LINEARNA ALGEBRA 1
skripta za nastavničke studije na PMF-MO

Zrinka Franušić, Juraj Šiftar

Predgovor

Ova skripta nastajala su bez prevelike žurbe, a prije petnaestak godina činilo se da za njih ni nema osobite potrebe. Nastava predmeta Linearna algebra, neovisno o varijantama za različite smjerove studija, o modifikacijama nastavnog programa i načinu podjele svojedobno dvosemestralnog kolegija na dva jednosemestralna, smatrala se "oduvijek", to jest preko 40 godina, temeljito pokrivenom opsežnim materijalom koji je napisao prof. Krešo Horvatić. Ni dodatne literature, na hrvatskom ili na stranim jezicima, nije u tom razdoblju nedostajalo, no nastavnici, asistenti i studenti tradicionalno su se većinom pouzdavali u "Horvatićevu Linearnu" ili, još kraće, u "Horvatića". Barem za "teoriju", dakako, a brojne, lako dostupne zbirke zadataka i naročito one popularne neslužbene arhive zadataka sa "starih rokova" upotpunjavale su studentski fond tekstova za pripremu ispita. Dakako, pojedini nastavnici služili su se i drugim izvorima, a pisali su i vlastita skripta, bolje prilagođena polaznicima drugih studija, obično onih nematematičkih.

Značajan pomak načinio je prof. Damir Bakić, napisavši na temelju dugogodišnjeg nastavnog iskustva i vlastitih bilješki s predavanja udžbenik "Linearna algebra", objavljen 2008. godine, s idejom, kako je sam napisao, da odabrani materijal organizira u praktičnom i efikasnom obliku. Skripta su i znatno ranije bila dostupna na web stranicama PMF-Matematičkog odsjeka. Prema vlastitom komentaru prof. Bakića, te uz malo slobodne interpretacije, cilj mu je bio pružiti studentima i općenito zainteresiranim čitateljima udžbenik kakav im je stvarno potreban na razini prve godine studija matematike, kako u smislu pragmatičnosti (ispiti, kolokviji, ispiti na višim godinama...) tako i za stvaranje čvrste podloge razumijevanja materije, neophodne za uspješan studij. Riječ je i o tome da velika većina studenata nema previše vremena ni volje proučavati izvore opsežnije i zahtjevnije od precizno onog što (smatraju da) im doista treba. Naprednija poglavlja, daljnje primjene... to će se eventualno potražiti kad se bude moralo, diktirano programom (kolegij Vektorski prostori i dalje), ali praktično je raspolagati udžbenikom u kojem se čim manje toga može "preskakati" ili birati po vlastitom nahođenju.

Ako je ovo prethodno primjenjivo na studij matematike koji se među matematičarima na Prirodoslovno-matematičkom fakultetu u Zagrebu još uvijek u žargonu naziva "inženjerskim", onda to pogotovo vrijedi za "profesorske" smjerove. Specifičnosti nastavničkih smjerova s vremenom su sve više dolazile do izražaja, a time je narastala potreba i motivacija pisanja skripata namijenjenih upravo njima. Objektivne su činjenice da studenti nastavničkih smjerova, gledano u cjelini i u prosjeku, dolaze na studij matematike s predznanjem slabijim od onih koji su izabrali "inženjerski" smjer, a pritom ni jedni ni drugi nemaju osobitog iskustva sa služenjem matematičkom literaturom. Naviknuti se na takvu literaturu i naučiti je čitati – važan je dio studija, naročito u početnim semestrima. Naravno da "sve se može naći kod Horvatića", primjerice, ali redoslijed poglavlja i njihove logičke poveznice nisu više jednake kao u nekadašnjem programu. Manje iskusnim čitateljima, dakle većini studenata, ozbiljna je zapreka pri učenju ako moraju sami birati i preslagivati dijelove izlaganja iz različitih izvora, koliko god samih po sebi kvalitetnih.

Pritom, iz uglavnom očitih razloga, mnogim studentima Linearna algebra je "previše apstraktna", "komplicirana" ili jednostavno "teška". Snalaženje u nizovima strogo poredanih definicija, propozicija, teorema, dokaza, korolara i primjera, proširenih dodatnim primjedbama, objašnjenjima, napomenama i zadacima za vježbu, doista nije lagano. Naročito kad se nakon uhodanog "konkretnog" računanja iz srednje škole, rjeđe prirodoslovno-matematičkog usmjerenja (upamti formule pa uvrsti zadane brojeve, memoriraj korake svakog postupka ne opterećujući se nužno njihovim smislom i slično) valja podići na višu razinu. Na pravu, ozbiljnu matematiku. Na strukture – logičke, skupovne, algebarske, geometrijske... Na ono što studenti neformalno, a neki i s priličnom odbojnošću, sažeto zovu "teorija".

Prednost je nastavničkih smjerova što prije Linearne algebre slušaju Analitičku geometriju, koja obuhvaća i Klasičnu algebru vektora (dva poglavlja u knjizi prof. Horvatića, u skladu s nekadašnjim programom dvosemestralnog kolegija). Izdvajanje Analitičke geometrije kao kolegija prethodnika Linearne algebre smatramo savršeno opravdanim potezom, a studentima na početku Linearne algebre 1 kao osnovni savjet ističemo da si osvježe gradivo tog predmeta koji su većinom ionako slušali prije par mjeseci, a položili prije par tjedana. Mnoge od ključnih koncepata, dakako, trebalo je upoznati i naviknuti se računski primjenjivati u klasičnom modelu vektorskog prostora sa "strelicama", što bi onda moralo bitno olakšati prijelaz na opće vektorske prostore i cjelokupnu pripadnu tehniku. U praksi baš i nije sasvim tako.

Ova skripta dostupna su na web stranicama već nekoliko godina, u radnom obliku koji se kontinuirano dopunjavao i korigirao. Značajan je aspekt da nisu koncipirana nakon što su u akademskoj godini 2018./2019. uvedene neke dosta važne promjene u programu, nego da su ažurno odražavala transformacije za koje su se zalagali autori, na temelju iskustva u nastavi i svojih procjena mogućih poboljšanja. Stjecajem okolnosti, te su promjene koincidirale s povećanjem broja sati predavanja iz Linearne algebre 2, s 2 sata na 3 sata, čime je, dakako, uveliko olakšano izlaganje gradiva bez forsiranja tempa kakav slušateljima nipošto ne odgovara.

U pisanju ovih skripata gotovo ništa nije izravno ili doslovno preuzimano iz drugih izvora, što bi u prvom redu bile već spomenute knjige prof. Horvatića i prof. Bakića, koje redovito navodimo kao obaveznu literaturu. Ipak, sličnosti su jako velike, neizbježno, ali ne zbog direktnog kopiranja, nego zato što je to Linearna algebra kakva se, u dobroj tradiciji i uz poneku modifikaciju, predaje i tumači onako kako smo odavno naučili, u uvjerenju da je temeljna koncepcija istinski dobra i vrijedna. Naravno da će dileme poput "što je prije – strelica ili matrica?", "idu li prvo sustavi ili linearni operatori?" različiti profesori razriješiti po svom shvaćanju, no za nastavničke smjerove dosta takvih nedoumica otpada već samom svrhom atributa nastavnički. Stariji koautor skripata učio je Linearnu algebru kod doc. Zdravka Kurnika, u davnoj godini kad je prvi put predavana pod tim naslovom, a vježbe su držali tadašnji asistenti Dragutin Svrtan i Mirko Polonijo. U "tandemu" s Hrvojem Šikićem izvodio je vježbe kod profesora Horvatića, čija je predavanja, znatno kasnije, slušala koautorica skripata. Imena koja danas, nakon više desetljeća, imaju itekakvu težinu na PMF-MO navodimo i iz zahvalnosti za sve naučeno, kao i u smislu naznake o kakvoj je to dobroj tradiciji riječ.

U Uvodu ćemo ukratko navesti neke konkretne napomene i komentare o sadržaju skripata.

Zahvaljujemo se svima koji su čitali taj materijal na web stranicama, u različitim etapama stvaranja te nam dostavili primjedbe, sugestije i korekcije. To su, među ostalima, prof. dr. sc. Ljiljana Arambašić i izv. prof. dr. sc. Ilja Gogić, koji su također predavali ove predmete u pojedinim semestrima kroz posljednjih nekoliko godina, kao i nekolicina studentica i studenata. U nastavi je svoj vrijedan doprinos, koji je možda neizravno ostavio traga i u skriptama, dalo i desetak asistentica i asistenata te im se svima zajedno također zahvaljujemo.

Zrinka Franušić i Juraj Šiftar

Sadržaj

Uvod

Vektorski prostor je ključni pojam u linearnoj algebri. Dosad nam je riječ "vektor" redovito bila povezana s geometrijskom predodžbom "strelice" u euklidskoj ravnini ili prostoru, često motivirane potrebom prikazivanja fizikalnih veličina poput brzine i sile, za čiji je opis uz numerički podatak iznosa potrebno poznavati i smjer te orijentaciju djelovanja. Kako bi takvi vektori-strelice postali stvarno korisni, uvode se operacije zbrajanja i množenja realnim brojem. Tada se, primjerice, u geometriji može pregledno i elegantno, jednim računom s vektorima, dokazati da se težišnice svakog trokuta sijeku u jednoj točki, a da ta točka dijeli sve tri težišnice u omjeru $2:1$. U mehanici se takvim metodama izračunavaju rezultante dviju ili više sila. U Analitičkoj geometriji naučili smo kako se matematički korektno definira skup vektora, na temelju euklidske geometrije te kako se taj skup snabdijeva strukturom vektorskog prostora, što znači da se definiraju operacije zbrajanja vektora i množenja vektora realnim brojem ("skalarom") tako da budu ispunjena određena poželjna svojstva. Uvedene su bile i operacije nešto drukčijeg tipa, skalarno množenje vektora i vektorsko množenje vektora, koje su također vrlo korisne, ali ne pripadaju osnovnoj strukturi vektorskog prostora.

Vektorski prostor u svom općenitom značenju, koje nije ograničeno na pojedini model poput V^2 ili V^3, upravo je pogodan matematički okvir za potpuni uvid u rješavanje sustava linearnih jednadžbi s bilo kojim (konačnim) brojem nepoznanica, a to je jedan od glavnih ciljeva Linearne algebre 1. Uvjerit ćemo se da su nam glavne ideje zapravo već poznate iz Analitičke geometrije pa čak i iz srednje škole ("geometrijsko rješavanje sustava dviju jednadžbi s dvije nepoznanice"). No, u tom međusobnom prožimanju geometrijske intuicije i algebarskog izražavanja trebat ćemo se "podići" od zornog (vizualnog) predočavanja u dvije ili tri dimenzije i naviknuti se na snalaženje i računanje u općenitom, a prvenstveno konačnodimenzionalnom vektorskom prostoru. Pritom će nam dobro razumijevanje klasične vektorske algebre u "vidljivim" dimenzijama i dalje ostati važna osnova, kroz primjere i analogije, za usvajanje novih pojmova i činjenica.

Preliminarni pojmovi i oznake

Počnimo s pregledom osnovnih pojmova, oznaka i važnijih činjenica elementarne matematike, posebice iz elementarne teorije skupova.

Skup je osnovni matematički pojam koji se ne definira. To je množina (kolekcija, familija, ...) elemenata (objekata) koje odlikuju neka zajednička svojstva. Najčešće ih označavamo velikim tiskanim slovima (A, B,..., X). Glavni skupovi brojeva s njihovim oznakama su

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

Skupove uglavnom **zadajemo** tako da navedemo sve njihove elemente ili pomoću karakterističnog svojstva. Na primjer, $A = \{x, y, z\}$ i $B = \{x : x^2 \geq 4\,, x \in \mathbb{Z}\}$. Za **prazan skup** (to jest skup bez ijednog elementa) rabit ćemo oznaku $\emptyset$.

Broj elemenata konačnog skupa A naziva se **kardinalni broj** skupa A i označava se s card A ili s $|A|$. Za prazan skup $\emptyset$ definira se card $\emptyset = 0$.

Ukratko ćemo navesti osnovne skupovne relacije i operacije te njihove pripadne oznake.

- Peanova relacija: $a \in A$ ('a je element skupa A'), $b \notin A$ ('b nije element skupa A')
- Podskup skupa: $A \subseteq B$ ($x \in A$ povlači $x \in B$)
- Jednakost skupova: $A = B$ (ako $A \subseteq B$ i $B \subseteq A$)
- Presjek skupova: $A \cap B = \{x \,:\, x \in A \text{ i } x \in B\}$
- Unija skupova: $A \cup B = \{x \,:\, x \in A \text{ ili } x \in B\}$
- Razlika skupova: $A \backslash B = \{x \,:\, x \in A \text{ i } x \notin B\}$
- Simetrična razlika skupova : $A \triangle B = (A \backslash B) \cup (B \backslash A)$
- Komplement skupa: $A \subseteq S$, $A^c = S \backslash A$
- Partitivni skup: za $A \neq \emptyset$, $\mathcal{P}(A)$ je skup svih podskupova od A
- Kartezijev produkt skupova: $A \times B = \{(x, y) \,:\, x \in A,\, y \in B\}$ (skup svih uređenih parova pri čemu je prvi član iz skupa A a drugi iz B), $A \times A = A^2$

Neka su X, Y skupovi i f *pravilo* po kojem se svakom elementu skupa X pridružuje *jedan* element skupa Y. Uređena trojka (X, Y, f) naziva se **preslikavanje** ili **funkcija** skupa X u skup Y koju obično zapisujemo kao

$$f : X \to Y.$$

Skup X naziva se **područje definicije** ili **domena**, skup Y **područje vrijednosti** ili **kodomena**, a f **pravilo** ili **zakon** preslikavanja.

Elementu $x \in X$ je po pravilu f pridružen element $f(x)$ i pišemo

$$x \mapsto f(x).$$

Kažemo da je $f(x)$ **slika elementa** x ili **vrijednost funkcije** f **u varijabli** (točki, argumentu) x.

Slika preslikavanja f je skup

$$f(X) = \{f(x) \,:\, x \in X\}.$$

Ponekad se još označava sa $S(f)$ ili $\mathrm{Im}(f)$. Jasno je da vrijedi da je $f(X) \subseteq Y$. Analogno, možemo definirati i sliku bilo kojeg podskupa $A \subseteq X$, $f(A)$.

Za $B \subseteq Y$ skup svih elemenata iz X čija slika pripada skupu B naziva se **praslika** podskupa B i označava se

$$f^{-1}(B) = \{x \in X \,:\, f(x) \in B\}.$$

Posebno, za $y \in Y$ i $B = \{y\}$ pišemo

$$f^{-1}(y) = \{x \in X \,:\, f(x) = y\}$$

i kažemo da je $f^{-1}(y) \subseteq X$ praslika elementa y. Primijetimo da praslika nekog elementa ili podskupa može biti prazan skup. Naglasimo da se oznaka $f^{-1}(B)$, odnosno $f^{-1}(y)$ ne odnosi na inverznu funkciju f^{-1} od f, koja ne mora postojati (ako f nije bijekcija).

Dvije funkcije $f : X \to Y$ i $f' : X' \to Y'$ su **jednake** ako su im domene jednake, to jest $X = X'$ i $f(x) = f'(x)$ za sve x iz X. Tada pišemo $f = f'$.

Neka su $f : X \to Y$ i $g : Y \to Z$ preslikavanja i neka vrijedi da je $f(X) = Y$. Tada je jedinstveno definirano preslikavanje

$$h : X \to Z, \quad h(x) = g(f(x)), \quad x \in X.$$

Preslikavanje h nazivamo **kompozicijom funkcija** f i g, te ga označavamo s $g \circ f$.

Jednostavnom provjerom definicije možemo ustanoviti da je komponiranje funkcija zadovoljava svojstvo *asocijativnosti*, to jest za dana preslikavanja $f : X \to Y$, $g : Y \to Z$ i $h : Z \to V$ (uz uvjete da je $f(X) = Y$ i $g(Y) = Z$) kompozicije $(h \circ g) \circ f$, $h \circ (g \circ f) : X \to V$ su jednake.

Komponiranje funkcija nije općenito *komutativno*, to jest općenito $g \circ f \neq f \circ g$.

Na kraju ovog preliminarnog dijela ponovimo još tri važna svojstva koja može imati funkcija. Kažemo da je $f : X \to Y$ **injekcija** ili **injektivno preslikavanje** ako

$$x_1, x_2 \in X,\ x_1 \neq x_2 \ \Rightarrow\ f(x_1) \neq f(x_2).$$

Injektivnost se najčešće ispituje korištenjem ekvivalentne tvrdnje: f je injekcija ako za $x_1, x_2 \in X$

$$f(x_1) = f(x_2) \ \Rightarrow\ x_1 = x_2.$$

Funkcija f će biti injektivna ako i samo se praslika svakog elementa iz Y, $f^{-1}(y)$, sastoji od najviše jednog elementa. Iz tog razloga se injektivna preslikavanja još nazivaju *1-1 preslikavanjima.*

Kažemo da je $f : X \to Y$ **surjekcija** ili **surjektivno preslikavanje** ako je slika domene jednaka kodomeni,

$$f(X) = Y.$$

Zbog toga se za surjekciju još rabi termin *preslikavanje na.*

Funkcija $f : X \to Y$ je **bijekcija** ako je injekcija i surjekcija. Vrijedi, da je f bijektivno preslikavanje ako i samo ako za svaki $y \in Y$ *postoji jedinstven* $x \in X$ takav $f(x) = y$. Iz prethodnog se lako zaključuje da je dobro definirano preslikavanje $g : Y \to X$ takvo da je $g(y) = x$ za svaki $y \in Y$. Preslikavanje g naziva se **inverzom** ili **inverznim preslikavanjem** i označava s f^{-1}.

Lako se vidi da je

$$f^{-1} \circ f = 1_X, \quad f \circ f^{-1} = 1_Y,$$

gdje su 1_X, 1_Y *identitete* na skupovima X, odnosno Y ($1_X : X \to X$, $1_X(x) = x$ za sve $x \in X$.)

Poglavlje 1

Vektorski prostori

1.1 Osnovne algebarske strukture

Algebarska struktura sastoji se, ukratko rečeno, od nepraznog skupa te jedne ili više "računskih operacija" na tom skupu za koje vrijede određena propisana svojstva.

Naviknuti smo najviše na računske operacije u skupovima brojeva, no također smo već različite operacije primjenjivali na polinome, na funkcije općenito, na vektore pa i na matrice, ali dosad se uglavnom nisu promatrale i međusobno uspoređivale "apstraktne" strukture, u kojima su objedinjena zajednička svojstva raznovrsnih pojedinačnih modela. Budući da je već sama definicija vektorskog prostora razmjerno složena, jer obuhvaća pojmove važnih struktura *komutativne grupe* i *polja*, izložit ćemo sažeti pregled osnovnih algebarskih struktura kako bismo postupno došli do grupe (strukture u kojoj binarna operacija ima svojstvo asocijativnosti, a svaka jednadžba $ax = b$ ima jednoznačno rješenje) i polja, kao prirodne strukture za rješavanje linearnih jednadžbi s dvije i više nepoznanica.

U linearnoj algebri posebno su važne i operacije s matricama, kod kojih postoje sličnosti, ali i bitne razlike u odnosu na operacije u skupovima brojeva. Poznavanje osnovnih algebarskih struktura znatno će nam pomoći i u matričnom računu, a taj je usko povezan sa sustavima linearnih jednadžbi.

1.1.1 Binarna operacija. Grupoid.

Definicija 1.1.1. *Neka je S neprazan skup. Preslikavanje*

$$\theta : S \times S \to S$$

naziva se ***binarna operacija*** *na skupu S. Binarna operacija θ svakom uređenom paru $(x, y) \in S \times S$ pridružuje element $z = \theta(x, y) \in S$ (ili alternativno $z = x\,\theta\,y$).*

Uređeni par (S, θ) naziva se ***grupoid****, odnosno kažemo da binarna operacija θ određuje na skupu S* ***algebarsku strukturu grupoida****.*

Navedimo primjere nekih binarnih operacija.

- Zbrajanje i množenje na skupovima brojeva ($\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$) nazivamo *standardno zbrajanje* i *standardno množenje.* Dakle, $(\mathbb{N}, +)$, $(\mathbb{N}, \cdot)$, $(\mathbb{Z}, +)$, $(\mathbb{Z}, \cdot)$, $(\mathbb{Q}, +)$, ... su grupoidi.

- Oduzimanje je binarna operacija na $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ i $\mathbb{C}$, ali nije na $\mathbb{N}$.
- Presjek, unija, razlika, simetrična razlika su binarne operacije na partitivnom skupu od nepraznog skupa S, $\mathcal{P}(S)$.
- Vektorsko množenje ($\times$) je binarna operacija na vektorskom prostoru V^3.
- Na skupu svih funkcija $f : S \to S$ standardnu binarnu operaciju predstavlja kompozicija funkcija (u oznaci $\circ$).
- Binarnu operaciju možemo definirati na različite načine koristeći se već nekim zadanim, poznatim binarnim operacijama na tom skupu. Na primjer, $a*b = a+b-ab$ za $a, b \in \mathbb{Z}$. Uočimo da je $(\mathbb{Z}, *)$ grupoid, ali $(\mathbb{N}, *)$ to nije.

Napomenimo da ćemo u daljnjem izlaganju binarnu operaciju θ zbog jednostavnosti označavati znakom $\cdot$, to jest $\theta(x, y) = x \cdot y = xy$, pri čemu ne ćemo nužno misliti na standardno množenje. U različitim primjerima i zadacima također se za neku binarnu operaciju mogu koristiti oznake poput $\star$, $\bullet$, $\diamond$, $\oplus$, $\otimes$ i drugi simboli, obično u slučaju kad se uvede neka nestandardna binarna operacija.

Definicija 1.1.2. *Neka je $(S, \cdot)$ grupoid. Elementi $x, y \in S$ **komutiraju** ako vrijedi*

$$xy = yx.$$

*Ako svaka dva elementa iz S komutiraju onda kažemo da je binarna operacija **komutativna**, odnosno da je $(S, \cdot)$ **komutativan grupoid**.*

Standardno zbrajanje i standardno množenje su komutativne operacije, dok vektorsko množenje to nije.

Definicija 1.1.3. *Neka je $(S, \cdot)$ grupoid. Binarna operacija je **asocijativna** ako je*

$$x(yz) = (xy)z,$$

*za sve $x, y, z \in S$. Grupoid s asocijativnom binarnom operacijom naziva se **polugrupa**. Ako je binarna operacija i komutativna, grupoid se naziva **komutativna polugrupa**.*

Neki primjeri polugrupa:

- Skupovi brojeva $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ s obzirom na standardno zbrajanje i standardno množenje su komutativne polugrupe.
- Binarna operacija oduzimanja na $\mathbb{Z}$ nije asocijativna.
- Kompozicija funkcija je asocijativna pa je $(\{f : S \to S\}, \circ)$ polugrupa, no općenito nekomutativna.
- Komutativne polugrupe su $(\mathcal{P}(S), \cap)$ i $(\mathcal{P}(S), \cup)$, ali $(\mathcal{P}(S), \setminus)$ nije polugrupa jer razlika skupova nije asocijativna.

Naglasimo važnost svojstva asocijativnosti za jednostavnu primjenu binarnih operacija. Može se dokazati, metodom matematičke indukcije, da u polugrupi bilo koji raspored zagrada, koje naznačuju prioritet izvođenja operacije, ne utječe na rezultat. Primjerice, u polugrupi $(S, \cdot)$ za svaka 4 elementa vrijedi $(ab)(cd) = a(b(cd))$ i slično. Posebno, može se definirati potenciranje a^n za svaki $n \in \mathbb{N}$ i tada vrijede uobičajena svojstva: $a^m a^n = a^{m+n}$ te $(a^m)^n = a^{mn}$.

Definicija 1.1.4. *Neka je $(S, \cdot)$ grupoid. Kažemo da je $e \in S$ **neutralni element** ili **jedinica** binarne operacije ako je*

$$ex = xe = x,$$

*za sve $x \in S$. Ako je binarna operacija asocijativna i dopušta neutralni element, onda se $(S, \cdot)$ naziva **monoid**. Ako je operacija još i komutativna, onda govorimo o **komutativnom monoidu**. Ponekad se monoid još naziva* polugrupa s jedinicom.

Lako se pokazuje da ako u grupoidu postoji neutralan element tada je on jedinstven. Zaista, ako pretpostavimo suprotno da su $e, e' \in S$ neutralni elementi onda mora vrijediti da je $ee' = e$ i $ee' = e'$ pa je $e = e'$.

Navedimo primjere nekih monoida.

- Skupovi brojeva $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ s obzirom na standardno zbrajanje i standardno množenje su komutativni monoidi. Neutralni element zbrajanja je 0, a množenja je 1. Uočimo da je $(\mathbb{N}, \cdot)$ komutativni monoid, ali da $(\mathbb{N}, +)$ to nije.
- Funkcija identiteta ($id(x) = x$, $\forall x \in S$) predstavlja neutralni element kompozicije funkcija i stoga je $(\{f \mid f : S \to S\}, \circ)$ monoid.
- $(\mathcal{P}(S), \cap)$ i $(\mathcal{P}(S), \cup)$ su komutativni monoidi. Neutralni elementi su redom S i $\emptyset$.

U nekomutativnim strukturama moguće je imati samo jednostranu jedinicu, *lijevu* ili *desnu*. Na primjer grupoid $(\mathcal{P}(S), \setminus)$ ima samo desnu jedinicu ($\emptyset$). No, ako postoje i desna i lijeva jedinica tada su one nužno jednake.

Napomena 1.1.5. Bez obzira na različite oznake za binarnu operaciju i na njezina moguća posebna svojstva, treba upamtiti da je to, po definiciji, preslikavanje (funkcija), dakle da se svakom uređenom paru elemenata nekog nepraznog skupa S pridružuje jednoznačno određeni element skupa S.

Često se spominje pojam "zatvorenosti" neke operacije na određenom skupu, naročito ako već imamo neki grupoid $(G, *)$ pa je pitanje je li stanoviti njegov podskup S također grupoid, s obzirom na "istu" operaciju. Zapravo je tada riječ o *restrikciji* preslikavanja $* : G \times G \to G$ na podskup $S \times S$. Za $(a, b) \in S \times S$ definiran je $a * b$ kao element skupa G, ali on se općenito ne mora nalaziti u S.

Primjerice, skup $\mathbb{N}$ nije "zatvoren" s obzirom na operaciju oduzimanja, koju primjenjujemo na cijele brojeve, dakle na nadskupu $\mathbb{Z}$ skupa $\mathbb{N}$.

Dakle, izraz "provjerimo zatvorenost operacije" zapravo se odnosi na provjeru je li doista zadana binarna operacija pa time onda i grupoid, prema Definiciji 1.1.1. Treba obratiti pozornost na to o kojoj je domeni i kodomeni riječ, jer se operacija za koju (katkad neprecizno) koristimo jednaki naziv ne može uvijek suziti (restringirati) na podskup ili proširiti na nadskup nekog grupoida.

1.1.2 Grupa

Kako smo već istaknuli u uvodu, *grupa* je iznimno važna algebarska struktura s jednom binarnom operacijom. Osim u više područja matematike, veliki značaj ima i u fizici, npr. kod *grupa simetrija.* U linearnoj algebri pojavljuju se raznovrsni primjeri grupa, a karakteristične su grupe regularnih (invertibilnih) matrica te još nekih posebnih tipova matrica. Također, za definiciju i svojstva determinante, trebat će poznavati osnovna svojstva grupe permutacija.

Definicija 1.1.6. *Neka je $(S, \cdot)$ grupoid i neka je e njegov neutralni element. Ako za $x \in S$ postoji $y \in S$ takav da vrijedi*

$$xy = yx = e,$$

onda kažemo da je element x ***invertibilan****, a element y zovemo* ***inverzni element*** *ili kraće* ***inverz*** *elementa x.*

U nekim nekomutativnim strukturama pojavljuju se jednostrani inverzi, *lijevi* (ako je $yx = e$) ili *desni*(ako je $xy = e$). Ako u monoidu $(S, \cdot)$ neki element x ima lijevi inverz y_L i desni inverz y_D, onda oni su nužno jednaki. Zaista,

$$y_L = y_L e = y_L(xy_D) = (y_L x)y_D = ey_D = y_D.$$

Nadalje, vrijedi:

Propozicija 1.1.7. *Ako je neki element monoida invertibilan, onda je njegov inverz jedinstven.*

Dokaz. Dokaz ove tvrdnje lako izvodimo iz prethodne, da se jednostrani inverzi nekog elementa, ako postoje, nužno podudaraju. Naime, ako pretpostavimo da su x' i x'' inverzi elementa x, onda iskoristimo da je x' kao lijevi inverz jednak elementu x'' u svojstvu desnog inverza. □

Inverz elementa x označavamo s x^{-1}, ali u slučajevima kad je binarna operacija označena znakom $+$ uobičajeno je koristiti oznaku $-x$ te inverz nazivati *suprotnim elementom.*

- U grupoidu $(\mathbb{N}, \cdot)$ invertibilan je samo element 1
- U $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$ su svi elementi invertibilni, to jest svaki x ima suprotni element $-x$ iz pripadnog skupa.
- U $(\mathbb{Q}, \cdot)$, $(\mathbb{R}, \cdot)$ su invertibilni svi elementi osim 0. Jedini invertibilni elementi u $(\mathbb{Z}, \cdot)$ su 1 i -1.
- U $(\{f \mid f : S \to S\}, \circ)$ invertibilni elementi su bijektivna preslikavanja.

Neutralni element e iz grupoida S je uvijek invertibilan jer je on sam vlastiti inverz, to jest $e^{-1} = e$. Stoga je podskup svih invertibilnih elemenata u monoidu neprazan jer sadrži barem neutralni element.

Propozicija 1.1.8. *Neka je $(G, \cdot)$ monoid.*

(a) *Ako je $x \in G$ invertibilan element onda je i x^{-1} invertibilan, te vrijedi*

$$\left(x^{-1}\right)^{-1} = x.$$

(b) *Ako su $x, y \in G$ invertibilni elementi, onda je i xy invertibilan, te vrijedi*

$$(xy)^{-1} = y^{-1}x^{-1}.$$

Dokaz. **(a)** Tvrdnja slijedi iz $xx^{-1} = x^{-1}x = e$ i činjenice da je inverz jedinstven.

(b) Zbog asocijativnosti vrijedi

$$(xy)(y^{-1}x^{-1}) = x(yy^{-1})x^{-1} = xex^{-1} = xx^{-1} = e,$$

te analogno $(y^{-1}x^{-1})(xy) = e$, pa slijedi tvrdnja.

□

Definicija 1.1.9. *Monoid u kojem su svi elementi invertibilni naziva se **grupa**. Ako je binarna operacija komutativna onda govorimo o **komutativnoj** ili **Abelovoj grupi**.*

Pojam grupe možemo odmah primijeniti u sljedećem, vrlo korisnom korolaru Propozicije 1.1.8.

Korolar 1.1.10. *Podskup svih invertibilnih elemenata u monoidu čini grupu.*

Važan primjer grupe invertibilnih elemenata u monoidu je skup svih bijekcija u monoidu $(\{f \mid f : S \to S\}, \circ)$.

Zadatak 1. *Dokažite Korolar 1.1.10.*

Ustanovimo koji skupovi brojeva s obzirom na standardne operacije zbrajanja i množenja čine Abelove grupe.

- $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$ su Abelove grupe. $(\mathbb{N}, +)$ je komutativna polugrupa.
- Uočimo da niti jedna od struktura $(\mathbb{N}, \cdot)$, $(\mathbb{Z}, \cdot)$, $(\mathbb{Q}, \cdot)$, $(\mathbb{R}, \cdot)$, $(\mathbb{C}, \cdot)$ nije grupa no nekima od njih nedostaje "malo" da to postanu. Svi elementi različiti od 0 u $\mathbb{Q}$, $\mathbb{R}$ i $\mathbb{C}$ su invertibilni. Stoga promotrimo te iste skupove bez nule, to jest

  $$\mathbb{Q}^* = \mathbb{Q}\backslash\{0\},\ \mathbb{R}^* = \mathbb{R}\backslash\{0\},\ \mathbb{C}^* = \mathbb{C}\backslash\{0\}.$$

  Bitno je ustanoviti da su svi ovi skupovi "zatvoreni" na operaciju množenja ($a \neq 0$, $b \neq 0$ povlači $ab \neq 0$) pa su $(\mathbb{Q}^*, \cdot)$, $(\mathbb{R}^*, \cdot)$, $(\mathbb{C}^*, \cdot)$ Abelove grupe. Ostala svojstva grupe ovdje se lako provjere, pri čemu se asocijativnost i komutativnost izravno prenose ("nasljeđuju") na podskup pa ih i ne treba posebno provjeravati.
- $(\{0\}, +)$ i $(\{1\}, \cdot)$ su Abelove grupe. Općenito, jednočlani podskup $\{x\}$ neke grupe $(G, \cdot)$ je grupa u odnosu na binarnu operaciju $\cdot$ ako i samo ako $x = e$.

Jedan od ishoda predmeta *Linearna algebra 1* jest naučiti rješavati sustave linearnih jednadžbi. Ako linearnu jednadžbu s jednom nepoznanicom rješavamo u ambijentalnom skupu koji ima strukturu grupe, onda će ta jednadžba imati jedinstveno rješenje. O toj važnoj činjenici govori sljedeća propozicija.

Propozicija 1.1.11. *Neka je* $(G, \cdot)$ *grupa. Jednadžbe*

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

imaju jedinstveno rješenje za svaki izbor elemenata $a, b \in G$*.*

Dokaz. Pretpostavimo da za neki $x \in G$ vrijedi $ax = b$. Primijenimo operaciju u grupi G na inverz a^{-1} elementa a i na ax. Dobivamo

$$a^{-1}(ax) = a^{-1}b.$$

Zbog asocijativnosti je

$$a^{-1}(ax) = (a^{-1}a)x = ex = x$$

pa je $x = a^{-1}b$. Kako je $a^{-1}b \in G$ i $a(a^{-1}b) = b$, doista je $a^{-1}b$ jedno rješenje zadane jednadžbe.

Jedinstvenost se lako pokazuje. Iz pretpostavke da su x_1 i x_2 rješenja slijedi $ax_1 = ax_2$ pa ponovo množenjem slijeva s a^{-1} dobivamo da je $x_1 = x_2$.

Analogno, jednadžba $ya = b$ ima jedinstveno rješenje $y = ba^{-1}$ u grupi G. □

Naglasimo još da u ovoj propoziciji nije pretpostavljeno svojstvo komutativnosti grupe pa treba razlikovati jednadžbe oblika $ax = b$ i $ya = b$, kao što i u dokazu nije svejedno u kojem redoslijedu se primjenjuje operacija u grupi na elemente a^{-1} i b. U slučaju standardnih operacija zbrajanja i množenja, naviknuti smo jednostavno "oduzeti a s obje strane" odnosno "skratiti obje strane jednadžbe s a", pod uvjetom da je $a \neq 0$. No, primjerice u grupi bijekcija s obzirom na kompoziciju funkcija, gdje komutativnost ne vrijedi općenito, nipošto nije svejedno hoćemo li za rješenje jednadžbe napisati npr. $f^{-1} \circ g$ ili $g \circ f^{-1}$.

Sasvim slično dokazuje se sljedeće svojstvo grupe o rješenju jednostavne, ali važne jednadžbe nešto drukčijeg oblika:

Propozicija 1.1.12. *Neka je* $(G, \cdot)$ *grupa. Jednadžba*

$$x \cdot x = x$$

ima jedinstveno rješenje $x = e$*.*

U Definiciji 1.1.9 grupa je definirana kao monoid u kojem je svaki element invertibilan. Ekvivalentno, grupa se može definirati tako da se navedu sva pojedina svojstva koja grupoid treba ispunjavati kako bi bio grupa, odnosno Abelova grupa, s obzirom na zadanu operaciju. Neka je G neprazan skup i $\cdot$ preslikavanje s domenom $G \times G$. Uređeni par $(G, \cdot)$ je **grupa** ako ima sljedeća svojstva:

(1) $xy \in G$ za sve $x, y \in G$, (*zatvorenost*)

(2) $(xy)z = x(yz)$ za sve $x, y, z \in G$, (*asocijativnost*)

(3) Postoji $e \in G$ takav da je $ex = xe = x$ za sve $x \in G$, (*neutralni element*)

(4) Za svaki $x \in G$ postoji $y \in G$ takav da je $xy = yx = e$. (*inverzni element*)

Ako vrijedi i svojstvo

(5) $xy = yx$ za sve $x, y \in G$, (*komutativnost*)

onda je $(G, \cdot)$ **komutativna** ili **Abelova grupa**.

U konkretnom primjeru ili zadatku, svojstva grupe uobičajeno je dokazivati upravo u redoslijedu kako su iskazana. Kao primarno svojstvo koje treba provjeriti ističe se zatvorenost, u smislu Napomene 1.1.5, dakle činjenica da je na skupu G doista korektno zadana binarna operacija, čime je $(G, \cdot)$ u prvom redu grupoid. Jasno je da (4) ima smisla samo ako vrijedi (3). Svojstvo komutativnosti (5) može se dokazati ili opovrgnuti nezavisno od ostalih svojstava.

U sljedećih nekoliko primjera detaljno ćemo pokazati kako se provjeravaju svojstva grupe. Napomenimo da se u pojedinim primjerima može dosta razlikovati težina provjere nekog svojstva. Primjerice, svojstvo asocijativnosti katkad se može provjeriti rutinskim računom, ali ponekad je znatno zahtjevnije za provjeru.

Primjer 1. ***Grupa ostataka modulo*** m
Neka je $m \in \mathbb{N}$ i $m > 1$. Definiramo skup

$$\mathbb{Z}_m = \{0, 1, 2 \ldots, m-1\}.$$

Prije nego što definiramo operaciju na $\mathbb{Z}_m$ prisjetimo se što kaže *Teorem o dijeljenju s ostatkom*: ako su $a, b \in \mathbb{Z}$ i $b \neq 0$ onda postoje jedinstveni $q \in \mathbb{Z}$ i $r \in \mathbb{Z}_m$ takvi da je $a = bq + r$. Broj r je jedinstveni ostatak broja a pri dijeljenju s b.

Sada, na skupu $\mathbb{Z}_m$ definiramo binarnu operaciju koja svakom uređenom paru $(x, y) \in \mathbb{Z}_m \times \mathbb{Z}_m$ pridružuje ostatak pri dijeljenju broja $x+y$ brojem m. Ova operacija se naziva *zbrajanje modulo* m i označava s $+_m$. Pišemo

$$x +_m y = z,$$

pri čemu je $x + y = mq + z$ za neki $q \in \mathbb{Z}$ i $z \in \mathbb{Z}_m$.

Krenimo redom ispitati svojstva grupe. Svojstvo **(1)** vrijedi prema samoj definiciji.

(5) Operacija $+_m$ je očito komutativna.

(2) Svojstvo asocijativnosti nije sasvim jednostavno za pokazati. Neka je

$$(x +_m y) +_m z = r +_m z = s,$$

gdje je

$$x + y = km + r, \tag{1.1}$$
$$r + z = lm + s, \tag{1.2}$$

za $k, l \in \mathbb{Z}$ i $r, s \in \mathbb{Z}_m$. Nadalje, neka je $y +_m z = t$, to jest

$$y + z = pm + t, \tag{1.3}$$

za $p \in \mathbb{Z}$ i $t \in \mathbb{Z}_m$. Ako zbrojimo jednakosti (1.1), (1.2) i (1.3) pomnoženu s -1 dobit ćemo

$$x + t = (k + l - p)m + s,$$

odnosno $x +_m t = s$ pa je

$$x +_m (y +_m z) = x +_m t = s,$$

što je i trebalo pokazati.

(3) 0 je neutralni element.

(4) Suprotni element (inverz) od $x \in \mathbb{Z}_m \backslash \{0\}$ je $m - x$, a element 0 je sam sebi inverz.

Zaključujemo da je $(\mathbb{Z}_m, +_m)$ Abelova grupa koja je poznata pod nazivom *grupa ostataka modulo m*. S njom ćemo se susretati na još nekim predmetima na ovom studiju, na primjer na *Elementarnoj teoriji brojeva*.

Za konkretnu vrijednost broja m, na primjer $m = 4$ rezultat operacije na svakom uređenom paru zapisujemo u tablici:

$+_4$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

Nije rijetko da upravo tablično definiramo binarnu operaciju na nekom konačnom skupu. Tu tablicu binarne operacije nazivamo *Cayleyeva tablica*.

Prirodno je analogno definirati i operaciju *množenja modulo m*, u oznaci $\cdot_m$ i pitati se je li $(\mathbb{Z}_m, \cdot_m)$ isto Abelova grupa. Odgovor je *ne*. No, situaciju možemo 'popraviti' u ovisnosti o tome je li broj m prost ili složen. Promotrimo tablicu za $m = 4$:

$\cdot_4$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Može pokazati da su zadovoljena svojstva komutativnosti, asocijativnosti (- ne lako!), i da je 1 neutralni element, no jasno je da elementi 0 i 2 nemaju multiplikativni inverz. Stoga je $(\mathbb{Z}_4, \cdot_4)$ komutativni monoid. Za $m = 5$ imamo sljedeću tablicu

$\cdot_5$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2

Nakon pomnijeg istraživanja tablice možemo zaključiti da je $(\mathbb{Z}_5, \cdot_5)$ komutativni monoid i da jedino 0 nema inverz. Ako iz skupa $\mathbb{Z}_5$ izbacimo nulu, $\mathbb{Z}_5^* = \mathbb{Z}_5 \backslash \{0\}$, struktura se 'popravila' i $(\mathbb{Z}_5^*, \cdot_5)$ je Abelova grupa.

♡

Primjer 2. Na kolegiju *Analitička geometrija* pokazalo se da operacija *zbrajanja vektora* na V^1, V^2 i V^3 zadovoljava sva svojstva Abelove grupe.

♡

Primjer 3. Grupa polinoma.

Neka je $n \in \mathbb{N}_0$ i $a_0, a_1, \ldots, a_n \in \mathbb{R}$, $a_n \neq 0$. Preslikavanje $p : \mathbb{R} \to \mathbb{R}$ zadano s

$$p(x) = a_0 + a_1 x + \cdots + a_n x^n$$

naziva se (realni) *polinom stupnja n*. *Nulpolinom* je polinom za kojeg vrijedi $p(x) = 0$, za sve $x \in \mathbb{R}$ i za njega se ne definira stupanj (ipak ponekad se uzima da mu je stupanj $-\infty$ ili -1). Polinome zbrajamo tako da im zbrojimo koeficijente uz odgovarajuće potencije. Neka je $\mathcal{P}_n$ skup koji se sastoji o nulpolinoma i svih polinoma stupnja manjeg ili jednakog n. Lako je za ustanoviti da je $(\mathcal{P}_n, +)$ Abelova grupa. Za razliku od toga množenje polinoma čak nije ni binarna operacija u $\mathcal{P}_n$ (osim u trivijalnom slučaju $n = 0$). Nadalje, ako s $\mathcal{P}$ označimo skup svih polinoma, to jest $\mathcal{P} = \cup_{n \geq 0} \mathcal{P}_n$, tada je $(\mathcal{P}, +)$ također Abelova grupa, a $(\mathcal{P}, \cdot)$ je komutativni monoid.

♡

Primjer 4. Grupa n-tih korijena jedinice.

Za $n \in \mathbb{N}$ definiramo

$$K_n = \{z \in \mathbb{C} \,:\, z^n = 1\}.$$

Skup K_n predstavlja skup svih rješenja jednadžbe $z^n - 1 = 0$ u skupu kompleksnih brojeva. Tih rješenja u $\mathbb{C}$ ima točno n i zovu se *n-ti korijeni jedinice* (ili korijeni jedinice stupnja n). Skup možemo i eksplicitno zapisati kao

$$K_n = \{\cos\frac{2k\pi}{n} + i\sin\frac{2k\pi}{n} \,:\, k = 0, 1, 2, \ldots, n-1\}.$$

Ispitajmo koju algebarsku strukturu čini ovaj skup s obzirom na operaciju standardnog množenja.

(1) Neka su $z_1, z_2 \in K_n$. Tada vrijedi

$$(z_1 \cdot z_2)^n = z_1^n \cdot z_2^n = 1 \cdot 1 = 1,$$

pa je i $z_1 z_2 \in K_n$.

(2) Standardno množenje u K_n je asocijativno.

(3) Postoji neutralni element $1 \in K_n$.

(4) Svaki $z \in K_n$ ima inverz z^{-1} u $\mathbb{C}$ (jer je očito $z \neq 0$). Provjerimo da je $z^{-1} \in K_n$:

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

(5) Standardno množenje je komutativno.

Zaključujemo da je $(K_n, \cdot)$ Abelova grupa a nazivamo ju *grupa n-tih korijena jedinice*. Navedimo primjere za prvih nekoliko vrijednosti broja n:

$$K_1 = \{1\},\ K_2 = \{1, -1\},\ K_3 = \{1, \frac{-1+i\sqrt{3}}{2}, \frac{-1-i\sqrt{3}}{2}\},\ \ K_4 = \{1, i, -1, -i\}, \dots$$

Lako možemo uočiti da elemente grupe K_n možemo shvatiti u kompleksnoj ravnini i kao vrhove pravilnog n-terokuta upisanog u jediničnu kružnicu.

♡

Primjer 5. Grupa $\mathbb{Q}(\sqrt{2})$.

Neka je
$$\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2}\ :\ a, b \in \mathbb{Q}\}.$$

Uz standardno zbrajanje lako se ustanovljava da $(\mathbb{Q}(\sqrt{2}), +)$ ima strukturu Abelove grupe. Zaista, provjerit ćemo sve aksiome grupe.

