavimo sada da je $p < t$ i zapišimo (11) u obliku

$$x_1^2 + \cdots + x_p^2 + y_{t+1}^2 + \cdots + y_r^2 = y_1^2 + \cdots + y_t^2 + x_{p+1}^2 + \cdots + x_r^2 \,. \tag{12}$$

Promatrajmo homogeni sustav jednadžbi

$$\begin{array}{ccccccccccc} x_1 & = & \tau_{11}y_1 & + & \cdots & + & \tau_{1r}y_r & = & 0 \\ \cdots & \cdots & \cdots\cdots & \cdots & \cdots & \cdots & \cdots\cdots & \cdots & \cdots \\ x_p & = & \tau_{p1}y_1 & + & \cdots & + & \tau_{pr}y_r & = & 0 \\ & & y_{t+1} & & & & & = & 0 \\ & & \cdots\cdots & \cdots & \cdots & \cdots & \cdots\cdots & \cdots & \cdots \\ & & y_r & & & & & = & 0 \end{array} \tag{13}$$

u nepoznanicama $y_1, \ldots, y_r$. Kako je po pretpostavci $p < t$, to je

$$p + (r - t) < r \,,$$

tj. u sustavu (13) je broj jednadžbi manji od broja nepoznanica pa sustav ima i netrivijalnih rješenja (vidi Kor. 2 u 11.5.). Neka je

$$y_1 = \gamma_1, \ \ldots, \ y_t = \gamma_t, \ y_{t+1} = 0, \ \ldots, \ y_r = 0 \,, \tag{14}$$

gdje je bar jedan od skalara $\gamma_1, \ldots, \gamma_t$ različit od nule, jedno takvo rješenje. Uvrštavanjem tih vrijednosti za varijable u identitet (12) dobivamo

$$0 = \gamma_1^2 + \cdots + \gamma_t^2 + \left(\sum_{j=1}^{r} \tau_{p+1\,j} \gamma_j \right)^2 + \cdots + \left(\sum_{j=1}^{r} \tau_{rj} \gamma_j \right)^2 . \tag{15}$$

Kako su kvadrati nenegativni, iz (15) specijalno slijedi da je nužno

$$\gamma_1 = \cdots = \gamma_t = 0 \,,$$

što je u kontradikciji s izborom (14). To znači da ne može biti $p < t$. Posve analogno pokazuje se da nije niti $p > t$, pa kao jedina mogućnost ostaje $p = t$ i tvrdnja je dokazana. ■

Navedimo još jedan dokaz teorema o inerciji, koji je više geometrijskog karaktera. Kako su forme $Q(x)$ i $Q(y)$ iz relacija (8) i (9) kongruentne, one prema Kor. 2 u 14.3. jesu prikazi istog kvadratnog funkcionala $q : V \to \mathbb{R}$, gdje je $\dim V = r$. Neka je (8) prikaz tog funkcionala u bazi

$$(a_1, \ldots, a_p, a_{p+1}, \ldots, a_r) , \tag{16}$$

a (9) prikaz u bazi

$$(b_1, \ldots, b_t, b_{t+1}, \ldots, b_r) \tag{17}$$

prostora V. Promatrajmo potprostor

$$L = [\{a_1, \ldots, a_p\}] < V ,$$

razapet vektorima $a_1, \ldots, a_p$, $\dim L = p$. Ako je $x \in L$ bilo koji vektor različit od nulvektora, njegov je koordinatni slog u bazi (16) oblika $(x_1, \ldots, x_p, 0, \ldots, 0)$, gdje je bar jedan x_i različit od nule, pa iz (8) zaključujemo da mora biti

$$q(x) > 0 . \tag{18}$$

U drugu ruku, ako je

$$M = [\{b_{t+1}, \ldots, b_r\}] < V$$

potprostor razapet vektorima $b_{t+1}, \ldots, b_r$, onda je $\dim M = r - t$, i nadalje, svaki vektor $y \in M$, $y \neq \Theta$, ima u bazi (17) koordinate

$$(0, \ldots, 0, y_{t+1}, \ldots, y_r) ,$$

gdje je $y_j \neq 0$ za bar jedno j, pa iz (9) čitamo da vrijedi

$$q(y) < 0 . \tag{19}$$

Iz (18) i (19) onda slijedi da je

$$L \cap M = \{\Theta\} ,$$

i prema tome suma $L + M$ je direktna. Onda redom imamo

$$p + (r - t) = \dim L + \dim M = \dim L \oplus M \leq \dim V = r ,$$

odakle je $p - t \leq 0$, dakle $p \leq t$. Analogno bismo zaključili da je nužno $t \leq p$, pa je zaista $p = t$, kako se i tvrdilo.

Iz Tm. 2 slijedi da su p i q dobro definirani brojevi, jednoznačno određeni danom formom. Umjesto tih invarijanti uvodimo novu,

$$s = p - q \,, \tag{20}$$

koju nazivamo **signatura** kvadratne forme.

Kako je iz (4) i (20) odmah

$$p = \frac{r+s}{2} \quad , \quad q = \frac{r-s}{2} \,, \tag{21}$$

imamo zaključak da je normalni oblik forme jednoznačno određen rangom i signaturom te forme. Drugim riječima, rang i signatura određuju kvadratnu formu do na kongruenciju (izbor varijabli). Preciznije, vrijedi ova karakterizacija:

PROPOZICIJA 3

Realne kvadratne forme istog reda su kongruentne onda i samo onda ako imaju isti rang i istu signaturu.

Dokaz

Zbog Tm. 2 i Prop. 1 dvije su kvadratne forme kongruentne ako i samo ako imaju isti normalni oblik, a to će biti ako i samo ako imaju isti rang i istu signaturu. ■

Pomoću ranga i signature u mogućnosti smo definirati određene tipove formi. Neka je

$$Q(x) = \sum_{i,j=1}^{n} \alpha_{ij} x_i x_j \tag{22}$$

realna kvadratna forma reda n, neka je r njezin rang, a s signatura. Kako smo već rekli, ta je forma **regularna** (**nedegenerirana**) ako je $r = n$, odnosno **singularna** (**degenerirana**) ako je $r < n$. Iz (21) slijedi da uvijek vrijedi nejednakost

$$-n \leq -r \leq s \leq r \leq n \,. \tag{23}$$

Kažemo da je forma $Q(x)$ **indefinitna** ako je ispunjeno

$$-r < s < r \,.$$

U protivnom, forma je **semidefinitna**, i to:

(1) **pozitivno semidefinitna** (ili **pozitivna**) ako je $s = r$. Ako je pritom forma i regularna, kažemo da je **pozitivno definitna** (ili **strogo pozitivna**).

(2) **negativno semidefinitna** (ili **negativna**), ako je $s = -r$. Ako je forma i regularna, kažemo da je **negativno definitna** (ili **strogo negativna**).

Tip forme prema ovoj klasifikaciji zovemo **definitnost forme**. Iz definicije i Prop. 3 odmah slijedi

PROPOZICIJA 4

Kongruentne forme su iste definitnosti. ■

Kako zbog (21) uvjet $s = r$ povlači $q = 0$, a uvjet $s = -r$ daje $p = 0$, vrijedi

PROPOZICIJA 5

Kvadratna forma je:

(1) *pozitivna, ako i samo ako je njezin normalni oblik*

$$x_1^2 + x_2^2 + \cdots + x_r^2 ;$$

(2) *negativna, ako i samo ako je njezin normalni oblik*

$$-x_1^2 - x_2^2 - \cdots - x_r^2 . \quad ■$$

Kako je pritom za strogo pozitivne (negativne) forme $r = n$, odmah zaključujemo da su sve strogo pozitivne (negativne) forme istog reda međusobno kongruentne.

Nadalje, iz Prop. 4 i Prop. 5 odmah razabiremo

KOROLAR 6

Kvadratna forma $Q(x)$ je:

(1) *pozitivna, ako i samo ako je*

$$Q(x) \geq 0 ,$$

za svaki izbor varijabli $x = (x_1, \ldots, x_n)$, a strogo pozitivna ako i samo ako je

$$Q(x) > 0 ,$$

za svaki $x \neq (0, \ldots, 0)$;

(2) *negativna, ako i samo ako je*

$$Q(x) \leq 0\,,$$

za svaki izbor varijabli $x = (x_1, \ldots, x_n)$, *a strogo negativna ako i samo ako je*

$$Q(x) < 0\,,$$

za svaki $x \neq (0, \ldots, 0)$.

Dokaz

Trivijalan. Za karakterizaciju stroge pozitivnosti koristi Kor. 3 iz točke 11.5. ■

Kor. 6 sugerira ovu definiciju na razini funkcionala: Kvadratni funkcional

$$q : V \to \mathbb{R}$$

jest :

(1) **pozitivno semidefinitan** (**pozitivan**) ako je

$$q(x) \geq 0\,,$$

za svaki $x \in V$, a **pozitivno definitan** (**strogo pozitivan**) ako je pritom

$$q(x) > 0\,,$$

za svaki $x \neq \Theta$;

(2) **negativno semidefinitan** (**negativan**) ako je

$$q(x) \leq 0\,,$$

za svaki $x \in V$, a **negativno definitan** (**strogo negativan**) ako je pritom

$$q(x) < 0\,,$$

za svaki $x \neq \Theta$;

(3) **indefinitan**, ako nije ni pozitivno ni negativno semidefinitan.

Zbog Prop. 4 onda vrijedi

PROPOZICIJA 7

Kvadratni funkcional je pozitivan (negativan) ako i samo ako je njegov prikaz u nekoj (pa onda i svakoj) bazi prostora pozitivna (negativna) kvadratna forma. Analogna karakterizacija vrijedi i za strogo pozitivan (negativan) kvadratni funkcional. ■

Na kraju navedimo (vidi Zad. 4. koji slijedi, kao i Zad. 25. u 13.5.) ovaj poznati kriterij za prepoznavanje pozitivnih formi, odnosno funkcionala:

TEOREM 8 (Jacobijev kriterij)

Kvadratni funkcional (forma) je pozitivan ako i samo ako predznaci koeficijenata u karakterističnom polinomu matrice funkcionala (forme) alterniraju. Ako je pritom neki od koeficijenata jednak nuli, i koeficijenti koji ga slijede moraju biti jednaki nuli. ■

ZADACI

1. Dokaži: Kvadratna forma $Q(x)$ je regularna ako i samo ako $Q(x) = 0$ povlači da je $x = (0, \ldots, 0)$. Isto vrijedi i za kvadratne funkcionale.

2. Kvadratna forma je semidefinitna (definitna) ako su sve svojstvene vrijednosti pripadne matrice istog predznaka (i ako nijedna od njih nije jednaka nuli). Dokaži!

3. Kvadratna forma $Q(x) = ax_1^2 + bx_1x_2 + cx_2^2$, $a, b, c \in \mathbb{R}$, jest pozitivno definitna ako i samo ako je $a > 0$ i $b^2 - 4ac < 0$. Dokaži!

4. Neka je $q : V \to \mathbb{R}$ kvadratni funkcional, a $f : U \to V$ linearni operator. Onda je $q' = q \circ f : U \to \mathbb{R}$ također kvadratni funkcional. Nadalje, ako je q strogo pozitivan, onda je q' pozitivan funkcional. Ako je f injekcija, q' je strogo pozitivan. Dokaži!

5. Neka je U realni unitarni prostor, a $q : U \to \mathbb{R}$ kvadratni funkcional. Neka je $E = (e_1, \ldots, e_n)$ ortonormirana baza za U,

$$Q(x) = \sum_{i,j=1}^{n} \alpha_{ij} x_i x_j$$

prikaz funkcionala q u toj bazi, a $A = [\alpha_{ij}]$ njegova matrica. Neka je $f : U \to U$ linearni operator, definiran matricom A u bazi E. Operator f je, dakako, simetričan. Pokaži da pridruženje

$$q \mapsto f$$

ne ovisi o izboru (ortonormirane) baze. Pokaži, nadalje, da je q (strogo) pozitivan ako i samo ako je operator f (strogo) pozitivan (vidi točku 13.5.). Isto vrijedi i za (strogo) negativne funkcionale i operatore.

6. Uvjeri se da je svaka realna simetrična bilinearna forma kongruentna s formom

$$x_1y_1 + \cdots + x_py_p - x_{p+1}y_{p+1} - \cdots - x_{p+q}y_{p+q} ,$$

gdje je $r = p + q$ rang forme koju zovemo **normalni oblik** polazne forme (vidi Zad. 6. i Zad. 8. u 14.3.).

7. Dokaži da i za bilinearne forme vrijedi **zakon inercije**: Broj p pozitivnih i broj q negativnih koeficijenata u normalnom obliku simetrične bilinearne forme ne ovisi o načinu kako je forma svedena na taj oblik. Ti su brojevi, dakle, isti za sve normalne oblike jedne forme.

8. Signaturu simetrične bilinearne forme definiramo kao $s = p - q$. Takve forme su kongruentne onda i samo onda ako imaju isti rang i istu signaturu. Dokaži!

9. Pojam definitnosti za simetrične bilinearne forme definiramo na isti način kao za kvadratne forme. Kongruentne forme su, dakako, iste definitnosti. Pokaži: Bilinearna forma $\Phi(x, y)$ je pozitivna ako i samo ako je $\Phi(x, x) \geq 0$ za svaki izbor varijabli $x = (x_1, \ldots, x_n)$, a strogo pozitivna ako i samo ako je $\Phi(x, x) > 0$ za $x \neq (0, \ldots, 0)$. Analogno se karakterizira negativna i strogo negativna forma.

10. Definiraj i karakteriziraj definitnost za simetrične bilinearne funkcionale.

11. **Par** kvadratnih formi $P(x)$ i $Q(x)$ je **kongruentan s parom** $P_1(y)$ i $Q_1(y)$ ako je forma P kongruentna s P_1 i forma Q s Q_1, pomoću iste transformacije koordinata. Pokaži da je to slučaj ako i samo ako postoji regularna matrica T takva da vrijedi

$$A_1 = T' A T , \quad B_1 = T' B T ,$$

gdje su A i A_1 matrice formi P i P_1, a B i B_1 matrice formi Q i Q_1.

12. Svaki par $P(x)$, $Q(x)$ realnih kvadratnih formi, gdje je $P(x)$ strogo pozitivna forma, kongruentan je s parom

$$\begin{aligned} P_1(y) &= y_1^2 + \cdots + y_n^2 , \\ Q_1(y) &= \lambda_1 y_1^2 + \cdots + \lambda_n y_n^2 , \end{aligned}$$

gdje su brojevi $\lambda_1, \ldots, \lambda_n$ (do na poredak) jednoznačno određeni polaznim formama, tj. ne ovise o načinu svođenja na ovaj, jednostavniji oblik. Točnije, ti brojevi su korijeni jednadžbe

$$\det(B - \lambda A) = 0 ,$$

gdje je A matrica forme P, a B matrica forme Q (vidi i Zad. 29. u 13.5.).

13. Dokaži ovaj teorem (J. Milnor): Neka su $P(x)$ i $Q(x)$ realne kvadratne forme reda n, gdje je $n \geq 3$ i vrijedi da

$$P(x) = Q(x) = 0$$

povlači $x = (0, \ldots, 0)$. Onda se te forme mogu istom transformacijom svesti na normalne oblike, tj. kongruentne su s parom dijagonalnih formi. U slučaju $n = 2$ teorem nije točan, jer se npr. forme $P(x) = x_1^2 - x_2^2$ i $Q(x) = 2x_1x_2$ ne mogu istodobno dijagonalizirati.

14. Definiraj pojam kongruencije parova za bilinearne forme i dokaži izreke analogne onima u Zad. 12. i Zad. 13. Formuliraj te izreke u terminima bilinearnih, odnosno kvadratnih funkcionala.

14.5. Hermitski funkcionali i pripadne forme

Rezultati iz prethodne točke općenito nisu istiniti ako umjesto realnih formi dopustimo forme nad poljem kompleksnih brojeva. Međutim, malom modifikacijom definicija i izreka, tipičnom za kompleksni slučaj, većina rezultata ostat će vrijediti i dalje.

Neka je V linearni prostor nad poljem $\mathbb{C}$ kompleksnih brojeva. Za razliku od opće definicije iz 14.1., **kompleksni bilinearni funkcional** je preslikavanje

$$\varphi : V \times V \to \mathbb{C}$$

koje je linearno u prvoj, a hermitski linearno u drugoj varijabli*), tj. za koje vrijedi biaditivnost, tj.

(1) $\varphi(x_1 + x_2, y) = \varphi(x_1, y) + \varphi(x_2, y)$;

(2) $\varphi(x, y_1 + y_2) = \varphi(x, y_1) + \varphi(x, y_2)$,

i homogenost u prvoj, a hermitska homogenost u drugoj varijabli, tj.

(3) $\varphi(\alpha x, y) = \alpha\, \varphi(x, y)$;

(4) $\varphi(x, \beta y) = \overline{\beta}\, \varphi(x, y)$,

*) Uobičajen je još i naziv **seskvilinearni** funkcional, što znači jedan-i-pol linearni.

gdje su $x, y, x_i, y_i \in V$ bilo koji vektori, a $\alpha, \beta \in \mathbb{C}$ skalari. Potezom je, kao i obično, označena operacija konjugiranja kompleksnog broja.

Ako je za takav funkcional ispunjeno još i

$$\varphi(x, y) = \overline{\varphi(y, x)}\,, \tag{5}$$

za svaki $x, y \in V$, kažemo da je φ **hermitski simetričan** ili, kraće, **hermitski bilinearni funkcional**. Ako je pak ispunjeno

$$\varphi(x, y) = -\overline{\varphi(y, x)}\,, \tag{6}$$

za svaki $x, y \in V$, onda kažemo da je φ **hermitski antisimetričan** ili, kraće, **antihermitski bilinearni funkcional**.

Odmah se vidi da je u definiciji hermitskog funkcionala dovoljno zahtijevati linearnost u prvoj varijabli i hermitsku simetriju, jer uvjeti (1), (3) i (5) očito povlače (2) i (4). Analogna tvrdnja vrijedi i za antihermitski funkcional. Primijetimo, nadalje, da je zbog (5) odnosno (6) za svaki $x \in V$

$$\varphi(x, x) \tag{7}$$

realan broj u slučaju hermitskog funkcionala, odnosno **čisto imaginaran broj** ako je φ antihermitski funkcional.

PROPOZICIJA 1

Kompleksni funkcional jednoznačno je određen svojim djelovanjem na bazi prostora. Drugim riječima, ako je $(a_1, \ldots, a_n) \subset V$ baza prostora V, a $\alpha_{ij} \in \mathbb{C}$, $i, j = 1, \ldots, n$, bilo koji izbor skalara, onda uvijek postoji jedan i samo jedan kompleksni bilinearni funkcional

$$\varphi : V \times V \to \mathbb{C}\,,$$

za koji vrijedi

$$\varphi(a_i, a_j) = \alpha_{ij}\,,$$

za sve $i, j = 1, \ldots, n$.

Dokaz

Analogan dokazu Prop. 1 u 14.1. ∎

Iz dokaza se razabire da funkcional u danoj bazi ima prikaz

$$\varphi(x, y) = \sum_{i,j=1}^{n} \alpha_{ij} x_i \overline{y}_j = X' A \overline{Y} = Y^* A X\,, \tag{8}$$

gdje su $X = [x_i]$ i $Y = [y_i]$ koordinatne matrice vektora $x, y \in V$, a Y^*, dakako, označava adjungiranu (hermitski konjugiranu) matricu od Y. Nadalje, $A = [\alpha_{ij}]$ je **matrica funkcionala** u promatranoj bazi.

Ako je B matrica tog istog funkcionala u nekoj drugoj bazi, vrijedi

$$B = T^* \cdot A \cdot T \,, \tag{9}$$

gdje je T matrica prijelaza iz jedne baze u drugu (vidi Prop. 2 u 14.1.). Prema tome, matrice istog funkcionala u različitim bazama su **hermitski kongruentne** (Zad. 19. u 9.5.).

Nas će posebno zanimati hermitski bilinearni funkcionali. Matrica takvog funkcionala je uvijek **hermitska**, jer vrijedi

$$\alpha_{ij} = \varphi(a_i, a_j) = \overline{\varphi(a_j, a_i)} = \overline{\alpha_{ji}} \,,$$

za svaki i i j, dakle $A = A^*$. Lako se vidi da vrijedi i obrat, tj. da to svojstvo karakterizira hermitske funkcionale.

Neka je sada $\varphi : V \times V \to \mathbb{C}$ hermitski bilinearni funkcional, a

$$q : V \to \mathbb{C}$$

funkcional na V definiran s

$$q(x) = \varphi(x, x) \,, \tag{10}$$

za svaki $x \in V$. Onda kažemo da je q **hermitski kvadratni funkcional**, ili kraće, **hermitski funkcional**, generiran s φ.

PROPOZICIJA 2

Hermitski kvadratni funkcional $q : V \to \mathbb{C}$ ima ova svojstva:

(1) $q(x + y) + q(x - y) = 2q(x) + 2q(y)$;

(2) $q(x)$ *je realan broj;*

(3) $q(ix) = q(x)$,

za svaki $x, y \in V$.

Dokaz

(1) smo provjerili u Prop. 1 iz 14.2. Tvrdnja (2) je očigledna. Pokažimo da vrijedi relacija (3):

$$q(ix) = \varphi(ix, ix) = i \cdot \bar{i} \cdot \varphi(x, x) = \varphi(x, x) = q(x) \,,$$

čime je propozicija dokazana. ■

Primijetimo da je hermitskim funkcionalom jednoznačno određen hermitski bilinearni funkcional koji ga generira (vidi Zad. 4.).

U danoj bazi prostora V hermitski funkcional zbog (8) ima prikaz

$$q(x) = \sum_{i,j=1}^{n} \alpha_{ij} x_i \overline{x}_j = X^* A X , \tag{11}$$

gdje je matrica $A = [\alpha_{ij}]$ funkcionala, dakako, hermitska. Njezin je rang invarijantan (neovisan o izboru baze) i nazivamo ga **rang hermitskog funkcionala**.

Funkciju

$$Q : \underbrace{\mathbb{C} \times \cdots \times \mathbb{C}}_{n} \to \mathbb{C} ,$$

definiranu s

$$Q(x) = Q(x_1, \ldots, x_n) = \sum_{i=1}^{n} \sum_{j=1}^{n} \alpha_{ij} x_i \overline{x}_j , \tag{12}$$

gdje je matrica koeficijenata $A = [\alpha_{ij}]$ hermitska, nazivamo **hermitska forma reda** n u (kompleksnim) varijablama $x_1, \ldots, x_n$. Forma je **ranga** r ako je r rang njezine matrice A. Ako s $X = [x_i]$ označimo stupčanu matricu varijabli, formu (12) možemo zapisati kao

$$Q(x) = X^* \cdot A \cdot X . \tag{13}$$

Uspoređujući (11) i (13) odmah razabiremo da se hermitske forme prirodno pojavljuju kao prikazi hermitskih funkcionala u bazi prostora.

Dvije forme su jednake ako i samo ako imaju istu matricu. Kažemo da je forma $Q(x)$ **kongruentna** s formom $Q(y)$ ako postoji regularna matrica T takva da transformacija varijabli

$$X = T Y$$

prevodi prvu formu u drugu. Radi se, očito, o dobro definiranoj relaciji ekvivalencije. Kažemo da je kongruencija formi **unitarna** ako je matrica T transformacije varijabli unitarna, tj. vrijedi $T^* = T^{-1}$.

PROPOZICIJA 3

Dvije hermitske forme su kongruentne ako i samo ako su njihove matrice hermitski kongruentne, dakle (geometrijski), ako i samo ako čine prikaze istog hermitskog funkcionala.

Dokaz

Pokažimo npr. dovoljnost. Neka su

$$Q(x) = X^*AX \qquad \text{i} \qquad Q(y) = Y^*AY$$

hermitske forme sa svojstvom da su njihove matrice hermitski kongruentne, tj. da postoji regularna matrica T takva, da je $B = T^*AT$. Ako na prvu formu primijenimo transformaciju varijabli $X = TY$, imamo

$$\begin{aligned} Q(x) &= X^*AX = (TY)^*A(TY) = \\ &= Y^*(T^*AT)Y = Y^*BY = Q(y)\,, \end{aligned}$$

pa su forme zaista kongruentne. Drugi dio tvrdnje izlazi neposredno iz relacije (9), gdje T treba interpretirati kao matricu prijelaza iz jedne baze prostora u drugu. ■

PROPOZICIJA 4

Svaka hermitska forma kongruentna je s nekom dijagonalnom formom

$$\alpha_1 x_1 \overline{x}_1 + \cdots + \alpha_r x_r \overline{x}_r = \alpha_1 |x_1|^2 + \cdots + \alpha_r |x_r|^2\,,$$

gdje je r rang polazne forme, a koeficijenti $\alpha_1, \ldots, \alpha_r \neq 0$ su realni. Geometrijski gledano, za svaki hermitski funkcional postoji baza prostora u kojoj on ima realnu dijagonalnu matricu.

Dokaz

Neka je A matrica dane hermitske forme. Onda je A hermitska matrica, pa je prema Zad. 11. u 13.5. unitarno slična s nekom dijagonalnom matricom D, tj. postoji unitarna matrica U sa svojstvom da je $D = U^{-1}AU$. Kako je, međutim, U unitarna matrica, vrijedi da je $U^{-1} = U^*$, i odatle $D = U^*AU$, što po definiciji znači da je matrica D hermitski (čak unitarno, vidi Zad. 19. i Zad. 20. u 9.5.) kongruentna s matricom A. Primijetimo da je, zbog $A^* = A$ i matrica D hermitska, jer vrijedi $D^* = (U^*AU)^* = U^*A^*U = U^*AU = D$, a u takvoj su matrici elementi na glavnoj dijagonali uvijek realni (vidi Zad. 10. u 13.5.).

Prema tome, D jednoznačno određuje hermitsku formu oblika

$$\alpha_1 x_1 \overline{x}_1 + \cdots + \alpha_r x_r \overline{x}_r\,,$$

gdje su koeficijenti α_i realni i različiti od nule. Konačno, prema Prop. 3, ta je forma kongruentna s polaznom. Kako je dijagonalna forma očito ranga r,

a kongruentne forme imaju isti rang, to je r rang polazne forme i tvrdnja je dokazana. ■

Iz dokaza se razabire da se uvijek može postići da transformacija varijabli koja prevodi danu formu u dijagonalnu bude unitarna, tj. da je kongruencija tih formi unitarna (vidi i Zad. 6.).

Svaka dijagonalna forma kongruentna s hermitskom formom $Q(x)$ zove se **kanonski oblik** forme $Q(x)$. Nadalje, koeficijenti u kanonskom obliku su uvijek realni (Zad. 7.). Svaka baza prostora u kojoj hermitski funkcional ima dijagonalni prikaz zove se **kanonska baza** za taj funkcional.

Općenito, hermitsku formu moguće je dijagonalizirati, svesti na kanonski oblik na razne načine. Ako ne inzistiramo na unitarnosti primijenjene transformacije, standardni postupak kojim se to postiže je **Lagrangeov algoritam**, detaljno opisan u 14.3., koji se bez ikakvih modifikacija može primijeniti i na hermitske forme.

Neka je

$$\alpha_1 x_1 \overline{x}_1 + \cdots + \alpha_p x_p \overline{x}_p + \alpha_{p+1} x_{p+1} \overline{x}_{p+1} + \cdots + \alpha_{p+q} x_{p+q} \overline{x}_{p+q}$$

bilo koji kanonski oblik dane hermitske forme, $p+q=r$. Pretpostavimo da su varijable numerirane tako da za (realne!) koeficijente vrijedi

$$\alpha_1, \ldots, \alpha_p > 0 \quad , \quad \alpha_{p+1}, \ldots, \alpha_{p+q} < 0 \, .$$

Onda daljnjom transformacijom

$$x_i = (\sqrt{\alpha_i})^{-1} \; y_i \quad , \quad i = 1, \ldots, p \, ,$$

$$x_j = (\sqrt{-\alpha_j})^{-1} \; y_j \quad , \quad j = p+1, \ldots, p+q \, ,$$

dolazimo do forme

$$y_1 \overline{y}_1 + \cdots + y_p \overline{y}_p - y_{p+1} \overline{y}_{p+1} - \cdots - y_{p+q} \overline{y}_{p+q} \, ,$$

koja je očito kongruentna (ali ne nužno unitarno) s polaznom formom, i koja se zove **normalni oblik** te forme. I ovdje vrijedi

TEOREM 5 (Zakon inercije)

Normalni oblik hermitske forme ne ovisi o načinu svođenja na taj oblik. Drugim riječima, broj pozitivnih i broj negativnih koeficijenata isti su u svim kanonskim (normalnim) oblicima dane hermitske forme.

Dokaz

Isti kao dokaz Tm. 2 u 14.4. ■

Prema tome, danom formom jednoznačno su određeni brojevi

$$r = p + q \quad , \quad s = p - q \, ,$$

tj. njezin rang i **signatura**, i tim je podacima forma određena do na izbor varijabli. To zapravo znači da dvije hermitske forme imaju isti rang i signaturu ako i samo ako su kongruentne. Odatle, zbog Prop. 3, slijedi da su rang i signatura dobro definirani pojmovi vezani uz hermitski funkcional.

Hermitska forma $Q(x)$ je **indefinitna** ako je

$$-r < s < r \, ,$$

a **semidefinitna** ako je

$$s = r \quad \text{ili} \quad s = -r \, .$$

U slučaju kad je $s = r$, govorimo o **pozitivno semidefinitnoj (pozitivnoj)** formi, a ako je $s = -r$, o **negativno semidefinitnoj (negativnoj)** formi. Ako je k tome $r = n$, tj. ako je forma i regularna, kažemo da je **pozitivno**, odnosno **negativno definitna** (**strogo pozitivna**, odnosno **strogo negativna**) .

Analogno se definira indefinitnost i pozitivna odnosno negativna semidefinitnost (definitnost) hermitskog funkcionala.

