Algebarske strukture

Boris Širola

UVOD

Cilj ovog kratkog uvoda je prvo, “neformalno”, upoznavanje sa pojmovima i objektima koji su predmet proučavanja ovog kolegija, od kojih je centralan pojam *algebarske strukture*. Tu dajemo i sažeti pregled glavnih primjera algebarskih struktura, pri čemu zapravo pretpostavljamo da su isti već prije barem spomenuti na nekom od prethodnih matematičkih kolegija. Naglasimo ipak kako je vrlo moguće da će pri prvom čitanju mnoge rečenice koje slijede biti nejasne, ili u najbolju ruku “polujasne”. No neka ta činjenica ne djeluje na Vas kao obeshrabrujući faktor, nego kao motivirajući faktor. Ponavljamo, namjera ovog uvoda je dati prvu “grubu ideju” i plan onoga s čim bi se kolegij Algebarske strukture trebao baviti. Ili drugim riječima, namjera je dati prvi, makar ne sasvim precizan, odgovor na sljedeće pitanje:

Što je to algebarska struktura?

$(\star \quad \star \quad \star)$

Algebra je jedna od fundamentalnih grana matematike. Jedna od mogućih “definicija” bila bi da je to *nauka o algebarskim operacijama*; tojest, proučavanje *algebarskih struktura*. Pritom priroda samih elemenata skupa na kojemu se izvode spomenute algebarske operacije nije od primarne važnosti; primarni je cilj proučavanje tih *algebarskih operacija*.

- **Algebarske operacije i algebarske strukture.**

Imamo dvije vrste algebarskih operacija, tzv. unutarnja množenja i vanjska množenja. Definirajmo precizno te pojmove.

Definicija. Neka je S neki neprazan skup. Svaka funkcija $u : S \times S \to S$,

$$S \times S \ni (x, y) \;\mapsto\; u(x, y) \overset{ozn.}{=} x \cdot y \quad (\text{ili samo } = xy),$$

zove se **unutarnje množenje** na S.

Neka je ponovo S neprazan skup i Ω neki drugi skup. Svaka funkcija $v : \Omega \times S \to S$,

$$\Omega \times S \ni (\alpha, x) \;\mapsto\; v(\alpha, x) \overset{ozn.}{=} \alpha.x \quad (\text{ili samo } = \alpha x),$$

zove se **vanjsko množenje** na S, elementima iz Ω; pritom je uobičajeno svaki element od Ω zvati **operator** na S, ili kraće samo *operator*.

Napomena. Neka je V realan ili kompleksan vektorski prostor i $\mathcal{L}(V)$ pripadna *linearna algebra*, tojest, prostor linearnih operatora na V. Ako stavimo $\Omega := \mathcal{L}(V)$, onda je sa

$$\Omega \times V \ni (A, v) \;\mapsto\; Av = A(v) \in V$$

definirano vanjsko množenje vektora $v \in V$ sa linearnim operatorima $A \in \mathcal{L}(V)$. To je jedan od prvih i glavnih primjera za vanjsko množenje; otuda i dolazi naziv “operatori”, za elemente iz Ω, u gore promatranoj općenitoj situaciji.

Sad ćemo definirati centralni pojam ovog kolegija, pojam *algebarske strukture*.

Definicija. Neka je S neki neprazan skup. **Algebarska struktura** na S je taj skup zajedno sa:

– Bar jednim unutarnjim množenjem i/ili bar jednim vanjskim množenjem, zajedno sa tzv. *aksiomima množenja.*

Napomena. Aksiomi množenja su u pravilu neka od sljedećih dobro poznatih svojstava: *komutativnost, asocijativnost, postojanje neutrala, postojanje inverza, asocijativnost vanjskog množenja, distributivnost,...*

- **Glavni reprezentanti algebarskih struktura.**

(0) **Skupovi.** Skupove možemo gledati kao "degenerirane slučajeve" algebarskih struktura; naime, tu imamo 0 unutarnjih množenja, 0 vanjskih množenja i 0 aksioma množenja.

(1) Strukture s unutarnjim množenjem/množenjima

(1.1) **Grupe.** (1 unutarnje množenje)

– Konačne/beskonačne grupe.
– Komutativne/nekomutativne grupe.
– Kompaktne/nekompaktne, Liejeve, algebarske,... grupe.

(1.2) **Prsteni.** (2 unutarnja množenja)

– Komutativni/nekomutativni prsteni.
– Apstraktni prsteni, topološki prsteni,...
– Prsteni s jedinicom/bez jedinice.

Jedna od specijalnih vrsta prstena su **tijela**; to su prsteni u kojima su svi nenul elementi invertibilni. Komutativna tijela zovu se **polja**. Polja imaju fundamentalnu ulogu npr. u *algebarskoj teoriji brojeva* i u *algebarskoj geometriji.* Kao glavne reprezentante (nekomutativnih) tijela spomenimo tzv. **kvaternione**.

Napomena. Naglasimo da, ukoliko posebno nije rečeno suprotno, pod prstenom uvijek podrazumijevamo *asocijativan prsten*; u ovom kolegiju mi ćemo se baviti isključivo takvim prstenima. No u matematici su od temeljne važnosti i neki neasocijativni prsteni. Tek spomenimo ovdje da su npr. tzv. *Liejevi* i *Jordanovi prsteni* jedni od glavnih reprezentanata iz te klase prstena.

(2) Strukture s barem jednim unutarnjim množenjem i barem jednim vanjskim množenjem.

(2.1) **Moduli.** (1 unutarnje množenje i 1 vanjsko množenje)

Definicija. Ako su dani neprazni skupovi M i Ω, pri čemu je M komutativna grupa i Ω prsten, te ako je zadano preslikavanje

$$\Omega \times M \ni (\alpha, x) \ \mapsto \ \alpha.x \in M,$$

zajedno sa tzv. *aksiomima modula*, onda govorimo da je M lijevi **modul** nad Ω, ili da je M lijevi **Ω-modul**; analogno se definira i pojam desnog modula.

Napomena. (I) Primjetimo da ako je Ω štoviše polje, onda je Ω-modul zapravo vektorski prostor nad poljem Ω. Tako možemo u biti govoriti da su moduli "vektorski prostori nad (ne nužno komutativnim) prstenima". Usput rečeno, da posljednja fraza nije nešto što je "daleko od istine" govori i činjenica da je *Teorija modula* naime i imala svoje prve početeke u vektorskim prostorima i linearnim operatorima na njima; tojest, u *linearnoj algebri.*

(II) Ako je R nekomutativan prsten, onda općenito nije moguće na neki prirodan način neki konkretan lijevi R-modul shvatiti kao desni R-modul. Ta činjenica u stvari govori da ima smisla gledati i lijeve i desne module. Ali u isto vrijeme treba primjetiti da u *Teoriji modula* proučavanje lijevih modula ide sasvim analogno kao i za desne module; mogli bismo to reći i tako da sve što radimo s lijevim modulima radimo "u zrcalnoj slici" i s desnim modulima. Tako se pri proučavanju modula uvijek izabere samo jednu vrstu, ili lijeve ili desne, jer će svi dobiveni rezultati za jednu vrstu po potpunoj analogiji vrijediti i za drugu vrstu.

(2.2) **Algebre.** (2 unutarnja množenja i 1 vanjsko množenje)

Definicija. Neka je A komutativan prsten s jedinicom, a $\mathcal{R} = (\mathcal{R}, +, \cdot)$ neki (ne nužno komutativan) prsten, koji je ujedno i A-modul. Tada kažemo da je $\mathcal{R}$ **algebra** nad A, ili **A-algebra**.

Napomena. Jedna od glavnih podjela algebri je na *komutativne* i *nekomutativne* algebre, gdje je algebra $\mathcal{R} = (\mathcal{R}, +, \cdot)$ komutativna ukoliko je operacija "$\cdot$" na $\mathcal{R}$ komutativna, a inače je $\mathcal{R}$ nekomutativna.

Druga podjela algebri, u važnom slučaju kada je A štoviše polje, je na konačnodimenzionalne i beskonačnodimenzionalne algebre. Jasno, u rečenom slučaju je svaka A-algebra $\mathcal{R}$ posebno i vektorski prostor nad A, pa je onda dimenzija algebre dobro definirana; naime, $\dim \mathcal{R} = \dim_A \mathcal{R}$ je standardna dimenzija A-vektorskog prostora $\mathcal{R}$.

Treća važna podjela algebri, analogno kao i kod prstena, je na *asocijativne* i *neasocijativne* algebre. Jasno, algebra $\mathcal{R}$ je asocijativna, ukoliko je $\mathcal{R} = (\mathcal{R}, +, \cdot)$ asocijativan prsten; u suprotnom govorimo da je $\mathcal{R}$ neasocijativna algebra. Sada su jedni od glavnih reprezentanata tzv. *Liejeve* i *Jordanove algebre.*

• **Prvi primjeri algebarskih struktura.**

(1.1) GRUPE.

Komutativne: *Grupa cijelih brojeva* $(\mathbb{Z}, +)$; *Grupa* $\mathbb{Z}_n = (\mathbb{Z}/n\mathbb{Z}, +)$, *ostataka modulo* n; *Multiplikativna grupa realnih brojeva* $(\mathbb{R}^\times, \cdot)$; (Jednodimenzionalni) *torus* $\mathbb{T} := \{z \in \mathbb{C} \mid |z| = 1\}$, uz standardno množenje u $\mathbb{C}$.

Nekomutativne: *Simetrična grupa* $\mathcal{S}_n$; *Alternirajuća grupa* $\mathcal{A}_n$; *Opće linearne grupe* $\mathrm{GL}(n, \mathbb{R})$ i $\mathrm{GL}(n, \mathbb{C})$; *Specijalne linearne grupe* $\mathrm{SL}(n, \mathbb{R})$ i $\mathrm{SL}(n, \mathbb{C})$; *Unitarna grupa* $\mathrm{U}(n)$.

(1.2) PRSTENI.

Komutativni: *Prsten cijelih brojeva* $(\mathbb{Z}, +, \cdot)$; *Prsten* $\mathbb{Z}_n = (\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ *ostataka modulo* n; *Prsten Gaussovih cijelih brojeva* $\mathbb{Z}[\imath] := \{a + b\imath \mid a, b \in \mathbb{Z}\}$, gdje je $\imath = \sqrt{-1}$; *Prsten kompleksnih polinoma u* n *varijabli* $\mathbb{C}[X_1, \ldots, X_n]$; $\mathbb{Z}[X_1, \ldots, X_n]$, *prsten polinoma nad* $\mathbb{Z}$ *u* n *varijabli.*

Nekomutativni: *Prsteni* n*-puta-*n *realnih, kompleksnih i cjelobrojnih matrica* $M_n(\mathbb{R}) = (M_n(\mathbb{R}), +, \cdot)$, $M_n(\mathbb{C})$ i $M_n(\mathbb{Z})$.

(1.3) POLJA.

Polja racionalnih, realnih i kompleksnih brojeva $\mathbb{Q}$, $\mathbb{R}$ i $\mathbb{C}$; Polja koja su tzv. *kvadratna proširenja* od $\mathbb{Q}$, a mogu se opisati kao

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

gdje je $d \in \mathbb{Z} \setminus \{0, 1\}$ *kvadratno slobodan*; Prosta konačna polja $\mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z}$, tojest, polja ostataka modulo p za $p \in \mathbb{N}$ *prim broj.*

(2.1) MODULI.

Neka je A proizvoljan komutativan prsten s jedinicom, a $M_n(A)$ prsten n-puta-n matrica sa koeficijentima iz A. Definirajmo $\mathcal{X} := A^n$, aditivnu grupu n*-torki* $(a_1, \ldots, a_n)$, $a_i \in A$; tojest, zbrajanje takovih n-torki je "po komponentama". Promatrajmo vanjska množenja

$$A \times \mathcal{X} \ni \big(\alpha, (a_1, \ldots, a_n)\big) \longmapsto \big(\alpha a_1, \ldots, \alpha a_n\big) \in \mathcal{X},$$

i

$$M_n(A) \times \mathcal{X} \ni (M, \boldsymbol{a}) \longmapsto M\boldsymbol{a} \in \mathcal{X},$$

gdje je $M\boldsymbol{a}$ standardno množenje kvadratne matrice M i jednostupčane matrice $\boldsymbol{a} = (a_1, \ldots, a_n)^t$ (t označava "transponiranje"). Tada ta dva vanjska množenja definiraju na komutativnoj grupi $\mathcal{X}$ dvije (bitno različite) strukture modula; tako govorimo da je $\mathcal{X}$ i A-modul, ali i $M_n(A)$-modul.

Kad god imamo neki prsten R, onda se unutarnje množenje od R može shvatiti i kao vanjsko množenje. Sasvim precizno, na komutativnoj grupi $R = (R, +)$ definiramo

$$R \times R \ni (r, x) \mapsto rx \in R.$$

Tako se R može shvatiti zapravo i kao lijevi i kao desni modul nad samim sobom; ti se moduli, da bismo razlikovali prsten R od R-a kao R-modula, obično označavaju sa ${}_RR$ i R_R.

(2.2) ALGEBRE.

Neka je $\mathbb{K}$ proizvoljno polje i V neki $\mathbb{K}$-vektorski prostor. Neka je $\mathcal{L}(V)$ skup svih linearnih operatora na V, na kojem gledamo standardne operacije, *zbrajanja* operatora i *množenja* operatora; tada je $\mathcal{L}(V)$ (nekomutativan) prsten s jedinicom. Jasno, $\mathcal{L}(V)$ je u isto vrijeme i $\mathbb{K}$-vektorski prostor, za standardno množenje operatora skalarima. Drugim riječima, ovo što smo rekli zapravo govori da je $\mathcal{L}(V)$ jedna $\mathbb{K}$-algebra. Slobodno možemo reći da je ta algebra na neki način "kanonski model" ili "prototip" za *algebru* kao algebarsku strukturu. I upravo rečena činjenica opravdava to što je ta struktura dobila i posebno ime: **linearna algebra**. (Primjetite da se upravo "u čast" toj algebarskoj strukturi istim imenom zovu i dva kolegija na 1. godini studija!)

POGLAVLJE 1

Grupe

1. Osnovni pojmovi, primjeri i rezultati

Grupa, kao algebarska struktura, je osnovni pojam u matematici. Grupe se pojavljuju u analizi, u algebri, u teoriji brojeva, u algebarskoj geometriji i u mnogim drugim granama matematike. Podsjetimo se nekih prvih i dobro poznatih primjera.

Primjer 1.1. Skup cijelih brojeva $\mathbb{Z}$, uz operaciju *zbrajanja*, je grupa. Ako želimo posebno naglasiti o kojoj se ovdje binarnoj operaciji radi, pisat ćemo $(\mathbb{Z},+)$. Dobro su poznata sljedeća svojstva zbrajanja:

$$\begin{gathered}(x+y)+z=x+(y+z) \qquad \forall x,y,z\in\mathbb{Z},\\ x+0=0+x=x \qquad \forall x\in\mathbb{Z},\\ (\forall x\in\mathbb{Z})(\exists!\,-x\in\mathbb{Z}): \qquad x+(-x)=(-x)+x=0,\\ x+y=y+x \qquad \forall x,y\in\mathbb{Z}.\end{gathered}$$

Analogno, gornja svojstva vrijede i ako promatramo skupove realnih brojeva $\mathbb{R}$, kompleksnih brojeva $\mathbb{C}$, ili racionalnih brojeva $\mathbb{Q}$, s obzirom na zbrajanje. Tako govorimo o grupama $(\mathbb{R},+)$, $(\mathbb{C},+)$ i $(\mathbb{Q},+)$. Ako sa $\mathbb{R}^\times$, $\mathbb{C}^\times$ i $\mathbb{Q}^\times$ označimo skupove realnih, kompleksnih i racionalnih brojeva različitih od nule, redom, operacija *množenja* na tim skupovima definira strukturu grupe; te grupe označavamo $(\mathbb{R}^\times,\cdot)$, $(\mathbb{C}^\times,\cdot)$ i $(\mathbb{Q}^\times,\cdot)$, redom. Ako označimo $\mathbb{R}_+ := \{x\in\mathbb{R} \mid x>0\}$, onda je taj skup, ponovo uz operaciju množenja, takodjer grupa; tu ćemo grupu označavati $(\mathbb{R}_+,\cdot)$.

Kao početnu motivaciju za uvođenje pojma homomorfizma grupa, podsjetimo se ovdje jednog važnog preslikavanja. Eksponencijalno preslikavanje $\exp:\mathbb{R}\to\mathbb{R}$, $x\mapsto e^x$, neprekidno je, zadovoljava osnovnu relaciju $e^{x+y}=e^x\cdot e^y$ i preslikava $\mathbb{R}$ na $\mathbb{R}_+=(0,+\infty)$. Drugim riječima,

$$\exp:(\mathbb{R},+)\to(\mathbb{R}_+,\cdot)$$

je izomorfizam grupa. Primjetimo isto tako da je sa $\ln:(\mathbb{R}_+,\cdot)\to(\mathbb{R},+)$ definirano pripadno inverzno preslikavanje; podsjetimo se da vrijedi $\ln(x\cdot y)=\ln x+\ln y$.

1.1. Definicije grupe, podgrupe i homomorfizma.

Nakon ovih početnih razmatranja, spremni smo za uvođenje precizne definicije grupe.

Definicija 1.2. Neprazan skup $G=(G,\cdot)$, gdje je $\cdot : G\times G\to G$ binarna operacija, zove se **grupa** ako vrijede sljedeća svojstva (ovdje govorimo i o *aksiomima grupe*):

$$\begin{gathered}(x\cdot y)\cdot z=x\cdot(y\cdot z) \quad \forall x,y,z\in G \qquad \text{(asocijativnost)},\\ (\exists\, e\in G): \qquad e\cdot x=x\cdot e=x \quad \forall x\in G \qquad \text{(neutralni element)},\\ (\forall x\in G)(\exists!\, x^{-1}\in G): \qquad x\cdot x^{-1}=x^{-1}\cdot x=e \qquad \text{(inverzni element)}.\end{gathered}$$

Element e, ili e_G ako želimo posebno naglasiti da je riječ o grupi G, zove se **neutralni element** grupe, ili kraće **neutral** grupe. Za zadani $x\in G$, element $x^{-1}\in G$ koji zadovoljava gore navedeno treće po redu svojstvo, zove se **inverzni element** od x, ili kraće **inverz** od x.

Ako još vrijedi i svojstvo

$$x \cdot y = y \cdot x \qquad \forall x, y \in G \qquad \text{(komutativnost)},$$

onda kažemo da je G **komutativna grupa**, a u suprotnom govorimo o **nekomutativnoj grupi**; jednako su u upotrebi i termini **abelova grupa** za komutativnu grupu, te **neabelova grupa** za nekomutativnu grupu.

NAPOMENA. Od sada nadalje, kada je riječ o nekoj grupi $G = (G, \cdot)$, mi pri množenju elemenata u toj grupi nećemo pisati simbol "$\cdot$"; tojest, ako su $x, y \in G$, onda

$$\text{pišemo} \quad xy \quad \text{namjesto} \quad x \cdot y.$$

Napomena 1.3. (1) Dobro je ovdje podsjetiti i na sljedeću standardnu terminologiju. Ako imamo neki skup G na kojemu je definirana operacija $\cdot : G \times G \to G$, tj. za bilo koje $x, y \in G$ je uvijek i $x \cdot y \in G$, kažemo da je $(G, \cdot)$ **grupoid**. Grupoid u kojemu vrijedi i asocijativnost zove se **polugrupa**. Polugrupa koja ima (jedinstven; v. (2) dolje) neutralni element zove se **monoid**. Jasno, monoid u kojemu postoji inverz svakog elementa je grupa.

Naravno, kao i za grupe, možemo promatrati i (ne)komutativnost gornjih struktura. Tako govorimo o *(ne)komutativnoj polugrupi*, odnosno o *(ne)komutativnom monoidu.*

(2) Primjetimo sljedeće važne činjenice: I neutralni element e i inverz x^{-1} od bilo kojeg elementa $x \in G$ su jedinstveni. Da bismo to dokazali, pretpostavimo da u nekoj grupi G postoje dva neutralna elementa e_1 i e_2. No tada je $e_1 = e_1 e_2$ (jer je e_2 neutral u G), ali isto tako imamo $e_2 = e_1 e_2$ (jer je i e_1 neutral u G). Slijedi da je onda $e_1 = e_2$, tojest, neutral u grupi je doista jedinstven. Da bismo dokazali drugu tvrdnju, pretpostavimo da za neki element $x \in G$ postoje dva inverza, recimo da su to neki elementi x_1 i x_2. No onda je $x_1 = x_1 e = x_1(x x_2)$; ovdje koristimo da je e neutral u grupi, ali i činjenicu da je x_2 inverz od x. Sada iskoristimo svojstvo asocijativnosti i činjenicu da je i x_1 jednako tako inverz od x, pa imamo $x_1(x x_2) = (x_1 x)x_2 = ex_2 = x_2$. Slijedi da je $x_1 = x_2$, što smo i morali pokazati.

(3) Prva moguća podjela grupa je na komutativne i nekomutativne grupe. Tek kažimo ovdje kako su obje klase vrlo intenzivno proučavane, ali je bitno napomenuti kako su u pravilu nekomutativne grupe puno kompliciraniji objekti.