(1) Zbrajanje je zatvoreno u $\mathbb{Q}(\sqrt{2})$, to jest
$$(a + b\sqrt{2}) + (c + d\sqrt{2}) = (a + c) + (b + d)\sqrt{2} \in \mathbb{Q}(\sqrt{2}), \quad \forall\, a, b, c, d \in \mathbb{Q},$$
jer $a + c, b + d \in \mathbb{Q}$

(2) Standardno zbrajanje je asocijativno. (Još kažemo da se nasljeđuje iz $\mathbb{R}$ jer je $\mathbb{Q}(\sqrt{2}) \subset \mathbb{R}$.)

(3) Postoji neutralni element $0 \in \mathbb{Q}(\sqrt{2})$ jer $0 \in \mathbb{Q}$.

(4) Svaki $a + b\sqrt{2} \in \mathbb{Q}(\sqrt{2})$ ima suprotni element (inverz) $-a - b\sqrt{2} \in \mathbb{Q}(\sqrt{2})$

(5) Standardno zbrajanje je komutativno.

Sada ispitajmo koju strukturu čini $\mathbb{Q}(\sqrt{2})$, odnosno $\mathbb{Q}(\sqrt{2})^* = \mathbb{Q}(\sqrt{2})\backslash\{0\}$ s obzirom na standardno množenje.

(1) Množenje je zatvoreno u $\mathbb{Q}(\sqrt{2})^*$, to jest
$$(a + b\sqrt{2}) \cdot (c + d\sqrt{2}) = (ac + 2bd) + (ad + bc)\sqrt{2} \in \mathbb{Q}(\sqrt{2}), \quad \forall\, a, b, c, d \in \mathbb{Q},$$
jer $ac + 2bd, ad + bc \in \mathbb{Q}$. Nadalje, $(a + b\sqrt{2}) \cdot (c + d\sqrt{2}) \neq 0$ jer je $a + b\sqrt{2} \neq 0$ i $c + d\sqrt{2} \neq 0$.

(2) Standardno množenje je asocijativno.

(3) Postoji neutralni element $1 \in \mathbb{Q}(\sqrt{2})^*$.

(4) Svaki $a + b\sqrt{2} \in \mathbb{Q}(\sqrt{2})^*$ ima inverz
$$(a + b\sqrt{2})^{-1} = \frac{a}{a^2 - 2b^2} - \frac{b}{a^2 - 2b^2}\sqrt{2} \in \mathbb{Q}(\sqrt{2})^*.$$

Uočimo da je $a^2 - 2b^2 \neq 0$ za $a, b \in \mathbb{Q}$ i $a^2 + b^2 \neq 0$, te $\frac{a}{a^2-2b^2}, \frac{-b}{a^2-2b^2} \in \mathbb{Q}$

(5) Standardno množenje je komutativno.

Dakle, $(\mathbb{Q}(\sqrt{2})^*, \cdot)$ je Abelova grupa.

♡

Napomena 1.1.13. Uočimo da u primjerima 4 i 5 nismo morali dokazivati svojstvo asocijativnosti i komutativnosti budući da ta svojstva vrijede na skupovima $\mathbb{C}$ i $\mathbb{R}$ koji sadrže K_n i $\mathbb{Q}(\sqrt{2})$. Štoviše, u Primjeru 4 pokazali smo da je skup K_n jedna *podgrupa* Abelove grupe $(\mathbb{C}^*, \cdot)$, a u Primjeru 5 da je $\mathbb{Q}(\sqrt{2})$ jedna *podgrupa* Abelove grupe $(\mathbb{R}, +)$. Općenito, kažemo da je podskup H grupe G *podgrupa* od G, ako je H grupa s obzirom na binarnu operaciju $\cdot$ uz koju je G grupa. Pišemo $H \leq G$. Lako se može ustanoviti da je $H \leq G$ ako i samo ako vrijedi

$$x \cdot y \in H, \; x^{-1} \in H,$$

za sve $x, y \in H$. Odnosno, $H \leq G$ ako i samo

$$x \cdot y^{-1} \in H,$$

za sve $x, y \in H$. Napominjemo da je suvišno pokazivati da je neutralni element operacije, e, sadržan u H, zato što pretpostavke da je $x \in H$ i $x^{-1} \in H$ impliciraju da je $e = x \cdot x^{-1} \in H$.

Primjer 6. Struktura s eksplicitno zadanom *novom* operacijom.

Zadan je skup

$$G = \{x \in \mathbb{R} : x > 0, x \neq 1\}$$

i operacija

$$x * y = x^{\log y}, \quad x, y \in G,$$

pri čemu je log *logaritam po bazi* 10.

Ispitujemo redom aksiome grupe.

(1) Za $x, y \in G$ je $z = x * y = x^{\log y} > 0$. Provjerimo da je $z \neq 1$. Zaista, ako $z = 1$, onda je $\log y = 0$ pa je $y = 1$ što je u proturječju s činjenicom $y \in G$. Dakle, $z \in G$ i operacija je $*$ je jedna *binarna* operacija na G, to jest ispunjeno je svojstvo *zatvorenosti.*

(2) Asocijativnost moramo provjeriti raspisivanjem. Za $x, y, z \in G$ vrijedi

$$\begin{aligned} (x * y) * z &= (x^{\log y}) * z = (x^{\log y})^{\log z} = x^{\log y \log z}, \\ x * (y * z) &= x * (y^{\log z}) = x^{\log(y^{\log z})} = x^{\log z \log y} = x^{\log y \log z}. \end{aligned}$$

(5) Operacija je komutativna jer je

$$x * y = x^{\log y} = (10^{\log x})^{\log y} = 10^{\log x \log y} = 10^{\log y \log x} = (10^{\log y})^{\log x} = y^{\log x} = y * x.$$

(3) Pitamo se postoji li $e \in G$ takav da je $x * e = x$ za sve $x \in G$, to jest $x^{\log e} = x$ a to vrijedi ako i samo ako je $e = 10$. Zbog komutativnosti imamo sljedeće

$$x * 10 = 10 * x = x, \; \forall x \in G.$$

(4) Neka je $x \in G$ i y takav da je $x * y = 10$. Tada je $x^{\log y} = 10$ i slijedi da je

$$y = 10^{\frac{1}{\log x}} = 10^{\log_x 10}.$$

Vrijedi da je $y > 0$ i $y \neq 1$, pa je $y = x^{-1} \in G$. (Provjerite još jednom direktnim uvrštavanjem da je $x * y = y * x = 10$.)

Pokazali smo, eksplicitno provjeravajući sve aksiome grupe, da je $(G, *)$ Abelova grupa. ♡

Napomena 1.1.14. U Primjeru 6 svojstva asocijativnosti i komutativnosti nisu nipošto očita ni nasljedna, budući da se radilo o 'novoj' operaciji. Ta smo svojstva morali provjeriti eksplicitno - raspisivanjem po definiciji same operacije.

Primjer 7. Simetrična grupa stupnja n.

Neka je S_n skup svih bijektivnih preslikavanja

$$f : \{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\}.$$

Pokažimo da je S_n grupa s obzirom na operaciju komponiranja funkcija. Vrijede sljedeće tvrdnje.

(1) Kompozicija bijekcija je bijekcija. Dakle, $\circ$ je *binarna* operacija na S_n.

(2) Komponiranje funkcija je asocijativno.

(3) Identiteta je bijekcija.

(4) Svaka bijektivna funkcija ima inverz f^{-1} i on je bijekcija.

Komponiranja funkcija općenito nije komutativno. Pokazali smo da je S_n grupa koja se naziva *simetrična grupa stupnja n*.

Bijekciju $f : \{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\}$ još nazivamo *permutacija* i zapisujemo

$$f = \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ f(1) & f(2) & f(3) & \cdots & f(n) \end{pmatrix}.$$

Konkretno, za $n = 4$ i za permutacije $f, g \in S_4$

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix}, \quad g = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix},$$

njihove kompozicije su

$$f \circ g = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix}, \quad g \circ f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 4 & 3 \end{pmatrix}.$$

Inverz od f je

$$f^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix}.$$

Jednostavno možemo ustanoviti da S_n ima konačno mnogo elemenata i to njih $n!$. Pišemo $|S_n| = n!$. Kao ilustraciju navedimo sve elemente grupe S_3:

$$S_3 = \{\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}\}.$$

♡

Zadatak 2. *Neka su $e, f, g \in S_4$ permutacije zadane s*

$$e = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}, \ f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}, \ g = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}.$$

Je li skup $\{e, f, g\}$ grupa s obzirom na kompoziciju permutacija? Ako nije, postoji li permutacije $h \in S_4$ takva da $(\{e, f, g, h\}, \circ)$ bude grupa?

Uputa: Korisno je, premda ne i nužno, poslužiti se tablicom operacije.

Zadatak 3. *Neka je $(G, *)$ grupa. Za svaki $a \in G$ definira se preslikavanje $L_a(x) = a * x$* (množenje slijeva *elementom a) i, analogno, $D_a(x) = x * a$* (množenje zdesna). *Dokažite da su L_a i D_a bijekcije na skupu G. Uočite da su svojstva injektivnosti i surjektivnosti ovih preslikavanja usko povezana (kako?) s rješavanjem jednadžbi iz Propozicije 1.1.11.*

U slučaju kad je G konačan skup, preslikavanja L_a i D_a su onda permutacije skupa G. Razmislite kako se ova svojstva odražavaju na tablicu operacije za konačnu grupu.

Zadatak 4. *U grupi $(G, *)$ možemo promatrati i jednadžbe oblika $x * x = a$, za zadani $a \in G$. Možemo li zaključiti nešto općenito o postojanju i jedinstvenosti rješenja takvih jednadžbi? Posebno, za jednadžbu $x * x = e$? Svoje odgovore argumentirajte primjerima.*

1.1.3 Prsten. Polje.

Dolazimo do algebarskih struktura s dvjema operacijama, zbrajanjem i množenjem, koje su međusobno usklađene svojstvom distributivnosti. U strukturi nazvanoj *polje* bit će moguće izvoditi sve osnovne operacije kako smo već naučeni s racionalnim i realnim brojevima, što obuhvaća i "dijeljenje" (osim, dakako, s nulom). To znači da će se u bilo kojem polju moći rješavati linearne jednadžbe s dvije, tri ili više nepoznanica, a stoga i sustavi linearnih jednadžbi. Struktura *prstena* znatno je restriktivnija, ali prsten cijelih brojeva i prsten polinoma važni su primjeri komutativnih prstena s jedinicom, vrlo korisnih, iako njihovi elementi uglavnom nisu invertibilni za operaciju množenja.

Definicija 1.1.15. *Neka je R neprazan skup na kojem su definirane dvije binarne operacije $+$ i $\cdot$. Kažemo da je uređena trojka $(R, +, \cdot)$* ***prsten*** *ako vrijedi*

(i) *$(R, +)$ je Abelova grupa,*

(ii) *$(R, \cdot)$ je polugrupa (to jest operacija $\cdot$ je asocijativna),*

(iii) distributivnost *operacije $\cdot$ obzirom na operaciju $+$:*

$$a(b + c) = ab + ac, \quad (a + b)c = ac + bc,$$

za sve $a, b, c \in R$.

Neutralni element grupe $(R, +)$ naziva se nula *i označava s 0. Ako postoji neutralni element strukture $(R, \cdot)$ onda se on naziva* jedinica *i označava s 1, a $(R, +, \cdot)$ se tada naziva* ***prsten s jedinicom****. Ako je operacija $\cdot$ komutativna, onda govorimo o* ***komutativnom prstenu****.*

Prsten koji se sastoji samo od jednog elementa, a taj je neutralni element za zbrajanje i za množenje, tzv. je *trivijalni prsten* $(\{0\}, +, \cdot)$. Nadalje ćemo pod pojmom *prsten* uglavnom smatrati da je riječ o netrivijalnom prstenu, a katkad ćemo to ipak i naglasiti.

Sljedeća propozicija pokazuje svojstvo prstena na koje smo naviknuti iz otprije poznatih primjera, da je umnožak bilo kojeg elementa s 0 jednak 0. To ujedno pokazuje da u netrivijalnom prstenu 0 nema multiplikativni inverz,

Propozicija 1.1.16. *Neka je $(R, +, \cdot)$ prsten. Tada je $a \cdot 0 = 0 \cdot a = 0$ za sve $a \in R$.*

Dokaz. Vrijedi

$$a \cdot 0 = a \cdot (0 + 0) = a \cdot 0 + a \cdot 0.$$

Pribrajanjem suprotnog elementa od $a \cdot 0$ jednakosti $a \cdot 0 = a \cdot 0 + a \cdot 0$ slijedi tvrdnja. (Ovo posljednje slijedi i prema Propoziciji 1.1.12 primijenjenom na grupu $(R, +)$.) □

Zadatak 5. *Dokažite da u svakom prstenu vrijedi*

$$a(-b) = (-a)b = -(ab).$$

Posebno, u prstenu s jedinicom vrijedi

$$(-1)a = a(-1) = -a.$$

Primijetimo da smo se u dokazu Propozicije 1.1.16 (a također i u prethodnom zadatku) morali poslužiti svojstvom distributivnosti, jer 0, kao neutralni element za zbrajanje, nema nikakvu posebnu ulogu kod množenja, ako ne iskoristimo distributivnost kojom su te operacije povezane. Uočimo još da u svakom prstenu možemo pomnožiti izraze poput $(a + b)(c + d)$ primjenom distributivnosti, no treba pripaziti vrijedi li u pojedinom prstenu i komutativnost množenja. Primjerice,

$$(a + b)^2 = (a + b)(a + b) = a^2 + ab + ba + b^2$$

ili

$$(a + b)(a - b) = a^2 - ab + ba - b^2,$$

ali poznate formule za kvadriranje i za razliku kvadrata primjenjive su samo ako elementi a i b komutiraju (što ne vrijedi općenito, ali vrijedi u komutativnom prstenu).

Propozicija 1.1.17. *Neka je $(R, +, \cdot)$ netrivijalni prsten i neka su elementi $a, b \in R$ invertibilni. Tada je $ab \neq 0$.*

Dokaz. Pretpostavimo suprotno $ab = 0$. Množenjem slijeva inverzom od a dobivamo $b = a^{-1} \cdot 0$, pa prema Propoziciji 1.1.16 slijedi $b = 0$, a to je u proturječju da je b invertibilan. □

U prstenu je općenito moguće postojanje tzv. *djelitelja nule*, a to su elementi prstena takvi da je njihov umnožak jednak 0 iako je svaki od njih različit od 0. To nam se može učiniti čudnim, jer se to ne može dogoditi za cijele, racionalne, realne niti za kompleksne brojeve.

Prethodne dvije propozicije "sugeriraju" da je smisleno promatrati strukturu definiranu na sljedeći način.

Definicija 1.1.18. *Komutativni prsten s jedinicom* $(R,+,\cdot)$ *u kojem je svaki element* $x \in R\backslash\{0\}$ *invertibilan naziva se* ***polje***. *Polje se često označava s* $\mathbb{F}$.

Na drugi način možemo reći da je $(\mathbb{F},+,\cdot)$ polje ako su $(\mathbb{F},+)$ i $(\mathbb{F},\cdot)$ grupoidi takvi da vrijedi:

(i) $(\mathbb{F},+)$ je Abelova grupa,

(ii) $(\mathbb{F}^*,\cdot)$ je Abelova grupa ($\mathbb{F}^* = \mathbb{F}\backslash\{0\}$),

(iii) *distributivnost* operacije $\cdot$ s obzirom na operaciju $+$.

Uočimo da su neutralni elementi za operacije $+$ i $\cdot$, dakle 0 i jedinica, nužno različiti, jer je F^* grupa pa se podrazumijeva da je to neprazan skup. Budući da je $(F,\cdot)$ grupoid, definirani su elementi $a \cdot 0$ i $0 \cdot a$ za svaki $a \in \mathbb{F}$. Nije nužno uvrstiti u definiciju zahtjev da bude $a \cdot 0 = 0 \cdot a = 0$, jer se to može dokazati. Jednakost $0 \cdot 0 = 0$ dokaže se kao u Propoziciji 1.1.16. Ako bi za neki $a \neq 0$ vrijedilo $a \cdot 0 = b$ i $b \neq 0$, slijedilo bi $0 = a^{-1}b$, što je različito od 0, dakle proturječje.

Koristeći tvrdnje i primjere iz prethodnog poglavlja možemo zaključiti sljedeće.

- $(\mathbb{Z},+,\cdot)$ je komutativni prsten s jedinicom.
- $(\mathbb{Q},+,\cdot)$, $(\mathbb{R},+,\cdot)$ i $(\mathbb{C},+,\cdot)$ su polja.
- $(\mathbb{Z}_m,+_m,\cdot_m)$ je komutativni prsten s jedinicom koji se naziva *prsten cijelih brojeva modulo m*. $(\mathbb{Z}_m,+_m,\cdot_m)$ je polje ako i samo ako je $m = p$ prost broj. $\mathbb{Z}_p$ je važan primjer tzv. *konačnog* polja, to jest polja s konačno mnogo elemenata.

  Uočimo da npr. u prstenu $(\mathbb{Z}_6,+_6,\cdot_6)$ postoje djelitelji nule, jer je $2 \cdot 3 = 0 \pmod 6$, a također i $3 \cdot 4 = 0 \pmod 6$. Općenito, ako je m složeni broj, u prstenu $(\mathbb{Z}_m,+_m,\cdot_m)$ postoje djelitelji 0 (zašto ?) tako da takav prsten ne može biti polje (v. Propoziciju 1.1.17). Na postojanje djelitelja nule trebat ćemo se kasnije naviknuti i kod množenja kvadratnih matrica.
- $(\mathcal{P},+,\cdot)$ je komutativni prsten s jedinicom ($e(x) = 1$ za sve x). Često se $\mathcal{P}$ naziva *prsten polinoma*. Nadalje, za prstene polinoma još se koriste oznake $\mathbb{Z}[x]$, $\mathbb{Q}[x]$, $\mathbb{R}[x]$ u ovisnosti u tome iz kojeg od skupova se uzimaju koeficijenti polinoma ($\mathbb{Z}$, $\mathbb{Q}$ ili $\mathbb{R}$).
- $(\mathbb{Q}(\sqrt{2}),+,\cdot)$ je polje (što je pokazanu u Primjeru 5). Općenito, za broj $d \in \mathbb{N}$ koji nije potpuni kvadrat definira se

  $$\mathbb{Q}(\sqrt{d}) = \{a + b\sqrt{d} \,:\, a,b \in \mathbb{Q}\}$$

  i pokazuje (slično kao u Primjeru 5) da je $(\mathbb{Q}(\sqrt{d}),+,\cdot)$ polje. Naziv mu je *kvadratno polje*. (Za d koji jest potpun kvadrat je $\mathbb{Q}(\sqrt{d}) = \mathbb{Q}$, a ako nije, onda vrijedi $\mathbb{Q} \subset \mathbb{Q}(\sqrt{d})$).

1.2 Definicija i osnovna svojstva vektorskog prostora. Primjeri

Slijedi definicija ključnog pojma, a to je vektorski prostor. Ta definicija može se činiti opsežnom i pritom zahtjevnom za razumijevanje, no budući da smo već upoznati sa strukturom Abelove grupe, preostaje još pridodati operaciju množenja elemenata te grupe elementima nekog polja, "skalarima" (najčešće realnim ili kompleksnim brojevima). Ta nova operacija nije binarna, nego "hibridna" jer po jednom skalaru i vektoru pridružuje ponovno vektor. Svojstva propisana za tu operaciju podudaraju se sa svojstvima poznatima za množenje vektora iz prostora V^3 realnim brojevima pa neće biti teško naviknuti se na njih.

Počevši od same definicije, služit ćemo se najjednostavnijim oznakama kakve su uobičajene za vektorske prostore. To znači da će jednaku oznaku $+$ imati operacije u dvjema različitim Abelovim grupama, zbrajanje vektora i zbrajanje skalara u polju, a da se za množenje u polju neće upotrebljavati nikakva posebna oznaka. Za umnožak skalara i vektora samo privremeno pisat će se oznaka $\cdot$ koju ćemo kasnije izostavljati, jer će iz oblika zapisa uvijek biti jasno koja se operacija primjenjuje. Naglašavamo, ipak, kako je riječ o ukupno četiri različite operacije, od toga tri binarne i jednoj "hibridnoj", a u zapisivanju računa poput

$$(\alpha+\beta)\cdot(a+b)=\alpha\cdot a+\beta\cdot a+\alpha\cdot b+\beta\cdot b$$

ili, još jednostavnije,

$$(\alpha+\beta)(a+b)=\alpha a+\beta a+\alpha b+\beta b,$$

podrazumijevat će se da $\alpha+\beta$ predstavlja zbroj skalara, $a+b$ zbroj vektora, dok je $\alpha\cdot a$ odnosno αa umnožak vektora a skalarom α.

Definicija 1.2.1. *Neka je $(V,+)$ Abelova grupa, a $\mathbb{F}$ polje. Ako je zadano preslikavanje $\cdot:\mathbb{F}\times V\to V$ koje zadovoljava sljedeća svojstva:*

(1) $\alpha\cdot(\beta\cdot a)=(\alpha\beta)\cdot a$, *za sve* $\alpha,\beta\in\mathbb{F}$, $a\in V$, *(kvaziasocijativnost)*

(2) $(\alpha+\beta)\cdot a=\alpha\cdot a+\beta\cdot a$, *za sve* $\alpha,\beta\in\mathbb{F}$, $a\in V$,
(distributivnost operacije $\cdot$ u odnosu na zbrajanje u $\mathbb{F}$)

(3) $\alpha\cdot(a+b)=\alpha\cdot a+\alpha\cdot b$, *za sve* $\alpha\in\mathbb{F}$, $a,b\in V$,
(distributivnost operacije $\cdot$ u odnosu na zbrajanje u V)

(4) $1\cdot a=a$, *za sve* $a\in V$.,

*tada se uređena trojka $(V,+,\cdot)$ naziva **vektorski** ili **linearni prostor nad poljem** $\mathbb{F}$. Ako je $\mathbb{F}=\mathbb{R}$ onda govorimo o **realnom vektorskom prostoru**, a ako je $\mathbb{F}=\mathbb{C}$ onda o **kompleksnom vektorskom prostoru**.*

*Elemente skupa V zovemo **vektorima**, a elemente polja $\mathbb{F}$ **skalarima**. Neutralni element (nulu) Abelove grupe $(V,+)$ zovemo **nulvektor** i označavamo s 0_V.*

*Operaciju $\cdot$ nazivamo **množenje vektora skalarom** i umjesto $\alpha\cdot a$ često pišemo αa.*

Skup koji se sastoji samo od nulvektora, $\{0_V\}$ također je vektorski prostor, a nazivamo ga trivijalni prostor.

Navedimo nekoliko napomena o načinu označavanja. Vektorski prostor $(V, +, \cdot)$ kratko označavat ćemo s V. Elemente vektorskog prostora V, vektore, označavat ćemo najčešće s a, b, ..., x, y, v (dakle bez strelice!). Ponekad, gdje je iz konteksta nedvosmisleno, nul-vektor 0_V označava se samo s 0. Skalare polja $\mathbb{F}$ označavamo, u pravilu, malim slovima grčkog alfabeta α, β, ..., λ, μ, ...

Primjer 8. Vektorski prostori V^1, V^2 i V^3.

Na kolegiju *Analitička geometrija* proučavali smo skup vektora, to jest skup klasa usmjerenih (orijentiranih) dužina na pravcu (V^1), u ravnini (V^2) i u prostoru (V^3). U onom što slijedi pišemo samo V^3, a sve tvrdnje se odnose i na V^1 i V^2. Na skupu V^3 smo definirali zbrajanje vektora pomoću pravila trokuta na odgovarajućim predstavnicima,

$$\vec{a} + \vec{b} = [\overrightarrow{AB}] + [\overrightarrow{BC}] = [\overrightarrow{AC}].$$

Budući da smo pokazali da je ovako zadana binarna operacija asocijativna i komutativna, zatim da postoji neutralni element $\vec{0} = [\overrightarrow{AA}]$, te je svakom vektoru $\vec{a} = [\overrightarrow{AB}]$ suprotan $[\overrightarrow{BA}] = -\vec{a}$, zaključujemo da je $(V^3, +)$ Abelova grupa.

Operacija množenja vektora skalarom uređenom paru $(\alpha, \vec{a})$, $\alpha \in \mathbb{R}\backslash\{0\}$, $\vec{a} \in V^3\backslash\{\vec{0}\}$, pridružuje vektor $\alpha\vec{a}$ čiji je modul $|\alpha||\vec{a}|$, smjer isti kao smjer vektora $\vec{a}$ i orijentacija ista kao $\vec{a}$ ako je $\alpha > 0$, odnosno suprotna ako $\alpha < 0$. U trivijalnom slučaju ($\alpha = 0$ ili $\vec{a} = \vec{0}$) je $\alpha\vec{a} = \vec{0}$. Pokazali smo da su zadovoljena svojstva (1) do (4) Definicije 1.2.1, pa je $(V^3, +, \cdot)$ vektorski prostor. Na sličan način se utvrđuje da je i skup radijvektora $V^3(O)$ vektorski prostor.

♡

U sljedeće tri propozicije sadržana su svojstva koja vrijede u svakom vektorskom prostoru V.

Propozicija 1.2.2. *Vrijedi*

(i) $0 \cdot a = 0_V$, *za sve* $a \in V$,

(ii) $\alpha \cdot 0_V = 0_V$, *za sve* $\alpha \in \mathbb{F}$.

Dokaz. **(i)** S jedne strane je $a = a + 0_V$ a s druge $a = (1+0)a = 1 \cdot a + 0 \cdot a = a + 0 \cdot a$. Stoga je

$$a + 0_V = a + 0 \cdot a,$$

pa pribrajanjem suprotnog vektora $-a$ prethodnoj jednakosti slijedi $0 \cdot a = 0_V$.

(ii) Iz $\alpha a = 0_V + \alpha a$ a s druge $\alpha a = \alpha(0_V + a) = \alpha 0_V + \alpha a$ je

$$0_V + \alpha a = \alpha 0_V + \alpha a.$$

Pribrajanjem suprotnog vektora $-\alpha a$ prethodnoj jednakosti slijedi $\alpha 0_V = 0_V$.

□

Uočimo da smo u vektorskom prostoru V^3 (odnosno V^1 i V^2) definirali da je $\alpha \cdot \vec{0} = \vec{0}$ i $0 \cdot \vec{a} = \vec{0}$ pa Propoziciju 1.2.2 nismo trebali dokazivati.

Propozicija 1.2.3. $\alpha \cdot a = 0_V$ *ako i samo ako je* $\alpha = 0$ *ili* $a = 0_V$.

Dokaz. Dovoljnost slijedi iz Propozicije 1.1.11.

Pokažimo nužnost. Pretpostavimo da je $\alpha \cdot a = 0_V$. Ako je $\alpha = 0$, onda smo pokazali tvrdnju. Stoga, pretpostavimo da $\alpha \neq 0$. Stoga postoji inverz $\alpha^{-1} \in \mathbb{F}$. Vrijedi da je

$$a = (\alpha^{-1}\alpha)a = \alpha^{-1}(\alpha a) = \alpha^{-1}0_V = 0_V,$$

što je i trebalo pokazati. □

Propozicija 1.2.4. *Vrijedi*

$$(-\alpha)a = -(\alpha a) = \alpha(-a),$$

za sve $\alpha \in F$ *i* $a \in V$.

Dokaz. Kako je

$$(-\alpha)a + \alpha a = (-\alpha + \alpha)a = 0 \cdot a = 0_V,$$

slijedi da je suprotan vektor od αa, to jest $-(\alpha a)$ jednak vektoru $(-\alpha)a$. □

Prethodna propozicija posebno kaže da je suprotan vektor od a jednak umnošku vektora a skalarom -1, to jest $-a = (-1)a$.

U nizu primjera koji slijede, pokazat ćemo da mnogi matematički objekti (uređene n-torke, polinomi, funkcije, ...) imaju 'karakter' vektora.

Primjer 9. Koordinatni prostor $\mathbb{R}^n$.

Neka je $n \in \mathbb{N}$ i $\mathbb{R}^n$ skup svih uređenih n-torki realnih brojeva, odnosno

$$\mathbb{R}^n = \mathbb{R} \times \mathbb{R} \times \cdots \times \mathbb{R} = \{(x_1, x_2, \ldots, x_n) \,:\, x_1, x_2, \ldots, x_n \in \mathbb{R}\}.$$

Uz prirodno definirano zbrajanje po koordinatama (ili koordinatno zbrajanje),

$$(x_1, x_2, \ldots, x_n) + (y_1, y_2, \ldots, y_n) = (x_1 + y_1, x_2 + y_2, \ldots, x_n + y_n),$$

je $(\mathbb{R}^n, +)$ Abelova grupa. Množenje uređene n-torke realnim brojem α definira se također koordinatno,

$$\alpha \cdot (x_1, x_2, \ldots, x_n) = (\alpha x_1, \alpha x_2, \ldots, \alpha x_n).$$

Budući da su obje operacije definirane koordinatno, lako se može ustanoviti da je $(\mathbb{R}^n, +, \cdot)$ realan vektorski prostor koji se ponekad naziva *realan n-dimenzionalni koordinatni prostor.*

Općenito, svaki skup uređenih n-torki elemenata iz nekog polja $\mathbb{F}$, $\mathbb{F}^n$, uz koordinatno definirane operacije zbrajanja i množenja (iz polja) bit će vektorski prostor nad poljem $\mathbb{F}$. U skladu s ovom opaskom, istaknimo vektorski prostor $(\mathbb{Z}_p^n, +_p, \cdot_p)$ s konačno mnogo elemenata (p^n).

Posebno, za $n = 1$ dobivamo da je polje $\mathbb{F}$ vektorski prostor *nad samim sobom.* Pri tome, elementi polja imaju dvostruku ulogu - oni su i vektori i skalari, a operacija množenja iz polja predstavlja operaciju množenja skalarom.

♡

Primjer 10. Kompleksni brojevi.

Kao što smo vidjeli u prethodnom primjeru, polje kompleksnih brojeva $\mathbb{C}$ možemo shvatiti i kao vektorski prostor nad samim sobom. No, možemo ga shvatiti i kao vektorski prostor nad poljem $\mathbb{R}$, odnosno kao realan vektorski prostor. U tom slučaju koristimo oznaku $\mathbb{C}_{\mathbb{R}}$.

Općenito, svaki vektorski prostor nad $\mathbb{C}$ je ujedno vektorski prostor nad $\mathbb{R}$.

♡

Primjer 11. Prostor nizova.

Neka je
$$\mathbb{R}^{\mathbb{N}} = \{(x_i) \, : \, x_i \in \mathbb{R}\}$$
skup svih nizova realnih brojeva. Uz koordinatno zbrajanje i množenje skalarom
$$(x_i) + (y_i) = (x_i + y_i), \quad \alpha(x_i) = (\alpha x_i),$$
$\mathbb{R}^{\mathbb{N}}$ je realan vektorski prostor.

♡

Primjer 12. Prostor polinoma.

Neka je $n \in \mathbb{N}$. S $\mathcal{P}_n$ smo označili skup svih polinoma u jednoj varijabli s realnim koeficijentima stupnja manjeg ili jednakog n zajedno s nulpolinomom,
$$\mathcal{P}_n = \{p \, : \, \mathrm{st}(p) \leq n\} \cup \{p \, : \, p(x) = 0, x \in \mathbb{R}\}.$$
U prethodnom odsječku ustanovili smo da je $\mathcal{P}_n$ uz uobičajeno zbrajanje polinoma Abelova grupa. Množenje polinoma p realnim brojem α definiramo prirodno, $\alpha p : \mathbb{R} \to \mathbb{R}$ je polinom definiran s
$$(\alpha p)(x) = \alpha(p(x)) = \sum_{i=0}^{n} (\alpha a_i) x^i, \ x \in \mathbb{R},$$
pri čemu je $p(x) = \sum_{i=0}^{n} a_i x^i$. Odmah se vidi da je uz ove operacije $\mathcal{P}_n$ realan vektorski prostor. Analogno, skup svih polinoma u jednoj varijabli s realnim koeficijentima $\mathcal{P}$ je također realan vektorski prostor.

♡

Primjer 13. Prostor funkcija.

Prethodni primjer možemo generalizirati na skup realnih funkcija realne varijable,
$$\mathbb{R}^{\mathbb{R}} = \{f : \mathbb{R} \to \mathbb{R}\}.$$
Operacije zbrajanja i množenja funkcija realnim brojem definiramo *po točkama*. Za $f, g \in \mathbb{R}^{\mathbb{R}}$ i $\alpha \in \mathbb{R}$
$$f + g : \mathbb{R} \to \mathbb{R}, \ (f+g)(t) = f(t) + g(t), \ t \in \mathbb{R}.$$
$$\alpha f : \mathbb{R} \to \mathbb{R}, \ (\alpha f)(t) = \alpha f(t), \ t \in \mathbb{R}.$$
Kako su operacije zadane po točkama, svojstva komutativnosti, asocijativnosti i distributivnosti vrijede jer vrijede u polju $\mathbb{R}$. Neutralni element zbrajanja je funkcija $n(t) = 0$, za sve $t \in \mathbb{R}$. Svaka funkcija f ima svoju suprotnu $-f$, $(-f)(t) = -f(t)$, $t \in \mathbb{R}$. Stoga je $\mathbb{R}^{\mathbb{R}}$ realan vektorski prostor.

♡

Primjer 14. Prostor matrica reda 2.

Uređena četvorka $(a, b, c, d) \in \mathbb{R}^4$ zapisana u kvadratnu shemu

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

naziva se *realna matrica reda* 2. Uobičajeno je matrice označavati velikim tiskanim slovima A, B, ..., te njihove elemente, npr. za matricu A, s a_{ij} gdje indeks upućuje na položaj elementa u matrici - a_{ij} se nalazi na presjeku i-tog retka i j-tog stupca. Dakle,

$$A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}.$$

Skup svih realnih matrica reda 2 označavamo s $M_2(\mathbb{R})$.

Na skupu $M_2(\mathbb{R})$ zbrajanje je definirano po elementima (što upravo odgovara koordinatnom zbrajanju),

$$A + B = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} + \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} = \begin{pmatrix} a_{11} + b_{11} & a_{12} + b_{12} \\ a_{21} + b_{21} & a_{22} + b_{22} \end{pmatrix}.$$

Stoga je ova binarna operacija očito komutativna i asocijativna. Neutralni element zbrajanja je matrica čiji su svi elementi jednaki 0,

$$\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix},$$

a zovemo ju *nulmatrica*. Svaka matrica A ima suprotnu matricu $-A$ danu s

$$-A = \begin{pmatrix} -a_{11} & -a_{12} \\ -a_{21} & -a_{22} \end{pmatrix}.$$

Prema svemu navedenom za zaključiti je da je $(M_2(\mathbb{R}), +)$ Abelova grupa.

Operacija množenja skalarom također se definira prirodno, po elementima (odnosno koordinatno). Za $\alpha \in \mathbb{R}$ i $A \in M_2(\mathbb{R})$ je

$$\alpha A = \alpha \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} = \begin{pmatrix} \alpha a_{11} & \alpha a_{12} \\ \alpha a_{21} & \alpha a_{22} \end{pmatrix}.$$

Jasno je da $M_2(\mathbb{R})$ realan vektorski prostor.

Na isti način, možemo ustanoviti da je skup svih matrica reda 2 čiji su elementi kompleksni brojevi, odnosno kompleksnih matrica reda 2, u oznaci $M_2(\mathbb{C})$ kompleksan vektorski prostor. U skladu s napomenom iz Primjera 10, skup $M_2(\mathbb{C})$ ćemo ponekad shvaćati kao realan vektorski prostor i prema tome označavati s $M_2(\mathbb{C})_{\mathbb{R}}$.

♡

Primjer 15. *'Egzotičan'* vektorski prostor.

Neka je $V = \mathbb{R}^+ = \{a \in \mathbb{R} : a > 0\}$. Za $a, b \in V$ i $\alpha \in \mathbb{R}$ definiramo 'neobične' operacije zbrajanja $\oplus$ i množenja vektora skalarom $\odot$ na sljedeći način:

$$a \oplus b = ab, \quad \alpha \odot a = a^\alpha.$$

Prvo provjerimo da je $(V, \oplus)$ Abelova grupa. Zaista, V je zatvoren u odnosu na operaciju $\oplus$ jer je $ab > 0$ za $a, b > 0$, to jest $a \oplus b \in V$ za sve $a, b \in V$. Operacija $\oplus$ je asocijativna i komutativna jer standardno množenje u $\mathbb{R}$ ima ta svojstva. Neutralni element je $1 \in V$, a inverz od $a \in V$ je $a^{-1} = \frac{1}{a} \in V$.

Sada provjeravamo potrebna svojstva operacije $\odot$. Zatvorenost vrijedi jer je $a^\alpha > 0$ za sve $a > 0$ i $\alpha \in \mathbb{R}$. Ispitujemo kvaziasocijativnost i distributivnosti. Neka su $\alpha, \beta \in \mathbb{R}$ i $a, b \in V$. Vrijedi

$$\alpha \odot (\beta \odot a) = \alpha \odot a^\beta = \left(a^\beta\right)^\alpha = a^{\beta\alpha} = a^{\alpha\beta} = (\alpha\beta) \odot a.$$

Nadalje,

$$(\alpha + \beta) \odot a = a^{\alpha+\beta} = a^\alpha a^\beta = a^\alpha \oplus a^\beta = (\alpha \odot a) \oplus (\beta \odot a),$$

te

$$\alpha \odot (a \oplus b) = \alpha \odot (ab) = (ab)^\alpha = a^\alpha b^\alpha = a^\alpha \oplus b^\alpha = (\alpha \odot a) \oplus (\alpha \odot b).$$

Konačno, jer je $1 \odot a = a^1 = a$, možemo zaključiti da je $(V, \oplus, \odot)$ jedan realan vektorski prostor.

♡

1.3 Linearna ljuska. Sustav izvodnica. Linearna nezavisnost

Višestrukom primjenom operacija zbrajanja vektora i množenja vektora skalarom u vektorskom prostoru dobivamo vektore oblika koji nazivamo *linearna kombinacija* (ili *linearni spoj*) određenih vektora. Linearna kombinacija vektora tipični je izraz pri svakom računu u vektorskom prostoru pa će pojmovi i svojstva povezana s linearnim kombinacijama imati ključnu ulogu u proučavanju i različitim primjenama vektorskih prostora.

Definicija 1.3.1. *Neka je V vektorski prostor nad poljem $\mathbb{F}$, te $k \in \mathbb{N}$. Za α_1, ...,$\alpha_k \in \mathbb{F}$ i a_1, ..., $a_k \in V$ vektor oblika*

$$\alpha_1 a_1 + \cdots + \alpha_k a_k$$

nazivamo ***linearna kombinacija vektora*** *a_1, ..., a_k s koeficijentima α_1, ...,α_k. Primjenom uobičajenog simbola $\sum$ za sumu, linearnu kombinaciju vektora a_1, ..., a_k sažeto zapisujemo kao $\sum_{i=1}^k \alpha_i a_i$.*

Neka je $S \subseteq V$, $S \neq \emptyset$. Skup svih linearnih kombinacija vektora iz S naziva se ***linearna ljuska*** *ili* ***linearni omotač skupa*** *S i označava $[S]$. Dakle,*

$$[S] = \{\alpha_1 a_1 + \cdots + \alpha_n a_n \,:\, n \in \mathbb{N}, a_1, \ldots, a_n \in S, \alpha_1, \ldots, \alpha_n \in \mathbb{F}\}.$$

Ako je $S = \{a_1, \ldots, a_k\}$, onda je

$$[S] = [\{a_1, \ldots, a_k\}] = \{\alpha_1 a_1 + \cdots + \alpha_k a_k \,:\, \alpha_1, \ldots, \alpha_k \in \mathbb{F}\},$$

te skup $[\{a_1, \ldots, a_k\}]$ (u oznaci i $[a_1, \ldots, a_k]$) nazivamo linearnom ljuskom *ili* linearnim omotačem vektora a_1, ..., a_k.

Za prazan skup definira se njegova linearna ljuska kao $[\emptyset] = \{0_V\}$.

Radi jednostavnosti zapisa, katkad ćemo izostaviti vitičaste zagrade pa linearnu ljusku zadanog skupa vektora, $\{a_1, \ldots, a_k\}$, kraće pisati kao $[a_1, \ldots, a_k]$.

Primijetimo da zahvaljujući svojstvima asocijativnosti i komutativnosti zbrajanja vektora pojedinu linearnu kombinaciju možemo pisati na više načina, a da se rezultat ne promijeni. Možemo mijenjati poredak pribrojnika odnosno grupirati pribrojnike po volji, npr.

$$2a - 5b + 2c - 3d = 2a + 2c - 5b - 3d = (2a + 2c) + (-5b - 3d),$$

za vektore $a, b, c, d \in V$. (Dakako, isti vektor dobivamo daljnjim pojednostavljivanjem zapisa i primjenom poznatih svojstava operacija u V, ako želimo, npr. kao $2(a + c) - (5b + 3d)$). Nadalje, uočimo što je sve varijabilno u definiciji linearne ljuske skupa S. Prvo, to je $n \in \mathbb{N}$ koji označava koliko se vektora iz S uzima u linearnu kombinaciju, zatim varijabilan je izbor n vektora iz S i izbor n skalara iz $\mathbb{F}$ kao koeficijenata. Pritom linearne kombinacije dobivene različitim izborom vektora i skalarnih koeficijenata općenito ne daju različite vektore, premda formalno "izgledaju različito".

Uočimo da iz definicije linearne ljuske lako slijede sljedeća jednostavna, ali praktično važna svojstva:

- Za bilo koji $S \subseteq V$ vrijedi: $S \subseteq [S] \subseteq V$ te $[[S]] = [S]$.
- Ako su $S_1, S_2 \subseteq V$ i $S_1 \subseteq S_2$, onda je $[S_1] \subseteq [S_2]$.

Također, čim je polje $\mathbb{F}$ beskonačan skup, npr. polje $\mathbb{R}$, postoji beskonačno mnogo linearnih kombinacija vektora skupa S različitog od $\{0_V\}$. Uskoro ćemo se naviknuti na činjenicu da linearna ljuska "malenog" skupa vektora može biti cijeli vektorski prostor, a upravo to bit će nam od bitne važnosti.

Propozicija 1.3.2. *Neka je V vektorski prostor nad poljem $\mathbb{F}$, $S \neq \emptyset$ i $S \subseteq V$. Onda je $[S]$ vektorski prostor nad poljem $\mathbb{F}$ obzirom na iste operacije zbrajanja i množenja skalarom koje su definirane u prostoru V.*

Dokaz.

- Neka su $x, y \in [S]$. Tada su vektori x i y linearne kombinacije vektora iz S pa je to i vektor $x + y$. Stoga je zbrajanje vektora binarna operacija na $[S]$.
- Svojstva asocijativnosti i komutativnosti nasljeđuju se jer je $[S] \subseteq V$.
- Neutralni element zbrajanja vektora, nulvektor, nalazi se u $[S]$ jer je $0_V = 0 \cdot a$ za bilo koji $a \in S$.
- Za $x \in [S]$, postoje a_1, ..., $a_k \in S$ i α_1, ...,$\alpha_k \in \mathbb{F}$ takvi da je $x = \alpha_1 a_1 + \cdots + \alpha_k a_k$. Suprotni vektor od x je $-x = (-\alpha_1)a_1 + \cdots + (-\alpha_k)a_k$ pa je $-x \in [S]$.

Sada možemo zaključiti da je $([S], +)$ Abelova grupa. Ustanovimo da vrijede i ostala svojstva vektorskog prostora.

- Neka je $x = \alpha_1 a_1 + \cdots + \alpha_k a_k \in [S]$. Onda je $\lambda x = (\lambda\alpha_1)a_1 + \cdots + (\lambda\alpha_k)a_k \in [S]$ za sve $\lambda \in \mathbb{F}$.
- Kvaziasocijativnost i distributivnosti se nasljeđuju iz vektorskog prostora V.

Dakle, $[S]$ je vektorski prostor nad poljem $\mathbb{F}$ obzirom na operacije iz V. $\square$

Na ovom mjestu može se učiniti zbunjujućom činjenica da je linearna ljuska podskupa S vektorskog prostora V također vektorski prostor, a jasno je da je $[S]$ podskup od V. Posebno će istaknut biti slučaj kad je $[S]$ jednak cijelom prostoru V, no općenito nije tako.

Na primjeru vektorskog prostora V^3 ili $V^3(O)$ možemo lako uočiti neke podskupove kojima je linearna ljuska jednaka cijelom prostoru, kao i podskupove za koje to nije ispunjeno. Razmislite kako može izgledati linearna ljuska $[S]$ za $S \subset V^3(O)$ ako to nije cijeli $V^3(O)$, imajući u vidu prethodnu propoziciju.

Definicija 1.3.3. *Neka je V vektorski prostor nad poljem $\mathbb{F}$ i $G \subseteq V$. Ako je*

$$V = [G],$$

*odnosno ako se svaki vektor iz V može prikazati kao linearna kombinacija (konačno mnogo) vektora iz G, onda kažemo da je G **sustav izvodnica** ili **generatora** za prostor V, odnosno* skup izvodnica *ili* generatora *za V. Još se može reći da skup G **razapinje** ili **generira** prostor V.*

Ako je $V = [G]$, onda za svaki $x \in V$ *postoje* vektori a_1, ..., $a_k \in G$ i skalari α_1, ..., $\alpha_k \in \mathbb{F}$ takvi da se x prikazuje kao

$$x = \alpha_1 a_1 + \cdots + \alpha_k a_k = \sum_{i=1}^{k} \alpha_i a_i.$$

Prikaz vektora x u obliku linearne kombinacije nekih vektora iz skupa S općenito nije jednoznačan, to jest, pojedini vektor općenito se može na više načina prikazati kao linearna kombinacija vektora iz nekog sustava izvodnica. Pitanje jedinstvenosti prikaza je važno, a njime ćemo se baviti nešto kasnije.