Kongruentne forme su, dakako, iste definitnosti pa vrijedi

PROPOZICIJA 6

Hermitska forma $Q(x)$ jest:

(1) *pozitivna, ako i samo ako je*

$$Q(x) \geq 0 \, ,$$

za svaki izbor varijabli $x = (x_1, \ldots, x_n)$, a strogo pozitivna, ako i samo ako je

$$Q(x) > 0 \, ,$$

za svaki $x \neq (0, \ldots, 0)$;

(2) *negativna, ako i samo ako je*

$$Q(x) \leq 0 \, ,$$

za svaki izbor varijabli $x = (x_1, \ldots, x_n)$, a strogo negativna, ako i samo ako je

$$Q(x) < 0 \, ,$$

za svaki $x \neq (0, \ldots, 0)$. ■

Zapišimo i analognu izreku za funkcionale:

PROPOZICIJA 7

Hermitski funkcional $q : V \to \mathbb{C}$ *jest:*

(1) *pozitivan, ako i samo ako je*

$$q(x) \geq 0 ,$$

za svaki $x \in V$, *a strogo pozitivan, ako i samo ako je*

$$q(x) > 0 ,$$

za svaki $x \neq \Theta$;

(2) *negativan, ako i samo ako je*

$$q(x) \leq 0 ,$$

za svaki $x \in V$, *a strogo negativan, ako i samo ako je*

$$q(x) < 0 ,$$

za svaki $x \neq \Theta$. ■

Kako svojstva iz Prop. 6 (Prop. 7) karakteriziraju pozitivnu, odnosno negativnu semidefinitnost i definitnost forme (funkcionala), često se uzimaju i kao definicije tih pojmova.

I za hermitske forme vrijedi **Jacobijev kriterij** za utvrđivanje pozitivnosti (Zad. 8.).

Na kraju, nekoliko riječi o bilinearnim formama. **Kompleksna bilinearna forma** u sustavima varijabli $x_1, \ldots, x_n$ i $y_1, \ldots, y_n$ jest svaka funkcija

$$\Phi : \underbrace{\mathbb{C} \times \cdots \times \mathbb{C}}_{n} \times \underbrace{\mathbb{C} \times \cdots \times \mathbb{C}}_{n} \to \mathbb{C}$$

dana s

$$\begin{aligned} \Phi(x, y) &= \Phi(x_1, \ldots, x_n; y_1, \ldots, y_n) = \\ &= \sum_{i,j=1}^{n} \alpha_{ij} x_i \overline{y}_j = Y^* A X , \end{aligned}$$

gdje je $A = [\alpha_{ij}]$ neka kompleksna matrica. Iz (8) se vidi da se takve forme prirodno pojavljuju kao prikazi kompleksnih bilinearnih funkcionala u danoj bazi.

Ako je matrica forme hermitska, govorimo o **hermitskoj bilinearnoj formi**, i ona se, dakako, može interpretirati kao prikaz hermitskog bilinearnog funkcionala. Zato je za takvu formu

$$\Phi(x,x)$$

realan broj, za svaki izbor varijabli.

Prirodna korespondencija između bilinearnih i kvadratnih hermitskih funkcionala i njihovih teorija prenosi se i na pripadne forme. Zato se posve analogno kao u slučaju hermitskih kvadratnih formi pokazuje da se svaka hermitska bilinearna forma može transformacijom varijabli (istom za oba sustava)

$$X = TU \quad , \quad Y = TV$$

svesti na **kanonski oblik**

$$\alpha_1 u_1 \overline{v}_1 + \cdots + \alpha_r u_r \overline{v}_r \ ,$$

gdje je r rang forme, a koeficijenti $\alpha_1, \ldots, \alpha_r \neq 0$ su realni. To se postiže npr. Lagrangeovim algoritmom. Korak dalje, očiglednom transformacijom dolazimo do **normalnog oblika**

$$\xi_1 \overline{\eta}_1 + \cdots + \xi_p \overline{\eta}_p - \xi_{p+1} \overline{\eta}_{p+1} - \cdots - \xi_r \overline{\eta}_r$$

polazne forme. Pritom vrijedi zakon inercije (vidi Tm. 5), pa su dobro definirani **rang** i **signatura** za hermitsku bilinearnu formu.

Pomoću njih definiramo **indefinitnost** i **pozitivnu**, odnosno **negativnu semidefinitnost** (**definitnost**) hermitske bilinearne forme, pa onda i hermitskog bilinearnog funkcionala, posve analogno kao u slučaju kvadratnih hermitskih formi i funkcionala. Pritom vrijede karakterizacije analogne onima u Prop. 6 i Prop. 7. Napose, vrijedi

PROPOZICIJA 8

Hermitski bilinearni funkcional

$$\varphi : V \times V \to \mathbb{C}$$

jest:

(1) *pozitivan, ako i samo ako je*

$$\varphi(x,x) \geq 0 \ ,$$

za svaki $x \in V$, *a strogo pozitivan, ako i samo ako je*

$$\varphi(x,x) > 0 \ ,$$

za svaki $x \neq \Theta$;

(2) *negativan, ako i samo ako je*

$$\varphi(x,x) \leq 0\,,$$

za svaki $x \in V$, *a strogo negativan, ako i samo ako je*

$$\varphi(x,x) < 0\,,$$

za svaki $x \neq \Theta$. ■

Svojstva iz Prop. 8 mogu se uzeti i za definiciju pozitivne, odnosno negativne semidefinitnosti (definitnosti) hermitskog bilinearnog funkcionala.

Za više detalja iz teorije hermitskih bilinearnih formi vidi Zad. 11.–24.

ZADACI

1. Uvjeri se da većina rezultata u ovoj točki ostaje sačuvana uzmemo li u definiciji kompleksnih i hermitskih funkcionala umjesto polja $\mathbb{C}$ bilo koje njegovo potpolje. Posebno, kao specijalni slučaj dobivamo teoriju realnih funkcionala i pripadnih formi.

2. Dokaži: Kompleksni bilinearni funkcional je antihermitski ako i samo ako je (svaka) njegova matrica antihermitska.

3. Dokaži: Svaki se kompleksni bilinearni funkcional može jednoznačno prikazati kao suma jednog hermitskog i jednog antihermitskog funkcionala. Pokaži nadalje, da (za razliku od hermitskih i antihermitskih funkcionala) kompleksni bilinearni funkcionali na istom prostoru V čine linearni prostor i da je taj prostor izomorfan s $\hom V$.

4. Kvadratne funkcionale možemo uvesti i aksiomatski. Svaki **neprekidni** funkcional $q : V \to \mathbb{C}$ koji ima svojstva:

   (1) $q(x+y) + q(x-y) = 2q(x) + 2q(y)$;

   (2) $q(x)$ je realan broj;

   (3) $q(ix) = q(x)$,

   za svaki izbor $x, y \in V$, nazivamo **hermitski kvadratni funkcional** na V. Pokaži da za svaki hermitski kvadratni funkcional q postoji i jednoznačno je određen hermitski bilinearni funkcional $\varphi : V \times V \to \mathbb{C}$, takav da vrijedi $q(x) = \varphi(x,x)$, za svaki $x \in V$. [Uputa: Uzmi

$$\varphi(x,y) = \frac{1}{4}[q(x+y) - q(x-y)] + \frac{1}{4}[q(x+iy) - q(x-iy)]\,.]$$

5. Kako smo već prije spominjali (Zad. 20. u 9.5.), matrice A i B su **unitarno kongruentne** ako postoji unitarna matrica U takva, da je $B = U^* A U$. Pokaži da su dvije hermitske forme unitarno kongruentne ako i samo ako su njihove matrice unitarno kongruentne.

6. Dokaži ovu strožu formulaciju Prop. 4: Svaka hermitska kvadratna forma unitarno je kongruentna s formom

$$\alpha_1 x_1 \overline{x}_1 + \cdots + \alpha_r x_r \overline{x}_r \ ,$$

kojoj je r rang, a $\alpha_1, \ldots, \alpha_r \neq 0$ od nule različite svojstvene vrijednosti matrice (vidi Zad. 5 u 10.9.) polazne forme. Prema tome, da bi dvije hermitske forme bile unitarno kongruentne, nužno je i dovoljno da matrice tih formi imaju iste karakteristične polinome.

7. Uvjeri se da su u svakom kanonskom obliku hermitske forme koeficijenti realni!

8. Dokaži: Hermitska forma je pozitivna ako i samo ako koeficijenti u karakterističnom polinomu njezine matrice alterniraju predznak. Ako je pritom neki koeficijent nula, svi koeficijenti uz niže potencije varijable moraju također biti nula.

9. Pokaži: Hermitska forma s matricom A je strogo pozitivna ako i samo ako postoji regularna matrica B, takva da je $A = B B^*$. [Uputa: Forma je strogo pozitivna ako i samo ako vrijedi $T^* A T = E$, gdje je E jedinična matrica.]

10. Dokaži: Hermitska forma je pozitivna (strogo pozitivna), ako su nule karakterističnog polinoma njezine matrice nenegativne (pozitivne). Analogna tvrdnja vrijedi i za negativnu (strogo negativnu) formu.

11. Kompleksni bilinearni funkcional je **regularan** ako je maksimalnog ranga, a inače je **singularan**. Pokaži da je takav funkcional $\varphi(x, y)$ singularan ako i samo ako postoji vektor $x_0 \neq \Theta$, takav da je $\varphi(x_0, y) = 0$, za svaki $y \in V$. Karakteriziraj analogno singularnost (degeneriranost) kompleksne bilinearne forme.

12. **Ekvivalentnost** kompleksnih bilinearnih formi definira se kao u Zad. 4. u 14.3. Pokaži da su takve forme ekvivalentne ako i samo ako su istog reda i istog ranga.

13. **Kongruencija** kompleksnih bilinearnih formi definira se kao u Zad. 6. u 14.3. Pokaži da su takve forme kongruentne ako i samo ako su njihove matrice hermitski kongruentne, dakle, (zbog (9) u tekstu) ako i samo ako su prikazi istog bilinearnoga funkcionala.

14. Svaka hermitska bilinearna forma kongruentna je svom kanonskom obliku

$$\alpha_1 x_1 \overline{y}_1 + \cdots + \alpha_r x_r \overline{y}_r$$

gdje je r rang forme, a koeficijenti $\alpha_i \neq 0$ su realni. Pritom se može postići da ta kongruencija bude unitarna i u tom su slučaju $\alpha_1, \ldots, \alpha_r$ od nule različiti korijeni karakteristične jednadžbe matrice polazne forme. Dokaži!

15. Svaka hermitska bilinearna forma kongruentna je svom normalnom obliku

$$x_1 \overline{y}_1 + \cdots + x_p \overline{y}_p - x_{p+1} \overline{y}_{p+1} - \cdots - x_r \overline{y}_r \,,$$

gdje je r rang forme. Svedi forme:

(a) $4x_1\overline{y}_1 + (1+i)x_1\overline{y}_2 + (1-i)x_2\overline{y}_1 + x_2\overline{y}_2$;

(b) $x_1\overline{y}_n + x_2\overline{y}_{n-1} + \cdots + x_n\overline{y}_1$

na normalni oblik i nađi matricu transformacije varijabli.

16. Dokaži zakon inercije za hermitske bilinearne forme.

17. Korespondencija

$$\sum_{i,j} \alpha_{ij} x_i \overline{x}_j \mapsto \sum_{i,j} \alpha_{ij} x_i \overline{y}_j$$

uspostavlja bijektivnu vezu između kvadratnih i bilinearnih hermitskih formi. Potonju formu nazivamo **polarna forma** dane hermitske kvadratne forme. Ako je hermitska forma prikaz hermitskog funkcionala u nekoj bazi, uvjeri se da je njezina polarna forma prikaz tom funkcionalu pridruženog (Zad. 4.) hermitskog bilinearnog funkcionala u istoj bazi.

18. Hermitske bilinearne forme su kongruentne ako i samo ako imaju isti rang i signaturu. Prema tome, dobro je definiran **rang** i **signatura hermitskog bilinearnog funkcionala** kao rang, odnosno signatura (bilo kojeg) njegova prikaza u bazi. Pokaži da rang i signatura funkcionala moraju biti iste parnosti.

19. Kongruentne forme su iste definitnosti. Pokaži: Hermitska bilinearna forma $\Phi(x, y)$ pozitivna je ako je $\Phi(x, x) \geq 0$, za svaki izbor varijabli, a strogo pozitivna ako i samo ako je $\Phi(x, x) > 0$, za sve $x \neq (0, \ldots, 0)$. Analogno se karakterizira i negativna te strogo negativna forma. Odatle, i zbog činjenice da (strogo) pozitivne, odnosno negativne forme čine prikaze istih takvih hermitskih funkcionala, dokaži Prop. 8.

20. Neka je $S = \{a_1, \ldots, a_k\} \subset V$ skup vektora iz V, a $\varphi : V \times V \to \mathbb{C}$ regularni hermitski bilinearni funkcional. Onda matricu

$$G(\varphi; S) = \begin{bmatrix} \varphi(a_1, a_1) & \cdots & \varphi(a_1, a_k) \\ \vdots & & \vdots \\ \varphi(a_k, a_1) & \cdots & \varphi(a_k, a_k) \end{bmatrix}$$

nazivamo **Gramova matrica** skupa S **s obzirom na funkcional** φ. Ta je matrica, dakako, hermitska. Pokaži: Skup S je linearno nezavisan ako i samo ako je njegova Gramova matrica regularna.

21. Pod kojim se uvjetom hermitska kvadratna forma može prikazati kao produkt linearnih formi?

22. Pojam **kongruencije para** bilinearnih (kvadratnih) hermitskih formi definira se kao u Zad. 11. u 14.4. Dokaži teorem analogan onome u Zad. 12. iz 14.4.

23. Dokaži ovaj teorem (H. Kraljević): Neka su $\Phi(x, y)$ i $\Psi(x, y)$ hermitske bilinearne forme istog reda, takve da

$$\Phi(x, x) = \Psi(x, x) = 0$$

povlači da je $x = (0, \ldots, 0)$. Onda je par Φ, Ψ kongruentan s parom dijagonalnih formi. Analogni teorem vrijedi za hermitske kvadratne forme. Formuliraj teorem u terminima hermitskih funkcionala.

24. Neka je $\varphi : V \times V \to \mathbb{C}$ hermitski bilinearni funkcional, a

$$I = \{x \in V \mid \varphi(x, y) = 0, \ \forall y \in V\} .$$

Onda je $I \subset V$ potprostor koji zovemo **izotropni prostor** (ili također **prostor degeneracije** ili **nulprostor**) za funkcional φ. Njegova dimenzija d je jednaka

$$d = n - r ,$$

gdje je n dimenzija od V, a r rang od φ, i nazivamo je **defekt** od φ. Funkcional φ je regularan ako i samo ako je $d = 0$. Definiraj te pojmove za hermitski kvadratni funkcional.

14.6. Pseudounitarni prostori

Koristeći se bilinearnim funkcionalima, pojam unitarnog prostora možemo poopćiti.

Neka je U linearni prostor nad poljem F kompleksnih ili realnih brojeva, a

$$\varphi : U \times U \to F$$

neka je strogo pozitivni hermitski bilinearni funkcional na tom prostoru. Uspoređujući svojstva takvog funkcionala s aksiomima skalarnog množenja (vidi točku 12.2.), odmah razabiremo da je s φ na prostoru U definiran jedan skalarni produkt, i prema tome je par (U, φ) unitarni prostor.

Tu situaciju sada generaliziramo. Ako je

$$\psi : U \times U \to F$$

bilo koji **regularni** (ne nužno pozitivno definitni) hermitski bilinearni funkcional, uređeni par (U, ψ) nazivamo **pseudounitarni prostor**. Kažemo još da je U pseudounitarni prostor nad poljem F, s **osnovnim funkcionalom** ψ. Prostor je **kompleksan** ako je $F = \mathbb{C}$, a **realan** za $F = \mathbb{R}$ (u tom je slučaju ψ, dakako, simetrični bilinearni funkcional). Dimenzija pseudounitarnog prostora je po definiciji jednaka dimenziji pripadnog linearnog prostora.

Uz kraću oznaku

$$\psi(x, y) = (x, y) \ ,$$

možemo reći da je osnovnim funkcionalom ψ na prostoru U definirano **pseudoskalarno množenje** , s ovim svojstvima:

(1) hermitska komutativnost: $(y, x) = \overline{(x, y)}$;

(2) kvaziasocijativnost: $(\lambda x, y) = \lambda\,(x, y)$;

(3) distributivnost: $(x_1 + x_2, y) = (x_1, y) + (x_2, y)$,

za svaki izbor $x, x_1, x_2, y \in U$ i $\lambda \in F$.

Za pseudounitarni prostor definiramo **signaturu** kao signaturu pripadnog osnovnog funkcionala. Lako se vidi (jer je funkcional regularan!) da signatura mora biti iste parnosti kao i dimenzija prostora.

Neka je U pseudounitarni prostor dimenzije n i signature s. Iz razmatranja u točki 14.5. slijedi da za taj prostor postoji baza $E = (e_1, \ldots, e_n)$ sa svojstvom da je za vektore $x = (\alpha_i)$, $y = (\beta_i)$ iz U, dane svojim koordinatama u toj bazi, njihov pseudoskalarni produkt opisan formulom

$$(x, y) = \alpha_1\overline{\beta}_1 + \cdots + \alpha_p\overline{\beta}_p - \alpha_{p+1}\overline{\beta}_{p+1} - \cdots - \alpha_n\overline{\beta}_n \ , \qquad (1)$$

gdje je $p = \dfrac{n+s}{2}$. Bazu s tim svojstvom nazivamo **normalna baza** prostora U. Za nju vrijedi

$$(e_i, e_j) = \begin{cases} 0 & , \quad i \neq j \\ 1 & , \quad i = j \leq p \\ -1 & , \quad i = j > p \end{cases} .$$

Za sve normalne baze prostora U broj p je isti (zakon inercije).

Sad nije teško klasificirati pseudounitarne prostore. Operator

$$f : U \to V$$

jest **izomorfizam pseudounitarnih prostora** ako je f izomorfizam linearnih prostora i čuva pseudoskalarni produkt, tj. ako vrijedi

$$(f(x), f(y)) = (x, y) ,$$

za svaki izbor $x, y \in U$. Pseudounitarni prostori U i V su **izomorfni** ako postoji bar jedan takav izomorfizam $f : U \to V$. Vrijedi

PROPOZICIJA 1

Pseudounitarni prostori nad istim poljem su izomorfni ako i samo ako imaju istu dimenziju i istu signaturu.

Dokaz

Neka je $f : U \to V$ izomorfizam pseudounitarnih prostora. Onda je $\dim U = \dim V$, a kako f prevodi normalnu bazu u U na normalnu bazu u V, zaključujemo da ti prostori imaju i iste signature. Obratno, neka su U i V prostori dimenzije n i signature s, a $(a_1, \ldots, a_n) \subset U$ i $(b_1, \ldots, b_n) \subset V$ normalne baze. Definirajmo $f : U \to V$ stavljajući $f(a_i) = b_i$, $i = 1, \ldots, n$, i proširujući linearno. Onda je f izomorfizam linearnih prostora, a lako se provjeri da vrijedi i $(f(x), f(y)) = (x, y)$, za svaki $x, y \in U$, pa je tvrdnja dokazana. ∎

Prema tome pseudounitarne prostore iste dimenzije n klasificira njihova signatura, pa tako imamo prostore sa signaturama

$$s = n,\ n-2, \ldots,\ -n .$$

Standardni model realnog pseudounitarnog prostora sa signaturom s je $\mathbb{R}^n$ zajedno s pseudoskalarnim produktom

$$(x, y) = \alpha_1\beta_1 + \cdots + \alpha_p\beta_p - \alpha_{p+1}\beta_{p+1} - \cdots - \alpha_n\beta_n ,$$

gdje je $p = \dfrac{n+s}{2}$. On se obično naziva **pseudoeuklidski prostor** (signature s). U slučaju kompleksnih prostora, standardni je model $\mathbb{C}^n$ s pseudoskalarnim produktom danim formulom (1). Ako je npr. $n = 4$, a $s = 2$, imamo

$$(x, y) = \alpha_1\overline{\beta}_1 + \alpha_2\overline{\beta}_2 + \alpha_3\overline{\beta}_3 - \alpha_4\overline{\beta}_4,$$

i to je tzv. **Lorentzov kompleksni prostor** , poznat iz fizike.

Ako je za pseudounitarni prostor $s = n$, njegov osnovni funkcional je strogo pozitivan te je prostor unitaran. Ako je $s = -n$, osnovni funkcional je strogo negativan, ali je s

$$(x, y) = -\psi(x, y)$$

na prostoru definirana unitarna struktura. Zato je ovdje od interesa jedino slučaj kad za signaturu vrijedi

$$-n < s < n\ .$$

Uz taj uvjet će pseudoskalarni produkt poprimati i pozitivne i negativne vrijednosti pa govorimo, da na prostoru imamo **indefinitnu metriku.**

Pribilježimo ovaj rezultat

PROPOZICIJA 2

Neka je U pseudounitarni prostor s osnovnim funkcionalom ψ. Onda postoje potprostori $L, M < U$ takvi da je $L \oplus M = U$ i da je restrikcija $\psi/_{L\times L}$ strogo pozitivni, a restrikcija $\psi/_{M\times M}$ strogo negativni funkcional.

Dokaz

Neka je $E = (e_1, \ldots, e_p, e_{p+1}, \ldots, e_n)$ normalna baza za U. Definirajmo

$$L = [\{e_1, \ldots, e_p\}] \quad , \quad M = [\{e_{p+1}, \ldots, e_n\}] \ .$$

Onda je $L \oplus M = U$ i potprostori L i M očito imaju traženo svojstvo. ■

Prema tome, L je unitarni potprostor od U. Njegova konstrukcija ovisi, dakako, o odabranoj bazi, ali mu je dimenzija jednoznačno određena pseudounitarnom strukturom na U (vidi i Zad. 3.).

Primijetimo još da u pseudounitarnom prostoru $(x, x) = 0$ ne povlači da je nužno $x = \Theta$. Ako su npr. e_1 i e_n vektori iz normalne baze prostora sa signaturom $s \neq n, -n$, a $x = e_1 + e_n$, bit će

$$(x, x) = 0\ ,$$

iako je $x \neq \Theta$.

U definiciji pseudounitarnog prostora zahtijevali smo da osnovni funkcional bude regularan. Izostavljajući taj zahtjev, dolazimo do daljnje generalizacije. Par (U, χ), gdje je χ bilo koji hermitski bilinearni funkcional, nazivamo **prostor s hermitskom (bilinearnom) metrikom**. I ovdje su za $(x, y) = \chi(x, y)$ ispunjeni aksiomi (1)–(3) pseudoskalarnog produkta.

Za prostore s hermitskom metrikom osim signature definiramo i **rang**, kao rang osnovnog funkcionala χ. Lako se vidi da dimenzija, rang i signatura takve prostore klasificiraju do na izomorfizam.

Prostor je **nedegeneriran** ako je maksimalnog ranga, dok je inače **degeneriran**. Nedegenerirani prostori s hermitskom metrikom su, dakako, pseudounitarni prostori. Od interesa su degenerirani prostori. Tu se mogu pojaviti neki novi fenomeni.

I u prostorima s hermitskom metrikom ima smisla govoriti o ortogonalnosti. Ako su vektori $a, b \in U$, kažemo da je a **ortogonalan** na b, ako je $(a, b) = 0$. Kako je zbog hermitske komutativnosti i $(b, a) = 0$, govorimo o **paru ortogonalnih vektora**. Ako je $S \subset U$ bilo koji podskup, a

$$S^{\perp} = \{x \in U \mid (x, a) = 0, \quad \forall a \in S\} ,$$

lako se vidi da je $S^{\perp}$ potprostor od U.

Za vektor $a \in U$, za koji vrijedi $\{a\}^{\perp} = U$, tj. koji je ortogonalan na sve vektore iz U, kažemo da je **izotropan** u U. Skup

$$I = \{a \in U \mid (a, x) = 0, \quad \forall x \in U\}$$

svih izotropnih vektora je zbog $I = U^{\perp}$ potprostor, koji zovemo **izotropni potprostor** od U. U unitarnim i pseudounitarnim prostorima je očito $I = \{\Theta\}$, ali u općem slučaju vrijedi

PROPOZICIJA 3

U prostoru U s hermitskom metrikom je

$$\dim I = \dim U - r ,$$

gdje je r rang prostora.

Dokaz

U točki 14.5. smo vidjeli da za U postoji baza $E = (e_1, \ldots, e_n)$, takva da u njoj pseudoskalarni produkt ima oblik

$$(x, y) = \alpha_1 \overline{\beta}_1 + \cdots + \alpha_p \overline{\beta}_p - \cdots - \alpha_r \overline{\beta}_r + 0 \cdot \alpha_{r+1} \overline{\beta}_{r+1} + \cdots + 0 \cdot \alpha_n \overline{\beta}_n ,$$

gdje su (α_i) koordinate vektora x, a (β_i) koordinate vektora y u toj bazi. Neka je

$$I = [\{e_{r+1}, \ldots, e_n\}] .$$

Onda je I potprostor od U, $\dim I = n - r$, i jasno je da je I izotropan. ■

Ako je $\dim I \neq 0$, prostor I je (teško) degeneriran jer je njegov rang jednak nuli. Dimenziju prostora I zovemo katkada **defekt prostora** U.

KOROLAR 4

Svaki se prostor U s hermitskom metrikom može prikazati kao

$$U = L \oplus I ,$$

gdje je L neki pseudounitarni, a I izotropni potprostor od U. ■

Lako se vidi da vrijedi i

PROPOZICIJA 5

Potprostor $L < U$ je pseudounitaran ako i samo ako vrijedi

$$L \oplus L^{\perp} = U .$$ ■

To je samo nekoliko nasumce odabranih činjenica iz teorije pseudounitarnih prostora i prostora s hermitskom metrikom. Teorija je vrlo bogata i zanimljiva, posebno u onom dijelu gdje se, po analogiji s unitarnim slučajem, na tim prostorima promatraju razni specijalni tipovi operatora (hermitski, antihermitski, izometrije itd.) i njihovi prikazi u prirodnim bazama.

ZADACI

1. Nađi primjere pseudounitarnih prostora.

2. Kao i obično, za skup $S = (a_1, \ldots, a_n)$ vektora iz pseudounitarnog prostora definiramo **Gramovu matricu**

$$G(S) = \begin{bmatrix} (a_1, a_1) & \cdots & (a_1, a_n) \\ \vdots & & \vdots \\ (a_n, a_1) & \cdots & (a_n, a_n) \end{bmatrix} .$$

Skup S je linearno nezavisan ako i samo ako je matrica $G(S)$ regularna. Uoči da se Gramova matrica za bazu prostora podudara s matricom osnovnog funkcionala prostora u toj bazi. Prema tome, Gramove matrice raznih bazâ istog prostora hermitski su kongruentne.

3. Dokaži: Za pseudounitarni prostor (U, ψ) postoji dekompozicija $U = L \oplus M$ sa svojstvom da je funkcional

$$\varphi : U \times U \to F ,$$

definiran za $x = a_1 + b_1$, $y = a_2 + b_2$, $a_i \in L$, $b_i \in M$ s

$$\varphi(x, y) = \psi(a_1, a_2) - \psi(b_1, b_2) ,$$

strogo pozitivan, i prema tome je (U, φ) unitarni prostor.

4. Osim pseudounitarnih prostora i prostora s hermitskom metrikom, u daljnjoj se generalizaciji promatraju i prostori (U, φ), gdje se za osnovni funkcional zahtijeva samo bilinearnost. Dokaži da su takvi prostori izomorfni onda i samo onda ako su Gramove matrice za po volji odabrane baze prostora međusobno kongruentne. Ako je osnovni funkcional kompleksni bilinearni funkcional, ta je kongruencija hermitska.

5. I u prostoru s bilo kojim bilinearnim funkcionalom ima smisla govoriti o ortogonalnosti vektora, s time da to svojstvo više nije simetrično. Zato u slučaju $(a, b) = 0$ kažemo da je a **lijevo ortogonalan** na b, odnosno da je b **desno ortogonalan** na a. Za skup $S \subset V$ definiramo

$$S^{\perp} = \{x \in U \mid (a, x) = 0, \quad \forall a \in S\} .$$

Analogno se definira i ${}^{\perp}S$. Pokaži da su $S^{\perp}$ i ${}^{\perp}S$ potprostori od U. Ako je $L < U$ nedegenerirani potprostor (tj. prostor maksimalnog ranga), onda je

$$U = L \oplus L^{\perp} = L \oplus {}^{\perp}L .$$

Obratno, ako vrijedi bar jedna od navedenih dekompozicija, potprostor L je nedegeneriran.

6. Nastavak: $U^{\perp}$, ${}^{\perp}U < U$ zovu se **desno**, odnosno **lijevo izotropni potprostori** od U. Pokaži da je

$$\dim U^{\perp} = \dim {}^{\perp}U = n - r ,$$

gdje je n dimenzija, a r rang prostora U. Prema tome prostor U je nedegeneriran ako i samo ako je $U^{\perp} = {}^{\perp}U = \{\Theta\}$.

7. Pokaži da za svaku dimenziju postoji do na izomorfizam samo jedan prostor (U, φ), gdje je U kompleksni prostor, a φ regularni simetrični

bilinearni funkcional (vidi točku 14.1.). Takav se prostor (prema standardnom modelu) zove **kompleksni euklidski prostor**. Uvjeri se da u njemu postoji baza u kojoj je pseudoskalarni produkt dan formulom

$$(x, y) = \alpha_1 \overline{\beta}_1 + \cdots + \alpha_n \overline{\beta}_n \,,$$

gdje je n dimenzija prostora.