U vezi s gore dokazanom jedinstvenosti inverza, u proizvoljnoj grupi, instruktivan je sljedeći jednostavan zadatak.

Zadatak 1. Neka je S neprazan skup i neka je δ neki "ekstra-element"; tj., $\delta \notin S$. Definirajmo skup

$$X := S \cup \{\delta\}.$$

Na podskupu $S \times X$, od $X \times X$, definirajmo operaciju $\circ$ ovako:

$$a \circ b = \delta \qquad \text{i} \qquad a \circ \delta = a, \qquad \forall a, b \in S.$$

Dokažite: Ako je $\operatorname{card} S = 2$, onda se gornja operacija $\circ$ može proširiti na cijeli Kartezijev produkt $X \times X$, tako da onda $X = (X, \circ)$ bude grupa. Vrijedi li nužno i obratno?

(*Uputa:* Pokažite da je δ neutral u X. Za obrat; pokažite da za $\operatorname{card} S \geq 3$ neće biti ispunjen aksiom o inverznom elementu.)

Definicija 1.4. Proizvoljan podskup $A \subseteq G$, gdje je G grupa, zvati ćemo **kompleks**. Za proizvoljne $A, B \subseteq G$, definiramo produkt tih kompleksa kao

$$A\,B := \{a\,b \mid a \in A \ \ \& \ \ b \in B\};$$

posebno u slučaju da je $B = \{x\}$, tojest jednočlan skup, pisat ćemo kraće $A\,x$ namjesto $A\{x\}$.

Kompleks $H \subseteq G$ je **podgrupa** od G ako je to ujedno i grupa za operaciju koja je definirana na G. Drugim riječima, H je podgrupa od G ako vrijede sljedeća dva uvjeta:

(**1**) $(\forall x, y \in H): \quad x\,y \in H$;
(**2**) $(\forall x \in H): \quad x^{-1} \in H$.

Činjenicu da je H podgrupa od G označavamo sa

$$H \leq G.$$

Sljedeći jednostavan rezultat je takozvani "*kriterij podgrupe*".

Propozicija 1.5. *Kompleks H je podgrupa grupe G* akko *vrijedi sljedeći uvjet:*

$$(\forall x, y \in H): \quad x\,y^{-1} \in H.$$

Dokaz. Pretpostavimo najprije da u H vrijede gore navedeni uvjeti (**1**) i (**2**). Sada, ako su x i y dva elementa iz H, onda po (**2**) je posebno i y^{-1} u H, a onda po (**1**) je i produkt $x\,y^{-1}$ također u H. Tako smo dokazali da vrijedi uvjet dan u iskazu propozicije. Da bismo dokazali obratnu implikaciju, moramo vidjeti da iz danog uvjeta slijede i (**1**) i (**2**). Ali ako su $x, y \in H$, onda je posebno i $e = x\,x^{-1} \in H$. Nadalje, za e i x iz H imamo onda da je i $x^{-1} = e\,x^{-1} \in H$; to je (**2**). Isto tako, iz $y \in H$, po dokazanom (**2**) slijedi i da je $y^{-1} \in H$. No onda, konačno, ponovo po uvjetu iz propozicije slijedi i da je $x(y^{-1})^{-1} = x\,y \in H$; to je (**1**). □

Napomena 1.6. Svaka grupa G ima barem dvije podgrupe; to su sama G i $\{e\}$. Budući da je ta činjenica sasvim očita, i nije od nikakve koristi za razumijevanje strukture dotične grupe G, te dvije podgrupe zovemo **trivijalnim** podgrupama. Pravi je problem u teoriji grupa razumijeti **netrivijalne** podgrupe od dane grupe G, tojest, one podgrupe $H \leq G$ koje nisu trivijalne; takve se podgrupe još zovu i **prave podgrupe**. Tek napomenimo ovdje i to da je u općenitoj situaciji problem razumijevanja *svih* netrivijalnih podgrupa neke grupe G vrlo kompliciran, tako da se često gledaju samo neke specijalnije klase podgrupa; npr. normalne podgrupe (vidi Definiciju 1.26).

Sljedeća moguća podjela grupa je na konačne grupe i na beskonačne grupe. Tako da bi daljnja specijalizacija bila npr. proučavanje konačnih nekomutativnih grupa, ili beskonačnih komutativnih grupa, itd.

Definicija 1.7. Ako je G grupa, definirajmo njezin **red** kao

$$|G| := \mathrm{card}(G);$$

tojest, red grupe je kardinalni broj skupa G. Kažemo da je grupa G **konačna grupa** ako je $|G| < \infty$; inače je G **beskonačna grupa**.

Sada, kada imamo definiran pojam grupe, sasvim je prirodno pitanje kako međusobno "povezati" dva takva objekta od interesa. Preciznije, kakova preslikavanja među tim objektima treba gledati.

Definicija 1.8. Neka su G i H dvije grupe. Preslikavanje $f : G \to H$ je **homomorfizam** grupa, ako "čuva strukturu", tojest, ako vrijedi

$$f(x\,y) = f(x)\,f(y) \qquad \forall x, y \in G.$$

Uvodimo oznaku

$$\mathrm{Hom}(G, H) := \text{skup svih homomorfizama iz } G \text{ u } H.$$

Nadalje, homomorfizam f koji je još i injekcija naziva se **monomorfizam**, f koji je i surjekcija zovemo **epimorfizam**, a homomorfizam koji je i mono- i epi-, tojest bijektivan homomorfizam, zovemo **izomorfizam**. Za dvije grupe G i H reći ćemo da su *izomorfne*, ako postoji neki izomorfizam f među njima; tu činjenicu označavamo sa

$$G \cong H.$$

Posebno, ako je $G = H$, tojest, ako imamo homomorfizam $f : G \to G$, onda kažemo da je f **endomorfizam** od G. Uvodimo oznaku

$$\mathrm{End}\, G := \text{skup svih endomorfizama od } G.$$

Endomorfizam koji je još i bijekcija zove se **automorfizam** od G. Uvodimo oznaku

$$\mathrm{Aut}\, G := \text{skup svih automorfizama od } G$$

(vidi Korolar 1.10).

Za proizvoljni homomorfizam $f : G \to H$ definirajmo njegovu **jezgru**

$$\mathrm{Ker}\, f := \{x \in G \mid f(x) = e_H\},$$

i njegovu **sliku**

$$\mathrm{Im}\, f := \{f(x) \mid x \in G\}.$$

Sada ćemo dokazati ovu jednostavnu lemu.

Lema 1.9. *Ako su $f : G \to H$ i $g : H \to K$ homomorfizmi grupa, onda je i njihova kompozicija $g \circ f : G \to K$ također homomorfizam grupa. Štoviše, ako su f i g oba monomorfizmi (tj. epimorfizmi, izomorfizmi), onda je i $g \circ f$ monomorfizam (tj. epimorfizam, izomorfizam).*

Dokaz. Za $x, y \in G$ imamo

$$(g \circ f)(x\,y) = g(f(x\,y)) = g(f(x)f(y)) = g(f(x))g(f(y)) = (g \circ f)(x)(g \circ f)(y);$$

ovdje koristimo definiciju kompozicije dviju funkcija i činjenicu da su i f i g homomorfizmi grupa. Za drugu tvrdnju leme trebamo se samo sjetiti da je kompozicija dvije injekcije (tj. surjekcije, bijekcije) ponovo injekcija (tj. surjekcija, bijekcija). $\square$

Sljedeći je korolar sasvim jasan.

Korolar 1.10. *Za proizvoljnu grupu G,* $\mathrm{Aut}\, G$ *je također grupa, uz operaciju komponiranja "$\circ$"; tako govorimo o* **grupi automorfizama** *od G.*

U prethodnoj definiciji smo za grupe uveli pojam "biti izomorfan". Precizno, dvije grupe G i H su izomorfne ako postoji neki izomorfizam $f : G \to H$; tada pišemo $G \cong H$. Tako je zapravo definirana relacija $\cong$, "izomorfizam grupa".

Propozicija 1.11. *Izomorfizam grupa je relacija ekvivalencije.*

Zadatak 2. Neka su G i H bilo koje grupe i neka je $f : G \to H$ proizvoljan homomorfizam.

(i) Dokažite: $f(e_G) = e_H$ i $f(x^{-1}) = f(x)^{-1}$, za sve $x \in G$.
(ii) Dokažite: f je monomorfizam akko je $\operatorname{Ker} f = \{e_G\}$.
(iii) Dokažite: ako je G_1 neka podgrupa od G, onda je njena homomorfna slika $f(G_1)$ podgrupa od H; posebno, $\operatorname{Im} f \leq H$. Ako je $H_1 \leq H$, mora li praslika $f^{-1}(H_1)$ biti nužno podgrupa od G?
(iv) Dokažite: ako je f štoviše bijektivan homomorfizam, tojest izomorfizam, onda je f^{-1} također homomorfizam.
(v) Dokažite detaljno Propoziciju 1.11, i zatim da je broj klasa po relaciji $\cong$ na skupu svih grupa beskonačan.

1.2. Primjeri nekih važnih grupa.

U ovom pododjeljku navodimo neke važne primjere grupa.

Primjer 1.12. Neka je $S \neq \emptyset$ neki skup. Definirajmo

$$\operatorname{Perm}(S) := \{f : S \to S \mid f \text{ je bijekcija}\}.$$

Ako je $f : S \to S$ bijekcija, onda postoji *inverzna funkcija* $f^{-1} : S \to S$ i ona je naravno isto bijekcija. Nadalje, za bilo koje funkcije $f, g : S \to S$, definirana je njihova kompozicija $g \circ f : S \to S$. Za tri funkcije $f, g, h : S \to S$, vrijedi asocijativnost kompozicije, tojest, $h \circ (g \circ f) = (h \circ g) \circ f$. Konačno, funkcija *identiteta* $\mathrm{id} = \mathrm{id}_S : S \to S$, $\mathrm{id}(x) = x$ za svaki $x \in S$, zadovoljava svojstvo $f \circ \mathrm{id} = \mathrm{id} \circ f = f$, za bilo koji f. Sve ovo navedeno zapravo govori da je $(\operatorname{Perm}(S), \circ)$ grupa. Ta se grupa zove **grupa permutacija**, ili **simetrična grupa**, skupa S.

Posebno, ako je skup S konačan, možemo bez smanjenja općenitosti pretpostaviti da je zapravo $S = \{1, 2, \ldots, n\}$. U tom slučaju standardno se permutacije f od S zapisuju u obliku

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

Nadalje, grupu permutacija ćemo sada označavati sa $\mathcal{S}_n$. Spomenimo ovdje još jedan važan pojam. Permutacija $\tau \in \mathcal{S}_n$ zove se **transpozicija** ako postoje $1 \leq i, j \leq n$, $i \neq j$, takvi da je $\tau(i) = j$, $\tau(j) = i$ i $\tau(k) = k$ za sve $k \neq i, j$.

Zadatak 3. Dokažite sljedeće tvrdnje:

(i) $\mid \mathcal{S}_n \mid = n!$

(ii) Grupa $\mathcal{S}_n$ je generirana transpozicijama; tojest, svaku se permutaciju $\sigma \in \mathcal{S}_n$ može napisati kao kompoziciju $\sigma = \tau_p \circ \cdots \circ \tau_1$, za neke transpozicije $\tau_1, \ldots, \tau_p$. (*Uputa*: Bez smanjenja općenitosti možemo pretpostaviti da je $\sigma(n) = m \neq n$; onda za transpoziciju τ koja preslikava $m \mapsto n$ i $n \mapsto m$ imamo $\tau \circ \sigma(n) = n$. Tako možemo shvatiti da je zapravo $\tau \circ \sigma \in \mathrm{Perm}(\{1, \ldots, n-1\})$; sada koristimo induktivni argument.)

(iii) Općenito, grupa $(\mathrm{Perm}(S), \circ)$ nije komutativna.

Primjer 1.13. Promatrajmo *euklidsku ravninu* $\mathcal{M} \equiv \mathbb{R}^2$, sa *euklidskom metrikom*

$$d(T_1, T_2) := \sqrt{(x_2 - x_1)^2 + (y_2 - y_1)^2},$$

gdje su $T_1 = (x_1, y_1)$ i $T_2 = (x_2, y_2)$ bilo koje dvije točke iz $\mathcal{M}$. Podsjetimo se da se preslikavanje $f : \mathcal{M} \to \mathcal{M}$ zove *izometrija* ako "čuva udaljenost", tojest, ako je $d(T_1, T_2) = d(f(T_1), f(T_2))$ za bilo koje točke T_1 i T_2. Definirajmo

$$\mathrm{Isom}(\mathcal{M}) := \{f : \mathcal{M} \to \mathcal{M} \mid f \text{ je izometrija}\}.$$

Tada je $\mathrm{Isom}(\mathcal{M})$ grupa; ta se grupa zove **grupa izometrija** ravnine $\mathcal{M}$.

Općenitije, ako je u euklidskoj ravnini $\mathcal{M}$ zadan neki skup X, onda se svaka izometrija $f \in \mathrm{Isom}(\mathcal{M})$ takva da je $f(X) = X$ zove **simetrija skupa** X. Jasno je da ako su f_1 i f_2 neke dvije simetrije od X, da je onda i njihova kompozicija $f_2 \circ f_1$ također simetrija od X. Isto tako i inverz f^{-1}, neke simetrije f od X, je ponovo simetrija od X. Definirajmo

$$\mathrm{Sim}(X) := \{f \in \mathrm{Isom}(\mathcal{M}) \mid f(X) = X\}.$$

Po gore rečenom, jasno je da je $\mathrm{Sim}(X)$ doista grupa, tojest, podgrupa od $\mathrm{Isom}(\mathcal{M})$; ta se grupa zove **grupa simetrija** skupa X.

Zadatak 4. Da li je $\mathrm{Isom}(\mathcal{M})$ abelova grupa?

Primjer 1.14. Neka je $\mathbb{K}$ proizvoljno polje, npr. $\mathbb{K} = \mathbb{R}, \mathbb{C}, \mathbb{Q}$, i neka je V neki konačnodimenzionalan vektorski prostor nad $\mathbb{K}$. Sa $\mathcal{L}(V)$ označimo pripadnu *linearnu algebru*, tojest, algebru linearnih operatora na V. Posebno, $(\mathcal{L}(V), +)$ je komutativna grupa. Pored te grupe, postoji i jedna puno zanimljivija nekomutativna grupa, čija je unutarnja operacija množenje operatora; preciznije, komponiranje operatora. (Ovdje, kako je to uobičajeno, za dva operatora A i B mi ćemo pisati $A\,B$ namjesto $A \circ B$.) Ali prije same definicije te grupe podsjetimo se nekih dobro poznatih činjenica o linearnoj algebri. Prvo, ako je $\dim_{\mathbb{K}}(V) = n$, onda je $\mathcal{L}(V) \cong M_n(\mathbb{K})$; tojest, linearna algebra $\mathcal{L}(V)$ je izomorfna (kao algebarska struktura) algebri $M_n(\mathbb{K})$ n-puta-n matrica sa koeficijentima iz $\mathbb{K}$. (Uzmimo bilo koju bazu $(e) = (e_1, \ldots, e_n)$ od V i onda se proizvoljan linearan operator $A \in \mathcal{L}(V)$ može zapisati u toj bazi kao matrica $A(e)$; sada je traženi izomorfizam rečenih dviju algebri dan kao $A \mapsto A(e)$.) Drugo, za operatore iz $\mathcal{L}(V)$, odnosno za matrice iz $M_n(\mathbb{K})$, vrijedi sljedeći poznati rezultat.

Teorem. (Binet-Cauchy) *Za proizvoljne* $A, B \in \mathcal{L}(V)$*, odnosno* $A, B \in M_n(\mathbb{K})$*, imamo*

$$\det(A\,B) = \det A \det B.$$

Sada definirajmo

$$\mathrm{GL}(V) := \{A \in \mathcal{L}(V) \mid A \text{ je invertibilan operator}\}.$$

Drugim riječima, linearni operatori A iz $\mathrm{GL}(V)$ su oni koji su još i bijekcije. Dobro je poznato da se isti karakteriziraju svojstvom $\det A \neq 0$; takvi se operatori zovu i **regularni**, dok su oni A za koje je $\det A = 0$ **singularni**. Tako je jasno da smo gornji skup mogli definirati i ovako:

$$\mathrm{GL}(V) := \{A \in \mathcal{L}(V) \mid \det A \neq 0\}.$$

Primjenom Binet-Cauchyjevog teorema, vidimo da je skup $\mathrm{GL}(V)$ zatvoren za operaciju množenja. Isto tako, ako je $A \in \mathrm{GL}(V)$, onda postoji njegov inverz A^{-1} i on je također u $\mathrm{GL}(V)$; naime, $1/\det A = \det A^{-1} \neq 0$. To pokazuje da je taj skup doista grupa; $\mathrm{GL}(V)$ se zove **opća linearna grupa**. Jednako tako, i njenu "matričnu realizaciju" $\mathrm{GL}_n(\mathbb{K})$ zovemo opća linearna grupa. Jasno, prije spomenuto preslikavanje $A \mapsto A(e)$, posredstvom neke baze u V, realizira sada izomorfizam grupa

$$\mathrm{GL}(V) \cong \mathrm{GL}_n(\mathbb{K}).$$

Primjetimo ovdje još dvije jednostavne posljedice Binet-Cauchyjevog teorema. Preslikavanje

$$\det : \mathrm{GL}(V) \to (K^\times, \cdot)$$

je homomorfizam grupa; štoviše, očito je to epimorfizam, ali nije monomorfizam. Nadalje, skup

$$\mathrm{SL}(V) := \{A \in \mathrm{GL}(V) \mid \det A = 1\}$$

je također grupa; nju zovemo **specijalna linearna grupa**. I ova grupa ima svoju matričnu realizaciju, koja se isto zove specijalna linearna grupa,

$$\mathrm{SL}_n(\mathbb{K}) := \{A \in \mathrm{GL}_n(\mathbb{K}) \mid \det A = 1\};$$

jasno, $\mathrm{SL}_n(\mathbb{K})$ je prava podgrupa od $\mathrm{GL}_n(\mathbb{K})$.

Grupe $\mathrm{GL}(V)$, odnosno njihove "matrične realizacije" $\mathrm{GL}_n(\mathbb{K})$, zasigurno su među glavnim reprezentantima iz klase nekomutativnih grupa. Nadalje, kao što ćemo vidjeti kasnije, te grupe pored specijalnih linearnih grupa sadrže i mnoge druge vrlo zanimljive podgrupe (vidi Pododjeljak 4.2).

Zadatak 5. (i) Što je $\mathrm{Ker}(\det)$, za $\det : \mathrm{GL}_n(\mathbb{K}) \to \mathbb{K}^\times$?

(ii) Neka je $K \leq (\mathbb{K}^\times, \cdot)$ proizvoljna podgrupa. Definirajmo

$$\mathcal{G}(K) := \{A \in \mathrm{GL}_n(\mathbb{K}) \mid \det A \in K\}.$$

(Za $K = \{1\}$ je $\mathcal{G}(K) = \mathrm{SL}_n(\mathbb{K})$.) Da li je $\mathcal{G}(K)$ grupa? Ako su $K_1 \subseteq K_2$ dvije podgrupe od $\mathbb{K}^\times$, koja je inkluzija između $\mathcal{G}(K_1)$ i $\mathcal{G}(K_2)$?

Primjer 1.15. Pogledajmo jediničnu kružnicu u kompleksnoj ravnini, sa središtem u 0; tojest, definirajmo

$$S^1 := \{z \in \mathbb{C} \;:\; |z| = 1\}.$$

Budući za modul kompleksnih brojeva vrijedi $|z_1 z_2| = |z_1|\,|z_2|$, jasno je da je S^1 (komutativna) grupa s obzirom na množenje u $\mathbb{C}$; tojest, $S^1 \leq (\mathbb{C}^\times, \cdot)$. (Grupa S^1 zove se 1-dimenzionalni **torus**. Općenitije, direktan produkt $S^1 \times \cdots \times S^1$, od n primjeraka S^1, zove se n-dimenzionalni torus; o direktnom produktu grupa govorit ćemo u Pododjeljku 3.1.)

Nadalje, za fiksirani $n \in \mathbb{N}$, definirajmo

$$\boldsymbol{\mu}_n := \{z \in \mathbb{C} \ : \ z^n = 1\};$$

to je skup svih n-tih korijena iz 1. Taj je skup, očito, podgrupa od S^1; nju zovemo **grupa** n-tih **korijena jedinice**. (Podsjetimo se da su elementi iz $\boldsymbol{\mu}_n$, za $n \geq 3$, oni kompleksni brojevi koji su vrhovi pravilnog n-terokuta upisanog u S^1 čiji je jedan vrh u broju 1; jasno, $\boldsymbol{\mu}_1 = \{1\}$ i $\boldsymbol{\mu}_2 = \{-1, 1\}$.)

Definirajmo isto tako i

$$\Omega := \bigcup_n \boldsymbol{\mu}_n.$$

Lako se vidi da je i Ω podgrupa od S^1; nju zovemo **grupa korijena jedinice**. Jasno, ova je grupa beskonačna.