Za početak se pitamo postoji li za svaki vektorski prostor V sustav izvodnica i zaključujemo da postoji jer čitav prostor V možemo shvatiti kao sustav izvodnica, to jest $G = V$. Nadalje, ako G generira prostor V, onda ga generira i svaki njegov nadskup. Stoga je prirodno pokušati odrediti najmanji mogući (minimalan) skup koji predstavlja sustav izvodnica. No, prije toga promotrimo primjere nekih sustava izvodnica.

- Ako je $\vec{a} \in V^1$ i $\vec{a} \neq \vec{0}$, onda $\{\vec{a}\}$ generira V^1.
- Neka su $\vec{a}$ i $\vec{b}$ u V^2 nekolinearni vektori. U kolegiju prethodniku, Analitička geometrija, pokazali smo da za svaki $\vec{c} \in V^2$ postoje (jedinstveni) skalari $\alpha, \beta \in \mathbb{R}$ takvi da je $\vec{c} = \alpha\vec{a} + \beta\vec{b}$. Dakle, možemo zaključiti da skup koji se sastoji od bilo koja dva nekolinearna vektora predstavlja sustav izvodnica za V^2.
- Analogno, skup od bilo koja tri nekomplanarna vektora predstavlja sustav izvodnica za V^3.
- Neka je $x = (x_1, x_2)$ proizvoljan vektor iz $\mathbb{R}^2$. Tada je

$$x = x_1(1,0) + x_2(0,1).$$

Zaključujemo da se svi $x = (x_1, x_2) \in \mathbb{R}^2$ mogu zapisati kao linearna kombinacija vektora $e_1 = (1, 0)$ i $e_2 = (0, 1)$ pa je stoga $\{e_1, e_2\}$ sustav izvodnica za $\mathbb{R}^2$.

Općenito, $\mathbb{R}^n = [e_1, e_2, \dots, e_n]$, gdje je $e_1 = (1, 0, \dots, 0)$, $e_2 = (0, 1, \dots, 0)$, ...,$e_n = (0, 0, \dots, 1)$.

- Neka je $S = \{(1, 0), (1, 1), (1, -1)\} \subset \mathbb{R}^2$. Lako se vidi da vrijedi jednakost

$$(x_1, x_2) = (x_1 - x_2)(1, 0) + x_2(1, 1),$$

za sve $(x_1, x_2) \in \mathbb{R}^2$. Stoga je skup $\{(1, 0), (1, 1)\}$ sustav izvodnica za $\mathbb{R}^2$ pa je to i njegov nadskup S. Nadalje, vrijedi da je

$$(x_1, x_2) = (x_1 - x_2 - 2t)(1, 0) + (x_2 + t)(1, 1) + t(1, -1),$$

za sve $(x_1, x_2) \in \mathbb{R}^2$ te proizvoljan $t \in \mathbb{R}$. Dakle, prikaz proizvoljnog vektora iz $\mathbb{R}^2$ kao linearne kombinacije vektora skupa S *nije jednoznačan.* (Štoviše, budući da se $t \in \mathbb{R}$ može izabrati po volji, prikaza ima beskonačno mnogo). Za razliku od toga, vektor iz $\mathbb{R}^2$ se *jednoznačno* prikazuje kao linearna kombinacija vektora $(1, 0)$ i $(1, 1)$.

- Neka je $\{p_0, p_1, \dots, p_n\} \subset \mathcal{P}_n$ pri čemu je $p_i(x) = x^i$ za $i = 0, 1, \dots, n$. Kako je za $p \in \mathcal{P}_n$

$$p(x) = \sum_{i=0}^{n} a_i x^i = \sum_{i=0}^{n} a_i p_i(x),\ \forall x \in \mathbb{R},$$

to jest $p = \sum_{i=0}^{n} a_i p_i$, slijedi da je $\{p_0, \dots, p_n\}$ sustav izvodnica za $\mathcal{P}_n$.

Skup $\{p_0, p_1, p_2, \dots\} \subset \mathcal{P}$ razapinje vektorski prostor $\mathcal{P}$. Uočimo da je $\{p_0, p_1, p_2, \dots\}$ beskonačan skup. Uz to, možemo zaključiti da ne postoji konačan skup polinoma koji razapinje prostor $\mathcal{P}$. Naime, u konačnom skupu polinoma postoji jedan ili više polinoma s najvećim stupnjem u tom skupu, recimo stupnjem m. Linearnim kombinacijama polinoma iz tog skupa ne može se dobiti polinom stupnja većeg od m pa taj skup očito ne može generirati čitav prostor $\mathcal{P}$.

- Kompleksan broj z je oblika $z = \alpha + i\beta$ za neke $\alpha, \beta \in \mathbb{R}$. Ako polje $\mathbb{C}$ shvatimo kao realan vektorski prostor, $\mathbb{C}_{\mathbb{R}}$, onda je skup $\{1, i\}$ očito njegov sustav izvodnica.

  Skup $\{1\}$ ili $\{z\}$ za $z \neq 0$ predstavlja sustav izvodnica za $\mathbb{C}$ - kompleksan vektorski prostor.

Definicija 1.3.4. *Vektorski prostor je* ***konačnogeneriran*** *ako sadrži bar jedan konačan sustav izvodnica.*

Iz gore navedenih primjera možemo zaključiti da su prostori V^1, V^2, V^3, $\mathbb{R}^2$, $\mathcal{P}_n$ konačnogenerirani, dok je $\mathcal{P}$ primjer prostora koji nije konačnogeneriran. Na ovom predmetu ćemo se baviti samo konačnogeneriranim vektorskim prostorima, ali ponekad, radi primjera i usporedbe, spomenut ćemo i neke vektorske prostore koji nisu konačnogenerirani.

Propozicija 1.3.5. *Neka je V vektorski prostor nad poljem $\mathbb{F}$ i $G \subseteq V$ skup izvodnica prostora V. Ako se vektor $a \in G$ može prikazati kao linearna kombinacija* preostalih *vektora iz G, onda je $G \backslash \{a\}$ također skup izvodnica prostora V.*

Dokaz. Proizvoljan vektor x iz V može se prikazati kao linearna kombinacija nekih vektora iz G pa pretpostavimo da je

$$x = \alpha a + \sum_{i=1}^{n} \beta_i b_i,$$

za $b_1, \dots, b_n \in G \backslash \{a\}$ i $\alpha, \beta_1, \dots, \beta_n \in \mathbb{F}$. Nadalje, $a \in G$ se može prikazati kao linearna kombinacija vektora iz $G \backslash \{a\}$, pa postoje $b'_1, \dots, b'_k \in G \backslash \{a\}$ i $\beta'_1, \dots, \beta'_k \in \mathbb{F}$ takvi da je

$$a = \sum_{j=1}^{k} \beta'_j b'_j.$$

Stoga je

$$x = \alpha(\sum_{j=1}^{k} \beta'_j b'_j) + \sum_{i=1}^{n} \beta_i b_i = \sum_{j=1}^{k} (\alpha \beta'_j) b'_j + \sum_{i=1}^{n} \beta_i b_i,$$

odnosno x je linearna kombinacija vektora iz $G \backslash \{a\}$. $\square$

Primijetimo da se za $S \subseteq V$ i bez pretpostavke da je S sustav izvodnica može ustvrditi: za $a \in S$ vrijedi

$$a \in [S \backslash \{a\}] \;\Leftrightarrow\; [S \backslash \{a\}] = [S].$$

Argument je isti kao u dokazu prethodne propoziciji, samo što se promatra prikaz bilo kojeg vektora $x \in [S]$ (a to nije nužno cijeli V kao $[S]$).

Već smo spomenuli da nas zanima odrediti što je moguće manji sustav izvodnica. Propozicija 1.3.5 nam kaže kako operativno smanjiti skup izvodnica konačnogeneriranog vektorskog prostora. Dakle, svaki vektor koji je linearna kombinacija preostalih vektora izbacujemo iz sustava izvodnica i na taj način dobijemo novi sustav izvodnica kojem se broj vektora smanji za jedan (uz pretpostavku da smo krenuli od konačnog skupa izvodnica). Ponavljajući postupak doći ćemo do *minimalnog* skupa izvodnica, to jest do skupa u kojem se niti jedan vektor ne može prikazati kao linearna kombinacija preostalih. Vidjet ćemo da je takav skup karakteriziran svojstvom *linearne nezavisnosti.*

Definicija 1.3.6. *Neka je V vektorski prostor nad poljem $\mathbb{F}$ i neka je $S = \{a_1, \dots, a_k\}$ njegov podskup. Kažemo da je S **linearno nezavisan** skup vektora ako se nulvektor 0_V može na jedinstven način prikazati pomoću vektora iz S, to jest ako iz*

$$\alpha_1 a_1 + \alpha_2 a_2 + \cdots + \alpha_k a_k = 0_V \tag{1.4}$$

*slijedi da je $\alpha_1 = \alpha_2 = \cdots = \alpha_k = 0$. U suprotnom, to jest ako postoji izbor skalara α_1, $\dots$, α_k takav da je bar jedan skalar $\alpha_i \neq 0$ i da vrijedi (1.4), onda kažemo da je skup S **linearno zavisan**.*

Često kažemo da S linearno nezavisan ako je prikaz nulvektora u (1.4) *nužno* trivijalan, odnosno ako je (1.4) moguć *samo za trivijalan izbor* skalara $\alpha_1, \ldots, \alpha_k$, dakle da su svi α_i jednaki nuli. S je linearno zavisan ako u (1.4) imamo *netrivijalan* prikaz, odnosno ako postoji *netrivijalan izbor skalara* $\alpha_1, \ldots, \alpha_k$ za koje vrijedi (1.4).

Napomenimo da se Definicija 1.3.6 odnosi samo na konačne skupove, a mi ćemo samo takve i promatrati. *Beskonačan* skup je *linearno nezavisan* samo ako je svaki njegov konačan podskup linearno nezavisan, odnosno *linearno zavisan* ako postoji bar jedan konačan podskup koji je linearno zavisan.

Prisjetimo se nekih primjera linearno nezavisnih skupova vektora o kojima je bilo riječi u *Analitičkoj geometriji*.

- Neka su $\vec{a}, \vec{b}$ u V^2 (ili u V^3) nekolinearni. Onda je skup $\{\vec{a}, \vec{b}\}$ linearno nezavisan.
- Neka su $\vec{a}, \vec{b}, \vec{c}$ u V^3 nekomplanarni. Onda je skup $\{\vec{a}, \vec{b}, \vec{c}\}$ linearno nezavisan.
- Neka su $e_1 = (1, 0)$ i $e_2 = (0, 1)$ iz $\mathbb{R}^2$. Tada je skup $\{e_1, e_2\}$ linearno nezavisan. Zaista, iz
$$\alpha e_1 + \beta e_2 = 0_V,$$
odnosno $\alpha(1, 0) + \beta(0, 1) = (\alpha, \beta) = (0, 0)$, slijedi $\alpha = 0$ i $\beta = 0$.

  Općenito, skup $\{e_1, e_2, \ldots, e_n\}$ u $\mathbb{R}^n$ je linearno nezavisan.
- Skup $\{p_0, p_1, \ldots, p_n\}$ je linearno nezavisan u prostoru $\mathcal{P}$. Zaista, iz
$$\sum_{i=0}^{n} \alpha_i p_i = 0_{\mathcal{P}},$$
pri čemu smo s $0_{\mathcal{P}}$ označili nulpolinom, slijedi da je
$$\sum_{i=0}^{n} \alpha_i p_i(x) = 0,$$
za sve $x \in \mathbb{R}$, a to je jedino moguće za $\alpha_0 = \cdots = \alpha_n = 0$ (Teorem o nulpolinomu).

Propozicija 1.3.7. *Jednočlan skup, $S = \{a\}$, linearno je nezavisan ako i samo ako je $a \neq 0_V$.*

Dokaz. Pokazujemo nužnost: ako je $\{a\}$ je linearno nezavisan, onda je $a \neq 0_V$. Obrat po kontrapoziciji te tvrdnje kaže: ako je $a = 0_V$, onda je $\{a\}$ je linearno zavisan. Zaista, prema Propoziciji 1.2.3 jednakost $\alpha \cdot a = \alpha \cdot 0_V = 0_V$ vrijedi za sve $\alpha \in \mathbb{F}$, pa je ispunjena netrivijalno (npr. za $\alpha = 1$).

Obratno, pretpostavimo da $a \neq 0_V$. Prema Propoziciji 1.2.3 jednakost $\alpha a = 0_V$ povlači da je $\alpha = 0$ (jer $a \neq 0_V$). Stoga je $S = \{a\}$ linearno nezavisan. $\square$

Korolar 1.3.8. *Jednočlan skup, $S = \{a\}$, linearno je zavisan ako i samo je $a = 0_V$.*

Propozicija 1.3.9. **(i)** *Podskup linearno nezavisnog skupa je linearno nezavisan.*

(ii) *Nadskup linearno zavisnog skupa je linearno zavisan.*

Dokaz. **(i)** Neka je $S = \{a_1, a_2, \ldots, a_n\}$ linearno nezavisan skup, te S_1 neki njegov pravi podskup. Bez smanjenja općenitosti pretpostavimo da se S_1 sastoji od prvih $1 \leq k < n$ vektora skupa S, $S_1 = \{a_1, a_2, \ldots, a_k\}$. Nadalje, pretpostavimo suprotno da je S_1 linearno zavisan. Tada postoje skalari α_1, ..., α_k takvi da je barem jedan $\alpha_j \neq 0$, $1 \leq j \leq k$ i

$$\sum_{i=1}^{k} \alpha_i a_i = 0_V.$$

Stavimo da $\alpha_j = 0$ za sve $j = k+1, \ldots, n$ i ustanovimo da je

$$\sum_{i=1}^{n} \alpha_i a_i = \sum_{i=1}^{k} \alpha_i a_i + \sum_{i=k+1}^{n} 0 \cdot a_i = 0_V$$

jedan netrivijalan prikaz nulvektora pomoću vektora iz S. Dakle, S je linearno zavisan što je u proturječju s početnom pretpostavkom. Znači, S_1 je linearno nezavisan.

(ii) Slično kao u (i), za linearno zavisan skup $S = \{a_1, \ldots, a_k\}$ i njegov nadskup $S_2 = \{a_1, \ldots, a_k, b_1, \ldots, b_n\}$ vrijedi da postoji netrivijalan izbor skalara α_1, ..., α_k, te $\beta_1 = \cdots = \beta_n = 0$ takvi da vrijedi

$$\sum_{i=1}^{k} \alpha_i a_i + \sum_{i=1}^{n} \beta_i b_i = 0_V,$$

pa je i S_2 linearno zavisan skup.

□

Budući da smo ustanovili da je skup $\{0_V\}$ linearno zavisan, imamo sljedeću posljedicu prethodne propozicije.

Korolar 1.3.10. *Svaki skup koji sadrži nulvektor je linearno zavisan.*

Propozicija 1.3.11. *Skup od barem dva vektora je linearno zavisan ako i samo ako se barem jedan vektor iz S može prikazati kao linearna kombinacija preostalih vektora iz S.*

Dokaz. Pretpostavimo da je $S = \{a_1, \ldots, a_n\}$ linearno zavisan i $n > 1$. Postoje skalari α_1, ..., α_n takvi da je $\alpha_i \neq 0$, za neki $i \in \{1, \ldots, n\}$ i $\sum_{i=1}^{n} \alpha_i a_i = 0_V$. Odatle je

$$\alpha_i a_i = (-\alpha_1)a_1 + \cdots + (-\alpha_{i-1})a_{i-1} + (-\alpha_{i+1})a_{i+1} + \cdots + (-\alpha_n)a_n,$$

pa množenjem cijelog izraza s α_i^{-1} (što je moguće jer $\alpha_i \neq 0$) slijedi da je

$$a_i = (-\alpha_1\alpha_i^{-1})a_1 + \cdots + (-\alpha_{i-1}\alpha_i^{-1})a_{i-1} + (-\alpha_{i+1}\alpha_i^{-1})a_{i+1} + \cdots + (-\alpha_n\alpha_i^{-1})a_n,$$

odnosno a_i je linearna kombinacija preostalih vektora iz S.

Obratno, bez smanjenja općenitosti pretpostavimo da se vektor a_n može prikazati kao linearna kombinacija preostalih vektora iz S. Tada postoje skalari α_1, ..., α_{n-1} za koje vrijedi

$$a_n = \alpha_1 a_1 + \cdots + \alpha_{n-1} a_{n-1}.$$

Otuda je

$$0_V = \alpha_1 a_1 + \cdots + \alpha_{n-1} a_{n-1} + (-1) a_n,$$

jedan netrivijalan prikaz nulvektora (jer je $\alpha_n = -1 \neq 0$), pa je skup S linearno zavisan. $\square$

Kao i u primjedbi nakon Propozicije 1.3.5, činjenica da se neki $a \in S$ može prikazati kao linearna kombinacija ostalih vektora iz S sažeto se zapisuje s $a \in [S \backslash \{a\}]$. Tvrdnja prethodne propozicije može se onda formulirati tako da je skup S od barem dva vektora linearno zavisan ako i samo ako postoji $a \in S$, $a \in [S \backslash \{a\}]$.

Pri ispitivanju linearne (ne)zavisnosti zadanog skupa posebno se korisnom pokazuje sljedeća inačica prethodne propozicije, u kojoj se taj skup promatra kao uređen skup. Tada se, umjesto o prikazu vektora pomoću preostalih vektora, govori o prikazu pomoću *prethodnih* vektora, što u konkretnom zadatku može znatno pojednostavniti postupak.

Propozicija 1.3.12. *Neka $S = \{a_1, \ldots, a_k\}$ skup vektora, $k > 1$, uređen u navedenom redoslijedu, pri čemu je $a_1 \neq 0_V$. Tada je S linearno zavisan skup ako i samo ako se bar jedan vektor iz S može zapisati kao linearna kombinacija svojih prethodnika.*

Dokaz. Pretpostavimo da je S linearno zavisan skup. Tada postoji netrivijalan izbor skalara $\alpha_1, \ldots, \alpha_k$ takvih da je

$$\alpha_1 a_1 + \cdots + \alpha_k a_k = 0_V.$$

Neka je α_i zadnji koeficijent koji je različit od nule, to jest $\alpha_i \neq 0$ i $\alpha_{i+1} = \cdots = \alpha_k = 0$ ako $i < k$ ili $\alpha_k \neq 0$ ako $i = k$. Jasno je da je $i > 1$ jer je $a_1 \neq 0_V$. Zaista, u protivnom iz $\alpha_1 a_1 = 0_V$ i $\alpha_1 \neq 0$ slijedi $a_1 = 0_V$ što je u kontradikciji s pretpostavkom. Konačno, množenjem jednakosti

$$\alpha_1 a_1 + \cdots + \alpha_{i-1} a_{i-1} + \alpha_i a_i = 0_V$$

s α_i^{-1} (koji postoji jer je $\alpha_i \neq 0$) dobivamo da je

$$a_i = (-\alpha_i^{-1} \alpha_1) a_1 + \cdots + (-\alpha_i^{-1} \alpha_{i-1}) a_{i-1}.$$

Dakle, $a_i \in [a_1, \ldots, a_{i-1}]$.

Obrat slijedi izravno iz Propozicije 1.3.11. $\square$

Zadatak 6. *Ispitajte linearnu (ne)zavisnost danih skupova u $\mathbb{R}^4$. Uočite u čemu je prednost primjene Propozicije 1.3.12.*

(a) $\{(1,0,1,3), (-1,0,0,2)\}$,

(b) $\{(1,1,2,2), (-1,2,-1,2), (-2,1,-3,0)\}$,

(c) $\{(1,1,0,0), (3,3,0,0), (1,0,0,4), (0,0,-1,2)\}$,

(d) $\{(1,0,1,1), (0,1,-1,2), (2,-1,0,0)\}$.

Zadatak 7. *Ako bar jedan element skupa $[a_1, \ldots, a_n]$ ima jedinstven prikaz u obliku linearne kombinacije elemenata $a_1, \ldots, a_n$, onda je skup $\{a_1, \ldots, a_n\}$ linearno nezavisan. Dokažite tvrdnju.*

1.4 Baza vektorskog prostora. Dimenzija.

Prethodno razmatranje konačnogeneriranih vektorskih prostora dovodi nas do pojmova bitnih za takve prostore i stoga istaknutih u naslovu ovog odjeljka.

Zamisao prikaza svakog vektora pomoću minimalnog sustava izvodnica pokazat će se, kako ćemo sad vidjeti, podudarnom s potrebom da svaki vektor ima jednoznačan prikaz u prikladnom sustavu izvodnica. Obje te poželjne karakteristike sustava izvodnica ostvaruju se svojstvom linearne nezavisnosti i time dolazimo do pojma baze vektorskog prostora.

Kad se jednom izabere baza, svaki vektor jednoznačno je određen uređenom n-torkom koeficijenata svog prikaza u toj bazi, pri čemu je n broj vektora te baze. Kako smo već naviknuti iz vektorskih prostora V^2 i V^3, vektori se na taj način praktički poistovjećuju (identificiraju) s uređenim parovima odnosno uređenim trojkama realnih brojeva, a općenito riječ je onda o uređenim n-torkama skalara iz pripadnog polja $\mathbb{F}$. Dakle, uvođenjem baze zapravo koordinatiziramo vektorski prostor, čime se značajno olakšava izvođenje operacija s vektorima.

Posebnu važnost ima činjenica koja se u površnom pristupu može učiniti "očiglednom", ali se iskazuje jednim od osnovnih teorema linearne algebre, čiji dokaz nije posve jednostavan: *Svake dvije baze vektorskog prostora su jednakobrojne.* To znači da je broj vektora (bilo koje) baze jednoznačno određen za svaki konačnogenerirani vektorski prostor. Taj broj naziva se *dimenzija* vektorskog prostora i predstavlja za njega bitan podatak.

Definicija 1.4.1. *Podskup B vektorskog prostora V je* ***baza*** *prostora V ako je B sustav izvodnica za V i linearno nezavisan skup u V.*

U prethodnom odsječku smo za neke skupove već ustanovili da su sustavi izvodnica i linearno nezavisni u konkretnim vektorskim prostorima.

- Skup $\{\vec{a}\} \subset V^1$ za $\vec{a} \neq \vec{0}$ je baza prostora V^1.

  Neka su $\vec{a}$ i $\vec{b}$ nekolinearni vektori u V^2. Skup $\{\vec{a}, \vec{b}\}$ je baza za V^2.

  Neka su $\vec{a}$, $\vec{b}$ i $\vec{c}$ nekomplanarni vektori u V^3. Skup $\{\vec{a}, \vec{b}, \vec{c}\}$ je baza za V^3.

- Skup $\{e_1, e_2, \ldots, e_n\}$ je baza za $\mathbb{R}^n$. Ta se baza naziva *kanonska* ili *standardna*. Naime, vrijedi
$$(x_1, x_2, \ldots, x_n) = x_1e_1 + x_2e_2 + \cdots + x_ne_n,$$
  tako da su koordinate uređene n-torke jednake upravo koeficijentima u njezinom prikazu kao linearne kombinacije vektora $e_1, e_2, \ldots, e_n$. U tom smislu je baza $(e_1, \ldots, e_n)$ najjednostavnija budući da se prikaz vektora u toj bazi izravno očita iz njegovih koordinata.

- Skup $\{p_0, p_1, \ldots, p_n\}$ je baza za $\mathcal{P}_n$.

- Skup $\{1\}$ je baza polja $\mathbb{F}$ kojeg shvaćamo kao vektorski prostor nad samim sobom. Općenito, svaki skup $\{a\}$, $a \neq 0$, je baza za $\mathbb{F}$.

  Skup $\{1, i\}$ je baza za realan vektorski prostor $\mathbb{C}_{\mathbb{R}}$.

Teorem 1.4.2. *Neka je $B = \{b_1, \dots, b_n\}$ baza vektorskog prostora V. Tada za svaki $a \in V$ postoje* jedinstveni *skalari $\beta_1, \dots, \beta_n$ takvi da je $a = \beta_1 b_1 + \cdots + \beta_n b_n$.*
Vrijedi i obrat. Ako se svaki vektor iz V jedinstveno prikazuje kao linearna kombinacija vektora iz B, onda je B baza za V.

Dokaz. Pretpostavimo da je B baza i da postoje barem dva prikaza vektora a kao linearne kombinacije vektora iz B, to jest

$$a = \beta_1 b_1 + \cdots + \beta_n b_n, \quad a = \alpha_1 b_1 + \cdots + \alpha_n b_n,$$

za neke $\beta_1, \dots, \beta_n, \alpha_1, \dots, \alpha_n \in \mathbb{F}$. Odatle je

$$0_V = (\alpha_1 - \beta_1) b_1 + \cdots + (\alpha_n - \beta_n) b_n.$$

Budući da je B baza pa stoga i linearno nezavisan skup, slijedi da je $\alpha_i - \beta_i = 0$, odnosno $\alpha_i = \beta_i$ za sve $i = 1, \dots, n$.

Obrat. Iz pretpostavke da se svaki vektor iz V prikazuje kao linearna kombinacija vektora iz B, slijedi da je B sustav izvodnica za V. Nadalje, prikaz $0_V = \alpha_1 b_1 + \cdots + \alpha_n b_n$ je jedinstven, pa je nužno $\alpha_i = 0$ za sve $i = 1, \dots, n$. Dakle, B je linearno nezavisan skup pa stoga i baza za V. □

Prisjetimo se da smo u kolegiju *Analitička geometrija* pokazali da skup od dva nekolinearna vektora u V^2, odnosno skup od tri nekomplanarna vektora u V^3 zadovoljava svojstvo iskazano u Teoremu 1.4.2 i to je bio razlog zbog kojeg smo te skupove tada proglasili bazom.

Napomena. Pretpostavimo da je $S \subseteq V$ neprazan i konačan skup. Tada svaki vektor $x \in [S]$ ima jedinstveni prikaz kao linearna kombinacija vektora iz S ako i samo ako je S linearno nezavisan skup. Pritom, ako je S linearno nezavisan skup, on ne mora biti baza prostora V, ali S je tada svakako baza vektorskog prostora $[S]$ (v. Propoziciju 1.3.2). Stoga Teorem 1.4.2 možemo shvatiti kao posebni (i naročito važan) slučaj općenitije tvrdnje u kojoj se govori o linearnoj ljusci bilo kojeg linearno nezavisnog skupa $S \subseteq V$. Ako se dodatno pretpostavi da je S sustav izvodnica prostora V, dobivamo tvrdnju o jednoznačnom prikazu svakog vektora iz V pomoću baze.

Prirodno nam se nameće pitanje postoji li u svakom netrivijalnom vektorskom prostoru baza. Odgovor na to pitanje je potvrdan, a mi ćemo ga obrazložiti za konačnogenerirane vektorske prostore. (Naime, za vektorske prostore koji nisu konačnogenerirani pitanje postojanja baze - kao beskonačnog skupa, dakako - dublje je teorijske naravi, a potvrdni odgovor ovisi o prihvaćanju određenih aksioma te nema neposredne praktične primjene). Dakle, nadalje je naša pretpostavka da je prostor V netrivijalan i konačnogeneriran, to jest da postoji skup $G = \{a_1, \dots, a_n\} \subset V$ takav da je $[G] = V$.

Teorem 1.4.3. *Neka je V konačnogeneriran i netrivijalan vektorski prostor. Ako je $G = \{a_1, \dots, a_n\} \subset V$ sustav izvodnica za V, onda G sadrži podskup koji je baza za V.*

Dokaz. Bez smanjenja općenitosti možemo pretpostaviti da su vektori u G različiti od nulvektora. Zaista, ako je $0_V \in G$, onda je $G \backslash \{0_V\}$ neprazan (jer je V netrivijalan) sustav izvodnica za V.

Ako je G linearno nezavisan skup u V, onda je prema definiciji skup G baza prostora V.

Pretpostavimo da je $G = \{a_1, \dots, a_n\}$ linearno zavisan skup. Tada prema Propoziciji 1.3.11 postoji vektor $a_i \in G$ koji se može prikazati kao linearna kombinacija vektora iz $G \backslash \{a_i\}$. No, prema Propoziciji 1.3.5 skup $G_1 = G \backslash \{a_i\}$ je također sustav izvodnica za V. Ako je G_1 linearno nezavisan skup, onda je i baza za V pa smo gotovi s dokazom. U protivnom, nastavljamo postupak. U svakom koraku uklanjamo neki vektor koji se može prikazati kao linearna kombinacija ostalih vektora skupa, dok god takav vektor postoji. Svakim korakom broj preostalih vektora smanjuje se za 1. Nakon najviše $n-1$ koraka dobit ćemo linearno nezavisan podskup skupa G. Taj podskup bit će također sustav izvodnica prostora V, jer ni u jednom koraku to svojstvo nije narušeno. U krajnjem mogućem slučaju, za $n-1$ koraka, dobit ćemo skup koji se sastoji od samo jednog vektora, različitog od 0_V. $\square$

Korolar 1.4.4. *Svaki netrivijalan konačnogeneriran vektorski prostor ima konačnu bazu.*

Definicija 1.4.5. *Vektorski prostor koji ima konačnu bazu naziva se* ***konačnodimenzionalnim****. Trivijalan prostor $V = \{0_V\}$ smatra se konačnodimenzionalnim. Netrivijalni vektorski prostor koji nema konačnu bazu je* ***beskonačnodimenzionalan****.*

Korolar 1.4.6. *Neka je V netrivijalan vektorski prostor. V je konačnogeneriran ako i samo ako je konačnodimenzionalan.*

Budući da je prethodnim korolarom iskazano da su pojmovi konačnogeneriranog i konačnodimenzionalnog prostora ekvivalentni, može se učiniti da je jedan od tih pojmova suvišan. Uočimo, ipak, da smo do spoznaje o ekvivalentnosti postojanja konačnog sustava izvodnica i (konačne) baze došli postupno, a da će naziv konačnodimenzionalni dobiti puni smisao nakon definiranja dimenzije.

Pitanje jednakobrojnosti (ili ekvipotentnosti) bilo kojih dviju baza postavlja se prirodno već stoga što u netrivijalnom, konačnogeneriranom vektorskom prostoru nad poljem koje se sastoji od beskonačno mnogo elemenata, za nas redovito nad poljem $\mathbb{R}$ ili $\mathbb{C}$, uvijek postoji više od jedne, a zapravo beskonačno mnogo različitih baza.

Kako bismo to uvidjeli, dovoljno je neki vektor baze pomnožiti bilo kojim skalarom različitim od 0 i 1, odnosno, ako baza sadrži barem dva vektora, označimo ih s a i b, zamijeniti vektor a u bazi s $a + b$, a sve ostale vektore baze ostaviti nepromijenjene. Višestrukom primjenom ovih jednostavnih operacija možemo iz jedne baze dobiti novu, koja će izgledati "sasvim različito" od početne, ali će se i dalje sastojati od jednakog broja vektora. Primjerice, bazu $\{a, b, c\}$ u nekoliko takvih koraka možemo lako "pretvoriti" u bazu $\{a + c, 2b - c, 3c\}$.

U dobro poznatim prostorima V^2 i V^3 imamo geometrijsku argumentaciju zašto se svaka baza sastoji od točno dva (nekolinearna) vektora, odnosno od točno tri (nekomplanarna) vektora. Za dokaz općenitog teorema o jednakobrojnosti baza u konačnogeneriranom vektorskom prostoru potreban je, dakako, i općeniti pristup koji neće ovisiti o specifičnim svojstvima nekih konkretnih prostora.

Najprije ćemo ustanoviti da linearno nezavisni podskup ne može biti "veći" (po broju elemenata) od bilo kojeg sustava izvodnica istog prostora. Pokazat će se da ako se linearno nezavisni podskup sastoji od jednako mnogo vektora kao neki sustav izvodnica, onda je taj linearno nezavisni podskup i sam također sustav izvodnica, dakle baza prostora.

Teorem 1.4.7. *Neka je V konačnogenerirani vektorski prostor. Ako u tom prostoru postoji sustav izvodnica, različit od $\{0_V\}$, koji se sastoji od n vektora, onda bilo koji linearno nezavisni podskup prostora V može sadržavati najviše n vektora.*

Dokaz. Uočimo da u slučaju $V = \{0_V\}$ ne postoji linearno nezavisan podskup u V. Nadalje uzimamo da je $V \neq \{0_V\}$.

Pretpostavimo da je $S = \{a_1, a_2, \ldots, a_n\}$ sustav izvodnica prostora V te da je X linearno nezavisni podskup prostora V koji sadrži barem n vektora. Označimo nekih n vektora iz X s x_1, x_2 , ..., x_n. Pokazat ćemo da je tada skup $X' = \{x_1, x_2, \ldots, x_n\}$ sustav izvodnica prostora V. Odatle će slijediti da X ne može sadržavati niti jedan vektor y koji se ne nalazi u X', jer u protivnom bi y pripadao linearnoj ljusci $[X']$, koja je jednaka cijelom V pa bi X bio linearno zavisan, suprotno pretpostavci. Uz to, budući da je X' linearno nezavisan, kao podskup linearno nezavisnog skupa X, slijedit će da je X' baza prostora V.

Dakle, za dokaz teorema preostaje pokazati da je $X' = \{x_1, x_2, \ldots, x_n\}$ sustav izvodnica prostora V. To ćemo postići postupnom zamjenom vektora iz skupa S vektorima iz X'. Pritom možemo pretpostaviti da su S i X' disjunktni, jer ako se neki vektori iz S podudaraju s nekima iz X', zamijenimo ih odmah tim vektorima iz X'.

Uzmimo vektor x_1 te razmotrimo skup

$$S_1 = \{x_1, a_1, a_2, \ldots, a_n\}$$

kao uređen skup, u navedenom redoslijedu vektora. S_1 je svakako sustav izvodnica, jer sadrži sustav izvodnica S, a pritom je linearno zavisan, jer se x_1 može napisati kao linearna kombinacija ostalih vektora tog skupa. Budući da x_1 nije nulvektor, po Propoziciji 1.3.12 neki se vektor iz S_1 može napisati kao linearna kombinacija njemu prethodnih vektora tog uređenog skupa. Taj vektor mora biti neki $a_j \in S$. Uklonimo li a_j iz skupa S_1, preostali skup $S_1 \backslash \{a_j\}$ također je sustav izvodnica, kao i S i S_1 (Propozicija 1.3.5). Time smo dobili novi sustav izvodnica koji se od S razlikuje time što je neki $a_j \in S$ zamijenjen vektorom $x_1 \in X'$.

Nastavljamo postupak tako da formiramo uređeni skup

$$S_2 = \{x_2, x_1\} \cup S \backslash \{a_j\} = \{x_2, x_1, a_1, \ldots, \widehat{a_j}, \ldots, a_n\},$$

pri čemu oznaka $\widehat{a_j}$ znači da smo vektor a_j izostavili iz nabrajanja. I S_2 je sustav izvodnica, pritom linearno zavisan pa u njemu postoji vektor koji se može prikazati kao linearna kombinacija prethodnih, a taj vektor nije x_2, kao ni x_1 nego neki vektor a_i, $i \neq j$, iz S. Nadalje, jasno je da je $S_2 \backslash a_i = \{x_2, x_1, a_1, \ldots, \widehat{a_j}, \ldots, \widehat{a_i}, \ldots, a_n\}$ sustav izvodnica za V.

Nakon n koraka dobivamo sustav izvodnica $S_n = \{x_n, \ldots, x_2, x_1\} = X'$, što nam je i bio cilj. Naglasimo još jedanput da je tijekom postupka zamjene vektora u svakom koraku bilo sačuvano svojstvo da je novodobiveni skup također sustav izvodnica prostora V.

Teorem je time dokazan. □

Kao posljedicu prethodnog teorema možemo lako izvesti ključnu činjenicu o jednakobrojnosti bilo kojih dviju baza konačnogeneriranog vektorskog prostora.

Teorem 1.4.8 (Steinitz). *Svake dvije baze netrivijalnog konačnogeneriranog vektorskog prostora su jednakobrojne* (ekvipotentne).

Dokaz. Podsjetimo da po Korolaru 1.4.4 netrivijalni konačnogenerirani vektorski prostor V svakako ima bazu. Neka su sada B_1 i B_2 bilo koje dvije baze prostora V. Označimo $\operatorname{card} B_1 = n_1$, $\operatorname{card} B_2 = n_2$ ($\operatorname{card} B$ je kardinalni broj skupa B, dakle broj elemenata tog skupa).

Kako je B_1 linearno nezavisan skup, a B_2 je sustav izvodnica, po Teoremu 1.4.7 slijedi $n_1 \leq n_2$. Obrnuto, kako je B_2 linearno nezavisan skup, a B_1 je sustav izvodnica, vrijedi $n_2 \leq n_1$. Očito mora biti $n_1 = n_2$ pa su dvije baze jednakobrojne. $\square$

Na temelju Teorema 1.4.8 možemo definirati dimenziju vektorskog prostora.

Definicija 1.4.9. *Neka je V konačnodimenzionalan vektorski prostor i $V \neq \{0_V\}$. Broj vektora u bilo kojoj bazi prostora V naziva se* ***dimenzija*** *vektorskog prostora V i označava s $\dim V$. Ako je $\dim V = n$, onda kažemo da je V n-**dimenzionalan vektorski prostor**.*

Za $V = \{0_V\}$ stavljamo da je $\dim V = 0$

Budući da znamo baze nekih vektorskih prostora sada lako možemo zaključiti i kolika im je dimenzija:

- $\dim V^1 = 1$, $\dim V^2 = 2$, $\dim V^3 = 3$,
- $\dim \mathbb{R}^n = n$,
- $\dim \mathcal{P}_n = n + 1$,
- $\dim \mathbb{C} = 1$, $\dim \mathbb{C}_\mathbb{R} = 2$, i općenito $\dim \mathbb{C}^n = n$, $\dim \mathbb{C}^n_\mathbb{R} = 2n$,
- $\dim M_2(\mathbb{R}) = 4$.

Naglasimo još jedanput da pojam dimenzije vektorskog prostora ima smisla tek kad se ustanovi da su sve baze konačnodimenzionalnog vektorskog prostora jednakobrojne. Kažemo li da je dimenzija vektorskog prostora, po definiciji, jednaka broju vektora u bazi tog prostora, podrazumijevamo da to znači u *bilo kojoj bazi* prostora i pozivamo se na teorem o jednakobrojnosti baza. Pojam dimenzije ne bi imao smisla ako bi se broj vektora u bazi mijenjao izborom različitih baza. No, sad također znamo da dimenziju određenog vektorskog prostora možemo ustanoviti poznavanjem ili, ako je potrebno, konstrukcijom jedne jedine njegove baze.

Kako općenito možemo odrediti (konstruirati) neku bazu vektorskog prostora? Po Teoremu 1.4.3 svaki konačan sustav izvodnica ili je i sam baza ili, ako je to linearno zavisan skup, sadrži neku bazu kao svoj pravi podskup. Takva baza dobiva se redukcijom do linearno nezavisnog podskupa koji je i sam sustav izvodnica.

S druge strane, ako imamo linearno nezavisan podskup konačnogeneriranog vektorskog prostora, bazu možemo izgraditi njegovim proširivanjem do sustava izvodnica, ne narušavajući pritom svojstvo linearne nezavisnosti prilikom tog proširivanja. Katkad je dosta lako izabrati vektore kojima se zadani linearno nezavisni skup može dopuniti do baze, ali općenito nije dovoljno pouzdati se u "pogađanje" nego nam treba praktični postupak koji sigurno dovodi do cilja. Takav postupak zapravo je sadržaj dokaza sljedeće propozicije.

Propozicija 1.4.10. *Svaki linearno nezavisan skup u konačnodimenzionalnom vektorskom prostoru V sadržan je u nekoj bazi prostora V.*

Dokaz. Neka je $S = \{a_1, \ldots, a_k\}$ linearno nezavisan skup u V i neka je $B = \{b_1, \ldots, b_n\}$ baza za V. Skup

$$S \cup B = \{a_1, \ldots, a_k, b_1, \ldots, b_n\}$$

je nadskup sustava izvodnica (to jest baze) pa i sam generira prostor V, odnosno $[S \cup B] = V$. Nadalje, $S \cup B$ je linearno zavisan skup jer se svaki vektor a_i može prikazati kao linearna kombinacija vektora iz baze B. Stoga se prema Lemi 1.3.12 barem jedan od vektora iz $S \cup B$ može prikazati kao kombinacija svojih prethodnika. Lako vidimo da to ne može biti niti jedan od vektora a_i jer je skup S linearno nezavisan pa stoga postoji neki b_{j_1}, $1 \leq j_1 \leq n$ takav da je $b_{j_1} \in [a_1, \ldots, a_k, b_1, \ldots, b_{j_1 - 1}]$. Izbacivanjem vektora b_{j_1} iz skupa $S \cup B$ dobivamo skup

$$S_1 = S \cup B \backslash \{b_{j_1}\}$$

koji je također sustav izvodnica za V prema Propoziciji 1.3.5. Ako je i S_1 linearno zavisan skup tada postoji neki b_{j_2}, $1 \leq j_2 \leq n$, koji se može prikazati kao kombinacija svojih prethodnika pa njegovim izbacivanjem dolazimo do skupa

$$S_2 = S_1 \backslash \{b_{j_2}\}$$

koji je također sustav izvodnica za V. Ponavljamo opisani postupak sve dok je skup S_i linearno zavisan. Nakon konačno mnogo koraka dolazimo do skupa S_l koji je linearno nezavisan, ali i sustav izvodnica za V. Stoga je S_l jedna baza za V i $S \subset S_l$. Uočimo da je zapravo $l = k$ jer je zbog Steinitzovog teorema 1.4.8 je $|S_l| = |B| = n$, pa je $k + n - l = n$. Ukratko, do tražene baze smo došli izbacivanjem k vektora b_j iz $S \cup B$. □

Primijetimo da se u ovom dokazu početnom linearno nezavisnom skupu S najprije "pripoji" cijela jedna baza, a zatim se provodi redukcija dobivenog sustava izvodnica pri čemu se sačuva skup S. Dakle, $n - k$ vektora za dopunu k-članog podskupa S do baze prostora dimenzije n nalazimo unutar neke "već poznate" baze B. Načelno, takva baza postoji po pretpostavci, a u nekom konkretnom slučaju (zadatku) redovito je riječ o prostoru čiju neku bazu znamo otprije, npr. standardnu bazu za prostor $\mathbb{R}^n$ ili $\mathcal{P}_n$.

Kao posljedicu gotovo svega dokazanog u ovom i prethodnom odsječku iskazat ćemo sljedeći korolar koji se sastoji od operativno vrlo korisnih tvrdnji u slučaju kad nam je poznata dimenzija ambijentalnog vektorskog prostora.

Korolar 1.4.11. *Neka je V n-dimenzionalan vektorski prostor i S njegov podskup. Vrijedi:*

(1) *Ako je S linearno nezavisan skup i $|S| = n$, onda je S baza za V.*

(2) *Ako je S sustav izvodnica za V i $|S| = n$, onda je S baza za V.*

(3) *Ako je S linearno nezavisan skup, onda je $|S| \leq n$.*
(Drugim riječima, maksimalan broj vektora u linearno nezavisnom skupu je n.)

(4) *Ako je S takav da je $|S| > n$, onda je S linearno zavisan skup.*

(5) *Ako je S sustav izvodnica za V, onda je $|S| \geq n$.*
(Drugim riječima, minimalan broj vektora u sustavu izvodnica za V je n.)

(6) *Ako je S takav da je $|S| < n$, onda S ne može biti sustav izvodnica za V.*

Za vježbu je važno i korisno samostalno dokazati sve tvrdnje iz prethodnog Korolara. Sve one jednostavno slijede iz propozicija i teorema u ovom odjeljku. Posebno, uočite kako tvrdnja (1) u Korolaru 1.4.11 slijedi iz dokaza Teorema 1.4.7.

Primjer 16. Neka je $B = \{a, b, c\}$ baza za V. Ispitajte je li neki od danih skupova linearno (ne)zavisan, sustav izvodnica ili baza za V:

(a) $A = \{a + b, a + b + c\}$,

(b) $B = \{a - b, b - c, a - c\}$,

(c) $C = \{a, a + b, a + b + c\}$,

(d) $D = \{a, a + b, a + b + c, b + c\}$.

Odgovori.

(a) A je linearno nezavisan, nije sustav izvodnica ni baza za V.

(b) B je linearno zavisan $(a - c = (a - b) + (b - c))$, nije sustav izvodnica ni baza za V.

(c) C je linearno nezavisan, sustav izvodnica i baza za V.

(d) $D = \{a, a + b, a + b + c, b + c\}$ je linearno zavisan, sustav izvodnica (jer sadrži bazu C) ali nije baza za V.

♡

Zadatak 8. *U vektorskom prostoru $\mathbb{R}^5$ zadani su vektori $a_1 = (1, 1, 2, 3, 5)$, $a_2 = (2, 0, 1, 9, 3)$ i $a_3 = (1, 0, 5, 0, 12)$. Provjerite da je skup $\{a_1, a_2, a_3\}$ linearno nezavisan te ga dopunite do baze prostora $\mathbb{R}^5$.*

Uputa: Može se primijeniti postupak iz dokaza Propozicije 1.4.10 tako da se za proširivanje do baze poslužimo standardnom bazom $\{e_1, e_2, e_3, e_4, e_5\}$. Nakon što provjerimo linearnu nezavisnost skupa $\{a_1, a_2, a_3\}$, promatramo skup $\{a_1, a_2, a_3, e_1, e_2, e_3, e_4, e_5\}$ i ispitujemo redom koji se vektori mogu izraziti kao linearna kombinacija prethodnih. Pokazat će se da e_1 nije takav pa ga možemo uvrstiti u traženu bazu, no za e_2 ustanovit će se da se nalazi u linearnoj ljusci $[a_1, a_2, a_3, e_1]$ pa stoga ne može ući u tu bazu. Sljedeći vektor, e_3, ne pripada navedenoj linearnoj ljusci pa je skup $\{a_1, a_2, a_3, e_1, e_3\}$ jedna (ne i jedina, dakako) baza koja sadrži vektore a_1, a_2 i a_3.