8. Kompleksni (realni) **simplektički prostor** je par (U, φ), gdje je U kompleksni (realni) linearni prostor, a φ regularni antisimetrični bilinearni funkcional. Pokaži da postoji baza za U u kojoj osnovni funkcional φ ima matricu

$$S = \begin{bmatrix} 0 & 1 & & & & & O \\ -1 & 0 & & & & & \\ & & 0 & 1 & & & \\ & & -1 & 0 & & & \\ & & & & \ddots & & \\ & & & & & 0 & 1 \\ O & & & & & -1 & 0 \end{bmatrix} ,$$

tj. blok dijagonalnu matricu s blokovima

$$\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$$

na glavnoj dijagonali. Takvu bazu nazivamo **simplektička baza prostora**, i u njoj je pseudoskalarni produkt dan formulom

$$(x, y) = \alpha_1 \beta_2 - \alpha_2 \beta_1 + \cdots + \alpha_{2n-1} \beta_{2n} - \alpha_{2n} \beta_{2n-1}$$

(usporedi sa Zad. 6. i 12. u 14.3.). Prema tome, simplektički prostor je nužno parne dimenzije. Pokaži da za svaki $n \in \mathbb{N}$ postoji do na izomorfizam točno jedan simplektički prostor dimenzije $2n$.

9. Dokaži: Gramova matrica (Zad. 2.) bilo koje baze simplektičkog prostora je regularna, simetrična i kongruentna s matricom S iz Zad. 8.

10. Kompleksna matrica A parnog reda je **simplektička** ako je

$$A' S A = S \,,$$

gdje je S matrica iz Zad. 8. Pokaži da je determinanta simplektičke matrice jednaka 1. Nadalje, ako je λ korijen karakteristične jednadžbe te matrice, dokaži da je i $1/\lambda$ korijen te jednadžbe.

11. Pokaži da transformacija varijabli sa simplektičkom matricom ne mijenja antisimetričnu bilinearnu formu $\Phi(x, y) = X' S Y$, tj. ostavlja je invarijantnom.

12. Regularni operator $f : U \to U$ na simplektičkom prostoru koji čuva pseudoskalarni produkt naziva se **izometrija** ili **simplektički operator**. Pokaži: Linearni operator je simplektički ako i samo ako je u simplektičkoj bazi reprezentiran simplektičkom matricom.

13. U daljnjim zadacima neka U označava nedegenerirani prostor s bilo kojim bilinearnim funkcionalom (vidi Zad. 4.). Neka je $l : U \to F$ linearni funkcional. Dokaži da postoji i jednoznačno je određen vektor $a \in U$ tako da vrijedi

$$l(x) = (x, a) ,$$

za svaki $x \in U$.

14. Neka je $f : U \to U$ linearni operator. Onda definiramo (kao i u točki 13.4. za unitarne prostore) operatore ${}^*f$, $f^* : U \to U$ s

$$(x, f(y)) = ({}^*f(x), y) ,$$

odnosno

$$(f(x), y) = (x, f^*(y)) ,$$

za svaki $x, y \in U$. ${}^*f$ zovemo **lijevi**, a f^* **desni adjungirani operator** za f. Pokaži da takvi operatori postoje, da su linearni i jednoznačno određeni s f (koristi Zad. 13.). Pokaži, nadalje, da vrijedi

$$\begin{aligned} (f + g)^* &= f^* + g^* , \\ (f \circ g)^* &= g^* \circ f^* , \\ (\lambda f)^* &= \overline{\lambda}\, f^* . \end{aligned}$$

Konačno, pokaži da je u prostorima sa simetričnim, odnosno antisimetričnim funkcionalom uvijek ${}^*f = f^*$.

15. Neka je $f : U \to U$ linearni operator. Onda je s $\psi(x, y) = (f(x), y)$ definiran jedan bilinearni funkcional na U. Obratno, za svaki bilinearni funkcional $\psi : U \times U \to F$ postoji i jednoznačno je određen linearni operator $f : U \to U$ tako da vrijedi $(f(x), y) = \psi(x, y)$, za svaki $x, y \in U$. Osnovnom funkcionalu φ prostora pridružen je, dakako, jedinični operator. Dokaži!

16. Operator $f : U \to U$ je **simetričan** ako je

$$f = f^* = {}^*f \,,$$

a **antisimetričan** ako je

$$f = -f^* = -{}^*f \,.$$

Ako je U prostor sa simetričnim osnovnim funkcionalom, dokaži da je simetričnom (antisimetričnom) bilinearnom funkcionalu na U, u smislu Zad. 15., pridružen simetrični (antisimetrični) operator. Ako je pak U prostor s antisimetričnim funkcionalom, simetričnom (antisimetričnom) bilinearnom funkcionalu je pridružen antisimetrični (simetrični) operator.

17. Formuliraj i dokaži tvrdnje iz Zad. 13.–16. za slučaj kad je U prostor s kompleksnim osnovnim funkcionalom ili, specijalno, prostor s hermitskom metrikom. U tom slučaju simetrične (antisimetrične) operatore zovemo **hermitski** (**antihermitski**) **operator**.

18. Regularni operator $f : U \to U$ je **izometrički** ili **izometrija** ako čuva pseudoskalarni produkt. Pokaži da je f izometrija ako i samo ako vrijedi

$$f^* \circ f = {}^*f \circ f = e \,,$$

gdje je e jedinični operator.

19. Neka je $f : U \to U$ linearni operator, a $a, b \in U$ njegovi svojstveni vektori koji pripadaju različitim svojstvenim vrijednostima λ i μ. Dokaži: Ako je f izometrija i vrijedi $\lambda\mu \neq 1$, onda su vektori a i b ortogonalni. Nadalje, ako je f simetrični operator, a i b su ortogonalni. Konačno, ako je f antisimetrični operator i vrijedi $\lambda + \mu \neq 0$, tada je $(a, b) = 0$. Slično vrijedi u kompleksnom i hermitskom slučaju.

20. Neka je $f : U \to U$ izometrija, simetrični ili antisimetrični operator. Neka je $L < U$ f-invarijantni potprostor. Dokaži da su $L^\perp$ i ${}^\perp L$ također f-invarijantni potprostori.

21. Generaliziraj prethodne rezultate na par (U, φ), gdje je U linearni prostor nad **bilo kojim** poljem, a φ bilinearni funkcional.

14.7. Geometrija linearnog prostora

Linearni prostor ima svoju geometriju. Skicirat ćemo kako se dolazi do njezinih elemenata. Radi jednostavnosti pretpostavimo da je dani prostor

realan; uz male modifikacije ideje se lako prenose i na opći slučaj, kad se definira geometrija u linearnom prostoru nad bilo kojim poljem.

Neka je V realni linearni prostor dimenzije n. Neka je $f : V \to \mathbb{R}$ bilo koji linearni funkcional na tom prostoru, različit od nulfunkcionala, a $\beta \in \mathbb{R}$ dani skalar. Onda skup

$$H = \{x \in V \mid f(x) = \beta\} \tag{1}$$

nazivamo **hiperravnina** u prostoru V. Pišemo kratko

$$H \ \ldots \ f(x) = \beta \, . \tag{2}$$

Neka je $B = (a_1, ..., a_n) \subset V$ bilo koja baza, tzv. **koordinatni sustav** za V. Ako označimo $f(a_i) = \alpha_i$, za $i = 1, ..., n$, definicijski uvjet (2) možemo pisati kao

$$H \ \ldots \ \sum_{i=1}^{n} \alpha_i x_i = \beta \, , \tag{3}$$

gdje je (x_i) koordinatni slog vektora $x \in H$ u bazi B, i to je **jednadžba hiperravnine** H u danom koordinatnom sustavu.

Kažemo da su hiperravnine

$$H_1 \ \ldots \ f_1(x) = \beta_1 \qquad \text{i} \qquad H_2 \ \ldots \ f_2(x) = \beta_2$$

paralelne ako postoji $\lambda \in \mathbb{R}$ takav da vrijedi

$$f_2 = \lambda f_1 \, . \tag{4}$$

Ako su

$$\sum_{i=1}^{n} \alpha_{i1} x_i = \beta_1 \qquad \text{i} \qquad \sum_{i=1}^{n} \alpha_{i2} x_i = \beta_2$$

jednadžbe hiperravnina u istom koordinatnom sustavu, one će biti paralelne ako i samo ako su koeficijenti u jednadžbama proporcionalni,

$$\alpha_{11} : \alpha_{21} : \ \ldots \ : \alpha_{n1} = \alpha_{12} : \alpha_{22} : \ \ldots \ : \alpha_{n2} \ . \tag{5}$$

Neka je $r \leq n$ bilo koji prirodni broj i $k = n - r$. Neka je

$$H_1, H_2, ..., H_r \subset V$$

kolekcija hiperravnina iz V,

$$H_i \ \ldots \ f_i(x) = \beta_i \, , \quad i = 1, ..., r \ , \tag{6}$$

i neka je

$$H = \bigcap_{i=1}^{r} H_i \tag{7}$$

njihov presjek. Ako su hiperravnine dane svojim jednadžbama u istom koordinatnom sustavu, skup H možemo opisati sustavom jednadžbi

$$\left.\begin{array}{c} \alpha_{11}x_1 + \alpha_{21}x_2 + \cdots + \alpha_{n1}x_n = \beta_1 \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ \alpha_{1r}x_1 + \alpha_{2r}x_2 + \cdots + \alpha_{nr}x_n = \beta_r \end{array}\right\}, \tag{8}$$

tj. vektor $x = (x_i)$ će pripadati skupu (7) ako i samo ako su njegove koordinate u danom koordinatnom sustavu rješenje sustava (8).

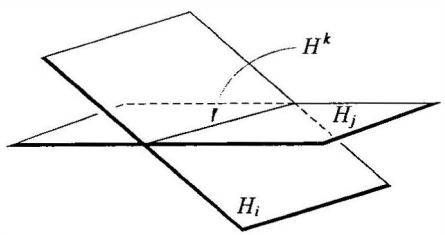
Neka je sada matrica $A = [\alpha_{ik}]$ sustava (8) maksimalnog ranga,

$$r(A) = r\,.$$

Onda je (zbog Kor. 2 u 11.3.) sustav (8) rješiv, i prema tome je

$$H \neq \emptyset\,.$$

U tom slučaju taj skup označavamo s $H = H^k$. Nazivamo ga k-**ravnina** u prostoru V, $k = n - r$, a za sustav (8) kažemo da je **analitičko predočenje** k-**ravnine** u danom koordinatnom sustavu. Posebno, za $k = 1$ imamo



pravac, za $k = 2$ **ravninu**, a u slučaju kad je $k = n - 1$ dobivamo hiperravninu u V. Diskutiraj i geometrijski interpretiraj slučajeve kad je $r(A) < r$.

Za $i = 1, \ldots, r$ označimo s J_i jezgru definicijskog funkcionala f_i iz (6). Neka je

$$J = \bigcap_{i=1}^{r} J_i\,.$$

Onda je $J \subset V$ potprostor i njegova je dimenzija (vidi 11.5.)

$$\dim J = n - r = k\,.$$

Ako je sada $a \in H^k$ bilo koji vektor, prema 11.6. bit će

$$H^k = a + J \,,$$

tj. k-ravnina nije ništa drugo nego linearna mnogostrukost u prostoru V, a njezina je dimenzija prema ranijoj definiciji (vidi točku 7.8.) jednaka

$$\dim H^k = k \,.$$

U prostoru V možemo definirati i nelinearne objekte, poopćenje ploha. Neka je $q : V \to \mathbb{R}$ bilo koji netrivijalni kvadratni funkcional, a $\beta \geq 0$ po volji odabran skalar. Onda skup

$$K = \{x \in V \mid q(x) = \beta\}$$

nazivamo (**centralna**) **hiperkvadrika** ili **hiperploha drugog reda** u prostoru V (vidi i Zad. 6.).

Jednostavnije pišemo

$$K \ \ldots \ q(x) = \beta \,.$$

U danoj bazi prostora imamo prikaz (vidi točku 14.2.)

$$K \ \ldots \sum_{i,j} \alpha_{ij} x_i x_j = \beta \,, \tag{9}$$

i to je **jednadžba hiperkvadrike** K u danom sustavu. Primijetimo da je po pretpostavci rang matrice $A = [\alpha_{ij}]$ različit od nule (funkcional q je netrivijalan!). Simetričnu matricu

$$B = \begin{bmatrix} \alpha_{11} & \cdots & \alpha_{1n} & 0 \\ \vdots & & \vdots & \\ \alpha_{n1} & \cdots & \alpha_{nn} & 0 \\ 0 & \cdots & 0 & \beta \end{bmatrix}$$

koeficijenata iz (9) zovemo **matrica hiperkvadrike** K u danom sustavu. Promjenom baze rang $R = r(B)$ te matrice se ne mijenja, kao ni rang $r = r(A)$ i signatura $s = s(A)$ matrice A (jednaki rangu, odnosno signaturi funkcionala q). Zato nam mogu poslužiti za klasifikaciju hiperkvadrika.

Uvijek je $r \leq n$, $R \leq n + 1$, i R je jednak r ili $r + 1$. Hiperkvadrika je **nedegenerirana** ako je njezina matrica maksimalnog ranga, $R = n + 1$ (tada, dakako, mora biti $r = n$), a inače je **degenerirana**. Degenerirana kvadrika je **hiperkonus** ako je $r = R = n$, a **hipercilindar** ako je $r = R < n$ ili $r + 1 = R \leq n$. Lako se vidi da nema druge mogućnosti. Finiju

klasifikaciju unutar pojedine od tih kategorija onda provodi signatura s, za koju, kako znamo, uvijek vrijedi

$$-r \leq s \leq r\,,$$

i iste je parnosti kao r.

Uvedeni nazivi imaju svoje geometrijsko opravdanje. Naime, pogodnim izborom baze jednadžba (9) može se znatno pojednostavniti, tako da u njoj lako prepoznajemo generalizaciju jednadžbe neke plohe drugog reda. Prema Prop. 1 u točki 14. 4., uvijek postoji koordinatni sustav u V, u kojemu matrica hiperkvadrike ima jedan od oblika

$$\begin{bmatrix} \varepsilon_1 & & O \\ & \ddots & \\ & & \varepsilon_n \\ O & & 1 \end{bmatrix} \quad \text{ili} \quad \begin{bmatrix} \varepsilon_1 & & O \\ & \ddots & \\ & & \varepsilon_n \\ O & & 0 \end{bmatrix},$$

gdje su ε_i jednaki 0, 1 ili -1. To je tzv. **normalna baza** i u njoj hiperkvadrika ima najjednostavniju, **normalnu jednadžbu**.

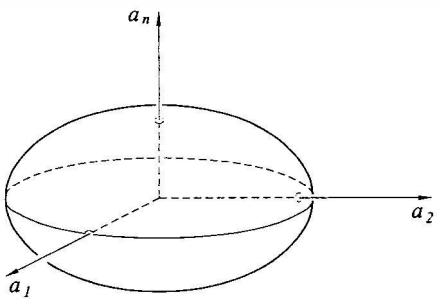
Normalna jednadžba nedegenerirane hiperkvadrike je oblika

$$\varepsilon_1 x_1^2 + \cdots + \varepsilon_n x_n^2 = 1\,,$$

gdje su svi $\varepsilon_i \neq 0$. Ako je pritom signatura $s = n$, imamo

$$x_1^2 + \cdots + x_n^2 = 1\,,$$

pa govorimo o **hiperelipsoidu**, a ako je $-n < s < n$, dobivamo razne



tipove **hiperhiperboloida**, ovisno o s. Ako je $s = -n$, skup K je prazan (**imaginarni hiperelipsoid**).

U normalnoj bazi hiperkonusi imaju jednadžbu

$$\varepsilon_1 x_1^2 + \cdots + \varepsilon_n x_n^2 = 0\,,$$

uz $\varepsilon_i \neq 0$, za sve $i = 1, \ldots, n$. Ako je $s \in \{n, -n\}$, konus degenerira u jedan jedini vektor, nulvektor. U protivnom, ovisno o s, dobivamo razne tipove **(hiperboličnih) konusa**. Konačno, u slučaju hipercilindara se jednadžba (9) može reducirati na

$$\varepsilon_1 x_1^2 + \cdots + \varepsilon_r x_r^2 = 0 \,,$$

ili

$$\varepsilon_1 x_1^2 + \cdots + \varepsilon_r x_r^2 = 1 \,,$$

gdje su svi $\varepsilon_i \neq 0$ i $r < n$. I opet, finiju klasifikaciju provodi signatura.

Idući korak je ispitivanje tangencijalnih objekata za hiperkvadrike. Neka je K nedegenerirana hiperkvadrika, dana s $q(x) = \beta$, a $\varphi(x, y)$ neka je polarni (bilinearni) funkcional od q (vidi točku 14.2.). Za bilo koji vektor $x_0 \in K$ definiramo **tangencijalnu hiperravninu** od K u x_0 kao skup

$$T = \{y \in V \mid \varphi(x_0, y) = \beta\} \,,$$

ili kraće

$$T \ \ldots \ \varphi(x_0, y) = \beta \,.$$

Kako je $y \mapsto f(y) = \varphi(x_0, y)$ linearni funkcional, T je svakako hiperravnina, kojoj zbog $\varphi(x_0, x_0) = q(x_0) = \beta$ vektor x_0 pripada. Nije teško vidjeti da je

$$T \cap K = \{x_0\} \,,$$

tj. T zaista ima očekivano svojstvo tangencijalnosti. U danoj bazi tangencijalna ravnina ima jednadžbu

$$T \ \ldots \ \sum_{i,j=1}^{n} \alpha_{ij} x_i^0 x_j = \beta \,,$$

gdje su (x_i^0) koordinate "**dirališta**" $x_0 \in K$ u toj bazi. Ako je baza normalna, jednadžba se reducira na

$$\varepsilon_1 x_1^0 x_1 + \cdots + \varepsilon_n x_n^0 x_n = \beta \,.$$

Ako je $T^k \subset V$ k-ravnina sa svojstvom da je $x_0 \in T^k$ i $T^k \subset T$, onda kažemo da je T^k **tangencijalna k-ravnina** u točki $x_0 \in K$.

Neka je H^{k+1} $(k+1)$-ravnina u V, a K hiperkvadrika. Onda skup

$$K^k = K \cap H^{k+1}$$

zovemo k-**kvadrika** u V. U bazi (npr. normalnoj za K) je k-kvadrika predočena sustavom jednadžbi

$$\left.\begin{array}{ccccccccc} \varepsilon_1 x_1^2 & + & \cdots & + & \varepsilon_n x_n^2 & = & \varepsilon \\ \alpha_{11} x_1 & + & \cdots & + & \alpha_{n1} x_n & = & \beta_1 \\ \cdots\cdots & \cdots & \cdots & \cdots & \cdots\cdots & \cdots & \cdots \\ \alpha_{1r} x_1 & + & \cdots & + & \alpha_{nr} x_n & = & \beta_r \end{array}\right\}, \tag{10}$$

gdje je ε jednak 1 ili 0, a $r = n - k - 1$ (ukupno je $n - k$ jednadžbi).

Dakako, ako je $H^{k+1} = L$ potprostor od V, k-kvadrike su hiperkvadrike u L, dane s $\overline{q}(x) = \beta$, gdje je $\overline{q} = q/_L$, a q je funkcional koji opisuje K.

Naveli smo ukratko neke elemente koji daju mogućnost razvijanja geometrije u prostoru V. Primijetimo da u toj geometriji nema metričkih odnosa, tj. ne postoje pojmovi kao duljina, udaljenost, kut, ortogonalnost. To je zato što obični linearni prostor nije opremljen metrikom. Za izgradnju metričke geometrije treba pretpostaviti da je prostor V unitaran.

ZADACI

1. Neka su H^k, $H^l \subset V$ ravnine u V, $H^k = a + L$, $H^l = b + M$. Kažemo da su te ravnine **paralelne**, i pišemo $H^k || H^l$, ako je $L < M$ ili $M < L$. Pokaži: Ako je $H^k || H^l$, onda je $H^k \cap H^l = \emptyset$ ili je $H^k \subset H^l$, odnosno $H^l \subset H^k$. Vrijedi li obrat te izreke? Je li "biti paralelan" za ravnine relacija ekvivalencije?

2. Dokaži: Ako pravac H^1 ne pripada hiperkvadriki, on s njom ima najviše dva zajednička vektora.

3. Potpuno klasificiraj krivulje 2. reda i plohe 2. reda.

4. Jednadžbe hiperploha 2. reda:

   (a) $x_1^2 - x_2^2 + 2x_1x_4 - 2x_2x_4 + 4x_3x_4 - 2x_1x_3 + 2x_2x_3 = 1$;

   (b) $x_1x_2 + x_2x_3 + x_3x_4 + x_4x_5 + x_5x_1 = 0$,

   svedi (npr. Lagrangeovim postupkom) na normalni oblik i nađi matricu prijelaza iz polazne baze u normalnu. O kojim se hiperkvadrikama radi?

5. Neka je s $q(x) = \beta$ zadana nedegenerirana hiperkvadrika K, a $\varphi(x, y)$ neka je polarni funkcional od q. Za svaki $x_0 \in V$ skup

$$P \ \ldots \ \varphi(x_0, y) = \beta$$

zovemo **polarna hiperravnina** od x_0 s obzirom na K, a vektor x_0 je njezin **pol**. Jasno je da je P zaista hiperravnina. Pokaži: Polarna hiperravnina je tangencijalna na K ako i samo ako je $x_0 \in K$. Što možeš reći o skupu polarnih hiperravnina kad x_0 prolazi k-ravninom H^k?

6. Hiperkvadrike u V možemo definirati i općenitije: Neka je $q : V \to \mathbb{R}$ netrivijalni kvadratni funkcional, $f : V \to \mathbb{R}$ linearni funkcional, a

$$k : V \to \mathbb{R}$$

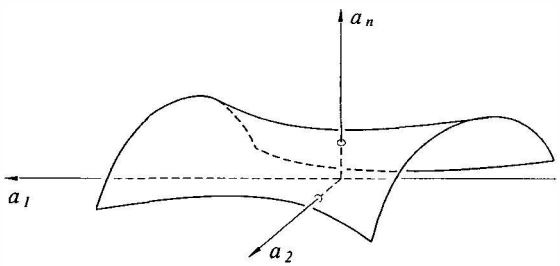
funkcional, definiran s

$$k(x) = q(x) + 2f(x)\,,$$

za svaki $x \in V$. Ako je $\beta \in \mathbb{R}$ bilo koji skalar, skup

$$K = \{x \in V \mid k(x) = \beta\}$$

nazivamo **hiperkvadrika** u V. Tom su definicijom obuhvaćene i "pomaknute" centralne hiperkvadrike, kao i **hiperparaboloidi**.



Nađi jednadžbu takve hiperkvadrike u danoj bazi. Nađi najjednostavnije (kanonske) jednadžbe hiperkvadrika i pokušaj ih klasificirati.

7. Neka je $\varphi : V \times V \times V \to \mathbb{R}$ trilinearni funkcional, a $t(x) = \varphi(x, x, x)$ kubni funkcional određen njime. Skup

$$T = \{x \in V \mid t(x) = \beta\}$$

nazivamo **hiperkubika** ili **hiperploha trećeg reda** u V. Nađi jednadžbu hiperkubike u danoj bazi. Kako te hiperplohe klasificirati? Definiraj analogno **hiperplohe n-tog reda**!

8. U geometriji smo navikli baratati skupovima izgrađenim od točaka, tj. preferiramo točkovnu strukturu prostora. To nas vodi na ovu definiciju: Neka je

$$A = \{P, Q, R, \ldots\}$$

neprazan skup, V linearni prostor nad poljem F, a

$$v : A \times A \to V$$

preslikavanje s ova dva svojstva:

(1) za svaki $P \in A$ i svaki $a \in V$ postoji i jednoznačno je određen $Q \in A$ tako da vrijedi

$$v(P, Q) = a\ ;$$

(2) za bilo koji izbor $P, Q, R \in A$ vrijedi

$$v(P, Q) + v(Q, R) = v(P, R).$$

Onda uređenu trojku (A, V, v) nazivamo **afini prostor**. Kažemo još, da je A **afini prostor nad poljem** F, **pridružen prostoru** V. Elemente od A zovemo **točke** afinog prostora. Po definiciji je **dimenzija** prostora A jednaka $\dim V$.

Pokaži da uz preslikavanje

$$v : V \times V \to V$$

dano s

$$v(a, b) = b - a,$$

svaki linearni prostor možemo shvatiti kao afini (s vektorima kao točkama!). Uvjeri se, nadalje, da preslikavanje

$$v : E^3 \times E^3 \to V^3$$

dano s

$$v(P, Q) = [\overrightarrow{PQ}] \in V^3$$

(vidi točku 5.3.) oprema naš intuitivni prostor E^3 afinom strukturom.

9. Neka je $O \in A$ točka afinog prostora. Za točku $P \in A$ vektor

$$v(O, P) \in V$$

zovemo **radijvektor** točke P. Pokaži da je na taj način uspostavljena korespondencija

$$A \mapsto V$$

bijektivna, i da A oprema strukturom linearnog prostora.

10. Za točke $P, Q \in A$ uređeni par (P, Q) nazivamo **orijentiranom dužinom**. Na skupu $A \times A$ svih orijentiranih dužina definiramo relaciju ekvivalencije $\equiv$, stavljajući $(P_1, Q_1) \equiv (P_2, Q_2)$ ako i samo ako je $v(P_1, Q_1) = v(P_2, Q_2)$. Pokaži da je preslikavanje

$$\Phi : A \times A/_{\equiv} \to V$$

dano s

$$\Phi([(P, Q)]) = v(P, Q)$$

bijektivno i da pomoću njega i $A \times A/_{\equiv}$ postaje linearni prostor. Tako vektor iz V možemo identificirati s klasom $[(P, Q)]$ orijentiranih dužina iz A (to je bila definicija vektora u V^3).

11. Dokaži: Aksiom (1) iz definicije afinog prostora može se oslabiti, tj. zamijeniti aksiomom:

(1') postoji točka $O \in A$, tako da za svaki $a \in V$ postoji jedinstvena točka $P \in A$ za koju je $v(O, P) = a$.

12. U afinom prostoru A je:

(a) $v(P, P) = \Theta$;

(b) $v(Q, P) = -v(P, Q)$,

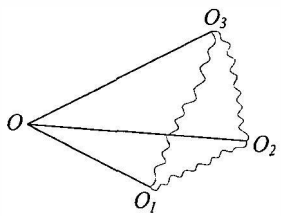
za sve $P, Q \in A$. Dokaži!

13. Podskup $A^k \subset A$ je **k-ravnina u A**, ako je za neku točku $O \in A^k$ skup

$$L = \{v(O, P) \mid P \in A^k\}$$

k-dimenzionalni potprostor od V. Pokaži da je A^k afini prostor dimenzije k. Pokaži, nadalje, da definicija ne ovisi o izboru točke O.

14. Neka su točka $O \in A$ i točke $O_1, O_2, ..., O_n \in A$ odabrane tako da je $(v(O, O_1), ..., v(O, O_n))$ baza za V. Onda izbor $\{O; O_1, ..., O_n\}$ nazivamo (**Kartezijev**) **koordinatni n-edar** u A. Točka O je njegovo **ishodište**, a O_i je **i-ta koordinatna točka**. Posredovanjem tog



n-edra dolazimo do pridruženja

$$P \mapsto v(O,P) = \sum_{i=1}^{n} x_i v(O,O_i) \mapsto (x_1,...,x_n) \ ,$$

i uređenu n-torku $(x_1,...,x_n)$ skalara iz F nazivamo **afine koordinate** točke P. Pokaži da je k-ravnina $A^k \subset A$ u tim koordinatama opisana jednadžbama

$$\sum_{j=1}^{n} \alpha_{ij} x_j = \beta_i \ ,$$

gdje je $i = 1,...,n-k$ i rang $r([\alpha_{ij}]) = n-k$.

15. Pokaži da **pravac** $A^1 \subset A$ određen svojim točkama $P_1 = (x_i^1)$ i $P_2 = (x_i^2)$ ima s obzirom na dani n-edar prikaz

$$\frac{x_1 - x_1^1}{x_1^2 - x_1^1} = \ \cdots \ = \frac{x_n - x_n^1}{x_n^2 - x_n^1} \ .$$

To su tzv. **kanonske jednadžbe** pravca A^1.

16. Afini prostor (E,U,v) nazivamo **euklidski**, ako je linearni prostor U unitaran. Koordinatni n-edar $\{O;O_1,...,O_n\}$ u takvom prostoru je **ortogonalan**, ako je $(v(O,O_1),...,v(O,O_n))$ ortonormirana baza za U. Nađi jednadžbe transformacije koordinata pri prijelazu iz jednog ortogonalnog n-edra u drugi.

17. **Udaljenost točaka** u euklidskom prostoru definirana je s

$$d(P,Q) = ||v(P,Q)|| \ .$$

Ako su točke dane svojim **ortogonalnim koordinatama** $P = (x_i)$, $Q = (y_i)$, njihova udaljenost je dana formulom

$$d(P,Q) = \sqrt{(y_1 - x_1)^2 + \cdots + (y_n - x_n)^2} \ .$$

Dokaži! Kako mjeriti kutove?

18. Definiraj i diskutiraj pojam i svojstva **ortogonalnosti** u euklidskom prostoru!

15

KATEGORIJE I FUNKTORI

Teorija kategorija je relativno mlada matematička disciplina (utemeljili su je 1945. godine S. Eilenberg i S. Mac Lane), koja je ubrzo našla korisne primjene u gotovo svim granama suvremene matematike. Slično kao u teoriji skupova, i tu se radi o pomalo apstraktnoj teoriji, čija je prednost u tome što njezini rezultati imaju prikladne interpretacije u vrlo raznorodnim matematičkim disciplinama, pojedinim konkretnim kategorijama. Nadalje, pomoću "preslikavanja" između kategorija, tzv. funktora, dovode se u vezu i uzajamno obogaćuju potpuno različite teorije. Klasični primjer takvog odnosa je topologija i algebra.

S dovoljno konkretnih primjera na raspolaganju te ideje, elemente teorije kategorija, neće biti teško razumjeti.