Zadatak 6. Za $m \in \mathbb{N}$ definirajmo skup

$$G_{m,n} := \{x \in \mathbb{C} \mid x^m \in \boldsymbol{\mu}_n\}.$$

Dokažite da je $G_{m,n}$ grupa. Koliki je red te grupe? Postoje li neki $m, n, k \in \mathbb{N}$ takvi da je $G_{m,n} \cong \boldsymbol{\mu}_k$, i ako da, koliki je taj k u ovisnosti o m i n?

Sada ćemo navesti jednu jednostavnu lemu; ona će nam, između ostalog, trebati u definiciji koja slijedi.

Lema 1.16. *Neka je G grupa, i neka su $\{H_i \mid i \in I\}$ neke njezine podgrupe. Tada je i njihov (skupovni) presjek*

$$\bigcap_{i \in I} H_i$$

također podgrupa od G.

Dokaz. Označimo $H := \bigcap_{i \in I} H_i$. Sada, za proizvoljne $x, y \in H$ je $x, y \in H_i$, za svaki $i \in I$. No kako je svaka H_i i sama grupa, to je onda po "kriteriju podgrupe" $xy^{-1} \in H_i$, za svaki i. No onda je, po definiciji presjeka skupova, također i $xy^{-1} \in H$. Ponovno koristimo "kriterij podgrupe", te zaključimo da je doista H i sama grupa; tojest, $H \leq G$. □

Zadatak 7. Dokažite da su sa

$$n\mathbb{Z} := \{nz \mid z \in \mathbb{Z}\}, \qquad n \in \mathbb{N}_0,$$

dane sve podgrupe od $(\mathbb{Z}, +)$, a zatim odredite koje su od njih međusobno izomorfne. Odredite posebno podgrupu $10\mathbb{Z} \cap 12\mathbb{Z}$. Što je općenito $m\mathbb{Z} \cap n\mathbb{Z}$?

Definicija 1.17. Za proizvoljan podskup S neke grupe G, definirajmo

$$\langle S \rangle := \bigcap_{\substack{H \leq G \\ S \subseteq H}} H.$$

To je podgrupa od G (po prethodnoj lemi) koju zovemo **grupa generirana** sa S; sam skup S zovemo **skup generatora**. Kažemo da je G **konačnogenerirana** grupa ako postoji konačan podskup $S = \{x_1, \dots, x_n\}$ takav da je $G = \langle S \rangle$; u tom slučaju pišemo i $G = \langle x_1, \dots, x_n \rangle$. Grupa G je **ciklička** ako se može generirati jednim elementom, tojest, ako postoji neki $g \in G$ takav da je $G = \langle g \rangle$; svaki takav g zove se **generator** cikličke grupe G. (Po Zadatku 8, jasno je da je svaka ciklička grupa nužno komutativna.)

Zadatak 8. Za podskup $S \subseteq G$ označimo $S^{-1} := \{x^{-1} \mid x \in S\}$. Dokažite da je

$$\langle S \rangle = \{e\} \cup \{x_1 \cdots x_r \mid r \in \mathbb{N},\ x_i \in S \cup S^{-1}\}.$$

Cikličke grupe su najjednostavnije (netrivijalne) grupe, i pomoću njih se raznim konstrukcijama mogu opisati neke druge, ponekad vrlo komplicirane, grupe. Kako ćemo kasnije pokazati, sljedećim primjerom dane su sve cikličke grupe; jasno, do na izomorfizam.

Primjer 1.18. (1) Grupa $\mathbb{Z} = (\mathbb{Z}, +)$ je (beskonačna) ciklička grupa; primjetimo da su 1 i -1 jedini generatori.

(2) Grupa $(\mathbb{Z}/n\mathbb{Z}, +)$, tzv. **grupa ostataka modulo** n, je (konačna) ciklička grupa; obično pišemo $\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \dots, \overline{n-1}\}$. Ako sa $\varphi : \mathbb{N} \to \mathbb{C}$ označimo *aritmetičku* funkciju

$$\varphi(n) := \mathrm{card}(\{1 \leq k \leq n \mid (k, n) = 1\}$$

(ovdje, za $a, b \in \mathbb{N}$, sa (a, b) označavamo njihovu *najveću zajedničku mjeru*), tzv. *Eulerovu funkciju*, onda je $\varphi(n)$ broj generatora grupe $\mathbb{Z}/n\mathbb{Z}$. Naprimjer, grupa $\mathbb{Z}/12\mathbb{Z}$ ima $\varphi(12) = 4$ generatora; to su $\overline{1}$, $\overline{5}$, $\overline{7}$ i $\overline{11}$.

Napomena 1.19. (*Ekvivalentna definicija konačnogenerirane grupe*)
Imajući Zadatak 8 u vidu, očito je da smo pojam konačnogenerirane grupe mogli definirati i ovako: Grupa G je *konačnogenerirana* ako postoji konačan podskup $S \subseteq G$ takav da

$$(\forall x \in G)(\exists x_i \in S \ \&\ \exists \varepsilon_i \in \{\pm 1\}) : \quad x = x_1^{\varepsilon_1} \cdots x_{n(x)}^{\varepsilon_{n(x)}}.$$

Naravno, u gornjem rastavu od x, $n(x) \in \mathbb{N}$ ovisi o x. Nadalje, rastav na x_i-ove nije općenito jedinstven.

Napomena 1.20. Primjetimo ovdje ovu skupovno-teorijsku činjenicu: Ako je grupa G konačnogenerirana, onda je G, kao skup, prebrojiv. Međutim, nije svaka prebrojiva grupa konačno generirana. Pokažimo da je to istina čak i ako je G komutativna.

Tvrdnja. Grupa $(\mathbb{Q}^\times, \cdot)$ nije konačnogenerirana.

[[*Dokaz.* Pretpostavimo da je $\mathbb{Q}^\times = \langle a_1/b_1, \dots, a_n/b_n \rangle$, za neke $0 \neq a_i \in \mathbb{Z}$ i $b_i \in \mathbb{N}$. Neka je p neki prim broj takav da vrijedi sljedeći uvjet: ($\bullet$) *p ne dijeli niti jedan a_i ni b_i*. No po pretpostavci da je $\mathbb{Q}^\times$ konačnogeneriran, slijedi da onda postoje neki $\alpha_i \in \mathbb{Z}$ takvi da je $p = (a_1/b_1)^{\alpha_1} \cdots (a_n/b_n)^{\alpha_n}$. Ali to je onda u proturječju sa ($\bullet$); time je tvrdnja dokazana.]]

Sljedeći primjer sugerira da struktura konačnogenerirane nekomutativne grupe može biti dosta komplicirana.

Primjer 1.21. Lako je provjeriti da je skup

$$G = \mathrm{SL}_2(\mathbb{Z}) := \left\{ A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \quad | \quad a, b, c, d \in \mathbb{Z} \;\; \& \;\; \det A = 1 \right\}$$

grupa; to je tzv. **modularna grupa**. (Zapravo, ponekad pod modularnom grupom podrazumijevamo kvocijentnu grupu $G/\{\pm \boldsymbol{I}\}$.) Sljedeći teorem daje jednu vrlo korisnu informaciju o toj (beskonačnoj nekomutativnoj) grupi. Njegov je dokaz, koji mi ovdje nećemo dati, sasvim elementaran ali ima “malo posla”.

Teorem. *Grupa G ima dva generatora; preciznije, $G = \langle S, T \rangle$, gdje su*

$$S := \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \qquad T := \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

Općenitije, za $N \in \mathbb{N}$, definirajmo tzv. **kongruencijske podgrupe** nivoa N:

$$\Gamma_0(N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G \quad | \quad c \equiv 0 \pmod{N} \right\}$$

$$\Gamma_1(N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G \quad | \quad a \equiv d \equiv 1 \pmod{N} \;\; \& \;\; c \equiv 0 \pmod{N} \right\}$$

$$\Gamma(N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G \quad | \quad a \equiv d \equiv 1 \pmod{N} \;\; \& \;\; b \equiv c \equiv 0 \pmod{N} \right\}$$

Zadatak 9. (i) Provjerite da su $\Gamma_0(N)$, $\Gamma_1(N)$ i $\Gamma(N)$ doista podgrupe od G.
(ii) Što su te grupe za $N = 1$?

NAPOMENA. U gornjem primjeru definirane kongruencijske podgrupe, i posebno sama modularna grupa, su fundamentalni objekti u matematici, posebno u Teoriji brojeva. Tek za informaciju spomenimo da su s njima u uskoj vezi tzv. *modularne funkcije* i *modularne forme*. Modularne forme, i njihove razne generalizacije i analogoni, kao što su npr. tzv. *automorfne forme* i *L-funkcije*, su objekti od centralnog interesa u današnjoj matematici.

1.3. Normalne podgrupe i kvocijentne grupe.

U ovom pododjeljku najprije uvodimo pojam *klase grupe*, po nekoj njezinoj podgrupi. Nakon toga dokazujemo i prvi zanimljiv rezultat u teoriji konačnih grupa; tzv. *Lagrangeov teorem*. Nakon toga definiramo *normalne podgrupe*, kao jedne od centralnih objekata u teoriji grupa. Zatim dajemo fundamentalnu konstrukciju tzv. *kvocijentne grupe*. Pododjeljak završavamo propozicijom koja govori o tzv. *komutatorskoj podgrupi*.

Najprije, neka je G neka grupa i $H \leq G$ neka podgrupa. Definirajmo jednu relaciju na $G \times G$ ovako:

$$\forall x, y \in G, \qquad x \sim y \overset{\text{def}}{\Longleftrightarrow} xH = yH \;\; \Leftrightarrow \;\; x^{-1}y \in H$$
$$(Hx = Hy \;\; \Leftrightarrow \;\; yx^{-1} \in H).$$

Zadatak 10. Dokažite da je $\sim$ relacija ekvivalencije.

Podsjetimo se da kad god na nekom skupu $\mathcal{X}$ imamo neku relaciju ekvivalencije ρ, onda se $\mathcal{X}$ "raspada" na *klase* po toj relaciji; sa $\mathcal{X}/\rho$ označava se skup svih klasa. Sada je sljedeća definicija jasna.

Definicija 1.22. Klase na koje se raspada grupa G po gornjoj relaciji ekvivalencije $\sim$ označavamo sa xH (tj. Hx) i zovemo **lijeve klase** (tj. **desne klase**) od G po $\sim$. Skup svih klasa $G/\sim$ označavamo sa G/H (tj. $H\backslash G$).

Ako je $\mathrm{card}(G/H) < \infty$, taj broj označavamo sa $(G : H)$ i zovemo **indeks** od G po H. (Naravno, možemo i u slučaju $\mathrm{card}(G/H) = \infty$ definirati indeks $(G : H) = \infty$, ali to nije od neke koristi.)

Primjer 1.23. (1) Za $G = \mathbb{Z}$ i $H = n\mathbb{Z}$ je $G/H = \mathbb{Z}/n\mathbb{Z}$, skup ostataka modulo n, i onda $(\mathbb{Z} : n\mathbb{Z}) = n$.

(2) Za vektorski prostor V nad poljem $\mathbb{K}$, i potprostor $W \leq V$, skup klasa V/W pripadnih aditivnih grupa, kao skup, 'standardni' je *kvocijentni prostor* od V po W.

Napomena 1.24. Ako su zadane dvije podgrupe $H_1, H_2 \leq G$, onda možemo definirati još jednu relaciju na G. Stavimo

$$\forall x, y \in G, \qquad x \sim y \overset{\text{def}}{\iff} H_1xH_2 = H_1yH_2 \;\;\Leftrightarrow\;\; y \in H_1xH_2.$$

Lako je provjeriti da smo ponovo dobili relaciju ekvivalencije. Sada se klase označavaju sa H_1xH_2, dok se skup svih klasa $G/\sim$ označava sa $H_1\backslash G/H_2$.

Jednostavna posljedica gornjih definicija je ovaj temeljni rezultat Teorije konačnih grupa.

Teorem 1.25. (Lagrange)
Ako je G konačna grupa i H neka njezina podgrupa, onda red podgrupe H dijeli red od G; tojest, $|H| \mid |G|$. Preciznije, imamo

$$|G| = |H|\,(G : H).$$

DOKAZ. Budući je $\sim$ relacija ekvivalencije, znamo da su dvije klase xH i yH ili jednake ili disjunktne. To znači da postoje neki reprezentanti $x_1, \ldots, x_t \in G$ tako da je

$$G = x_1H \cup \cdots \cup x_tH \qquad \& \qquad x_iH \cap x_jH = \emptyset \text{ za } i \neq j;$$

tojest, gornja je unija disjunktna. Nadalje, broj klasa u G/H je, po definiciji indeksa, točno $(G : H)$; tojest, $(G : H) = t$. Još samo preostaje vidjeti da je u svakoj klasi x_iH jednak broj elemenata; preciznije,

$$\mathrm{card}(x_iH) = |H|.$$

No to slijedi iz činjenice da je, za proizvoljan $x \in G$, funkcija $\varphi : H \to xH$, dana sa $\varphi(h) := xh$, bijekcija. (Zašto!?) $\square$

Sada definiramo važan pojam "normalne podgrupe". Napomenimo ovdje, što je evidentno iz same definicije, da je u komutativnoj grupi svaka podgrupa normalna; zato pojam normalne podgrupe ima smisla samo u nekomutativnim situacijama. Nadalje, primjetimo da su trivijalne podgrupe $\{e\}$ i G, od proizvoljne grupe G, uvijek normalne.

Definicija 1.26. Podgrupa $N \leq G$ grupe G je **normalna podgrupa** ako vrijedi uvjet

$$xNx^{-1} = N \qquad \forall x \in G.$$

Činjenicu da je podgrupa N normalna u G označavamo sa

$$N \trianglelefteq G.$$

Zadatak 11. Dokažite sljedeće ekvivalencije: Podgrupa N je normalna u G akko $xN = Nx,\ \ \forall x \in G$, akko $xNx^{-1} \subseteq N,\ \ \forall x \in G$.

Kad god se bavimo nekim algebarskim strukturama, od velikog je interesa vidjeti kako se od već danih struktura mogu dobiti neke nove. Prva osnovna tehnika je dobivanje kvocijentnih struktura. Sljedeći rezultat koji uvodi kvocijentnu strukturu u Teoriji grupa je, u tom smislu, fundamentalan.

Teorem 1.27. *Neka je G proizvoljna grupa i N neka njezina normalna podgrupa. Tada kvocijentni skup G/N sa operacijim*

$$G/N \times G/N \to G/N, \qquad (xN, yN) \mapsto xyN,$$

ima strukturu grupe; sada se G/N zove **kvocijentna grupa** *od G po N. Nadalje, preslikavanje*

$$\pi = \pi_N : G \to G/N, \qquad x \mapsto xN,$$

je epimorfizam grupa sa jezgrom $\mathrm{Ker}\,\pi = N$*; π zovemo* **kanonski epimorfizam***, ili* **kanonska surjekcija***.*

Dokaz. Prvo ćemo pokazati da je gore dana operacija množenja dobro definirana. U tu svrhu, pretpostavimo da su dani $x, x', y, y' \in G$ takvi da je $xN = x'N$ i $yN = y'N$; te su dvije jednakosti ekvivalentne sa

$$x^{-1}x' \in N \quad \text{ i } \quad y^{-1}y' \in N. \tag{1}$$

Ali sada imamo

$$xyN = x'y'N \quad \Leftrightarrow \quad y^{-1}x^{-1}x'y' \in N \quad \Leftrightarrow \quad \big(y^{-1}(x^{-1}x')y\big)\,\big(y^{-1}y'\big) \in N.$$

Koristeći (1) i činjenicu $N \trianglelefteq G$ slijedi tvrdnja.

Sada je jasno da smo na G/N doista dobili strukturu grupe. Isto tako, jasno je da je π homomorfizam grupa, te da je surjektivan; naime, za klasu $xN \in G/N$ je $\pi(x) = xN$. Nadalje,

$$\mathrm{Ker}\,\pi = \{x \in G \mid xN = e_{G/N} = e_G N = N\} = \{x \in G \mid x \in N\} = N.$$

Tako je teorem dokazan. □

Primjer 1.28. $\mathrm{SL}_n(\mathbb{K}) \trianglelefteq \mathrm{GL}_n(\mathbb{K})$, za bilo koje polje $\mathbb{K}$.

Sljedeći jednostavan rezultat, o "faktorizaciji homomorfizma", zapravo je posljedica gornjeg teorema i njegovog dokaza. Ovdje ćemo preskočiti detalje, budući će potrebni argumenti biti dani u dokazu tzv. "Prvog teorema o izomorfizmu" (Teorem 2.2).

Korolar 1.29. *Neka je $f : G \to H$ homomorfizam i $N \trianglelefteq G$ takva da je $N \subseteq \operatorname{Ker} f$. Tada postoji, i jedinstven je, homomorfizam*

$$\overline{f} : G/N \to H, \qquad \overline{f}(xN) = f(x) \quad \forall x \in G.$$

Nadalje, $\operatorname{Im} \overline{f} = \operatorname{Im} f$ *i* $\operatorname{Ker} \overline{f} = (\operatorname{Ker} f)/N$. $\overline{f}$ *je izomorfizam akko je f epimorfizam i* $N = \operatorname{Ker} f$.

Napomena 1.30. Kažemo da je $\overline{f}$ dobiven **faktorizacijom** f kroz N. Tu činjenicu možemo prikazati i pomoću komutativnog dijagrama:

Komutativni dijagram!!

Napomena 1.31. U vezi sa konstrukcijom kvocijentne grupe, primjetimo kako ćemo tom metodom iz dane grupe G dobiti neke nove grupe samo ukoliko G ima netrivijalne normalne podgrupe. Time se prirodno postavlja pitanje razumijevanja onih grupa koje nemaju netrivijalnih normalnih podgrupa; takve se zovu **proste grupe**. Pokazuje se da su proste grupe "osnovni blokovi" pomoću kojih je moguće bolje razumijeti mnoge "kompliciranije" grupe. (No to nipošto ne znači da su i sve proste grupe jednostavni objekti!) Spomenimo kako je dugi niz godina glavni problem Teorije konačnih grupa bio *Problem klasifikacije konačnih prostih grupa.* (Danas se smatra da je taj težak problem riješen, iako svi tehnički detalji i dokazi nisu dovedeni do kraja...) Za ilustraciju, navedimo ovdje dvije serije prostih grupa. Najjednostavnija je serija komutativnih grupa $\mathbb{Z}/p\mathbb{Z}$, za $p \in \mathbb{N}$ prim broj. Jedna druga serija je tzv. serija alternirajućih grupa. Da bismo iste precizno definirali, podsjetimo se da svaku permutaciju $\sigma \in \mathcal{S}_n$ možemo napisati kao produkt transpozicija. Kažemo da je σ *parna permutacija*, ako je broj transpozicija paran, a da je *neparna* ako je taj broj neparan; može se vidjeti da, iako dani produkt od σ po transpozicijama nije jedinstven, parnost broja transpozicija ne ovisi o rastavu. Sada stavimo

$$\mathcal{A}_n := \text{skup svih parnih permutacija u } \mathcal{S}_n.$$

Pokazuje se da su $\mathcal{A}_n$ (normalne) podgrupe, indeksa 2, u simetričnoj grupi $\mathcal{S}_n$; one se zovu **alternirajuće grupe**. Nadalje, za $5 \leq n \in \mathbb{N}$, $\mathcal{A}_n$ je prosta grupa.

Sljedeća propozicija govori kako od familija normalnih podgrupa dobivati nove normalne podgrupe.

Propozicija 1.32. *Neka su $N_i \trianglelefteq G$, $i \in I$, normalne podgrupe. Tada su*

$$\bigcap_I N_i \qquad i \qquad \langle \bigcup_I N_i \rangle$$

također normalne podgrupe od G.

Dokaz. Dokažimo da je $N := \langle \bigcup_I N_i \rangle \trianglelefteq G$; tvrdnja za presjek je jasna. U tu svrhu najprije primjetimo (vidi Zadatak 8) da svaki $x \in N$ možemo napisati kao

$$x = n_{i_1} \cdots n_{i_r}, \quad n_{i_j} \in N_{i_j}.$$

Sada za proizvoljan $g \in G$, koristeći činjenicu da su sve podgrupe N_{i_j} sadržane u N i normalne u G, imamo

$$gxg^{-1} = \prod_{j=1}^{r} (gn_{i_j}g^{-1}) \in N.$$

Znači da je $gNg^{-1} \subseteq N$; tojest, $N \trianglelefteq G$. $\square$

Pojmovi komutatora i komutatorske podgrupe, koje ćemo sada definirati, također su vrlo važni u Teoriji grupa.

Definicija 1.33. Neka je G proizvoljna grupa. Za bilo koje elemente $x, y \in G$ definiramo njihov **komutator**

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

Podgrupa

$$G' := \langle [x, y] \mid x, y \in G \rangle$$

od G, tojest, podgrupa generirana svim komutatorima elemenata iz G, zove se **komutatorska podgrupa**.

Sljedeći rezultat navodi glavne informacije o komutatorskoj podgrupi; osim toga, daje i razlog za uvedenu terminologiju.