Primjer 17. Pretpostavimo da je skup $\{v_1, v_2, \ldots, v_n\}$ neka baza vektorskog prostora V nad poljem $\mathbb{F}$. Ako za neke vektore $a, b \in V$ imamo njihove prikaze u toj bazi,

$$a = \sum_{i=1}^{n} \alpha_i v_i, \ b = \sum_{i=1}^{n} \beta_i v_i,$$

provjerite da tada prikaz zbroja $a+b$ u istoj bazi glasi

$$a+b=\sum_{i=1}^{n}(\alpha_i+\beta_i)v_i.$$

Nadalje, ako je $\lambda \in \mathbb{F}$, onda je

$$\lambda a=\sum_{i=1}^{n}(\lambda\alpha_i)v_i.$$

(Uočite koja svojstva operacija u vektorskom prostoru treba primijeniti u tim jednostavnim računima). Odatle vidimo da, kad imamo izabranu jednu bazu, operacije zbrajanja i množenja skalarom u V možemo izvoditi i tako da ne pišemo uvijek cjelovite linearne kombinacije nego se prikazima u bazi služimo kao koordinatnim n- torkama:

$$(\alpha_1,\alpha_2,\ldots,\alpha_n)+(\beta_1,\beta_2,\ldots,\beta_n)=(\alpha_1+\beta_1,\alpha_2+\beta_2,\ldots,\alpha_n+\beta_n),$$

$$\lambda(\alpha_1,\alpha_2,\ldots,\alpha_n)=(\lambda\alpha_1,\lambda\alpha_2,\ldots,\lambda\alpha_n).$$

Kao što smo naviknuti u prostorima V^2 i V^3, računske operacije “prevodimo” u prostor $\mathbb{R}^2$, odnosno $\mathbb{R}^3$ gdje je zapis jednostavniji. Općenito, operacije iz prostora V, posredstvom prikaza u nekoj odabranoj bazi, “prenosimo” u prostor $\mathbb{F}^n$. Na kraju računa treba se ipak vratiti u početni prostor V i krajnje rezultate izraziti u tom prostoru.

Primjerice, neka je riječ o prostoru polinoma $\mathcal{P}_3$ stupnja najviše 3, s realnim koeficijentima i uzmimo da smo se poslužili njegovom standardnom bazom $\{p_0,p_1,p_2,p_3\}$ (v. primjere baze) kako bismo umjesto pisanja polinoma radili u koordinatnom prostoru $\mathbb{R}^4$. Ako je završni rezultat prikazan vektorom $(-3,2,0,-1)\in\mathbb{R}^4$, rješenje ćemo napisati kao polinom $-3+2t-t^3$.

1.5 Potprostori

U primjerima vektorskih prostora koje smo dosad upoznali mogli smo uočiti kako se neki od njih pojavljuju kao podskupovi drugih vektorskih prostora, a s jednakim (preciznije, naslijeđenim) operacijama zbrajanja i množenja skalarom (nad istim poljem). Zapravo je to vrlo uobičajena situacija, da se unutar nekih “standardnih” vektorskih prostora, poput V^3, $\mathbb{R}^n$ ili $\mathcal{P}$, stanovitim svojstvima izdvajaju podskupovi koji su također vektorski prostori, a onda ih je, zahvaljujući posjedovanju takve strukture, lakše proučavati.

Također, već smo naučili da će linearna ljuska bilo kakvog nepraznog podskupa S vektorskog prostora V također biti vektorski prostor – katkad identičan cijelom prostoru (tada je S sustav izvodnica za V), a katkad sadržan u V kao njegov pravi podskup. Dobro su nam poznati primjeri vektorskih prostora V^1, V^2 i V^3 koji su “ulančano” sadržani jedan u drugom: $V^1\subseteq V^2\subseteq V^3$, a geometrijski ih znamo ostvariti tako da u trodimenzionalnom prostoru V^3 najprije jednim vektorom “razapnemo” pravac, a onda pridodamo neki drugi vektor, nekolinearan s prvim, tako da zajedno “razapinju” ravninu.

Time dolazimo do važnog pojma vektorskog potprostora.

Definicija 1.5.1. *Neka je V vektorski prostor nad poljem $\mathbb{F}$ i $L\neq\emptyset$ neki podskup od V. Kažemo da je L* ***vektorski potprostor*** *prostora V ako je L i sam vektorski prostor nad* *poljem $\mathbb{F}$ s obzirom na operacije zbrajanja i množenja skalarom definirane u V. Kraće ćemo reći da je L* ***potprostor*** *od V i pisati $L \leq V$.*

Prostore $L = V$ i $L = \{0_V\}$ nazivamo ***trivijalnim potprostorima****.*

Za L ćemo reći da je ***pravi potprostor*** *od V ako je $\{0_V\} \subsetneqq L \subsetneqq V$. U slučaju $L \subsetneqq V$ pišemo $L < V$ ili $L \lneqq V$.*

Da bismo ustanovili da je neki skup L vektorski potprostor potrebno je općenito ispitati deset svojstava - prvih pet odnosi se na strukturu Abelove grupe, koju bi morao posjedovati i podskup L, a drugih pet su svojstva operacije množenja skalarom. No, ako je naš skup L podskup nekog vektorskog prostora V i želimo ispitati je li on sam vektorski potprostor s obzirom na iste operacije iz V, onda se mnoga svojstva *nasljeđuju* i stoga ih nema potrebe dokazivati. Konkretno, nasljeđuje se asocijativnost i komutativnost zbrajanja, te kvaziasocijativnost množenja skalarom, obje distributivnosti i svojstvo množenja s 1. Dakle, da bismo ustanovili da je L potprostor od V morali bismo provjeriti sljedeća svojstva:

- $a + b \in L$, za sve $a, b \in L$,
- nulvektor (tj. neutralni element zbrajanja) je u L, odnosno $0_V \in L$,
- za svaki $a \in L$ je i njegov suprotan vektor $-a \in L$,
- $\alpha a \in L$, za sve $a \in L$ i $\alpha \in \mathbb{F}$.

No, pokazuje se da je dovoljno provjeriti samo prvo i posljednje svojstvo, odnosno dovoljno je samo provjeriti da je skup L zatvoren na zbrajanje vektora i množenje vektora skalarom. (Kad govorimo o "istim" operacijama na vektorskom prostoru i njegovom potprostoru, zapravo imamo restrikciju preslikavanja $+ : V \times V \to V$ na $L \times L \to L$ te restrikciju $\cdot : F \times V \to V$ na $F \times L \to L$, a zatvorenost znači da je kodomena u oba slučaja upravo L).

Teorem 1.5.2. *Neka je $L \neq \emptyset$ neki podskup vektorskog prostora V. L je potprostor od V ako i samo ako je zatvoren u odnosu na operacije iz V, odnosno ako i samo ako vrijedi*

(1) *$a + b \in L$, za sve $a, b \in L$,*

(2) *$\alpha a \in L$, za sve $a \in L$ i $\alpha \in \mathbb{F}$.*

Dokaz. Ako je L potprostor od V, onda je L i sam vektorski prostor pa je zatvoren na zbrajanje vektora i množenje vektora skalarom.

Pokažimo dovoljnost. Pretpostavimo da je L zatvoren na zbrajanje vektora i množenje vektora skalarom. Tada za $a \in L$ vrijedi da je i $(-1)a \in L$. Kako je $-a = (-1)a$, pokazali smo da je suprotan vektor od a također iz L. Nadalje, i $0_V = a + (-a) \in L$, jer je L zatvoren na zbrajanje. Dakle, L je vektorski prostor s obzirom na iste operacije iz V. □

Prisjetimo se da smo u Propoziciji 1.3.2 pokazali da je linearna ljuska proizvoljnog skupa S iz V, $[S]$, potprostor od V. Uočimo još da je (samo) nulvektor zajednički element svih potprostora nekog vektorskog prostora V.

Korolar 1.5.3. *Skup $L \subseteq V$, $L \neq \emptyset$, je potprostor od V ako i samo ako je $\alpha a + \beta b \in L$, za sve $a, b \in L$ i $\alpha, \beta \in \mathbb{F}$.*

Dokaz. Za $\alpha = \beta = 1$ dobivamo svojstvo (1), a za $\beta = 0$ svojstvo (2) Teorema 1.5.2. $\square$

Korolar 1.5.4. *Skup $L \subseteq V$, $L \neq \emptyset$, je potprostor od V ako i samo ako je $\alpha a + b \in L$, za sve $a, b \in L$ i $\alpha \in \mathbb{F}$.*

Prisjetimo se Propozicije 1.3.2 u kojoj se još nije izričito spominjao pojam potprostora vektorskog prostora, a njezina tvrdnja zapravo govori: *za bilo koji podskup S vektorskog prostora V njegova linearna ljuska $[S]$ je potprostor od V.* Dakle, $S \subseteq V \Rightarrow [S] \leq V$. Iz Korolara 1.5.3 očito je $[L] \leq L$ za svaki potprostor $L \leq V$. Budući da trivijalno vrijedi $S \subseteq [S]$ za svaki podskup $S \subseteq V$, dobivamo sljedeću karakterizaciju potprostora kao podskupa koji se podudara s vlastitom linearnom ljuskom. (Izuzetak je samo prazan skup).

Korolar 1.5.5. *Skup $L \subseteq V$, $L \neq \emptyset$, potprostor je od V ako i samo ako je $L = [L]$.*

Dosad navedene tvrdnje o potprostorima vrijede za bilo koje vektorske prostore, ne nužno konačnodimenzionalne. Ako je V konačnodimenzionalan, a L njegov potprostor, zanima nas odnos njihovih dimenzija. Za očekivati je da vrijedi $\dim L \leq \dim V$. To će se pokazati istinitim, no bitno je najprije ustanoviti da je potprostor konačnodimenzionalnog prostora i sam konačnodimenzionalan. Ovo svojstvo "intuitivno" se čini posve neupitnim, ali zapravo nije sasvim očito te ga ipak treba dokazati.

Propozicija 1.5.6. *Neka je V konačnodimenzionalan vektorski prostor i L njegov potprostor. Tada je i L konačnodimenzionalan vektorski prostor i $\dim L \leq \dim V$.*
Ako je $\dim L = \dim V$, onda je $L = V$.

Dokaz. Najprije ustanovimo da je L konačnodimenzionalan vektorski prostor. Ako je $L = \{0_V\}$, tvrdnja trivijalno vrijedi. Pretpostavimo da $L \neq \{0_V\}$. Stoga postoji $a_1 \in L$ i $a_1 \neq 0_V$. Ako je $[a_1] = L$, onda je L konačnogeneriran, odnosno konačnodimenzionalan prostor. Ako $[a_1] \neq L$, to jest $[a_1] < L$, onda postoji $a_2 \in L \backslash [a_1]$ i $a_2 \neq 0_V$. Očito je skup $\{a_1, a_2\}$ linearno nezavisan. Ako je $[a_1, a_2] = L$, onda smo pokazali da je L konačnodimenzionalan. U suprotno, nastavljamo postupak. Broj koraka u ovom postupku je konačan i maksimalno jednak $n = \dim V$, jer je maksimalan broj vektora u linearno nezavisnom skupu u prostoru V jednak n.

Neka je B_L baza za L. Ako je B_L i baza za V, onda $\dim L = \dim V$. Ako B_L nije baza za V, onda je to linearno nezavisan skup u V koji mora biti sadržan u nekoj bazi B za V (Teorem 1.4.10). Stoga je $\dim L = |B_L| < |B| = \dim V$. $\square$

U sljedećim primjerima dajemo još neke primjere potprostora.

Primjer 18. Opišimo sve prave potprostore od V^3. Kako je $\dim V^3 = 3$, dimenzija pravog potprostora L od V^3 može biti 1 ili 2.

Ako je $\dim L = 1$, onda postoji $\vec{a} \in V^3 \backslash \{\vec{0}\}$ takav da je $L = [\vec{a}]$, to jest $L = \{\alpha\vec{a} : \alpha \in \mathbb{R}\}$.

Ako je $\dim L = 2$, onda postoje nekolinearni vektori $\vec{a}, \vec{b} \in V^3$ takvi da je $L = [\vec{a}, \vec{b}]$, to jest $L = \{\alpha\vec{a} + \beta\vec{b} : \alpha, \beta \in \mathbb{R}\}$.

Ako promatramo prostor $V^3(O)$ radijvektora sa zajedničkim ishodištem O, onda potprostori dimenzije 1 i 2 odgovaraju upravo pravcima, odnosno ravninama sa zajedničkom točkom O i tako ih geometrijski predočavamo.

$\heartsuit$

Primjer 19. Ustanovit ćemo koji je danih skupova potprostor od $\mathbb{R}^n$, te mu odrediti jednu bazu i dimenziju,

(a) $A = \{(x_1, \dots, x_n) : x_1, \dots, x_n \in \mathbb{Z}\}$,

(b) $B = \{(x_1, \dots, x_n) \in \mathbb{R}^n : x_1 = 2x_2\}$,

(c) $C = \{(x_1, \dots, x_n) \in \mathbb{R}^n : \sum_{i=1}^n x_i = 0\}$,

(d) $D = \{(x_1, \dots, x_n) \in \mathbb{R}^n : \sum_{i=1}^n x_i = 1\}$,

(e) $E = \{(x_1, x_1, \dots, x_1) : x_1 \in \mathbb{R}\}$.

(a) A nije potprostor od $\mathbb{R}^n$. Za to je dovoljno naći samo jedan konkretan primjer koji ne zadovoljava uvjete iz Teorema 1.5.2, to jest protuprimjer. Recimo, $e_1 = (1, 0, \dots, 0) \in A$, ali $\frac{1}{2}e_1 \notin A$.

(b) Neka su $x = (x_1, \dots, x_n)$ i $y = (y_1, \dots, y_n)$ elementi skupa B. Tada je $x_1 = 2x_2$ i $y_1 = 2y_2$. Za $\alpha \in \mathbb{R}$ je

$$\alpha x + y = (\alpha x_1 + y_1, \dots, \alpha x_n + y_n).$$

Kako je $\alpha x_1 + y_1 = \alpha(2x_2) + (2y_2) = 2(\alpha x_2 + y_2)$, slijedi da je $\alpha x + y \in B$. Stoga je B potprostor od $\mathbb{R}^n$.

Odredimo mu sada jednu bazu i dimenziju. Za $x = (x_1, \dots, x_n) \in B$ vrijedi

$$x = (x_1, x_2, x_3, \dots, x_n) = (2x_2, x_2, x_3, \dots, x_n) = x_2 \underbrace{(2, 1, 0, \dots, 0)}_{2e_1+e_2} + x_3e_3 + \cdots + x_ne_n.$$

Skup vektora $\{2e_1 + e_2, e_3, \dots, e_n\}$ je očito sustav izvodnica za B. Lako se provjeri da je i linearno nezavisan, pa je to baza za B i $\dim B = n - 1$.

(c) Neka su $x = (x_1, \dots, x_n)$ i $y = (y_1, \dots, y_n)$ elementi skupa C, te $\alpha \in \mathbb{R}$. Vrijedi

$$\alpha x + y = (\alpha x_1 + y_1, \dots, \alpha x_n + y_n),$$

te

$$\sum_{i=1}^n (\alpha x_i + y_i) = \alpha \sum_{i=1}^n x_i + \sum_{i=1}^n y_i = \alpha \cdot 0 + 0 = 0,$$

pa je $\alpha x + y \in C$. Stoga je C potprostor od $\mathbb{R}^n$.

Odredimo mu sada jednu bazu i dimenziju. Za $x = (x_1, \dots, x_n) \in C$ vrijedi da je $x_1 = -x_2 \cdots - x_n$ pa je

$$\begin{aligned} x &= (-x_2 - x_3 \cdots - x_n, x_2, x_3, \dots, x_n) \\ &= x_2 \underbrace{(-1, 1, 0, \dots, 0)}_{-e_1+e_2} + x_3 \underbrace{(-1, 0, 1, \dots, 0)}_{-e_1+e_3} + \cdots + x_n \underbrace{(-1, 0, \dots, 0, 1)}_{-e_1+e_n}. \end{aligned}$$

Skup vektora $\{-e_1 + e_2, -e_1 + e_3, \dots, -e_1 + e_n\}$ razapinje C i lako se provjeri da je linearno nezavisan, pa je to baza za C i $\dim C = n - 1$.

(d) Skup D nije potprostor od $\mathbb{R}^n$. Zaista, za $e_1, e_2 \in D$ vrijedi da $e_1 + e_2 \notin D$ (jer je zbroj koordinata vektora $e_1 + e_2$ jednak 2).

(e) Uočimo da je $E = [(1, 1, \dots, 1)]$, pa je E jednodimenzionalni potprostor od $\mathbb{R}^n$.

♡

Primijetimo da smo u točkama (b), (c) i (e) mogli odjednom pokazati i to da je zadani skup potprostor i odrediti njegovu bazu. Naime, kad prikažemo opći vektor iz skupa B, C ili E kao linearnu kombinaciju nekih vektora istog skupa, vidimo da je taj jednak linearnoj ljusci nekog svog podskupa. Samim time, skup B, odnosno C i E je potprostor, prema Propoziciji 1.3.2. Uočeni podskup je tada sustav izvodnica tog potprostora, a zatim se provjeri je li ujedno i baza, kao što je napisano u rješenjima. Na taj način ne moramo izravno primijeniti kriterij pomoću zatvorenosti na operacije, iz Teorema 1.5.2. Prikladnost takvog pristupa ovisi o načinu kako je skup zadan.

Primjer 20. U realnom vektorskom prostoru $\mathbb{R}^\mathbb{R} = \{f : \mathbb{R} \to \mathbb{R}\}$ (svih realnih funkcija realne varijable) ispitajmo jesu li sljedeći skupovi potprostori:

(a) P - skup svih parnih funkcija u $\mathbb{R}^\mathbb{R}$,

(b) N - skup svih neparnih funkcija u $\mathbb{R}^\mathbb{R}$,

(c) C - skup svih neprekidnih funkcija u $\mathbb{R}^\mathbb{R}$.

Prisjetimo da se operacije zbrajanja i množenja skalarom u $\mathbb{R}^\mathbb{R}$ definiraju po točkama, to jest

$$(f+g)(x) = f(x) + g(x), \quad (\alpha f)(x) = \alpha f(x), \forall\, x \in \mathbb{R}.$$

(a) Funkcija $f \in \mathbb{R}^\mathbb{R}$ je parna ako je $f(-x) = f(x)$. Neka su $f, g \in P$ i $\alpha \in \mathbb{R}$. Tada je

$$(f+g)(-x) = f(-x) + g(-x) = f(x) + g(x) = (f+g)(x), \forall\, x \in \mathbb{R},$$

$$(\alpha f)(-x) = \alpha f(-x) = \alpha f(x) = (\alpha f)(x),\ \forall\, x \in \mathbb{R}.$$

Stoga su $f + g$ i αf parne funkcije, odnosno P je potprostor od $\mathbb{R}^\mathbb{R}$.

(b) Funkcija $f \in \mathbb{R}^\mathbb{R}$ je neparna ako je $f(-x) = -f(x)$. Neka su $f, g \in N$ i $\alpha \in \mathbb{R}$. Tada je

$$(f+g)(-x) = f(-x)+g(-x) = -f(x)+(-g(x)) = -(f(x)+g(x)) = -(f+g)(x), \forall\, x \in \mathbb{R},$$

$$(\alpha f)(-x) = \alpha f(-x) = \alpha(-f(x)) = -(\alpha f(x)) = -(\alpha f)(x),\ \forall\, x \in \mathbb{R}.$$

Stoga su $f + g$ i αf neparne funkcije, odnosno N je potprostor od $\mathbb{R}^\mathbb{R}$.

(c) Ako su f i g neprekidne u točki x, onda su $f + g$ i αf neprekidne u x. Stoga je C potprostor od $\mathbb{R}^\mathbb{R}$.

♡

Primjer 21. Neka je Q skup svih polinoma iz $\mathcal{P}_n$ koji imaju nultočku u $c = 1$, to jest

$$Q = \{p \in \mathcal{P}_n \,:\, p(1) = 0\}.$$

Svaki polinom iz Q djeljiv je polinomom $t - 1$, to jest $p \in Q$ je oblika

$$p(t) = (t - 1)q(t),$$

gdje je q polinom stupnja manjeg ili jednakom od $n - 1$. Odatle odmah slijedi da će i linearna kombinacija polinoma iz Q imati također nultočku u $c = 1$. Stoga je Q potprostor od $\mathcal{P}_n$.

Odredimo mu jednu bazu i dimenziju. Za $p \in Q$ je

$$p(t) = (t - 1)(a_{n-1}t^{n-1} + \cdots + a_1 t + a_0),$$

za neke $a_{n-1}, \ldots, a_1, a_0 \in \mathbb{R}$, odnosno

$$p(t) = a_{n-1}\underbrace{(t-1)t^{n-1}}_{q_n(t)} + a_{n-2}\underbrace{(t-1)t^{n-2}}_{q_{n-1}(t)} + \cdots + a_1\underbrace{(t-1)t}_{q_2(t)} + a_0\underbrace{(t-1)}_{q_1(t)}.$$

Skup $\{q_1, \ldots, q_n\}$ je sustav izvodnica i očito linearno nezavisan pa on predstavlja bazu za Q i $\dim Q = n - 1$.

♡

Primjer 22. Neka je $\mathcal{L}(V)$ skup svih potprostora vektorskog prostora V. *Biti potprostor* je refleksivna i tranzitivna relacija na skupu $\mathcal{L}(V)$.

♡

Zadatak 9. *Neka je S skup svih polinoma $p(t)$ s realnim koeficijentima, stupnja najviše 3, takvih da za svaki $t \in \mathbb{R}$ vrijedi: $p(t-1) + p(t+1) = 2p(t)$. Odredite opći oblik polinoma iz S te pokažite da je S potprostor vektorskog prostora $\mathcal{P}_3$ polinoma stupnja najviše 3. Odredite $\dim S$. (Smatramo da skup S obuhvaća i nulpolinom).*

Zadatak 10. *Neka je $B = \{(z_1, z_2, z_3) \in \mathbb{C}^3 \,:\, z_1 + z_2 - z_3 = 0\}$. Je li B potprostor od $\mathbb{C}^3$, odnosno $\mathbb{C}^3_{\mathbb{R}}$? Ako jest, odredite mu bazu i dimenziju. Obratite pozornost na moguće razlike za prostor nad poljem $\mathbb{C}$, odnosno $\mathbb{R}$.*

Zadatak 11. *Neka je $n \geq 2$ i $L \leq \mathbb{R}^n$, $\dim L \geq 2$. Tada za svaka dva različita $i, j \in \{1, 2, \ldots, n\}$ postoji vektor $a = (\alpha_1, \alpha_2, \ldots, \alpha_n) \in L$, različit od nulvektora, takav da je $\alpha_i = \alpha_j$.*

1.6 Presjek i suma potprostora.

Kad promatramo potprostore nekog vektorskog prostora, korisnima i potrebnima pokazuju se operacije kojima se od nekih potprostora dobivaju drugi potprostori. Primjenom skupovne operacije presjeka na bilo koje potprostore uvijek se dobiva potprostor, dok odgovarajuća tvrdnja ne vrijedi općenito za operaciju unije na bilo koje potprostore. No, linearna ljuska unije dvaju ili više potprostora bit će također potprostor, takozvana suma potprostora.

Propozicija 1.6.1. *Neka su L i M potprostori vektorskog prostora V. Tada je $L \cap M$ potprostor od V.*

Dokaz. Neka su $a, b \in L \cap M$, te $\alpha, \beta \in \mathbb{F}$. Tada je $\alpha a + \beta b \in L$, jer su $a, b \in L$ i L je potprostor od V. Na isti način, $\alpha a + \beta b \in M$, pa je $\alpha a + \beta b \in L \cap M$. Prema Korolaru 1.5.3 slijedi tvrdnja. □

Na temelju prethodne propozicije lako zaključujemo da je presjek tri ili više potprostora prostora V također potprostor. Primjerice, ako su $L_1, L_2, L_3 \leq V$, onda je $L_1 \cap L_2 \cap L_3 = (L_1 \cap L_2) \cap L_3$ pa je taj skup presjek dvaju potprostora, $L_1 \cap L_2$ i L_3, stoga je i sam potprostor. Ovakav zaključak možemo induktivno proširiti na presjek konačno mnogo potprostora, označimo ih $L_1, L_2, \ldots, L_k$. Tada pišemo $\bigcap\limits_{i=1}^{k} L_i = L$ pa vrijedi $L \leq V$.

Štoviše, presjek bilo koje kolekcije (ili "množine") potprostora, moguće beskonačne, ponovno je potprostor, to jest $\bigcap\limits_{\alpha \in A} L_\alpha \leq V$. Taj presjek uvijek je neprazan skup jer sadrži barem nulvektor. Radi lakšeg predočavanja, zamislimo npr. tri različita 2-dimenzionalna potprostora vektorskog prostora $V^3(O)$, a geometrijski to su tri ravnine koje sadrže točku O. Njihov presjek je ili $\{O\}$ ili zajednička presječnica (pravac) svih triju ravnina, dakle ili nulpotprostor ili jednodimenzionalni potprostor. Isti su mogući ishodi ako uzmemo bilo koliko ravnina kroz točku O, konačno ili beskonačno mnogo.

Definicija 1.6.2. *Neka su L i M potprostori vektorskog prostora V. Potprostor $L \cap M$ se naziva* ***presjek potprostora*** *L i M.*

Dalje nam se prirodno nameće pitanje hoće li i skup $L \cup M$, to jest unija potprostora bit potprostor od V. Općenito, ne! Na primjer, za potprostore $L = [\vec{i}]$ i $M = [\vec{j}]$ od V^3 vidimo da $\vec{i} + \vec{j} \notin L \cup M$, pa $L \cup M$ nije vektorski prostor. Zanimat će nas koji je "najmanji" potprostor koji sadrži dva ili više potprostora vektorskog prostora V, a to onda znači da sadrži njihovu uniju. Pritom se izraz "najmanji" ovdje odnosi na uspoređivanje po relaciji inkluzije među skupovima. Uzmimo da je S neki podskup (ne nužno potprostor) vektorskog prostora S. Za $L \leq V$ kažemo da je *najmanji potprostor* od V koji sadrži S ako je $S \subseteq L$, a ne postoji potprostor $L' \neq L$ takav da je $S \subseteq L' \subseteq L$.

Propozicija 1.6.3. *Neka je S podskup vektorskog prostora V i L najmanji potprostor od V koji sadrži S. Tada je $L = [S]$.*

Dokaz. Ako je $S = \emptyset$, onda je $L = \{0_V\}$, pa je $L = [S]$.

Pretpostavimo da $S \neq \emptyset$. Jasno je da je $L \subseteq [S]$ jer je $[S]$ potprostor koji sadrži skup S, a L *najmanji* takav potprostor. Pokažimo inkluziju $[S] \subseteq L$. Neka je $x \in [S]$. Tada postoje vektori $a_1, \ldots, a_k \in S$ i skalari $\alpha_1, \ldots, \alpha_k \in \mathbb{F}$ takvi da je $x = \alpha_1 a_1 + \cdots + \alpha_k a_k$. No, $a_1, \ldots, a_k \in L$, jer $S \subseteq L$ i kako je L potprostor, slijedi da je $x \in L$. □

Definicija 1.6.4. *Neka su L i M potprostori vektorskog prostora V. Potprostor $[L \cup M]$ naziva se* ***suma potprostora*** *L i M te se označava s $L + M$.*

Na temelju Propozicije 1.6.3 znamo da je $L + M$ najmanji potprostor od V koji sadrži L i M. Definicija sume potprostora proširuje se na bilo koji konačan broj potprostora pa i na bilo koju kolekciju (množinu) potprostora, moguće beskonačnu.

Prema Propoziciji 1.6.3 je $L + M = [L \cup M]$. Nadalje vrijedi da je suma konačno mnogo potprostora L_1,..., L_k od V jednaka je $L_1 + \cdots + L_k = \sum_{i=1}^k L_i = [\bigcup_{i=1}^k L_i]$, odnosno suma bilo koje množine potprostora je $\displaystyle\sum_{\alpha \in A} L_\alpha = [\bigcup_{\alpha \in A} L_\alpha]$.

Sljedeća tvrdnja opravdat će naziv *suma* i pokazati sa se svaki vektor iz $L + M$ može reprezentirati kao zbroj po jednog vektora iz L i vektora iz M.

Propozicija 1.6.5. *Neka su L i M potprostori vektorskog prostora V. Vrijedi*

$$L + M = \{a + b \,:\, a \in L,\, b \in M\}.$$

Dokaz. Stavimo $W = \{a + b \,:\, a \in L,\, b \in M\}$. Neka je $a \in L$ i $b \in M$. Tada je $a, b \in L \cup M$, pa je $a + b \in [L \cup M] = L + M$. Stoga smo pokazali da je $W \subseteq L + M$.

S druge strane, ako je $x \in L + M = [L \cup M]$, onda postoje $a_1, \ldots, a_k \in L \cup M$ i $\alpha_1, \ldots, \alpha_k \in \mathbb{F}$ takvi da je $x = \alpha_1 a_1 + \cdots + \alpha_k a_k$. Kako je $a_i \in L \cup M$, to znači da je $a_i \in L$ ili $a_i \in M$. Bez smanjenja općenitosti pretpostavimo da je prvih $1 \leq l < k$ vektora a_i iz potprostora L a preostali da su iz M. Tada je

$$x = \underbrace{\alpha_1 a_1 + \cdots + \alpha_l a_l}_{a \in L} + \underbrace{\alpha_{l+1} a_{l+1} + \cdots + \alpha_k a_k}_{b \in M} = a + b.$$

U slučaju da je $l = 0$, tj. ako su svi vektori a_i iz potprostora M stavljamo $a = 0_V$ i $b = x$, te ako je $l = k$, onda $a = x$ i $b = 0_V$. Ovim smo pokazali da je $L + M \subseteq W$. □

Teorem 1.6.6. *Neka su L i M konačnodimenzionalni potprostori vektorskog prostora V. Tada je $L + M$ konačnodimenzionalan potprostor te vrijedi*

$$\dim(L + M) = \dim L + \dim M - \dim L \cap M.$$

Dokaz. Uočimo najprije da tvrdnja teorema vrijedi u slučaju kad je jedan od potprostora L i M sadržan u drugom. Npr. ako je $L \leq M$ onda je $L \cap M = L$, $L + M = [M] = M$ pa se jednakost svodi na $\dim M = \dim L + \dim M - \dim L$.

Posebno, ako je neki od potprostora L i M jednak $\{0_V\}$ ili V, jednakost vrijedi trivijalno.

Razmotrimo nadalje slučaj kad su L i M netrivijalni potprostori, a $L \cap M = \{0_V\}$. Lako se vidi da će tada unija $B_L \cup B_M$ bilo koje baze od L i bilo koje baze od M biti baza sume $L + M$. Tada očito vrijedi jednakost iz Teorema.

Preostaje slučaj kada je $L \cap M \neq \{0_V\}$. Pretpostavimo da je $dimL = l$, $\dim M = m$ i $\dim L \cap M = k$. Neka je $B_{L \cap M} = \{c_1, \ldots, c_k\}$ baza potprostora $L \cap M$. Kako je $L \cap M \leq L, M$, bazu $B_{L \cap M}$ možemo nadopuniti do baza prostora L i M. Stoga, neka su

$$B_L = \{c_1, \ldots, c_k, a_1, \ldots, a_r\},\ B_M = \{c_1, \ldots, c_k, b_1, \ldots, b_s\}$$

baze za L i M. Uočimo da je $k + r = l$ i $k + s = m$. Sada formiramo skup

$$B = B_L \cup B_M = \{c_1, \ldots, c_k, a_1, \ldots, a_r, b_1, \ldots, b_s\}.$$

Jasno je da je B jedan sustav izvodnica za $[L \cup M] = L + M$. No, vrijedi i više - B je baza za $L + M$ jer je B linearno nezavisan skup. Zaista, pretpostavimo da je

$$\sum_{i=1}^{k} \gamma_i c_i + \sum_{i=1}^{r} \alpha_i a_i + \sum_{i=1}^{s} \beta_i b_i = 0_V, \tag{1.5}$$

za neke skalare $\alpha_i, \beta_i, \gamma_i$. Uočimo da je vektor

$$x = \sum_{i=1}^{k} \gamma_i c_i + \sum_{i=1}^{r} \alpha_i a_i = \sum_{i=1}^{s} (-\beta_i) b_i,$$

iz L i iz M, pa je x iz $L \cap M$. Odatle slijedi da je linearna kombinacija vektora a_i, to jest

$$\sum_{i=1}^{r} \alpha_i a_i = x - \sum_{i=1}^{k} \gamma_i c_i$$

također iz $L \cap M$ što je jedino zadovoljeno za 0_V. Kako je $\{a_1, \ldots, a_r\}$ linearno nezavisan skup, nužno vrijedi $\alpha_1 = \cdots = \alpha_r = 0$. Sada (1.5) povlači

$$\sum_{i=1}^{k} \gamma_i c_i + \sum_{i=1}^{s} \beta_i b_i = 0_V,$$

pa je $\gamma_1 = \cdots = \gamma_k = \beta_1 = \cdots = \beta_s = 0$. Dakle, B je baza za $L + M$ i stoga

$$\dim(L + M) = k + r + s = (k + r) + (k + s) - k = \dim L + \dim M - \dim L \cap M.$$

□

Definicija 1.6.7. *Za sumu potprostora L i M kažemo da je* ***direktna suma*** *ako $L \cap M = \{0_V\}$. Tada pišemo $L \dot{+} M$.*

Propozicija 1.6.8. *Suma potprostora L i M je direktna ako i samo ako za svaki $x \in L + M$ postoje jedinstveni $a \in L$ i $b \in M$ takvi da je $x = a + b$.*

Dokaz. Pretpostavimo da je suma direktna, tj. $L \dot{+} M$. Prema Propoziciji 1.6.5 znamo da za svaki $x \in L + M$ postoje $a \in L$ i $b \in M$ takvi da je $x = a + b$. Još trebamo pokazati njihovu jedinstvenost. Pretpostavimo suprotno. Neka su i $a' \in L$ i $b' \in M$ takvi da je $x = a' + b'$. Iz $x = a + b = a' + b'$ slijedi da je $a - a' = b' - b$. Stoga je $y = a - a' \in L$ i $y = b' - b \in M$, odnosno $y \in L \cap M$. Kako je suma direktna, $L \cap M = \{0_V\}$, pa je $y = 0_V$, tj. $a = a'$ i $b = b'$.

Sada pokažimo obrat. Pretpostavimo da se svaki vektor iz $L + M$ jedinstveno prikazuje kao zbroj vektora iz L i vektora iz M, te pretpostavimo da $L \cap M \neq \{0_V\}$. Znači da postoji $a \in L \cap M$ i $a \neq 0_V$. U tom slučaju za nulvektor vrijede dva različita prikaza oblika $a + b$, $a \in L$ i $b \in M$,

$$0_V = 0_V + 0_V, \; 0_V = \underbrace{a}_{\in L \cap M \leq L} + \underbrace{(-a)}_{\in L \cap M \leq M},$$

a to je u kontradikciji s pretpostavkom. Dakle, $L \cap M = \{0_V\}$. □

Korolar 1.6.9. *Suma potprostora L i M je direktna ako i samo ako*

$$\dim(L+M) = \dim L + \dim M.$$

Korolar 1.6.10. *Ako je suma potprostora L i M direktna, te ako su B_L i B_M baze potprostora L i M, respektivno, onda je $B_L \cup B_M$ baza potprostora $L \dot{+} M$.*

Propozicija 1.6.11. *Neka je L potprostor konačnodimenzionalnog vektorskog prostora V. Tada postoji potprostor M od V takav da je $V = L \dot{+} M$.*

Dokaz. Ako je $L = \{0_V\}$, onda je $M = V$. I obrnuto, ako je $L = V$, onda $M = \{0_V\}$.

Neka je L netrivijalan potprostor od V. Stoga je $1 \leq \dim L = k < \dim V = n$. Bazu potprostora L,

$$B_L = \{a_1, \dots, a_k\}$$

nadopunimo do baze čitavog prostora V:

$$B = \{a_1, \dots, a_k, a_{k+1}, \dots, a_n\}.$$

Tvrdimo da je $M = [a_{k+1}, \dots, a_n]$. Zaista, za $x \in V$ postoje $\alpha_1, \dots, \alpha_n \in \mathbb{F}$ za koje je

$$x = \sum_{i=1}^{n} \alpha_i a_i = \underbrace{\sum_{i=1}^{k} \alpha_i a_i}_{a \in L} + \underbrace{\sum_{i=k+1}^{n} \alpha_i a_i}_{b \in M} = a + b,$$

pa je $x \in L + M$, odnosno $V \leq L + M$. Kako je uvijek $L + M \leq V$, slijedi $V = L + M$. Još moramo vidjeti da je suma direktna. Ako je $y \in L \cap M$, onda je

$$y = \sum_{i=1}^{k} \alpha_i a_i \in L, \;\; y = \sum_{i=k+1}^{n} \alpha_i a_i \in M.$$

Otuda je

$$\sum_{i=1}^{k} \alpha_i a_i + \sum_{i=k+1}^{n} (-\alpha_i) a_i = 0_V.$$

Kako je $\{a_1, \dots, a_n\}$ baza za V, slijedi $\alpha_1 = \cdots = \alpha_n = 0$. Dakle, $y = 0_V$ i $L \cap M = \{0_V\}$. $\square$

Prema prethodnoj propoziciji sljedeća je definicija je smislena.

Definicija 1.6.12. *Ako je L potprostor prostora V, onda se potprostor M za koji vrijedi da je $V = L \dot{+} M$ naziva* ***direktni komplement*** *potprostora L. Još kažemo da smo V* rastavili na direktnu sumu potprostora *L i M.*

Propozicija 1.6.11 kaže da svaki potprostor konačnodimenzionalnog vektorskog prostora ima direktni komplement. Važno je naglasiti da on ne mora biti jedinstven.

Primjer 23. Pokazat ćemo na dva načina kako naći baze za sumu i presjek potprostora M i N u $\mathbb{R}^5$ koji su zadani svojim bazama: $B_M = \{a_1, a_2, a_3\}$ i $B_N = \{b_1, b_2, b_3\}$, gdje su

$$a_1 = (1, 0, 0, 0, 0), a_2 = (0, 1, -1, 0, 0), a_3 = (1, 0, 0, 1, 0),$$

te

$$b_1 = (0, 0, 0, -1, 0), b_2 = (0, 0, 1, 0, 0), b_3 = (1, 1, -2, 0, 0).$$

<u>*I. način:*</u> Prvo ćemo odrediti bazu sume potprostora, $M+N$, a zatim za presjek $M \cap N$. Skup $B_M \cup B_N$ čini sustav izvodnica za $M + N$, a baza za $M + N$ je njen maksimalan linearno nezavisan podskup. Do nje operativno dolazimo tako što bazu za M redom nadopunjavamo vektorima iz N i provjeravamo linearnu nezavisnost "nadopunjenog" skupa. Ako je skup linearno zavisan, odbacujemo vektor iz B_N, dok ga u suprotnom zadržavamo. Za provjeru linearne (ne)zavisnosti skupa koristit ćemo se Propozicijom 1.3.12 kroz sljedeća tri koraka:

- Provjeravam linearnu (ne)zavisnost skupa

$$\{ \underbrace{a_1, a_2, a_3}_{lin.\ nezavisan}, b_1\}$$

tako što ispitujemo može li se nadodani vektor b_1 prikazati kao linearna kombinacija svojih prethodnika:

$$b_1 = \alpha_1 a_1 + \alpha_2 a_2 + \alpha_3 a_3.$$

Rješavanjem prethodne jednadžbe dobiva se

$$b_1 = a_1 - a_3 \tag{1.6}$$

Dakle, skup $\{a_1, a_2, a_3, b_1\}$ je linearno zavisan pa vektor b_1 odbacujemo.

- Ispitujemo linearnu (ne)zavisnost skupa

$$\{\underbrace{a_1, a_2, a_3}_{lin.\ nez.}, b_2\}.$$

Pokazuje se da jednadžba

$$b_2 = \alpha_1 a_1 + \alpha_2 a_2 + \alpha_3 a_3$$

nema rješenja (tj. odgovarajući sustav linearnih jednadžbi je nekonzistentan) i stoga je skup $\{a_1, a_2, a_3, b_2\}$ linearno nezavisan.

- Ispitujemo linearnu (ne)zavisnost skupa

$$\{\underbrace{a_1, a_2, a_3, b_2}_{lin.\ nez.}, b_3\}.$$

Rješavanjem jednadžbe

$$b_3 = \alpha_1 a_1 + \alpha_2 a_2 + \alpha_3 a_3 + \beta_2 b_2$$

dobivamo da je

$$b_3 = a_1 + a_2 - b_2, \tag{1.7}$$

odnosno da je skup $\{a_1, a_2, a_3, b_2, b_3\}$ je linearno zavisan. Odbacujemo vektor b_3.

Sada možemo zaključiti da je skup $\{a_1, a_2, a_3, b_2\}$ maksimalan linearno nezavisan podskup od $B_M \cup B_N$ pa stoga čini jednu bazu za $M+N$. Nadalje, kako je $\dim(M+N) = 4$, prema formuli za dimenziju presjeka i sume potprostora (Teorem 1.6.6) slijedi da je

$$\dim M \cap N = \dim M + \dim N - \dim(M+N) = 2.$$

Kako bismo odredili bazu za $M \cap N$, iskorist ćemo "odbačene" vektore b_1 i b_3, odnosno preciznije relacije (1.6) i (1.7). Uočimo da nam te relacije daju dva vektora koja se nalaze upravo u presjeku:

$$\underbrace{b_1}_{\in N} = \underbrace{a_1 - a_3}_{\in M}, \quad \underbrace{b_2 + b_3}_{\in N} = \underbrace{a_1 + a_2}_{\in M}.$$

Skup $\{b_1, b_2 + b_3\} = \{(0,0,0,-1,0), (1,1,-1,0,0)\}$ linearno je nezavisan pa je to baza za presjek potprostora $M \cap N$.

II. način: Najprije ćemo odrediti bazu presjeka $M \cap N$. Krenimo od toga da se u presjeku potprostora nalaze svi vektori koji se mogu prikazati kao linearne kombinacije vektora a_i, $i = 1,2,3$, a također i vektora b_i, $i = 1,2,3$:

$$v \in M \cap N \Leftrightarrow v = \alpha_1 a_1 + \alpha_2 a_2 + \alpha_3 a_3 = \beta_1 b_1 + \beta_2 b_2 + \beta_3 b_3, \text{ za neke } \alpha_i, \beta_i \in \mathbb{R}.$$

Jednadžba $\sum_{i=1}^{3} \alpha_i a_i = \sum_{i=1}^{3} \beta_i b_i$ svodi se sustav linearnih jednadžbi

$$\begin{aligned} \alpha_1 + \alpha_3 - \beta_3 &= 0, \\ \alpha_2 - \beta_3 &= 0, \\ -\alpha_2 - \beta_2 + 2\beta_3 &= 0, \\ \alpha_3 + \beta_1 &= 0, \end{aligned}$$

čije je rješenje

$$\alpha_3 = -\alpha_1 + \alpha_2, \beta_1 = \alpha_1 - \alpha_2, \beta_2 = \alpha_2, \beta_3 = \alpha_2,$$

za sve $\alpha_1, \alpha_2 \in \mathbb{R}$. Stoga je $M \cap N$ skup svih vektora $v \in \mathbb{R}^5$ oblika

$$v = \alpha_1 a_1 + \alpha_2 a_2 + (-\alpha_1 + \alpha_2) a_3 = \alpha_1 (a_1 - a_3) + \alpha_2 (a_2 + a_3), \forall \alpha_1, \alpha_2 \in \mathbb{R}.$$

Dakle, skup

$$\{a_1 - a_3, a_2 + a_3\} = \{(0,0,0,-1,0), (1,1,-1,1,0)\}$$

razapinje $M \cap N$ i očito je linearno nezavisan pa je to jedna baza za $M \cap N$. Formula za dimenziju presjeka i sume potprostora (Teorem 1.6.6) daje nam

$$\dim(M+N) = \dim M + \dim N - \dim M \cap N = 4$$

i stoga bazu za $M \cap N$ trebamo nadopuniti s dva vektora iz $B_M \cup B_N$ tako da taj četveročlani skup bude linearno nezavisan. Pokazuje se da je skup $\{a_1 - a_3, a_2 + a_3, a_1, b_2\}$ linearno nezavisan i stoga predstavlja jednu bazu za $M+N$. (Uočite da skup $\{a_1 - a_3, a_2 + a_3, a_1, b_1\}$ nije baza za $M+N$ jer je $b_1 = a_1 - a_3$, tj. taj skup je linearno zavisan).

♡

Zadatak 12. Zadani su potprostori $L = [(1,0,-1), (1,2,1)]$ i $M = [(0,0,1), (1,1,0)]$ u $\mathbb{R}^3$. Odredite po jednu bazu za $L \cap M$ i $L + M$.