15.1. Definicija kategorije

U dosadašnjim smo se razmatranjima susretali sa skupovima opremljenim raznim strukturama (grupe, prstena, linearnog i unitarnog prostora, algebre, itd.) i zajedno s njima izučavali preslikavanja koja vode računa o tim strukturama. Takvom situacijom i primjerima motiviran je apstraktni pojam kategorije. Formalna definicija je sljedeća:

Kategorija $\mathcal{C}$ sastoji se od:

(1) klase $\mathrm{Ob}(\mathcal{C})$ **objekata** u $\mathcal{C}$,

(2) svakom uređenom paru (X, Y) objekata iz $\mathcal{C}$ pridruženog skupa

$$\mathrm{Mor}_{\mathcal{C}}(X, Y)$$

morfizama[*)] s **domenom** X i **kodomenom** Y,

(3) svakoj uređenoj trojci (X, Y, Z) objekata iz $\mathcal{C}$ pridruženog preslikavanja

$$\circ : \mathrm{Mor}_{\mathcal{C}}(X, Y) \times \mathrm{Mor}_{\mathcal{C}}(Y, Z) \to \mathrm{Mor}_{\mathcal{C}}(X, Z) ,$$

zvanog **komponiranje** morfizama, koje svakom paru (f, g) morfizama iz domene pridružuje morfizam

$$g \circ f$$

iz kodomene, odabranih tako da vrijedi:

(C1) disjunktnost:
$\mathrm{Mor}_{\mathcal{C}}(X, Y) \cap \mathrm{Mor}_{\mathcal{C}}(X', Y') = \emptyset$, osim u slučaju kad je $X' = X$ i $Y' = Y$;

(C2) asocijativnost:
za svaki $f \in \mathrm{Mor}_{\mathcal{C}}(X, Y)$, $g \in \mathrm{Mor}_{\mathcal{C}}(Y, Z)$ i $h \in \mathrm{Mor}_{\mathcal{C}}(Z, W)$ je

$$h \circ (g \circ f) = (h \circ g) \circ f ;$$

(C3) egzistencija identitete:
za svaki objekt Y iz $\mathcal{C}$ postoji morfizam $1_Y \in \mathrm{Mor}_{\mathcal{C}}(Y, Y)$, takav da $f \in \mathrm{Mor}_{\mathcal{C}}(X, Y)$ povlači da je

$$1_Y \circ f = f ,$$

a $g \in \mathrm{Mor}_{\mathcal{C}}(Y, Z)$ povlači da je

$$g \circ 1_Y = g .$$

Zahtjeve (C1)–(C3) nazivamo **aksiomi kategorije**. Ako je $f \in \mathrm{Mor}_{\mathcal{C}}(X, Y)$, obično pišemo

$$f : X \to Y \qquad \text{ili} \qquad X \xrightarrow{f} Y .$$

Ako je $f : X \to Y$ i $g : Y \to Z$, onda pridruženi morfizam

$$g \circ f : X \to Z$$

zovemo **kompozit** morfizama f i g.

Primijetimo da se u definiciji kategorije govori o klasi objekata. To je zato što promatranih objekata može biti "previše" da bi predstavljali skup

*) Skup morfizama pridružen paru objekata (X, Y) u kategoriji $\mathcal{C}$ često se označava i kao $\mathcal{C}(X, Y)$.

(npr. svi skupovi, sve grupe, itd. ne čine skup)*). Ako je u kategoriji $\mathcal{C}$ klasa $\mathrm{Ob}(\mathcal{C})$ skup, kažemo da je $\mathcal{C}$ **mala kategorija**.

Iz aksioma (C3) odmah slijedi

PROPOZICIJA 1

Za bilo koji objekt X iz $\mathcal{C}$ morfizam $1_X : X \to X$ je jedinstven.

Dokaz

Neka su $1_X, 1'_X \in \mathrm{Mor}(X, X)$ morfizmi koji zadovoljavaju (C3). Onda mora vrijediti

$$1_X \circ 1'_X = 1'_X \circ 1_X = 1'_X \qquad \text{i} \qquad 1'_X \circ 1_X = 1_X \circ 1'_X = 1_X \,,$$

odakle je $1'_X = 1_X$. ■

Morfizam 1_X nazivamo **jedinični morfizam, identički morfizam** ili **identiteta** na X.

Kažemo da je kategorija $\mathcal{C}$ **diskretna** ako su jedini morfizmi u toj kategoriji identitete. Takva kategorija je potpuno određena klasom $\mathrm{Ob}(\mathcal{C})$ svojih objekata. Prema tome, svaku klasu (specijalno i skup) možemo shvatiti kao diskretnu kategoriju.

Kategorija $\mathcal{C}$ je **trivijalna** ako ima samo jedan objekt. Trivijalna kategorija određena je skupom $\mathrm{Mor}(X, X)$ svojih morfizama. Uz kompoziciju kao binarnu operaciju taj je skup, dakako, monoid. Vrijedi i obratno: Svaki se monoid (specijalno i grupa) može shvatiti kao trivijalna kategorija (vidi Zad. 1.).

Da bismo pred očima imali primjere, navedimo nekoliko osnovnih kategorija:

1. Kategorija $\mathcal{S}$: Klasa $\mathrm{Ob}(\mathcal{S})$ objekata je klasa **svih** skupova, a za svaki izbor (X, Y) skupova je $\mathrm{Mor}(X, Y)$ skup **svih** preslikavanja $X \to Y$;

2. Kategorija $\mathcal{G}$: $\mathrm{Ob}(\mathcal{G})$ je klasa svih grupa, a $\mathrm{Mor}(G, H)$ je skup svih homomorfizama $G \to H$;

3. Kategorija $\mathcal{L}$: $\mathrm{Ob}(\mathcal{L})$ su svi linearni prostori nad zadanim poljem F, a skup morfizama $\mathrm{Mor}(U, V)$ je baš $\mathrm{Hom}(U, V)$, tj. čine ga svi linearni operatori $U \to V$;

*) Pojam **klase** strogo je fundiran u modificiranoj Gödel-Bernays-von Neumannovoj aksiomatici.

4. Kategorija $\mathcal{T}$: Za $\mathrm{Ob}(\mathcal{T})$ je uzeta klasa svih topoloških prostora (vidi Zad. 8. i pripadnu bilješku u 12.6.), a $\mathrm{Mor}(X, Y)$ je skup svih neprekidnih*) preslikavanja $X \to Y$;

5. Kategorija $\mathcal{O}$: Klasa $\mathrm{Ob}(\mathcal{O})$ je prazna, što znači da nema objekata, pa onda ni morfizama. Koji put prikladno je na raspolaganju imati i takvu kategoriju.

Nije teško provjeriti da se u svakom od navedenih slučajeva zaista radi o dobro definiranoj kategoriji. Redom, te kategorije kratko nazivamo **kategorija skupova, grupa, linearnih prostora,** odnosno **topološka kategorija** i **prazna kategorija**. Mnogo daljnjih primjera kategorija dat ćemo u sljedećoj točki.

Neka je $\mathcal{C}$ dana kategorija. Morfizam $f : X \to Y$ u toj kategoriji nazivamo **ekvivalencija** (također **izomorfizam**), ako postoji morfizam $g : Y \to X$ sa svojstvom da je

$$g \circ f = 1_X \quad \text{i} \quad f \circ g = 1_Y .$$

U tom slučaju kažemo da je g **inverzni morfizam** ili **inverz** morfizma f.

PROPOZICIJA 2

Ako je $f : X \to Y$ ekvivalencija, njezin je inverz određen jednoznačno.

Dokaz

Neka su $g, g' : Y \to X$ inverzi od f. Onda je

$$(g \circ f) \circ g' = 1_X \circ g' = g'$$

i

$$g \circ (f \circ g') = g \circ 1_Y = g ,$$

pa je zbog asocijativnosti $g' = g$. ∎

Jedinstveni inverz morfizma f označavamo s f^{-1}.

PROPOZICIJA 3

Identiteta je ekvivalencija. Inverz ekvivalencije je ekvivalencija. Kompozit ekvivalencija je ekvivalencija.

*) Grubo govoreći, preslikavanje je **neprekidno** ako bliske točke prevodi u bliske točke. Ta se "bliskost" u metričkim prostorima uočava pomoću dane metrike (uobičajenom $\varepsilon - \delta$ tehnikom), a u općim topološkim prostorima pomoću dane topološke strukture (tj. pripadanjem istom otvorenom skupu, vidi Zad. 8. u 12.6.).

Dokaz

Trivijalan. Odmah se provjeri da je za ekvivalencije $(f^{-1})^{-1} = f$ i da je $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$. ■

Kažemo da je objekt X **ekvivalentan** objektu Y u kategoriji $\mathcal{C}$, i pišemo $X \cong Y$, ako postoji bar jedna ekvivalencija $f : X \to Y$. Iz Prop. 3 odmah slijedi da se zaista radi o dobro definiranoj relaciji ekvivalencije na objektima kategorije $\mathcal{C}$, pomoću koje se provodi klasifikacija objekata. U svakoj je kategoriji klasifikacija objekata do na ekvivalenciju važan problem.

Na primjer, u kategoriji $\mathcal{S}$ ekvivalencije su bijektivna preslikavanja, a ekvivalentni su oni i samo oni skupovi koji su ekvipotentni, tj. imaju isti kardinalni broj. U kategoriji $\mathcal{G}$ ekvivalencije su izomorfizmi grupa, a u kategoriji $\mathcal{L}$ izomorfizmi linearnih prostora. Konačno, u kategoriji $\mathcal{T}$ ekvivalencije su **homeomorfizmi** (neprekidne bijekcije čiji su i inverzi neprekidni), pa su ekvivalentni oni i samo oni prostori koji su **homeomorfni**, tj. istog topološkog tipa.

Kažemo da je kategorija $\mathcal{C}'$ **potkategorija** od $\mathcal{C}$, i pišemo $\mathcal{C}' \prec \mathcal{C}$, ako su ispunjeni ovi uvjeti:

(1) svaki objekt od $\mathcal{C}'$ je objekt i u $\mathcal{C}$;

(2) za svaki par objekata (X', Y') iz $\mathcal{C}'$ je

$$\mathrm{Mor}_{\mathcal{C}'}(X', Y') \subset \mathrm{Mor}_{\mathcal{C}}(X', Y'),$$

tj. skup morfizama u kategoriji $\mathcal{C}'$ je podskup skupa morfizama za taj par objekata u kategoriji $\mathcal{C}$;

(3) zakon komponiranja u $\mathcal{C}'$ je naslijeđen iz kategorije $\mathcal{C}$, tj. ako su $f \in \mathrm{Mor}_{\mathcal{C}'}(X', Y')$ i $g \in \mathrm{Mor}_{\mathcal{C}'}(Y', Z')$ morfizmi u $\mathcal{C}'$, njihov se kompozit $g \circ f$ u $\mathcal{C}'$ podudara s kompozitom $g \circ f$ u kategoriji $\mathcal{C}$.

Kažemo da je $\mathcal{C}' \prec \mathcal{C}$ **puna potkategorija od** $\mathcal{C}$, ako umjesto (2) vrijedi stroži uvjet

(2') $$\mathrm{Mor}_{\mathcal{C}'}(X', Y') = \mathrm{Mor}_{\mathcal{C}}(X', Y'),$$

za svaki par (X', Y') objekata iz $\mathcal{C}'$, tj. za svaki par objekata iz $\mathcal{C}'$ skup morfizama je isti kao onaj za taj par u kategoriji $\mathcal{C}$.

Svaka kategorija $\mathcal{C}$ ima potkategoriju koja, uz iste objekte kao $\mathcal{C}$, za morfizme dopušta samo ekvivalencije iz kategorije $\mathcal{C}$. U kategoriji $\mathcal{S}$ potkategorije dobivamo ako za morfizme uzmemo samo injektivna ili samo surjektivna preslikavanja. Isto tako, potkategorije od $\mathcal{S}$ dobivamo ako za objekte dopustimo samo konačne ili samo prebrojive skupove. Te su potkategorije, dakako,

pune. Daljnji primjer je **kategorija $\mathcal{A}$ Abelovih grupa** s homomorfizmima kao morfizmima, koja je puna potkategorija od $\mathcal{G}$.

Lako se vidi da vrijedi ova

PROPOZICIJA 4

Neka je s $\mathcal{K}$ označen neki izbor objekata i morfizama iz kategorije $\mathcal{C}$. Onda je $\mathcal{K}$ je potkategorija od $\mathcal{C}$ ako i samo ako je ispunjeno:

(1) *Ako je $f : X \to Y$ morfizam iz $\mathcal{K}$, onda su X i Y objekti u $\mathcal{K}$;*

(2) *Ako su $f : X \to Y$ i $g : Y \to Z$ morfizmi iz $\mathcal{K}$, onda je i $g \circ f$ morfizam iz $\mathcal{K}$;*

(3) *Za svaki objekt X iz $\mathcal{K}$ je $1_X : X \to X$ morfizam iz $\mathcal{K}$.* ■

Neka su $\mathcal{C}_1$ i $\mathcal{C}_2$ bilo koje kategorije. Onda definiramo njihov **produkt**

$$\mathcal{C}_1 \times \mathcal{C}_2$$

kao kategoriju čiji su objekti uređeni parovi (X, Y), gdje je X objekt u $\mathcal{C}_1$, Y objekt u $\mathcal{C}_2$, a za svaki par objekata skup morfizama definiran je s

$$\mathrm{Mor}_{\mathcal{C}_1 \times \mathcal{C}_2}((X_1, Y_1), (X_2, Y_2)) = \mathrm{Mor}_{\mathcal{C}_1}(X_1, X_2) \times \mathrm{Mor}_{\mathcal{C}_2}(Y_1, Y_2) ,$$

tj. podudara se sa skupom uređenih parova (f, g), gdje je $f \in \mathrm{Mor}_{\mathcal{C}_1}(X_1, X_2)$ morfizam u $\mathcal{C}_1$, a $g \in \mathrm{Mor}_{\mathcal{C}_2}(Y_1, Y_2)$ morfizam u $\mathcal{C}_2$.

Odmah se vidi da se zaista radi o dobro definiranoj kategoriji. Posve analogno se definira i produkt bilo koje familije kategorija.

ZADACI

1. Uvjeri se da se svaki monoid M može shvatiti kao kategorija s jednim jedinim objektom, u kojoj su morfizmi elementi od M, a kompozit morfizama je definiran množenjem u M. Posebno, svaka grupa je kategorija u kojoj su svi morfizmi ekvivalencije.

2. Dokaži: Za svaki objekt X u kategoriji $\mathcal{C}$ je skup morfizama $\mathrm{Mor}_{\mathcal{C}}(X, X)$ monoid, a skup ekvivalencija $\mathrm{Aut}_{\mathcal{C}}(X, X)$ grupa s obzirom na operaciju komponiranja morfizama. Objekt X, zajedno s $\mathrm{Mor}_{\mathcal{C}}(X, X)$, odnosno $\mathrm{Aut}_{\mathcal{C}}(X, X)$, jesu potkategorije od $\mathcal{C}$, od kojih je prva potkategorija puna.

3. Svakoj kategoriji $\mathcal{C}$ možemo pridružiti **kategoriju** $\mathcal{M}_\mathcal{C}$ **morfizama** od $\mathcal{C}$. Objekti u $\mathcal{M}_\mathcal{C}$ su morfizmi iz $\mathcal{C}$, a morfizmi u $\mathcal{M}_\mathcal{C}$ su za par objekata $f : X \to Y$ i $f' : X' \to Y'$ definirani kao parovi morfizama $g : X \to X'$, $h : Y \to Y'$ iz $\mathcal{C}$ sa svojstvom da dijagram

$$\begin{array}{ccc} X & \xrightarrow{f} & Y \\ {\scriptstyle g}\downarrow & & \downarrow{\scriptstyle h} \\ X' & \xrightarrow{f'} & Y' \end{array}$$

komutira, tj. da je $h \circ f = f' \circ g$. Konačno, komponiranje morfizama definiramo prirodno, "nadovezivanjem" dijagrama. Dokaži da je $\mathcal{M}_\mathcal{C}$ zaista kategorija.

4. Neka je $f : X \to Y$ dani morfizam u $\mathcal{C}$. Morfizam $g : Y \to X$ je **lijevi inverz** od f (katkad zvan **retrakcija**), ako vrijedi $g \circ f = 1_X$. Morfizam $h : Y \to X$ je **desni inverz** od f (katkad zvan **prerez**), ako je $f \circ h = 1_Y$. Općenito, f može imati više lijevih (desnih) inverza. Dokaži: Ako f ima i lijevi i desni inverz, oni su nužno jednaki i prema tome je f ekvivalencija.

5. Morfizam $f : X \to Y$ je **mono** ako iz $g_1, g_2 : Z \to X$ i $f \circ g_1 = f \circ g_2$ slijedi da je $g_1 = g_2$, tj. ako se kompozit može skratiti slijeva. Slično, $f : X \to Y$ je **epi** ako iz $h_1, h_2 : Y \to Z$ i $h_1 \circ f = h_2 \circ f$ slijedi da je $h_1 = h_2$, tj. ako se kompozit može skratiti zdesna. U kategorijama $\mathcal{S}$ i $\mathcal{G}$ se mono podudaraju s injekcijama, odnosno injektivnim homomorfizmima (monomorfizmima). Slično, epi se u tim kategorijama podudaraju sa surjekcijama, odnosno surjektivnim homomorfizmima (epimorfizmima, što nije trivijalno). Pokaži da je kompozit dvaju epi opet epi, a kompozit dvaju mono opet mono. Nadalje, ako je kompozit $g \circ f$ mono, onda je f mono. Mora li g biti mono? U drugu ruku, ako je $g \circ f$ epi, onda je g epi. Je li nužno i f epi? Pokaži da je svaki morfizam s desnim inverzom nužno epi. Obrat općenito ne vrijedi (npr. istinit je u $\mathcal{S}$, a nije u $\mathcal{G}$). Slično, svaki morfizam s lijevim inverzom nužno je mono.

6. Morfizam koji je i mono i epi nazivamo **bimorfizam**. Svaka ekvivalencija je, dakako, bimorfizam, ali obrat općenito nije istinit. Dokaži da su u kategoriji grupa i kategoriji linearnih prostora ti pojmovi ekvivalentni. Pokaži primjerima da postoje kategorije u kojima bimorfizam nije nužno i ekvivalencija (takva je npr. kategorija $\mathcal{T}$, gdje promatraj neprekidna preslikavanja $\mathbb{Q} \to \mathbb{R}$).

7. Neka je $f : X \to X$ morfizam. Kažemo da je f **idempotentan**, ako vrijedi $f \circ f = f$. Kažemo da se f **cijepa**, ako postoje morfizmi $g : X \to Y$ i $h : Y \to X$ takvi da je $f = h \circ g$ i $g \circ h = 1_Y$. Pokaži da je svaki morfizam koji se cijepa idempotentan. Pokaži nadalje, da je u cijepanju $f = h \circ g$ morfizam g uvijek epi, a h mono. Uvjeri se da se u kategoriji $\mathcal{S}$ svi idempotentni morfizmi cijepaju.

8. Morfizam $f : X \to Y$ je **regularan** ako postoji $g : Y \to X$ takav da je $f \circ g \circ f = f$. Pokaži: Ako f ima bilo lijevi, bilo desni inverz, f je regularan. Uvjeri se, nadalje, da je u kategoriji $\mathcal{S}$ svaki morfizam regularan.

9. Kažemo da je P **inicijalni** (**početni**) objekt u kategoriji $\mathcal{C}$ ako je skup $\mathrm{Mor}_{\mathcal{C}}(P, X)$ jednočlan za svaki objekt X iz $\mathcal{C}$. Analogno, K je **terminalni** (**konačni**) objekt u $\mathcal{C}$ ako skup $\mathrm{Mor}_{\mathcal{C}}(X, K)$ ima točno jedan element za svaki objekt X iz $\mathcal{C}$. Konačno, O je **nulobjekt** u kategoriji $\mathcal{C}$ ako je istodobno inicijalni i terminalni objekt. U kategorijama $\mathcal{S}$ i $\mathcal{T}$ je prazan skup jedini inicijalni objekt, dok su jednočlani skupovi (prostori) terminalni objekti. U kategoriji $\mathcal{G}$ je trivijalna grupa i inicijalni i terminalni objekt, dakle nulobjekt. Isto vrijedi za trivijalni prostor u kategoriji $\mathcal{L}$. U kategoriji skupova i bijektivnih preslikavanja nema ni inicijalnih ni terminalnih objekata. Pokaži: Ako u kategoriji $\mathcal{C}$ ima inicijalnih objekata, svi su oni ekvivalentni. Isto vrijedi i za terminalne objekte te nulobjekte. Ako je O nulobjekt u kategoriji $\mathcal{C}$, za bilo koja dva objekta X i Y iz $\mathcal{C}$ postoji jedinstveni morfizam $n : X \to Y$, koji se **faktorizira kroz** O,

$$\begin{array}{ccc} & O & \\ \nearrow & & \searrow \\ X & \xrightarrow{n} & Y \end{array} ,$$

i koji se naziva **nulmorfizam**. Kompozit nulmorfizma s bilo kojim morfizmom je nulmorfizam.

10. Svakoj kategoriji $\mathcal{C}$ možemo pridružiti **dualnu** (**suprotnu**) **kategoriju** $\mathcal{C}^*$. Objekti u $\mathcal{C}^*$ su isti kao oni u $\mathcal{C}$, a morfizmi u $\mathcal{C}^*$ su u bijektivnoj korespondenciji s onima u $\mathcal{C}$, s time da je morfizmu $f : X \to Y$ u $\mathcal{C}$ pridružen morfizam $f^* : Y \to X$ u $\mathcal{C}^*$. Konačno, komponiranje u $\mathcal{C}^*$ je definirano s $f^* \circ g^* = (g \circ f)^*$. Pokaži da je $\mathcal{C}^*$ zaista kategorija i da je $(\mathcal{C}^*)^* = \mathcal{C}$. Pokaži nadalje: Za svaku identitetu u $\mathcal{C}^*$ je $1^* = 1$. Morfizam f^* je ekvivalencija ako i samo ako je f ekvivalencija, f^* je desni (lijevi) inverz od g^* ako i samo ako je f lijevi (desni) inverz od g. Isto tako, f^* je epi (mono), ako i samo ako je f mono (epi). Konačno,

X je inicijalni (terminalni) objekt u $\mathcal{C}^*$ ako i samo ako je X terminalni (inicijalni) objekt u $\mathcal{C}$. Generaliziraj pojam dualne kategorije na slučaj kad objekti u $\mathcal{C}$ i $\mathcal{C}^*$ nisu isti, ali su u bijektivnoj korespondenciji.

15.2. Primjeri kategorija

Sada ćemo navesti primjere kategorija detaljnije . To su prije svega standardne kategorije, utemeljene na strukturama s kojima smo se susretali u prethodnim poglavljima. Na kraju je dodano nekoliko egzotičnih primjera, koji pokazuju da morfizmi ne moraju biti preslikavanja.

1. Već opisana kategorija $\mathcal{S}$ skupova i preslikavanja sadrži obilje raznih potkategorija. Te se kategorije dobivaju promatranjem skupova s nekim dodatnim svojstvom, npr. samo prebrojivih skupova, konačnih skupova ili skupova istog kardinalnog broja. Slično, morfizme možemo restringirati na injektivna, surjektivna, odnosno bijektivna preslikavanja.

2. Ako je $A \subset X$, onda (X, A) nazivamo **par skupova**. **Preslikavanje parova** $f : (X, A) \to (Y, B)$ je svako preslikavanje $f : X \to Y$ za koje je $f(A) \subset B$. **Kategoriju parova** čine parovi skupova kao objekti i preslikavanja parova kao morfizmi, a ona se označava sa $\mathcal{S}^2$. Važnu (malu) potkategoriju od $\mathcal{S}^2$ čine svi parovi (X, A), gdje je X zadani skup.

3. **Punktirani skup** je par (X, x) koji se sastoji od nepraznog skupa X i istaknutog elementa $x \in X$, tzv. **bazne točke**. **Punktirana kategorija** se sastoji od punktiranih skupova i preslikavanja koja čuvaju baznu točku. To je, dakako, puna potkategorija kategorije parova (dakako, uz identifikaciju bazne točke x s jednočlanim skupom $\{x\}$). U punktiranoj kategoriji postoje nulobjekti (Zad. 9. u 15.1.). To su svi skupovi koji imaju samo jedan element.

4. Kako smo već rekli, grupe zajedno s homomorfizmima čine kategoriju $\mathcal{G}$. Slično, primjeri kategorija su grupoidi, polugrupe i monoidi zajedno s homomorfizmima tih struktura. Potkategorije u $\mathcal{G}$ dobivamo ako promatramo samo grupe konačnog reda, samo cikličke grupe itd. ili ako za morfizme uzmemo samo monomorfizme, epimorfizme, odnosno izomorfizme. I tu imamo kategoriju $\mathcal{G}^2$ parova grupa i homomorfizama parova.

5. Važnu potkategoriju od $\mathcal{G}$ čini **kategorija $\mathcal{A}$ Abelovih grupa** i homomorfizama.

6. Kategoriju čine prstenovi kao objekti, zajedno s homomorfizmima prstenova. Slično, imamo kategorije integralnih domena, tijela, odnosno polja.

7. Već smo spomenuli kategoriju $\mathcal{L} = \mathcal{L}_F$ linearnih prostora i linearnih operatora nad danim poljem F. Važna je potkategorija $\mathcal{L}_{FK}$ konačnodimenzionalnih prostora, pa onda i njezina potkategorija prostora zadane dimenzije. Isto tako, imamo kategoriju normiranih prostora, kategoriju F-modula itd.

8. Algebre nad danim poljem s homomorfizmima algebri također čine kategoriju. Posebno, kategoriju čine Liejeve algebre.

9. Kategoriju tvore unitarni prostori s linearnim, odnosno unitarnim operatorima kao morfizmima. Slično, kategoriju čine pseudounitarni prostori, s preslikavanjima koja čuvaju pseudoskalarni produkt.

10. Osim već spomenute kategorije $\mathcal{T}$ svih topoloških prostora i neprekidnih preslikavanja, imamo i druge zanimljive topološke kategorije. Do njih dolazimo tako što se ograničimo na neku specijalnu klasu prostora: konačne dimenzije, iste dimenzije, ili na klasu metričkih, odnosno normalnih, regularnih, Hausdorffovih prostora, ili pak kompaktnih, parakompaktnih prostora itd. Umjesto svih neprekidnih preslikavanja, možemo dopustiti samo injektivna ili surjektivna preslikavanja, ili samo smještenja, odnosno homeomorfizme. Važne su i **homotopske kategorije**, gdje su morfizmi homotopske klase preslikavanja (vidi Zad. 3.). Imamo i kategoriju $\mathcal{T}^2$ parova topoloških prostora, kao i kategoriju punktiranih prostora.

11. Izuzetno važna potkategorija topološke kategorije je kategorija $\mathcal{M}$, u kojoj su objekti metrički prostori (vidi točku 12.6.), a morfizmi neprekidna preslikavanja među njima. To je tzv. **metrička kategorija**. Istaknutu ulogu u matematici igra i **puna** trivijalna potkategorija od $\mathcal{M}$, u kojoj je jedini objekt prostor $\mathbb{R}$ realnih brojeva. To je tzv. **realna analiza**.

12. I sustave linearnih jednadžbi možemo organizirati u kategoriju. Objekti u njoj su rješivi sustavi, a za dva takva sustava S i S' će postojati morfizam $S \to S'$ ako i samo ako je svako rješenje sustava S ujedno rješenje sustava S'. Tu morfizmi, dakako, nisu preslikavanja. Naravno, u toj su kategoriji dva sustava ekvivalentna ako i samo ako su ekvivalentni i u standardnom smislu (vidi točku 11.7.).

13. Matrice nad istim poljem F možemo interpretirati kao kategoriju $\mathcal{M}_F$ na ovaj način: Objekti u $\mathcal{M}_F$ su elementi skupa $\mathbb{N}$ prirodnih brojeva, a za dani izbor $m, n \in \mathbb{N}$ skup morfizama $\mathrm{Mor}(n, m)$ čine sve matrice tipa (m, n) s elementima iz polja F, $\mathrm{Mor}(n, m) = M_{mn}$. Iako se ne radi o preslikavanju, pišemo $A : n \to m$. Odmah se vidi da uz množenje matrica kao komponiranje zaista dobivamo kategoriju (jedinični morfizmi su tu, dakako, jedinične matrice, $1_n = E_n$).

14. Neka je $(X, \leq)$ parcijalno uređen skup. Njega uvijek možemo shvatiti kao kategoriju u kojoj su objekti elementi od X, a za svaki uređeni par (a, b) elemenata iz X se $\mathrm{Mor}(a, b)$ sastoji od jednog jedinog elementa ili je prazan, već prema tome je li $a \leq b$ ili $a \not\leq b$. Iz refleksivnosti i tranzitivnosti relacije uređaja slijedi da se zaista radi o kategoriji, a iz antisimetrije zaključujemo da su objekti u toj kategoriji ekvivalentni samo u slučaju kad su jednaki. Specijalno, svaki je totalno uređen skup kategorija.

15. Za svaki cijeli broj $n \geq 0$ definiramo skup

$$\Delta^n = \{0, 1, 2, \ldots, n\} .$$

Onda formiramo kategoriju u kojoj su objekti $\Delta^0, \Delta^1, \ldots$, a morfizmi $f : \Delta^m \to \Delta^n$ su funkcije koje čuvaju uređaj, tj. takve da $i < j$ povlači $f(i) \leq f(j)$, za $i, j \in \Delta^m$. Ta se kategorija zove **monotona** ili također (zbog nekih primjena) **simplicijalna kategorija**.

Kako vidimo, uz prikladne definicije morfizama se mnogo toga u matematici može interpretirati kao kategorija.