Propozicija 1.34. *Neka je G proizvoljna grupa. Tada vrijedi sljedeće:*

(i) *Komutatorska podgrupa G' je normalna podgrupa od G; tojest, $G' \trianglelefteq G$.*

(ii) *Kvocijentna grupa G/G' je komutativna.*

(iii) *G' je* najmanja *normalna podgrupa od G za koju je odgovarajuća kvocijentna grupa komutativna. Preciznije, ako je $H \trianglelefteq G$ podgrupa takva da je G/H komutativna grupa, onda H sadrži G'.*

Dokaz. (i) Trebamo vidjeti da je $g\,\omega\,g^{-1} \in G'$, za svaki $g \in G$ i $\omega \in G'$. Ali, jasno, to je dovoljno pokazati na generatorima; tojest, za slučaj $\omega = [x, y]$, za neke $x, y \in G$. Sada, koristeći po tko zna koji put činjenicu da je $g\,g^{-1} = e$ i "trik" da je $u\,v = u\,e\,v = u\,g\,g^{-1}\,v$ za bilo koje $u, v, g \in G$, imamo

$$\begin{aligned} g\,[x, y]\,g^{-1} &= g\,x\,y\,x^{-1}y^{-1}g^{-1} = (g\,x\,g^{-1})(g\,y\,g^{-1})(g\,x\,g^{-1})^{-1}(g\,y\,g^{-1})^{-1} \\ &= [g\,x\,g^{-1}, g\,y\,g^{-1}] \in G'. \end{aligned}$$

Time je (i) pokazano.

(ii) Za $x, y \in G$, u kvocijentnoj grupi G/G', je

$$\begin{aligned} xG'\,yG' = yG'\,xG' \quad &\Leftrightarrow \quad [xG', yG'] = e_{G/G'} = G' \quad \Leftrightarrow \quad [x, y]\,G' = G' \\ &\Leftrightarrow \quad [x, y] \in G'. \end{aligned}$$

Time je (ii) pokazano.

(iii) Pretpostavimo da je H normalna podgrupa od G takva da je kvocijentna grupa G/H komutativna. Onda za bilo koje $x, y \in G$, u G/H, imamo

$$xH\,yH = yH\,xH \quad \Leftrightarrow \quad [x, y] \in H;$$

to pokazuje da se svi generatori komutatorske podgrupe G' nalaze u H, tojest, $G' \subseteq H$. $\square$

1.4. Centralizator, normalizator i centar grupe.

U ovom pododjeljku definiramo pojmove *centralizatora* i *normalizatora* kompleksa, te *centra* grupe. Primjetimo ovdje kako su ti pojmovi interesantni samo ako je grupa G nekomutativna.

Definicija 1.35. Neka je G proizvoljna grupa, $A \subseteq G$ neki kompleks i $x \in G$ bilo koji element. Definiramo **centralizator elementa** x kao

$$\mathcal{C}_G(x) := \{g \in G \mid gx = xg\},$$

i općenitije **centralizator kompleksa** A kao

$$\mathcal{C}_G(A) := \{g \in G \mid gx = xg, \ \ \forall x \in A\} \qquad \Big(= \bigcap_{x \in A} \mathcal{C}_G(x)\Big).$$

Nadalje, definiramo **normalizator** od A kao

$$\mathcal{N}_G(A) := \{g \in G \mid g^{-1}Ag = A\}.$$

Centar grupe definiran je kao centralizator od G, tojest,

$$\mathcal{Z}(G) := \{g \in G \mid gx = xg, \ \ \forall x \in G\}.$$

Dokaz sljedeće jednostavne leme ćemo izostaviti. (Dokažite to sami!)

Lema 1.36. (i) *Ako je $A \subseteq G$, onda su $\mathcal{C}_G(A)$ i $\mathcal{N}_G(A)$ podgrupe od G; nadalje, imamo $\mathcal{C}_G(A) \leq \mathcal{N}_G(A)$.*
(ii) *$\mathcal{Z}(G) \trianglelefteq G$.*

Zadatak 12. Neka je G grupa i $A \subseteq G$ proizvoljan kompleks. Dokažite da je $\mathcal{C}_G(A) \trianglelefteq \mathcal{N}_G(A)$.

Primjer i zadatak koji slijede daju centre nekih vrlo zanimljivih grupa.

Primjer 1.37. Za $n \geq 2$ promatrajmo grupu permutacija $\mathcal{S}_n$. Sa $\mathbf{1}$ označavamo neutral te grupe, tj. permutaciju identitete. Najprije, jasno je da je grupa $\mathcal{S}_2$ komutativna, pa je jednaka svom centru; tj., imamo $\mathcal{Z}(\mathcal{S}_2) = \mathcal{S}_2$. Međutim, za $n \geq 3$ situacija je bitno drukčija. Sasvim precizno, centar je sada *trivijalan*; tj., može se pokazati da vrijedi

$$\mathcal{Z}(\mathcal{S}_n) = \{\mathbf{1}\}, \qquad \text{za } n \geq 3.$$

(Dokažite gornju tvrdnju barem u slučajevima $n = 3, 4$.)

Zadatak 13. (i) Odredite centre sljedećih grupa: $\mathrm{SL}_2(\mathbb{R})$, $\mathrm{SL}_2(\mathbb{C})$, $\mathrm{SL}_3(\mathbb{R})$ i $\mathrm{SL}_3(\mathbb{C})$. (Probajte izračunati i centre grupa $\mathrm{SL}_n(\mathbb{R})$ i $\mathrm{SL}_n(\mathbb{C})$, za proizvoljne n-ove.)

(ii) Odredite centre sljedećih grupa: $\mathrm{GL}_2(\mathbb{R})$, $\mathrm{GL}_2(\mathbb{C})$, $\mathrm{GL}_3(\mathbb{R})$ i $\mathrm{GL}_3(\mathbb{C})$. (Probajte izračunati i centre grupa $\mathrm{GL}_n(\mathbb{R})$ i $\mathrm{GL}_n(\mathbb{C})$, za proizvoljne n-ove.)

Sada ćemo dati još jedan zanimljiv primjer grupe, te ćemo joj odrediti centar.

Primjer 1.38. U $\mathbb{R}^3$ definirajmo operaciju $*$ ovako: Za proizvoljne trojke realnih brojeva (x, y, z) i (x', y', z') stavimo

$$(x, y, z) * (x', y', z') := (x + x' \cos z - y' \sin z, y + x' \sin z + y' \cos z, z + z').$$

Sa G označimo skup $\mathbb{R}^3$, uz gornju operaciju; tj.

$$G = (\mathbb{R}^3, *).$$

Tada vrijedi sljedeće:

Tvrdnja.

(i) G je grupa. (Preciznije rečeno, G je primjer tzv. *rješive Liejeve grupe*.)

(ii) Centar grupe G dan je kao

$$\mathcal{Z}(G) = \{(0, 0, 2k\pi) \mid k \in \mathbb{Z}\}.$$

Uz malo posla, može se vidjeti da (i) doista vrijedi. Prvo, pokazuje se direktnim računom asocijativnost množenja; to je u stvari glavni dio računa. Onda se provjeri da je neutral od G jednak $e_G = (0, 0, 0)$. Konačno, lako se izračuna da je inverz elementa $(x, y, z) \in G$ jednak

$$(-x \cos z - y \sin z, x \sin z - y \cos z, -z).$$

Za (ii) radimo ovako: Lako se provjeri da ako je (x_0, y_0, z_0) trojka takva da je

$$(x, y, z) * (x_0, y_0, z_0) = (x_0, y_0, z_0) * (x, y, z), \qquad \forall (x, y, z) \in G,$$

onda je nužno $(x_0, y_0, z_0) = (0, 0, 2k\pi)$, za neki $k \in \mathbb{Z}$. Odavde odmah slijedi (ii).

Navedimo još dva instruktivna zadatka.

Zadatak 14. Neka je $G = \mathrm{GL}_2(\mathbb{K})$, za polje $\mathbb{K} = \mathbb{R}, \mathbb{C}$ ili $\mathbb{Q}$. Označimo

$$B := \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in G \right\} \qquad \text{gornje trokutaste matrice iz } G,$$

$$H := \left\{ \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} \in G \right\} \qquad \text{dijagonalne matrice iz } G.$$

(i) Dokažite da su B i H podgrupe od G. Da li su normalne podgrupe?

(ii) Izračunajte $\mathcal{N}_G(B)$ i $\mathcal{N}_G(H)$.

(iii) Izračunajte centar grupe G.

(iv) Neka je $x = \begin{pmatrix} 2 & \alpha \\ 0 & 1 \end{pmatrix} \in B \subseteq G$. Izračunajte $\mathcal{C}_G(x)$, posebno za $\alpha = 0$ i kada $\alpha \neq 0$. Kada je podgrupa $\mathcal{C}_G(x)$ komutativna, a kada nije?

Zadatak 15. Neka je G grupa i $A \subseteq G$ kompleks takav da je $Aa = aA$, $\forall a \in A$. Dokažite da je onda $\langle A \rangle \trianglelefteq \mathcal{N}_G(A)$.

Napomena 1.39. Primjetimo da ako je G grupa i $H \leq G$ bilo koja podgrupa, onda je $H \trianglelefteq \mathcal{N}_G(H)$; tojest, svaka podgrupa od G je normalna podgrupa u svom normalizatoru. Posebno primjetimo da ako je H štoviše normalna podgrupa od G, onda je $\mathcal{N}_G(H) = G$. Zapravo, za $H \leq G$, normalizator $\mathcal{N}_G(H)$ je najveća podgrupa od G u kojoj je H normalna podgrupa.

Zadatak 16. Dokažite sve tvrdnje iz prethodne napomene. (Zadnja tvrdnja, precizno rečeno, kaže da je $\mathcal{N}_G(H) = \left\langle \bigcup_{\substack{A \leq G \\ H \trianglelefteq A}} A \right\rangle$; tojest, $A \leq \mathcal{N}_G(H)$, za svaku podgrupu A od G takvu da je H u njoj normalna podgrupa.)

2. Homomorfizmi grupa

Ovaj odjeljak sadrži tri osnovna rezultata o homomorfizmima među grupama; to su tzv. *Teoremi o izomorfizmima.* Naglasimo kako se važnost tih teorema, u Teoriju grupa, ne može precijeniti!

Od sada nadalje koristimo sljedeću skraćenu notaciju za grupe:

$$\begin{aligned} \mathbb{R} &\equiv (\mathbb{R},+); &&\text{analogno } \mathbb{Z},\mathbb{Q},\mathbb{C}\\ \mathbb{R}^\times &\equiv (\mathbb{R}^\times,\cdot); &&\text{analogno } \mathbb{Q}^\times,\mathbb{C}^\times\\ \mathbb{R}_+ &\equiv (\mathbb{R}_+,\cdot) &&\Big(\equiv \big((0,+\infty),\cdot\big)\Big). \end{aligned}$$

Već smo se sreli sa nekim homomorfizmima grupa. Naprimjer:

- $\exp : \mathbb{R} \to \mathbb{R}^\times \quad (\operatorname{Im}\exp = \mathbb{R}_+)$.
- $\det : \mathrm{GL}_n(\mathbb{K}) \to \mathbb{K}^\times$ je epimorfizam; nije mono-, jer $\operatorname{Ker}\det = \mathrm{SL}_n(\mathbb{K})$.
- Ako su V i W vektorski prostori nad poljem $\mathbb{K}$, onda su posebno $(V,+)$ i $(W,+)$ aditivne abelove grupe. Preslikavanje $f : V \to W$ je *linearan operator* ako je f *aditivan* i *homogen.* Ali aditivnost znači točno to da je f homomorfizam aditivnih grupa.

Zadatak 17. (i) Dokažite da je za proizvoljan $n \in \mathbb{Z}$ preslikavanje $f = f_n : \mathbb{Z} \to \mathbb{Z}$, $f(x) := nx$, monomorfizam; nije epi- za $n \neq \pm 1$.
(ii) Preslikavanje $\varepsilon : \mathbb{R} \to S^1 := \{z \in \mathbb{C} \mid |z| = 1\}$, $\varepsilon(x) := e^{2\pi\imath x}$, je epimorfizam, ali nije mono-. Što je $\operatorname{Ker}\varepsilon$?

Primjer 2.1. (1) Za bilo koju grupu G i proizvoljan $g \in G$ definirajmo **konjugiranje** sa elementom g sa

$$I_g : G \to G, \quad I_g(x) := gxg^{-1}.$$

Jasno je da $I_g \in \operatorname{Aut} G$; svaki takav I_g zove se **unutarnji automorfizam** od G. Označimo

$$\operatorname{Int} G := \{I_g \mid g \in G\}.$$

Budući je $I_{g_1} \circ I_{g_2} = I_{g_1g_2}$ i $(I_g)^{-1} = I_{g^{-1}}$, za $g, g_1, g_2 \in G$, $\operatorname{Int} G$ je podgrupa od $\operatorname{Aut} G$; zovemo ju **grupa unutarnjih automorfizama** od G. Kažimo ovdje i da se svaki automorfizam $\alpha \in \operatorname{Aut} G \setminus \operatorname{Int} G$, tojest svaki automorfizam koji nije unutarnji, zove **vanjski automorfizam** od G.

(2) Za proizvoljnu komutativnu grupu G, *invertiranje* $\mathcal{I} : G \to G$, $\mathcal{I}(x) := x^{-1}$, je automorfizam od G.

Zadatak 18. Dokažite da je $\operatorname{Int} G \trianglelefteq \operatorname{Aut} G$.

Zadatak 19. Ako je $G = \mathrm{SL}_2(\mathbb{K})$, da li je preslikavanje $f(X) := \mathcal{I}(X)^t$ iz $\operatorname{Int} G$? (Ovdje je $\mathcal{I} : G \to G$ invertiranje, a "t" označava transponiranje na matricama.)

Zadatak 20. Neka je $f : G \to H$ epimorfizam grupa i neka je $G_1 \leq G$ neka podgrupa takva da je $\operatorname{Ker} f \leq G_1$. Dokažite da je $f^{-1}(f(G_1)) = G_1$.

Sada ćemo dokazati prvi od tri važna teorema o izomorfizmima.

Teorem 2.2. (Prvi teorem o izomorfizmu)
Neka je $f : G \to H$ *proizvoljan homomorfizam grupa. Tada je* $\operatorname{Ker} f \trianglelefteq G$, $\operatorname{Im} f \leq H$ *i preslikavanje*

$$\overline{f} : G/\operatorname{Ker} f \to \operatorname{Im} f, \qquad \overline{f}(g \operatorname{Ker} f) := f(g),$$

je (dobro definiran) izomorfizam grupa; tojest,

$$G/\operatorname{Ker} f \cong \operatorname{Im} f.$$

Dokaz. (Usp. Korolar 1.29) Dokažimo prvu tvrdnju, da je $N := \operatorname{Ker} f$ normalna podgrupa od G. U tu svrhu primjetimo najprije da je, po definiciji jezgre, $n \in N \Leftrightarrow f(n) = e_H$. Onda za bilo koji $x \in G$ imamo:

$$f(xnx^{-1}) = f(x)f(n)f(x^{-1}) = f(x)e_H f(x^{-1}) = f(x)f(x^{-1}) = f(xx^{-1}) = f(e_G) = e_H;$$

tojest, imamo

$$xnx^{-1} \in N, \qquad \forall n \in N, \forall x \in G.$$

Drugim riječima, za svaki $x \in G$ je $xNx^{-1} \subseteq N$, što po definiciji normalne podgrupe znači $N \trianglelefteq G$.

Sada ćemo pokazati da je $\operatorname{Im} f$ podgrupa od H. (Općenito, to ne mora biti normalna podgrupa!). U tu svrhu uzmimo proizvoljne $\alpha, \beta \in \operatorname{Im} f$ i pokažimo da je $\alpha\beta^{-1} \in \operatorname{Im} f$; po "kriteriju podgrupe", imat ćemo $\operatorname{Im} f \leq H$. Za to vidjeti, neka su $a, b \in G$ bilo koji elementi takvi da je $f(a) = \alpha$ i $f(b) = \beta$ (takvi a i b postoje, općenito nejedinstveni, po definiciji slike $\operatorname{Im} f$). No onda imamo

$$\alpha\beta^{-1} = f(ab^{-1}) \in f(G) = \operatorname{Im} f,$$

što smo i tvrdili.

Dalje, pokažimo da je preslikavanje $\overline{f}$ *dobro definirano*, drugim riječima, da vrijednost $\overline{f}(gN)$ ne ovisi o izboru reprezentanta g koji definira klasu $gN \in G/N$. Pa neka su g i g' neka dva reprezentanta neke klase iz G/N. Onda imamo

$$\begin{aligned} gN = g'N \;&\Leftrightarrow\; g^{-1}g' \in N \;\Leftrightarrow\; f(g^{-1}g') = e_H \\ &\Leftrightarrow\; f(g)^{-1}f(g') = e_H \;\Leftrightarrow\; f(g') = f(g) \;\Leftrightarrow\; \overline{f}(gN) = \overline{f}(g'N); \end{aligned}$$

dakle doista definicija $\overline{f}$ ne ovisi o izboru reprezentanta klase, kako smo i tvrdili.

Još preostaje vidjeti da je $\overline{f}$ izomorfizam. Da je homomorfizam, slijedi odmah iz definicije množenja u kvocijentnoj grupi G/N. Isto tako, jasno je da je $\overline{f}$ surjekcija; naime, za $h \in \operatorname{Im} f$ proizvoljan postoji bar jedan $g \in G$ takav da je $f(g) = h$, i onda je $\overline{f}(gN) = h$. Za injektivnost od $\overline{f}$ dovoljno je vidjeti da je $\operatorname{Ker} \overline{f} = \{e_{G/N}\} = \{N\}$. Ali za $g \in G$ takav da je $\overline{f}(gN) = f(g) = e_H$ je, po definiciji jezgre, $g \in \operatorname{Ker} f = N \Leftrightarrow gN = N$; što smo i tvrdili. Time je teorem u potpunosti dokazan. □

Zadatak 21. Dokažite da za proizvoljnu grupu G imamo

$$G/\mathcal{Z}(G) \cong \operatorname{Int} G.$$

Primjer 2.3. (1) Koristeći činjenice da je determinanta $\det : \mathrm{GL}_n(\mathbb{K}) \to \mathbb{K}^\times$ epimorfizam, te da je $\operatorname{Ker} \det = \mathrm{SL}_n(\mathbb{K})$, po Prvom teoremu o izomorfizmu slijedi

$$\mathrm{GL}_n(\mathbb{K}) / \mathrm{SL}_n(\mathbb{K}) \cong \mathbb{K}^\times.$$

(2) Za grupu $S^1 = \{z \in \mathbb{C} \mid |z| = 1\}$ imamo

$$S^1 \cong \mathbb{R}/\mathbb{Z}.$$

[[*Dokaz.* Definirajmo preslikavanje $\varepsilon : \mathbb{R} \to S^1$, $\varepsilon(x) := e^{2\pi \imath x}$; očito je to dobro definirano, tojest, $\varepsilon(x) \in S^1$ za svaki $x \in \mathbb{R}$. Nadalje, to je preslikavanje epimorfizam grupa. Ali nije monomorfizam; preciznije, imamo

$$\operatorname{Ker} \varepsilon = \{x \in \mathbb{R} \mid e^{2\pi \imath x} = \cos(2\pi x) + \imath \sin(2\pi x) = 1\} = \mathbb{Z}.$$

Slijedi, po Prvom teoremu o izomorfizmu, da je $\mathbb{R}/\operatorname{Ker} \varepsilon = \mathbb{R}/\mathbb{Z} \cong S^1$, kako smo i tvrdili.]]

(3) Prije smo definirali *grupu korijena iz* 1,

$$\Omega := \{z \in \mathbb{C} \mid \exists n \in \mathbb{N},\ z^n = 1\}.$$

Ako sada restringiramo gornje preslikavanje ε na $\mathbb{Q}$, tojest, gledamo $\varepsilon : \mathbb{Q} \to S^1$, onda imamo $\operatorname{Im} \varepsilon = \Omega$. Slijedi, jer je ponovo $\operatorname{Ker} \varepsilon = \mathbb{Z}$,

$$\Omega \cong \mathbb{Q}/\mathbb{Z}.$$

Idući nam je korak dokazati druga dva teorema o izomorfizmima. Kao pripremu za to dokažimo najprije ovu lemu.

Lema 2.4. *Neka je G grupa, $A \leq G$ neka podgrupa i $N \trianglelefteq G$ neka normalna podgrupa. Tada je*

$$\langle A \cup N \rangle = AN;$$

posebno, AN je podgrupa od G.