♡

Poglavlje 2

Matrice

2.1 Definicija matrice. Vektorski prostor $M_{mn}(\mathbb{F})$.

Definicija 2.1.1. *Neka su $m, n \in \mathbb{N}$. Preslikavanje*

$$A : \{1, \ldots, m\} \times \{1, \ldots, n\} \to \mathbb{F}$$

naziva se ***matrica tipa*** *(m, n) (ili $m \times n$) s koeficijentima (ili elementima) iz polja $\mathbb{F}$. Skup svih takvih označavamo s $M_{mn}(\mathbb{F})$.*

Dakle, matrica A uređenom paru (i, j), $1 \leq i \leq m$, $1 \leq j \leq n$, pridružuje neki skalar iz polja $\mathbb{F}$. Uobičajeno je te funkcijske vrijednosti $A(i, j)$ označiti s a_{ij} te ih zapisati u pravokutnu shemu, odnosno tabelarno na sljedeći način

$$A = \begin{bmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ a_{21} & a_{22} & \ldots & a_{2n} \\ \vdots & \vdots & \ldots & \vdots \\ a_{m1} & a_{m2} & \ldots & a_{mn} \end{bmatrix}.$$

Umjesto uglatih zagrada često koristimo i okrugle zagrade . Elementi matrice A raspoređeni su u m *redaka* i n *stupaca.* Uređenu n-torku

$$(a_{i1}, a_{i2}, \ldots, a_{in})$$

nazivamo i*-ti redak* matrice A, a uređenu m-torku

$$(a_{1j}, a_{2j}, \ldots, a_{mj})$$

j*-ti stupac* matrice A. Elementi matrice A indeksirani su na način koji odmah ukazuje na njihov položaj u matrici. Element a_{ij} nalazi se na presjeku i-tog retka i j-tog stupca. U različitim situacijama bit će nam praktičnije taj element označiti s $[A]_{ij}$ ili $(A)_{ij}$, a čitavu matricu kraće ćemo zapisati kao $A = (a_{ij})$ ili $A = [a_{ij}]$.

Definicija 2.1.2. *Matrica tipa (n, n) naziva se* ***kvadratna matrica*** *ili* ***matrica reda*** *n. Skup svih matrica reda n s elementima iz $\mathbb{F}$ označavamo s $M_n(\mathbb{F})$.*

Ako je $A = [a_{ij}] \in M_n(\mathbb{F})$, onda uređenu n-torku

$$(a_{11}, a_{22}, \ldots, a_{nn})$$

zovemo ***glavnom dijagonalom*** *(ili samo* dijagonalom*) matrice A. Uređenu n-torku*

$$(a_{1n}, a_{2,n-1}, \dots, a_{n1})$$

zovemo ***sporednom dijagonalom*** *matrice A.*

Definicija 2.1.3. *Matrica tipa $(m,1)$ naziva se* ***stupčana****, a matrica tipa $(1,n)$ -* ***retčana****.*

Na primjer, matrica $\begin{pmatrix} 1 & 2 & 3 \end{pmatrix}$ je retčana matrica, a $\begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix}$ je stupčana matrica.

Definicija 2.1.4. *Matrice $A = [a_{ij}]$ i $B = [b_{ij}]$ su* ***jednake*** *što pišemo $A{=}B$ ako su jednake kao preslikavanja, to jest ako su istog tipa te ako su im elementi na odgovarajućim pozicijama jednaki. (Ako su A i B tipa (m,n), onda $a_{ij} = b_{ij}$ za sve $i = 1,\dots,m$ i $j = 1,\dots,n$.)*

Sada ćemo uvesti osnovne operacije s matricama - zbrajanje matrica i množenje matrica skalarom. Operacije se definiraju prirodno - po elementima matrice što je u skladu s činjenicom da smo matrice definirali kao preslikavanja. Naime, zbrajanje funkcija i množenje funkcija skalarom realizirali smo po točkama.

Definicija 2.1.5. ***Zbroj matrica*** *$A = [a_{ij}]$ i $B = [b_{ij}]$ tipa (m,n) je matrica $C = [c_{ij}]$ tipa (m,n) za čije elemente vrijedi*

$$c_{ij} = a_{ij} + b_{ij},$$

za sve $i = 1,\dots,m$ i $j = 1,\dots,n$. Pišemo $C = A + B$.

Napomenimo da **ne definiramo** zbroj matrica različitog tipa. Na primjer, nije definirano

$$\begin{pmatrix} 1 & -1 \\ 3 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 1 & 3 \\ -1 & 2 & 2 \end{pmatrix}.$$

Definicija 2.1.6. ***Nulmatrica*** *je matrica čiji su svi elementi jednaki nuli. Označavat ćemo je s 0 ili s 0_{mn} ako želimo istaknuti da je tipa (m,n).*

Propozicija 2.1.7. *Skup matrica $M_{mn}(\mathbb{F})$ uz operaciju zbrajanja matrica je Abelova grupa.*

Dokaz. Zbrajanje matrica je očito binarna operacija koja je asocijativna i komutativna jer se operacija definira po elementima matrice, a oni su iz polja $\mathbb{F}$. Neutralni element je nulmatrica, 0_{mn}. Svaka matrica $A = [a_{ij}]$ ima suprotnu matricu $-A = [-a_{ij}]$. □

Definicija 2.1.8. ***Umnožak matrice*** *$A = [a_{ij}]$ tipa (m,n)* ***skalarom*** *$\lambda \in \mathbb{F}$ je matrica $B = [b_{ij}]$ tipa (m,n) za čije elemente vrijedi*

$$b_{ij} = \lambda a_{ij},$$

za sve $i = 1,\dots,m$ i $j = 1,\dots,n$. Pišemo $B = \lambda A$.

Teorem 2.1.9. *Skup matrica $M_{mn}(\mathbb{F})$ uz operacije zbrajanja matrica i množenje matrica skalarom je vektorski prostor nad poljem $\mathbb{F}$ čija je dimenzija jednaka $m \cdot n$.*

Dokaz. Pokazali smo da je $(M_{mn}(\mathbb{F}), +)$ Abelova grupa, a ostala pravila (kvaziasocijativnosti, obje distributivnosti i množenje s 1) vrijede jer su operacije definirane po elementima (točkama).

Neka je $A = [a_{ij}] \in M_{mn}(\mathbb{F})$. Tada je

$$A = \sum_{i=1}^{m} \sum_{j=1}^{n} a_{ij} E_{ij},$$

gdje je E_{ij} matrica čiji su svi elementi jednaki nuli osim elementa na presjeku i-tog retka i j-tog stupca, odnosno

$$[E_{ij}]_{kl} = \begin{cases} 1, & k = i,\ l = j \\ 0, & \text{inače} \end{cases}.$$

Skup $B = \{E_{ij} : i = 1, \ldots, m,\ j = 1, \ldots, n\}$ je očito sustav izvodnica za $M_{mn}(\mathbb{F})$ i linearno nezavisan skup (jer se očito niti jedna matrica E_{ij} ne može prikazati kao linearna kombinacija preostalih matrica iz B). Dakle, skup B je baza za $M_{mn}(\mathbb{F})$, pa je $\dim M_{mn}(\mathbb{F}) = |B| = mn$. □

Napomenimo da se svaka $A = [a_{ij}]$ tipa (m, n) može shvatiti kao uređena mn-torka

$$(a_{11}, \ldots, a_{1n}, a_{21}, \ldots, a_{2n}, \ldots, a_{m1}, \ldots, a_{mn}).$$

Dakle, postoji prirodna bijekcija $M_{mn}(\mathbb{F}) \to \mathbb{F}^{mn}$. Stoga je tvrdnja Teorema 2.1.9 usklađena s činjenicom da je i $\mathbb{F}^{mn}$ vektorski prostor nad poljem $\mathbb{F}$ dimenzije mn. Takve prostore zovemo *izomorfnima* a tome će više biti govora na kolegiju *Linearna algebra 2.*

2.2 Neke posebne matrice

U ovom dijelu istaknut ćemo neke matrice koje su posebne 'sadržajem' odnosno nekim specifičnim svojstvom koje zadovoljavaju.

Definicija 2.2.1. *Matrica reda n*

- *$D = (d_{ij})$ je* ***dijagonalna*** *ako $d_{ij} = 0$ za sve $i \neq j$.*
- *$S = (s_{ij})$ je* ***skalarna*** *ako je dijagonalna i $s_{ii} = \alpha$ za sve $i = 1, \ldots, n$.*
- *$I = (\delta_{ij})$ je* ***jedinična*** *ako je skalarna i $\delta_{ii} = 1$ za sve $i = 1, \ldots, n$.*
- *$G = (g_{ij})$ je* ***gornjetrokutasta*** *ako je $g_{ij} = 0$ za sve $1 \leq j < i \leq n$.*
- *$H = (h_{ij})$ je* ***donjetrokutasta*** *ako je $h_{ij} = 0$ za sve $1 \leq i < j \leq n$.*

Konkretno, pogledajmo neke primjere upravo definiranih matrica:

- $D = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 2 \end{pmatrix}$ je dijagonalna matrica. Kraće pišemo $D = \mathrm{diag}(1, 0, 2)$.
- $S = \begin{pmatrix} 2 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 2 \end{pmatrix}$ je skalarna matrica.
- $I = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ je jedinična matrica (reda 3). Uočimo, $S = 2I$.
- $G = \begin{pmatrix} 1 & 0 & 2 \\ 0 & 3 & 3 \\ 0 & 0 & 0 \end{pmatrix}$ je gornjetrokutasta matrica.
- $H = \begin{pmatrix} 1 & 0 & 0 \\ 2 & 3 & 0 \\ -1 & 0 & 2 \end{pmatrix}$ je donjetrokutasta matrica.

Primjer 24. Sljedeći skupovi:

- skup svih dijagonalnih matrica reda n,
- skup svih skalarnih matrica reda n,
- skup svih gornjetrokutastih (donjetrokutastih) matrica reda n

predstavljaju vektorske potprostore od $M_n(\mathbb{F})$ dimenzija n, 1 i $\frac{n(n+1)}{2}$, respektivno. Zaista, lako se ustanovi da su gornji skupovi zatvoreni na zbrajanje matrica i množenje matrica skalarom. Dalje, skup

$$B_D = \{E_{ii} \,:\, i = 1, \ldots, n\}$$

je baza za potprostor dijagonalnih matrica reda n. Skup

$$B_S = \{I\}$$

je baza za potprostor skalarnih matrica reda n, a

$$B_G = \{E_{ij} \,:\, 1 \le i \le j \le n\}$$

baza za potprostor gornjetrokutastih matrica reda n. ♡

Definicija 2.2.2. *Neka je $A = [a_{ij}] \in M_{mn}(\mathbb{F})$.* ***Transponirana matrica*** *matrice A je matrica $B = [b_{ij}] \in M_{nm}(\mathbb{F})$ za čije elemente vrijedi*

$$b_{ij} = a_{ji},$$

za sve $i = 1, \ldots, n$, $j = 1, \ldots, m$. Pišemo $B = A^t$.

Operacija

$$t : M_{mn}(\mathbb{F}) \to M_{nm}(\mathbb{F}),\ A \mapsto A^t,$$

naziva se ***transponiranje****.*

Ponekad se transponirana matrica označava s A^τ ili s A'.

Primjer 25. Neka je

$$A = \begin{pmatrix} 1 & 2 \\ 3 & 4 \\ 5 & 6 \end{pmatrix}.$$

Tada je

$$A^t = \begin{pmatrix} 1 & 3 & 5 \\ 2 & 4 & 6 \end{pmatrix}.$$

Uočimo da redci matrice A predstavljaju stupce matrice A^t i obratno.

♡

Propozicija 2.2.3. *Neka su $A, B \in M_{mn}(\mathbb{F})$, te $\lambda \in \mathbb{F}$. Vrijedi*

(1) $(A^t)^t = A$,

(2) $(A+B)^t = A^t + B^t$,

(3) $(\lambda A)^t = \lambda A^t$.

Dokaz. Svaka od tvrdnji se dokazuje na isti način. Prvo ustanovimo da se s lijeve i desne strane jednakosti nalaze matrice istog tipa, a zatim pokažemo jednakost odgovarajućih elemenata. Na primjer, u (2) vidimo da su $(A+B)^t$ i $A^t + B^t$ tipa (m, n) i vrijedi

$$[(A+B)^t]_{ij} = [A+B]_{ji} = [A]_{ji} + [B]_{ji} = [A^t]_{ij} + [B^t]_{ij} = [A^t + B^t]_{ij},$$

za sve $i = 1, \ldots, n$ i $j = 1, \ldots, m$. □

Definicija 2.2.4. *Matrica $A \in M_n(\mathbb{F})$ je **simetrična** ako vrijedi*

$$A = A^t,$$

*odnosno **antisimetrična** ako*

$$A = -A^t.$$

Primjer 26. Neka su $\mathcal{S}$, odnosno $\mathcal{A}$ skup svih simetričnih, odnosno antisimetričnih matrica reda n s elementima iz polja $\mathbb{R}$. Tada su $\mathcal{S}$ i $\mathcal{A}$ vektorski potprostori od $M_n(\mathbb{R})$. Zaista, ako su $A, B \in \mathcal{S}$ i $\lambda \in \mathbb{R}$ tada je

$$(\lambda A + B)^t = \{\textit{Prop. 2.2.3}\} = \lambda A^t + B^t = \lambda A + B,$$

pa je matrica $\lambda A + B$ simetrična, to jest $\lambda A + B \in \mathcal{S}$. Znači, $\mathcal{S} \leq M_n(\mathbb{R})$. Analogno, za $A, B \in \mathcal{A}$ imamo

$$(\lambda A + B)^t = \lambda A^t + B^t = \lambda(-A) + (-B) = -(\lambda A + B),$$

pa je $\lambda A + B \in \mathcal{A}$, odnosno $\mathcal{A} \leq M_n(\mathbb{R})$.

Uočimo da je nulmatrica jedina realna matrica reda n koja je i simetrična i antisimetrična. Naime, ako za matricu A vrijedi $A = A^t$ i $A^t = -A$, to znači da je $A = -A$ pa je tada $A = 0$. Dakle, presjek potprostora $\mathcal{S} \cap \mathcal{A} = \{0\}$.

Odredimo sada dimenzije potprostora $\mathcal{S}$ i $\mathcal{A}$. Prema definiciji simetrične matrice jasno je da je $A \in \mathcal{S}$ ako i samo ako je oblika

$$A = \begin{pmatrix} a_{11} & a_{12} & a_{13} & \dots & a_{1n} \\ a_{12} & a_{22} & a_{23} & \dots & a_{2n} \\ a_{13} & a_{23} & a_{33} & \dots & a_{3n} \\ \vdots & \vdots & \vdots & \dots & \vdots \\ a_{1n} & a_{2n} & a_{3n} & \dots & a_{nn} \end{pmatrix}.$$

Vidimo da je

$$A = \sum_{i=1}^{n} a_{ii} E_{ii} + \sum_{i=1}^{n-1} \sum_{j=i+1}^{n} a_{ij}(E_{ij} + E_{ji}),$$

gdje je E_{ij} matrica reda n koja na mjestu (i, j) ima vrijednost 1, a na svim ostalim mjestima se nalazi 0. Stoga skup

$$\{E_{ii} \, : \, i = 1, \dots, n\} \cup \{E_{ij} + E_{ji} \, : \, 1 \le i < j \le n\}$$

predstavlja sustav izvodnica za $\mathcal{S}$, ali i bazu jer se lako može ustanoviti da je linearno nezavisan. Broj elemenata tog skupa je

$$n + (1 + 2 + \ldots + n - 1) = n + \frac{(n-1)n}{2} = \frac{n(n+1)}{2},$$

pa je

$$\dim \mathcal{S} = \frac{n(n+1)}{2}.$$

Slično, $B \in \mathcal{A}$ ako i samo ako je

$$B = \begin{pmatrix} 0 & b_{12} & b_{13} & \dots & b_{1n} \\ -b_{12} & 0 & b_{23} & \dots & b_{2n} \\ -b_{13} & -b_{23} & 0 & \dots & b_{3n} \\ \vdots & \vdots & \vdots & \dots & \vdots \\ -b_{1n} & -b_{2n} & -b_{3n} & \dots & 0 \end{pmatrix}.$$

Uočavamo da su dijagonalni elementi antisimetrične matrice jednaki 0 jer iz definicije slijedi da je $b_{ii} = -b_{ii}$, odnosno $2b_{ii} = 0$ što povlači da je $b_{ii} = 0$ za sve $i = 1, \dots, n$. Dalje, možemo ustanoviti da skup

$$\{E_{ij} - E_{ji} \, : \, 1 \le i < j \le n\}$$

predstavlja bazu za $\mathcal{A}$ pa je

$$\dim \mathcal{A} = 1 + 2 + \ldots + n - 1 = \frac{(n-1)n}{2}.$$

Uočimo i ovo

$$\dim \mathcal{S} + \dim \mathcal{A} = \frac{n(n+1)}{2} + \frac{(n-1)n}{2} = n^2 = \dim M_n(\mathbb{R}).$$

Kako je $\dim(\mathcal{S}\cap\mathcal{A}) = 0$, suma potprostora $\mathcal{S}+\mathcal{A}$ je direktna pa po Korolaru 1.6.9 vrijedi $\dim(\mathcal{S}\dot{+}\mathcal{A}) = \dim\mathcal{S} + \dim\mathcal{A}$. Tada je $\dim(\mathcal{S}\dot{+}\mathcal{A}) = n^2 = \dim M_n(\mathbb{R})$. Iz Propozicije 1.5.6. slijedi da je

$$\mathcal{S}\dot{+}\mathcal{A} = M_n(\mathbb{R}).$$

Naime, $\mathcal{S}\dot{+}\mathcal{A}$ je potprostor dimenzije jednake dimenziji cijelog prostora pa je ta suma jednaka prostoru $M_n(\mathbb{R})$. Kao posljedicu te činjenice dobivamo da se *svaka kvadratna matrica može jedinstveno prikazati kao zbroj jedne simetrične i jedne antisimetrične matrice.* Konkretno, za $C \in M_n(\mathbb{R})$ iz $C = X + Y$, pri čemu $X = X^t$ i $Y = -Y^t$, lako se dobiva

$$C = \underbrace{\frac{1}{2}(C + C^t)}_{X} + \underbrace{\frac{1}{2}(C - C^t)}_{Y}.$$

♡

Za kvadratne matrice definirat ćemo još i pojam *traga matrice*, čija važnost će više doći do izražaja u Linearnoj algebri 2.

Definicija 2.2.5. *Neka je $A = [a_{ij}] \in M_n(\mathbb{F})$.* ***Trag*** *matrice A, u oznaci $\operatorname{tr} A$, jednak je zbroju svih koeficijenata na dijagonali, to jest*

$$\operatorname{tr} A = \sum_{i=1}^{n} a_{ii}.$$

Tako je zadano preslikavanje $\operatorname{tr} A : M_n(\mathbb{F}) \to \mathbb{F}$ koje matrici A pridružuje njezin trag $\operatorname{tr} A$.

Zadatak 13. *Neka su $A, B \in M_n(\mathbb{F})$, te $\lambda \in \mathbb{F}$. Dokažite da vrijedi:*

(i) $\operatorname{tr}(A + B) = \operatorname{tr} B$, $\operatorname{tr}(\lambda A) = \lambda \operatorname{tr} A$.

(ii) Skup $\{A \in M_n(\mathbb{F}) : \operatorname{tr} A = 0\}$ je potprostor vektorskog prostora $M_n(\mathbb{F})$. Odredite jednu bazu i dimenziju tog potrostora.

2.3 Množenje matrica

Definicija 2.3.1. *Matrice A i B su* ***ulančane*** *ako je broj stupaca matrice A jednak broju redaka matrice B.*

Često govorimo o paru ulančanih matrica (A, B) iz razloga što ovo svojstvo nije općenito simetrično. Zaista, ako je A tipa (m, n) i B tipa (n, p), onda je par matrica (A, B) ulančan, dok je par (B, A) ulančan samo ako je $m = p$.

Definicija 2.3.2. *Neka su $A = [a_{ij}]$ i $B = [b_{ij}]$ ulančane matrice tipa (m, n) i (n, p), respektivno.* ***Umnožak matrica*** *A i B je matrica $C = [c_{ij}]$ tipa (m, p) čiji su elementi dani sljedećom formulom*

$$c_{ij} = a_{i1}b_{1j} + a_{i2}b_{2j} + \cdots + a_{in}b_{nj} = \sum_{k=1}^{n} a_{ik}b_{kj},$$

za $i = 1, \ldots, m$, $j = 1, \ldots, p$. *Pišemo,* $C = A \cdot B = AB$. *Na ovaj način definirali smo operaciju* ***množenja matrica***

$$\cdot : M_{mn}(\mathbb{F}) \times M_{np}(\mathbb{F}) \to M_{mp}(\mathbb{F}).$$

Prvo što opažamo da je množenje matrice bitno složenija operacija od svih do sada definiranih operacijama na matricama (zbrajanje, množenje matrica skalarom, transponiranje). Možda to na prvi pogled izgleda čudno, no vidjet ćemo da ovakva definicija množenja itekako ima smisla. Ukratko, možemo pamtiti da (i, j)-ti element produkta AB dobivamo tako što i-ti redak matrice A, $(a_{i1}, \ldots, a_{in})$, pomnožimo *skalarno* s j-tim stupcem matrice B, $(b_{1j}, \ldots, b_{nj})$.

Jedan od razloga ovakve definicije množenja matrica možemo vidjeti na sljedećem primjeru.

Primjer 27. Zadan je sustav linearnih jednadžbi

$$\begin{array}{ccccc} 2x_1 & - & 3x_2 & = & 1 \\ 4x_1 & + & 5x_2 & = & 2 \end{array}.$$

Zamislimo da ga želimo zapisati u obliku jedne linearne jednadžbe $ax = b$. Jasno je da umjesto koeficijenta a imamo 'paket koeficijenata' uz nepoznanice x_1 i x_2. Taj je 'paket koeficijenata' prirodno zapisati kao matricu

$$A = \begin{pmatrix} 2 & -3 \\ 4 & 5 \end{pmatrix}.$$

Analogno tome slobodne koeficijente zapisujemo kao stupčastu matricu

$$B = \begin{pmatrix} 1 \\ 2 \end{pmatrix},$$

a nepoznanice kao

$$X = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}.$$

Uočimo da je

$$AX = \begin{pmatrix} 2 & -3 \\ 4 & 5 \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} 2x_1 - 3x_2 \\ 4x_1 + 5x_2 \end{pmatrix},$$

pa dani sustav ima isti zapis kao i linearna jednadžba s jednom nepoznanicom, $AX = B$.

♡

Sada ćemo pokazati osnovna svojstva množenja matrica. Neka od tih svojstva su na prvi pogled neobična, baš kao što je i sama definicija množenja. Tako množenje matrica općenito *nije komutativna operacija.* Za početak, uočimo da je o komutativnosti smisleno govoriti samo ako su A i B kvadratne matrice istog reda. Zaista, ako nisu i ako je umnožak AB definiran, BA to ne treba biti jer smo već napomenuli da svojstvo *biti ulančan* nije simetrično. Nadalje, ako A i B nisu kvadratne nego tipa (m, n) i (n, m), onda su oba umnoška definirana, AB i BA. No, to su kvadratne matrice različitih redova (AB je reda m, a BA je reda n)

Primjer 28. Vrijedi

$$AB = \begin{pmatrix} 1 & 2 \\ 3 & 1 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 2 \end{pmatrix} = \begin{pmatrix} 2 & 5 \\ 1 & 5 \end{pmatrix}, \quad BA = \begin{pmatrix} 0 & 1 \\ 1 & 2 \end{pmatrix}\begin{pmatrix} 1 & 2 \\ 3 & 1 \end{pmatrix} = \begin{pmatrix} 3 & 1 \\ 7 & 4 \end{pmatrix}.$$

Dakle, $AB \neq BA$, odnosno množenje matrica *nije komutativna operacija.* S druge strane, postoje matrice koje *komutiraju.* Na primjer,

$$\begin{pmatrix} 1 & 1 \\ -2 & 1 \end{pmatrix}\begin{pmatrix} 1 & -1 \\ 2 & 1 \end{pmatrix} = \begin{pmatrix} 3 & 0 \\ 0 & 3 \end{pmatrix}, \quad \begin{pmatrix} 1 & -1 \\ 2 & 1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ -2 & 1 \end{pmatrix} = \begin{pmatrix} 3 & 0 \\ 0 & 3 \end{pmatrix}.$$

♡

Propozicija 2.3.3. *Vrijedi*

$$(AB)C = A(BC),$$

za sve matrice za koje je gornji izraz definiran.

Dokaz. Neka je A matrica tipa (m,n), B tipa (n,p) i C tipa (p,q). Lako možemo ustanoviti da su matrice $(AB)C$ i $A(BC)$ tipa (m,q). Zaista, matrica AB je tipa (m,p), pa je $(AB)C$ tipa (m,q). Nadalje, BC je (n,q), pa je $A(BC)$ također tipa (m,q).

Provjerimo sada jednakost odgovarajućih elemenata tih matrice,

$$\begin{aligned} [(AB)C]_{ij} &= \sum_{k=1}^{p}[AB]_{ik}[C]_{kj} = \sum_{k=1}^{p}\left(\sum_{l=1}^{n}[A]_{il}[B]_{lk}\right)[C]_{kj} \\ &= \sum_{l=1}^{n}[A]_{il}\left(\sum_{k=1}^{p}[B]_{lk}[C]_{kj}\right) = \sum_{l=1}^{n}[A]_{il}[BC]_{lj} = [A(BC)]_{ij}, \end{aligned}$$

za sve $i =, \ldots, m$, $j = 1, \ldots, q$. □

Propozicija 2.3.4. *Množenje matrica je*

(1) *kvaziasocijativno, to jest*

$$(\lambda A)B = \lambda(AB) = A(\lambda B),$$

za sve $\lambda \in \mathbb{F}$, te A i B za koje je gornji izraz definiran.

(2) *distributivno prema zbrajanju matrice, to jest*

$$(A+B)C = AC + BC, \quad A(B+C) = AB + AC$$

za sve A, B i C za koje je gornji izraz definiran.

Dokaz. **(1)** Neka je $A \in M_{mn}(\mathbb{F})$, te $B \in M_{np}(\mathbb{F})$. Tada su matrice $(\lambda A)B$, $\lambda(AB)$ i $A(\lambda B)$ tipa (m,p). Vrijedi

$$[(\lambda A)B]_{ij} = \sum_{k=1}^{n}[\lambda A]_{ik}[B]_{kj} = \sum_{k=1}^{n}(\lambda[A]_{ik})[B]_{kj} = \lambda\sum_{k=1}^{n}[A]_{ik}[B]_{kj} = \lambda[AB]_{ij},$$

za sve $i = 1, \ldots, m$, $j = 1, \ldots, p$. Na isti način provjerimo preostalu jednakost.

(2) Neka su $A, B \in M_{mn}(\mathbb{F})$, te $C \in M_{np}(\mathbb{F})$. Tada su $(A+B)C, AC+BC \in M_{mp}(\mathbb{F})$. Vrijedi

$$\begin{aligned} [(A+B)C]_{ij} &= \sum_{k=1}^{n}[A+B]_{ik}[C]_{kj} = \sum_{k=1}^{n}([A]_{ik}+[B]_{ik})[C]_{kj} \\ &= \sum_{k=1}^{n}[A]_{ik}[C]_{kj} + \sum_{k=1}^{n}[B]_{ik}[C]_{kj} = [AC]_{ij} + [BC]_{ij} = [AC+BC]_{ij}, \end{aligned}$$

za sve $i = 1, \dots, m$, $j = 1, \dots, p$.

□

Propozicija 2.3.5. *Neka je $A \in M_{mn}(\mathbb{F})$. Vrijedi $I_m A = A$ i $AI_n = A$, gdje su I_m i I_n jedinične matrice reda m, odnosno n.*

Dokaz. Očito je $I_m A$ tipa (m, n). Neka je $I_m = I = (\delta_{ij})$, te $A = (a_{ij})$. Tada

$$IA = \sum_{k=1}^{m} \delta_{ik} a_{kj} = \{\delta_{ik} = 1, \text{ za } i = k, \text{ inače } \delta_{ik} = 0\} = a_{ij}.$$

□

Množenje matrica na skupu matrica reda n, $M_n(\mathbb{F})$, predstavlja jednu binarnu operaciju. Na temelju svega što smo pokazali u propozicijama 2.3.3, 2.3.4 i 2.3.5 vidimo da $(M_n(\mathbb{F}), \cdot)$ ima jednu algebarsku strukturu koju smo već upoznali.

Korolar 2.3.6. *Skup $M_n(\mathbb{F})$ s obzirom na operaciju množenja matrica je nekomutativan monoid.*

Dokaz. Prema Propoziciji 2.3.3, množenja matrica je asocijativno u $M_n(\mathbb{F})$. Propozicija 2.3.5 povlači da je $AI = IA = A$, za sve $A \in M_n(\mathbb{F})$. □

Štoviše, $M_n(\mathbb{F})$ je primjer strukture koja se naziva **asocijativna algebra s jedinicom**. Naime, algebra je svaki vektorski prostor s definiranim tzv. bilinearnim množenjem (to jest množenjem koje zadovoljava svojstva distributivnosti i kvaziasocijativnosti). Budući je množenje još i asocijativno, dobiva pridjev *asocijativna*, te zbog postojanja neutralnog elementa množenja (I) ističemo i ono s *jedinicom*. Prisjetimo se da smo se već susreli s ovom strukturom. Na kolegiju *Analitička geometrija* pokazuje se da je prostor V^3 jedna (neasocijativna) algebra pri čemu ulogu množenja ima operacija vektorskog produkta.

Zadatak 14. *Neka je $A \in M_n(\mathbb{R})$, $n \geq 2$ te neka je $C(A) = \{X \in M_n(\mathbb{R}) \,:\, AX = XA\}$. Tada je $C(A) \leq M_n(\mathbb{R})$ i $\dim C(A) \geq 2$. Dokažite.*

Primjer 29. Sljedeći skupovi:

- skup svih dijagonalnih matrica reda n,
- skup svih skalarnih matrica reda n,
- skup svih gornjetrokutastih (donjetrokutastih) matrica reda n.

predstavljaju podalgebre od $M_n(\mathbb{F})$ (i to asocijativne s jedinicom). U Primjeru 24 pokazali smo da su to potprostori od $M_n(\mathbb{F})$. Sada jedino moramo ustanoviti da su zatvoreni na množenje. Neka su $C = \operatorname{diag}(c_1, \dots, c_n)$ i $D = \operatorname{diag}(d_1, \dots, d_n)$ dijagonalne matrice reda n. Za $i \neq j$ vrijedi

$$[CD]_{ij} = \sum_{k=1}^{n} [C]_{ik}[D]_{kj} = c_i[D]_{ij} + [C]_{ij}d_j = 0,$$

za $i = j$ je

$$[CD]_{ii} = \sum_{k=1}^{n} [C]_{ik}[D]_{ki} = c_i d_i,$$

pa je

$$CD = \operatorname{diag}(c_1 d_1, \dots, c_n d_n).$$

Ako su $S = sI$, $T = tI$ skalarne matrice, onda je i $ST = (st)I$ skalarna matrica.

Neka su G i H gornjetrokutaste matrice. Izračunajmo element njihovog umnoška na mjestu (i, j) za $1 \leq j < i \leq n$,

$$[GH]_{ij} = \sum_{k=1}^{n} [G]_{ik}[H]_{kj} = \underbrace{\sum_{k=1}^{i-1} [G]_{ik}[H]_{kj}}_{[G]_{ik}=0,\ k=1,\dots,i-1} + \underbrace{\sum_{k=i}^{n} [G]_{ik}[H]_{kj}}_{[H]_{kj}=0,\ k=i,\dots,n,\ jer\ k>j} = 0.$$

Stoga je GH gornjetrokutasta matrica.

♡

Primjer 30. U svakoj asocijativnoj algebri s jedinicom, nad poljem $\mathbb{F}$, ima smisla promatrati polinome s koeficijentima iz $\mathbb{F}$. To vrijedi i za algebru $M_n(\mathbb{F})$ pa tako dobivamo *matrične polinome*. Ako je polinom p s koeficijentima iz polja $\mathbb{F}$ zadan s

$$p(t) = \sum_{i=0}^{k} \alpha_i t^i,$$

definirana je vrijednost polinoma $p(A)$ za matricu $A \in M_n(\mathbb{F})$ kao

$$p(A) = \sum_{i=0}^{k} \alpha_i A^i.$$

Pritom se definira $A^0 = I$.

Očito je $p(A)$ također kvadratna matrica reda n. Matrični polinomi pokazuju se važnima u linearnoj algebri. Svojstva matričnih polinoma ne podudaraju se u svemu s polinomima u kojima varijabla poprima vrijednost u nekom polju. Primjerice, u pogledu nultočaka, $p(t) = t^2 - 1$ ima u polju $\mathbb{R}$ točno dvije nultočke, 1 i -1, dok u skupu $M_2(\mathbb{R})$ postoji više matrica koje "poništavaju" taj polinom. Iako vrijedi faktorizacija $A^2 - I = (A + I)(A - I)$, odakle je očito $p(-I) = p(I) = 0$ (nulmatrica), npr. za

$$B = \begin{bmatrix} 1 & 0 \\ 1 & -1 \end{bmatrix}$$

također vrijedi $p(B) = 0$. Štoviše, u $M_2(\mathbb{R})$ postoji beskonačno mnogo matrica čiji kvadrat je jedinična matrica I.

S druge strane, polinom $q(t) = t^2 + 1$ nema nultočaka u polju $\mathbb{R}$, ali u skupu $M_2(\mathbb{R})$ postoje matrice čiji kvadrat je matrica $-I$, primjerice

$$C = \begin{bmatrix} 1 & -2 \\ 1 & -1 \end{bmatrix}$$

pa je $q(C) = 0$. I za ovaj polinom postoji beskonačno mnogo realnih matrica za koje matrični polinom poprima vrijednost 0.

Ovako bitne razlike pojavljuju se stoga što je jedna matrična polinomijalna jednadžba ekvivalentna sustavu algebarskih jednadžbi u polju. Određivanje skupa rješenja takvog sustava općenito je znatno složeniji problem. ♡

Propozicija 2.3.7. *Vrijedi*

$$(AB)^t = B^t A^t,$$

čim je umnožak definiran.

Dokaz. Ako je A tipa (m, n) i B tipa (n, p), onda su matrice $(AB)^t$ i $B^t A^t$ tipa (p, m). Za (i, j) takve da je $1 \leq i \leq p$ i $1 \leq j \leq m$ vrijedi

$$[(AB)^t]_{ij} = [AB]_{ji} = \sum_{k=1}^{n} [A]_{jk} [B]_{ki} = \sum_{k=1}^{n} [A^t]_{kj} [B^t]_{ik} = \sum_{k=1}^{n} [B^t]_{ik} [A^t]_{kj} = [B^t A^t]_{ij}.$$

□

Jasno je da prethodni rezultat možemo poopćiti na konačno mnogo matrica, $(A_1 \cdots A_k)^t = A_k^t \cdots A_1^t$.

Ustanovili smo da $(M_n(\mathbb{F}), \cdot)$ monoid. Možemo pitati je li možda ova struktura i grupa. Odgovor je niječan, što možemo zorno vidjeti u sljedećem primjeru.

Primjer 31. Zadana je matrica

$$A = \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}.$$

Pitamo se postoji li matrica X reda 2 za koju $AX = XA = I$. Neka je

$$X = \begin{pmatrix} x_1 & x_2 \\ x_3 & x_4 \end{pmatrix}.$$

Iz $AX = I$ dobivamo sustav

$$\begin{array}{ccccc} x_1 & + & 2x_3 & = & 1 \\ x_1 & + & 2x_3 & = & 0 \end{array},$$

te isti sustav za x_2 i x_4. Očito ti sustavi nemaju rješenja, pa matrica X ne postoji. ♡

Definicija 2.3.8. *Kvadratna matrica $A \in M_n(\mathbb{F})$ je* ***invertibilna*** *ili* ***regularna*** *ako postoji matrica $B \in M_n(\mathbb{F})$ takva da je*

$$AB = BA = I.$$

Matricu B zovemo ***inverznom matricom*** *od A i pišemo, $B = A^{-1}$. U protivnom je A* ***singularna*** *matrica.*

Prisjetimo se nekih tvrdnji koje vrijede u svakom monoidu koje smo pokazali u odsječku 1.1.2 (Propozicija 1.1.8). Budući je $(M_n(\mathbb{F}), \cdot)$ multiplikativni monoid, vrijedi sljedeće:

- Ako inverz postoji, onda je on jedinstven. Stoga je opravdano inverz matrice A označiti s A^{-1}. Nadalje, i A^{-1} je regularna i vrijedi $(A^{-1})^{-1} = A$.
- Ako su A i B regularne matrice, onda je to AB, te vrijedi $(AB)^{-1} = B^{-1}A^{-1}$. Tvrdnju možemo poopćiti i na konačno mnogo regularnih matrica A_1, ..., A_k. Tada je $(A_1 \cdots A_k)^{-1} = A_k^{-1} \cdots A_1^{-1}$.

Kod množenja matrica moguće je da umnožak dviju matrica A i B, koje su obje različite od 0, bude nulmatrica, $AB = 0$. To je jedna od bitnih razlika u odnosu na množenje brojeva poput cijelih, racionalnih ili realnih.

Primjer 32. Za

$$A = [1\ 2\ 3],\ B = [4\ 1\ -2]$$

je $AB^t = [0]$. Slično se može dogoditi i za kvadratne matrice jednakog tipa, npr.

$$G = \begin{bmatrix} 3 & 0 \\ 5 & 0 \end{bmatrix},\ H = \begin{bmatrix} 0 & 0 \\ 0 & 2 \end{bmatrix}$$

daju umnožak

$$GH = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}.$$

♡

Kod prstena smo spomenuli mogućnost postojanja tzv. djelitelja nule (v. str. 20), a skup kvadratnih matrica $M_n(\mathbb{R})$ s operacijama zbrajanja i množenja matrica primjer je nekomutativnog prstena s jedinicom u kojem postoje djelitelji nule (čim je $n \geq 2$).

Dakle, za kvadratne matrice A, B i C jednakog reda, pri čemu je $A \neq 0$, ne možemo izvoditi "skraćivanje" na kakvo smo naviknuti kod brojeva, tj. u polju. Iz $AB = AC$ ne slijedi nužno $B = C$, jer $A(B - C) = 0$ općenito ne povlači da je $B - C = 0$. Na ovu činjenicu valja pripaziti jer često dovodi do pogrešaka u rješavanju zadataka.

No, ako je matrica ne samo različita od 0 nego i invertibilna, skraćivanje se jednostavno izvodi množenjem matricom A^{-1}. U polju je invertibilnost ekvivalentna s različitosti od 0, dok u prstenu, posebno u prstenu kvadratnih matrica, to ne vrijedi općenito.

2.4 Elementarne transformacije i elementarne matrice

Neka je $A = [a_{ij}] \in M_{mn}(\mathbb{F})$. Označimo sa $S_1, \dots, S_n$ redom stupce matrice A, to jest

$$S_1 = \begin{pmatrix} a_{11} \\ a_{21} \\ \vdots \\ a_{m1} \end{pmatrix}, \dots, S_n = \begin{pmatrix} a_{1n} \\ a_{2n} \\ \vdots \\ a_{mn} \end{pmatrix} \in M_{m,1}(\mathbb{F}).$$

Kažemo da je

$$(S_1, \dots, S_n)$$

stupčana reprezentacija matrice A. Doista, ova uređena n-torka jednostupčanih matrica potpuno određuje matricu A, jer važan je redoslijed stupaca, a neki stupci mogu se u matrici i ponavljati pa nije dovoljno precizno govoriti samo o "skupu stupaca".

Međutim, redoslijed stupaca matrice i moguće jednakosti nekih stupaca ne utječu na linearnu ljusku

$$[S_1, \dots, S_n]$$

kao potprostor vektorskog prostora $M_{m,1}(\mathbb{F})$, razapet stupcima matrice. Pritom, dimenzija potprostora $[S_1, \dots, S_n]$ nije veća od $m = \dim M_{m,1}(\mathbb{F})$. S druge strane, dimenzija te linearne ljuske nije veća od n, jer skup od n vektora sadrži bazu svoje linearne ljuske. Stoga je

$$\dim[S_1, \dots, S_n] \leq \min(m, n).$$

Na isti način, možemo promatrati retčanu reprezentaciju matrice A:

$$(R_1, \dots, R_m),$$

gdje je

$$R_1 = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \end{pmatrix}, \dots, R_m = \begin{pmatrix} a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix} \in M_{1,n}(\mathbb{F}).$$

Analogno, vrijedi

$$\dim[R_1, \dots, R_m] \leq \min(m, n).$$

Lako je ustanoviti da neke operacije (transformacije) nad skupom vektora koji razapinje ljusku ne će promijeniti dimenziju ljuske. Neka je $S = \{x_1, x_2, \dots, x_n\}$ podskup nekog vektorskog prostora V nad poljem $\mathbb{F}$. Nad skupom S izvodimo sljedeće operacije:

1. Međusobna zamjena neka dva vektora. Na primjer, imamo $S' = \{x_2, x_1, \dots, x_n\}$. Jasno je $[S] = [S']$.

2. Množenje nekog vektora skalarom $\lambda \neq 0$. Na primjer, $S' = \{\lambda x_1, x_2, \dots, x_n\}$. I ovdje vrijedi $[S] = [S']$.

3. Pribrajanje nekog vektora nekom drugom vektoru. Na primjer, $S' = \{x_1, x_2 + x_1, x_3, \dots, x_n\}$. Ponovo, lako je za ustanoviti da je $[S] = [S']$.

Opisane operacije izvodit ćemo nad stupcima ili redcima matrice.

Definicija 2.4.1. ***Elementarne transformacije nad matricom*** *$A \in M_{mn}(\mathbb{F})$ su:*

(I) *zamjena dva stupca (retka),*

(II) *množenje nekog stupca (retka) skalarom $\lambda \neq 0$,*

(III) *pribrajanje nekom stupcu (retku) nekog drugog stupca (retka) pomnoženog skalarom λ.*

Uočimo da se primjenom elementarnih transformacija nad stupcima matrice A ne mijenja potprostor $[S_1, \dots, S_n] \leq M_{m,1}(\mathbb{F})$ pa se tako ne mijenja ni njegova dimenzija. Analogno, primjenom elementarnih transformacija nad redcima matrice A ne mijenja se potprostor $[R_1, \dots, R_m] \leq M_{1,n}(\mathbb{F})$ pa se tako ne mijenja ni njegova dimenzija.

U sljedećim primjerima uočit ćemo da se sve elementarne transformacije nad matricom mogu realizirati množenjem te matrice slijeva ili zdesna posebnim matricama.

Primjer 33. Neka je

$$A = \begin{pmatrix} 1 & 2 & -1 & 0 \\ 2 & 0 & 3 & 1 \\ -1 & 2 & 1 & 2 \end{pmatrix}.$$

Uočimo,

$$\underbrace{\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}}_{=F} \cdot A = \underbrace{\begin{pmatrix} 1 & 2 & -1 & 0 \\ \mathbf{-1} & \mathbf{2} & \mathbf{1} & \mathbf{2} \\ \mathbf{2} & \mathbf{0} & \mathbf{3} & \mathbf{1} \end{pmatrix}}_{zamjena\ 2.\ i\ 3.\ retka}.$$

Dakle, matrica FA je dobivena iz matrice A zamjenom 2. i 3. retka. Na isti način,

$$A \cdot \underbrace{\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}}_{=G} = \underbrace{\begin{pmatrix} 1 & \mathbf{-1} & \mathbf{2} & 0 \\ 2 & \mathbf{3} & \mathbf{0} & 1 \\ -1 & \mathbf{1} & \mathbf{2} & 2 \end{pmatrix}}_{zamjena\ 2.\ i\ 3.\ stupca},$$

odnosno množenje AG realizira zamjenu 2. i 3. stupca matrice. Uočimo, da smo za realizaciju elementarne transformacije nad redcima množili matricu A slijeva, a za transformaciju nad stupcima zdesna. Nadalje, matrice F i G dobili smo upravo transformacijom prve vrste (konkretno, zamjenom 2. i 3. stupca ili retka) jedinične matrice I reda 3, odnosno 4. Lako se vidi da je

$$F \cdot F = I_3, \ G \cdot G = I_4.$$

Matrice F i G su invertibilne. I više, kažemo da su *involutorne* jer im je inverz jednak njima samima.

♡

Primjer 34. Neka je A kao u Primjeru 33, te neka su

$$F = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \ G = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 3 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

Uočimo,

$$F \cdot A = \underbrace{\begin{pmatrix} 1 & 2 & -1 & 0 \\ \mathbf{6} & \mathbf{0} & \mathbf{9} & \mathbf{3} \\ -1 & 2 & 1 & 2 \end{pmatrix}}_{2.\ redak\ pomno\check{z}en\ s\ 3},$$

te

$$A \cdot G = \underbrace{\begin{pmatrix} 1 & \mathbf{6} & -1 & 0 \\ 2 & \mathbf{0} & 3 & 1 \\ -1 & \mathbf{6} & 1 & 2 \end{pmatrix}}_{2.\ stupac\ pomno\check{z}en\ s\ 3}.$$

Kao i prethodnom primjeru, množenje 2. retka ili stupca skalarom različitim od 0 realizirali smo množenjem matrice A slijeva, odnosno zdesna s matricom kojoj je 2. redak (ili stupac) jedinične matrice pomnožen odgovarajućim skalarom ($\lambda = 3$). Lako se vidi da su matrice F i G invertibilne. Zaista,

$$F \cdot F' = I_3, \ G \cdot G' = I_4,$$

gdje je

$$F' = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \frac{1}{3} & 0 \\ 0 & 0 & 1 \end{pmatrix}, \ G' = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & \frac{1}{3} & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

♡

Primjer 35. Neka je A kao u Primjeru 33, te neka su

$$F = \begin{pmatrix} 1 & 3 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \ G = \begin{pmatrix} 1 & 3 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

Uočimo,

$$FA = \underbrace{\begin{pmatrix} 7 & 2 & 8 & 3 \\ \mathbf{2} & \mathbf{0} & \mathbf{3} & \mathbf{1} \\ -1 & 2 & 1 & 2 \end{pmatrix}}_{1.\ retku\ pribrojen\ je\ 2.\ redak\ pomno\check{z}en\ s\ 3},$$

$$AG = \underbrace{\begin{pmatrix} 1 & \mathbf{5} & -1 & 0 \\ 2 & \mathbf{6} & 3 & 1 \\ -1 & \mathbf{-1} & 1 & 2 \end{pmatrix}}_{2.\ stupcu\ pribrojen\ je\ 1.\ stupac\ pomno\check{z}en\ s\ 3},$$

Matrice F i G su invertibilne. Inverzi su dani s

$$F^{-1} = \begin{pmatrix} 1 & -3 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \; G = \begin{pmatrix} 1 & -3 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

♡

U primjerima 33, 34 i 35 opisali smo matrice F i G koje množenjem slijeva ili zdesna realiziraju elementarne transformacije 1., 2. i 3. vrste nad redcima ili stupcima. Takve se matrice nazivaju *elementarne matrice.* Nadalje, u primjerima smo vidjeli da su te matrice invertibilne a njihovi inverzi su također elementarne matrice. Te se tvrdnje pokazuju i općenito.