ZADACI

1. Specijalni slučaj malih kategorija su **konačne kategorije**, tj. kategorije koje se sastoje od konačnog broja objekata i morfizama. Osim nulkategorije, takva je kategorija s jednim objektom i jednim morfizmom, identitetom, zatim kategorije s dva objekta, koje osim dvije identitete imaju samo jedan morfizam, npr. $X \to Y$, ili dva morfizma $X \to Y$ i $Y \to X$, odnosno $X \leftrightarrows Y$. Kategorija s tri objekta i morfizmima različitim od identitete, kao na dijagramu

$$\begin{array}{ccc} & X & \\ & \swarrow \quad \searrow & \\ Y & \longrightarrow & Z \end{array} ,$$

dopušta samo jednu definiciju kompozicije. Dokaži i generaliziraj!

2. Neka su $f, g : G \to H$ homomorfizmi grupa. Kažemo da je f **konjugiran s** g, ako postoji unutrašnji automorfizam (Zad. 1. u 3.2.) a grupe H tako da vrijedi $g = a \circ f$. Pokaži da je konjugiranost relacija ekvivalencije. Dokaži da grupe kao objekti i klase konjugiranih homomorfizama kao morfizmi čine kategoriju.

3. Neka su $f, g : X \to Y$ (neprekidna) preslikavanja topoloških prostora. Kažemo da je f **homotopno s** g, i pišemo $f \simeq g$, ako postoji familija preslikavanja $f_t : X \to Y$, neprekidna u parametru $t \in [0, 1]$, tako da je $f_0 = f$, a $f_1 = g$. Uvjeri se da je $\simeq$ relacija ekvivalencije. Topološki prostori s klasama homotopnih preslikavanja kao morfizmima čine kategoriju. To je tzv. **homotopska kategorija** topoloških prostora. Za ekvivalentne objekte u toj kategoriji kažemo da su **istog homotopskog tipa**.

4. Neka je X dani topološki prostor. Onda definiramo kategoriju u kojoj su objekti otvoreni skupovi u X, a za par (U, V) takvih skupova je

$$\mathrm{Mor}(U,V) = \begin{cases} \{U,V\} & \text{, ako je } U \subset V \\ \emptyset & \text{, ako } U \not\subset V \end{cases} .$$

Uvjeri se da se, uz očiglednu operaciju komponiranja, zaista radi o (maloj) kategoriji.

15.3. Funktori

Funktori su preslikavanja između kategorija. Preciznije:

Neka su $\mathcal{C}$ i $\mathcal{D}$ bilo koje kategorije. **Funktor** F s domenom $\mathcal{C}$ i kodomenom $\mathcal{D}$, u oznaci

$$F : \mathcal{C} \to \mathcal{D} ,$$

jest uređeni par koji se sastoji od:

(1) **funkcije na objektima**, koja svakom objektu X iz $\mathcal{C}$ pridružuje jednoznačno određen objekt $F(X)$ iz $\mathcal{D}$, i

(2) **funkcije na morfizmima**, koja

(a) svakom morfizmu $f : X \to Y$ u kategoriji $\mathcal{C}$ pridružuje jednoznačno određen morfizam

$$F(f) : F(X) \to F(Y)$$

u kategoriji $\mathcal{D}$, i to tako da vrijedi

$$F(1_X) = 1_{F(X)} , \qquad F(g \circ f) = F(g) \circ F(f) ,$$

za svaki objekt X i kad god je kompozicija $g \circ f$ definirana,

ili

(b) svakom morfizmu $f : X \to Y$ iz $\mathcal{C}$ pridružuje jednoznačno određen morfizam

$$F(f) : F(Y) \to F(X)$$

u kategoriji $\mathcal{D}$, i to tako da vrijedi

$$F(1_X) = 1_{F(X)}, \quad F(g \circ f) = F(f) \circ F(g) ,$$

za svaki objekt X i kad god je kompozicija $g \circ f$ definirana.

Ako je ispunjeno (a), kažemo da je funktor F **kovarijantan**, a ako je ispunjeno (b), funktor je **kontravarijantan**.

Primijetimo da smo u definiciji uvjetno upotrijebili naziv funkcija za pridruživanja na razini klasa. Uočimo također da je (zbog zahtjeva $F(1_X) = 1_{F(X)}$) funktor zapravo zadan svojim djelovanjem na morfizmima.

Navedimo nekoliko primjera funktora:

1. Neka je $\mathcal{C}_0 \prec \mathcal{C}$ potkategorija od $\mathcal{C}$. Onda je **inkluzija** $I : \mathcal{C}_0 \to \mathcal{C}$, dana sa $I(X) = X$, za svaki objekt X u $\mathcal{C}_0$, i s $I(f) = f$ za svaki morfizam u $\mathcal{C}_0$, kovarijantni funktor. Posebno, **identični funktor** ili **identiteta** $I : \mathcal{C} \to \mathcal{C}$ je kovarijantni funktor.

2. **Projekcija** $P_1 : \mathcal{C}_1 \times \mathcal{C}_2 \to \mathcal{C}_1$ produkta kategorija na faktor, dana s $P_1(X, Y) = X$ i $P_1(f, g) = f$, jest kovarijantni funktor. Isto tako, projekcija $P_2 : \mathcal{C}_1 \times \mathcal{C}_2 \to \mathcal{C}_2$ je kovarijantni funktor.

3. Neka je $\mathcal{C}$ bilo koja kategorija, a A fiksni objekt iz $\mathcal{C}$. Onda definiramo kovarijantni funktor $F : \mathcal{C} \to \mathcal{S}$, u kategoriju skupova, pridružujući svakom objektu X iz $\mathcal{C}$ skup $F(X) = \mathrm{Mor}\,(A, X)$, a svakom morfizmu $f : X \to Y$ u $\mathcal{C}$ morfizam

$$F(f) : \mathrm{Mor}(A, X) \to \mathrm{Mor}(A, Y) ,$$

dan s $[F(f)](g) = f \circ g$, gdje je $g : A \to X$ bilo koji morfizam. Analogno, ako je B dani objekt iz $\mathcal{C}$, definiramo kontravarijantni funktor $G : \mathcal{C} \to \mathcal{S}$ s $G(X) = \mathrm{Mor}(X, B)$, za svaki objekt X iz $\mathcal{C}$, i s

$$G(f) : \mathrm{Mor}(Y, B) \to \mathrm{Mor}(X, B) ,$$

dan s $[G(f)](g) = g \circ f$, za svaki morfizam $f : X \to Y$ u $\mathcal{C}$, gdje je $g : Y \to B$ bilo koji morfizam. Lako se provjeri da su F i G zaista dobro definirani funktori.

4. Klasičan primjer kovarijantnog funktora je **funktor koji zaboravlja** (**funktor zaborava, zaboravljivi funktor**). Radi se o funktoru koji je identiteta na objektima i na morfizmima, ali "zaboravlja" nešto od njihove strukture, shvaćajući ih na različite načine. Takav je npr. funktor $\mathcal{G} \to \mathcal{S}$ koji svakoj grupi pridružuje tu istu grupu, shvaćenu kao skup (zaboravlja strukturu grupe), a homomorfizmu između grupa pridružuje taj isti homomorfizam, sada shvaćen kao preslikavanje među skupovima. Drugi je primjer funktor $\mathcal{L} \to \mathcal{A}$, koji svakom linearnom prostoru pridružuje taj isti prostor, shvaćen kao Abelova grupa (zaboravlja strukturu induciranu hibridnim množenjem), a svakom linearnom operatoru taj isti operator, shvaćen kao homomorfizam grupa. Konačno, takav je funktor $\mathcal{T} \to \mathcal{S}$, koji zaboravlja topološku strukturu.

5. Neka je, kao i obično, $\mathcal{P}(X) = \{A \mid A \subset X\}$ oznaka za partitivni skup skupa X. Kovarijantni funktor $P : \mathcal{S} \to \mathcal{S}$ definiramo stavljajući $P(X) = \mathcal{P}(X)$, za svaki skup X, a svakom preslikavanju $f : X \to Y$ pridružimo

$$P(f) : \mathcal{P}(X) \to \mathcal{P}(Y) ,$$

dano s $[P(f)](A) = f(A) \subset Y$, za svaki $A \subset X$. Analogno, možemo definirati kontravarijantni funktor $Q : \mathcal{S} \to \mathcal{S}$ sa $Q(X) = \mathcal{P}(X)$ i s

$$Q(f) : \mathcal{P}(Y) \to \mathcal{P}(X) ,$$

dano s $[Q(f)](B) = f^{-1}(B) \subset X$, za svaki $B \subset Y$.

6. Neka je s $\mathcal{P}$ označena kategorija polja i homomorfizama polja i neka je n dani prirodni broj. Onda možemo definirati funktor

$$GL_n : \mathcal{P} \to \mathcal{G} ,$$

koji svakom polju F pridružuje opću linearnu grupu $GL(n, F)$ nad tim poljem (vidi točku 9.5.), a svakom homomorfizmu $f : E \to F$ polja homomorfizam grupa

$$GL(n, E) \to GL(n, F) ,$$

koji svakoj matrici $A = [\alpha_{ik}] \in GL(n, E)$ pridružuje matricu $B = [f(\alpha_{ik})] \in GL(n, F)$. Nije teško vidjeti da je GL_n kovarijantni funktor, za svaki n.

7. Neka je s $\mathcal{A}^2$ označena kategorija parova Abelovih grupa. Ako svakom paru (G, A) grupa iz $\mathcal{A}^2$ pridružimo kvocijentnu grupu G/A, a svakom

homomorfizmu parova $h : (G, A) \to (H, B)$ inducirani homomorfizam (vidi točku 3.8.)

$$h^* : G/A \to H/B ,$$

dolazimo do kovarijantnog funktora

$$K : \mathcal{A}^2 \to \mathcal{A} .$$

8. Svakoj grupi G pridružimo njezinu komutatorsku podgrupu $[K] < G$ (vidi Zad. 8. u 2.7.). Kako svaki homomorfizam $G \to H$ prevodi komutatorsku podgrupu u komutatorsku podgrupu, na očigledan način dobivamo kovarijantni funktor

$$\mathcal{G} \to \mathcal{G} .$$

Nadalje, jer je $G/[K]$ uvijek Abelova grupa (Zad. 14. u 3.7.), konstrukcijom analognom onoj u Zad. 7., dolazimo do funktora

$$\mathcal{G} \to \mathcal{A} .$$

9. Na kategoriji linearnih prostora definiramo kontravarijantni funktor $D : \mathcal{L} \to \mathcal{L}$, koji linearnom prostoru V pridružuje njegov dual V^*, a linearnom operatoru $f : U \to V$ dualni operator

$$\widehat{f} : V^* \to U^* ,$$

(vidi Zad. 13. u 8.7.).

10. Ako je M dani linearni prostor, imamo funktor $F : \mathcal{L} \to \mathcal{L}$, definiran s $F(V) = V \times M$ na objektima, i s $F(f) = f \times 1_M$ na morfizmima.

11. I opet, ako je M fiksni linearni prostor, do kovarijantnog funktora $\mathcal{L} \to \mathcal{L}$ dolazimo pridružujući svakom vektorskom prostoru V prostor $\mathrm{Hom}(M, V)$, odnosno do kontravarijantnog funktora $\mathcal{L} \to \mathcal{L}$ pridružujući prostoru V prostor $\mathrm{Hom}(V, M)$. Na morfizmima ti su funktori definirani prirodno, kao u Prim. 3.

Važno je svojstvo funktora da prevodi ekvivalenciju u ekvivalenciju. Vrijedi

PROPOZICIJA 1

Neka je $F : \mathcal{C} \to \mathcal{D}$ bilo koji funktor, a f ekvivalencija u kategoriji $\mathcal{C}$. Onda je $F(f)$ ekvivalencija u kategoriji $\mathcal{D}$.

Dokaz

Neka je npr. F kovarijantni funktor. Ako je $f : X \to Y$ ekvivalencija, a $f^{-1} : Y \to X$ njezin inverz, onda je $f^{-1} \circ f = 1_X$ i $f \circ f^{-1} = 1_Y$, pa iz definicije funktora slijedi

$$1_{F(X)} = F(1_X) = F(f^{-1} \circ f) = F(f^{-1}) \circ F(f)$$

i

$$1_{F(Y)} = F(1_Y) = F(f \circ f^{-1}) = F(f) \circ F(f^{-1}) ,$$

što pokazuje da $F(f) : F(X) \to F(Y)$ ima inverz $[F(f)]^{-1} = F(f^{-1})$, tj. $F(f)$ je ekvivalencija. Dokaz je analogan, i u slučaju kad je F kontravarijantni funktor. ■

Prema tome, funktor $F : \mathcal{C} \to \mathcal{D}$ ekvivalentnim objektima u kategoriji $\mathcal{C}$ pridružuje ekvivalentne objekte u kategoriji $\mathcal{D}$. Obrat, dakako, općenito ne vrijedi. Ta je činjenica posebno korisna kad želimo dokazati da dva objekta iz kategorije $\mathcal{C}$ **nisu** ekvivalentna. Kako bismo npr. utvrdili da topološki prostori X i Y nisu homeomorfni, dovoljno je konstruirati funktor $\mathcal{T} \to \mathcal{G}$ (a takvih ima!) i ustanoviti da pridružene grupe nisu izomorfne, što je obično znatno jednostavnije.

Kažemo da je funktor $F : \mathcal{C} \to \mathcal{D}$ **pun** ako za svaki par (X, Y) objekata iz $\mathcal{C}$ i svaki morfizam $g : F(X) \to F(Y)$ postoji morfizam $f : X \to Y$, tako da vrijedi $F(f) = g$. U drugu ruku, funktor $F : \mathcal{C} \to \mathcal{D}$ je **vjeran** (ili je **smještenje**), ako za bilo koji par morfizama $f : X \to Y$ i $g : X \to Y$ u $\mathcal{C}$ iz $F(f) = F(g)$ slijedi $f = g$. Na primjer, funktori koji zaboravljaju su vjerni. Inkluzija $I : \mathcal{C}_0 \to \mathcal{C}$ je vjeran funktor, a bit će i pun ako i samo ako je $\mathcal{C}_0 \prec \mathcal{C}$ puna potkategorija.

Ako su $F : \mathcal{C} \to \mathcal{D}$ i $G : \mathcal{D} \to \mathcal{E}$ funktori, definiramo njihov **kompozit**

$$G \circ F : \mathcal{C} \to \mathcal{E}$$

s

$$\begin{aligned} (G \circ F)(X) &= G[F(X)], && \text{za svaki objekt } X \text{ iz } \mathcal{C}, \text{ i} \\ (G \circ F)(f) &= G[F(f)], && \text{za svaki morfizam } f \text{ iz } \mathcal{C}. \end{aligned}$$

Odmah se vidi da vrijedi

PROPOZICIJA 2

Kompozit $G \circ F$ dvaju funktora F i G je funktor. Taj je funktor kovarijantan, ako su F i G iste varijantnosti (tj. oba kovarijantna ili oba kontravarijantna), odnosno kontravarijantan ako su F i G suprotne varijantnosti.

■

Iz definicije je također jasno da je komponiranje funktora asocijativno.

Kažemo da je funktor $F : \mathcal{C} \to \mathcal{D}$ **izomorfizam kategorija**, ako postoji funktor $G : \mathcal{D} \to \mathcal{C}$ sa svojstvom

$$G \circ F = I_{\mathcal{C}} \quad \text{i} \quad F \circ G = I_{\mathcal{D}} \,,$$

gdje su $I_{\mathcal{C}}$, odnosno $I_{\mathcal{D}}$ identični funktori na kategorijama $\mathcal{C}$ i $\mathcal{D}$. Ako postoji, G je jedinstven, a nazivamo ga **inverzni funktor** od F i označavamo s $G = F^{-1}$. Izomorfizam kategorija je, dakako, i pun i vjeran funktor. Obrat, međutim, ne vrijedi (jer ne moramo imati bijektivnu korespondenciju na objektima).

Kažemo da je **kategorija $\mathcal{C}$ izomorfna s kategorijom $\mathcal{D}$**, i pišemo

$$\mathcal{C} \cong \mathcal{D} \,,$$

ako postoji bar jedan izomorfizam kategorija $F : \mathcal{C} \to \mathcal{D}$. Očito se radi o dobro definiranoj relaciji ekvivalencije. Na primjer, svaka je kategorija $\mathcal{C}$ izomorfna sa svojom dualnom kategorijom $\mathcal{C}^*$ (Zad. 8.).

ZADACI

1. Za dani skup S promatramo formalne (konačne!) linearne kombinacije.

$$\sum_i n_i a_i \quad , \quad a_i \in S \,,$$

s cjelobrojnim koeficijentima $n_i \in \mathbb{Z}$. Pokaži da je skup $F(S)$ svih takvih kombinacija, uz prirodno zbrajanje

$$\sum_i n_i a_i + \sum_i m_i a_i = \sum_i (n_i + m_i) a_i \,,$$

Abelova grupa (tzv. **slobodna Abelova grupa generirana skupom** S). Pokaži, nadalje, da bilo koje preslikavanje $f : S \to T$ ima jedinstveno proširenje do homomorfizma

$$F(f) : F(S) \to F(T)$$

pridruženih Abelovih grupa, i da pritom vrijedi

$$F(g \circ f) = F(g) \circ F(f) \,.$$

Na taj način dolazimo do kovarijantnog funktora

$$F : \mathcal{S} \to \mathcal{A}$$

iz kategorije skupova u kategoriju Abelovih grupa.

2. Interpretiraj pojam funktora između ovih specijalnih kategorija:

   (a) dvaju monoida ili dviju grupa (vidi Zad. 1. u 15.1.);

   (b) dvaju parcijalno uređenih skupova (vidi Prim. 14. u 15.2.).

3. Uvjeri se da ne postoji funktor $\mathcal{G} \to \mathcal{A}$ koji bi svaku grupu slao u njezin centar (vidi Zad. 4. u 2.7.).

4. Neka je $\mathcal{T}^2$ kategorija topoloških parova. Pokaži da postoji funktor $\mathcal{T}^2 \to \mathcal{T}$, koji svakom paru (X, A) pridružuje kvocijentni prostor X/A.

5. Neka je $(X, \mathcal{U})$ topološki prostor gdje je s $\mathcal{U}$ označena topološka struktura na X (vidi Zad. 8. u 12.6.). Uz uređenje po inkluziji, $\mathcal{U}$ je parcijalno uređen skup, dakle i kategorija (vidi Prim. 14. u 15.2.). Neka je $C(U)$ skup svih neprekidnih funkcija $f : U \to \mathbb{R}$, definiranih na $U \in \mathcal{U}$. Za bilo koji par (V, U), $U \subset V$, definiramo preslikavanje

   $$C(V) \to C(U) ,$$

   koje svakoj funkciji $f : V \to \mathbb{R}$ pridružuje restrikciju

   $$\overline{f} = f/U : U \to \mathbb{R}.$$

   Dokaži da je

   $$C : \mathcal{U} \to \mathcal{S}$$

   dobro definirani kontravarijantni funktor.

6. Kovarijantni funktor $F : \mathcal{C} \to \mathcal{D}$ možemo shvatiti kao korespondenciju

   $$F : Ob\,(\mathcal{C}) \to Ob\,(\mathcal{D})$$

   na klasama objekata i familiju preslikavanja

   $$F_{X,Y} : \mathrm{Mor}(X, Y) \to \mathrm{Mor}(F(X), F(Y)) ,$$

   definiranih za svaki par (X, Y) objekata iz $\mathcal{C}$, s time da su ispunjeni zahtjevi o identiteti i kompoziciji. Analogno interpretiramo i kontravarijantni funktor.

   Pokaži da je funktor F pun ako i samo ako je svako preslikavanje $F_{X,Y}$ surjektivno. Nadalje, F je vjeran ako i samo ako je svako preslikavanje $F_{X,Y}$ injektivno.

7. Pokaži da je kompozicija punih funktora puni funktor, a kompozicija vjernih funktora vjerni funktor. Pokaži nadalje: Ako je F vjerni funktor i f je mono, onda je i $F(f)$ mono.

8. Neka je $\mathcal{C}^*$ dualna kategorija od $\mathcal{C}$. Kontravarijantni funktor $D : \mathcal{C} \to \mathcal{C}^*$ definiramo tako da bude identiteta na objektima i da svakom morfizmu $f : X \to Y$ u $\mathcal{C}$ pridružuje morfizam $D(f) = f^*$ u $\mathcal{C}^*$ (vidi Zad. 10. u 15.1.). Pokaži da je D izomorfizam kategorija. Ako je $F : \mathcal{C} \to \mathcal{D}$ kontravarijantni funktor, onda je $F \circ D^{-1} : \mathcal{C}^* \to \mathcal{D}$ kovarijantni funktor, tj. kontravarijantni funktori se mogu interpretirati kao kovarijantni funktori na dualnoj kategoriji, i obratno.

9. Za svaki funktor $F : \mathcal{C} \to \mathcal{D}$ definiramo **dualni funktor** $F^* : \mathcal{C}^* \to \mathcal{D}^*$ s $F^* = D_2 \circ F \circ D_1^{-1}$ (vidi dijagram)

$$\begin{array}{ccc} \mathcal{C} & \xrightarrow{F} & \mathcal{D} \\ {\scriptstyle D_1}\downarrow & & \downarrow{\scriptstyle D_2} \\ X' & \xrightarrow{F^*} & \mathcal{D}^* \end{array} .$$

Pokaži da je F^* iste varijantnosti kao F i da se na objektima podudara s F.

10. Pokaži da male kategorije kao objekti i funktori između tih kategorija kao morfizmi formiraju kategoriju koju označavamo s $\mathcal{C}at$. Pokaži, nadalje, da je

$$\Phi : \mathcal{C}at \to \mathcal{C}at ,$$

dan s $\Phi(\mathcal{C}) = \mathcal{C}^*$ i $\Phi(F) = F^*$, dobro definirani kovarijantni funktor. Je li Φ izomorfizam?

11. Neka je $\mathcal{A}$ kategorija Abelovih grupa. Funktor $F : \mathcal{A} \to \mathcal{A}$ je **aditivan**, ako za svaki par morfizama $f, g : G \to H$ vrijedi

$$F(f + g) = F(f) + F(g).$$

Navedi primjere aditivnih funktora. Pokaži: Ako je F aditivan funktor, onda $f = n$ povlači $F(f) = n$, gdje je n nulhomomorfizam, i nadalje, $G = E$ povlači $F(G) = E$, gdje $E = \{0\}$ trivijalna grupa. Analogno se definiraju i ista svojstva imaju aditivni funktori $\mathcal{L} \to \mathcal{L}$ i $\mathcal{A} \to \mathcal{L}$.

12. Funktor $\mathcal{C} \times \mathcal{D} \to \mathcal{E}$ naziva se **funktor u dvije varijable** ili **bifunktor**. Pokaži da je $B : \mathcal{S} \times \mathcal{S} \to \mathcal{S}$, dan s $B(X, Y) = X \times Y$ i $B(f, g) = f \times g$, primjer bifunktora. Pokaži da je uz fiksiranu jednu varijablu bifunktor običan funktor u drugoj varijabli. Generaliziraj, promatrajući funktore u više varijabli, kovarijantne u nekima od njih, a kontravarijantne u ostalima. Na primjer, $\mathrm{Hom} : \mathcal{L} \times \mathcal{L} \to \mathcal{L}$ je funktor u dvije varijable, kontravarijantan u prvoj i kovarijantan u drugoj varijabli.

13. Neka su $F : \mathcal{C} \to \mathcal{C}'$ i $G : \mathcal{D} \to \mathcal{D}'$ funktori. Definiramo njihov produkt

$$F \times G \ : \ \mathcal{C} \times \mathcal{D} \to \mathcal{C}' \times \mathcal{D}'$$

s $(F \times G)(X, Y) = (F(X), G(Y))$ i s $(F \times G)(f, g) = (F(f), G(g))$. Pokaži da je $F \times G$ funktor. Pokaži, nadalje, da je

$$\times : \mathcal{C}at \times \mathcal{C}at \to \mathcal{C}at \, ,$$

gdje je $\times(\mathcal{C}, \mathcal{D}) = \mathcal{C} \times \mathcal{D}$, $\times(F, G) = F \times G$, također funktor.

14. Pokaži da je kategorija $(\mathcal{C} \times \mathcal{D})^*$ izomorfna s kategorijom $\mathcal{C}^* \times \mathcal{D}^*$.

15.4. Prirodne transformacije

Prirodne transformacije služe za uspoređivanje funktora s istom domenom i istom kodomenom.

Neka su $F, G : \mathcal{C} \to \mathcal{D}$ funktori iste varijantnosti. **Prirodna transformacija** φ funktora F u funktor G, u oznaci

$$\varphi : F \to G \, ,$$

je funkcija koja svakom objektu X iz $\mathcal{C}$ pridružuje jedinstveni morfizam

$$\varphi_X : F(X) \to G(X)$$

u kategoriji $\mathcal{D}$, i to tako da je ispunjen ovaj **uvjet prirodnosti**: Ako je $f : X \to Y$ bilo koji morfizam u $\mathcal{C}$, i vrijedi:

(1) F i G su kovarijantni, onda je dijagram

$$\begin{array}{ccc} F(X) & \xrightarrow{\varphi_X} & G(X) \\ {\scriptstyle F(f)}\downarrow & & \downarrow{\scriptstyle G(f)} \\ F(Y) & \xrightarrow{\varphi_Y} & G(Y) \end{array}$$

komutativan, tj. imamo

$$G(f) \circ \varphi_X = \varphi_Y \circ F(f) \, ;$$

ili

(2) F i G su kontravarijantni, onda je dijagram

$$\begin{array}{ccc} F(X) & \xrightarrow{\varphi_X} & G(X) \\ {\scriptstyle F(f)}\uparrow & & \uparrow{\scriptstyle G(f)} \\ F(Y) & \xrightarrow{\varphi_Y} & G(Y) \end{array}$$

komutativan, tj. imamo

$$G(f) \circ \varphi_Y = \varphi_X \circ F(f) \, .$$

Prirodna transformacija $\varphi : F \to G$ je, dakle, familija morfizama $\{\varphi_X\}$ iz $\mathcal{D}$, parametrizirana klasom objekata iz $\mathcal{C}$, odabrana tako da je ispunjen zahtjev prirodnosti. Članove te familije zovemo **komponentama** prirodne transformacije φ.

Evo nekoliko primjera prirodnih transformacija:

1. Ako je $F : \mathcal{C} \to \mathcal{D}$ bilo koji funktor, **identiteta** $\varepsilon : F \to F$ dana s

$$\varepsilon_X = 1_{F(X)} : F(X) \to F(X)$$

je, svakako, prirodna transformacija.

2. Neka su A_i, $i = 1, 2$, fiksni objekti u kategoriji $\mathcal{C}$, a $F_i : \mathcal{C} \to \mathcal{S}$, $i = 1, 2$, kovarijantni funktori, opisani u Prim. 3. iz 15.3., tj. definirani s $F_i(X) = \mathrm{Mor}(A_i, X)$ na objektima, a na morfizmima s

$$[F_i(f)](g) = f \circ g \, ,$$

za svaki morfizam $g : A_i \to X$. Onda bilo koji morfizam

$$h : A_1 \to A_2$$

generira jednu prirodnu transformaciju

$$\varphi_h : F_2 \to F_1 \, ,$$

danu komponentama

$$(\varphi_h)_X : \mathrm{Mor}(A_2, X) \to \mathrm{Mor}(A_1, X)$$

definiranim s

$$(\varphi_h)_X(g) = g \circ h \, ,$$

za svaki $g : A_2 \to X$. Prirodnost se lako provjeri, što pokazuje da je φ_h zaista prirodna transformacija.

Analogno, ako su B_i, $i = 1, 2$, fiksni objekti u $\mathcal{C}$, a $G_i : \mathcal{C} \to \mathcal{S}$ kontravarijantni funktori, definirani s $G_i(X) = \mathrm{Mor}\,(X, B_i)$ i $[G_i(f)](g) = g \circ f$, za svaki $g : X \to B_i$, $i = 1, 2$, onda bilo koji morfizam

$$h : B_1 \to B_2$$

generira prirodnu transformaciju

$$\varphi^h : G_1 \to G_2\ ,$$

danu po komponentama morfizmima

$$(\varphi^h)_X : \mathrm{Mor}(X, B_1) \to \mathrm{Mor}(X, B_2)\ ,$$

koji su definirani s

$$(\varphi^h)_X(g) = h \circ g\ ,$$

za svaki $g : X \to B_1$.

3. Neka su H_i, $i = 1, 2$, fiksne grupe, a $F_i : \mathcal{G} \to \mathcal{G}$ kovarijantni funktori definirani s

$$F_i(G) = H_i \times G\ , \quad F_i(f) = 1_{H_i} \times f\ , \quad i = 1, 2.$$

Ako je

$$h : H_1 \to H_2$$

bilo koji homomorfizam grupa, njime je određena prirodna transformacija

$$\varphi_h : F_1 \to F_2$$

s komponentama

$$(\varphi_h)_X : H_1 \times G \to H_2 \times G$$

koje su definirane formulom

$$(\varphi_h)_X = h \times 1_G.$$

Analogno se definiraju i prirodne transformacije između funktora na kategoriji $\mathcal{L}$ linearnih prostora, opisanih na isti način (vidi Prim. 10. u 15.3.).

4. Primjer 3. pokazuje kako se determinanta može interpretirati kao prirodna transformacija. Neka je $\mathcal{P}$ kategorija polja i homomorfizama polja. Neka je

$$GL_n : \mathcal{P} \to \mathcal{G}$$

funktor, opisan u Prim. 6. u 15.3. U drugu ruku, neka je

$$M : \mathcal{P} \to \mathcal{G}$$

funktor koji svakom polju pridružuje njegovu multiplikativnu grupu, tj. definiran s $M(F) = F - \{0\}$ i s $M(f) = f/_{E-\{0\}}$, za svaki homomorfizam polja $f : E \to F$. Onda definiramo transformaciju

$$\det : GL_n \to M$$

kao familiju preslikavanja

$$\det_F : GL(n, F) \to F - \{0\} ,$$

gdje je $\det_F(A)$ determinanta matrice A. Zbog Binet-Cauchyjeva teorema (vidi točku 9.8.), $\det_F$ je homomorfizam grupa, dakle morfizam u kategoriji $\mathcal{G}$. Konačno, odmah se provjeri da za svaki homomorfizam $f : E \to F$ dijagram

$$\begin{array}{ccc} GL(n,E) & \xrightarrow{\det_E} & E - \{0\} \\ {\scriptstyle GL_n(f)}\downarrow & & \downarrow {\scriptstyle f/_{E-\{0\}}} \\ GL(n,F) & \xrightarrow{\det_F} & F - \{0\} \end{array}$$

komutira, i prema tome je det zaista prirodna transformacija.