Dokaz. Prvo primjetimo sljedeće: Za sve $\alpha \in A$ i $\nu \in N$ imamo

$$\nu\alpha = \alpha\nu', \qquad \text{gdje je } \nu' := \alpha^{-1}\nu\alpha \in N. \tag{2}$$

Sada, za dokaz leme, trebamo pokazati ovu tvrdnju: Svaki $x \in \langle A \cup N \rangle$ može se napisati u obliku

$$x = a\,n, \qquad \text{za neke } a \in A \text{ i } n \in N.$$

No da bismo to vidjeli, za početak napišimo x u obliku $x = x_1 \cdots x_k$, za neke $x_i \in A \cup N$ (vidi Zadatak 8 i Napomenu 1.19). Tu, jasno, smijemo pretpostaviti da su ti x_i-ovi naizmjence iz A, odnosno N. Preciznije, da su $x_1, x_3, \ldots \in A$ i $x_2, x_4, \ldots \in N$, ili pak obratno, tojest, $x_1, x_3, \ldots \in N$ i $x_2, x_4, \ldots \in A$. Pretpostavimo da imamo npr. drugu mogućnost i onda, da bismo lakše vidjeli o čemu se radi, označimo

$$x_1 = n_1,\ x_3 = n_2,\ x_5 = n_3, \ldots \qquad \text{i} \qquad x_2 = a_1,\ x_4 = a_2,\ x_6 = a_3, \ldots;$$

dakle, $x = n_1 a_1 n_2 a_2 \ldots$ za neke $n_i \in N$ i $a_i \in A$. Sada, po (2), imamo $x = a_1 n_1' n_2 a_2 \ldots$, gdje je $n_1' := a_1^{-1} n_1 a_1$. Sada označimo $\nu_2 := n_1' n_2$, pa je onda $x = a_1 \nu_2 a_2 \ldots$. Primjenimo isti "trik" i napišimo, ponovo po (2), $\nu_2 a_2 = a_2 \nu_2'$, gdje je $\nu_2' \in N$; sada je $x = a_1 a_2 \nu_2' n_3 \ldots$. Očito, nakon konačno koraka, x ćemo napisati kao $x = an$, gdje je $a = a_1 a_2 \ldots$ i n je produkt nekih elemenata iz N; svakako, $a \in A$ i $n \in N$, kako smo i tvrdili. $\square$

Primjetimo da gornja lema ne mora vrijediti ukoliko obje podgrupe, A i N, nisu normalne u G. Sasvim precizno, pogledajmo sljedeći jednostavan primjer.

Primjer 2.5. Neka je grupa $G = \mathcal{S}_3$, simetrična grupa na skupu $\{1,2,3\}$. Promatrajmo permutacije, reda 2,

$$\boldsymbol{x} := \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \qquad \boldsymbol{y} := \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}.$$

Ako sa **1** označimo identitetu, onda su sa

$$X := \{\mathbf{1}, \boldsymbol{x}\}, \qquad Y := \{\mathbf{1}, \boldsymbol{y}\},$$

definirane dvije podgrupe, reda 2, od G. Sada,

$$XY = \{\mathbf{1}, \boldsymbol{x}, \boldsymbol{y}, \boldsymbol{xy}\}$$

očito nije podgrupa od G (jer npr., imajući na umu Lagrangeov teorem, 4 ne dijeli 6, red od G); ovdje je $\boldsymbol{xy} := \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$. (Jasno, podgrupe $X, Y \leq G$ obje nisu normalne, što se lako može vidjeti i direktnom provjerom.)

Sada ćemo dokazati tzv. Drugi teorem o izomorfizmu.

Teorem 2.6. (Drugi teorem o izomorfizmu)
Neka je G grupa, $A \leq G$ neka podgrupa i $N \trianglelefteq G$ neka normalna podgrupa. Tada je

$$A/A \cap N \cong AN/N.$$

Dokaz. Prvo primjetimo da je, po prethodnoj lemi, AN grupa; i, jasno, $N \trianglelefteq AN$. Dalje, definirajmo preslikavanje $\phi : A \to AN/N$ kao $\phi(a) := aN$, za $a \in A$. Očito je ϕ homomorfizam grupa, i surjektivan je; tojest, to je epimorfizam. Njegova je jezgra jednaka

$$\operatorname{Ker} \phi = A \cap N.$$

[[Naime, za $x \in A$ imamo $x \in \operatorname{Ker} \phi$ akko $\phi(x) = xN = N$ akko $x \in N$; drugim riječima, x je u jezgri od ϕ akko je $x \in A$ i $x \in N$, tojest, $x \in A \cap N$.]]
Sada, konačno, po Prvom teoremu o izomorfizmu slijedi da je

$$A/\operatorname{Ker} \phi \cong AN/N;$$

time je teorem dokazan. □

Sljedeća je propozicija potrebna za dokaz tzv. Trećeg teorema o izomorfizmu, ali je i sama za sebe interesantna. Ona daje preciznu vezu između (normalnih) podgrupa u kvocijentu G/N i onih (normalnih) podgrupa u G koje sadrže N; ovdje je, jasno, $N \trianglelefteq G$.

Propozicija 2.7. *Neka je G proizvoljna grupa i neka je $N \trianglelefteq G$ neka normalna podgrupa. Uz oznaku $\overline{G} := G/N$, preslikavanje*

$$\begin{aligned} \Phi : \{H \mid H \leq G \ \& \ N \leq H\} &\longrightarrow \{\overline{H} \mid \overline{H} \leq \overline{G}\}, \\ H &\longmapsto H/N, \end{aligned}$$

je monotona *bijekcija; ovdje monotonost znači da za dvije podgrupe H_1 i H_2 od G, koje obje sadrže N, imamo $H_1 \leq H_2$* akko *$\Phi(H_1) \leq \Phi(H_2)$.*

Nadalje, $H \trianglelefteq G$ akko je $\overline{H} \trianglelefteq \overline{G}$.

Dokaz. Neka je $\pi : G \to \overline{G}$ kanonski epimorfizam. Za $\overline{H} \leq \overline{G}$, definirajmo H kao prasliku od $\overline{H}$ po π, tojest,

$$H := \pi^{-1}(\overline{H}) = \{g \in G \mid gN \in \overline{H}\}.$$

Tada je jasno da vrijedi sljedeće:

(**1**) $H \leq G$, tojest, H je podgrupa od G;
(**2**) $N \leq H$, tojest, H sadrži N;
(**3**) $\pi(H) = \overline{H}$ (jer je π surjekcija).

To znači da je doista Φ bijektivno preslikavanje; njegov je inverz $\Phi^{-1} : \overline{H} \mapsto H := \pi^{-1}(\overline{H})$.

Nadalje, ako je $N \leq H \trianglelefteq G$, onda za svaki $g \in G$ imamo:

$$gN\overline{H}(gN)^{-1} = \{ghg^{-1}N \mid h \in H\} = \{h'N \mid h' \in H\} = H/N = \overline{H};$$

tojest, doista je $\overline{H} \trianglelefteq \overline{G}$. Slično se vidi i obratna implikacija; tojest, ako je $\overline{H} \trianglelefteq \overline{G}$, onda je $\pi^{-1}(\overline{H}) = H \trianglelefteq G$. Time je propozicija dokazana. $\square$

Konačno, dokažimo i tzv. Treći teorem o izomorfizmu. Grubo govoreći, taj teorem kaže da se kvocijentne strukture grupa smiju "kratiti", kao što to radimo sa dvostrukim razlomcima u $\mathbb{Q}$.

Teorem 2.8. (Treći teorem o izomorfizmu)
Neka je G grupa i neka su $M, N \trianglelefteq G$ dvije normalne podgrupe takve da je $N \leq M$. Tada je

$$(G/N)\big/(M/N) \cong G/M.$$

Dokaz. Najprije primjetimo da je, po prethodnoj propoziciji, $M/N \trianglelefteq G/N$; posebno, lijeva strana u gore napisanom izomorfizmu ima smisla. Sada, za kanonski epimorfizam $\pi = \pi_M : G \to G/M$ imamo $N \leq \operatorname{Ker}\pi = M$. Faktorizacijom π kroz N (vidi Korolar 1.29), dobijemo homomorfizam

$$\overline{\pi} : G/N \to G/M,$$
$$\overline{\pi}(xN) := xM;$$

jasno, $\overline{\pi}$ je, štoviše, epimorfizam. Po Prvom teoremu o izomorfizmu, imamo

$$(G/N)\big/\operatorname{Ker}\overline{\pi} \cong G/M = \operatorname{Im}\overline{\pi}.$$

Preostaje još samo pokazati sljedeću tvrdnju:

$$\operatorname{Ker}\overline{\pi} = M/N.$$

[[Doista, ponovo koristeći prethodnu propoziciju, znamo da je $\operatorname{Ker}\overline{\pi} = H/N$, za neku podgrupu H takvu da je $N \leq H \trianglelefteq G$. Ali, za svaki $x \in H$ imamo:

$$eM = M = \overline{\pi}(xN) = xM \quad \Rightarrow \quad x \in M.$$

Znači, imamo $H \subseteq M$. Ali, s druge strane, očito imamo i obratnu inkluziju, tojest, $M \subseteq H$; dakle, imamo i jednakost $M = H$. Slijedi $\operatorname{Ker}\overline{\pi} = M/N$, kako smo i tvrdili.]]
Time je teorem dokazan. $\square$

Sljedeći je rezultat, također, sam za sebe interesantan; to je generalizacija Korolara 1.29, koji smo koristili u gornjem dokazu. (Za $N_2 = \{e_G\}$ dobijemo Korolar 1.29.)

Propozicija 2.9. *Neka su* G_1, G_2 *grupe i neka su* $N_i \trianglelefteq G_i$ *normalne podgrupe, za* $i = 1, 2$. *Pretpostavimo da je* $f : G_1 \to G_2$ *neki homomorfizam takav da je* $f(N_1) \subseteq N_2$. *Tada je preslikavanje*

$$\begin{aligned} &F : G_1/N_1 \to G_2/N_2, \\ &F(xN_1) := f(x)N_2 \qquad x \in G_1, \end{aligned}$$

homomorfizam grupa. Drugim riječima, imamo komutativan dijagram

$$\begin{array}{ccc} G_1 & \xrightarrow{f} & G_2 \\ {\scriptstyle \pi_1}\big\downarrow & & \big\downarrow{\scriptstyle \pi_2} \\ G_1/N_1 & \xrightarrow{F} & G_2/N_2 \ ; \end{array}$$

tojest, $\pi_2 \circ f = F \circ \pi_1$.

Dokaz. Dati ćemo dva dokaza. (Iako, zapravo, prvi (direktan) dokaz daje argument koji kao specijalan slučaj dokazuje Korolar 1.29, koji pak onda koristimo u drugom dokazu propozicije.)

1. Dokaz.

(F dobro definiran)

Ako je $xN_1 = x'N_1 \Leftrightarrow x' = xn_1$, za $n_1 \in N_1$, onda imamo

$$f(x') = f(x)\, f(n_1) \in f(x)N_2 \qquad (\text{jer je } n_2 := f(n_1) \in N_2),$$

a to je dalje ekvivalentno

$$f(x')N_2 = f(x)N_2 \iff F(x'N_1) = F(xN_1)$$

(kod zadnje ekvivalencije koristili smo samo definiciju od F).

Jasno je da je F i homomorfizam grupa.

2. Dokaz.

Za kanonski epimorfizam $\pi_2 : G_2 \to G_2/N_2$ je i preslikavanje

$$\varphi := \pi_2 \circ f : G_1 \to G_2/N_2,$$

kao kompozicija dva homomorfizma, također homomorfizam grupa. Budući je

$$\varphi(N_1) = (\pi_2 \circ f)(N_1) \subseteq \pi_2(N_2) = e_{G_2/N_2} \implies N_1 \subseteq \operatorname{Ker} \varphi,$$

prema Korolaru 1.29 slijedi da postoji jedinstven homomorfizam $\overline{\varphi} : G_1/N_1 \to G_2/N_2$, koji se dobije faktorizacijom φ kroz N_1. Jasno, $\overline{\varphi} = F$. □

(* * *)

Na kraju ovog odjeljka dajemo još neke zadatke o grupama i homomorfizmima.

Zadatak 22. Neka je G grupa i pretpostavimo da su $A, B \leq G$ dvije podgrupe takve da niti A sadrži B, niti B sadrži A. Dokažite da onda skup $A \cup B$ nije podgrupa od G.

Zadatak 23. Neka je G grupa i neka su $A, B \leq G$ dvije podgrupe. Dokažite da vrijedi ekvivalencija: Kompleks AB je podgrupa od G akko imamo $AB = BA$.

Zadatak 24. Neka je G grupa i neka su $M, N \trianglelefteq G$ neke dvije normalne podgrupe. Dokažite da je $MN \trianglelefteq G$.

Primjetimo sljedeće: Podgrupa $N \leq G$ je normalna ako imamo

$$\alpha(N) \subseteq N \qquad \forall \alpha \in \operatorname{Int} G,$$

tojest, ako je $I_g(N) = gNg^{-1} \subseteq N$ za sve $g \in G$. U vezi s tim uvodimo ovu definiciju: Podgrupa $K \leq G$ je **karakteristična podgrupa** od G ako je

$$\alpha(K) \subseteq K \qquad \forall \alpha \in \operatorname{Aut} G.$$

Primjetimo isto tako da je svaka karakteristična podgrupa od G ujedno i normalna podgrupa od G. Međutim, obratno općenito ne vrijedi; tojest, postoje grupe G i neke njihove normalne podgrupe N koje nisu u isto vrijeme i karakteristične podgrupe. (Jasno, za takove grupe G je inkluzija $\operatorname{Int} G \subseteq \operatorname{Aut} G$ prava!)

Zadatak 25. Dokažite: Ako je G grupa, $H \trianglelefteq G$ neka normalna podgrupa i $K \leq H$ karakteristična, u H, podgrupa, onda je $K \trianglelefteq G$.

U vezi s prethodnim zadatkom primjetimo sljedeće: Relacija "biti normalna podgrupa" nije tranzitivna. Precizno rečeno, postoje grupe $M \leq N \leq G$ takve da je $M \trianglelefteq N$ i $N \trianglelefteq G$, ali M *nije* normalna podgrupa od G.

Sljedeći zadatak pokazuje da grupa automorfizama neke dosta jednostavne komutativne grupe može biti "dosta velika" nekomutativna grupa. Isto tako primjetimo, uz oznake kao u zadatku, da je grupa $\operatorname{Int}(\mathbb{Z} \oplus \mathbb{Z})$ trivijalna, tojest, jednaka $\{1_{\mathbb{Z}\oplus\mathbb{Z}}\}$; drugim riječima, tu su svi netrivijalni automorfizmi vanjski. (Zapravo, općenito, ako je A abelova grupa, onda je grupa unutarnjih automorfizama od A trivijalna.)

Zadatak 26.* Definirajmo

$$G := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \;\middle|\; a, b, c, d \in \mathbb{Z} \;\&\; ad - bc \in \{\pm 1\} \right\};$$

jasno, G je grupa. Dokažite:

$$\operatorname{Aut}(\mathbb{Z} \oplus \mathbb{Z}) \cong G.$$

Ovdje je $\mathbb{Z} \oplus \mathbb{Z} := \{(z, w) \mid z, w \in \mathbb{Z}\}$, uz operaciju zbrajanja parova "po komponentama"; to je, u terminologiji sljedećeg odjeljka, direktna suma $\mathbb{Z}$ sa $\mathbb{Z}$.

Zadatak 27. Neka je G grupa, $H \leq G$ neka podgrupa i $G_1 \trianglelefteq G$ neka normalna podgrupa. Pretpostavimo da su obje grupe G_1 i G/G_1 abelove. Dokažite: Postoji grupa H_1 takva da je $H_1 \trianglelefteq H$, te da su grupe H_1 i H/H_1 obje abelove. (*Uputa:* $H_1 := G_1 \cap H$.)

Zadatak 28. Dokažite: Ako je G konačna grupa i ako je $H \leq G$ podgrupa indeksa $(G : H) = 2$, onda je $H \trianglelefteq G$. Vrijedi li nužno ista tvrdnja ukoliko je grupa G beskonačna?

U svezi sa prethodnim zadatkom primjetimo da se rečeni rezultat ne može poopćiti na neki "dobar" način. Naime, rezultat ne vrijedi ako se gore namjesto indeksa 2 uzme npr. indeks 3. (Recimo, u simetričnoj grupi $\mathcal{S}_3$, koja je reda 6, postoje 3 podgrupe reda 2 koje nisu normalne u $\mathcal{S}_3$ (vidi Primjer 2.5); jasno, te su podgrupe indeksa 3.)

Zadatak 29. Neka je G grupa i $\varphi : G \to G$ preslikavanje definirano sa $\varphi(x) := x^2$. Dokažite da je φ endomorfizam akko je grupa G abelova. Nadalje, odredite indeks $(G : \varphi(G))$ u sljedećim slučajevima: $G = \mathbb{R}_+$, $\mathbb{R}^\times$, $\mathbb{Q}^\times$.

(*Uputa:* Za $G = \mathbb{Q}^\times$ pretpostavite da postoje $q_1, \dots q_n \in G$ takvi da je $G = q_1\varphi(G) \cup \dots \cup q_n\varphi(G)$, disjunktna unija. Zatim uzmite $p \in \mathbb{N}$ prim broj takav da p ne dijeli niti brojnik niti nazivnik od q_i, za $i = 1, \dots, n$.)

3. Direktan i semidirektan produkt grupa

Kao što smo već rekli, kad imamo neke algebarske strukture, osnovno je pitanje kako iz njih dobiti neke nove strukture iste vrste. Jednu od konstrukcija za grupe smo upoznali; to je dobivanje kvocijentne grupe G/N neke grupe G po nekoj njezinoj (netrivijalnoj) normalnoj podgrupi N. Sada ćemo pokazati kako od familije grupa dobiti tzv. produkt tih grupa, odnosno sumu grupa. Posebno, za slučaj kada imamo samo dvije grupe, pojam njihovog produkta će se dalje generalizirati; to će biti tzv. semidirektan produkt tih grupa.

3.1. Direktan produkt.

Najprije ćemo uvesti pojam direktnog produkta. Zapravo, sa konstrukcijom produkta grupa smo se već sreli. Naprimjer, $\mathbb{R}^2 = \mathbb{R} \times \mathbb{R}$, $\mathbb{R}^n = \mathbb{R}^{n-1} \times \mathbb{R}$, $\mathbb{C}^n$, ... Da bismo lakše razumijeli ono što slijedi, započnimo sa slučajem kada imamo samo dva faktora. Neka su G, H grupe i definirajmo Kartezijev produkt (skupova) $G \times H$ i operaciju "množenja po komponentama" na $G \times H$ ovako:

$$(g_1, h_1) \cdot (g_2, h_2) := (g_1 g_2, h_1 h_2).$$

Tako je dobivena na $G \times H$ struktura grupe; zovemo ju *direktan produkt grupa* G i H.

Napomena 3.1. Primjetimo da za $G \times H$ vrijedi sljedeće:

(1) $e_{G\times H} = (e_G, e_H)$, neutralni element u $G \times H$;
(2) $(g^{-1}, h^{-1}) = (g, h)^{-1}$, inverzni element od $(g, h) \in G \times H$;
(3) $G \times H$ je abelova grupa akko su i G i H abelove grupe;
(4) $|G \times H| = |G|\,|H|$;
(5) Imamo izomorfizme

$$G \cong G \times \{e_H\} = \{(g, e_H) \mid g \in G\} \leq G \times H,$$
$$H \cong \{e_G\} \times H = \{(e_G, h) \mid h \in H\} \leq G \times H;$$

tako podrazumijevamo, uz identifikaciju $G \equiv G \times \{e_H\}$ i $H \equiv \{e_G\} \times H$,

$$G, H \leq G \times H.$$

Štoviše, to su i normalne podgrupe; tj.,

$$G, H \trianglelefteq G \times H.$$

Nadalje, jasno je i da vrijedi

$$G \cap H = \{e_{G\times H}\} \qquad \text{i} \qquad \langle G \cup H \rangle = G \times H.$$

Neka je sada $\{G_i \mid i \in I\}$ proizvoljna familija grupa; sa $e_i \in G_i$ ćemo označavati pripadne neutralne elemente u tim grupama.

Definicija 3.2. Kartezijev produkt

$$\prod_{i\in I} G_i := \{f : I \to \bigcup_{i\in I} G_i \mid f(i) \in G_i\},$$

uz operaciju "množenja po komponentama"

$$(f \cdot g)(i) := f(i) \cdot g(i),$$

zove se **direktan produkt grupa** $\{G_i\}_I$.

Podgrupa

$$\bigoplus_{i \in I} G_i := \{f \in \prod_{i \in I} G_i \mid f(i) \neq e_i \text{ za konačno mnogo } i \in I\},$$

od direktnog produkta $\prod_I G_i$, zove se **direktna suma grupa** $\{G_i\}_I$.

Primjetimo da smo u gore definiranim objektima doista dobili strukturu grupe. Naime, ako je f neka funkcija iz $\prod_I G_i$, onda je sa $I \ni i \mapsto f(i)^{-1} \in G_i$ definiran inverz f^{-1} od f. Nadalje, sa $\boldsymbol{e}(i) := e_i$ za svaki $i \in I$, definiran je neutralni element od $\prod_I G_i$. Asocijativnost je posljedica definicije množenja i činjenice da isto svojstvo vrijedi u svakoj G_i. Da bismo se uvjerili da je i $\bigoplus_I G_i$ također grupa, jedino što moramo vidjeti je da je taj skup zatvoren za definirano množenje po komponentama. Ali, ako su $f, g \in \bigoplus_I G_i$, onda postoje konačni podskupovi $J_f, J_g \subseteq I$ takvi da je $f(i) = e_i$ za svaki $i \in I \setminus J_f$ i $g(i) = e_i$ za svaki $i \in I \setminus J_g$. No onda je, očito, i $(f \cdot g)(i) = e_i$ za svaki $i \in I \setminus (J_f \cup J_g)$; tj., $(f \cdot g)(i) \neq e_i$ za najviše konačno i-ova.