Definicija 2.4.2. ***Elementarna matrica*** *reda n je matrica koja je dobivena jednom elementarnom transformacijom nad stupcima ili redcima jedinične matrice reda n.*

Propozicija 2.4.3. *Svaka elementarna matrica je regularna. Inverz elementarne matrice je elementarna matrica.*

Dokaz. Ako je elementarna matrica dobivena zamjenom dva stupca ili retka jedinične matrice, onda je ona involutorna, to jest inverz sama sebi.

Ako je elementarna matrica dobivena množenjem i-tog retka (stupca) jedinične matrice skalarom $\lambda \neq 0$, onda je njoj inverzna matrica dobivena množenjem i-tog retka (stupca) jedinične matrice skalarom $\frac{1}{\lambda}$.

Ako je elementarna matrica dobivena pribrajanjem i-tog retka (stupca) pomnoženog s λ, j-tom retku (stupcu) jedinične matrice, onda je njoj inverzna matrica dobivena pribrajanjem i-tog retka (stupca) pomnoženog s $-\lambda$, j-tom retku (stupcu) jedinične matrice.

□

Propozicija 2.4.4. *Neka je $A \in M_{mn}(\mathbb{F})$. Elementarne transformacije nad* redcima *matrice A mogu se realizirati* množenjem slijeva *s odgovarajućim elementarnim matricama reda m. Elementarne transformacije nad* stupcima *matrice A mogu se realizirati* množenjem zdesna *s odgovarajućim elementarnim matricama reda n.*

Definicija 2.4.5. *Neka su $A, B \in M_{mn}(\mathbb{F})$. Matrica A je* ***ekvivalentna*** *matrici B ako se B može dobiti iz A primjenom konačno mnogo elementarnih transformacija. Pišemo $A \sim B$.*

Prema Propoziciji 2.4.4, ako je $A \sim B$, onda postoje elementarne matrice $F_1, \ldots, F_k$ reda m i elementarne matrice $G_1, \ldots, G_l$ reda n takve da je

$$B = (F_k \cdots F_1)A(G_1 \cdots G_l).$$

Kako su elementarne matrice regularne, to su i njihovi umnošci $S = F_k \cdots F_1$ i $T = G_1 \cdots G_l$ također regularne matrice i vrijedi

$$B = SAT.$$

Ovim smo pokazali sljedeću tvrdnju.

Propozicija 2.4.6. *Neka su A i B ekvivalentne matrice tipa (m,n). Tada postoje regularna matrica S reda m i regularna matrica T reda n za koje vrijedi $B = SAT$.*

Propozicija 2.4.7. *Relacija $'\sim'$ je relacija ekvivalencije na skupu $M_{mn}(\mathbb{F})$.*

Dokaz. Relacija $'\sim'$ je očito refleksivna ($A \sim A$).

Pretpostavimo da je $A \sim B$. Tada postoje elementarne matrice $F_1, \ldots, F_k$ reda m i elementarne matrice $G_1, \ldots, G_l$ reda n takve da je $B = (F_k \cdots F_1)A(G_1 \cdots G_l)$. Množenjem s inverzima $F_1^{-1}, \ldots, F_k^{-1}$ slijeva, te s $G_l^{-1}, \ldots, G_1^{-1}$ zdesna dobivamo da je

$$F_1^{-1} \cdots F_k^{-1} B G_l^{-1} \cdots G_1^{-1} = A,$$

odnosno $B \sim A$ budući da su inverzi elementarnih matrica - elementarne matrice.

Pretpostavimo da je $A \sim B$ i $B \sim C$. Tada postoje odgovarajuće elementarne matrice F_i, G_i, H_i, K_i za koje je $B = (F_k \cdots F_1)A(G_1 \cdots G_l)$ i $C = (H_p \cdots H_1)B(K_1 \cdots K_q)$. Kako je

$$C = (H_p \cdots H_1 F_k \cdots F_1)A(G_1 \cdots G_l K_1 \cdots K_q),$$

slijedi $A \sim C$.

□

2.5 Rang matrice

Definicija 2.5.1. *Neka je $A = [a_{ij}] \in M_{mn}(\mathbb{F})$, te $(S_1, \ldots, S_n)$, $S_j \in M_{m1}(\mathbb{F})$, stupčana reprezentacija matrice A.* ***Rang matrice*** *A je dimenzija linearne ljuske razapete skupom stupaca od A. Pišemo*

$$r(A) = \dim[S_1, \ldots, S_n].$$

Uočimo da je nulmatrica jedina matrica (bilo kojeg tipa) ranga 0, tj. $r(A) = 0$ ako i samo ako je $A = 0$.

U uvodnom razmatranju linearne ljuske skupa stupaca matrice A tipa (m,n) u odjeljku 2.4 ustanovili smo da dimenzija te linearne ljuske nije veća ni od m ni od n. Analogna tvrdnja vrijedi i za linearnu ljusku skupa redaka matice A. Te činjenice sad možemo iskazati pomoću pojma ranga matrice.

Propozicija 2.5.2. *Neka je $A \in M_{mn}(\mathbb{F})$. Tada vrijedi:*

(a) $r(A) \le \min(m,n)$,

(b) $r(A^t) \le \min(m,n)$.

Napomenimo da se rang matrice često definira kao *maksimalan broj linearno nezavisnih stupaca matrice A.* Ta je definicija ekvivalentna s našom jer znamo da se svaki sustav izvodnica (to jest skup $\{S_1, \ldots, S_n\}$) može reducirati do baze prema Teoremu 1.4.3.

U onom što slijedi opisat ćemo kako operativno odrediti rang neke matrice. Ustanovili smo da se dimenzija linearne ljuske ne mijenja ako nad vektorima izvodimo elementarne operacije (transformacije). Dakle, vrijedi sljedeći teorem.

Teorem 2.5.3. *Neka je matrica A' dobivena iz A primjenom elementarnih transformacija nad stupcima. Tada je*

$$r(A) = r(A').$$

Uskoro ćemo pokazati da se rang matrice neće promijeniti ako primjenjujemo elementarne transformacije i nad redcima. Sljedeću tvrdnju katkad se sažeto, iako ne sasvim korektno, iskazuje tako da je *rang matrice po stupcima jednak rangu po redcima.* Pritom "rang po redcima" valja shvatiti kao dimenziju linearne ljuske razapete redcima matrice. Ovakva "ravnopravnost" stupaca i redaka matrice može se učiniti prirodnom, ali zapravo nije nimalo očigledna i dokaz je tehnički dosta zahtjevan.

Teorem 2.5.4. *Neka je dana matrica $A \in M_{mn}(\mathbb{F})$. Maksimalan broj linearno nezavisnih stupaca matrice A jednak je maksimalnom broju linearno nezavisnih redaka matrice A.*

Dokaz. Neka je $r(A) = r$. Ako je $(S_1, \ldots, S_n)$ stupčana reprezentacija matrice A, onda je

$$\dim[S_1, \ldots, S_n] = r.$$

Bez smanjenja općenitosti neka je $\{S_1, \ldots, S_r\}$ linearno nezavisan skup (u suprotnom možemo zamijeniti poredak stupaca jer te elementarne transformacije ne mijenjaju rang matrice, prema Teoremu 2.5.3). Dakle, $S_j \in [S_1, \ldots, S_r]$ za sve $j = r+1, \ldots, n$, odnosno

$$S_j = \gamma_{1j} S_1 + \cdots + \gamma_{rj} S_r,\ j = r+1, \ldots, n,$$

za neke $\gamma_{ij} \in \mathbb{F}$.

Neka je $\overline{A}$ matrica tipa (m, r) čija je stupčana reprezentacija $(S_1, \ldots, S_r)$ (to jest matrica koju smo dobili tako što smo iz matrice A izbacili zadnjih $n - r$ stupaca). Pretpostavimo da matrica $\overline{A}$ ima p linearno nezavisnih redaka. Tada je

$$p \leq \min\{m, r\}.$$

Zaista, $p \leq m$ jer m broj redaka u $\overline{A}$, te $p \leq r$ jer je svaki redak vektor iz $M_{1,r}(\mathbb{F})$ (ili $\mathbb{F}^r$). Označimo s $\overline{R_1}, \ldots, \overline{R_m}$ retke u matrici $\overline{A}$, te bez smanjenja općenitosti pretpostavimo da je skup $\{\overline{R_1}, \ldots, \overline{R_p}\}$ linearno nezavisan. Stoga postoje $\lambda_{ki} \in \mathbb{F}$, $k = 1, \ldots, p$, $i = p+1, \ldots, m$ takvi da je

$$\overline{R_i} = \lambda_{1i} \overline{R_1} + \cdots + \lambda_{pi} \overline{R_p},\ i = p+1, \ldots, n.$$

Može se pokazati da prethodne relacije vrijede i za retke matrice A, odnosno

$$R_i = \lambda_{1i} R_1 + \cdots + \lambda_{pi} R_p,\ i = p+1, \ldots, n.$$

(Napominjemo da smo precizan dokaz prethodne jednakosti izostavili). Sada je očito maksimalan broj linearno nezavisnih redaka u A manji ili jednak od p, odnosno vrijedi

$$t \leq p \leq r,$$

gdje smo s t označili broj linearno nezavisnih redaka u A.

Ako tvrdnju da je maksimalan broj linearno nezavisnih redaka u nekoj matrici manji ili jednak od maksimalnog broja linearno nezavisnih stupaca primijenimo na matricu A^t, dobit ćemo upravo nejednakost $r \leq t$. Dakle, $t = r$. □

Korolar 2.5.5. *Vrijedi* $r(A) = r(A^t)$.

Korolar 2.5.6. *Ako je matrica* A *ekvivalentna matrici* B*, onda je* $r(A) = r(B)$.

Dokaz. Matrica B je dobivena pomoću konačno mnogo elementarnih transformacija nad stupcima i redcima matrice A, pa tvrdnja slijedi prema teoremima 2.5.3 i 2.5.4. □

Naš cilj je primjenom elementarnih transformacija nad stupcima i redcima matrice tako pojednostavniti početnu matricu da se rang može lako iščitati.

Primjer 36. Zadana je matrica

$$A = \begin{pmatrix} 1 & 0 & 2 & -1 \\ 3 & 1 & -3 & 1 \\ -1 & -1 & 7 & -3 \end{pmatrix}.$$

Izvodimo sljedeće elementarne transformacije nad stupcima i redcima:

$$A \sim \left\{ \begin{array}{c} \textit{2. retku dodamo 1. redak pomnožen s } -3 \\ \textit{3. retku dodamo 1. redak} \end{array} \right\} \sim \begin{pmatrix} 1 & 0 & 2 & -1 \\ 0 & 1 & -9 & 4 \\ 0 & -1 & 9 & -4 \end{pmatrix}$$

$$\sim \left\{ \begin{array}{c} \textit{3. stupcu dodamo 1. stupac pomnožen s } -2 \\ \textit{4. stupcu dodamo 1. stupac} \end{array} \right\} \sim \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & -9 & 4 \\ 0 & -1 & 9 & -4 \end{pmatrix}$$

$$\sim \left\{ \textit{3.retku dodamo 2. redak} \right\} \sim \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & -9 & 4 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

$$\sim \left\{ \begin{array}{c} \textit{3. stupcu dodamo 2. stupac pomnožen s } 9 \\ \textit{4. stupcu dodamo 2. stupac pomnožen s} -4 \end{array} \right\} \sim \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} = D_2$$

Jasno je da je $r(D_2) = 2$, jer prva dva stupca očito čine linearno nezavisan skup, pa je i $r(A) = 2$.

♡

Definicija 2.5.7. *Neka je* $0 < r \leq \min(m, n)$*. Matrica* $D_r \in M_{mn}(\mathbb{F})$ *takva da je* $[D_r]_{ii} = 1$*, za sve* $i = 1, \ldots, r$*, a svi ostali elementi su jednaki nuli, naziva se* ***kanonska matrica ranga*** r *i tipa* (m, n)*.*

Matrica

- $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$ je tipa $(2, 3)$ i ranga 1,
- $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$ je tipa $(2, 3)$ i ranga 2,
- $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ je reda 3 i ranga 3 - maksimalnog ranga, te je očito jednaka jediničnoj matrici.

Kanonska matrica D_r određenog tipa (m, n) i ranga r služi nam kao najjednostavniji standardni oblik matrice iz kojeg možemo izravno očitati rang matrice. U Primjeru 36 prikazan je postupak kakav se zapravo može izvesti općenito, za bilo koju matricu, u svrhu određivanja njezinog ranga. U praksi nećemo uvijek morati elementarne transformacije izvoditi sve dok ne dobijemo baš kanonsku matricu, nego će se rang vidjeti i prije toga, kad se uoči maksimalni linearno nezavisni skup stupaca ili redaka. No, važno je imati takav standardni oblik kojim se možemo poslužiti u praktičnim postupcima i u dokazima propozicija.

Propozicija 2.5.8. *Neka je $A \in M_{mn}(\mathbb{F})$ ranga r. Tada se matrica A može primjenom konačno mnogo elementarnih transformacija nad stupcima ili redcima svesti na kanonsku matricu tipa (m, n) i ranga r.*

Ovu važnu propoziciju nećemo dokazati formalno i općenito, jer je ispisivanje dokaza pomoću općih koeficijenata matrice razmjerno komplicirano, a svi se bitni koraci mogu opisati i shvatiti na primjerima. Najprije, ako u matrici postoje stupci ili redci čiji su svi elementi jednaki 0, takve premjestimo na zadnja mjesta (stupce desno, retke dolje). Dalje, uz pomoć elementarnih transformacija ako je potrebno, na poziciji $(1, 1)$ dobivamo koeficijent jednak 1. Zatim elementarnim transformacijama 2. i 3. tipa možemo na svim ostalim pozicijama u 1. retku i 1. stupcu dobiti koeficijente 0. Time postižemo da 1. redak i 1. stupac postanu jednaki onima u kanonskoj matrici. Postupak nastavljamo analogno od pozicije $(2, 2)$ u matrici, pri čemu više ne mijenjamo ni prvi stupac ni prvi redak. Ako je $r(A) = r$, ovim postupkom doći ćemo do kanonske matrice D_r.

Iz Korolara 2.5.6 i Propozicije 2.5.8 izravno slijedi:

Propozicija 2.5.9. *Neka je $A \in M_{mn}(\mathbb{F})$. Vrijedi $r(A) = r$ ako i samo ako $A \sim D_r$.*

Teorem 2.5.10. *Matrice jednakog tipa su ekvivalentne ako i samo ako su jednakog ranga.*

Dokaz. Jedan smjer je pokazan u Korolaru 2.5.6. Obrnuto, pretpostavimo da su $A, B \in M_{mn}(\mathbb{F})$ jednakog ranga r. Po Propoziciji 2.5.8 obje su ekvivalentne kanonskoj matrici D_r, a kako je ekvivalencija matrica simetrična i tranzitivna relacija, slijedi da su A i B ekvivalentne. Konkretno, matricu A možemo elementarnim transformacijama pretvoriti u D_r, a D_r možemo zatim pretvoriti u matricu B, postupkom obrnutim pretvaranju B u D_r. □

Primijetimo još da iz Propozicije 2.5.9 slijedi da za svaku matricu A ranga r postoje regularne matrice S i T takve da vrijedi $A = SD_rT$. Pritom su A i D_r jednakog tipa (m, n), S je kvadratna reda m, a T kvadratna reda n. Ovo slijedi iz Propozicije 2.4.6, a prikaz oblika $A = SD_rT$ često je koristan.

Propozicija 2.5.11. *Neka su $A \in M_{mn}(\mathbb{F})$ i $B \in M_{np}(\mathbb{F})$ dvije (ulančane) matrice te označimo njihov umnožak sa $C = AB$. Nadalje, neka je $(S_1, \ldots, S_n)$ stupčana reprezentacija matrice A, a $(C_1, \ldots, C_p)$ stupčana reprezentacija matrice C. Tada se svaki stupac $C_k \in M_{m1}(\mathbb{F})$ može napisati kao linearna kombinacija stupaca $S_1, \ldots S_n \in M_{m1}(\mathbb{F})$.*

Dokaz. Po definiciji množenja matrica, uz oznake $A = [a_{ij}]$, $B = [b_{jk}]$, $C = [c_{ik}]$ imamo

$$C_k = \begin{pmatrix} c_{1k} \\ c_{2k} \\ \vdots \\ c_{mk} \end{pmatrix} = \begin{pmatrix} \sum_{i=1}^n a_{1i}b_{ik} \\ \sum_{i=1}^n a_{2i}b_{ik} \\ \vdots \\ \sum_{i=1}^n a_{mi}b_{ik} \end{pmatrix} = \begin{pmatrix} a_{11}\boxed{b_{1k}} \\ a_{21}\boxed{b_{1k}} \\ \vdots \\ a_{m1}\boxed{b_{1k}} \end{pmatrix} + \cdots + \begin{pmatrix} a_{1n}\boxed{b_{nk}} \\ a_{2n}\boxed{b_{nk}} \\ \vdots \\ a_{mn}\boxed{b_{nk}} \end{pmatrix}$$

odnosno

$$C_k = b_{1k}\underbrace{\begin{pmatrix} a_{11} \\ a_{21} \\ \vdots \\ a_{m1} \end{pmatrix}}_{S_1} + \cdots + b_{nk}\underbrace{\begin{pmatrix} a_{1n} \\ a_{2n} \\ \vdots \\ a_{mn} \end{pmatrix}}_{S_n} = \sum_{j=1}^n b_{jk}S_j.$$

□

Propozicija 2.5.12. *Neka su A i B ulančane matrice. Tada rang njihovog umnoška nije veći od ranga pojedinih matrica, to jest $r(AB) \leq r(A), r(B)$.*

Dokaz. Primijenimo prethodnu propoziciju na matrice A i AB, uz iste oznake kao u dokazu te propozicije. Tada je linearna ljuska $[C_1, \ldots, C_p]$ potprostor vektorskog prostora $M_{m1}(\mathbb{F})$, sadržan u potprostoru $[S_1, \ldots, S_n]$, jer se svaki od stupaca C_k, $k = 1, \ldots, p$, može izraziti kao linearna kombinacija stupaca $S_1, \ldots, S_n$ matrice A. Stoga je $\dim[C_1, \ldots, C_p] \leq \dim[S_1, \ldots, S_n]$, dakle $r(AB) \leq r(A)$,

Primjenom dokazanog na matricu B^tA^t dobivamo $r(B^tA^t) \leq r(B^t)$, odakle je $r((AB)^t) = r(B^tA^t) \leq r(B^t)$. Zatim iskoristimo Korolar 2.5.5 po kojem se rang matrice ne mijenja transponiranjem pa dobivamo $r(AB) \leq r(B)$. □

Uočimo da se tvrdnja ove propozicije može indukcijom proširiti na umnožak bilo kojeg broja ulančanih matrica.

2.6 Inverzna matrica. Grupa regularnih matrica.

Skup svih regularnih, to jest invertibilnih matrica u multiplikativnom monoidu $M_n(\mathbb{F})$ čini nekomutativnu grupu. Tu grupu označavat ćemo s $GL(n, \mathbb{F})$ i nazivati *opća linearna grupa.*

Teorem 2.6.1. *Matrica reda n je regularna ako i samo ako je ranga n.*

Dokaz. Pretpostavimo da je matrica $A \in M_n(\mathbb{F})$ regularna i ranga $1 \leq r$. Tada je prema Teoremu 2.5.9 $A \sim D_r$, gdje je D_r kanonska matrica ranga r i reda n. Propozicija 2.4.6 povlači da je $D_r = SAT$ za neke regularne matrice S i T reda n. Stoga je i D_r nužno regularna jer je umnožak regularnih matrica. No, D_r je regularna ako i samo ako je $r = n$, pa je A ranga n.

Obratno, ako je A ranga n, tada je $A \sim D_n = I$, odnosno zbog simetričnosti $I \sim A$. Prema Propoziciji 2.4.6 postoje regularne matrice S i T reda n takve da je $A = SIT = ST$, pa slijedi da je A regularna. □

Korolar 2.6.2. *Svaka regularna matrica može se napisati kao umnožak elementarnih matrica.*

Dokaz. Neka je $A \in M_n(\mathbb{F})$ regularna, tada je prema Teoremu 2.6.1 ranga n, a prema Teoremu 2.5.9 je $A \sim I$. Stoga postoje elementarne matrice $F_1, \dots, F_k$ i $G_1, \dots, G_l$ reda n takve da je $A = (F_k \cdots F_1)I(G_1 \cdots G_l) = F_k \cdots F_1 G_1 \cdots G_l$. Dakle, A je umnožak elementarnih matrica. $\square$

Korolar 2.6.3. *Neka su $A, B \in M_{mn}(\mathbb{F})$. Matrice A i B su ekvivalentne ako i samo postoji regularna matrica S reda m i regularna matrica T reda n za koje vrijedi $B = SAT$.*

Dokaz. Jedan smjer smo pokazali u Propoziciji 2.4.6, a drugi slijedi iz prethodnog korolara 2.6.2. $\square$

Regularne matrice posebne su i po tome što se mogu transformirati do jedinične matrice primjenom elementarnih transformacija *samo po redcima* ili *samo po stupcima.* Zaista, neka je $A = (a_{ij})$ regularna, odnosno $r(A) = n$. Bez smanjenja općenitosti možemo pretpostaviti da je $a_{11} \neq 0$. (U suprotnom u prvom stupcu mora postojati element $a_{j1} \neq 0$ jer je matrica A punog ranga, te napravimo zamjenu prvog i j-tog retka.) Stoga vrijedi

$$A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \dots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{pmatrix} \sim \begin{pmatrix} 1 & a'_{12} & \dots & a'_{1n} \\ 0 & a'_{22} & \dots & a'_{2n} \\ \vdots & \vdots & \dots & \vdots \\ 0 & a'_{n2} & \dots & a'_{nn} \end{pmatrix} = A',$$

gdje smo matricu A' dobili nakon sljedećih transformacija: pribrajanjem 1. retka pomnoženog s $-a_{j1}/a_{11}$ j-tom retku, za sve $j = 2, \dots, n$, te množenjem 1. retka s $1/a_{11}$. Sada uočimo da među elementima 2. stupca $\{a'_{22}, \dots, a'_{n2}\}$ mora postojati barem jedan element različit od nule. Zaista, ako bi svi bili jednaki nuli, onda bi 2. stupac matrice A' bio nužno kolinearan s 1. stupcem što bi značilo da je $r(A') < n$, a to je u proturječju sa činjenicom da su A i A' ekvivalentne matrice. Stoga, ponovo bez smanjenja općenitosti možemo pretpostaviti da je $a_{22} \neq 0$, te na sličan način transformirajući matricu A' dobivamo

$$A \sim A' \sim \begin{pmatrix} 1 & 0 & a''_{13} & \dots & a''_{1n} \\ 0 & 1 & a''_{23} & \dots & a''_{2n} \\ 0 & 0 & a''_{33} & \dots & a''_{2n} \\ \vdots & \vdots & \vdots & \dots & \vdots \\ 0 & 0 & a''_{n3} & \dots & a''_{nn} \end{pmatrix} = A''.$$

Analognim zaključivanjem dobivamo da među elementima 3. stupca $\{a''_{33}, \dots, a''_{n3}\}$ mora postojati barem jedan element različit od nule i nastavljamo postupak. U posljednjem koraku imat ćemo

$$A \sim \begin{pmatrix} 1 & 0 & \dots & 0 & a^{(n-1)}_{1n} \\ 0 & 1 & \dots & 0 & a^{(n-1)}_{2n} \\ \vdots & \vdots & \dots & \vdots & \vdots \\ 0 & 0 & \dots & 1 & a^{(n-1)}_{2,n-1} \\ 0 & 0 & \dots & 0 & a^{(n-1)}_{nn} \end{pmatrix} = A^{(n-1)},$$

pri čemu je nužno $a_{nn}^{(n-1)} \neq 0$ jer bi u suprotnom imali $r(A) = r(A^{(n-1)}) = n - 1 < n$. Stoga smo dobili da je $A \sim I$ pri čemu smo rabili samo elementarne transformacije nad redcima matrice.

Posve analogno mogli bismo provoditi elementarne transformacije samo nad stupcima matrice i doći do istog zaključka.

Primjer 37. Transformirat ćemo zadanu matricu A koristeći samo elementarne transformacije nad redcima matrice.

$$\begin{aligned}
A &= \begin{pmatrix} 1 & 2 & -1 \\ 2 & 3 & 5 \\ 0 & -1 & 9 \end{pmatrix} \\
&\sim \left\{ \textit{2.retku dodamo 1. redak pomnožen s} -2 \right\} \sim \begin{pmatrix} 1 & 2 & -1 \\ 0 & -1 & 7 \\ 0 & -1 & 9 \end{pmatrix} \\
&\sim \left\{ \begin{array}{c} \textit{1. retku dodamo 2. redak pomnožen s } 2 \\ \textit{3. retku dodamo 2. redak pomnožen s} -1 \end{array} \right\} \sim \begin{pmatrix} 1 & 0 & 13 \\ 0 & -1 & 7 \\ 0 & 0 & 2 \end{pmatrix} \\
&\sim \left\{ \begin{array}{c} \textit{2. redak pomnožimo s } -1 \\ \textit{3. redak pomnožimo s } \frac{1}{2} \end{array} \right\} \sim \begin{pmatrix} 1 & 0 & 13 \\ 0 & 1 & -7 \\ 0 & 0 & 1 \end{pmatrix}
\end{aligned}$$

$$\sim \left\{ \begin{array}{c} \textit{1. retku dodamo 3. redak pomnožen s } -13 \\ \textit{2. retku dodamo 3. redak pomnožen sa } 7 \end{array} \right\} \sim \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = I.$$

♡

Svojstvo da se regularna matrica može svesti na jediničnu matricu koristeći elementarne transformacije samo nad redcima matrice (ili samo nad stupcima) može se iskoristiti za *postupak određivanja inverza.* Zaista, ako je $A \in GL(n, \mathbb{F})$, onda postoje elementarne matrice $F_1, \ldots, F_k$ reda n takve da je

$$I = F_k \cdots F_1 A.$$

Zbog jedinstvenosti inverza jasno je da je

$$A^{-1} = F_k \cdots F_1.$$

No i više, jer je

$$A^{-1} = (F_k \cdots F_1)I,$$

slijedi da ćemo inverz A^{-1} dobiti transformirajući matricu I istim transformacijama koje činimo nad redcima matrice A sa ciljem dobivanja jedinične matrice A. Prirodno je da se te transformacije izvode istovremeno. Ukratko, događa se sljedeće

$$(A \vdots I) \sim \{ \text{ elementarne transformacije nad redcima } \} \sim (I \vdots A^{-1}).$$

Primjer 38. Odredimo inverz matrice A iz prethodnog primjera.

$$
\begin{aligned}
(A \vdots I) &= \left(\begin{array}{ccc|ccc} \boxed{1} & 2 & -1 & 1 & 0 & 0 \\ 2 & 3 & 5 & 0 & 1 & 0 \\ 0 & -1 & 9 & 0 & 0 & 1 \end{array}\right) \\
&\sim \left(\begin{array}{ccc|ccc} 1 & 2 & -1 & 1 & 0 & 0 \\ 0 & \boxed{-1} & 7 & -2 & 1 & 0 \\ 0 & -1 & 9 & 0 & 0 & 1 \end{array}\right) \\
&\sim \left(\begin{array}{ccc|ccc} 1 & 0 & 13 & -3 & 2 & 0 \\ 0 & -1 & 7 & -2 & 1 & 0 \\ 0 & 0 & 2 & 2 & -1 & 1 \end{array}\right) \\
&\sim \left(\begin{array}{ccc|ccc} 1 & 0 & 13 & -3 & 2 & 0 \\ 0 & 1 & -7 & 2 & -1 & 0 \\ 0 & 0 & \boxed{1} & 1 & -\frac{1}{2} & \frac{1}{2} \end{array}\right) \\
&\sim \left(\begin{array}{ccc|ccc} 1 & 0 & 0 & -16 & \frac{17}{2} & \frac{-13}{2} \\ 0 & 1 & 0 & 9 & -\frac{9}{2} & \frac{7}{2} \\ 0 & 0 & 1 & 1 & -\frac{1}{2} & \frac{1}{2} \end{array}\right) = (I \vdots A^{-1}).
\end{aligned}
$$

Oznaka elementa $\boxed{a_{ij}}$ znači da se transformacije izvode nad svim redcima matrice osim na i-tom sa ciljem da svi elementi j-tog stupca postanu nule, osim samog elementa a_{ij}. Taj se element često zove *pivotni*.

♡

Propozicija 2.6.4. *Umnožak dviju kvadratnih matrica je regularna matrica ako i samo ako su obje matrice regularne.*

Dokaz. Otprije znamo da je umnožak regularnih matrica A i B reda n također regularna matrica.

Obrnuto, ako je AB regularna matrica, onda je $r(AB) = n$ po Teoremu 2.6.1 Prema Propoziciji 2.5.12 tada obje matrice A i B imaju rang jednak n.

□

Primjer 39. Kažemo da je matrica $A \in M_n(\mathbb{F})$ *ortogonalna* ako je $AA^t = A^tA = I$, to jest ako je $A^{-1} = A^t$. Skup ortogonalnih matrica reda n s elementima iz $\mathbb{F}$ označavamo s $O(n, \mathbb{F})$ i on čini podgrupu opće linearne grupe $GL(n, \mathbb{F})$. Zaista, ako su $A, B \in O(n, \mathbb{F})$, tada je

$$(AB)(AB)^t = (AB)(B^tA^t) = A(BB^t)A^t = AIA^t = AA^t = I.$$

Dakle, $AB \in O(n, \mathbb{F})$. Nadalje, inverz $A^{-1} = A^t$ je ortogonalna matrica, pa je $O(n, \mathbb{F})$ podgrupa od $GL(n, \mathbb{F})$.

Matrica

$$A = \begin{pmatrix} 3/5 & 4/5 \\ -4/5 & 3/5 \end{pmatrix}$$

je jedna ortogonalna matrica reda 2. Uočimo da je

$$\left(\frac{3}{5}\right)^2 + \left(\frac{4}{5}\right)^2 = 1, \ \left(-\frac{4}{5}\right)^2 + \left(\frac{3}{5}\right)^2 = 1, \ \frac{3}{5} \cdot \frac{4}{5} + \left(-\frac{4}{5}\right)\frac{3}{5} = 0.$$

Dakle, zbroj kvadrata elemenata nekog retka je 1, a zbroj umnožaka odgovarajućih koeficijenata prvog i drugog retka je 0. Lako se vidi da isto vrijedi i za stupce matrice A. No, opaženo svojstvo vrijedi i općenito za $A = [a_{ij}] \in O(n, \mathbb{F})$. Kako je $AA^t = I$, imamo da je i $[AA^t]_{ij} = [I]_{ij} = \delta_{ij}$ i

$$[AA^t]_{ij} = \sum_{k=1}^{n} [A]_{ik}[A^t]_{kj} = \sum_{k=1}^{n} a_{ik}a_{jk},$$

pa je

$$\sum_{k=1}^{n} a_{ik}a_{jk} = \delta_{ij}.$$

Za $i = j$ je

$$\sum_{k=1}^{n} a_{ik}^2 = 1,$$

a za $i \neq j$

$$\sum_{k=1}^{n} a_{ik}a_{jk} = 0.$$

Na temelju ovih relacija, naziv *ortogonalna matrica* postat će jasniji u Linearnoj algebri 2, kad se bude proučavala operacija *skalarnog množenja* na vektorskom prostoru. Redci ortogonalne matrice činit će tada tzv. ortonormirani skup vektora.

Analogno svojstvo imaju stupci matrice A, jer iz jednakost $A^tA = I$ dobivamo

$$\sum_{k=1}^{n} a_{ki}^2 = 1, \ \sum_{k=1}^{n} a_{ki}a_{kj} = 0, \ i \neq j.$$

Dakle, i stupci matrice A su normirani vektori i međusobno ortogonalni.

Poznati primjer ortogonalne matrice je

$$\begin{pmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix}, \ \alpha \in \mathbb{R}.$$

♡

Poglavlje 3

Sustavi linearnih jednadžbi

3.1 Osnovni pojmovi i definicije

Definicija 3.1.1. ***Linearna jednadžba s*** n ***nepoznanica nad poljem*** $\mathbb{F}$ *je svaka jednadžba oblika*

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n = b, \tag{3.1}$$

pri čemu su x_1, *...,* x_n *nepoznanice,* a_1, *...,* $a_n \in \mathbb{F}$ *koeficijenti, te* $b \in \mathbb{F}$ *slobodni koeficijent. Ako je* $b = 0$, *onda se jednadžba (3.1) naziva* ***homogenom****.*

Rješenje jednadžbe *(3.1) je svaka uređena n-torka* $(\gamma_1, \ldots, \gamma_n) \in \mathbb{F}^n$ *takva da supstitucijom* $x_1 = \gamma_1$, *...,* $x_n = \gamma_n$ *u (3.1) dobivamo numerički identitet.*

Riješiti jednadžbu *(3.1) znači odrediti skup svih njenih rješenja.*

Primjer 40. Jednadžba

$$2x - y + z + 3 = 0$$

predstavlja opći ili implicitni oblik jednadžbe ravnine u E^3 (odnosno $\mathbb{R}^3$). Za $x = t$ i $y = s$ dobivamo pripadni parametarski koordinatni oblik jednadžbe te ravnine

$$\begin{aligned} x &= t, \\ y &= s, \\ z &= -2t + s - 3, \ \ s, t \in \mathbb{R}, \end{aligned}$$

iz kojeg možemo iščitati skup rješenja početne jednadžbe

$$\{(t, s, -2t + s - 3) \, : \, t, s \in \mathbb{R}\} = \{(0, 0, -3) + t(1, 0, -2) + s(0, 1, 1) \, : \, t, s \in \mathbb{R}\}.$$

Još kažemo da ova ravnina prolazi točkom $(0, 0, -3)$ i razapeta je vektorima $(1, 0, -2)$ i $(0, 1, 1)$.

♡

Definicija 3.1.2. *Neka su* $m, n \in \mathbb{N}$. ***Sustav od*** m ***linearnih jednadžbi s*** n ***nepoznanica nad poljem*** $\mathbb{F}$ *je sustav jednadžbi oblika*

$$\begin{array}{ccccccccc} a_{11}x_1 & + & a_{12}x_2 & + & \cdots & + & a_{1n}x_n & = & b_1 \\ a_{21}x_1 & + & a_{22}x_2 & + & \cdots & + & a_{2n}x_n & = & b_2 \\ \vdots & & \vdots & & \cdots & & \vdots & & \vdots \\ a_{m1}x_1 & + & a_{m2}x_2 & + & \cdots & + & a_{mn}x_n & = & b_m \end{array} \tag{3.2}$$

pri čemu su x_1, ..., x_n nepoznanice, $a_{ij} \in \mathbb{F}$ koeficijenti, te $b_i \in \mathbb{F}$ slobodni koeficijenti, $i = 1, \ldots, m$, $j = 1, \ldots, n$. Ako je $b_1 = \cdots = b_m = 0$, onda se sustav (3.2) naziva ***homogen sustav****.*

Rješenje sustava *(3.2) je svaka uređena n-torka $(\gamma_1, \ldots, \gamma_n) \in \mathbb{F}^n$ takva da supstitucijom $x_1 = \gamma_1$, ..., $x_n = \gamma_n$ u (3.2) dobivamo m numeričkih identiteta.*

Riješiti sustav *(3.2) znači odrediti skup svih njegovih rješenja.*

Ako je R_i skup svih rješenja i-te jednadžbe u (3.2), onda je skup svih rješenja sustava (3.2) jednak

$$R = \bigcap_{i=1}^{m} R_i.$$

Sustav je *rješiv* ili *konzistentan* ako ima bar jedno rješenje, odnosno ako $R \neq \emptyset$.

Primjer 41. Sustav

$$\begin{array}{rcrcr} 2x & + & y & = & -1 \\ x & - & y & = & 4 \end{array}$$

je rješiv. Štoviše, ima jedinstveno rješenje $(1, -3)$. Dakle, $R = \{(1, -3)\}$.

Sustav

$$\begin{array}{rcrcr} 2x & + & y & = & -1 \\ -4x & - & 2y & = & 2 \end{array}$$

je također rješiv. Na primjer, uređeni par $(0, -1)$ zadovoljava sustav. No, ovaj sustav ima beskonačno mnogo rješenja. Skup svih rješenja jednak je

$$R = \{(t, -2t - 1) \, : \, t \in \mathbb{R}\}.$$

Sustav

$$\begin{array}{rcrcr} 2x & + & y & = & -1 \\ -4x & - & 2y & = & 5 \end{array}$$

nema rješenja, to jest nekonzistentan je.

Navedeni primjeri opisuju sve slučajeve koje možemo dobiti prilikom rješavanja sustava s dvije linearne jednadžbe u dvije nepoznanice. Zaista, kako se jedna linearna jednadžba u dvije nepoznanice geometrijski interpretira kao pravac u ravnini, rješavanje sustava "2 puta 2" interpretiramo kao traženje presjeka dvaju pravaca u ravnini. Stoga se pravci mogu sjeći u jednoj točki (jedinstveno rješenje sustava), mogu se poklapati (beskonačno rješenja sustava) ili mogu biti paralelni (sustav nema rješenja).

♡

Primjer 42. Svaki homogeni sustav je rješiv, jer ima barem jedno, očigledno rješenje:

$$x_1 = x_2 = \cdots = x_n = 0,$$

to jest $(0, 0, \ldots, 0)$. To rješenje naziva se *trivijalnim*. Dakle, za homogene sustave od interesa je pitanje ima li samo trivijalno rješenje ili ima i drugačijih, netrivijalnih rješenja. Pokazat će se da je to pitanje važno za opis strukture svakog sustava linearnih jednadžbi.

♡

Pitanja koja se prirodno nameću i s kojima ćemo se baviti u nastavku su sljedeća:

- Kada je sustav linearnih jednadžbi rješiv?
- Ako je sustav linearnih jednadžbi rješiv, kako opisati skup svih njegovih rješenja?
- Postoji li univerzalna metoda rješavanja sustava linearnih jednadžbi?

Prije toga uvest ćemo kraći, odnosno *matrični zapis* sustava (3.2). Koeficijente sustava (3.2) 'smjestimo' u matricu tipa (m, n),

$$A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \dots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix},$$

a slobodne koeficijente i nepoznanice u stupčane matrice tipa $(m, 1)$, odnosno $(n, 1)$

$$B = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_m \end{pmatrix}, \; X = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}.$$

Sada uočimo da je sustav (3.2) ekvivalentan *matričnoj jednadžbi*

$$AX = B, \tag{3.3}$$

pri čemu AX predstavlja umnožak matrica A i X. Riješiti sustav (3.2) ekvivalentno je rješavanju matrične jednadžbe (3.3). Iz tog razloga rješenja sustava (3.2) često prikazujemo i zapisujemo kao stupčane matrice iz $M_{n1}(\mathbb{F})$,

$$\mathbb{F}^n \ni (\gamma_1, \dots, \gamma_n) \;\leftrightsquigarrow\; \begin{pmatrix} \gamma_1 \\ \gamma_2 \\ \vdots \\ \gamma_n \end{pmatrix} \in M_{n1}(\mathbb{F}).$$

Matrica A naziva se *matrica sustava* (3.2). Sustavu (3.2) pridružujemo i takozvanu *proširenu matricu sustava*,

$$A_p = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} & b_1 \\ a_{21} & a_{22} & \dots & a_{2n} & b_2 \\ \vdots & \vdots & \dots & \vdots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} & b_m \end{pmatrix} = (A \,\vdots\, B).$$

Uočimo, $A_p \in M_{m,n+1}(\mathbb{F})$.

3.2 Rješivost sustava. Kriterij jednoznačnosti rješenja.

Propozicija 3.2.1. *Neka je $(\gamma_1, \dots, \gamma_n) \in \mathbb{F}^n$ rješenje sustava (3.2). Tada je*

$$B = \gamma_1 S_1 + \cdots + \gamma_n S_n,$$

gdje je $(S_1, \dots, S_n)$ stupčana reprezentacija matrice sustava A, te B matrica slobodnih koeficijenata sustava.

Obratno, ako se B može prikazati u obliku $B = \gamma_1 S_1 + \cdots + \gamma_n S_n$ pri čemu su $\gamma_1, \dots, \gamma_n \in \mathbb{F}$, onda je uređena n-torka $(\gamma_1, \dots, \gamma_n)$ jedno rješenje sustava (3.2).

Dokaz. Najprije primijetimo da prva tvrdnja slijedi iz Propozicije 2.5.11 kao poseban slučaj kad se matrica tipa (m, n) množi jednostupčanom matricom tipa $(n, 1)$. Radi preglednosti kod rješavanja sustava linearnih jednadžbi, napišimo to ipak i ovdje, za rješenje $(\gamma_1, \dots, \gamma_n) \in \mathbb{F}^n$ sustava (3.2). Vrijedi

$$\begin{aligned}
B &= \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \dots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix} \begin{pmatrix} \gamma_1 \\ \gamma_2 \\ \vdots \\ \gamma_n \end{pmatrix} = \begin{pmatrix} \sum_{k=1}^n a_{1k}\gamma_k \\ \sum_{k=1}^n a_{2k}\gamma_k \\ \vdots \\ \sum_{k=1}^n a_{mk}\gamma_k \end{pmatrix} \\
&= \gamma_1 \begin{pmatrix} a_{11} \\ a_{21} \\ \vdots \\ a_{m1} \end{pmatrix} + \gamma_2 \begin{pmatrix} a_{12} \\ a_{22} \\ \vdots \\ a_{m2} \end{pmatrix} + \cdots + \gamma_n \begin{pmatrix} a_{1n} \\ a_{2n} \\ \vdots \\ a_{mn} \end{pmatrix}.
\end{aligned}$$

Odavde je očito da vrijedi i obrat tvrdnje. □

Uočimo da je homogenom sustavu pridružena matrična jednadžba $AX = 0$ te da za trivijalno rješenje vrijedi $0 = 0 \cdot S_1 + \cdots + 0 \cdot S_n$.

Teorem 3.2.2 (Kronecker-Capelli). *Sustav $AX = B$ je rješiv ako i samo ako je rang matrice sustava A jednak rangu proširene matrice sustava A_p.*

Dokaz. Prisjetimo se,

$$r(A) = \dim[S_1, \dots, S_n],$$

gdje $(S_1, \dots, S_n)$ stupčana reprezentacija matrice sustava A.

Prema Propoziciji 3.2.1 sustav $AX = B$ je rješiv ako i samo ako je $B \in [S_1, \dots, S_n]$. Uočimo da je ovo ispunjeno ako i samo ako vrijedi jednakost potprostora

$$[S_1, \dots, S_n] = [S_1, \dots, S_n, B].$$

Budući da svakako vrijedi $[S_1, \dots, S_n] \leq [S_1, \dots, S_n, B]$, ovi potprostori jednaki su ako i samo ako su im jednake dimenzije,

$$r(A) = \dim[S_1, \dots, S_n] = \dim[S_1, \dots, S_n, B] = r(A_p).$$

□

Korolar 3.2.3. *Sustav (3.2) ima jedinstveno rješenje ako i samo ako je*

$$r(A) = r(A_p) = n.$$

Dokaz. Ako sustav (3.2) ima jedinstveno rješenje $(\gamma_1, \dots, \gamma_n) \in \mathbb{F}^n$, onda je prikaz vektora B kao linearne kombinacije, $B = \gamma_1 S_1 + \cdots + \gamma_n S_n$, jedinstven. Stoga je skup $\{S_1, \dots, S_n\}$ linearno nezavisan, pa i baza linearne ljuske $[S_1, \dots, S_n]$. Naime, ako bi postojala netrivijalna linearna kombinacija $\lambda_1 S_1 + \cdots + \lambda_n S_n = 0$ onda bi uređena n-torka $(\gamma_1 + \lambda_1, \dots, \gamma_n + \lambda_n)$ bila rješenje sustava različito od $(\gamma_1, \dots, \gamma_n)$, suprotno pretpostavci. Dakle, $r(A) = n$, a $r(A) = r(A_p)$ (prema Propoziciji 3.2.1).