5. Neka je $P : \mathcal{G} \to \mathcal{G}$ funktor, definiran s $P(G) = G/_{[K]}$, gdje je $[K] < G$ komutatorska podgrupa. Tada imamo prirodnu transformaciju

$$\pi : I \to P,$$

gdje je I identiteta na $\mathcal{G}$, u kojoj je za svaku grupu G

$$\pi_G : G \to G/_{[K]}$$

projekcija na kvocijentnu grupu, $\pi_G(a) = a[K]$, za svaki $a \in G$.

Prirodne transformacije možemo komponirati. Točnije, neka su $\varphi : F \to G$ i $\psi : G \to H$ prirodne transformacije funktora $F, G, H : \mathcal{C} \to \mathcal{D}$. Onda definiramo **kompzit** $\psi \circ \varphi$ transformacija φ i ψ kao familiju

$$(\psi \circ \varphi)_X = \psi_X \circ \varphi_X ,$$

parametriziranu objektima iz $\mathcal{C}$.

PROPOZICIJA 1

Kompozit $\psi \circ \varphi$ prirodnih transformacija φ i ψ je prirodna transformacija

$$\psi \circ \varphi : F \to H.$$

Dokaz

Kako su za svaki objekt X

$$\varphi_X : F(X) \to G(X) \quad \text{i} \quad \psi_X : G(X) \to H(X)$$

morfizmi u $\mathcal{D}$, iz definicije kategorije slijedi da je i njihov kompozit

$$\psi_X \circ \varphi_X : F(X) \to H(X)$$

dobro definirani morfizam u $\mathcal{D}$. Prirodnost se lako provjeri pa je $\psi \circ \varphi$ zaista prirodna transformacija. ■

Komponiranje transformacija je asocijativno i, nadalje, za svaku prirodnu transformaciju je

$$\varepsilon \circ \varphi = \varphi \quad \text{i} \quad \varphi \circ \varepsilon = \varphi\,,$$

gdje su s ε označene (odgovarajuće) identične transformacije (Prim. 1.).

Prirodna transformacija $\varphi : F \to G$, u kojoj je svaka komponenta

$$\varphi_X : F(X) \to G(X)$$

ekvivalencija, naziva se **prirodna ekvivalencija**. Kako u tom slučaju svaki od morfizama φ_X ima jedinstveni inverz

$$\varphi_X^{-1} : G(X) \to F(X),$$

dolazimo do familije morfizama

$$\{\varphi_X^{-1} \mid X \text{ je objekt u } \mathcal{C}\},$$

za koju se lako provjeri da definira jednu prirodnu transformaciju

$$\psi : G \to F.$$

Kažemo da je ψ **inverzna transformacija** ili **inverz** od φ, i označavamo ga (jer je jedinstven) s $\psi = \varphi^{-1}$. Primijetimo da iz činjenice da su morfizmi φ_X^{-1} također ekvivalencije, slijedi da je i transformacija φ^{-1} prirodna ekvivalencija. Nadalje, odmah se vidi da je kompozit prirodnih ekvivalencija opet prirodna ekvivalencija.

PROPOZICIJA 2

Ako je $\varphi : F \to G$ prirodna ekvivalencija, onda je:

$$\varphi^{-1} \circ \varphi = \varepsilon_F \quad i \quad \varphi \circ \varphi^{-1} = \varepsilon_G ,$$

gdje su ε_F i ε_G identične transformacije.

Dokaz

Za svaki objekt X iz $\mathcal{C}$ je

$$(\varphi^{-1} \circ \varphi)_X = \varphi_X^{-1} \circ \varphi_X = 1_{F(X)} .$$

Slično se vidi da je $(\varphi \circ \varphi^{-1})_X = 1_{G(X)}$ i tvrdnja je dokazana. ■

Neka su $F, G : \mathcal{C} \to \mathcal{D}$ funktori. Kažemo da je F **prirodno ekvivalentan** s G, i pišemo $F \approx G$, ako postoji bar jedna prirodna ekvivalencija $\varphi : F \to G$. Iz svojstava prirodnih ekvivalencija odmah slijedi da je $\approx$ jedna relacija ekvivalencije, koja provodi klasifikaciju svih funktora $\mathcal{C} \to \mathcal{D}$.

Kao klasični primjer promatrajmo kategoriju $\mathcal{L} = \mathcal{L}_K$ konačnodimenzionalnih linearnih prostora i kovarijantni funktor

$$D^2 = D \circ D : \mathcal{L} \to \mathcal{L} ,$$

gdje je D funktor koji svakom prostoru pridružuje njegov dual (vidi Prim. 9. u 15.3.). Onda postoji prirodna transformacija

$$\varphi : I \to D^2$$

identitete I na $\mathcal{L}$ u D^2, definirana na komponentama s

$$\varphi_V : V \to V^{**} ,$$

gdje je φ_V prirodni izomorfizam prostora na njegov bidual (vidi točku 8.7.). Jasno je da je φ prirodna ekvivalencija, i prema tome je $D^2 \approx I$.

Daljnji primjer su funktori $F_1, F_2 : \mathcal{C} \to \mathcal{S}$, opisani u Prim. 2., za koje se lako vidi da će biti prirodno ekvivalentni ako i samo ako su objekti A_1 i A_2, koji ih generiraju, ekvivalentni u $\mathcal{C}$. Analogna tvrdnja vrijedi i za funktore $G_1, G_2 : \mathcal{G} \to \mathcal{S}$ iz tog primjera.

Konačno, funktori $F_1, F_2 : \mathcal{G} \to \mathcal{G}$ iz Prim. 3. su prirodno ekvivalentni ako i samo ako su grupe H_1 i H_2, pomoću kojih su definirani, izomorfne.

PROPOZICIJA 3

Neka su $F, G : \mathcal{C} \to \mathcal{D}$ prirodno ekvivalentni funktori, $F \approx G$. Ako je $H : \mathcal{D} \to \mathcal{E}$ bilo koji funktor, onda je

$$H \circ F \approx H \circ G .$$

Ako je $K : \mathcal{B} \to \mathcal{C}$ bilo koji funktor, onda je

$$F \circ K \approx G \circ K \, .$$

Dokaz

Po pretpostavci postoji prirodna ekvivalencija $\varphi : F \to G$ s komponentama

$$\varphi_X : F(X) \to G(X)$$

koje su ekvivalencije u $\mathcal{D}$. Kako je H funktor, to je

$$H(\varphi_X) : H[F(X)] \to H[G(X)]$$

morfizam u $\mathcal{E}$. Tako dolazimo do familije morfizama

$$\psi_X : (H \circ F)(X) \to (H \circ G)(X) \, ,$$

gdje je

$$\psi_X = H(\varphi_X) \, ,$$

za svaki objekt X iz $\mathcal{C}$, za koju se lako provjeri da određuje prirodnu transformaciju

$$\psi : H \circ F \to H \circ G \, .$$

Nadalje, jer su φ_X ekvivalencije, prema Prop. 1 u 15.3. i ψ_X su ekvivalencije, pa je ψ prirodna ekvivalencija i tvrdnja da je $H \circ F \approx H \circ G$ je dokazana. Slično, da bismo dokazali drugu tvrdnju, definiramo prirodnu ekvivalenciju

$$\chi : F \circ K \to G \circ K$$

s komponentama

$$\chi_X : F[K(X)] \to G[K(X)] \, ,$$

gdje je $\chi_X = \varphi_{K(X)}$, za svaki objekt X iz $\mathcal{B}$. ■

Kažemo da je funktor $F : \mathcal{C} \to \mathcal{D}$ **ekvivalencija kategorija** ako postoji funktor $G : \mathcal{D} \to \mathcal{C}$ tako da vrijedi

$$G \circ F \approx I_{\mathcal{C}} \quad \text{i} \quad F \circ G \approx I_{\mathcal{D}} \, ,$$

gdje su $I_{\mathcal{C}}$ i $I_{\mathcal{D}}$ identični funktori. U tom slučaju očito je i G ekvivalencija kategorija i nazivamo ga **inverznom ekvivalencijom** od F. Primijetimo da G **nije** jednoznačno određen s F. Nadalje, vrijedi

PROPOZICIJA 4

Ako su $F : \mathcal{C} \to \mathcal{D}$ *i* $H : \mathcal{D} \to \mathcal{E}$ *ekvivalencije kategorija, i njihova kompozicija*

$$H \circ F : \mathcal{C} \to \mathcal{E}$$

je ekvivalencija kategorija.

Dokaz

Neka su $G : \mathcal{D} \to \mathcal{C}$ i $K : \mathcal{E} \to \mathcal{D}$ inverzne ekvivalencije od F, odnosno H. Onda je $G \circ F \approx I$, $F \circ G \approx I$ i $K \circ H \approx I$, $H \circ K \approx I$. Tvrdimo da je $G \circ K$ inverzna ekvivalencija od $H \circ F$. Zaista, iz $K \circ H \approx I$ primjenom Prop. 3 imamo

$$(G \circ K) \circ (H \circ F) = G \circ (K \circ H) \circ F \approx G \circ I \circ F = G \circ F \approx I \,,$$

a slično se vidi da je i

$$(H \circ F) \circ (G \circ K) \approx I \,,$$

i tvrdnja je dokazana. ■

Kažemo da je kategorija $\mathcal{C}$ **ekvivalentna** s kategorijom $\mathcal{D}$, i pišemo

$$\mathcal{C} \approx \mathcal{D} \,,$$

ako postoji bar jedna ekvivalencija kategorija $F : \mathcal{C} \to \mathcal{D}$. Iz prethodnog je jasno da se radi o dobro definiranoj relaciji ekvivalencije.

Primijetimo i ovo: Ako su $\mathcal{C}$ i $\mathcal{D}$ izomorfne kategorije, onda postoji izomorfizam kategorija $F : \mathcal{C} \to \mathcal{D}$, i za njega je

$$F^{-1} \circ F = I \quad \text{i} \quad F \circ F^{-1} = I \,,$$

što pokazuje da su te kategorije i ekvivalentne. Obrat, međutim, ne vrijedi. Klasifikacija kategorija do na ekvivalenciju je "grublja" od one do na izomorfizam.

Tu tvrdnju ilustrirat ćemo jednim primjerom. Neka je F bilo koje polje, $\mathcal{L} = \mathcal{L}_{FK}$ kategorija konačnodimenzionalnih prostora nad poljem F, a $\mathcal{M}_F$ kategorija matrica nad poljem F, opisana u Prim. 13. u točki 15.2. Ako u svakom od linearnih prostora fiksiramo bazu, možemo definirati funktor

$$H : \mathcal{L} \to \mathcal{M}_F$$

s

$$H(V) = \dim V$$

na objektima, a za svaki linearni operator $f : U \to V$ s

$$H(f) : \dim U \to \dim V ,$$

gdje je $H(f) = A$ matrica operatora f u danim bazama. Obratno, ako definiramo

$$K : \mathcal{M}_F \to \mathcal{L}$$

s

$$K(n) = F^n ,$$

gdje je F^n standardni (koordinatni) prostor dimenzije n nad poljem F, a za svaku matricu $A : n \to m$ (ta je tipa (m, n)!) uzmemo za

$$K(A) : F^n \to F^m$$

linearni operator $K(A) = f$, koji je u danim bazama jednoznačno određen matricom A, lako se provjeri da je

$$K \circ H \approx I \quad \text{i} \quad H \circ K = I ,$$

tj. da je H ekvivalencija kategorija. U drugu ruku, te kategorije nisu izomorfne, jer ne postoji bijektivna korespondencija na objektima (linearnih prostora ima neprebrojivo mnogo).

Ekvivalentne kategorije su one koje imaju sličnu strukturu, ali se mogu razlikovati u "veličini" (vidi Zad. 6.-8.).

ZADACI

1. Prirodne transformacije su zapravo morfizmi između funktora. Točnije, ako su $\mathcal{C}$ i $\mathcal{D}$ bilo koje kategorije, onda funktori $\mathcal{C} \to \mathcal{D}$ kao objekti i prirodne transformacije funktora kao morfizmi, konstituiraju kategoriju, koju obično označavamo s Fun $(\mathcal{C}, \mathcal{D})$. Dokaži!

2. Neka je S fiksni skup, a X^S skup svih preslikavanja $h : S \to X$ u skup X. Onda definiramo funktor

   $$F_S : \mathcal{S} \to \mathcal{S}$$

   s $F_S(X) = X^S \times S$ na objektima, a s $F_S(f) = (f \circ h) \times 1_S$ na morfizmima. Pokaži da je **funkcijom evaluacije**

   $$\varphi_X : X^S \times S \to X ,$$

   danom s $\varphi_X(h, s) = h(s)$, definirana prirodna transformacija

   $$\varphi : F_S \to I ,$$

   gdje je $I : \mathcal{S} \to \mathcal{S}$ identični funktor.

3. Neka su G i H grupe, shvaćene kao kategorije (vidi Zad. 1. u 15.1.), a $f, g : G \to H$ funktori (tj. homomorfizmi grupa). Pokaži da postoji prirodna transformacija $\varphi : f \to g$ ako i samo ako su f i g konjugirani (vidi Zad. 2. u 15.2.). Uz koji će uvjet f i g biti prirodno ekvivalentni?

4. Neka su $F, G : \mathcal{C} \to \mathcal{D}$ funktori u parcijalno uređeni skup $\mathcal{D} = (S, \leq)$, koji je shvaćen kao kategorija (vidi Prim. 14. u 15.2.). Pokaži da postoji prirodna transformacija $\varphi : F \to G$ ako i samo ako je $F(X) \leq G(X)$, za svaki objekt X iz $\mathcal{C}$. Ako transformacija φ postoji, ona je određena jednoznačno.

5. Definiraj kategoriju $\mathcal{L}_{FK}/\cong$, u kojoj su objekti klase međusobno izomorfnih konačnodimenzionalnih prostora i pokaži da je ta kategorija izomorfna s kategorijom $\mathcal{M}_F$ (vidi primjer na kraju teksta u ovoj točki).

6. Neka je $\mathcal{K} \prec \mathcal{C}$ puna potkategorija od $\mathcal{C}$. Kažemo da je $\mathcal{K}$ **skelet** od $\mathcal{C}$, ako je svaki objekt iz $\mathcal{C}$ ekvivalentan točno jednom objektu iz $\mathcal{K}$. Na primjer, kategorija $\mathcal{S}_K$ konačnih skupova kao skelet ima punu potkategoriju određenu skupovima $\Delta^0, \Delta^1, \Delta^2, ...$, gdje je $\Delta^0 = \emptyset$, a $\Delta^n = \{0, 1, ..., n-1\}$, za svaki $n = 1, 2, \ldots$. Isto tako, u kategoriji $\mathcal{L}_{FK}$ skelet čine koordinatni prostori $F^0, F^1, F^2, \ldots$. Pokaži da su svi skeleti neke kategorije međusobno izomorfni (kao kategorije). Kažemo da je kategorija $\mathcal{C}$ **skeletna** ako je sama svoj skelet (tj. ako su u $\mathcal{C}$ ekvivalentni objekti samo oni koji su jednaki). Nađi primjere skeletnih kategorija.

7. Pokaži: Ako je $\mathcal{K}$ skelet od $\mathcal{C}$, onda je inkluzija $\mathcal{K} \to \mathcal{C}$ ekvivalencija kategorija, tj. kategorija je ekvivalentna sa svakim svojim skeletom.

8. Neka je $\mathcal{K}$ skelet od $\mathcal{C}$, a $\mathcal{H}$ skelet od $\mathcal{D}$. Kategorije $\mathcal{C}$ i $\mathcal{D}$ su ekvivalentne ako i samo ako su kategorije $\mathcal{K}$ i $\mathcal{H}$ izomorfne. Dokaži!

9. Pokaži: Funktor $F : \mathcal{C} \to \mathcal{D}$ je ekvivalencija kategorija ako i samo ako je F pun, vjeran (vidi točku 15.3.) i ima svojstvo da za svaki objekt Y iz $\mathcal{D}$ postoji objekt X iz $\mathcal{C}$, tako da je Y ekvivalentan s $F(X)$.

10. Neka je $\mathcal{C}_0 \prec \mathcal{C}$ puna potkategorija. Ako postoji funktor $R : \mathcal{C} \to \mathcal{C}_0$ tako da je $R \circ J = I_{\mathcal{C}_0}$, gdje je $J : \mathcal{C}_0 \to \mathcal{C}$ inkluzija, kažemo (po analogiji iz topologije) da je $\mathcal{C}_0$ **retrakt** od $\mathcal{C}$, a funktor R nazivamo **retrakcija**. Ako uz to vrijedi

$$J \circ R \approx I_{\mathcal{C}} ,$$

kažemo da je $\mathcal{C}_0$ **deformacijski retrakt**, a R je **deformacijska retrakcija**. Deformacijski retrakt je, dakako, ekvivalentan s kategorijom $\mathcal{C}$. Navedi primjere retrakata i deformacijskih retrakata. Je li svaki skelet retrakt? A obratno?

11. Generaliziraj pojam prirodne transformacije i prirodne ekvivalencije na funktore u više varijabli.

LITERATURA

AGLIĆ, A. — ELEZOVIĆ, N. , *Zbirka zadataka iz linearne algebre* (drugo izdanje) Element, Zagreb, 2001.

BAKIĆ, N. — MILAS, A., *Zbirka zadataka iz linearne algebre* PMF — Matematički odjel i HMD, Zagreb, 1996.

BILINSKI, S., *Analitička geometrija s uvodom u linearnu algebru* (skripta) Sveučilište u Zagrebu, Zagreb, 1963.

BLANUŠA, D., *Viša matematika, I. i II. dio* Tehnička knjiga, Zagreb, 1970., 1974.

DIEUDONNÉ, I. C.,*Linearna algebra i elementarna geometrija* (prijevod s francuskog), Školska knjiga, Zagreb, 1977.

ELEZOVIĆ, N., *Linearna algebra* Element, Zagreb, 2001.

KUREPA, S., *Konačnodimenzionalni vektorski prostori* Tehnička knjiga, Zagreb, 1967.

KUREPA, S., *Uvod u matematiku* Tehnička knjiga, Zagreb, 1971.

KUREPA, S., *Uvod u linearnu algebru* Školska knjiga, Zagreb, 1975.

KUREPA, S., *Funkcionalna analiza* Školska knjiga, Zagreb, 1981.

KURNIK, Z. — VOLENEC, V., *Matematika* 2 Školska knjiga, Zagreb, 1974.

MARDEŠIĆ, S., *Matematička analiza u n-dimenzionalnom realnom prostoru, I. i II. dio* Školska knjiga, Zagreb, 1974., 1977.

PAVKOVIĆ, B. — VELJAN, D., *Elementarna matematika* 1. Školska knjiga, Zagreb, 2004.

PAVKOVIĆ, B. — VELJAN, D., *Elementarna matematika* 2. Školska knjiga, Zagreb, 1995.

VELJAN, D., *Kombinatorika i diskretna matematika*
Algoritam, Zagreb, 2004.

ŽUBRINIĆ, D., *Linearna algebra*
(poslijediplimski studij FER-a), Element, Zagreb, 2003.

* * *

PERIĆ, V., *Predavanja iz linearne algebre*
(skripta) Univerzitet u Sarajevu, Sarajevo, 1963.

PERIĆ, V., *Algebra, I. i II. dio*
Svjetlost, Sarajevo, 1980.

* * *

KRIŽANIČ, F., *Linearna algebra in linearna analiza*
Mladinska knjiga, Ljubljana, 1969.

KRIŽANIČ, F., *Vektori, metrike, tenzorji*, I, II
Mladinska knjiga, Ljubljana, 1972.

VIDAV, I., *Algebra*
Mladinska knjiga, Ljubljana, 1972.

* * *

ANĐELIĆ, T. P., *Matrice*
Naučna knjiga, Beograd, 1962.

MITRINOVIĆ, D. S. — MIHAJLOVIĆ, D., *Linearna algebra, analitička geometrija, polinomi*
Naučna knjiga, Beograd, 1959.

* * *

ABRAHAM, R., *Linear and Multilinear Algebra*
Benjamin Inc., New York, 1966.

ARTIN,E., *Geometric Algebra*
Interscience, New York, 1957.

AXLER, S., *Linear Algebra Done Right*
Springer Vrlg., New York, 1997.

BEAUMONT, R. A., *Linear Algebra*
Harcourt, Brace and World Inc., New York, 1965.

COHN, P. M., *Algebra, Vol. I*
John Wiley and Sons Inc., London, 1974.

FLETCHER, T. J., *Linear Algebra through its Applications*
Van Nostrand Reinhold Co., London, 1972.

HALMOS, P. R., *Finite-dimensional Vector Spaces*
Van Nostrand Co., Princeton, 1958.

HERNSTEIN, I. N., *Topics in Algebra*
John Wiley and Sons Inc., New York, 1975.

HOFFMAN, K. — KUNZE, R., *Linear Algebra*
Prentice-Hall Inc., Englewood Cliffs, 1961.

HU, S. T., *Elements of Modern Algebra*
Holden-Day Inc., San Francisco, 1965.

JACOBSON, N., *Lectures in Abstract Algebra I, II*
Van Nostrand Co., Princeton, 1952.

JACOBSON, N., *Basic Algebra I*
Freeman and Comp., San Francisco, 1974.

LANG, S., *Linear Algebra*
Addison-Wesley Publ. Co., Reading, 1969.

LANG, S., *Undergraduate Algebra*
Springer Vrlg., Berlin, 1990.

LANG, S., *Algebra*
Addison-Wesley Publ. Co., Reading, 1993.

LIPSON, M. — LIPSCHUTZ, S., *Outline of Linear Algebra*
Schaum Outline Series, McGraw-Hill Book Co., New York, 2000.

LIPSCHUTZ, S., 3000 *Solved Problems in Linear Algebra*
Schaum Outline Series, McGraw-Hill Book Co., New York, 1989.

MAC LANE, S., *Categories for the Working Mathematician*
Springer Vrlg., New York, 1971.

MC COY, N. H. — BERGER, T. R., *Algebra: Groups, Rings and other Topics*
Allyn and Bacon Inc., Boston, 1977.

NERING, E. D., *Linear Algebra and Matrix Theory*
John Wiley and Sons Inc., New York, 1970.

NOMIZU, K., *Fundamentals of Linear Algebra*
Mc Graw-Hill Book Co., New York, 1966.

SAMELSON, H., *An Introduction to Linear Algebra*
John Wiley and Sons Inc., New York, 1974.

SHIELDS, P. C., *Linear Algebra*
Addison-Wesley Publ. Co., Reading, 1964.

SMITH, L., *Linear Algebra*
Springer Vrlg., Berlin, 1978.

STEWART, F. M., *Introduction to Linear Algebra*
Van Nostrand Co., Princeton, 1963.

ZELINSKY, D., A first Course in Linear Algebra
Academic Press Inc., New York, 1968.

WHITE, P. A., *Linear Algebra*
Dickenson Publ. Co., Belmont, 1966.

* * *

BRIESKORN, E., *Lineare Algebra und Analitische Geometrie, I, II*
Friedr. Vieweg und Sohn, Wiesbaden, 1985.

GRAAUB, W., *Lineare Algebra*
Springer Vrlg., Berlin, 1958.

KOWALSKY, H. J., *Lineare Algebra*
Walter de Gruter and Co., Berlin, 1963.

KLIN, M. CH. — PÖSCHEL, R. — ROSENBAUM, K., *Angewandte Algebra für Mathematiker und Informatiker*
Friedr. Vieweg und Sohn, Wiesbaden, 1988.

LÜNEBURG, H., *Einführung in die Algebra*
Springer Vrlg., Berlin, 1973.

WILLE, D., *Repetitorium der Linearen Algebra*, I, II
Harri Deutsch Vrlg., 1991.

* * *

CUBERBILLER, O. N., *Zadači i upražnenija po analitičeskoj geometrii*
Nauka, Moskva, 1970.

EFIMOV, N. V. — ROZENDORN, E. R., *Linejnaja algebra i mnogomernaja geometrija*
Nauka, Moskva, 1970.

GANTMAHER, F. R., *Teorija matric*
Nauka, Moskva, 1967.

GEL'FAND, I. M., *Lekcii po linejnoj algebre*
Nauka, Moskva, 1966.

IKRAMOV, H. D., *Zadačnik po linejnoj algebre*
Nauka, Moskva, 1975.

KOSTRIKIN, A. I., *Vvedenije v algebru*
Nauka, Moskva, 1977.

KOSTRIKIN, A. I., *Sbornik zadač po linejnoj algebre*
Nauka, Moskva, 1987.

KOSTRIKIN, A. I. — MANIN, Ju. I., *Linejnaja algebra i geometrija*
Nauka, Moskva, 1986.

KUROŠ, A. G., *Kurs vyššej algebry*
Nauka, Moskva, 1965.

KUROŠ, A. G., *Teorija grupp*
Nauka, Moskva, 1967.

MAL'CEV, A. I., *Osnovy linejnoj algebry*
Nauka, Moskva, 1970.

PROSKURJAKOV, I. V., *Sbornik zadač po linejnoj algebre*
Gos. Izd. Fiz.-Mat. Lit., Moskva 1962. (također englesko izdanje: Mir Publ., Moscow, 1985.)

RAJKOV, D. A., *Vektornije prostranstva*
Gos. Izd. Fiz.-Mat. Lit., Moskva, 1962.

RUBLEV, A. N., *Linejnaja algebra*
Vyššaja škola, Moskva, 1968.

ŠILOV, G. E., *Vvedenie v teoriju linejnyh prostranstv*
Gos. Izd. Tehn.-Teor. Lit., Moskva, 1956.

VOEVODIN, V. V., *Linejnaja algebra*
Nauka, Moskva, 1974.

* * *

I za kraj, kao kuriozitet:

ASANO, K., *Senkei daisûgaku teiyô*
(na japanskom: Priručnik za linearnu algebru), Kyôritu, 1948.

TAKAGI, T., *Daisûgaku Kôgi*
(na japanskom: Predavanja iz algebre), Kyôritu, 1948.

KAZALO IMENA

Brojevi na kraju imena upućuju na stranicu na kojoj se ime prvi put spominje.