Napomena 3.3. (1) Ako je skup indeksa I konačan, bez smanjenja općenitosti možemo uzeti $I = \{1, 2, \ldots, n\}$. I onda je

$$G_1 \times \cdots \times G_n = \prod_{i=1}^{n} G_i = \bigoplus_{i=1}^{n} G_i = G_1 \oplus \cdots \oplus G_n.$$

Sada elemente produkta, tj. sume grupa G_i, zapisujemo kao n-torke $(g_1, \ldots, g_n)$, $g_i \in G_i$, i onda je množenje doista "uobičajeno" množenje po komponentama,

$$(g_1, \ldots, g_n) \cdot (g'_1, \ldots, g'_n) = (g_1 g'_1, \ldots, g_n g'_n).$$

Naravno, neutral je $(e_1, \ldots, e_n)$, a inverz od nekog $(g_1, \ldots, g_n)$ je $(g_1^{-1}, \ldots, g_n^{-1})$.

(2) Podskup

$$\widetilde{G}_j := \{f \in \bigoplus_I G_i \mid f(i) = e_i \qquad \forall i \neq j\}$$

je podgrupa od direktne sume $\bigoplus_I G_i$, i očito je $\widetilde{G}_j \cong G_j$; tako te grupe identificiramo i podrazumijevamo da je G_j podgrupa od $\bigoplus_I G_i$. Preciznije, preslikavanje

$$\boldsymbol{\imath}_j : G_j \hookrightarrow \bigoplus_I G_i \qquad \forall j,$$

definirano na evidentan način, je *ulaganje*; tj., injektivan homomorfizam grupa. Kažemo da je $\boldsymbol{\imath}_j$ **j-ta kanonska injekcija**.

Slijedi važan rezultat o "*karakterizaciji direktne sume grupa*".

Teorem 3.4. *Neka je G grupa i neka su $G_i \leq G$, $i \in I$, neke njezine podgrupe za koje vrijede sljedeća tri uvjeta:*

(1) $G_i \trianglelefteq G$, $\forall i \in I$;
(2) $G_j \cap \langle \bigcup_{i \neq j} G_i \rangle = \{e\}$, $\forall j \in I$;

(**3**) $G = \langle \bigcup_I G_i \rangle$.

Tada je

$$G \cong \bigoplus_I G_i.$$

DOKAZ. Bez smanjenja općenitosti možemo pretpostaviti da je skup indeksa I konačan, tj. da je $I = \{1, 2, \ldots, n\}$ i onda $\bigoplus_I G_i = G_1 \oplus \cdots \oplus G_n$; sa e_i označimo neutralni element od G_i. (Za proizvoljan I je dokaz sasvim isti onom koji slijedi, samo što namjesto sa n-torkama $(g_1, \ldots, g_n)$ moramo raditi sa funkcijama $f \in \bigoplus_I G_i$.)

Neka vrijede uvjeti $(\mathbf{1}) - (\mathbf{3})$, pa dokažimo da je onda $G \cong \bigoplus_I G_i$. Precizno, pokažimo da vrijedi

Tvrdnja. Preslikavanje

$$\phi : G_1 \oplus \cdots \oplus G_n \to G, \qquad \phi(g_1, \ldots, g_n) := g_1 \cdots g_n,$$

je izomorfizam grupa; tj., traženi se izomorfizam $G \cong \bigoplus_I G_i$ realizira posredstvom ϕ.

[[Najprije primjetimo da vrijedi

$$(\star) \qquad g_i g_j = g_j g_i, \qquad \forall\, i \neq j.$$

Da to vidimo, definirajmo komutator $\omega := g_i\, g_j\, g_i^{-1} g_j^{-1}$. Ako napišemo $\omega = (g_i\, g_j\, g_i^{-1}) g_j^{-1}$, budući po (**1**) imamo $g_i\, g_j\, g_i^{-1} \in G_j$, to je $\omega \in G_j$. Ali isto tako, ako pak napišemo ω u obliku $\omega = g_i(g_j\, g_i^{-1} g_j^{-1})$, isti argument daje $\omega \in G_i$. Znači, imajući u vidu uvjet (**2**),

$$\omega \in G_j \cap G_i \subseteq G_j \cap \langle \bigcup_{k \neq j} G_k \rangle = \{e\} \quad \Longrightarrow \quad \omega = e;$$

tako je $(\star)$ dokazano.]]

(ϕ homomorfizam)

Za dvije n-torke $(x_1, \ldots, x_n)$ i $(y_1, \ldots, y_n)$, imamo

$$\phi\big((x_1, \ldots, x_n)(y_1, \ldots, y_n)\big) = \phi(x_1 y_1, \ldots, x_n y_n) = x_1 y_1 \cdots x_n y_n.$$

Sada, koristeći višestruko $(\star)$, imamo

$$\begin{aligned} x_1 y_1 x_2 y_2 x_3 y_3 \cdots x_n y_n &= x_1 (y_1 x_2) y_2 x_3 y_3 \cdots x_n y_n = x_1 x_2 y_1 y_2 x_3 y_3 \cdots x_n y_n = \\ &= \cdots \quad \cdots = (x_1 x_2 \cdots x_n)(y_1 y_2 \cdots y_n) \\ &= \phi(x_1, \ldots, x_n) \phi(y_1, \ldots, y_n). \end{aligned}$$

(Ovdje, zapravo, koristimo induktivni argument po n.) Slijedi da je ϕ doista homomorfizam grupa.

(ϕ monomorfizam)

Sada kada znamo da je ϕ homomorfizam, njegova injektivnost je ekvivalentna tomu da je jezgra $\operatorname{Ker} \phi$ trivijalna. Pa pretpostavimo onda

$$\phi(g_1, \ldots, g_n) = e \quad \Leftrightarrow \quad g_1 \cdots g_n = e \quad \Leftrightarrow \quad g_n^{-1} = g_1 \cdots g_{n-1} := \omega.$$

Ali, kako po (**2**) imamo $\omega \in G_n \cap \langle \bigcup_{j \neq n} G_j \rangle = \{e\}$, slijedi $\omega = e$. Posebno je onda $g_n = e$ i $g_1 \cdots g_{n-1} = e$. Sada primjenimo sasvim isti argument, kao gore, na posljednju jednakost, tj. na $g_{n-1}^{-1} = g_1 \cdots g_{n-2}$. Onda ćemo dobiti $g_{n-1} = e$ i $g_1 \cdots g_{n-2} = e$. Induktivno nastavljajući, zaključujemo da je

$$g_1 = g_2 = \cdots = g_n = e;$$

što smo i trebali pokazati.

(ϕ epimorfizam)

Po ($\star$) i (**3**) slijedi, očito, da se svaki $x \in G$ može napisati u obliku

$$x = g_1 \cdots g_n, \qquad g_i \in G_i.$$

Sada primjetimo da je onda $\phi(g_1, \ldots, g_n) = x$; to je surjektivnost od ϕ.

Tako je teorem u potpunosti dokazan. $\square$

Primjer 3.5. (1) Imamo ovaj izomorfizam aditivnih grupa:

$$\mathbb{R} \oplus \mathbb{R} \cong \mathbb{C}.$$

(2) Imamo izomorfizam aditivnih grupa

$$\mathbb{Z}/m\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/mn\mathbb{Z},$$

ukoliko je najveća zajednička mjera $(m, n) = 1$; tj., m i n su relativno prosti.

[[*Dokaz:* Označimo $A = \mathbb{Z}/mn\mathbb{Z}$; to je abelova grupa čiji je jedan od generatora element $1 + mn\mathbb{Z}$. Definirajmo preslikavanja $\alpha_1 : \mathbb{Z}/m\mathbb{Z} \to A$ i $\alpha_2 : \mathbb{Z}/n\mathbb{Z} \to A$, dana sa $\alpha_1(k + m\mathbb{Z}) := kn + mn\mathbb{Z}$ i $\alpha_2(l + n\mathbb{Z}) := lm + mn\mathbb{Z}$. Ta preslikavanja su monomorfizmi grupa. Definirajmo podgrupe $A_1 := \alpha_1(\mathbb{Z}/m\mathbb{Z}) \hookrightarrow A$ i $A_2 := \alpha_2(\mathbb{Z}/n\mathbb{Z}) \hookrightarrow A$. Sada, mi tvrdimo da je

$$A_1 \oplus A_2 \cong A;$$

tj., $\mathbb{Z}/m\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z} \cong A$. Za to, najprije pokažimo da je

$$A_1 \cap A_2 = \{mn\mathbb{Z}\} \qquad \text{(neutral u grupi } A).$$

Da to vidimo, pretpostavimo da je $A_1 \ni kn + mn\mathbb{Z} = lm + mn\mathbb{Z} \in A_2$, za neke k i l; tj., $kn - lm \in mn\mathbb{Z}$. Slijedi, koristeći $(m, n) = 1$, da imamo

$$mn \mid kn - lm \quad \Rightarrow \quad m \mid kn \;\;\&\;\; n \mid lm \quad \Rightarrow \quad m \mid k \;\;\&\;\; n \mid l.$$

Dakle je $kn + mn\mathbb{Z} = lm + mn\mathbb{Z} = mn\mathbb{Z}$, što je i trebalo pokazati. Nadalje, pokažimo da je (vidi Lemu 2.4)

$$\langle A_1 \cup A_2 \rangle = A_1 + A_2 = A.$$

Da to vidimo treba se sjetiti da za relativno proste m i n postoje neki $k, l \in \mathbb{Z}$ takvi da je $kn + ml = 1$. (Dokažite to!) Kao očitu posljedicu imamo da onda postoje i neki $k_0 \in \{1, \ldots, m-1\}$ i $l_0 \in \{1, \ldots, n-1\}$ takvi da je

$$k_0 n + m l_0 \equiv 1 \pmod{mn} \quad \Longleftrightarrow \quad k_0 n + m l_0 + mn\mathbb{Z} = 1 + mn\mathbb{Z}.$$

To znači da $A_1 + A_2$ sadrži generator $1 + mn\mathbb{Z}$ grupe A, tj. imamo $A_1 + A_2 = A$, što je i trebalo pokazati. Po prethodnom teoremu, imamo sada $A_1 \oplus A_2 \cong A$.]]

Primjer 3.6. Podsjetimo se da je za proizvoljno polje $\mathbb{K}$ i proizvoljan $n \in \mathbb{N}$, $\mathrm{SL}_n(\mathbb{K}) \trianglelefteq \mathrm{GL}_n(\mathbb{K})$. Nadalje, ako je $\boldsymbol{I}$ jedinična n-puta-n matrica, onda je sa $x \mapsto x\boldsymbol{I}$ definiran izomorfizam grupa

$$\mathbb{K}^\times \cong \mathbb{K}^\times \boldsymbol{I} = \{x\boldsymbol{I} \mid x \in \mathbb{K}^\times\} \leq \mathrm{GL}_n(\mathbb{K});$$

posredstvom toga izomorfizma, smatramo da je $\mathbb{K}^\times$ podgrupa od $\mathrm{GL}_n(\mathbb{K})$. Štoviše, očito je $\mathbb{K}^\times \trianglelefteq \mathrm{GL}_n(\mathbb{K})$.

Neka je sada $\mathbb{K} = \mathbb{R}$ i n neparan broj. Primjetimo da se onda svaka matrica $A \in \mathrm{GL}_n(\mathbb{R})$ može napisati u obliku

$$A = \left(\sqrt[n]{\det A}\,\boldsymbol{I}\right)\left((1/\sqrt[n]{\det A})\,A\right);$$

ovdje je $\sqrt[n]{\det A}$ realni n-ti korijen iz $\det A$. Prvi faktor u gornjem rastavu je iz $\mathbb{R}^\times$, dok je drugi iz $\mathrm{SL}_n(\mathbb{R})$. Drugim riječima, imamo da je

$$\mathrm{GL}_n(\mathbb{R}) = \mathbb{R}^\times\ \mathrm{SL}_n(\mathbb{R}) = \langle \mathbb{R}^\times \cup \mathrm{SL}_n(\mathbb{R})\rangle.$$

Nadalje, uz istu pretpostavku da je n neparan, imamo ispunjen i uvjet

$$\mathbb{R}^\times \cap \mathrm{SL}_n(\mathbb{R}) = \{\boldsymbol{I}\};$$

naime, $x = 1$ je jedino rješenje u $\mathbb{R}$ od jednadžbe $\det(x\boldsymbol{I}) = x^n = 1$. Sada, po prethodnom teoremu, slijedi da je

$$\mathrm{GL}_n(\mathbb{R}) \cong \mathbb{R}^\times \times \mathrm{SL}_n(\mathbb{R}) = \mathbb{R}^\times \oplus \mathrm{SL}_n(\mathbb{R}).$$

3.2. Semidirektan produkt.

Neka su sada N i H neke grupe i pretpostavimo da je zadan neki *homomorfizam*

$$\varphi : H \to \mathrm{Aut}\, N, \qquad H \ni h \mapsto \varphi(h) \overset{\text{ozn.}}{=} \varphi_h \in \mathrm{Aut}\, N.$$

Definirajmo na Kartezijevom produktu

$$N \times H = \{(n,h) \mid n \in N,\ \ h \in H\}$$

ovo *množenje*:

$$(\diamondsuit) \qquad (n_1,h_1) * (n_2,h_2) := (n_1\varphi_{h_1}(n_2), h_1h_2).$$

Sljedeći rezultat govori da smo tako dobili strukturu grupe na $N \times H$; tj., imamo ovaj

Teorem 3.7. *$(N \times H, *)$ je grupa.*

Dokaz. (grupoidnost)

Iz gornje definicije množenja je jasno da je $N \times H$ zatvoren za $*$. Naime, jer je $\varphi_{h_1} \in \mathrm{Aut}\, N$ i $n_2 \in N$, to je isto i $\varphi_{h_1}(n_2) \in N$, a onda je i $n_1\,\varphi_{h_1}(n_2) \in N$. S druge strane, jasno je da je $h_1h_2 \in H$.

(asocijativnost)

Za tri para (n_i, h_i), $i = 1, 2, 3$, računamo:

$$\begin{aligned}
\big((n_1,h_1)*(n_2,h_2)\big)*(n_3,h_3) &\overset{(\diamondsuit)}{=} \big(n_1\varphi_{h_1}(n_2), h_1h_2\big)*(n_3,h_3) = \\
&\overset{(\diamondsuit)}{=} \big(n_1\varphi_{h_1}(n_2)\,\varphi_{h_1h_2}(n_3), (h_1h_2)h_3\big) = \\
&\qquad \text{(jer je } \varphi \text{ homomorfizam i } H \text{ grupa)} \\
&= \big(n_1\varphi_{h_1}(n_2)\,\varphi_{h_1}(\varphi_{h_2}(n_3)), h_1(h_2h_3)\big) = \\
&\qquad \text{(jer je } \varphi_{h_1} \text{ automorfizam)} \\
&= \big(n_1\,\varphi_{h_1}(n_2\,\varphi_{h_2}(n_3)), h_1(h_2h_3)\big) \\
&\overset{(\diamondsuit)}{=} (n_1,h_1)*\big(n_2\,\varphi_{h_2}(n_3), h_2h_3\big) = \\
&\overset{(\diamondsuit)}{=} (n_1,h_1)*\big((n_2,h_2)*(n_3,h_3)\big);
\end{aligned}$$

tako je asocijativnost dokazana.

(neutral)

Neutralni je element (e_N, e_H). Naime, za proizvoljan par $(n,h) \in N \times H$, po definiciji množenja $(\diamondsuit)$, imamo:

$$(e_N, e_H)*(n,h) = \big(e_N\,\varphi_{e_H}(n), e_H h\big) = (e_N\,n, h) = (n,h).$$

Ovdje smo koristili činjenicu da svaki homomorfizam grupa šalje neutral u neutral, pa je posebno za slučaj homomorfizma φ ispunjeno $\varphi_{e_H} = 1_N$, identiteta na N.

S druge strane, imamo:

$$(n,h)*(e_N,e_H) = \big(n\,\varphi_h(e_N), he_H\big) = (n\,e_N, h) = (n,h).$$

Ovdje smo ponovo koristili činjenicu da homomorfizam šalje neutral u neutral, samo što je to sada primjenjeno na homomorfizme $\varphi_h \in \operatorname{Aut} N$, $h \in H$.

(inverz)

Ako je (n,h) neki element koji ima inverz, označimo ga sa (n',h'), onda mora biti

$$\begin{aligned}
(n,h)*(n',h') &\overset{(\diamondsuit)}{=} \big(n\varphi_h(n'), h\,h'\big) = (e_N, e_H) \\
\Leftrightarrow &\qquad h\,h' = e_H \quad \& \quad n\,\varphi_h(n') = e_N \\
\Leftrightarrow &\qquad h' = h^{-1} \quad \& \quad n' = \varphi_{h^{-1}}(n^{-1});
\end{aligned}$$

ovdje smo koristili činjenicu da je φ homomorfizam grupa, pa onda posebno imamo

$$\begin{aligned}
\varphi_{h^{-1}}(n^{-1}) &= \varphi_{h^{-1}}(\varphi_h(n')) = (\varphi_{h^{-1}} \circ \varphi_h)(n') = \\
&\varphi(h^{-1}h)(n') = \varphi(e_H)(n') = 1_N(n') = n'.
\end{aligned}$$

Sada se odmah provjeri da za dobivene n' i h' imamo ispunjenu i jednakost

$$(n',h')*(n,h) = (e_N, e_H)$$

Dakle, inverz od (n,h) u $N \times H$ je dan kao

$$(n,h)^{-1} = \big(\varphi_{h^{-1}}(n^{-1}), h^{-1}\big).$$

Tako smo dokazali teorem. □

Definicija 3.8. Grupu $(N \times H, *)$ označavamo sa

$$N \rtimes_{\varphi} H,$$

ili samo $N \rtimes H$ ako znamo o kojem se homomorfizmu φ radi, i zovemo **semidirektan produkt** grupe N sa H određen sa φ; u upotrebi je još i naziv **normalan produkt** grupa.

Napomena 3.9. Ako za bilo koje grupe N i H gledamo trivijalan homomorfizam $\varphi : H \to \operatorname{Aut} N$, tj. $H \ni h \mapsto \varphi_h := 1_N \in \operatorname{Aut} N$, onda je

$$N \rtimes H \cong N \times H;$$

doista, sada definicija množenja $(\diamondsuit)$ postaje

$$(n_1, h_1) * (n_2, h_2) = (n_1\, \varphi_{h_1}(n_2), h_1\, h_2) = (n_1\, n_2, h_1\, h_2),$$

što je "obično" množenje po komponentama, kako smo ga definirali u direktnom produktu. Znači, semidirektan produkt je doista generalizacija "običnog", direktnog, produkta dvije grupe.

Sljedeći nam je cilj dokazati analogon *Teorema karakterizacije direktne sume* grupa u slučaju semidirektnog produkta; jasno, sada ćemo imati samo dvije grupe, neke H i N, kao faktore. Kao pripremu dokažimo ovu propoziciju; zapravo, ta propozicija će biti jedan smjer u dokazu ekvivalencije iz teorema.

Propozicija 3.10. *Neka su H, N i φ kao gore, i označimo onda $G := N \rtimes H$. Tada imamo sljedeće:*

(i) *Skup $\big\{(n, e_H) \mid n \in N\big\}$ je normalna podgrupa od G, izomorfna sa N; tako identificiramo te dvije grupe i onda podrazumijevamo da je $N \trianglelefteq G$.*
Skup $\big\{(e_N, h) \mid h \in H\big\}$ je podgrupa od G, izomorfna sa H; tako identificiramo te dvije grupe i onda podrazumijevamo da je $H \leq G$.

(ii) *Vrijedi, uz oznaku $e = e_H = e_N$,*

$$I_{(e,h)}\big((n,e)\big) \quad \Big(:= (e,h) * (n,e) * (e,h)^{-1}\Big) \quad = (\varphi_h(n), e);$$

slijedi, posebno, da je svaki automorfizam φ_h od N, za $h \in H \leq G$, potpuno određen sa unutarnjim automorfizmom $I_h \in \operatorname{Int} G \trianglelefteq \operatorname{Aut} G$.

(iii) *Vrijedi*

$$G = \langle N \cup H \rangle \qquad \& \qquad N \cap H = \{e\}.$$

Dokaz. Najprije računamo, za $\nu, n \in N$ i $h \in H$:

$$\begin{aligned} I_{(\nu,h)}\big((n,e)\big) &= (\nu, h) * (n, e) * (\nu, h)^{-1} = \\ &= \big(\nu\, \varphi_h(n), h\big) * \big(\varphi_{h^{-1}}(\nu^{-1}), h^{-1}\big) = \\ &= \big(\nu\, \varphi_h(n)\, \varphi_h(\varphi_{h^{-1}}(\nu^{-1})), h\, h^{-1}\big) = \\ &= \big(\nu\, \varphi_h(n)\, \nu^{-1}, e\big). \end{aligned}$$

Sada, ako stavimo $\nu = e_N$, dobijemo tvrdnju (ii).