Obratno, ako je $r(A) = r(A_p)$, onda sustav ima rješenja i $B \in [S_1, \dots, S_n]$ (Propozicija 3.2.1). Kako je $r(A) = n$, skup $\{S_1, \dots, S_n\}$ je linearno nezavisan, pa je prikaz vektora B u bazi $\{S_1, \dots, S_n\}$ jedinstven što povlači jedinstvenost rješenja sustava. □

Napomenimo da smo u prvom dijelu dokaza ovog korolara mogli primijeniti tvrdnju Zadatka 7. Umjesto toga, radi cjelovitosti dokaza korolara, tvrdnju smo dokazali unutar konteksta koji nam je ovdje važan. Uz prilagodbu oznaka, tu zapravo vidimo rješenje Zadatka 7. Uvjerite se u to sami, za vježbu.

3.3 Homogen sustav. Struktura skupa rješenja.

Već znamo da homogeni sustav $AX = 0$ uvijek ima barem trivijalno rješenje 0, to jest $(0, 0, \dots, 0)$. Uočimo jedan jednostavan dovoljan uvjet (ne i nužan) za postojanje netrivijalnog rješenja homogenog sustava: ako je $m < n$, dakle broj jednadžbi homogenog sustava manji od broja nepoznanica, onda taj sustav ima neko rješenje različito od trivijalnog. Naime, kako rang matrice nije veći od broja redaka matrice, u tom slučaju imamo $r(A) \le m < n$ pa iz Korolara 3.2.3 slijedi da rješenje sustava nije jedinstveno. Sad ćemo pokazati da skup svih rješenja homogenog sustava ima strukturu koja nam je vrlo dobro poznata:

Propozicija 3.3.1. *Skup svih rješenja homogenog sustava $AX = 0$ čini vektorski potprostor od $M_{n1}(\mathbb{F})$, odnosno $\mathbb{F}^n$.*

Dokaz. Označimo s

$$\mathcal{H} = \{H \in M_{n1}(\mathbb{F}) \,:\, AH = 0\}.$$

Neka su $H_1, H_2 \in \mathcal{H}$, te $\lambda \in \mathbb{F}$. Tada je

$$A(\lambda H_1 + H_2) = \lambda(AH_1) + (AH_2) = 0,$$

pa je i $\lambda H_1 + H_2$ rješenje homogenog sustava $AX = 0$, odnosno $\lambda H_1 + H_2 \in \mathcal{H}$. Dakle, $\mathcal{H} \le M_{n1}(\mathbb{F})$. □

Neka je $\{H_1, \dots, H_d\}$ baza potprostora $\mathcal{H}$. Tada je

$$\mathcal{H} = \{\lambda_1 H_1 + \cdots + \lambda_d H_d \,:\, \lambda_1, \dots, \lambda_d \in \mathbb{F}\}.$$

Drugim riječima, svako rješenje H homogenog sustava $AX = 0$ oblika je

$$H = \lambda_1 H_1 + \cdots + \lambda_d H_d,$$

za neke $\lambda_1, \ldots, \lambda_d \in \mathbb{F}$. Prethodno opažanje vrijedi u svakom vektorskom prostoru, no za sada još ne znamo kako pronaći bazu i dimenziju za $\mathcal{H}$. Na ta pitanja dat ćemo odgovor u sklopu metode za rješavanje sustava.

Skup svih rješenja nehomogenog sustava $AX = B$ usko je povezan sa skupom svih rješenja pripadnog homogenog sustava $AX = 0$.

Teorem 3.3.2. *Neka je $R_0 \in M_{n1}(\mathbb{F})$ neko rješenje sustava $AX = B$. Skup svih rješenja sustava $AX = B$ je*

$$\mathcal{R} = R_0 + \mathcal{H} = \{R_0 + H \,:\, H \in \mathcal{H}\}.$$

Dokaz. Treba pokazati inkluzije, $\mathcal{R} \subseteq \{R_0 + H \,:\, H \in \mathcal{H}\}$ i $\{R_0 + H \,:\, H \in \mathcal{H}\} \subseteq \mathcal{R}$. Ako je $R_1 \in \mathcal{R}$, onda je $A(R_1 - R_0) = B - B = 0$, pa je $R_1 - R_0 \in \mathcal{H}$ i $R_0 + (R_1 - R_0) \in \{R_0 + H \,:\, H \in \mathcal{H}\}$.

S druge strane, $A(R_0 + H) = AR_0 + AH = B + 0 = B$, pa je $R_0 + H \in \mathcal{R}$. □

Istaknuto rješenje R_0 sustava $AX = B$ naziva se *partikularno rješenje.* Teorem 3.3.2 nam kaže da se svako rješenje nehomogenog sustava može izraziti kao zbroj nekog partikularnog rješenja i nekog rješenja pripadnog homogenog sustava. Skup oblika $R_0+\mathcal{H}$ naziva se *linearna mnogostrukost* (pri čemu je bitno da je $\mathcal{H}$ potprostor). Uočimo da bilo koje rješenje sustava može poslužiti kao odabrano partikularno rješenje. Naravno, ako sustav $AX = B$ ima jedinstveno rješenje R_0, onda je $\mathcal{H} = \{0\}$ i $\mathcal{R} = \{R_0\}$.

Linearnu mnogostrukost možemo geometrijski shvatiti kao translatirani potprostor. U slučaju sustava s tri nepoznanice to može biti točka, pravac ili ravnina kao translatirani potprostor dimenzije 0, 1 ili 2. U Primjeru 40 skup rješenja zapisan je kao jednadžba ravnine u parametarskom obliku. To je linearna mnogostrukost $R_0 + \mathcal{H} = (0, 0, -3) + [(1, 0, -2), (0, 1, 1)]$.

3.4 Postupak rješavanja sustava. Gaussova metoda.

Definicija 3.4.1. *Dva sustava linearnih jednadžbi nad istim poljem $\mathbb{F}$ su* ***ekvivalentna*** *ako imaju isti broj nepoznanica i isti skup rješenja.*

Ideja našeg postupka rješavanja sustava bit će u tome da sustav transformiramo u njemu ekvivalentan, ali jednostavniji od početnog u smislu da iz njega možemo lako iščitati rješenje.

Primjer 43. Sljedeća tri sustava su ekvivalentna;

$$(1)\quad \left\{\begin{array}{rcrcrcr} x_1 & + & 3x_2 & + & 2x_3 & = & -1 \\ 2x_1 & + & 3x_2 & + & 8x_3 & = & 1 \\ x_1 & + & x_2 & + & 3x_3 & = & 1 \end{array}\right. ,$$

$$(2)\quad \left\{\begin{array}{rcrcrcr} x_1 & + & 2x_2 & + & 3x_3 & = & 0 \\ & - & x_2 & + & 2x_3 & = & 1 \\ & & & & x_3 & = & 0 \end{array}\right. ,$$

$$(3)\quad \left\{\begin{array}{rrrcr} x_1 & & & = & 2 \\ & x_2 & & = & -1 \\ & & x_3 & = & 0 \end{array}\right. .$$

Rješenje ovih sustava je jedinstveno - $(2,-1,0)$. Lako je odabrati koji je ovih sustava najlakše riješiti - to je sustav (3). I sustav (2) se lako rješava, supstitucijom unazad, dok je sustav (1) potrebno dodatno transformirati kako bi se došlo do rješenja.

$\heartsuit$

Iz prethodnog primjera možemo zaključiti da jednostavnim sustavima smatramo one čija je matrica sustava dijagonalna (jedinična) ili gornjetrokutasta. No, to nije uvijek moguće dobiti budući da matrica sustava ne mora biti kvadratna, a i rješenje ne mora biti nužno jedinstveno. Ipak, koristeći elementarne transformacije nad redcima proširene matrice moguće je dobiti takvu matricu da ćemo rješenje samo 'pročitati'.

Propozicija 3.4.2. *Primjenom elementarnih transformacija na jednadžbama sustava, odnosno na redcima pripadne proširene matrice, dobivamo sustav ekvivalentan polaznom.*

Dokaz. Neka je zadan sustav $AX = B$, $A \in M_{mn}(\mathbb{F})$. Elementarne transformacije na redcima pripadne proširene matrice realiziraju se množenjem lijeva s elementarnim matricama, odnosno nekom regularnom matricom $T \in M_m(\mathbb{F})$. Stoga nakon provedenih transformacija dobivamo sustav $(TA)X = TB$. Jasno je da je sustav $AX = B$ rješiv ako i samo ako je $(TA)X = TB$ rješiv, jer je $r(A) = r(TA)$ i $r(A_p) = r(TA_p)$, te $TA_p = (TA \vdots TB)$. Nadalje, ako je $R \in M_{n1}(\mathbb{F})$ rješenje sustava $AX = B$, to jest $AR = B$, onda je i $(TA)R = TB$. Obratno, ako $(TA)R = TB$, onda množenjem inverzom T^{-1} slijeva, slijedi da je $AR = B$. Stoga, matrične jednadžbe $AX = B$ i $(TA)X = TB$ imaju isti skup rješenja, odnosno one su ekvivalentne. $\square$

Pretpostavimo prvo da je $r(A) = r < n$. Primjenom konačno mnogo elementarnih transformacija nad redcima proširene matrice A_p (i do na eventualnu zamjenu redoslijeda varijabli) možemo dobiti sljedeće

$$A_p \sim \left(\begin{array}{cccc|ccc:c} 1 & 0 & \cdots & 0 & a'_{1,r+1} & \cdots & a'_{1,n} & b'_1 \\ 0 & 1 & \cdots & 0 & a'_{2,r+1} & \cdots & a'_{2,n} & b'_2 \\ \vdots & \vdots & \cdots & \vdots & \vdots & \cdots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & a'_{r,r+1} & \cdots & a'_{r,n} & b'_r \\ \hline 0 & 0 & \cdots & 0 & 0 & \cdots & 0 & b'_{r+1} \\ \vdots & \vdots & \cdots & \vdots & \vdots & \cdots & \vdots & \vdots \\ 0 & 0 & \cdots & 0 & 0 & \cdots & 0 & b'_m \end{array}\right), \tag{3.4}$$

gdje su $a'_{ij} \in \mathbb{F}$ za $i = 1,\dots,r$, $j = r+1,\dots,n$, zatim $b'_1,\dots,b'_r \in \mathbb{F}$, te $(b'_{r+1},\dots,b'_m) = (0,\dots,0)$ ili $(b'_{r+1},\dots,b'_m) = (1,\dots,0)$. Uočimo, da je jedinična podmatrica (blok) reda r. Postupak transformiranja proširene matrice sustava na matricu u (3.4) zovemo *Gaussova metoda eliminacije.*

Ako je $(b'_{r+1},\dots,b'_m) = (0,\dots,0)$, onda očito $r(A) = r(A_p) = r$, pa prema Kronecker-Capellijevom teoremu 3.2.2, sustav $AX = B$ ima rješenje. Ako je $(b'_{r+1},\dots,b'_m) = (1,\dots,0)$, onda $r(A) = r < r(A_p) = r+1$, pa sustav nije konzistentan.

Pretpostavimo da je sustav rješiv i da je $r < n$. Stoga je prema (3.4) početni sustav ekvivalentan sljedećem:

$$\begin{array}{ccccccccccc} x_1 & & & + & a'_{1,r+1}x_{r+1} & + & \cdots & + & a'_{1,n}x_n & = & b'_1 \\ & x_2 & & + & a'_{2,r+1}x_{r+1} & + & \cdots & + & a'_{2,n}x_n & = & b'_2 \\ & & & & & & & & & \vdots & \\ & & x_r & + & a'_{r,r+1}x_{r+1} & + & \cdots & + & a'_{r,n}x_n & = & b'_r \end{array}. \tag{3.5}$$

U (3.5) vidimo da se nepoznanice $x_1, \ldots, x_r$ mogu izraziti pomoću nepoznanica $x_{r+1}, \ldots, x_n$. Zaista,

$$\begin{array}{ccl} x_1 & = & b'_1 - a'_{1,r+1}x_{r+1} - \cdots - a'_{1,n}x_n \\ x_2 & = & b'_2 - a'_{2,r+1}x_{r+1} - \cdots - a'_{2,n}x_n \\ \vdots & & \\ x_r & = & b'_1 - a'_{r,r+1}x_{r+1} - \cdots - a'_{r,n}x_n \end{array}. \tag{3.6}$$

Stoga je prirodno nepoznanice $x_1, \ldots, x_n$ razvrstati u dvije skupine: skup $\{x_1, \ldots, x_r\}$ i skup $\{x_{r+1}, \ldots, x_n\}$ koje ćemo proglasiti *slobodnim parametrima* u $\mathbb{F}$. Za svaki izbor $(x_{r+1}, \ldots, x_n) \in \mathbb{F}^{n-r}$ dobivamo točno jedno rješenje sustava. Stavljamo

$$\lambda_1 = x_{r+1}, \ \lambda_2 = x_{r+2}, \ \ldots, \ \lambda_{n-r} = x_n,$$

i (3.6) zapisujemo matrično

$$\begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_r \\ x_{r+1} \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} b'_1 - a'_{1,r+1}\lambda_1 - \cdots - a'_{1,n}\lambda_{n-r} \\ b'_2 - a'_{2,r+1}\lambda_1 - \cdots - a'_{2,n}\lambda_{n-r} \\ \vdots \\ b'_r - a'_{r,r+1}\lambda_1 - \cdots - a'_{r,n}\lambda_{n-r} \\ \lambda_1 \\ \vdots \\ \lambda_{n-r} \end{pmatrix},$$

odnosno

$$\begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_r \\ x_{r+1} \\ x_{r+2} \\ \vdots \\ x_n \end{pmatrix} = \underbrace{\begin{pmatrix} b'_1 \\ b'_2 \\ \vdots \\ b'_r \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}}_{R_0} + \lambda_1 \underbrace{\begin{pmatrix} -a'_{1,r+1} \\ -a'_{2,r+1} \\ \vdots \\ -a'_{r,r+1} \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}}_{H_1} + \lambda_2 \underbrace{\begin{pmatrix} -a'_{1,r+2} \\ -a'_{2,r+2} \\ \vdots \\ -a'_{r,r+2} \\ 0 \\ 1 \\ \vdots \\ 0 \end{pmatrix}}_{H_2} + \cdots + \lambda_{n-r} \underbrace{\begin{pmatrix} -a'_{1,n} \\ -a'_{2,n} \\ \vdots \\ -a'_{r,n} \\ 0 \\ 0 \\ \vdots \\ 1 \end{pmatrix}}_{H_{n-r}}.$$

Uočimo,

$$AR_0 = B, \ AH_1 = 0, \ \ldots, AH_{n-r} = 0,$$

odnosno R_0 je partikularno rješenje sustava očito dobiveno izborom $(\lambda_1, \ldots, \lambda_{n-r}) = (0, \ldots, 0)$, dok su $H_1, \ldots, H_{n-r}$ rješenja pripadnog homogenog sustava $AX = 0$. Lako možemo ustanoviti da je skup $\{H_1, \ldots, H_{n-r}\}$ linearno nezavisan i razapinje potprostor $\mathcal{H}$ - skup svih rješenja homogenog sustava $AX = 0$. Dakle, $\{H_1, \ldots, H_{n-r}\}$ je baza za $\mathcal{H}$. Ovime smo pokazali sljedeći teorem.

Teorem 3.4.3. *Neka je $\mathcal{H}$ skup svih rješenja homogenog sustava $AX = 0$, za $A \in M_{mn}(\mathbb{F})$. Tada je $\mathcal{H}$ vektorski potprostor od $M_{n1}(\mathbb{F})$ (odnosno $\mathbb{F}^n$) dimenzije $n - r$, gdje je $r = r(A)$.*

Napomenimo da u slučaju $n = r$ i $n < m$, umjesto (3.4) imamo

$$A_p \sim \left(\begin{array}{ccc|c} 1 & \cdots & 0 & b'_1 \\ \vdots & \ddots & \vdots & \vdots \\ 0 & \cdots & 1 & b'_n \\ \hline 0 & \cdots & 0 & b'_{n+1} \\ \vdots & \cdots & \vdots & \vdots \\ 0 & \cdots & 0 & b'_m \end{array}\right),$$

pa ako je $b'_{n+1} = \cdots = b'_m = 0$, onda sustav ima jedinstveno rješenje

$$R_0 = \begin{pmatrix} b'_1 \\ \vdots \\ b'_n \end{pmatrix}.$$

U slučaju kvadratnog sustava ($n = m$) i $n = r$, slijedi da je

$$A_p \sim \left(\begin{array}{ccc|c} 1 & \cdots & 0 & b'_1 \\ \vdots & \ddots & \vdots & \vdots \\ 0 & \cdots & 1 & b'_n \end{array}\right).$$

Dakle, kvadratni sustav kojem je pripadna matrica punog ranga ima uvijek jedinstveno rješenje R_0. Tada je matrica A i regularna, pa je $R_0 = A^{-1}B$.

Primjer 44. Gaussovom metodom rješit ćemo sustav:

$$\begin{array}{rcrcrcrcl} x_1 & + & 2x_2 & - & x_3 & + & 3x_4 & = & 8, \\ 2x_1 & + & 3x_2 & & & - & x_4 & = & 8, \\ & & x_2 & - & 2x_3 & + & 7x_4 & = & 8, \\ 3x_1 & + & 5x_2 & - & x_3 & + & 2x_4 & = & 16. \end{array}$$

Primjenjujemo elementarne transformacije nad retcima proširene matrice:

$$A_p = \left(\begin{array}{cccc|c} \boxed{1} & 2 & -1 & 3 & 8 \\ 2 & 3 & 0 & -1 & 8 \\ 0 & 1 & -2 & 7 & 8 \\ 3 & 5 & -1 & 2 & 16 \end{array}\right) \sim \left(\begin{array}{cccc|c} 1 & 2 & -1 & 3 & 8 \\ 0 & \boxed{-1} & 2 & -7 & -8 \\ 0 & 1 & -2 & 7 & 8 \\ 0 & -1 & 2 & -7 & -8 \end{array}\right) \sim$$

$$\left(\begin{array}{cccc|c} 1 & 0 & 3 & -11 & -8 \\ 0 & -1 & 2 & -7 & -8 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{array}\right) \sim \left(\begin{array}{cc|cc|c} 1 & 0 & 3 & -11 & -8 \\ 0 & 1 & -2 & 7 & 8 \\ \hline 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{array}\right).$$

Uočimo da smo matricu A_p upravo sveli na oblik (3.4) iz kojeg možemo iščitati rješenje sustava:

$$\begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} = \underbrace{\begin{pmatrix} -8 \\ 8 \\ 0 \\ 0 \end{pmatrix}}_{R_0} + \lambda_1 \underbrace{\begin{pmatrix} -3 \\ 2 \\ 1 \\ 0 \end{pmatrix}}_{H_1} + \lambda_2 \underbrace{\begin{pmatrix} 11 \\ -7 \\ 0 \\ 1 \end{pmatrix}}_{H_2}, \quad \lambda_1, \lambda_2 \in \mathbb{R}.$$

R_0 je partikularno rješenje sustava, a skup $\{H_1, H_2\}$ je baza za potprostor svih rješenja pripadnog homogenog sustava. Rješenje možemo provjeriti uvrštavanjem u dani sustav linearnih jednadžbi: $x_1 = -8 - 3\lambda_1 + 11\lambda_2$, $x_2 = 8 + 2\lambda_1 - 7\lambda_2$, $x_3 = \lambda_1$, $x_4 = \lambda_2$, ili množenjem matrica:

$$AR_0 = \begin{pmatrix} 8 \\ 8 \\ 8 \\ 16 \end{pmatrix}, \quad AH_1 = AH_2 = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}.$$

♡

U sljedećem primjeru pokazujemo da nije potrebno "forsirati" dobivanje jedinične matrice u gornjem lijevom kutu proširene matrice sustava, a to ponekad nije ni moguće bez zamjene redoslijeda nepoznanica. Dakle, sustav linearnih jednadžbi Gaussovom metodom nastojimo riješiti optimalno - u što je moguće manje koraka.

Primjer 45. Zadan je sustav linearnih jednadžbi:

$$\begin{array}{rcrcrcrcrcr} & & 2x_2 & + & x_3 & - & 3x_4 & & & = & 2, \\ & & 3x_2 & + & x_3 & - & x_4 & + & x_5 & = & 5, \\ & - & 4x_2 & - & x_3 & - & x_4 & - & 2x_5 & = & -8, \\ 2x_1 & & & - & x_3 & + & x_4 & + & x_5 & = & 4. \end{array}$$

Proširena matrica danog sustava je

$$A_p = \left(\begin{array}{rrrrr|r} 0 & 2 & 1 & -3 & 0 & 2 \\ 0 & 3 & 1 & -1 & \boxed{1} & 5 \\ 0 & -4 & -1 & -1 & -2 & -8 \\ 2 & 0 & -1 & 1 & 1 & 4 \end{array}\right).$$

Plavom bojom označili smo elemente podmatrice A iz koje je optimalno izabrati pivotni element, jer izaberemo li element iz zadnjeg, četvrtog, retka "pokvarit" ćemo prvi stupac. Odlučili smo se za pivotni element na mjestu $(2, 5)$ jer ćemo u sljedećem koraku provesti samo 2 elementarne transformacije:

$$A_p \sim \left(\begin{array}{rrrrr|r} 0 & 2 & \boxed{1} & -3 & 0 & 2 \\ 0 & 3 & 1 & -1 & 1 & 5 \\ 0 & 2 & 1 & -3 & 0 & 2 \\ 2 & -3 & -2 & 2 & 0 & -1 \end{array}\right).$$

Izbor pivotnog elementa se dodatno suzio - na elemente prvog retka (jer je treći redak jednak prvom). Zbog preglednosti dozvoljeno je u zapisu izbaciti jednake retke ili nulretke iako to nije sasvim korektno s obzirom na zapis jer relacija $\sim$ ne mijenja tip matrice.

$$A_p \sim \left(\begin{array}{ccccc|c} 0 & 2 & 1 & -3 & 0 & 2 \\ 0 & 1 & 0 & 2 & 1 & 3 \\ 2 & 1 & 0 & -4 & 0 & 3 \end{array}\right) \begin{array}{l} \\ \\ / \cdot \frac{1}{2} \end{array} \sim \left(\begin{array}{ccccc|c} 0 & 2 & 1 & -3 & 0 & 2 \\ 0 & 1 & 0 & 2 & 1 & 3 \\ 1 & \frac{1}{2} & 0 & -2 & 0 & \frac{3}{2} \end{array}\right).$$

Naš sustav je sada sređen i možemo iščitati rješenje, no ovaj put ćemo prije toga istaknuti sustav ekvivalentan početnom kojeg smo dobili opisanim postupkom. Nepoznanice koje ćemo zamijeniti tzv. slobodnim parametrima označili smo zelenom bojom.

$$\begin{array}{c} \begin{array}{cccccc} x_1 & {\color{green}x_2} & x_3 & {\color{green}x_4} & x_5 & \end{array} \\ \left(\begin{array}{ccccc|c} 0 & 2 & 1 & -3 & 0 & 2 \\ 0 & 1 & 0 & 2 & 1 & 3 \\ 1 & \frac{1}{2} & 0 & -2 & 0 & \frac{3}{2} \end{array}\right) \end{array} \rightsquigarrow \begin{array}{rcrcrcrcrcr} & & 2{\color{green}x_2} & + & x_3 & - & 3{\color{green}x_4} & & & = & 2, \\ & & {\color{green}x_2} & & & + & 2{\color{green}x_4} & + & x_5 & = & 3, \\ x_1 & + & \frac{1}{2}{\color{green}x_2} & & & - & 2{\color{green}x_4} & & & = & \frac{3}{2}; \\ & & \downarrow & & & & \downarrow & & & & \\ & & t_1 & & & & t_2 & & & & \end{array}$$

$$\begin{array}{rcrcrcr} x_1 & = & \frac{3}{2} & - & \frac{1}{2}t_1 & + & 2t_2, \\ x_2 & = & & & t_1 & & , \\ x_3 & = & 2 & - & 2t_1 & + & 3t_2, \\ x_4 & = & & & & & t_2, \\ x_5 & = & 3 & - & t_1 & - & 2t_2, \end{array} \rightsquigarrow X = \begin{pmatrix} \frac{3}{2} \\ 0 \\ 2 \\ 0 \\ 3 \end{pmatrix} + t_1 \begin{pmatrix} -\frac{1}{2} \\ 1 \\ -2 \\ 0 \\ -1 \end{pmatrix} + t_2 \begin{pmatrix} 2 \\ 0 \\ 3 \\ 1 \\ -2 \end{pmatrix}, t_1, t_2 \in \mathbb{R}.$$

♡

Primjer 46. Riješimo sustav u ovisnosti o parametru $t \in \mathbb{R}$:

$$\begin{array}{rcrcrcr} 2x_1 & + & tx_2 & - & x_3 & = & 2, \\ x_1 & + & x_2 & & & = & 1, \\ & - & 2x_2 & + & (t-1)x_3 & = & 3-t. \end{array}$$

Gaussovom metodom dobivamo:

$$A_p = \left(\begin{array}{ccc|c} 2 & t & -1 & 2 \\ 1 & \boxed{1} & 0 & 1 \\ 0 & -2 & t-1 & 3-t \end{array}\right) \sim \left(\begin{array}{ccc|c} 2-t & 0 & \boxed{-1} & 2-t \\ 1 & 1 & 0 & 1 \\ 2 & 0 & t-1 & 5-t \end{array}\right) \sim$$

$$\left(\begin{array}{ccc|c} 2-t & 0 & -1 & 2-t \\ 1 & 1 & 0 & 1 \\ \boxed{{\color{red}(3-t)t}} & 0 & 0 & (3-t)(t+1) \end{array}\right).$$

Sljedeći korak nije moguće provesti bez odgovarajuće diskusije, pa tako razlikujemo slučajeve: $(3-t)t \neq 0$, $t = 0$ i $t = 3$.

<u>Slučaj $(3-t)t \neq 0$:</u>

$$A_p \sim \left(\begin{array}{ccc|c} 0 & 0 & -1 & \frac{t-2}{t} \\ 0 & 1 & 0 & -\frac{1}{t} \\ 1 & 0 & 0 & \frac{t+1}{t} \end{array}\right) \sim \left(\begin{array}{ccc|c} 1 & 0 & 0 & \frac{t+1}{t} \\ 0 & 1 & 0 & -\frac{1}{t} \\ 0 & 0 & 1 & \frac{2-t}{t} \end{array}\right)$$

U ovom slučaju rješenje je jedinstveno:

$$X = \begin{pmatrix} \frac{t+1}{t} \\ -\frac{1}{t} \\ \frac{2-t}{t} \end{pmatrix}. \tag{3.7}$$

<u>Slučaj $t = 0$:</u>

$$A_p(t=0) \sim \left(\begin{array}{ccc|c} 2 & 0 & -1 & 2 \\ 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 3 \end{array}\right).$$

Sustav nema rješenja (- uočimo da zadnji redak matrice znači $0 = 3$ što nije moguće).

<u>Slučaj $t = 3$:</u>

$$A_p(t=3) \sim \left(\begin{array}{ccc|c} -1 & 0 & -1 & -1 \\ 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{array}\right) \sim \left(\begin{array}{ccc|c} 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{array}\right).$$

Rješenje je jednoparametarsko:

$$X = \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix} + \lambda \begin{pmatrix} 1 \\ -1 \\ -1 \end{pmatrix},\ \lambda \in \mathbb{R}. \tag{3.8}$$

Rezimirajmo: za

$\lambda \in \mathbb{R}\backslash\{0, 3\}$, sustav ima jedinstveno rješenje (3.7),
$\lambda = 0$, sustav nema rješenja,
$\lambda = 3$, sustav ima beskonačno rješenja koja su dana s (3.8).

♡

Poglavlje 4

Determinante

4.1 Definicija determinante. Grupa permutacija.

Na kolegiju Analitička geometrija definirali smo determinantu reda 2 i reda 3, odnosno determinantu matrice reda 2 i 3, jer se pokazala vrlo korisnim alatom za ispitivanje linearne nezavisnosti, računanje vektorskog i mješovitog produkta, itd. Prisjetimo se, determinanta reda 2 definira se kao

$$\begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix} = a_{11}a_{22} - a_{12}a_{21},$$

a determinanta reda 3 kao

$$\begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix} = a_{11}a_{22}a_{33} + a_{12}a_{23}a_{31} + a_{21}a_{32}a_{13} - a_{13}a_{22}a_{31} - a_{12}a_{21}a_{33} - a_{23}a_{32}a_{11}.$$

Formula kojom je zadana determinanta reda 3 može se učiniti prilično kompliciranom, no uočimo u njoj određenu pravilnost koja će nam pomoći da shvatimo kako se definira determinanta matrice općenitog reda n. Vidimo da se u toj formuli pojavljuje 6 članova, od kojih tri s predznakom $+$, a tri s predznakom $-$. Zanemarimo li privremeno izbor tih predznaka, uočimo da je svaki član umnožak tri koeficijenta iz matrice. Pritom se svaki od brojeva 1, 2 i 3 u svakom takvom umnošku pojavljuje i na mjestu prvog indeksa i na mjestu drugog indeksa za neki koeficijent. Jednostavno rečeno, u svakom članu pomnožena su neka tri koeficijenta iz matrice, ali tako da je svaki redak i svaki stupac matrice zastupljen s po jednim koeficijentom.

Za formiranje svakog člana trebamo "proći kroz matricu" tako da iz svakog retka izaberemo po jedan koeficijent, ali pazeći pritom da izabrani koeficijenti budu iz različitih stupaca. Primjerice, u prvom članu gornjeg izraza prošli smo matricom "dijagonalno" od gornjeg lijevog kuta do donjeg desnog kuta, a u četvrtom članu također "dijagonalno", ali po onoj drugoj dijagonali. Ovakvi članovi formirani su na sve moguće načine. Kako to vidimo? Istaknemo li prvi indeks svakog izabranog koeficijenta (možemo isto tako krenuti od drugog indeksa), pojedini umnožak mora imati oblik $a_{1\ldots}a_{2\ldots}a_{3\ldots}$, pri čemu su na mjestu drugog indeksa također brojevi 1, 2, 3 raspoređeni na bilo koji način. Takvih poredaka ima 6, to su permutacije skupa $\{1, 2, 3\}$. Svaki izbor po tri koeficijenta u skladu s navedenim pravilom može se zadati jednom permutacijom i primjena takvog zapisa ključna je za općenitu definiciju determinante.

$$\left|\begin{array}{ccc|cc} \cancel{a_{11}} & \cancel{a_{12}} & \cancel{a_{13}} & a_{11} & a_{12} \\ a_{21} & \cancel{a_{22}} & \cancel{a_{23}} & \cancel{a_{21}} & a_{22} \\ a_{31} & a_{32} & \cancel{a_{33}} & \cancel{a_{31}} & \cancel{a_{32}} \end{array}\right. \quad \rightsquigarrow \quad a_{11}a_{22}a_{33} + a_{12}a_{23}a_{31} + a_{21}a_{32}a_{13},$$

$$\left|\begin{array}{ccc|cc} a_{11} & a_{12} & \cancel{a_{13}} & \cancel{a_{11}} & \cancel{a_{12}} \\ a_{21} & \cancel{a_{22}} & \cancel{a_{23}} & \cancel{a_{21}} & a_{22} \\ \cancel{a_{31}} & \cancel{a_{32}} & \cancel{a_{33}} & a_{31} & a_{32} \end{array}\right. \quad \rightsquigarrow \quad -a_{13}a_{22}a_{31} - a_{12}a_{21}a_{33} - a_{23}a_{32}a_{11}.$$

(Za determinantu reda 2 vrijedi isto pravilo, ali rezultat je krajnje jednostavan jer postoje samo dvije mogućnosti "prolaza" kroz matricu reda 2, oba "dijagonalna").

Permutacije će nam, dakle, poslužiti kako bismo pregledno i jednostavno zapisali pravilo formiranja umnožaka po n koeficijenata matrice koji pripadaju različitim redcima i različitim stupcima, odnosno tako da je svaki redak i svaki stupac zastupljen u umnošku s točno jednim koeficijentom. Znamo da skup od n elemenata ima točno $n!$ permutacija, tako da determinanta reda 2 ima $2! = 2$ članova, reda 3 ima $3! = 6$ članova, reda 4 ima $4! = 24$ članova itd. Broj članova stoga vrlo brzo raste s povećavanjem reda matrice tako da eksplicitno ispisivanje članova postaje vrlo nepraktično za $n > 3$. (No, obično nam takvo ispisivanje nije ni potrebno).

Sljedeće pitanje, izbor predznaka koji se pridružuju pojedinim članovima, iznimno je važno jer o njemu ovise neka bitna svojstva determinante. Već ranije moglo se uočiti kako se kod rješavanja sustava linearnih jednadžbi s 2 nepoznanice metodom *suprotnih koeficijenata* pojavljuje izraz koji prepoznajemo kao determinantu reda 2 (i za koji je važno je li različit od 0 ili je jednak 0). Slično, uz više truda, mogli bismo rješavati sustav od 3 linearne jednadžbe s 3 nepoznanice tako da se kao važan izraz, zahvaljujući pogodnom izboru predznaka, pojavi determinanta reda 3.

Zasad naglasimo samo to da će se svakoj permutaciji p po određenom pravilu pridružiti njezin predznak $\operatorname{sign} p$ iz skupa $\{1, -1\}$, što znači da će izbor predznaka u članovima determinante biti diktiran stanovitim svojstvom permutacije kojom je zadan dotični član. Pokazat će se da točno polovica od $n!$ permutacija (za $n > 1$) ima predznak 1, a druga polovica -1.

Prije same definicije determinante podsjetimo se još da je *permutacija* nekog konačnog skupa po definiciji svaka bijekcija koja taj skup preslikava na samog sebe te da sve bijekcije nekog konačnog skupa čine grupu s obzirom na kompoziciju preslikavanja kao binarnu operaciju. Ta se grupa naziva *simetrična grupa stupnja* n i označava se sa S_n (vidi Odjeljak 1.1, Primjer 7). Struktura grupe S_n bit će važna za svojstva determinante. Napomenimo da je za grupu permutacija bitan broj elemenata skupa koji se permutira, a ne oznake za pojedine elemente, no ovdje je taj skup jednostavno $\{1, 2, ..., n\}$.

Općenito definiramo determinantu reda n na sljedeći način.

Definicija 4.1.1. *Neka je* $A \in M_n(\mathbb{F})$. ***Determinanta matrice*** A *je skalar iz polja* $\mathbb{F}$ *koji se definira kao*

$$\det A = \sum_{p \in S_n} (\operatorname{sign} p) a_{1p(1)} a_{2p(2)} \cdots a_{np(n)}, \tag{4.1}$$

gdje je S_n *grupa permutacija skupa* $\{1, \ldots, n\}$, *a* $\operatorname{sign} p \in \{-1, 1\}$ *predznak permutacije. Dakle, determinanta je preslikavanje*

$$\det : M_n(\mathbb{F}) \to \mathbb{F}, \ A \mapsto \det A.$$

Determinanta matrice A zapisuje se također kao kvadratna tablica poput matrice A ali je ta tablica omeđena vertikalnim crtama, a ne okruglim ili uglatim zagradama:

$$A = \begin{vmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ a_{21} & a_{22} & \ldots & a_{2n} \\ \vdots & \vdots & \cdots & \vdots \\ a_{n1} & a_{n2} & \ldots & a_{nn} \end{vmatrix}.$$

Istaknimo i razjasnimo redom sve oznake i pojmove u izrazu (4.1) za determinantu: *Permutacija* $p \in S_n$ je bijekcija na skupu $\{1, \ldots, n\}$. Označavali smo ju s

$$p = \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ p(1) & p(2) & p(3) & \cdots & p(n) \end{pmatrix}.$$

Još jednom napomenimo da je skup svih permutacija p skupa $\{1, \ldots, n\}$, S_n, (nekomutativna) grupa s obzirom na operaciju komponiranja. Budući da ova grupa broji $n!$ elemenata, suma u (4.1) se sastoji od točno $n!$ pribrojnika.

Predznak permutacije p definira se kao

$$\operatorname{sign} p = (-1)^{I(p)},$$

gdje je $I(p)$ broj inverzija permutacija p. *Inverzija permutacije* p je svaki par (i, j) takav da je $1 \leq i < j \leq n$ i $p(i) > p(j)$. Ako je broj inverzija permutacije p, $I(p)$, paran, kažemo da je p *parna* permutacija, dok je u suprotnom p *neparna* permutacija.

Navedimo neka svojstva permutacija, osobito s naglaskom na predznak permutacije.

- Za broj inverzija permutacija p vrijedi

  $$0 \leq I(p) \leq \frac{n(n-1)}{2} = \binom{n}{2}.$$

  Uočimo da identiteta

  $$\begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ 1 & 2 & 3 & \cdots & n \end{pmatrix},$$

  ima 0 inverzija, dok u permutaciji

  $$\begin{pmatrix} 1 & 2 & \cdots & n-1 & n \\ n & n-1 & \cdots & 2 & 1 \end{pmatrix},$$

  inverzija nastupa za svaki par (i, j) takav da je $1 \leq i < j \leq n$. Stoga je broj inverzija ove permutacije jednak $\frac{n(n-1)}{2} = \binom{n}{2}$.

- Može se pokazati da točno polovicu grupe S_n čine parne permutacije. Stoga u (4.1) $\frac{1}{2}n!$ članova dolazi s predznakom $+$ i isto toliko s predznakom $-$.
- Pokazuje se da je
$$\operatorname{sign}(p \circ q) = (\operatorname{sign} p)(\operatorname{sign} q).$$
Posebno, $(\operatorname{sign} p)(\operatorname{sign} p^{-1}) = \operatorname{sign}(p \circ p^{-1}) = \operatorname{sign} id = 1$, pa je $\operatorname{sign} p = \operatorname{sign} p^{-1}$.

Ova svojstva lako pamtimo i kad ih iskažemo riječima: Međusobno inverzne permutacije jednakog su predznaka to jest obje su parne ili obje neparne. Kompozicija dviju permutacija jednake parnosti (obje parne ili obje neparne) uvijek je parna permutacija dok je kompozicija parne i neparne permutacija uvijek neparna permutacija. Uočite ovdje analogiju sa svojstvom parnosti cijelih brojeva pri operaciji zbrajanja: zbroj dva parna broja je paran broj, zbroj dva neparna je paran, itd.

Dokazi prethodno navedenih svojstava povezanih s predznakom permutacije nalaze se u odjeljku 4.4. Zasad su samo iskazana bez dokaza kako bismo se njima mogli poslužiti pri dokazivanju važnih svojstava determinante.

Primjer 47. Zadana je permutacija $p \in S_6$,
$$p = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 3 & 1 & 6 & 2 & 5 \end{pmatrix}.$$
Inverzije permutacije p su
$$(1,2),\ (1,3),\ (1,5),\ (2,3),\ (2,5),\ (4,5),\ (4,6),$$
pa je $I(p) = 7$ i $\operatorname{sign} p = -1$. Dakle, p je neparna permutacija.

♡

Primjer 48. Uvjerimo se da izrazi za determinantu reda 2 i reda 3 slijede točno prema definiciji (4.1). Neka je $n = 2$. Tada je
$$S_2 = \{p_1 = \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}, p_2 = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}\}.$$
Očito je, $I(p_1) = 0$ i $I(p_2) = 1$. Za $A = [a_{ij}] \in M_2(\mathbb{F})$ prema (4.1) imamo
$$\det A = (\operatorname{sign} p_1) a_{1p_1(1)} a_{2p_1(2)} + (\operatorname{sign} p_2) a_{1p_2(1)} a_{2p_2(2)} = a_{11}a_{22} - a_{12}a_{21}.$$

Članove grupe S_3 već smo raspisali u Primjeru 7, odjeljak 1.1. No, navedimo ih još jednom,
$$\begin{aligned} S_3 = \{ \quad p_1 &= \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, p_2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, p_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \\ p_4 &= \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, p_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, p_6 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}\}. \end{aligned}$$

Vrijedi $I(p_1) = 0$, $I(p_2) = I(p_3) = 1$, $I(p_4) = I(p_5) = 2$, $I(p_6) = 3$. Stoga, za $A = [a_{ij}] \in M_3(\mathbb{F})$ dobivamo

$$\begin{aligned}\det A &= \sum_{i=1}^{6} (\operatorname{sign} p_i) a_{1p_i(1)} a_{2p_i(2)} a_{3p_i(3)} \\ &= a_{11}a_{22}a_{33} - a_{11}a_{23}a_{32} - a_{12}a_{21}a_{33} + a_{12}a_{23}a_{31} + a_{13}a_{21}a_{32} - a_{13}a_{22}a_{31}.\end{aligned}$$

♡

Propozicija 4.1.2. *Vrijedi:*

(1) *Ako matrica A ima neki redak u kojem su svi elementi jednaki nuli, onda je*

$$\det A = 0.$$

Posebno, determinanta nulmatrice je 0.

(2) *Ako je $A = [a_{ij}] \in M_n(\mathbb{F})$ gornjetrokutasta (ili donjetrokutasta) matrica, onda je*

$$\det A = a_{11}a_{22} \cdots a_{nn}.$$

Specijalno, determinanta jedinične matrice je $\det I = 1$, a determinanta skalarne matrice $A = \alpha I$, $\alpha \in \mathbb{F}$, je $\det A = \alpha^n$.

Dokaz. **(1)** Neka su svi koeficijenti i-tog retka su jednaki nuli, to jest $a_{ij} = 0$ za sve $j = 1, \ldots, n$. Uočimo da se u svakom pribrojniku sume u (4.1) nalazi točno jedan faktor iz i-tog retka, pa je

$$\det A = \sum_{p \in S_n} (\operatorname{sign} p) a_{1p(1)} a_{2p(2)} \cdots \underbrace{a_{ip(i)}}_{0} \cdots a_{np(n)} = 0.$$

(2) Pretpostavimo da je $A = [a_{ij}]$ gornjetrokutasta matrica reda n. Tada je $a_{ij} = 0$ za sve $1 \leq j < i \leq n$. Uočimo da je jedina permutacija u kojoj je $i \geq p(i)$ za sve $i = 1, \ldots, n$ identiteta. Dakle, ako je p permutacija različita od identitete, onda postoji $i \in \{2, \ldots, n\}$ takav da je $i > p(i)$, pa je u tom slučaju $a_{ip(i)} = 0$ kao i čitav pribrojnik $a_{1p(1)} \cdots a_{ip(i)} \cdots a_{np(n)} = 0$. Stoga, $\det A = a_{11}a_{22} \cdots a_{nn}$.

□

Dokaz tvrdnje (2) zapisan algebarski korisno je pratiti i promatranjem gornjetrokutaste matrice tako da se uoči način biranja jedinog člana determinante koji nije općenito jednak nuli. Iz prvog stupca moramo izabrati a_{11} jer svi ostali koeficijenti u tom stupcu su nula. Zatim, u tom članu determinante drugi stupac mora biti zastupljen koeficijentom a_{22}, jer svi ispod njega su nula, dok a_{12} ne dolazi u obzir budući da je iz prvog retka već izabran a_{11}. Analogno se zaključuje dalje, sve do koeficijenta a_{nn}.

Propozicija 4.1.3. *Transponiranjem matrice se ne mijenja determinanta, to jest*

$$\det A = \det A^t.$$

Dokaz. Neka je $A = [a_{ij}]$ matrica reda n. Tada je

$$\det A^t = \sum_{p \in S_n} (\operatorname{sign} p)[A^t]_{1p(1)}[A^t]_{2p(2)} \cdots [A^t]_{np(n)} = \sum_{p \in S_n} (\operatorname{sign} p) a_{p(1)1} a_{p(2)2} \cdots a_{p(n)n}.$$

Uočimo da je permutacija

$$\begin{pmatrix} p(1) & p(2) & \cdots & p(n) \\ 1 & 2 & \cdots & n \end{pmatrix}$$

inverzna permutacija od

$$p = \begin{pmatrix} 1 & 2 & \cdots & n \\ p(1) & p(2) & \cdots & p(n) \end{pmatrix}.$$

Dakle,

$$\det A^t = \sum_{p \in S_n} (\operatorname{sign} p) a_{1p^{-1}(1)} a_{2p^{-1}(2)} \cdots a_{np^{-1}(n)}.$$

Nadalje, uočimo da je $I(p) = I(p^{-1})$. Zaista, ako je (i, j) inverzija od p, tada je $i < j$ i $p(i) > p(j)$. Za $i' = p(j)$ i $j' = p(i)$, imamo $i' < j'$ i $p^{-1}(i') = j > i = p^{-1}(j')$. Dakle, (i', j') je pripadna inverzija od p^{-1}. Konačno, ako p 'prolazi' skupom svih permutacija S_n, onda će cijelim tim skupom 'proći' i p^{-1}, pa smo dobili

$$\det A^t = \sum_{p^{-1} \in S_n} (\operatorname{sign} p^{-1}) a_{1p^{-1}(1)} a_{2p^{-1}(2)} \cdots a_{np^{-1}(n)} = \det A.$$

□

Korolar 4.1.4. *Ako matrica A ima neki stupac u kojem su svi elementi jednaki nuli, onda je* $\det A = 0$.

4.2 Osnovna svojstva determinante. Binet-Cauchyjev teorem.

Budući da smo se uvjerili da se determinanta gornjetrokutaste matrice vrlo lako računa, prirodno je pokušati transformirati proizvoljnu matricu na takav oblik. Pritom je ključno koristiti transformacije koje ne mijenjaju determinantu ili je barem mijenjaju na način koji se jednostavno kontrolira. Pokazuje se da će za tu svrhu opet poslužiti elementarne transformacije na stupcima i redcima matrice. Prije nego što to iskažemo i dokažemo navedimo još neka svojstva permutacija koja će nam trebati.

Permutacija oblika

$$t = \begin{pmatrix} 1 & 2 & \cdots & i & \cdots & j & \cdots & n-1 & n \\ 1 & 2 & \cdots & j & \cdots & i & \cdots & n-1 & n \end{pmatrix}$$

naziva se ciklus duljine 2 ili *transpozicija*. Kraće ju ponekad označavamo s $t = (ij)$. Pokazuje se da je svaka transpozicija neparna permutacija, to jest $\operatorname{sign} t = -1$. Još vrijedi da je $t \circ t = id$, odnosno $t = t^{-1}$.