ABEL, N. H., norveški matematičar (1802. - 1829.); 42

BERNAYS, P., švicarski matematičar (1888. - 1977.); 635

BESSEL, F. W., njemački astronom i matematičar (1784. - 1846.); 491

BINET, J. P. M., francuski matematičar i astronom (1786. - 1856.); 370

BOOLE, G., engleski matematičar i logičar (1815. - 1864.); 49

BUNJAKOVSKI, V. J. B., ruski matematičar (1804. - 1889.); 176

CANTOR, G. F. L. P., njemački matematičar (1845. - 1918.); 20

CAPELLI, A., talijanski matematičar (1855. - 1910.); 442

CAUCHY, A. L., francuski matematičar (1789. - 1857.); 75

CAYLEY, A., engleski matematičar (1821. - 1895.); 41

CRAMER, G., švicarski matematičar (1704. - 1752.); 443

ČEBIŠEV, P. L., ruski matematičar (1821. - 1894.); 497

DE MORGAN, A., engleski matematičar i logičar (1806. - 1871.); 10

EILENBERG, S., američki matematičar poljskog podrijetla (1913. - 1998.); 633

EUKLID, grčki matematičar (oko 330. - 275. pr. Kr.); 146, 470

EULER, L., švicarski matematičar, fizičar i astronom (1707. - 1783.); 64

FADEJEV, D. K., ruski matematičar (1907. - 1989.); 384

FERMAT, P., francuski matematičar (1601. - 1665.); 64

FOURIER, J.-B. J., francuski matematičar i fizičar (1768. - 1830.); 489

FRAME, I. S., američki matematičar (1907. - 1997.); 384

FROBENIUS, G., njemački matematičar (1849. - 1917.); 332

GALOIS, E., francuski matematičar (1811. - 1832.); 75

GAUSS, K. F., njemački matematičar i astronom (1777. - 1855.); 75

GÖDEL, K., američki matematičar i logičar austrijskog podrijetla (1906. - 1977.); 635

GRAM, J. P., danski matematičar (1850. - 1916.); 482

GRASSMANN, H., njemački matematičar (1809. - 1877.); 145

HAMEL, G., njemački matematičar (1877. - 1954.); 260

HAMILTON, W. R., irski matematičar i fizičar (1805. - 1865.); 145

HAUSDORFF, F., njemački matematičar (1868. - 1942.); 642

HERMITE, C., francuski matematičar (1822. - 1901.); 332

HESSE, L. O., njemački matematičar (1811. - 1874.); 212

HILBERT, D., njemački matematičar (1862. - 1943.); 146

JACOBI, C. G., njemački matematičar (1804. - 1851.); 124

JORDAN, M. E. C., francuski matematičar (1838. - 1902.); 124

KARTEZIUS (DESCARTES), R., francuski filozof, matematičar i fizičar (1596. - 1650.); 22

KLEIN, F., njemački matematičar (1849. - 1925.); 73

KRALJEVIĆ, H., hrvatski matematičar (1944. -); 613

KRONECKER, L., njemački matematičar (1823. - 1891.); 322

LAGRANGE, P. J. L., francuski matematičar (1736. - 1813.); 75

LAPLACE, P. S., francuski matematičar i astronom (1749. - 1827.); 375

LEGENDRE, A. M., francuski matematičar (1752. - 1833.); 497

LIE, M. S., norveški matematičar (1842. - 1899.); 124

LORENTZ, H. A., nizozemski fizičar (1853. - 1928.); 616

MAC LANE, S., američki matematičar (1909. -); 633

MILNOR, J., američki matematičar (1931. -); 601

MINKOWSKI, H., njemački matematičar i fizičar (1864. - 1909.); 478

NEUMANN, J. von, američki matematičar mađarskog podrijetla (1903. - 1957.); 635

PARSEVAL, M. A., francuski matematičar (1776. - 1836.); 491

PITAGORA, grčki filozof i matematičar (oko 582. - 496. pr. Kr.); 491

ROUCHÉ, E., francuski matematičar (1832. - 1910.); 448

SARRUS, P. F., njemački matematičar (1789. - 1861.); 365

SCHMIDT, E., njemački matematičar (1876. - 1959.); 492

SCHWARZ, K. H. A., njemački matematičar (1843. - 1921.); 176

STEINITZ, E., njemački matematičar (1871. - 1928.); 264

STEVIN, S., nizozemski fizičar (1548. - 1620.); 145

SYLVESTER, J. J., engleski matematičar (1814. - 1897.); 310

TÖPLITZ, O., njemački matematičar (1881. - 1940.); 539

VANDERMONDE, A. T., belgijski matematičar (1735. - 1796.); 370

VENN, J., engleski logičar (1834. - 1923.); 6

VIVIANI, V., talijanski matematičar (1622. - 1703.); 239

WEIERSTRASS, K., njemački matematičar (1815. - 1897.); 332

ZORN, M., američki matematičar njemačkog podrijetla (1906. - 1993.); 262

KAZALO POJMOVA

A

Abelov (komutativni) grupoid, 42
Abelova (komutativna) grupa, 52
— familija operatora, 547
—, slobodna grupa generairana skupom, 649
aditivna grupa, 53
— — prstena, 119
aditivni monoid cijelih brojeva mod m, 48
aditivnost linearnog operatora na V^3, 193
adjungirana (hermitski konjugirana) matrica, 335
adjungirani (hermitski konjugirani, hermitski adjungirani) operator, 526
adjungiranje, 339
adjunkta matrice, 379
afina grupa ravnine, 70
afine koordinate, 632
— — točke u E^3, 211
afini koordinatni sustav u E^3, 211
— operator, 292
— prostor (nad poljem F), 630
afino preslikavanje, 70
aksiom, 4
aksiom grupe, 52
— kategorije, 634
— linearnog prostora, 248
— norme, 477
— prstena, 119
— topologije, 482
— unitarnog prostora, 468
algebarska (Hamelova) baza, 260
— dimenzija prostora, 262
— kratnost svojstvene vrijednosti, 424
— struktura, 40
algebarski broj, 21
— komplement (kofaktor), 376
algebra, 182
—, Liejeva, 183, 319
— nad poljem F, 316
s dijeljenjem, 319
—, linearna, 316
—, realna, 318
algoritam, Frame-Fadejevljev, 384
—, Lagrangeov, 586
alternirajuća grupa stupnja n, 79
anihilator skupa, 326
antihermitska (hermitski antisimetrična) matrica, 338
antihermitski operator, 530
antiizomorfizam linearnih prostora, 339
antikomutativnost množenja u prstenu, 124
antilinearni operator, 511
antisimetrična matrica, 338
antisimetrični operator, 530
antiunitarni operator, 511
aplikata (kota) točke u E^3, 209
apscisa točke u E^3, 209
apstraktna grupa, 92
asocijativni grupoid (polugrupa), 43
automorfizam, 86
— grupe, 90
— linearnog prostora, 299
—, unutrašnji grupe, 93
azimut točke u E^3, 242

B

baza, desno orijentirana (desna) za V^3, 166
—, koordinatna (koordinatni sustav) linearnog prostora,

385
— — (koordinatni sustav), za V^3, 166
— , lijevo orijetirana (lijeva) za V^3, 166
— linearnog prostora, 260
— — —, Hamelova (algebarska), 260
— — — , kanonska, 261
— , normalna, 626
— , — pseudounitarnog prostora, 615
— , ortonormirana u V^3, 174
— prostora V^2, 168
— , simplektička prostora, 620
— topologije, 482
— , ortogonalna, 487
— , ortonormirana, 487
beskonačan skup, 20
— — , neprebrojivo, 20
— — , prebrojivo, 20
beskonačna grupa, 52
— — , ciklička, 63
Besselova nejednakost, 491
bidual prostora, 322
bijekcija, 16
bilinearna forma, 589
— — , antisimetrična, 591
— — , hermitska, 609
— — , kompleksna, 608
— — , simetrična, 591
bilinearne forme, ekvivalentne, 590
— — , kongruentne, 590
— — , ortogonalno kongruentne, 591
bilinearni funkcional, 329, 572
— — , antihermitski (hermitski antisimetričan), 602
— — , antisimetričan, 575
— — , hermitski (hermitski simetričan), 602
— — , kompleksni, 601
— — , regularan, 575
— — , simetričan, 329, 575
— — , singularan, 575
— operator, 344, 580
binarna operacija, 39
— — , asocijativna, 43
— — , komutativna, 42
— relacija, 37
blokmatrica, 415, 416
Booleovo množenje, 49
— zbrajanje, 49

C

Cauchyjeve nejednakosti, 474
Cayleyjev transformat, 538
Cayleyjeva tablica, 41
Cayleyjeve transformacijske formule, 557
Cayleyjevi brojevi (oktave), 68
centar grupe, 64
— prstena, 130
centralizator skupa, 64
centralna hiperkvadrika (hiperploha 2. reda), 625
— normalna podgrupa, 102
— simetrija u $\mathbb{R}^2$, 506
— — u unitarnom prostoru, 506
Charlesova relacija, 156
cijepanje morfizma, 640
ciklička grupa, 63
— — , beskonačna, 63
— — reda n, 63
— podgrupa, 63
ciklus (ciklička permutacija), 80
cilindar, 23
— drugog reda, 236
— — — , eliptički, 237
— — — , hiperbolički, 237
— — — , parabolički, 237
cilindrična spirala, 239
Cramerov sustav, 444

Č

Čebiševljevi polinomi, 497
član (element, točka) skupa, 6

D

defekt hermitskog bilinearnog funkcionala, 613
— linearnog operatora, 305
— prostora, 618
definitnost kvadratne forme, 597
De Morganove formule, 10

desna jedinica, 45
— susjedna klasa podgrupe, 104
— translacija (u grupi), 71
desni ideal, 127
— inverz, 49
— inverz morfizma (prerez), 639
— koordinatni sustav u E^3, 208
— kvocijentni skup (grupe po podgrupi), 104
desno orijentirana (desna) baza za V^3, 166
determinanta drugog reda, 185
— , Gramova, 484
— matrice, 364
— operatora, 400
— trećeg reda, 185
— , Vandermondeova, 370
determinantna funkcija, 364
diferencija skupova, 9
dijagonala Kartezijeva kvadrata, 22
— kvadratne matrice, glavna, 333
— — — , sporedna, 334
dijagonalizacija matrice trećeg reda, 204
— operatora, 425
dijagonalna forma matrice trećeg reda, 204
— inkluzija, 26, 580
— matrica, 345
dijagonalni (kanonski) oblik bilinearne forme, 591
— — — kvadratne forme, 586
dijeljenje dužine u zadanom omjeru, 210
dilatacija (homotetija), 251
— u V^3, 199
dimenzija afinog prostora, 630
— linearne mnogostrukosti, 282
— linearnog prostora, 262
— — — , algebarska, 262
— unitarnog prostora, 468
dio operatora, antihermitski, 549
— — , hermitski, 549
direktna razlika prostora, 280
— suma operatora, 413
— — potprostora, 277, 281, 287
direktni komplement potprostora, 280
— produkt grupa, 114
— — homomorfizama grupa, 116
— — unitarnih prostora, 472
— sumandi prostora, 279
disjunkcija, 1
disjunktni skupovi, 9
diskretna metrika, 481
djelitelji nule u prstenu, 125
— — u algebri, 319
domena, 11
— morfizma u kategoriji, 634
donja trokutasta matrica, 346
dualna baza, 322
dualni operator, 327
— prostor linearnog prostora (dual), 321
— — prostora V^3, 205
— prostori, 330
— skalarni produkt, 567
— unitarni prostor, 568
duljina (modul) vektora, 151
— (norma, modul) vektora u unitarnom prostoru, 474

E

egzaktni niz, 309
— — , kratki, 309
ekstenzija funkcije, 15
ekvimetrični operator, 550
ekvipotentni skupovi, 19
ekvivalencija, 2
— (izomorfizam), 636
— , inverzna, 658
— kategorija, 658
ekvivlantne matrice, 358
— orijentirane dužine, 146
ekvivalentni objekti u kategoriji, 637
— sustavi linearnih jednadžbi, 452
element (član, točka) skupa, 6
— beskonačnog reda u grupi, 55
— , idempotentan, 41
— , invertibilan, 49
— , involutoran u grupi, 56
— konačnog reda u grupi, 55

— , maksimalni, 37
— , minimalni, 33
— , nilpotentan, 126
— , recipročni, 51
— , suprotni, 51
elementarna matrica, 362
elementarne transformacije nad matricom, 357
— — nad sustavom, 452
elementi matrice, 333
elipsoid, 234
endomorfizam, 86
epi, 639
epimorfizam, 86
euklidska grupa, 524
euklidski prostor, 470, 632
— — , kompleksni, 620
Eulerovi kutovi, 390

F

familija, 5
forma, 589
— , bilinearna, 589
— , Jordanova matrice, 429
— , Kartezijeva (dekompozicija) operatora, 549
— , kubna, 583
— , kvadratna, 583, 584
— , linearna, 328, 583, 589
— , multilinearna, 589
— , normalna matrice, 432
— , — unitarnog (ortogonalnog) operatora, 522
— , polarna (dekompozicija) operatora, 553
— , regularna 584, 590
— , singularna, 590
— , spektralna (dekompozicija) operatora, 558
— , stupnja p, 583
— , trilinearna, 589
Fourierovi koeficijenti vektora, 489
Frame-Fadejevljev algoritam, 384
fundamentalni skup rješenja homogenog sustava, 449
funkcija, 11
— , determinantna, 364
— evaluacije, 660
— izjavna, 3
— , karakteristična, 18
— na morfizmima, 644
— na objektima, 644
— , realna, 12
— udaljenosti (metrička funkcija, metrika), 480
funkcijski skup, 17
funkcional, 320
— , bilinearni, 329, 572
— , kvadratni, 580, 581
— , linearni, 320
— , — na V^3, 205
— , multilinearni, 571
— na V^3, 205
— , osnovni, 614
— , polarni, 582
— , simetrični bilinearni, 329
— , transponirani, 579
funktor, 644
— , aditivni, 651
— , dualni, 651
— , ekvivalencija kategorija, 658
— , identični (identiteta), 645
— , inverzna ekvivalencija kategorija, 658
— , inverzni, 649
— koji zaboravlja (funktor zaborava, zaboravljivi funktor), 646
— , kontravarijantan, 645
— , kovarijantan, 645
— , puni, 648
— u dvije varijable (bifunktor), 651
— , vjerni (smještenje), 648
funktori, prirodno ekvivalentni, 657

G

Gauss-Jordanova metoda eliminacije, 452
geometrijska kratnost svojstvene vrijednosti, 418
glavna dijagonala matrice, 333
glavni ideal, 130
gornja trokutasta matrica, 346

graf preslikavanja, 35
Gramova determinanta, 484
— matrica, 484
— — skupa s obzirom na funkcional, 613
— — u prostoru s hermitskom metrikom, 618
Gram-Smidtov postupak ortogonalizacije u V^3, 492
— — — u unitarnom prostoru, 493
grupa, 52
—, aditivna, 53
— , — prstena, 119
— , afina ravnine, 70
— , alternirajuća stupnja n, 79
— , apstraktna, 92
— , beskonačna, 52
— , — ciklička, 63
— , ciklička, 63
— , — reda n, 63
— cilindra, 114
— euklidska $I(\mathbb{R}^3)$; 524
— gibanja $\mathcal{G}(U)$, 524
— — ravnine, 70
— izometrija, 511
— — prostora $\mathbb{R}^3$; $I(\mathbb{R}^3)$, 524
— klasa ostataka mod m, 108
— , Kleinova četvorna, 73
— , kompleksna, 68
— , komutativna (Abelova), 52
— , konačna, 52
— kružnice, 66
— , kvaternionska, 68
— , kvocijentna (faktorska), 107
— lijevih translacija, 70
— , multiplikativna, 53
— , muliplikativna tijela, 138
— , opća linearna $GL(3)$, 204
— , — — $GL(n, F)$, 348
— , — — Aut V, 396
— , ortogonalna $O(3)$, 204
— , — $O(n, F)$, 349
— , — $\mathcal{O}(U)$, 519
— ortogonalnih operatora $\mathcal{O}(U)$, 515
— , periodična, 55
— permutacija skupa, 68, 75
— poliedra, 74
— poligona, 73
— polinoma, 69
— realnih brojeva *mod* 1, 110
— , recipročna, 93
— , reducirana permutacija, 82
— romba, 73
— rotacija (specijalna ortogonlna) $SO(3)$, 204
— — kvadrata, 72
— — pravilnog n-terokuta, 72
— — tetraedra, 74
— — trokuta, 72
— , simetrična, stupnja n, 76
— , slobodna Abelova generirana skupom, 649
— , specijalna linearna $SL(n, F)$, 383
— , — ortogonalna $SO(n)$, 524
— , — — $SO(n, F)$, 384
— , — unitarna $SU(n)$, 524
— torusa, 114
— translacija $T(3)$, 205
— — prostora, 510
— — s centralnom simetrijom, 510
— , unimodularna $UM(n, F)$, 383
— , unitarna $U(n)$, 352
— unitarnih operatora $\mathcal{U}(U)$, 515
grupoid, 39
— , asocijativni (polugrupa), 43
— , komutativni (Abelov), 42

H

Hamelova (algebarska) baza, 260
helikoid, 233
hermitska (hermitski simetrična) matrica, 338
— forma, 604
— — , indefinitna, 607
— — , negativno definitna (strogo negativna), 607
— — , — semidefinitna (negativna), 607

— —, pozitivno definitna (strogo pozitivna), 607
— —, — semidefinitna (pozitivna), 607
— —, semidefinitna, 607
— ortonormiranost redaka (stupaca) matrice, 352
hermitske forme, kongruentne, 604
— —, unitarno kongruentne, 604
— komponente operatora, 549
hermitski funkcional generiran hermitskim bilinearnim funkcionalom, 603
— konjugirana (adjungirana) matrica, 335
— kvadratni funkcional, 603, 610
— operator, 530
hermitsko množenje, 466
hibridno (vanjsko) množenje, 247
hiperbolični konus, 627
hiperboloid, dvoplohi, 235
—, jednoplohi, 235
hipercilindar, 625
hiperelipsoid, 626
— imaginarni, 626
hiperhiperboloid, 626
hiperkonus, 625
hiperkubika, 629
hiperkvadrika, 625, 629
hiperparaboloid, 629
hiperploha drugog reda (hiperkvadrika), 625
— — —, degenerirana, 625
— — —, nedegenerirana, 625
— n-tog reda, 629
— trećeg reda (hiperkubika), 629
hiperravnina, 623
—, tangencijalna, 627
—, polarna, 629
$Hom(U, V)$, 310
$HomV$, 315
homeomorfizam, 637
homeomorfni prostori, 637
homogeni sustav, 447
homomorfizam algebri, 319
— grupa, 85
—, inducirani, 111, 132
— linearnih prostora, 289
— parova, 111, 132
— prostora V^3, 193
— prstenova, 130
—, trivijalni (nulhomomorfizam), 86
homomorfizmi grupa, konjugirani, 644
homotetija (dilatacija), 251
— u linearnom prostoru, 292

I

ideal, 127
—, desni, 127
— generiran skupom, 130
—, glavni, 130
—, lijevi, 127
—, maksimalni, 142
—, obostrani, 127
—, pravi, 128
—, trivijalni, 128
ideali, svakog čovjeka!, 128
idempotentna matrica, 352
idempotentni element, 41
— operator, 319
identična relacija, 34
identični (jedinični) operator na V^3, 195
identično preslikavanje (identiteta) 46
identitet, Jacobijev, 183
—, Lagrangeov (za brojeve), 187
—, — (za vektore u V^3), 184
identiteta, 12, 653
implikacija, 2
indefinitni operator, 534
indeks operatora, 412
— podgrupe (u grupi), 105
inducirani homomorfizam, 111, 132
injekcija, 16
inkluzija, 7, 12, 25, 292, 645
—, dijagonalna, 26, 580
integralna domena, 126
— —, komutativna, 126
invarijante linearnog operatora, 398
— sličnosti, 398

invarijantna podgrupa, 102
invarijantni potprostor, 412
— — u V^3, 203
invertibilna (regularna) matrica, 347
inverz u grupi, 49
— , desni, 49
— , desni morfizma (prerez), 639
— , lijevi, 49
— , lijevi morfizma (retrakcija), 639
— , obostrani, 49
inverzija u permutaciji, 77
inverzna matrica (inverz), 347
— relacija, 34
inverzno preslikavanje, 17
involutorna matrica, 351
involutorni element u grupi, 56
— operator, 530
ireducibilni polinom, 410
ishodište Kartezijevog koordinatnog n-edra, 631
— koordinatnog sustava u E^3, 208
izjava, 1
— , negacija, 4
— , složena, 1
izjavna funkcija, 3
izometrički operator, 508, 510
— — (izometrija) u V^3, 200
izometrija, 510
— ravnine, 69
izomorfizam algebri, 319
— grupa, 86, 90
— kategorija, 649
— linearnih prostora, 299
— , prirodni (kanonski), 324
— prostora V^3 (regularni operator), 193
— prostora i biduala, 324
— prstenova, 131
— pseudounitarnih prostora, 615
— unitarnih prostora, 509
— vektorskih prostora V^3 i $\mathbb{R}^3$, 169
izomorfne grupe, 92
— kategorije, 649
izomorfni linearni prostori, 300
— prstenovi, 131
izotropni potprostor, 617
— prostor (prostor degenracije, nulprostor) za funkcional, 613
— vektor, 617

J

Jacobijev identitet, 183
— kriterij, 599
— — , za hermitske forme, 608
jedinična matrica, 334
jedinični (identični) operator na V^3, 195
— (normirani) vektor u unitarnom prostoru, 476
— operator (identiteta), 292
— vektor (ort) u V^3, 160
— — u smjeru vektora, 160
jedinica, 45
— , desna, 45
— grupe, 53
— , lijeva, 45
— , obostrana (neutralni element, jedinica), 45
— prstena, 120
jednadžba hiperkvadrike, 625
— — , normalna, 626
— hiperravnine, 623
— krivulje u E^3, opći oblik, 239
— — — — , parametarske jednadžbe, 238
— — — — , vektorska, 238
plohe u E^3, eksplicitni oblik, 232
— — — — , implicitni oblik, 232
— — 2. reda, kanonski oblik, 234
— — — — , parametarske jednadžbe, 232
— — — — , vektorska, 231
— pravca u afinom prostoru, kanonske jednadžbe, 632
— — u E^3, kanonske (normalne) jednadžbe pravca kroz dvije

točke, 222
— — — — ,kanonski (normalni) oblik, 221
— — — — , opći oblik, 222
— — — — , parametarske jednadžbe pravca, 220
— — — — , — — pravca kroz dvije točke, 222
— — — — , — — pravca u vektorskom obliku, 220
— — — — , reducirane jednadžbe, 223
— — — — , vektorska kroz dvije točke, 221
— — — — , vektorski oblik normalne jednadžbe pravca, 221
— — — — , vektorski opći oblik, 222
jednadžbe ravnine u E^3 kroz tri točke, 214
— — — — , normalni (Hesseov) oblik, 208
— — — — , određene fiksnom točkom i dva nekolinearna vektora, 214
— — — — , opći oblik, 215
— — — — , parametarske jednadžbe, 213
— — — — , segmentni oblik, 216
— — — — , vektorski parametarski oblik, 213
jednadžbe transformacije koordinata, 388
jednostavna (prosta) grupa, 100
jezgra homomorfizma grupa, 88
— — prstenova, 131
— linearnog operatora, 304
Jordanov blok, 429
— prsten, 124
Jordanova forma (Jordanov normalni oblik) matrice, 429
— matrica, 429

K

k-kvadrika, 628
k-ravnina, 624
— , tangencijalna, 627
— u afinom prostoru, 631
kanonska baza, 261
— matrica ranga r, 359
kanonski (dijagonalni) oblik kvadratne forme, 586
— (prirodni) izomorfizam prostora i biduala, 324
— oblik bilinearne forme, 590, 591
— — hermitske bilinearne forme, 609
— — — forme, 606
— prikaz kvadratnog funkcionala, 586
karakteristična (svojstvena) jednadžba matrice, 399
— — matrica matrice, 399
— — vrijednost matrice, 424
— funkcija, 18
karakteristični (svojstveni) polinom matrice, 399
— — — operatora, 400
karakteristično svojstvo skupa, 7
karakteristika prstena, 135
kardinalni broj skupa, 20, 35
Kartezijev (pravokutni) koordinatni sustav u E^3, 208
— — — — — — , desni, 208
— — — — — — , lijevi, 208
— koordinatni n-edar u afinom prostoru, 631
— — — — — — , ortogonalan, 632
— kvadrat skupa, 22
— rastav (dekompozicija, forma, reprezentacija) operatora, 549
— produkt familije skupova, 27
— — preslikavanja, 25
— — skupova, 22
Kartezijeva potencija skupa, 27
kategorija, 633
— Abelovih grupa, 638, 641
— , diskretna, 635

— , dualna (suprotna), 640
— grupa, 636
— , homotopska, 642, 644
— , konačna, 643
— linearnih prostora, 636
— , mala, 635
— , matrica, 643
— , monotona, 643
— morfizama, 639
— parova, 641
— , prazna, 636
— , punktirana, 641
— , simplicijalna, 643
— skeletna, 661
— skupova, 636
— , topološka, 636
— , trivijalna, 635
kategorije, ekvivalentne, 659
klasa ekvivalencije, 29
— objekata u kategoriji, 633
— svih skupova, 35
klase ostataka mod m, 108
Kleinova četvorna grupa, 73
kodimenzija potprostora u prostoru, 285
kodomena, 11
— morfizma u kategoriji, 634
koeficijent dilatacije u V^3, 199
— kontrakcije u V^3, 199
koeficijenti u linearnoj jednadžbi, 435
kofaktor (algebarski komplement), 376
kolinearni vektori, 161
komplanarni vektori, 162
kompleksna grupa, 68
kompleksne bilinearne forme, ekvivalentne, 611
— — — , kongruentne, 611
kompleksni bilinearni funkcional, 601
— — — , regularan, 611
— — — , singularan, 611
komplement skupa, 9
— — , ortogonalni, 498
komponenta prirodne tranformacije, 653
komponente vektora u V^3, 167
komponiranje morfizama, 634
kompozicija preslikavanja, 14
— relacija, 34
kompozit funktora, 648
— morfizama, 634
— prirodnih transformacija, 655
komutativna (Abelova) grupa, 52
— integralna domena, 126
— polugrupa, 44
komutativni (Abelov) grupoid, 42
— monoid, 47
— prsten, 120
komutator para, 64
komutatorska podgrupa, 64
komutatorsko (Liejevo) množenje, 124, 319
konačni skup, 20
konačna grupa, 52
konačnodimenzionalni linearni prostor, 262, 263
kongruencija para bilinearnih (kvadratnih) formi, 613
— parova kvadratnih formi, 600
kongruentni operator (izometrički operator, izometrija), 510
konjugirana matrica, 335
— — , hermitski (adjungirana), 335
konjugiranje kompleksnih brojeva, 296
— matrica, 339
— (sprezanje) para matrica, 353
konjunkcija, 1
konstanta, 12
kontrakcija u V^3, 199
konus 2. reda, 236
koordinate, afine, 632
— , geografske na sferi, 243
— , ortogonalne u euklidskom prostoru, 632
— , polarne u ravnini, 244
— pravca u E^3, 223
— , pravokutne radijvektora, 208
— točke u E^3, afine, 211
— — — — , cilindrične, 241
— — — —, Kartezijeve (pravokutne), 209
— — — — , polarne, 243
— — — — , sferne, 242
— vektora, 385

— — u V^3, 167
— — — — , ortogonalne (pravokutne), 174
koordinatizacija prostora E^3, 209
— — , linearnog, 386
— — V^3, 167
koordinatna baza (koordinatni sustav) linearnog prostora, 385
— funkcija, 295
— matrica vektora, 386
— ploha, 244
— točka Kartezijevog koordinatnog n-edra, 631
— trojka (koordinatni slog) vektora u V^3, 167
koordinatne ravnine u E^3, 208
koordinatni prostor, n-dimenzionalni nad poljem F, 252
— — , realni n-dimenzionalni, 251
— slog vektora, 385
— sustav (baza) za V^3, 166
— — , ortonormirani u unitarnom prostoru, 487
— — Kartezijev (pravokutni) u E^3, 208
— — , afini u E^3, 211
— — , cilindrični u E^3, 241
— — , sferni u E^3,242
— — u ravnini, polarni, 244
— vektori u E^3, 208
korijen jedinice n-tog stupnja , primitivni, 67
— operatora, kvadratni (drugi), 535
— — , n-ti, 538
— — , n-ti, normalni, 548
korijeni jedinice, 67
korolar, 4
kosinusi smjera vektora u V^3, 176
kota (aplikata) točke u E^3, 209
kraj orijentirane dužine, 146
kratki egzaktni niz, 309
kratnost svojstvene vrijendosti, algebarska, 424
— — — , geometrijska, 418
kriterij za prepoznanvanje potprostora, 269
krivulja drugog reda (konika), 244
— u E^3, 238
Kroneckerov simbol, 322
kubna parabola, 240
kugla u metričkom prostoru, 482
kut dvaju pravaca u E^3, 223
— dviju ravnina u E^3, 218
— između vektora u unitarnom prostoru, 477
— — — u V^3, 169
— nutacije, 390
— pravca i ravnine u E^3, 224
— precesije, 390
— vlastite rotacije, 390
kvadratna forma, 583
— — , dijagonalna, 586
— — , indefinitna, 596
— — , negativno definitna (strogo negativna), 59
— — , negativno semidefinitna (negativna), 597
— — , pozitivno definitna (strogo pozitivna), 596
— — , pozitivno semidefinitna (pozitivna), 596
— — , regularna (nedegenerirana), 584, 596
— — , semidefinitna, 596
— — , singularna (degenerirana), 596
— matrica, 333
kvadratne forme, kongruentne, 585
— — , ortogonalno kongruentne, 585
kvadratni funkcional, 580, 581
— — , indefinitan, 598
— — , negativno definitan (strogo negativan), 598
— — , negativno semidefinitan (negativan), 598
— — , pozitivno definitan (strogo pozitivan), 598
— — , pozitivno semidefinitan (pozitivan), 598
kvadrika (ploha 2. reda), 234

kvantifikator, egzistencijalni, 3
— , univerzalni, 3
kvaternion, 68, 139
kvaternionska grupa, 68
kvazidijagonalna matrica, 415
kvazigrupa (monoid), 47
kvocijentna (faktorska) grupa, 107
kvocijentni operator, 293
— prostor, 283
— prsten, 129
— skup, 30, 107
— — (grupe po podgrupi), desni, 104
— — — — — , lijevi, 104
kvocijentno preslikavanje, 31

L
Lagrangeov algoritam, 586
— — za hermitske forme, 606
— identitet za brojeve, 187
— — za vektore u V^3, 184
Laplaceov razvoj determinante, 376
Legendreovi polinomi, 497
leksikografski uređaj, 37
lema, 4
Liejev prsten, 124
Liejeva algebra, 183, 319
Liejevo (komutatorsko) množenje, 124
lijeva jedinica, 45
— susjedna klasa podgrupe, 104
— translacija u grupi, 70
lijevi anihilator prstena, 134
— ideal, 127
— inverz morfizma (retrakcija), 639
— — u grupi, 49
— koordinatni sustav u E^3, 208
— kvocijentni skup (grupe po podgrupi), 104
lijevo orijentirana (lijeva) baza za V^3, 166
linearna algebra, 316
— forma, 328
— jednadžba, 435
— kombinacija (linearni spoj) vektora, 255
— ljuska (linearni omotač) skupa, 270
— matrična jednadžba, 462
— mnogostrukost, 282
linearni funkcional, 320
— — na unitarnom prostoru, 564
— — na V^3, 205
— operator, 289
— — na V^3, 193
— (vektorski) prostor, 159, 248
— — — , kompleksni, 248
— — — , realni, 248
— — — , n-dimenzionalan, 266
— — — , beskonačnodimenzionalan, 262
— — — , konačnodimenzionalan 262, 263
linearno nezavisan skup, beskonačan, 255
— — — , konačan, 255
— preslikavanje (linearna transformacija), 289
— zavisan skup, beskonačan, 255
— — — , konačan, 255
logaritanski zakon, 287

M
maksimalni ideal, 142
matrica, antihermitska (hermitski antisimetrična), 338
— antisimetrična, 338
— bilinearnog funkcionala, 574
— , dijagonalna, 345
— , donja trokutasta, 346
— , elementarna, 362
— forme, 584, 590
— , gornja trokutasta, 346
— , Gramova, 484
— — , s obzirom na funkcional, 613
— , hermitska (hermitski simetrična), 338
— , hermitski konjugirana (adjungirana), 335
— hiperkvadrike, 625
— , idempotentna, 352