(i) Očito je preslikavanje $N \ni n \mapsto (n, e) \in N \times H$ izomorfizam iz N na $\big\{(n, e) \mid n \in N\big\}$. Sada, po već dokazanoj tvrdnji (ii), jasno je da $N \trianglelefteq G$. Analogno imamo izomorfnost $H \cong \big\{(e, h) \mid h \in H\big\}$; primjetimo da H ne mora biti normalna podgrupa od G.

(iii) Po Lemi 2.4 (vidi i Zadatak 23), imamo

$$\langle H \cup N \rangle = HN = NH.$$

Još primjetimo da je

$$(n, e) * (e, h) = (n, h),$$

pa onda slijedi jednakost $NH = G$. Očito vrijedi i jednakost $H \cap N = \{e\}$. Tako je propozicija dokazana. $\square$

Zadatak 30. Dokažite da je sa

$$\theta : G/N \to H, \qquad (n, h)N \mapsto h,$$

definiran izomorfizam grupa.

NAPOMENA. Od sada nadalje, kod množenja elemenata u semidirektnom produktu, izostavljamo simbol $*$.

Sad ćemo dokazati najavljeni analogon Teorema 3.4.

Teorem 3.11. *Grupa G je izomorfna semidirektnom produktu grupe N sa H (za neki homomorfizam φ)* akko *vrijede sljedeća tri uvjeta:*

(**1**) $N \trianglelefteq G$ *i* $H \leq G$*;*
(**2**) $N \cap H = \{e\}$*;*
(**3**) $G = \langle N \cup H \rangle$.

Dokaz. ($\Rightarrow$) To je Propozicija 3.10.

($\Leftarrow$) Neka sada vrijede uvjeti (**1**) – (**3**). Posebno, ponovo po Lemi 2.4, iz (**1**) i (**3**), slijedi da je $G = NH$; tj., svaki element $g \in G$ možemo napisati kao

$$g = n\,h, \qquad n \in N,\ h \in H.$$

Primjetimo da je gornji rastav *jedinstven*. [[Doista, pretpostavimo da imamo i neki drugi rastav $g = n'h'$. Tada je $n^{-1}n' = h\,h'^{-1} \in N \cap H = \{e\}$; ovdje koristimo (**2**). Slijedi $n = n'$ i $h = h'$.]]

Nadalje, po (**1**) je $N \trianglelefteq G$, i onda je posebno

$$h\,n\,h^{-1} = I_h(n) \in N, \qquad h \in H,\ n \in N;$$

jasno, restrikcija $(I_h)_{|N} \in \operatorname{Aut} N$. Štoviše, preslikavanje

$$\varphi : H \to \operatorname{Aut} N, \qquad \varphi(h) = \varphi_h := (I_h)_{|N},$$

je homomorfizam grupa.

Konačno, uzmimo proizvoljne elemente $g_1, g_2 \in G$ i napišimo ih kao prije, $g_1 = n_1 h_1$ i $g_2 = n_2 h_2$. Tada imamo

$$g_1 g_2 = n_1 h_1 n_2 h_2 = n_1 h_1 n_2 (h_1^{-1} h_1) h_2 = n_1 I_{h_1}(n_2)\; h_1 h_2 = n_1 \big(\varphi_{h_1}(n_2)\big)\;\; h_1 h_2.$$

Dakle, vidimo da je pravilo za množenje,

$$(n_1h_1)(n_2h_2) = n_1\big(\varphi_{h_1}(n_2)\big)\ \ h_1h_2,$$

sasvim isto kao u prije danoj definiciji semidirektnog produkta; sasvim precizno, sa

$$G \ni g = nh \mapsto (n,h) \in N \rtimes_\varphi H$$

je realiziran izomorfizam $G \cong N \rtimes_\varphi H$. Tako je teorem dokazan. □

Sada ćemo dati dva interesantna primjera koji daju rastav grupe kao semidirektan produkt dviju svojih pravih podgrupa; jedan je primjer za konačne grupe, a drugi za beskonačne (matrične) grupe.

Primjer 3.12. (*Diedralna grupa*)
Promatrajmo pravilni n-terokut $\boldsymbol{P} = \boldsymbol{P}_n$ u euklidskoj ravnini $\mathcal{M}$ (vidi Primjer 1.13), i njegovu *grupu simetrija*; tj., podgrupu

$$D_n := \mathrm{Sim}(\boldsymbol{P}) \leq \mathrm{Isom}(\mathcal{M}).$$

Ta se grupa zove n-ta **diedralna grupa**, ili diedralna grupa pravilnog n-terokuta. Lako se može pokazati da je grupa D_n generirana rotacijama i osnim simetrijama. Preciznije, ta je grupa generirana sa dvije simetrije; to su *rotacija* $\boldsymbol{a}$, oko središta n-terokuta, za kut $2\pi/n$ (u negativnom smjeru, tj., smjeru kazaljki na satu), i *osna simetrija* $\boldsymbol{b}$ s obzirom na pravac koji prolazi jednim vrhom n-terokuta i njegovim središtem. Ako vrhove n-terokuta označimo brojevima $1, 2, \ldots, n$ (idući u negativnom smjeru), onda se oni pri djelovanju simetrija $\boldsymbol{a}$ i $\boldsymbol{b}$ pridružuju jedni drugima kako slijedi:

$$\begin{aligned}
\boldsymbol{a}: &\quad 1 \mapsto 2, \quad k \mapsto k+1 \ \text{ za } k = 2,3,\ldots,n-1, \quad n \mapsto 1;\\
\boldsymbol{b}: &\quad 1 \mapsto 1, \quad k \mapsto n+2-k \ \text{ za } k = 2,3,\ldots,n-1;
\end{aligned}$$

ovdje smo, bez smanjenja općenitosti, pretpostavili da je os osne simetrije $\boldsymbol{b}$ pravac kroz vrh 1 i središte.

Zapravo, iz gornjih razmatranja je sasvim jasno da se D_n može promatrati i kao podgrupa grupe permutacija $\mathcal{S}_n$, na skupu $\{1, 2, \ldots, n\}$. Preciznije rečeno, imamo da je

$$D_n \equiv \langle \boldsymbol{a}, \boldsymbol{b} \rangle \leq \mathcal{S}_n,$$

gdje se sada $\boldsymbol{a}$ i $\boldsymbol{b}$ mogu shvatiti kao permutacije (vrhova poligona)

$$\boldsymbol{a} = \begin{pmatrix} 1 & 2 & 3 & \cdots & n-1 & n \\ 2 & 3 & 4 & \cdots & n & 1 \end{pmatrix}, \qquad \boldsymbol{b} = \begin{pmatrix} 1 & 2 & 3 & \cdots & n-1 & n \\ 1 & n & n-1 & \cdots & 3 & 2 \end{pmatrix}.$$

Lako se može vidjeti da vrijedi sljedeća tvrdnja; ovdje je $\boldsymbol{1} := \begin{pmatrix} 1 & 2 & \cdots & n \\ 1 & 2 & \cdots & n \end{pmatrix}$ identiteta, tj. neutral u grupi permutacija $\mathcal{S}_n$.

Tvrdnja. (i) Za $n \geq 3$, D_n je nekomutativna grupa reda $2n$ generirana elementima $\boldsymbol{a}$ i $\boldsymbol{b}$; ti elementi zadovoljavaju:

$$\boldsymbol{a}^n = \boldsymbol{1} = \boldsymbol{b}^2, \qquad \boldsymbol{a}^k \neq \boldsymbol{1} \ \text{ za } 0 < k < n, \qquad \boldsymbol{a}^{-1}\boldsymbol{b} = \boldsymbol{b}\,\boldsymbol{a}.$$

(ii) Svaka grupa $\mathcal{D}$, generirana nekim elementima a i b, koji zadovoljavaju iste relacije kao i $\boldsymbol{a}$ i $\boldsymbol{b}$ u (i), izomorfna je n-toj diedralnoj grupi; tj., $\mathcal{D} \cong D_n$.

[[Za dokaz gornje tvrdnje, treba samo provjeriti da permutacije $\boldsymbol{a}$ i $\boldsymbol{b}$ doista zadovoljavaju relacije navedene u (i), i zatim da je

$$D_n = \{\mathbf{1}, \boldsymbol{a}, \boldsymbol{a}^2, \ldots, \boldsymbol{a}^{n-1},\ \ \boldsymbol{b}, \boldsymbol{a}\,\boldsymbol{b}, \boldsymbol{a}^2\boldsymbol{b}, \ldots, \boldsymbol{a}^{n-1}\boldsymbol{b}\}.$$

Da je grupa D_n nekomutativna slijedi iz gore navedene relacije $\boldsymbol{a}^{-1}\boldsymbol{b} = \boldsymbol{b}\,\boldsymbol{a}$; naime, kad bi to bila komutativna grupa, bilo bi posebno

$$\boldsymbol{a}^{-1}\boldsymbol{b} = \boldsymbol{b}\,\boldsymbol{a} = \boldsymbol{a}\,\boldsymbol{b} \quad \Rightarrow \quad \boldsymbol{a}^{-1}\boldsymbol{b} = \boldsymbol{a}\,\boldsymbol{b} \quad \Rightarrow \quad \boldsymbol{a}^{-1} = \boldsymbol{a} \quad \Rightarrow \quad \boldsymbol{a}^2 = \mathbf{1},$$

što je u suprotnosti sa pretpostavkom $n \geq 3$.]]

Sada primjetimo sljedeće:

$$\begin{aligned} \mathbb{Z}/n\mathbb{Z} &\cong N := \langle \boldsymbol{a} \rangle = \{\mathbf{1}, \boldsymbol{a}, \ldots, \boldsymbol{a}^{n-1}\} \trianglelefteq D_n, \\ \mathbb{Z}/2\mathbb{Z} &\cong H := \langle \boldsymbol{b} \rangle = \{\mathbf{1}, \boldsymbol{b}\} \leq D_n. \end{aligned}$$

[[Za dokaz da je $N \trianglelefteq D_n$ treba samo primjetiti da je $\boldsymbol{a}^{-1}\boldsymbol{b} = \boldsymbol{b}\,\boldsymbol{a}$ ekvivalentno jednakosti $\boldsymbol{b}\,\boldsymbol{a}\,\boldsymbol{b} = \boldsymbol{a}^{-1}$, i da onda imamo

$$(\boldsymbol{a}^k\boldsymbol{b})\boldsymbol{a}^l(\boldsymbol{a}^k\boldsymbol{b})^{-1} = \boldsymbol{a}^k\boldsymbol{b}\,\boldsymbol{a}^l\boldsymbol{b}\,\boldsymbol{a}^{-k} = \boldsymbol{a}^k(\boldsymbol{b}\,\boldsymbol{a}\,\boldsymbol{b})^l\boldsymbol{a}^{-k} = \boldsymbol{a}^k(\boldsymbol{a}^{-1})^l\boldsymbol{a}^{-k} = \boldsymbol{a}^k\boldsymbol{a}^{-l}\boldsymbol{a}^{-k} = \boldsymbol{a}^{-l} \in N;$$

ovdje smo koristili gore rečenu činjenicu da je svaki $x \in D_n$ oblika $x = \boldsymbol{a}^k\boldsymbol{b}$ ili $x = \boldsymbol{a}^k$, za neki k. (Drugi način dokaza da je $N \trianglelefteq D_n$ je primjetiti kako je indeks $(D_n : N) = 2$ i onda primjeniti Zadatak 28.)]]

Nadalje, očito vrijedi i

$$N \cap H = \{\mathbf{1}\} \qquad \& \qquad \langle N \cup H \rangle = NH = D_n.$$

Zaključak je, po prethodnom teoremu, da je

$$\mathbb{Z}/n\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z} \cong D_n.$$

Napomena 3.13. Primjetimo da je semidirektan produkt $D_n \cong \mathbb{Z}/n\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$ nekomutativna grupa, ali da su oba faktora, $\mathbb{Z}/2\mathbb{Z}$ i $\mathbb{Z}/n\mathbb{Z}$, komutativne grupe.

Zadatak 31. Što je φ koji definira semidirektan produkt $\mathbb{Z}/n\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z} \cong D_n$? Napišite eksplicite taj homomorfizam $\varphi : \mathbb{Z}/2\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$.

Primjer 3.14. Definirajmo sljedeće skupove kompleksnih 2-puta-2 matrica:

$$P := \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \ \middle| \ a, c \in \mathbb{C}^\times, \quad b \in \mathbb{C} \right\} \qquad \text{(gornje trokutaste regularne matrice)},$$

$$N := \left\{ \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \ \middle| \ x \in \mathbb{C} \right\} \qquad \text{(tzv. unipotentne matrice)},$$

$$H := \left\{ \begin{pmatrix} u & 0 \\ 0 & v \end{pmatrix} \ \middle| \ u, v \in \mathbb{C}^\times \right\} \qquad \text{(dijagonalne regularne matrice)}.$$

Lako se provjeri da su P, N i H podgrupe od $\mathrm{GL}_2(\mathbb{C})$; N i H su abelove, ali P nije abelova. Nadalje, $H \leq P$ i $N \trianglelefteq P$. Budući je

$$\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} = \begin{pmatrix} a & 0 \\ 0 & c \end{pmatrix} \begin{pmatrix} 1 & b/a \\ 0 & 1 \end{pmatrix},$$

slijedi da imamo $P = HN$. Po prethodnom teoremu, zaključujemo da je

$$N \rtimes H \cong P.$$

Zadatak 32. Dokažite detaljno da su doista P, N i H podgrupe od $\mathrm{GL}_2(\mathbb{C})$, da je $N \trianglelefteq P$ normalna podgrupa, ali H nije normalna podgrupa od P. Nadalje, pokažite da P nije abelova grupa. Napišite pripadni homomorfizam $\varphi : H \to \operatorname{Aut} N$, koji realizira semidirektan produkt $N \rtimes H \cong P$, eksplicite.

Gornji se primjer može i poopćiti. Naime, neka je $\mathbb{K}$ proizvoljno polje i onda $G = \mathrm{GL}_n(\mathbb{K})$. Definirajmo H kao **grupu dijagonalnih matrica** (regularnih), tj. kao skup svih n-puta-n matrica oblika

$$\begin{pmatrix} d_1 & 0 & \dots & 0 \\ 0 & d_2 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & d_n \end{pmatrix}, \qquad d_i \in \mathbb{K}^\times;$$

H je abelova podgrupa od G. Dalje, definirajmo $P \leq G$ kao **grupu gornjih trokutastih matrica** (regularnih), tj. kao skup svih n-puta-n matrica oblika

$$\begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ 0 & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & a_{nn} \end{pmatrix}, \qquad a_{ii} \in \mathbb{K}^\times, \ \ a_{ij} \in \mathbb{K} \text{ za } i < j;$$

jasno, P nije abelova grupa. Isto tako definirajmo podgrupu $N \leq G$, kao tzv. **grupu unipotentnih matrica**, koja se sastoji od svih onih matrica iz P koje svuda na glavnoj dijagonali imaju 1; tj., N se sastoji od svih matrica oblika

$$\begin{pmatrix} 1 & a_{12} & a_{13} & \dots & a_{1n} \\ 0 & 1 & a_{23} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & 1 \end{pmatrix}, \qquad a_{ij} \in \mathbb{K} \text{ za } i < j;$$

N je abelova grupa akko je $n \leq 2$. Sada, nije teško pokazati da su N i H podgrupe od P, te da je štoviše $N \trianglelefteq P$; H nije normalna podgrupa od P, za $n \geq 2$. Nadalje, imamo $N \cap H = \{\boldsymbol{I}\}$; $\boldsymbol{I}$, naravno, označava jediničnu matricu, neutral u grupi G. Slično kao za $n = 2$ pokaže se i da je $P = HN$. Zaključak je, ponovo po teoremu karakterizacije za semidirektan produkt, da je

$$N \rtimes H \cong P.$$

Zadatak 33. Dokažite detaljno sve navedene korake za dokaz da je $N \rtimes H \cong P$.

4. Primjeri grupa

Podsjetimo se: Ako je G neka grupa i $S \subseteq G$ neki podskup, kažemo da je S skup generatora od G ako je $G = \langle S \rangle$. Ako je $S = \{g\}$, tj. $G = \langle g \rangle$, G se zove ciklička grupa. Ako postoji konačan podskup $S \subseteq G$ takav da je $G = \langle S \rangle$, kažemo da je G konačno generirana grupa. (Kao što smo vidjeli, konačno generirane grupe sa $n \geq 2$ generatora ne moraju biti komutativne; npr., $\mathrm{SL}_2(\mathbb{Z}) = \langle S, T \rangle$, gdje su $S := \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ i $T := \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$, i $D_n = \langle \boldsymbol{a}, \boldsymbol{b} \rangle$, gdje su $\boldsymbol{a}$ i $\boldsymbol{b}$ kao u Primjeru 3.12.)

Osnovni cilj ovog odjeljka je dati još neke zanimljive primjere grupa, kao i neke važne rezultate koji opisuju strukture nekih grupa.

4.1. Komutativne grupe.

U ovom pododjeljku u kratkim se crtama bavimo nekim komutativnim grupama. Najprije govorimo o *cikličkim grupama*, za koje dajemo tzv. strukturni teorem. Sljedeći nam je korak iskazati, te ilustrirati na primjerima, još jedan osnovni teorem. To je tzv. *Strukturni teorem za konačno generirane komutativne grupe.*

Najjednostavnije komutativne grupe su cikličke grupe. Postoje dva tipa cikličkih grupa:

$\longrightarrow$ G ciklička i red $|G| < \infty$; onda je $G \cong \mathbb{Z}/n\mathbb{Z}$, za neki $n \in \mathbb{N}$.

$\longrightarrow$ G ciklička i red $|G| = \infty$; onda je $G \cong \mathbb{Z}$.

Zapravo, imamo ovaj teorem "o strukturi cikličkih grupa".

Teorem 4.1. *Neka je G ciklička grupa . Tada imamo:*

(i) *Svaka podgrupa $H \leq G$ je također ciklička.*
(ii) *$G \cong \mathbb{Z}$ ili $G \cong \mathbb{Z}/n\mathbb{Z}$, za neki $n \in \mathbb{N}$.*
(iii) *Svaka homomorfna slika od G je ciklička; tj., ako je $f : G \to H$ homomorfizam, onda je $\operatorname{Im} f$ ciklička grupa.*

Dokaz. Neka je G ciklička, tj. $G = \langle g \rangle = \{g^m \mid m \in \mathbb{Z}\}$.

(i) Pretpostavimo da je $H \neq \{e\}$ neka podgrupa i neka je $m \in \mathbb{N}$ *minimalan* takav da je $g^m \in H$; m sa navedenim svojstvom očito postoji.

Tvrdnja. $H = \langle g^m \rangle$.

[[Inkluzija ($\supseteq$) je jasna. Da bismo dokazali obratnu inkluziju, uzmimo bilo koji $h \in H$ i napišimo taj element kao $h = g^n = g^{qm+r}$, gdje je $n = qm + r$ i $0 \leq r < m$; tu koristimo teorem o dijeljenju s ostatkom za cijele brojeve. Slijedi

$$g^r = (g^m)^{-q}\, h \in H \qquad \text{(jer su i } (g^m)^{-q} \text{ i } h \text{ iz } H.)$$

Znači, $g^r \in H$ i $r < m$. Zbog minimalnosti od m, zaključujemo da je $r = 0$, tj. $h = g^{qm} = (g^m)^q \in \langle g^m \rangle$.]]

(ii) Očito je

$$f : \mathbb{Z} \to G = \langle g \rangle, \qquad m \mapsto g^m,$$

epimorfizam grupa. Sada, ako je $\operatorname{Ker} f = \{0\}$, onda je f izomorfizam; tj., $\mathbb{Z} \cong G$. A ako je $\{0\} \neq \operatorname{Ker} f \leq \mathbb{Z}$, onda je, po (i), $\operatorname{Ker} f = \langle m \rangle = m\mathbb{Z}$, za neki $m \in \mathbb{N}$. Po Prvom teoremu o izomorfizmu, slijedi da je $\mathbb{Z}/m\mathbb{Z} \cong G$.

(iii) Ako je $f : G \to H$ homomorfizam, onda je $\operatorname{Im} f = \langle f(g) \rangle$; tj., $\operatorname{Im} f$ je ciklička grupa. □

Sljedeće, po složenosti njihove strukture, su (konačne) direktne sume cikličkih grupa. Drugim riječima, radi se o konačno generiranim komutativnim grupama. Ta je činjenica predmet sljedećeg fundamentalnog rezultata. Iako njegov dokaz ne zahtjeva nikakve nove tehnike ni rezultate (pored onih koje smo mi do sada uveli), dokaz ćemo izostaviti budući da ipak nije "sasvim kratak"...