Nadalje, svaka se permutacija može napisati kao kompozicija (produkt) transpozicija. Taj rastav nije jedinstven, ali je broj transpozicija u rastavu uvijek iste parnosti.

Propozicija 4.2.1. *Neka su $A, B \in M_n(\mathbb{F})$. Ako je B dobivena iz A:*

(1) *međusobnom zamjenom dva retka (stupca), onda* $\det B = -\det A$,

(2) *množenjem skalarom $\lambda \neq 0$ nekog retka (stupca), onda* $\det B = \lambda(\det A)$,

(3) *pribrajanjem nekog retka (stupca) pomnoženog s λ nekom drugom retku (stupcu), onda* $\det B = \det A$.

Dokaz. Dokažimo tvrdnju (1). Pretpostavimo da je $B = [b_{ij}]$ dobivena iz $A = [a_{ij}]$ zamjenom k-tog i l-tog retka, $1 \leq k < l \leq n$.

$$\begin{aligned}
\det B &= \sum_{q \in S_n} (\operatorname{sign} q) b_{1q(1)} b_{2q(2)} \cdots b_{kq(k)} \cdots b_{lq(l)} \cdots b_{nq(n)} \\
&= \sum_{q \in S_n} (\operatorname{sign} q) a_{1q(1)} a_{2q(2)} \cdots a_{lq(k)} \cdots a_{kq(l)} \cdots a_{nq(n)}.
\end{aligned}$$

Neka je t transpozicija dana s

$$t = \begin{pmatrix} 1 & 2 & \cdots & l & \cdots & k & \cdots & n-1 & n \\ 1 & 2 & \cdots & k & \cdots & l & \cdots & n-1 & n \end{pmatrix}.$$

Vrijedi $q(t(l)) = q(k)$, $q(t(k)) = q(l)$ i $q(t(i)) = q(i)$, za sve $i \neq k, l$. Stoga je

$$\det B = \sum_{q \in S_n} (\operatorname{sign} q) a_{1(q \circ t)(1)} a_{2(q \circ t)(2)} \cdots a_{l(q \circ t)(l)} \cdots a_{k(q \circ t)(k)} \cdots a_{n(q \circ t)(n)}.$$

Stavimo $p = q \circ t$, pa je $q = p \circ t$ jer je $t \circ t = id$. Kako je $\operatorname{sign}(p \circ t) = (\operatorname{sign} p)(\operatorname{sign} t) = -\operatorname{sign} p$, dobivamo

$$\begin{aligned}
\det B &= \sum_{p \circ t \in S_n} (-\operatorname{sign} p) a_{1p(1)} a_{2p(2)} \cdots a_{lp(l)} \cdots a_{kp(k)} \cdots a_{np(n)} \\
&= -\sum_{p \in S_n} (\operatorname{sign} p) a_{1p(1)} a_{2p(2)} \cdots a_{lp(l)} \cdots a_{kp(k)} \cdots a_{np(n)} = -\det A,
\end{aligned}$$

pri čemu su sume (po p i $p \circ t$) jednake jer je preslikavanje $p \mapsto p \circ t$ je bijekcija skupa S_n. Tvrdnja za stupce vrijedi jer je $\det A = \det A^t$ prema Propoziciji 4.1.3. □

Prije nego što nastavimo dokaz tvrdnji (2) i (3) prethodne propozicije, iskažimo korisnu posljedicu tvrdnje (1).

Korolar 4.2.2. *Ako su u matrici A dva retka (stupca) jednaka, onda* $\det A = 0$.

Dokaz. Pretpostavimo da A ima isti i-ti i j-ti redak. Ako napravimo transformaciju zamjene i-tog i j-tog retka, ponovo ćemo dobiti matricu A, a prema Propoziciji 4.2.1 (1) je $\det A = -\det A$. Dakle, $\det A = 0$. □

Nastavimo s dokazom Propozicije 4.2.1.

Dokaz. Pretpostavimo da je $B = [b_{ij}]$ dobivena iz $A = [a_{ij}]$ množenjem skalarom $\lambda \neq 0$ i-tog retka. Vrijedi

$$\begin{aligned}
\det B &= \sum_{p\in S_n} (\operatorname{sign} p)\, \underbrace{b_{1p(1)}}_{a_{1p(1)}} \underbrace{b_{2q(2)}}_{a_{2p(2)}} \cdots \underbrace{b_{ip(i)}}_{\lambda a_{ip(i)}} \cdots \underbrace{b_{np(n)}}_{a_{np(n)}} \\
&= \sum_{p\in S_n} (\operatorname{sign} p) a_{1p(1)} a_{2p(2)} \cdots (\lambda a_{ip(i)}) \cdots a_{np(n)} \\
&= \lambda \sum_{p\in S_n} (\operatorname{sign} p) a_{1p(1)} a_{2p(2)} \cdots a_{ip(i)} \cdots a_{np(n)} = \lambda \det A.
\end{aligned}$$

Sada, neka je $B = [b_{ij}]$ dobivena iz $A = [a_{ij}]$ pribrajanjem i-tog retka pomnoženog s λ j-tom retku. Uz pretpostavku $i < j$ dobivamo

$$\begin{aligned}
\det B &= \sum_{p\in S_n} (\operatorname{sign} p)\, \underbrace{b_{1p(1)}}_{a_{1p(1)}} \underbrace{b_{2q(2)}}_{a_{2p(2)}} \cdots \underbrace{b_{ip(i)}}_{a_{ip(i)}} \cdots \underbrace{b_{jp(j)}}_{a_{jp(j)}+\lambda a_{ip(i)}} \cdots \underbrace{b_{np(n)}}_{a_{np(n)}} \\
&= \sum_{p\in S_n} (\operatorname{sign} p) a_{1p(1)} a_{2p(2)} \cdots a_{ip(i)} \cdots (a_{jp(j)} + \lambda a_{ip(i)}) \cdots a_{np(n)} \\
&= \underbrace{\sum_{p\in S_n} (\operatorname{sign} p) a_{1p(1)} a_{2p(2)} \cdots a_{ip(i)} \cdots a_{jp(j)} \cdots a_{np(n)}}_{\det A} + \\
&+ \underbrace{\lambda \sum_{p\in S_n} (\operatorname{sign} p) a_{1p(1)} a_{2p(2)} \cdots a_{ip(i)} \cdots a_{ip(i)} \cdots a_{np(n)}}_{0} \\
&= \det A.
\end{aligned}$$

Zaista, druga suma predstavlja determinantu matrice kojoj su i-ti i j-ti redak jednaki, $(a_{i1}, \ldots, a_{in})$, pa prema je Korolaru 4.2.2 vrijednost determinante takve matrice jednaka nuli.

Za stupce vrijede analogne tvrdnje jer $\det A = \det A^t$. □

Sljedeći primjer dajemo zbog boljeg razumijevanja dokaza Propozicije 4.2.1 (1).

Primjer 49. Pretpostavimo da su A i B matrice reda 4, te da je $B = [b_{ij}]$ dobivena iz $A = [a_{ij}]$ zamjenom 2. i 3. retka. Nadalje, promotrimo što se događa sa članom sume koji odgovara permutaciji

$$p = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}.$$

Vrijedi

$$\det A = \begin{vmatrix} a_{11} & \boxed{a_{12}} & a_{13} & a_{14} \\ a_{21} & a_{22} & \boxed{a_{23}} & a_{24} \\ a_{31} & a_{32} & a_{33} & \boxed{a_{34}} \\ \boxed{a_{41}} & a_{42} & a_{43} & b_{44} \end{vmatrix} = \cdots \quad \underbrace{-a_{12}a_{23}a_{34}a_{41}}_{(\operatorname{sign} p) a_{1p(1)} a_{2p(2)} a_{3p(3)} a_{4p(4)}} \quad + \cdots .$$

$$\det B = \begin{vmatrix} a_{11} & \boxed{a_{12}} & a_{13} & a_{14} \\ a_{31} & a_{32} & \boxed{a_{33}} & a_{34} \\ a_{21} & a_{22} & a_{23} & \boxed{a_{24}} \\ \boxed{a_{41}} & a_{42} & a_{43} & a_{44} \end{vmatrix} = \cdots \quad \underbrace{+a_{12}a_{33}a_{24}a_{41}}_{(\operatorname{sign} q)a_{1q(1)}a_{2q(2)}a_{3q(3)}a_{4q(4)}} \quad + \cdots ,$$

gdje je

$$p \circ t = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 2 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix} = q.$$

♡

Dakle, za zaključiti je da se primjenom elementarnih transformacija nad redcima ili stupcima matrice, determinanta može promijeniti, ali na točno određeni način. Nadalje, ako je $A \sim B$, to jest ako je B dobivena provođenjem konačno mnogo elementarnih transformacija matrice A, onda postoji $\alpha \in \mathbb{F}$ i $\alpha \neq 0$ takav da je $\det B = \alpha \det A$. Naime, tvrdnje iz prethodne propozicije mogu se izraziti i tako da se primjenom pojedinih transformacija na matricu A vrijednost njezine determinante pomnoži s -1, odnosno s $\lambda \neq 0$ ili da se pomnoži s 1 kad se ne promijeni. Stoga se u svakom slučaju determinanta množi skalarom različitim od nule, a uzastopna primjena nekoliko transformacija rezultira množenjem determinante umnoškom svih tih skalara što je ponovno skalar različit od nule. Odatle je jasno da ekvivalentne matrice ili obje imaju determinantu jednaku nuli ili obje imaju determinantu različitu od nule.

Propozicija 4.2.3. *Matrica A je regularna ako i samo ako je* $\det A \neq 0$.

Dokaz. Matrica A je regularna ako i samo ako je $r(A) = n$, odnosno ako i samo ako je $A \sim I$. Kako je $\det I = 1$, slijedi da je $\det A \neq 0$.

Ako pretpostavimo da A nije regularna, onda je $r(A) = r < n$ i $A \sim D_r$ gdje je D_r kanonska matrica ranga r i reda n, pa slijedi da $\det A = 0$ jer $\det D_r = 0$. □

Tvrdnju ove propozicije možemo objediniti s otprije poznatim svojstvom kvadratne matrice da je regularna ako i samo ako je punog ranga. Tako dobivamo tri ekvivalentna svojstva budući da je regularnost (invertibilnost) karakterizirana i pomoću ranga i pomoću determinante.

Teorem 4.2.4. *Neka je $A \in M_n(\mathbb{F})$. Sljedeće tvrdnje su ekvivalentne:*

(1) *A je regularna,*

(2) $r(A) = n$,

(3) $\det A \neq 0$.

Napomenimo da iz $\det A \neq 0$ zaključujemo da je $r(A) = n$. Ali, ako $\det A = 0$, onda ne znamo točnu vrijednost ranga nego samo da je $r(A) < n$.

Primjer 50. U ovisnosti o parametru $t \in \mathbb{R}$ treba odrediti rang matrice

$$A = \begin{pmatrix} 3 & -2 & t-2 & 1 \\ 3 & -2 & -4 & 1 \\ -1 & 0 & 2 & -2 \\ t+1 & 0 & 2 & -2 \end{pmatrix}.$$

Kako je $\det A = 4(t+2)^2$, prema Teoremu 4.2.4 slijedi da je $r(A) = 4$ za $t \neq -2$. Za $t = -2$ znamo da je $r(A) \leq 3$, no točnu vrijednost ranga možemo dobiti primjenom elementarnih transformacija. Lako se može ustanoviti da je

$$A = \begin{pmatrix} 3 & -2 & -4 & 1 \\ 3 & -2 & -4 & 1 \\ -1 & 0 & 2 & -2 \\ -1 & 0 & 2 & -2 \end{pmatrix} \sim D_2,$$

odnosno da je $r(A) = 2$ za $t = -2$.

$\heartsuit$

Teorem 4.2.5 (Binet-Cauchy)**.** *Neka su* $A, B \in M_n(\mathbb{F})$*. Tada je*

$$\det(AB) = \det A \cdot \det B.$$

Dokaz. Tvrdnja očito vrijedi za dijagonalne matrice. Dokaz provodimo u više slučajeva. Najprije, ustanovimo koje su vrijednosti determinanti elementarnih matrica. Prema Propoziciji 4.2.1 slijedi:

- $\det E_1 = -1$, gdje je E_1 elementarna matrica koja odgovara elementarnoj transformaciji 1. vrste (zamjeni dva retka ili stupca jedinične matrice),
- $\det E_2 = \lambda$, gdje je E_2 elementarna matrica koja odgovara elementarnoj transformaciji 2. vrste (množenju nekog retka ili stupca skalarom $\lambda \neq 0$ jedinične matrice),
- $\det E_3 = 1$, gdje je E_3 elementarna matrica koja odgovara elementarnoj transformaciji 3. vrste (pribrajanju nekog retka ili stupca skalarom pomnoženim $\lambda \neq 0$ nekom drugom retku ili stupcu jedinične matrice).

1. slučaj. Pretpostavimo da je B elementarna matrica, tada je

- $\det(AE_1) = \{\text{Prop.4.2.1 (1)}\} = -\det A = (\det A)(\det E_1)$,
- $\det(AE_2) = \{\text{Prop.4.2.1 (2)}\} = \lambda \det A = (\det A)(\det E_2)$,
- $\det(AE_3) = \{\text{Prop.4.2.1 (3)}\} = \det A = (\det A)(\det E_3)$.

2. slučaj. Pretpostavimo da je B regularna matrica, tada se B može prikazati kao umnožak elementarnih matrica (Korolar 2.6.2). Znači,

$$B = F_1 F_2 \cdots F_k.$$

Uzastopnom primjenom rezultata iz 1. slučaja dobivamo

$$\det B = \det F_1 \det F_2 \cdots \det F_k.$$

Tada je

$$\begin{aligned} \det(AB) &= \det(AF_1F_2\cdots F_k) = \{\text{1. slučaj}\} = \det(AF_1F_2\cdots F_{k-1}) \det F_k = \cdots \\ &= \det A \underbrace{\det F_1 \det F_2 \cdots \det F_k}_{\det B} = \det A \det B. \end{aligned}$$

3. slučaj. Pretpostavimo da B nije regularna matrica, tada je $\det B = 0$. Tada ni umnožak AB nije regularna matrica jer je $r(AB) \leq \min\{r(A), r(B)\} < n$ (Propozicija 2.5.12). Stoga je $\det(AB) = 0$ i $\det(AB) = \det A \cdot 0 = \det A \det B$. $\square$

Primjer 51. Ako je kvadratna matrica A regularna tada je

$$\det A^{-1} = (\det A)^{-1}.$$

Tvrdnja slijedi iz $\det(AA^{-1}) = \det I = 1$ primjenom Binet-Cauchyjevog teorema.

♡

Zadatak 15. *(a) Neka je $S = \{A \in M_n(\mathbb{F}) : \det A = 1\}$. Tada je S grupa s obzirom na množenje matrica.*

(Ta grupa sadržana je kao podgrupa u općoj linearnoj grupi $GL(n, \mathbb{F})$, naziva se specijalna linearna grupa *te se označava $SL(n, \mathbb{F})$).*

(b) Neka je $T = \{A \in M_n(\mathbb{R}) : \det A > 0\}$. Tada je T grupa s obzirom na množenje matrica.

4.3 Laplaceov razvoj. Inverzna matrica. Cramerov sustav.

U naslovu ovog odjeljka navedeno je nekoliko pojmova, među kojima nam je pojam inverzne matrice dobro poznat otprije. Ovdje se inverzna matrica ističe zato što ćemo doći do eksplicitne formule za njezino izračunavanje, a ta formula bit će izvedena kao jedna od posljedica tzv. Laplaceovog razvoja determinante, u kojem se vrijednost determinante izražava pomoću determinanti nižeg reda. Nadalje, formula za inverznu matricu omogućit će nam da jedinstveno rješenje Cramerovog sustava, a to je sustav linearnih jednadžbi kojem je matrica kvadratna i regularna, također izrazimo eksplicitnim formulama, pomoću stanovitih determinanti.

Kao i dosad, neka je $A = [a_{ij}]$ kvadratna matrica reda n. Znamo da je njezina determinanta definirana kao suma $n!$ pribrojnika, članova determinante. Grupirat ćemo sada tih $n!$ članova na poseban način, tako da izaberemo neki određeni redak ili stupac matrice pa svaki koeficijent iz odabranog retka (stupca) izlučimo iz svih članova u kojima se on pojavljuje. Recimo da smo se odlučili za grupiranje po koeficijentima iz i-tog retka. Koeficijent a_{ij} pojavljuje se u svakom članu determinante koji je zadan permutacijom takvom da se i preslikava u j (u zapisu $\det A$ to znači da $p(i) = j$). Po definiciji determinante znamo da se u svakom članu javlja točno jedan faktor oblika a_{ij}, za neki $j \in \{1, 2, \ldots, n\}$. Koliko ima takvih članova za odabrani i, uz varijabilni j? Ima ih točno koliko i permutacija p takvih da je $p(i) = j$, što znači $(n-1)!$ permutacija, jer $n-1$ elemenata različitih od i može se upravo na toliko načina bijektivno preslikati u $n-1$ elemenata različitih od j.

Zbroj svih članova koji kao faktor sadrže a_{ij} možemo sad napisati u obliku $a_{ij}A_{ij}$, pri čemu je A_{ij} samo kratka oznaka za zbroj odgovarajućih $(n-1)!$ monoma, dobivenih izlučivanjem a_{ij} iz članova determinante. A_{ij} se naziva *algebarskim komplementom* ili *kofaktorom* koeficijenta a_{ij} determinante. (Izraz kofaktor naznačuje jednostavno faktor kojim je pomnožen a_{ij} unutar cjelokupne sume koja čini $\det A$, a malo kasnije pokazat će se pravilnost u njegovoj strukturi, to jest da je i to zapravo jedna determinanta, samo reda nižeg za 1).

Možemo pisati

$$\det A = \sum_{j=1}^{n} a_{ij}A_{ij} = \sum_{i=1}^{n} a_{ij}A_{ij},$$

jer sve vrijedi analogno za izbor i-tog retka ili j-tog stupca kao istaknutog na početku. Kao primjer za lakše razumijevanje postupka izračunavanja determinante koji upravo provodimo možete riješiti sljedeći zadatak.

Zadatak 16. *Ispišite algebarski komplement A_{31} za determinantu matrice A reda 4. Uvjerite se da je dobiveni izraz jednak determinanti reda 3, koja se dobiva tako da se iz matrice A uklone treći redak i prvi stupac pa se izrazi determinanta preostale matrice reda 3.*

Determinanta matrice koja se dobiva uklanjanjem nekog retka i nekog stupca zadane matrice ima ključnu ulogu za izračunavanje algebarskog komplementa pa stoga i za "razvoj" determinante reda n pomoću determinanti reda $n-1$.

Definicija 4.3.1. *Neka je $A = [a_{ij}] \in M_n(\mathbb{F})$. Determinanta matrice koja nastaje uklanjanjem i-tog retka i j-tog stupca matrice A naziva se* ***minora*** *reda $n-1$ i označava s Δ_{ij}.*

Algebarski komplement A_{ij} i minora Δ_{ij} usko su povezani, a u formuli koja izražava tu vezu važan je predznak, određen pozicijom (i, j) s obzirom na koju se uzima algebarski komplement.

Propozicija 4.3.2. *Neka je $A = [a_{ij}] \in M_n(\mathbb{F})$. Tada za sve $i, j = 1, 2, \ldots, n$ vrijedi*

$$A_{ij} = (-1)^{i+j}\Delta_{ij}.$$

Dokaz. Tvrdi se, dakle, da je algebarski komplement ili jednak odgovarajućoj minori ili suprotnoj vrijednosti te minore, ovisno o tome je li zbroj $i + j$ paran ili neparan broj.

Propoziciju ćemo dokazati tako da formulu najprije provjerimo za posebni slučaj A_{nn} kad ona vrijedi gotovo očito, a zatim opći slučaj svedemo na taj posebni primjenom otprije poznatih svojstava determinante. Uzimamo, dakle, poziciju (n, n) u determinanti, što za A_{nn} znači sve članove određene permutacijama za koje je $p(n) = n$. Eksplicitno,

$$A_{nn} = \sum_{p \in S_n, p(n)=n} (\operatorname{sign} p) a_{1p(1)} a_{2p(2)} \cdots a_{n-1,p(n-1)}.$$

Naime, predznak permutacije p za koju $p(n) = n$ jednak je predznaku njezine restrikcije na podskup $\{1, 2, \ldots, n\}$, budući da na parovima oblika (i, n) nema inverzije. Stoga je doista

$$A_{nn} = \Delta_{nn} = (-1)^{n+n}\Delta_{nn}.$$

Sad uzmimo opću poziciju (i, j) u determinanti. Koeficijent a_{ij} "preselimo" na poziciju (n, n) tako da i-ti redak dovedemo u položaj n-tog retka pomoću $n-i$ uzastopnih zamjena sa sljedećim retkom, a zatim j-ti stupac dovedemo u položaj n-tog stupca, analogno, pomoću $n - j$ zamjena sa sljedećim stupcem. Znamo da je vrijednost ovako dobivene determinante jednaka

$$(-1)^{(n-i)+(n-j)} \det A = (-1)^{i+j} \det A.$$

U toj determinanti algebarski komplement koeficijenta na poziciji (n, n) upravo je jednak minori Δ_{ij}. Naime, u postupku zamjene uzastopnih redaka i stupaca početne determinante nije se poremetio međusobni položaj redaka s izuzetkom i-tog, kao ni međusobni položaj stupaca s izuzetkom j-tog stupca. U "novoj" determinanti, prema dokazanom, algebarski komplement koeficijenta a_{ij}, koji se sad nalazi na poziciji (n, n), stoga je jednak determinanti dobivenoj uklanjanjem i-tog retka i j-tog stupca iz $\det A$, a to je Δ_{ij}.

Usporedbom $\det A$ i nove determinante, koja iznosi $(-1)^{i+j} \det A$ vidimo da vrijedi

$$(-1)^{i+j} a_{ij} A_{ij} = a_{ij} \Delta_{ij},$$

pa je $A_{ij} = (-1)^{i+j} \Delta_{ij}$.

Primijetimo da vrijednost A_{ij} ne ovisi o vrijednosti koeficijenta upisanog na poziciji (i, j), nego o koeficijentima iz svih redaka osim i-tog i svih stupaca osim j-tog stupca. Nadalje, kao posebni slučaj prvo smo mogli uzeti A_{11} pa onda premjestiti a_{ij} na položaj $(1, 1)$, no tada bismo promatrali restrikciju permutacije na podskup $\{2, \ldots, n-1\}$. $\square$

Teorem 4.3.3 (Laplaceov razvoj)**.** *Neka je $A = [a_{ij}] \in M_n(\mathbb{F})$. Tada za sve $i, j = 1, 2, \ldots, n$ vrijedi*

$$\det A = \sum_{j=1}^{n} (-1)^{i+j} a_{ij} \Delta_{ij} \tag{4.2}$$

i

$$\det A = \sum_{i=1}^{n} (-1)^{i+j} a_{ij} \Delta_{ij}. \tag{4.3}$$

Formula (4.2) naziva se *Laplaceov razvoj po i-tom retku* determinante. Analogno, (4.3) je *Laplaceov razvoj po j-tom stupcu.*

Definicija 4.3.4. *Neka je $A = [a_{ij}] \in M_n(\mathbb{F})$.* ***Adjunkta matrice*** *A je matrica $\widetilde{A} = [A_{ji}] \in M_n(\mathbb{F})$, to jest transponirana matrica algebarskih komplemenata matrice A*

Teorem 4.3.5. *Za svaku matricu $A \in M_n(\mathbb{F})$ vrijedi*

$$A \cdot \widetilde{A} = \widetilde{A} \cdot A = (\det A) I.$$

Dokaz. Neka je $i \neq j$. Tada

$$[A \cdot \widetilde{A}]_{ij} = \sum_{k=1}^{n} [A]_{ik} [\widetilde{A}]_{kj} = \sum_{k=1}^{n} a_{ik} A_{jk}.$$

Prema (4.2) prethodna suma je upravo jednaka vrijednosti sljedeće determinante

$$\begin{array}{l} \begin{vmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \cdots & \vdots \\ a_{i1} & \cdots & a_{in} \\ \vdots & \cdots & \vdots \\ a_{i1} & \cdots & a_{in} \\ \vdots & \cdots & \vdots \\ a_{n1} & \cdots & a_{nn} \end{vmatrix} \begin{array}{l} \\ \\ \rightsquigarrow j\text{-ti redak} \\ \\ \rightsquigarrow i\text{-ti redak} \\ \\ \\ \end{array} \end{array},$$

odnosno determinante kojoj su i-ti i j-ti redak jednaki, pa je prema Korolaru 4.2.2 njena vrijednost jednaka 0.

Nadalje,

$$[A \cdot \widetilde{A}]_{ii} = \sum_{k=1}^{n} [A]_{ik} [\widetilde{A}]_{ki} = \sum_{k=1}^{n} a_{ik} A_{ik} = \det A,$$

prema (4.2), pa smo pokazali da je $A \cdot \widetilde{A} = (\det A) I$.

Analogno se pokazuje $\widetilde{A} \cdot A = (\det A) I$. □

Korolar 4.3.6. *Ako je* $\det A \neq 0$, *onda*

$$A^{-1} = \frac{1}{\det A} \widetilde{A}.$$

Primjer 52. Odredit ćemo sve vrijednosti parametra $t \in \mathbb{R}$ za koje je matrica

$$A = \begin{pmatrix} t+3 & -2 & -2 \\ 1 & t-1 & 0 \\ 1 & t & 1 \end{pmatrix}$$

invertibilna, te inverz odrediti pomoću adjunkte. Budući da je $\det A = (t-1)(t+3)$, iz Teorema 4.2.4 slijedi da je A invertibilna ako i samo ako je $t \in \mathbb{R} \backslash \{-3, 1\}$, te

$$A^{-1} = \frac{1}{\det A} \widetilde{A} = \frac{1}{(t-1)(t+3)} \begin{pmatrix} t-1 & -2(t-1) & 2(t-1) \\ -1 & t+5 & -2 \\ 1 & -(t+1)(t+2) & t^2+2t-1 \end{pmatrix}.$$

♡

Definicija 4.3.7. *Sustav* $AX = B$ *je* ***Cramerov sustav*** *ako je* A *kvadratna matrica punog ranga.*

Cramerov sustav $AX = B$ ima isti broj jednadžbi i nepoznanica. Matrica sustava A je ranga n što je ekvivalentno s činjenicom da je A regularna. Znači, Cramerov sustav ima jedinstveno rješenje $(\gamma_1, \ldots, \gamma_n)$. Nadalje,

$$X = A^{-1} B,$$

pa prema Korolaru 4.3.6 slijedi

$$X = \frac{1}{\det A} \widetilde{A} B.$$

Raspisivanjem elemenata umnoška $\widetilde{A}B$ dobivamo

$$[\widetilde{A}B]_i = \sum_{j=1}^{n} [\widetilde{A}]_{ij} b_j = \sum_{j=1}^{n} [A]_{ji} b_j = \sum_{j=1}^{n} b_j [A]_{ji}, \ 1 \leq i \leq n,$$

a to je upravo Laplaceov razvoj po i-tom stupcu sljedeće determinante

$$D_i = \begin{vmatrix} a_{11} & \cdots & a_{1,i-1} & b_1 & a_{1,i+1} & \cdots & a_{1n} \\ a_{21} & \cdots & a_{2,i-1} & b_2 & a_{2,i+1} & \cdots & a_{2n} \\ \vdots & \cdots & \vdots & \vdots & \vdots & \cdots & \vdots \\ a_{n1} & \cdots & a_{n,i-1} & b_n & a_{n,i+1} & \cdots & a_{nn} \end{vmatrix}, \tag{4.4}$$

to jest determinante matrice koju smo dobili zamjenom i-tog stupca matrice A stupcem slobodnih koeficijenata $B = \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix}$. Uobičajeno je komponente rješenja Cramerovog sustava zapisati formulama

$$\gamma_i = \frac{D_i}{D}, \ i = 1, \ldots, n, \tag{4.5}$$

gdje je $D = \det A$, a D_i su dani s (4.4).

Napomena 4.3.8. *U zapisu (4.5), komponenti rješenja Cramerovog sustava, prepoznajemo formule za komponente rješenja sustava danog dvjema jednadžbama s 2 nepoznanice*

$$a_1x + b_1y = c_1,$$

$$a_2x + b_2y = c_2,$$

a to su

$$x = \frac{\begin{vmatrix} c_1 & b_1 \\ c_2 & b_2 \end{vmatrix}}{\begin{vmatrix} a_1 & b_1 \\ a_2 & b_2 \end{vmatrix}} = \frac{c_1b_2 - b_1c_2}{a_1b_2 - a_2b_1},$$

$$y = \frac{\begin{vmatrix} a_1 & c_1 \\ a_2 & c_2 \end{vmatrix}}{\begin{vmatrix} a_1 & b_1 \\ a_2 & b_2 \end{vmatrix}} = \frac{a_1c_2 - a_2c_1}{a_1b_2 - a_2b_1}.$$

Primjer 53. Riješit ćemo Primjer 46 (u kojem je trebalo riješiti sustav u ovisnosti o parametru) na drugi način - korištenjem determinante i Cramerovog pravila. Kako je $\det A = -(t-3)t$, gdje je A matrica sustava, slijedi da sustav ima jedinstveno rješenje ako i samo ako je $t \neq 0, 3$. Primjenom Cramerove metode dobivamo:

$$x_1 = \frac{\begin{vmatrix} 2 & t & -1 \\ 1 & 1 & 0 \\ 3-t & -2 & t-1 \end{vmatrix}}{(3-t)t} = \frac{(t-3)(1+t)}{(3-t)t} = -\frac{1+t}{t},$$

$$x_2 = \frac{\begin{vmatrix} 2 & 2 & -1 \\ 1 & 1 & 0 \\ 0 & 3-t & t-1 \end{vmatrix}}{(3-t)t} = \frac{t-3}{(3-t)t} = -\frac{1}{t},$$

$$x_3 = \frac{\begin{vmatrix} 2 & t & 2 \\ 1 & 1 & 1 \\ 0 & -2 & 3-t \end{vmatrix}}{(3-t)t} = \frac{(t-3)(t-2)}{(3-t)t} = \frac{2-t}{t}.$$

Za $t = 0$ i $t = 3$ rješavamo sustave Gaussovom metodom:

$$A_p(t=0) = \left(\begin{array}{ccc|c} 2 & 0 & -1 & 2 \\ 1 & 1 & 0 & 1 \\ 0 & -2 & -1 & 3 \end{array}\right) \sim \cdots \sim \left(\begin{array}{ccc|c} 2 & 0 & -1 & 2 \\ 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 3 \end{array}\right),$$

$$A_p(t=3) = \left(\begin{array}{ccc|c} 2 & 3 & -1 & 2 \\ 1 & \boxed{1} & 0 & 1 \\ 0 & -2 & 2 & 0 \end{array}\right) \sim \cdots \sim \left(\begin{array}{ccc|c} 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{array}\right),$$

iz čega slijedi da za $t = 0$ sustav nema rješenja, a za $t = 3$ ima jednoparametarsko rješenje $(0, 1, 1) + \lambda(1, -1, -1)$, $\lambda \in \mathbb{R}$.

♡

4.4 Dodatak - svojstva permutacija i simetrične grupe

Radi upotpunjavanja poglavlja o determinantama navodimo još neke tvrdnje i njihove dokaze koje se odnose na permutacije, a važne su za svojstva determinante. Dokazi će biti raspisani u mjeri dostatnoj za razumijevanje bitnih činjenica.

(1) *Svaka transpozicija je neparna permutacija.*

Ovo svojstvo lako je uočljivo ako transpozicija međusobno preslikava dva susjedna elementa, jer tada ima samo jednu inverziju. Općenito, neka je $1 \leq i < j \leq n$, a t transpozicija zadana s $(i\ j)$. Prebrojimo inverzije u ovoj permutaciji. Lako razabiremo da inverzije nastupaju samo na parovima oblika (i, k) i (k, j), pri čemu je $i < k < j$ te, dakako, na paru (i, j). Tih parova ima $2(j-i-1)+1 = 2(j-i)-1$, dakle neparan broj.

(2) *Svaka permutacija može se napisati kao kompozicija nekih transpozicija.*

Najprije ukratko razmotrimo rastav permutacije u cikluse, dakle permutacije oblika $(a_1\ a_2\ \cdots\ a_n)$, pri čemu ovaj zapis znači da se svaki element preslikava u sljedeći (zapisan s njegove desne strane), a posljednji, a_n , preslikava se u a_1. Npr. $(1\ 2\ 3\ 4)$, $(2\ 4\ 1\ 3)$ i $(1\ 4\ 3\ 2)$ su ciklusi duljine 4, zapisi $(1\ 2\ 3\ 4)$ i $(3\ 4\ 1\ 2)$ označavaju istu permutaciju (izbor početnog elementa nije bitan, čita se ciklički), a ciklusi $(1\ 2\ 3\ 4)$ i $(1\ 4\ 3\ 2)$ predstavljaju uzajamno inverzne permutacije. Već prije je spomenuto kako je svaka transpozicija ciklus duljine 2.

Neku permutaciju p skupa $\{1, 2, \ldots, n\}$ možemo napisati kao kompoziciju (disjunktnih) ciklusa tako da krenemo npr. od 1 pa sastavimo ciklus $(1\ p(1)\ p(p(1))\ \ldots)$ koji će završiti elementom x takvim da je $p(x) = 1$. Da takav element postoji vidi se zbog konačnosti skupa na kojem djeluje permutacija, jer uzastopnom primjenom p možemo dobiti najviše n različitih elemenata. Ako se svih n elemenata skupa našlo u tom prvom ciklusu, prikaz je završen. Ako pak postoji neki $y \in \{1, 2, \ldots, n\}$ koji nije obuhvaćen tim ciklusom, formiramo sljedeći ciklus kao $(y\ p(y)\ \ldots)$ itd. Na taj način "iscrpit" ćemo čitav skup $\{1, 2, \ldots, n\}$, a ako postoje takvi elementi koje p preslikava same u sebe (čvrsti ili fiksni elementi), onda svaki od takvih čini ciklus duljine 1 koji se, dogovorno, niti ne navodi u prikazu. Uočimo još da disjunktni ciklusi komutiraju pri kompoziciji. Npr. permutacija p koja elemente $1, 2, \ldots, 9$ preslikava redom u $7, 6, 4, 3, 5, 8, 9, 1, 2$ može se zapisati kao $p = (1\ 7\ 9\ 2\ 6\ 8) \circ (3\ 4)$, a za 5 se onda podrazumijeva da je fiksni za p.

Pogledajmo najprije na primjeru ciklusa $(1\ 7\ 9\ 2\ 6\ 8)$ kako se ta permutacija može napisati kao kompozicija ciklusa duljine 2, to jest transpozicija. Lako se provjeri da vrijedi

$$(1\ 7\ 9\ 2\ 6\ 8) = (1\ 8) \circ (1\ 6) \circ (1\ 2) \circ (1\ 9) \circ (1\ 7),$$

pri čemu transpozicije na desnoj strani jednakosti primjenjujemo zdesna nalijevo, kako je i uobičajeno za operaciju kompozicije preslikavanja. (Primjenom transpozicija slijeva nadesno dobivamo inverznu permutaciju $(1\ 8\ 6\ 2\ 9\ 7\ 1)$). Radi jednostavnosti zapisa, znak $\circ$ kod kompozicije ciklusa redovito se izostavlja.

Općenito, možemo uzeti element x iz promatranog ciklusa te odabrati transpozicije $(x\ p(x))$, $(x\ p^2(x))$, $(x\ p^3(x))$, ...,$(x\ p^{k-1}(x))$ za ciklus duljine k pa će vrijediti

$$(x\ p(x)\ p^2(x) \ldots p^{k-1}(x)) = (x\ p^{k-1}(x)) \cdots (x\ p^2(x))(x\ p(x)).$$

Analogno postupimo za svaki pojedini ciklus, a kompoziciju ciklusa možemo onda napisati u bilo kojem redoslijedu, jer disjunktni ciklusi komutiraju pri kompoziciji. Vidimo da je na ovaj način ciklus duljine k prikazan kao kompozicija $k-1$ transpozicije. Dolazimo sad do bitnog svojstva, kako se predznak permutacija ponaša kod kompozicije.

(3) *Za svake dvije permutacije p i q vrijedi:*

$$\operatorname{sign}(p \circ q) = \operatorname{sign} p \cdot \operatorname{sign} q.$$

Za dokaz ovog svojstva iskoristit ćemo jednu eksplicitnu formulu za predznak permutacije.

Svakom paru (i, j), $1 \leq i < j \leq n$, pridružimo razlomak $\dfrac{p(j) - p(i)}{j - i}$. Ako permutacija p ima inverziju na paru (i, j), vrijednost razlomka je negativan broj, a ako nema inverziju, taj broj je pozitivan. Ključno je sada uočiti da je $\operatorname{sign} p$ jednak umnošku svih takvih razlomaka, kad se oni pomnože za svih $n(n-1)/2$ parova (i, j), $1 \leq i < j \leq n$:

$$\operatorname{sign} p = \prod_{(i,j), 1 \leq i < j \leq n} \frac{p(j) - p(i)}{j - i}.$$

Naime, za svaki par (i, j) u brojniku točno jednog razlomka pojavi se ili $j - i$ ili $i - j = (-1)(j - i)$, budući da je p bijekcija. Predznak -1 pojavljuje se u brojnicima ukupno onoliko puta koliko p ima inverzija, dakle $I(p)$ puta, a $(-1)^{I(p)} = \operatorname{sign} p$. Svaki od faktora $j - i$ pojavi se točno jedanput u brojniku nekog razlomka i jedanput u nazivniku nekog razlomka. Množenjem svih razlomaka ovi faktori se pokrate pa je produkt na kraju jednak $\operatorname{sign} p$. Kad smo na ovakav način izrazili predznak permutacije, možemo to primijeniti na izračunavanje predznaka kompozicije dviju permutacija,

$$\operatorname{sign}(p \circ q) = \prod \frac{(p \circ q)(j) - (p \circ q)(i)}{j - i}.$$

Produkt na desnoj strani pomnožit ćemo umnoškom $\prod \frac{q(j)-q(i)}{q(j)-q(i)}$, koji je očito jednak 1 pa se vrijednost desne strane time ne mijenja, ali ćemo je napisati kao umnožak

$$\prod \frac{(p \circ q)(j)-(p \circ q)(i)}{q(j)-q(i)} \prod \frac{q(j)-q(i)}{j-i}.$$

Drugi faktor sad je očito jednak $\operatorname{sign} q$, a u prvom možemo prepoznati vrijednost $\operatorname{sign} p$. Naime,

$$\prod \frac{(p \circ q)(j)-(p \circ q)(i)}{q(j)-q(i)} = \prod \frac{p(q(j))-p(q(i))}{q(j)-q(i)},$$

a kako je q permutacija, parovi $\{q(i), q(j)\}$ predstavljaju svih $n(n-1)/2$ različitih parova elemenata skupa $\{1, 2, \ldots, n\}$. Pojedini razlomak u produktu opet ima negativnu ili pozitivnu vrijednost u skladu s tim ima li p ili nema inverziju na paru $(q(i), q(j))$. (Primijetimo da ovdje nije bitno je li $q(i) < q(j)$ ili $q(i) > q(j)$). Time je dokazana tvrdnja (3).

Vratimo se na svojstvo (2). Prikaz permutacije kao kompozicije nekih transpozicija nije jednoznačan, ali sad, na temelju svojstva (3), možemo još precizirati:

(4) *Svaka permutacija može se napisati kao kompozicija nekih transpozicija. Za parnu permutaciju broj takvih transpozicija je paran, a za neparnu permutaciju neparan.*

Svojstvo (3) možemo, naime, proširiti na kompoziciju m permutacija, za bilo koji m:

$$\operatorname{sign}(p_1 \circ \cdots p_m) = \operatorname{sign} p_1 \cdots \operatorname{sign} p_m.$$

Stoga i kompozicija m transpozicija ima predznak $(-1)^m$. Zbog toga se u rastavu parne (neparne) permutacije na transpozicije mora pojaviti paran (neparan) broj transpozicija.

Napokon, možemo dokazati da parnih i neparnih permutacija u simetričnoj grupi S_n ima jednako mnogo, čim je $n > 1$. Štoviše, parne permutacije čine grupu.

(5) *Za $n \geq 2$ simetrična grupa S_n sastoji se od po $n!/2$ parnih i $n!/2$ neparnih permutacija. Podskup parnih permutacija u S_n je grupa s obzirom na kompoziciju.*

Iz svojstva (3) vidimo da je kompozicija parnih permutacija također parna, znamo da je identiteta (neutralni element) parna permutacija, a za parnu permutaciju inverzna permutacija također je parna. Stoga parne permutacije čine grupu.

Pokažimo još da za $n \geq 2$ postoji jednako mnogo parnih i neparnih permutacija. Uspostavit ćemo bijekciju između podskupova parnih i neparnih permutacija u grupi S_n. Uzmimo bilo koju transpoziciju t (zapravo trebamo bilo koju neparnu permutaciju, a transpozicija sigurno postoji čim je $n \geq 2$). Ako načinimo kompoziciju bilo koje parne permutacije p s transpozicijom t, $p \circ t$ je neparna permutacija i pritom za različite parne p dobivamo različite neparne permutacije $p \circ t$. (Naime, u svakoj grupi iz $ax = bx$ slijedi $a = b$ pa tako i ovdje, iz $p \circ t = q \circ t$ slijedi $(p \circ t) \circ t = (q \circ t) \circ t$, odatle $p = q$). Time je uspostavljeno injektivno preslikavanje podskupa parnih permutacija u podskup neparnih permutacija, što povlači da broj parnih ne može biti veći od broja neparnih permutacija. No, isto tako možemo neparne permutacije, komponiranjem s t, preslikati u parne permutacije pa neparnih permutacija nema više od parnih. Ima ih, dakle, jednako mnogo, a to znači $n!/2$.

Podgrupa parnih permutacija u simetričnoj grupi S_n naziva se *alternirajućom grupom stupnja n* te se označava s A_n. Na primjer,

$$A_4 = \{id, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3), (1\ 2\ 3), (1\ 3\ 2), (1\ 2\ 4),$$

$$(1\ 4\ 2), (1\ 3\ 4), (1\ 4\ 3), (2\ 3\ 4), (2\ 4\ 3)\}.$$

Bibliografija

[1] D. Bakić, *Linearna algebra*, Školska knjiga, Zagreb 2008.

[2] K.Horvatić, *Linearna algebra I, II*, PMF-Matematički odjel, Zagreb 1995.

Indeks pojmova

Indeks oznaka

$\mathbb{N}$	skup prirodnih brojeva
$\mathbb{Z}$	skup (prsten) cijelih brojeva
$\mathbb{Q}$	skup (polje) racionalnih brojeva
$\mathbb{R}$	skup (polje) realnih brojeva
$\mathbb{C}$	skup (polje) kompleksnih brojeva
$\mathbb{Z}_m$	prsten cijelih brojeva modulo m
$\mathcal{P}$	skup (prsten, vektorski prostor) polinoma (s koeficijentima iz $\mathbb{R}$)
$\mathcal{P}_n$	skup (prsten, vektorski prostor) polinoma stupnja manjeg ili jednakog n zajedno s nulpolinom (s koeficijentima iz $\mathbb{R}$)
$\mathbb{Q}(\sqrt{d})$	kvadratno proširenje polja $\mathbb{Q}$ (kvadratno polje)
0_V	nulvektor iz vektorskog prostora V
V^1, V^2, V^3	skupovi (vektorski prostori) klasa orijentiranih dužina na pravcu, u ravnini i u prostoru
$V^i(O)$	$i = 1, 2, 3$, skupovi (vektorski prostori) radijvektora s početnom točkom O na pravcu, u ravnini i u prostoru
$\mathbb{R}^n$	skup (vektorski prostor) svih uređenih n-torki realnih brojeva
$\mathbb{C}^n$	skup (vektorski prostor) svih uređenih n-torki kompleksnih brojeva
$\mathbb{C}_{\mathbb{R}}$	skup kompleksnih brojeva shvaćen kao realan vektorski prostor
$\mathbb{R}^{\mathbb{N}}$	skup (vektorski prostor) realnih nizova
$\mathbb{R}^{\mathbb{R}}$	skup (vektorski prostor) svih realnih funkcija realne varijable
$[S]$	linearna ljuska skupa S
$\dim V$	dimenzija vektorskog prostora V
$L \leq V$	L je potprostor od V
$L < V$	L je pravi potprostor od V
$L \cap M$	presjek potprostora L i M
$L + M$	suma potprostora L i M
$L \dot{+} M$	direktna suma potprostora L i M
$M_{mn}(\mathbb{F})$	skup (vektorski prostor) svih matrica tipa (m, n) s elementima iz polja $\mathbb{F}$
$A = [a_{ij}]$	matrica zadana općim elementom a_{ij}
A^t	transponirana matrica matrice A
A^{-1}	inverz matrice A
$A \sim B$	matrica A je ekvivalentna matrici B
$M_n(\mathbb{F})$	skup (algebra) svih kvadratnih matrica (reda n) s elementima iz polja $\mathbb{F}$
I_n	jedinična matrica reda n
$r(A)$	rang matrice A
D_r	kanonska matrica određenog tipa ranga r

$\det A$	determinanta matrice A
$\operatorname{sign} p$	predznak permutacije p
$I(p)$	broj inverzija permutacije p
Δ_{ij}	minora (određena elementom matrice na poziciji (i, j))
A_{ij}	algebarski komplement (kofaktor)
$\widetilde{A}$	adjunkta matrice A