— , inverzna (inverz), 347
— , involutorna, 351
— , jedinična 334
— , kanonska, ranga r, 359
— , karakteristična (svojstvena) 399
— , kompleksna, 335
— kompleksnog bilinearnog funkcionala, 603
— , konjugirana, 335
— , koordinatna, vektora, 386
— , kvadratna, 333
— kvadratnog funkcionala, 583
— , kvazidijagonalna, 415
— (matrični zapis) operatora na V^3, 195
— (matrični zapis) linearnog operatora, 331, 391
— , negativna, 539
— , nilpotentna, 538
— , normalna, 346, 540
— , ortogonalna, 348, 517
— , polinomska, 404
— , pozitivna, 539
— , prijelaza (transformacije), 387
— , proširena, sustava, 436
— , realna, 335
— , regularna (invertibilna), 347
— , redčana (matrica redak), 333
— , simetrična, 338
— , simplektička, 620
— , singularna, 347
— , skalarna, 346
— skupa vektora, 386
— , strogo negativna, 539
— , strogo pozitivna, 539
— , stupčana (matrica stupac), 333
— sustava, 436
— tipa (m, n) nad poljem F, 332
— transformacije varijabli, 584
— , transponirana, 334
— trećeg reda, ortogonalna, 201
— — — , simetrična, 198
— , unitarna, 352, 515
matrice, ekvivalentne, 358
— , hermitski kongruentne, 353
— , kongruentne, 353, 575
— , ortogonalno kongruentne, 353, 523, 585
— , ortogonalno slične, 353, 523
— , slične, 353, 398
— , ulančane, 340
— , unitarno kongruentne, 353, 523
— , unitarno slične, 353, 523
matrična jednadžba, 437
matrični polinom, 401
metrički prostor, 480
metrika (metrička funkcija, funkcija udaljenosti), 480
— , diskretna, 481
— , indefinitna, 616
minimalna jednadžba matrice, 405
minimalni polinom matrice, 405
— — operatora, 407
minora (subdeterminanta) matrice, 377
— reda k, 382
mješoviti produkt, 187
množenje, hibridno (vanjsko), 247
— , komutatorsko (Liejevo), 124, 319
— matrica, 340
— mnogostrukosti skalarima, 283
— mod m, 48
— , pseudoskalarno, 614
— , simetrizirano, 124
— , skalarno u unitarnom prostoru, 468
— vektora u V^3, mješovito (vektorskoskalarno), 187
— — — — realnim brojem, 156
— — — — , skalarno, 169
— — — — , vektorsko, 177
množina, 5
modul (duljina) vektora u V^3, 151
— — — , u unitarnom prostoru, 474
modul, 249
— , F-modul, 249

— , $\mathbb{Z}$ -modul, 253
mono, 639
monoid (kvazigrupa), 47
— aditivni cijelih brojeva mod m, 48
— , komutativni, 47
— , multiplikativni cijelih brojeva mod m, 48
monomorfizam, 86
morfizam, bimorfizam, 639
— , ekvivalencija (izomorfizam), 636
— , epi, 639
— , idempotentni, 640
— , inverzni (inverz), 636
— , jedinični (identički, identiteta), 635
— , mono, 639
— , nulmorfizam, 640
— , regularan, 640
— u kategoriji, 634
multiplikativna grupa, 53
— — tijela, 138
— polugrupa prstena, 119

N

n-arna relacija, 37
nadskup, 7
najkraća udaljenost dvaju pravaca, 228
namatanje pravca na kružnicu, 90
negacija izjave, 4
negativni operator, 534
nehomogeni sustav, 449
nejednakost, Besselova, 491
— , Cauchyjeva, 474
— , Minkowskog, 478
— mnogokuta, 481
— Schwarz – Cauchy – Bunjakovskog, 472
— — — — u V^3, 176
— , Schwarzova, 474
— trokuta u V^3, 176
neparna permutacija, 77
nepoznanice u sustavu linearnih jednadžbi, 435
— — — — — , glavne, 460
— — — — — , slobodne, 460
neprebrojivo beskonačan skup, 20
neutralni element (jedinica), 45
nilpotentni element u prstenu, 126
— operator, 412, 547
niz, 12
— , egzaktni, 309
— , kratki egzaktni, 309
norma (duljina, modul) vektora u unitarnom prostoru, 474, 476
— inducirana skalarnim produktom, 476
normalizator skupa, 64
normalna baza pseudounitarnog prostora, 615
— forma matrice, 432
— — — normalnog operatora, 545
— — unitarnog (ortogonalnog) operatora, 522
— matrica, 346, 540
— podgrupa, 99
normalni oblik forme, bilinearne, 600
— — — , hermitske, 606
— — — , hermitske bilinearne, 609
— — — , kvadratne, 593
normirani (jedinični) vektor u unitarnom prostoru, 476
— prostor, 476
nula grupe, 53
— prstena, 119
nulhomomorfizam (trivijalni homomorfizam) grupa, 86
nulmatrica, 333
nulmorfizam, 640
nulobjekt, 640
nuloperator, 292
— na V^3, 195
nulprsten (trivijalni prsten), 121
nulvektor, 149, 248

O

objekt, inicijalni (početni), 640
— , nulobjekt, 640
— , terminalni (konačni), 640
— u kategoriji, 633

objekti, istog homotopskog tipa, 644
obostrani inverz u grupi, 49
obrubljivanje matrice, 380
ograničenje (restrikcija) funkcije, 15
okomiti vektori u V^3, 169
oktanti u E^3, 210
oktave (Cayleyjevi brojevi), 68
opća linearna grupa $GL(3)$, 204
— — — $GL(n, F)$, 348
— — — Aut V, 396
operacija, binarna, 39
— , ternarna, 39
— , unarna, 39
operator, 289
— , adjungirani (hermitski konjugirani, hermitski adjungirani), 526
— , adjungirani (samoadjungirani), 530
— , afini, 292
— , antihermitski (hermitski antisimetričan), 530, 622
— , antilinearni, 511
— , antisimetrični, 530, 622
— , antiunitarni, 511, 568
— , bilinearni, 344, 580
— deriviranja, 294
— ,dualni, 327, 569
— , hermitski (hermitski simetričan), 530, 622
— , idempotentni, 319
— , indefinitni, 534
— integriranja, 294
— , involutorni, 530
— , izometrički, 508, 510
— , jedinični, 292
— , kongruentni (izometrički, izometrija), 510
— , kvocijentni, 293
— , desni adjungirani, 621
— , lijevi adjungirani, 621
— , linearni, 289
— , negativni, 534
— , nilpotentni, 412, 547
— , normalni, 539
— , ortogonalni, 505
— , polujednostavni (poluprosti), 425
— , potpuno reducibilan, 413
— , pozitivni (pozitivno semidefinitni), 534
— , reducibilan, 413
— , regularni, 299
— , simetrični, 530, 622
— , singularni, 299
— , strogo negativni, 534
— , strogo pozitivni (pozitivno definitni), 534
— , translacije, 511
— , transponirani, 526
— , unitarni, 505
— u V^3, 193
— — — , dilatacija, 199
— — — , izometrički (izometrija), 200
— — — , jedinični (identični), 195
— — — ,kontrakcija, 199
— — — , linearni, 193
— — — , nuloperator, 195
— — — , (ortogonalnog) projiciranja na pravac, 197
— — — ,(ortogonalnog) projiciranja na ravninu, 197
— — — , centralne simetrije, 196
— — —, homotetije, 196
— — — , rotacije oko pravca, 197
— — — translacije, 198
— — — , zrcaljenja na pravcima, 196
— — — , zrcaljenja na ravninama, 196
— — — , ortogonalni, 200
— — — , regularni (izomorfizam), 193
— — — , simetrični, 198
operatori, ekvimetrični (izometrički jednaki), 550
— , unitarno slični, 523
operatorska jednadžba, 440
ordinata točke u E^3, 209

orijentacija (smisao) vektora, 151, 152
— u E^3, 210
orijentirana dužina, 146
— — u afinom prostoru, 631
orijentirane dužine, ekvivalentne, 146
— — , suprotne, 150
ort (jedinični vektor), 160
ortogonalna baza, 487
— grupa $O(3)$, 204
— — $O(n)$, 517
— — $O(n, F)$, 349
— matrica 348, 517
— — trećeg reda, 201
— projekcija (ortogonalni projektor), 501
— suma potprostora, 498, 503
— transformacija varijabli, 585
ortogonalne (pravokutne) koordinate vektora u V^3, 174
ortogonalni komplement skupa, 498
— operator, 505
— — u V^3, 200
— skup, maksimalni, 488
— — vektora, 487
— skupovi, 497
— vektori u prostoru s hermitskom metrikom, 617
— — u unitarnom prostoru, 486
ortonormirana baza, 487
— — u V^3, 174
ortonormirani koordinatni sustav u unitarnom prostoru, 487
— skup vektora, 487
— sustav redaka matrice, 350
— — u V^3, 201
os aplikata (kota), 208
— apscisa, 208
— ordinata, 208
— sveska ravnina u E^3, 217
osnovna jednadžba sustava, 460
— matrica sustava, 436
osnovni funkcional, 614
— sumand u determinanti, 364
— sustav, 460
osnovno polje, 248, 332
otvoreni skup, 482

P
par adjungiranih operatora, 527
— komplementarnih potprostora, 280
— međusobno ortogonalnih projektora, 557
— ortogonalnih skupova, 497
— skupova, 641
— — vektora u unitarnom prostoru, 486
paraboloid, eliptički, 235
— , hiperbolički, 236
paralelnost hiperravnina, 623
— ravnina, 628
paralelotop, 485
parcijalni (djelomični) uređaj, 32
parnost (paritet) permutacije, 77
Parsevalova jednakost, 491
particija (rastav, dekompozicija) skupa, 36
partitivni skup, 8
periodična grupa, 55
permutacija, ciklička (ciklus), 80
— , neparna, 77
— , parna, 77
— skupa, 75
ploha, koordinatna, 244
— u E^3, 231
— — — , algebarska, 234
— — — , — , reda n, 234
— — — , drugog reda (kvadrika), 234
— — — , transcedentna, 234
početak orijetirane dužine, 146
podalgebra, 318
poddomena, 127
podgrupa, 60
— , centralna normalna, 102
— , ciklička, 63
— generirana skupom, 62
— , invarijantna, 102
— , komutatorska, 64
— konačnog indeksa, 105
— , normalna, 99
— , prava, 60
— , prosta (jednostavna), 100
— , trivijalna, 60

podgrupoid, 60
podmatrica (submatrica) matrice, 362
područje definicije preslikavanja, 11
— vrijednosti preslikavanja, 11
podskup, 7
— , pravi, 8
podtijelo, 140
pojam, definirani, 4
— , osnovni, 4
pol, 240, 243, 244, 629
polarna forma hermitske kvadratne forme, 612
— — kvadratne forme, 591
— hiperravnina, 629
— jednadžba konike, 245
— os, 240, 243, 244
— poluravnina, 240
polarni rastav (faktorizacija, dekompozicija, forma, prikaz) operatora, 553
polinom, ireducibilan, 410
— , karakteristični (svojstveni) matrice, 399
— , — — operatora, 400
— , matrični, 401
— , minimalni matrice, 405
— , — operatora, 407
— , reducibilan, 410
— s matričnim koeficijentima, 404
polinomi, Legendreovi, 497
— , Čebiševljevi, 497
polinomska matrica, 404
polugrupa, 43
— , komutativna, 44
— , multiplikativna prstena, 119
polujednostavni (poluprosti) operator, 425
polje, 138
— , algebarski zatvoreno, 419
— , osnovno, 248, 332
potencija skupa, 35
potkategorija, 637
— , puna, 637
potpolje, 140
potpolugrupa, 60
potprostor, 268
— , desno izotropni, 619
— , f-invarijantan, 412
— , invarijantan, 412
— , izotropni, 617
— , lijevo izotropni, 619
— , svojstveni, operatora, 418
— , trivijalni, 268
— prostora V^3, 195
— — — , dvodimenzionalni (ravnina), 195
— — — , invarijantni, 203
— — — , jednodimenzionalni (pravac), 195
potprsten, 126
— generiran skupom, 127
potpuno reducibilan operator, 413
pozitivni (pozitivno semidefinitni) operator, 534
praslika elemenata, 11
— podskupa, 12
pravčasta ploha, 238
pravac u afinom prostoru, 632
— u E^3, 239
— u linearnom prostoru, 624
— u V^3, 195
pravi ideal, 128
pravilo, Sarrusovo, 365
— desnog vijka, 177
— paralelograma, 155
— trokuta, 154
pravokutne (ortogonalne) koordinate radijvektora, 208
— — — vektora u V^3, 174
prazan skup, 7
prebrojivo beskonačan skup, 20
predstavnik (reprezentant) vektora, 148
prerez (desni inverz morfizma), 639
presjek familije potprostora, 273
— potprostora, 273
— skupova, 8
preslikavanje, 11
— , afino, 70
— , bijektivno, 16
— , homotopno, 644
— , injektivno, 16
— , inverzno, 17

— , kvocijentno, 31
— parova, 641
— , surjektivno, 16
primideal, 130
primitivni korijen jedinice n-tog stupnja, 67
prirodna ekvivalencija, 656
— injekcija (faktora u direktni produkt grupa), 115
— projekcija, 109
— — direktnog produkta grupe na faktore, 114
— transformacija, 652
— — , inverzna (inverz), 656
prirodni uređaj (na $\mathbb{R}$), 33
problem svojstvenih vrijednosti operatora, 417
produkt kategorija, 638
— linearnih operatora, 315
— matrica, 340
— matrice sa skalarom, 336
— realnog broja i vektora, 156
— skalara i operatora, 311
projekcija, 25, 645
— direktnog produkta prostora na faktore, 296
— , ortogonalna, 501
— , prirodna, prostora na kvocijentni prostor, 293
— prostora na potprostor (projektor), 293
— , skalarna u V^3, 173
projektor na i-tu koordinatu, 295
— , ortogonalni, 501
propozicija, 4
prostor, afini (nad poljem F), 630
— , degenerirani, 617
— , euklidski, 470
— funkcija (funkcijski prostor), 253
— , izotropni za funkcional, 613
— , linearni (vektorski), 148, 159, 248, 261, 263, 266
— , Lorentzov kompleksni, 616
— , metrički, 480
— M_{mn}, 336
— , nedegenerirani, 617
— , normirani, 476
— polinoma, 252
— , pseudoeuklidski, 616
— , pseudounitarni, 614
— , refleksivni, 325
— rješenja sustava, 448
— s hermitskom (bilinearnom) metrikom, 617
— , simplektički, 620
— , standardni kompleksni $\mathbb{C}^n$, 470
— , topološki, 482
— , trivijalni, 253
— radijvektora, 150
— vektora (vektorski prostor), 148
prostori, dualni, 330
— , homeomorfni, 637
proširena matrica sustava, 436
proširenje funkcije, 15
prsten, 119
— cijelih brojeva, 120
— — — mod m, 120
— endomorfizama grupe, 120
— , glavnih ideala, 130
— , Jordanov, 124
— , komutativni, 120
— , kvocijentni, 129
— , Liejev, 124
— polinoma, 121
— realnih funkcija, 121
— , reducirani, 129
— s jedinicom, 120
— , trivijalni (nulprsten), 121
pseudoeuklidski prostor, 616
pseudometrika, 481
pseudoskalarno množenje, 614
pseudounitarni prostor, 614

R

radijvektor, 150
— točke afinog prostora, 630
— — u E^3, 242
rang bilinearnog funkcionala, 575
— forme, 584, 590
— hermitske bilinearne forme, 609

— — forme, 604
— hermitskog bilinearnog funkcionala, 612
— — funkcionala, 604
— kvadratnog funkcionala, 583
— linearnog operatora, 305
— matrice, 357, 383
— — po redcima, 355
— — po stupcima, 354
— prostora s hermitskom metrikom, 617
— linearnog sustava, 450
ravnina u E^3, 232
— — linearnom prostoru, 624
— — — — , k-dimenzionalna, 624
razlika skupova, 9
— vektora, 156
realna analiza, 642
— funkcija, 12
recipročna grupa, 93
red elemenata u grupi, 55
— forme, 590
— grupe, 52
— matrice, 333
redak matrice, 333
reducibilni operator, 413
— polinom, 410
reducirana grupa permutacija, 82
reducirani prsten, 129
refleksija (zrcaljenje), 521
refleksivni prostor, 325
regularna (invertibilna) matrica, 347
regularni operator, 299
— — (izomorfizam) na V^3, 193
relacija, 28
— , antisimetrična, 29
— , binarna, 37
— ekvivalencije, 29
— , identična, 34
— , inverzna, 34
— klasifikacije, 29
— kongruencije mod m, 110
— n-arna, 37
— na uređenom paru skupova, 34
— paralelograma, 477
— , refleksivna, 29
— , simetrična, 29
— , tranzitivna, 29
— , ternarna, 37
— trokuta u E^3, 210
— uređaja, 32
— — , parcijalnog (djelomičnog), 32
— — , totalnog (potpunog, linearnog), 32
reprezentacija matrice, redčana, 355
— — , stupčana, 354
reprezentant (predstavnik) vektora, 148
restrikcija funkcije, 15
redčana matrica (matrica redak), 333
retrakcija (lijevi inverz morfizma), 639, 662
— , deformacijska, 662
retrakt, deformacijski, 662
rješenje linearne matrične jednadžbe, 462
— sustava linearnih jednadžbi, 436
— — — — , fundamentalno, homogenog, 449
— — — — , netrivijalno, 447
— — — — , opće, homogenog, 449
— — — — , opće, nehomogenog, 452
— — — — , partikularno, 450
— — — — , trivijalno, 447
rotacija, 294, 506, 521
— koordinatnog sustava u E^3, 389

S

Sarrusovo pravilo, 365
Schwarzova nejednakost, 474
sekularna jednadžba, 539
seskvilinearni funkcional, 601
sfera u E^3, 232
signatura hermitske bilinearne forme, 609
— — forme, 607

— hermitskog bilinearnog funkcionala, 612
— kvadratne forme, 596
— pseudounitarnog prostora, 614
simetrična grupa stupnja n, 76
— matrica, 338
— razlika (diferencija) skupova, 40
simetrični operator, 530
simetrizirano množenje, 124
simplektička baza prostora, 620
— matrica, 620
simplektički operator (izometrija), 621
— prostor, 620
singularna matrica, 347
sigularni operator, 299
skalar, 145, 248
skalarna matrica, 346
— projekcija u V^3, 173
skalarni kvadrat vektora u V^3, 170
— produkt, dualni, 567
— — vektora u V^3, 170
— — — u linearnom prostoru, 468
skalarno množenje u V^3, 170
— — u linearnom prostoru, 468
skelet kategorije, 661
skup, 5
— , beskonačan, 20
— , desni kvocijentni, 104
— , dobro uređeni, 33
— , funkcijski, 17
— generatora (izvodnica) grupe, 62
— — linearnog prostora, 260
— izvodnica linearnog prostora, 260
— , karakteristično svojstvo, 7
— , komplement skupa, 9
— , konačan, 20
— , konveksan, 537
— , kvocijentni, 30, 107
— , lijevi kvocijentni, 104
— , nadskup, 7
— , neprebrojiv, 20
— , ortogonalni, vektora, 487
— , ortonormirani, vektora, 487
— , otvoren, 482
— , parcijalno uređen, 32
— , partitivni, 8
— , podskup, 7
— , prazan, 7
— , prebrojiv, 20
— , presjek skupova, 8
— , punktirani, 641
— , razlika skupova, 9
— realnih brojeva modulo 1, 35
— smjerova u E^3, 152
— , totalno uređen, 32
— , unija skupova, 8
— , zatvoren, 59
skupovi, disjunktni, 9
— , ekvipotentni, 19
— , jednaki, 7
— , ortogonalni, 497
slične matrice, 353
sličnost matrica, ortogonalna, 523
— — , unitarna, 523
slika, 11
— domene, 12
— podskupa, 12
— homomorfizma grupa, 88
— — prstenova, 131
— linearnog operatora, 304
slobodni član, 435
složena izjava, 1
smisao (orijentacija) vektora, 151, 152
smjer pravca u E^3, 152
— u E^3, 152
— u ravnini, 31
— vektora, 151
snop pravaca u E^3, 223
specijalna linearna grupa $SL(n, F)$, 383
— ortogonalna grupa $SO(n)$, 524
— — — $SO(n, F)$, 384
— — — (grupa rotacija) $SO(3)$, 204
— unitarna grupa $SU(n)$, 524
specijalni ortogonalni operator (rotacija), 521
spektar operatora, 418

spektralni rastav (dekompozicija, forma, reprezentacija, prikaz) operatora, 558
sporedna dijagonala matrice, 334
sprezanje (konjugiranje) para matrica, 353
standardna kompozicija,41
standardni n-dimenzionalni prostor nad poljem F, 252
— model linearnog prostora, 303
— skalarni produkt na $\mathbb{R}^n$, 470
standardno množenje, 40
— zbrajanje, 40
strogo negativan (negativno definitni) operator, 534
— pozitivan (pozitivno definitni) operator, 534
stupčana matrica (matrica stupac), 333
stupac matrice, 333
subdeterminanta (minora) matrice, 377
submatrica (podmatrica) matrice, 362
— , osnovna, 459
suma familije potprostora, 275
— potprostora, 274
— — , direktna, 277
— — , ortogonalna, 498
suprotni uređaj, 36
— vektor, 149
suprotno orijentirane dužine, 150
surjekcija, 16
susjedna klasa podgrupe, desna, 104
— — — , lijeva, 104
sustav linearnih jednadžbi, 435
— — — , Cramerov, 444
— — — , 447
— — — , nehomogen, 449
— — — , nerješiv (nemoguć, inkompatibilan), 437
— — — , rješiv (moguć, kompatibilan), 437
— , ortonormirani redaka matrice, 350
svezak (pramen) ravnina u E^3, 217
svežanj (snop) ravnina u E^3, 217
svojstvena (karakteristična) jednadžba matrice, 399
— matrica, 399
— (karakteristična) vrijednost matrice, 424
— — — operatora, 417
— — — — na V^3, 203
svojstveni (karakteristični) polinom matrice, 399
— — — operatora, 400
— potprostor operatora, 418
— — — na V^3, 203
— vektor operatora, 417
— — — na V^3, 203
Sylvesterov zakon defekta, 310
— — inercije, 593

T

tablica, Cayleyjeva, 41
— istinitosti, 5
— množenja, 41
tangencijalna hiperravnina, 627
— k-ravnina, 627
tautologija, 5
temeljni Jordanov blok (Jordanova klijetka), 429
teorem, 4
— , Autonneov, 552
— , Binet-Cauchyjev, 370
— , Cayleyjev, 98
— , Euler-Fermatov, 64
— , Eulerov, 204
— , Gram-Schmidtov, 493
— , Hamilton-Cayleyjev, 401
— , Jacobijev kriterij, 599
— , Kraljevićev, 613
— , Kronecker-Capellijev, 442
— , Lagrangeov, 105
— , Milnorov, 601
— o dimenziji, 276
— o izomorfizmu grupa, 112
— o izomorfizmu prstenova, 133
— o rangu i defektu, 305
— , Pitagorin, 491
— , Roucheov, 448
— , spektralni, 533, 545
— , Steinitzov, 264

— , Sylvesterov zakon inercije, 593
— , zakon inercije za hermitske forme, 606
ternarna operacija, 39
— relacija, 37
tijelo, 138
— kvaterniona, 139
točka afinog prostora, 630
— , bazna, 641
Toeplitzov prikaz matrice, 539
topologija, 482
topološki prostor, 482
torus, 23, 232
totalni (potpuni, linearni) uređaj, 32
trag matrice, 334
— operatora, 400
translacija, 295, 510
— , desna (u grupi), 71
— , lijeva (u grupi), 70
transponirana matrica, 334
transponirani funkcional, 579
— operator, 526
transponiranje, 339
trivijalni homomorfizam (nulhomomorfizam) grupa, 86
— ideal, 128
— prsten (nulprsten), 121

U

udaljenost točaka u euklidskiom prostoru, 632
— točke od pravca u E^3, 225
— — od ravnine u E^3, 211
— dvaju vektora u normiranom prostoru, 479
ulančane matrice, 340
unarna operacija, 39
unija skupova, 8
unimodularna grupa $UM(n, F)$, 383
unitarna grupa $U(n)$, 352, 517
— matrica, 352, 515
unitarni opertor, 505
— prostor, 468
— — , dualni, 568
— — V^3, 173
unitarno izomorfni unitarni prostori, 509
unutrašnji automorfizam grupe, 93
uređaj , leksikografski, 37
— , parcijalni (djelomični), 32
— , prirodni na $\mathbb{R}$, 33
— , suprotni, 36
— , totalni (potpuni, linearni), 32
uvjet, dovoljan, 2
— , nuždan, 2
— , prirodnosti, 652

V

valuacija, 320
Vandermondeova determinanta, 370
vanjsko (hibridno) množenje, 247
vektor, 145, 248
— , desno ortogonalan, 619
— , izotropni, 617
— , lijevo ortogonalan, 619
— na pravcu, 160
— normale ravnine u E^3, 216
— , normirani (jedinični) u unitarnom prostoru, 476
— , suprotan, 149
— u ravnini, 160
vektori, kolinearni, 161
— , komplanarni, 162
— , koordinatni, 166
— , okomiti, 169
— , ortogonalni u unitarnom prostoru, 486
vektorski (linearni) prostor, 159, 248
— produkt, 177
— prostor (prostor vektora) V^3, 148
vektorsko množenje, 177
vektorskoskalarno (mješovito) množenje u V^3, 187
Vivianijev prozor, 239
volumen paralelepipeda u V^3, 191
— paralelotopa, 485
vrh svežnja ravnina u E^3, 217
vrijednost funkcije, 11

Z

zajednička normala dvaju mimosmjernih pravaca, 227
zakon inercije za bilinearne forme, 600
— preslikavanja, 11
zbrajanje mod m, 48
— vektora u E^3, 153
zbroj linearnih operatora, 310
— matrica, 336
zenitna distanca točke u E^3, 242
zrcaljenje, 295, 506, 521

BILJEŠKA O AUTORU

Krešimir Horvatić, rođen je 1930. u Zagrebu, gdje je završio osnovnu i srednju školu. Na Prirodoslovno-matematičkom fakultetu 1954. diplomirao, a 1965. magistrirao matematiku. Godine 1966. – 1968. provodi na studijskom boravku u SAD-u, gdje je na University of Georgia, Athens, doktorirao disertacijom *Embedding Polyhedra in Euclidean Space*. Kao gostujući profesor boravio je školske godine 1976/77. na University of Utah, Salt Lake City. U nekoliko navrata (1973., 1975., 1982.) kraće je vrijeme proveo u Varšavi, kao gost Poljske akademije nauka, i onda 1988. na Ludwig Maximilian Universität u Münchenu. Redovito sudjeluje na periodičkim sastancima *Mathematikertreffen Zagreb-Graz*, kao i tradicionalnom (već 30 godina) *Topološkom seminaru Zagreb-Ljubljana*.

Cijeli radni vijek proveo je na Matematičkom odjelu PMF-a u Zagrebu, od 1954. kao asistent, pa do 2002., kada je umirovljen u znanstveno nastavnom zvanju redovitog profesora i znanstvenog savjetnika. Tijekom godina predavao je cijeli niz kolegija iz geometrije, linearne algebre i raznih topoloških disciplina, kako na dodiplomskoj tako i postdiplomskoj razini. Napisao je trodijelni udžbenik *Linearna algebra*, kojemu je do danas objavljeno osam izdanja.

Posebno je zaslužan za organizaciju studija matematike, redovnog i izvanrednog, na Pedagoškom fakultetu, Sveučilišta u Osijeku. Tamo je godinama i gostovao, predavajući nekoliko matematičkih kolegija. Također, kao predavač sudjelovao je u ostvarenju osebujnog studija filozofije i matematike, na Filozofskom fakultetu, danas Sveučilišta u Zadru.

Područje znanstvenog interesa Krešimira Horvatića je topologija, posebno geometrijska: smještavanje, neuzlanje, ulančenost odnosno neulančenost poliedara. Osim toga, bavio se i vezom raznih topoloških problema i rezultata s čuvenom Poincaréovom hipotezom, što je sažeo u monografiji *Klasični problemi geometrijske topologije* (Tehnička knjiga, Zagreb, 1990.).

Sudjelovao je na brojnim domaćim i međunarodnim skupovima, gdje je održao 33 znanstvena te brojna stručna i popularna predavanja i priopćenja. Uz internacionalne kongrese, posebno treba istaknuti cijenjene *Zimske škole geometrijske topologije* u IUC-u, Dubrovnik (1976., 1981., 1986.), kao i *The Topology Semester* u IBC, Varšava (1986.). Objavio je 18 znanstvenih i mnogo stručnih radova u renomiranim stranim i domaćim časopisima. Recenzent je referativnog časopisa *Mathematical Review.*

Član je Hrvatskog matematičkog društva i American Mathematical Society.

Krešimir Horvatić
LINEARNA ALGEBRA

Nakladnik
Golden marketing – Tehnička knjiga
Zagreb, Jurišićeva 10
tel.: 01/4810-819, 4810-820
faks: 01/4810-821
e-mail: golden-marketing©zg.htnet.hr
www.golden-marketing.hr

Izvršni urednik
Željko Prodanović, ing. grafike

Lektorica
Alka Zdjelar-Paunović, prof.

Korektori
dr. sc. Aleksandra Čižmešija
dr. sc. Siniša Žampera

Likovno oblikovanje naslovnice
Studio Golden, Zagreb
Željko Prodanović, ing. grafike

Računalna priprema
LPC – Zagreb
Nevenka Trumbetaš-Bakić, dipl. ing. mat.

Slike u računalnoj grafici
Element, Zagreb
Sandra Gračan, dipl. ing. mat.

Tisak:
Profil International, d.o.o.

CIP – Katalogizacija u publikaciji
Nacionalna i sveučilišna knjižnica – Zagreb

UDK 512.64(075.8)

HORVATIĆ, Krešimir
Linearna algebra / Krešimir Horvatić. – 1. (9.) izd. – Zagreb
Golden marketing – Tehnička knjiga, 2004. –
(Udžbenici Sveučilišta u Zagrebu = Manualia Universitatis Studiorum Zagrabiensis)

Bibliografija. Kazala.

ISBN 953-212-182-X

I. Linearna algebra – udžbenik

440219034