Teorem 4.2. (Strukturni teorem za konačno generirane komutativne grupe)
Neka je G konačno generirana komutativna grupa. Tada postoji $k \in \mathbb{N}_0$ i postoje

$$m_1 \mid m_2 \mid \cdots \mid m_t, \qquad m_i \in \mathbb{N} \setminus \{1\},$$

takvi da je

$$G \cong \big(\mathbb{Z}/m_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/m_t\mathbb{Z}\big) \oplus \mathbb{Z}^k;$$

ovdje je, naravno, $\mathbb{Z}^k = \mathbb{Z} \oplus \cdots \oplus \mathbb{Z}$, k primjeraka od $\mathbb{Z}$.

Definicija 4.3. Broj k, kao u teoremu, zove se **rang** od G. Brojevi m_i zovu se **invarijante** od G.

Gornji se teorem može dati i u alternativnom obliku.

Teorem. 4.2.′
Neka je G konačno generirana komutativna grupa. Tada postoji konačan skup prim brojeva $\mathcal{P}(G) = \{p_1, \ldots, p_s\}$, postoji $k \in \mathbb{N}_0$, i za svaki p_i postoji niz brojeva

$$1 \leq \alpha_1(p_i) \leq \alpha_2(p_i) \leq \cdots \leq \alpha_{n_i}(p_i)$$

takvih da je

$$G \cong \Big(\bigoplus_{p_i \in \mathcal{P}(G)} S(p_i)\Big) \oplus \mathbb{Z}^k,$$

gdje je

$$S(p_i) := \mathbb{Z}/p_i^{\alpha_1(p_i)}\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/p_i^{\alpha_{n_i}(p_i)}\mathbb{Z}$$

tzv. **Sylowska p_i-podgrupa** *od G.*

Jedan se prikaz od G (kao u Teoremu 4.2) prevodi u drugi prikaz (kao u Teoremu 4.2′) pomoću ove jednostavne leme. (Zapravo, mi smo tu lemu već dokazali u Primjeru 3.5(2)).

Lema 4.4. *Ako su $m, n \in \mathbb{N}$ relativno prosti brojevi, onda je*

$$\mathbb{Z}/m\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/mn\mathbb{Z}.$$

Dokaz. Identificirajmo $\mathbb{Z}/m\mathbb{Z} \equiv A_1 \hookrightarrow \mathbb{Z}/mn\mathbb{Z}$ i $\mathbb{Z}/n\mathbb{Z} \equiv A_2 \hookrightarrow \mathbb{Z}/mn\mathbb{Z}$, pomoću izomorfizama

$$\mathbb{Z}/m\mathbb{Z} \ni k + m\mathbb{Z} \longmapsto kn + mn\mathbb{Z} \in A_1 := \{kn + mn\mathbb{Z} \mid k \in \mathbb{Z}\},$$
$$\mathbb{Z}/n\mathbb{Z} \ni l + n\mathbb{Z} \longmapsto lm + mn\mathbb{Z} \in A_2 := \{lm + mn\mathbb{Z} \mid l \in \mathbb{Z}\}.$$

Sada je $A_1 \oplus A_2 \cong \mathbb{Z}/mn\mathbb{Z}$; za detalje vidi Primjer 3.5(2).

(("Drugi način" dokaza leme je da se direktno pokaže kako je sa

$$\phi : \mathbb{Z}/m\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z} \longrightarrow \mathbb{Z}/mn\mathbb{Z},$$
$$\phi(k + m\mathbb{Z}, l + n\mathbb{Z}) := kn + lm + mn\mathbb{Z},$$

dan izomorfizam grupa; primjetimo da je konstrukcija od ϕ ista kao u dokazu Teorema 3.4.)) □

Primjer 4.5. Promatrajmo grupu

$$G = \underbrace{\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/9\mathbb{Z} \oplus \mathbb{Z}/27\mathbb{Z}} \oplus \underbrace{\mathbb{Z}/5\mathbb{Z} \oplus \mathbb{Z}/25\mathbb{Z}} \oplus \underbrace{\mathbb{Z}/121\mathbb{Z}}$$
$$= S(3) \oplus S(5) \oplus S(11);$$

ovdje je $\mathcal{P}(G) = \{3, 5, 11\}$. Po prethodnoj lemi je

$$\mathbb{Z}/9\mathbb{Z} \oplus \mathbb{Z}/5\mathbb{Z} \cong \mathbb{Z}/45\mathbb{Z} \qquad \& \qquad \mathbb{Z}/27\mathbb{Z} \oplus \mathbb{Z}/25\mathbb{Z} \oplus \mathbb{Z}/121\mathbb{Z} \cong \mathbb{Z}/(27 \cdot 25 \cdot 121)\mathbb{Z}.$$

Dakle

$$G \cong \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/45\mathbb{Z} \oplus \mathbb{Z}/(27 \cdot 25 \cdot 121)\mathbb{Z};$$

invarijante od G su $m_1 = 3$, $m_2 = 45$ i $m_3 = 27 \cdot 25 \cdot 121$, dok je rang, jasno, jednak $k = 0$.

Napomena 4.6. (1) Beskonačno generirana komutativna grupa može imati dosta kompliciranu strukturu. (Npr., netrivijalan je opis svih podgrupa grupe $(\mathbb{Q}, +)$!)

(2) Postoje i "dosta jednostavne" beskonačno generirane komutativne grupe (tu fraza "dosta jednostavne" zapravo ovisi o tome što mi o dotičnoj grupi želimo doznati). Jedne od takvih grupa su n-**dimenzionalni torusi**

$$\mathbb{T} := S^1 \times \cdots \times S^1,$$

n primjeraka $S^1 = \{z \in \mathbb{C} \mid |z| = 1\} \cong \mathbb{R}/\mathbb{Z}$.

4.2. Nekomutativne grupe.

Glavni je cilj ovog pododjeljka dati cijelo mnoštvo primjera beskonačnih nekomutativnih grupa. Sve su te grupe tzv. *matrične grupe*.

<u>Konačne</u> nekomutativne grupe

Važni primjeri ovdje su simetrične grupe $\mathcal{S}_n$, grupe permutacija skupova $\{1, 2, \ldots, n\}$. Vidjeli smo da su tzv. alternirajuće grupe $\mathcal{A}_n$ i diedralne grupe D_n podgrupe od simetričnih grupa; tj.,

$$\mathcal{A}_n \trianglelefteq \mathcal{S}_n \qquad \& \qquad D_n \leq \mathcal{S}_n.$$

Beskonačne nekomutativne grupe

Kako smo već najavili, kada smo definirali opću linearnu grupu $\mathrm{GL}_n(\mathbb{K})$, sada ćemo navesti još neke vrlo zanimljive matrične grupe i/ili neke kvocijentne grupe matričnih grupa. U ovome što slijedi, za $n \in \mathbb{N}$, pisat ćemo

$$\boldsymbol{I}_n = n\text{-puta-}n \text{ jedinična matrica.}$$

(**0**) Ako je V n-dimenzionalan vektorski prostor nad poljem $\mathbb{K}$ (npr., $\mathbb{K} = \mathbb{R}, \mathbb{Q}, \mathbb{C}$), definirali smo *opću linearnu grupu*

$$\mathrm{GL}(V) \cong \mathrm{GL}_n(\mathbb{K}) := \{A \mid \det A \neq 0\}.$$

(**1**) *Specijalna linearna grupa* definirana je kao podgrupa od $\mathrm{GL}_n(\mathbb{K})$ onih matrica čija je determinanta jednaka 1, tj.

$$\mathrm{SL}_n(\mathbb{K}) := \{A \in \mathrm{GL}_n(\mathbb{K}) \mid \det A = 1\}.$$

(**2**) *Projektivna grupa* definirana je kao

$$\mathrm{PGL}_n(\mathbb{K}) := \mathrm{GL}_n(\mathbb{K})/\mathbb{K}^\times;$$

ovdje je $\mathbb{K}^\times \equiv \mathbb{K}^\times \boldsymbol{I}_n \trianglelefteq \mathrm{GL}_n(\mathbb{K})$, kao i u Primjeru 3.6.

(**3**) *Modularna grupa* je grupa $\mathrm{SL}_2(\mathbb{Z})$ (ili grupa $\mathrm{SL}_2(\mathbb{Z})/\{\pm \boldsymbol{I}_2\}$). Općenitije, možemo gledati grupu

$$\mathrm{SL}_n(\mathbb{Z}),$$

svih n-puta-n matrica, sa koeficijentima iz $\mathbb{Z}$, determinante 1.

(**4**) Definirajmo *ortogonalnu grupu*

$$\mathrm{O}(n) := \{A \in \mathrm{GL}_n(\mathbb{R}) \mid A^t A = A\,A^t = \boldsymbol{I}_n\};$$

jasno,

$$\mathrm{O}(n) \leq \mathrm{GL}_n(\mathbb{R}).$$

Isto tako, definirajmo *unitarnu grupu*

$$\mathrm{U}(n) := \{A \in \mathrm{GL}_n(\mathbb{C}) \mid A^* A = A\,A^* = \boldsymbol{I}_n\};$$

po definiciji gornjih dviju grupa jasno je da imamo

$$\mathrm{O}(n) \leq \mathrm{U}(n) \leq \mathrm{GL}_n(\mathbb{C}).$$

(Ovdje je sa $A \mapsto A^* := \overline{A}^{\,t}$ označeno *hermitsko adjungiranje* na kompleksnim matricama; jasno, $A \mapsto \overline{A}$ je konjugiranje, a $A \mapsto A^t$ je transponiranje.)

Specijalna ortogonalna grupa i *specijalna unitarna grupa* su definirane kao

$$\mathrm{SO}(n) := \mathrm{O}(n) \cap \mathrm{SL}_n(\mathbb{R}),$$
$$\mathrm{SU}(n) := \mathrm{U}(n) \cap \mathrm{SL}_n(\mathbb{C}).$$

(**5**) *Simplektička grupa* definirana je sa

$$\mathrm{Sp}(n) := \left\{ \begin{pmatrix} A & -\overline{B} \\ B & \overline{A} \end{pmatrix} \in \mathrm{U}(2n) \mid A, B \in M_n(\mathbb{C}) \right\}.$$

(To je primjer tzv. realne Liejeve grupe.)

Isto tako, za $2n$-puta-$2n$ matricu

$$J := \begin{pmatrix} \mathbf{0} & -\boldsymbol{I}_n \\ \boldsymbol{I}_n & \mathbf{0} \end{pmatrix},$$

gdje $\mathbf{0}$ označava n-puta-n nul-matricu, definirajmo *kompleksnu simplektičku grupu*

$$\mathrm{Sp}(n,\mathbb{C}) := \{A \in \mathrm{GL}_{2n}(\mathbb{C}) \mid A^t J A = J\}.$$

(To je primjer tzv. kompleksne Liejeve grupe.)

Zadatak 34. (i) Dokažite da su gore definirani skupovi matrica $\mathrm{O}(n)$, $\mathrm{U}(n)$, $\mathrm{Sp}(n)$ i $\mathrm{Sp}(n,\mathbb{C})$ doista grupe. Nadalje, dokažite da su sve te grupe, osim za "jako male n-ove", nekomutativne.

(ii) Dokažite da smo ortogonalnu i unitarnu grupu mogli ekvivalentno definirati i kao

$$\mathrm{O}(n) := \{A \in \mathrm{GL}_n(\mathbb{R}) \mid A^t A = \boldsymbol{I}_n\},$$
$$\mathrm{U}(n) := \{A \in \mathrm{GL}_n(\mathbb{C}) \mid A^* A = \boldsymbol{I}_n\}.$$

Drugim riječima, dokažite da za $A \in \mathrm{GL}_n(\mathbb{R})$ imamo $A^t A = \boldsymbol{I}_n$ akko je $A\,A^t = \boldsymbol{I}_n$, te da za $A \in \mathrm{GL}_n(\mathbb{C})$ imamo $A^* A = \boldsymbol{I}_n$ akko je $A\,A^* = \boldsymbol{I}_n$.

Zadatak 35. Dokažite da je indeks $\big(\mathrm{O}(n) : \mathrm{SO}(n)\big) = 2$. (*Uputa:* Za dijagonalnu matricu $\Omega \in \mathrm{O}(n)$ koja na glavnoj dijagonali ima svuda 1, osim na mjestu $(1,1)$ gdje je -1, imamo disjunktnu uniju $\mathrm{O}(n) = \mathrm{SO}(n) \cup \Omega\,\mathrm{SO}(n)$.)

Napomena 4.7. Ako definiramo grupu

$$\mathrm{GL}_m^+(\mathbb{R}) := \{A \mid \det A > 0\},$$

onda imamo ovaj "dijagram grupa i podgrupa"; ovdje strelica "$\longrightarrow$" između dvije grupe H i G, $H \longrightarrow G$, znači da je $H \le G$ podgrupa. (Ovo što slijedi su sve primjeri tzv. *Liejevih grupa*, realnih i/ili kompleksnih.)

$$\begin{tikzcd}
 & & \mathrm{GL}_{2n}^+(\mathbb{R}) & & \\
\mathrm{GL}_n^+(\mathbb{R}) \arrow[r] & \mathrm{GL}_n(\mathbb{R}) \arrow[r] & \mathrm{GL}_n(\mathbb{C}) \arrow[u] \arrow[r] & --- \arrow[r] & \mathrm{GL}_{2n}(\mathbb{C}) \\
\mathrm{SO}(n) \arrow[u] \arrow[r] & \mathrm{O}(n) \arrow[u] \arrow[r] & \mathrm{U}(n) \arrow[u] \arrow[r] \arrow[d] & \mathrm{Sp}(n) \arrow[r] \arrow[d] & \mathrm{Sp}(n,\mathbb{C}) \arrow[u] \\
 & & \mathrm{SO}(2n) & \mathrm{U}(2n) &
\end{tikzcd}$$

Primjetimo ovdje kako zapravo gornji dijagram ima smisla tek kada kažemo kako to zapravo neka grupa H "sjedi", kao podgrupa, u nekoj "većoj" grupi G. Tako npr. $\mathrm{GL}_n(\mathbb{R}) \longrightarrow \mathrm{GL}_n(\mathbb{C})$, tj. $\mathrm{GL}_n(\mathbb{R}) \le \mathrm{GL}_n(\mathbb{C})$, na "prirodan način"; preciznije, ovdje se radi o ulaganju grupe $\mathrm{GL}_n(\mathbb{R})$ u grupu $\mathrm{GL}_n(\mathbb{C})$ tako da svaku realnu n-puta-n matricu A drugi put shvatimo kao kompleksnu n-puta-n matricu (kao što su i sami realni brojevi u stvari i "posebna vrsta" kompleksnih brojeva). Na iste "prirodne načine", koristeći gore dane definicije za odgovarajuće grupe, realiziraju se i ova ulaganja: $\mathrm{SO}(n) \longrightarrow \mathrm{GL}_n^+(\mathbb{R})$, $\mathrm{SO}(n) \longrightarrow \mathrm{O}(n)$, $\mathrm{GL}_n^+(\mathbb{R}) \longrightarrow \mathrm{GL}_n(\mathbb{R})$, $\mathrm{O}(n) \longrightarrow \mathrm{GL}_n(\mathbb{R})$, $\mathrm{O}(n) \longrightarrow \mathrm{U}(n)$, $\mathrm{U}(n) \longrightarrow \mathrm{GL}_n(\mathbb{C})$, $\mathrm{Sp}(n) \longrightarrow \mathrm{U}(2n)$ i $\mathrm{Sp}(n,\mathbb{C}) \longrightarrow \mathrm{GL}_{2n}(\mathbb{C})$; preciznije, u svim navedenim situacijama $H \longrightarrow G$ je zapravo $H \subseteq G$.

Da bismo opravdali ulaganje $\mathrm{GL}_n(\mathbb{C}) \longrightarrow \mathrm{GL}_{2n}(\mathbb{C})$, treba samo primjetiti da je npr. sa

$$\psi : \mathrm{GL}_n(\mathbb{C}) \to \mathrm{GL}_{2n}(\mathbb{C}), \qquad A \longmapsto \begin{pmatrix} A & \mathbf{0} \\ \mathbf{0} & A \end{pmatrix},$$

definiran monomorfizam između danih grupa. (Na taj način, identifikacijom $\mathrm{GL}_n(\mathbb{C})$ sa svojom slikom po promatranom monomorfizmu ψ, smatramo da je $\mathrm{GL}_n(\mathbb{C})$ podgrupa od $\mathrm{GL}_{2n}(\mathbb{C})$.) Primjetimo kako gornje ulaganje nije jedino koje je "sasvim evidentno"; npr., i preslikavanje

$$\mathrm{GL}_n(\mathbb{C}) \ni A \longmapsto \begin{pmatrix} A & \mathbf{0} \\ \mathbf{0} & \boldsymbol{I}_n \end{pmatrix} \in \mathrm{GL}_{2n}(\mathbb{C})$$

realizira monomorfizam grupa koje gledamo.

Preostala 4 ulaganja su "nešto delikatnija"; mi ćemo tu detalje preskočiti.

4.3. Pojam reprezentacije grupe.

U ovom kratkom pododjeljku dajemo definiciju (konačno-dimenzionalne) *reprezentacije grupe*. Tek kažimo kako su reprezentacije grupa od neprocijenjive vrijednosti za mnoge grane matematike; kako konačno- tako i beskonačno-dimenzionalne reprezentacije.

Neka je G grupa i V konačno dimenzionalan vektorski prostor nad $\mathbb{K}$.

Definicija 4.8. Svaki homomorfizam grupa

$$\pi : G \to \mathrm{GL}(V)$$

zove se **reprezentacija** grupe G na vektorskom prostoru V; kažemo da je $\dim V$ **dimenzija** reprezentacije.

Ako je $W \leq V$ vektorski potprostor, kažemo da je W π-**invarijantan** ako je

$$\pi(g)W \leq W \qquad \forall g \in G.$$

Reprezentacija π je (algebarski) **reducibilna** ako postoji π-invarijantan potprostor $0 \neq W \leq V$; inače je π **ireducibilna** reprezentacija.

Napomena 4.9. Jer je $\mathrm{GL}(V) \simeq \mathrm{GL}_n(\mathbb{K})$, onda možemo gledati

$$\pi : G \to \mathrm{GL}_n(\mathbb{K});$$

sada govorimo da je π **matrična reprezentacija**.

Primjer 4.10. (1) Neka je $G = \mathbb{R}$ i $V = \mathbb{R}^n$, te gledajmo matričnu reprezentaciju

$$\pi = \pi_A : \mathbb{R} \to \mathrm{GL}_n(\mathbb{R}), \qquad \pi(t) := e^{tA},$$

gdje je $A \in M_n(\mathbb{R})$ proizvoljno izabrana matrica. (Jasno je da se radi o reprezentaciji, tj. da vrijedi

$$\pi(s)\,\pi(t) = \pi(s+t), \qquad \forall s, t \in \mathbb{R}.)$$

Posebno, neka je $n = 2$:

Za $A = \mathbf{0}$, $\pi(t) = \boldsymbol{I} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, $\forall t \in \mathbb{R}$; to je tzv. *trivijalna reprezentacija.*
Za $A = \boldsymbol{I}$,

$$\pi(t) = e^{t\boldsymbol{I}} = \boldsymbol{I} + t\boldsymbol{I} + (t\boldsymbol{I})^2/2! + \cdots = e^t \boldsymbol{I} = \begin{pmatrix} e^t & 0 \\ 0 & e^t \end{pmatrix}.$$

Za $A = \begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix}$ je $A^n = \begin{pmatrix} 1 & n\alpha \\ 0 & 1 \end{pmatrix}$, i onda

$$\pi(t) = \boldsymbol{I} + tA + (tA)^2/2! + \cdots = e^t \boldsymbol{I} + \begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix},$$

gdje je

$$b = t\alpha + (t^2/2!)2\alpha + (t^3/3!)3\alpha + \cdots = t\alpha e^t.$$

Tojest,

$$\pi(t) = \begin{pmatrix} e^t & t\,\alpha\, e^t \\ 0 & e^t \end{pmatrix}.$$

(2) Preslikavanje

$$\rho : \mathbb{R} \to \mathrm{GL}_2(\mathbb{R}), \qquad \rho(t) := \begin{pmatrix} \cos t & -\sin t \\ \sin t & \cos t \end{pmatrix},$$

je 2-dimenzionalna reprezentacija grupe $\mathbb{R}$.

(3) Neka je grupa $G = \mathcal{S}_n$, simetrična grupa. Definirajmo

$$\pi : \mathcal{S}_n \to \mathrm{GL}_n(\mathbb{K}), \qquad \pi(\sigma) := E_{\sigma(1),1} + \cdots + E_{\sigma(n),n};$$

ovdje je sa E_{ij} označena standardna "kanonska" n-puta-n matrica koja na mjestu (i,j) ima 1, a na ostalim mjestima 0. Računajmo, za $\sigma, \tau \in \mathcal{S}_n$:

$$\begin{aligned} \pi(\sigma)\pi(\tau) &= \big(E_{\sigma(1),1} + \cdots + E_{\sigma(n),n}\big)\,\big(E_{\tau(1),1} + \cdots + E_{\tau(n),n}\big) = \\ &= \big(\text{jer je } E_{\sigma(1),1} + \cdots + E_{\sigma(n),n} = E_{\sigma(\tau(1)),\tau(1)} + \cdots + E_{\sigma(\tau(n)),\tau(n)}\big) \\ &= E_{\sigma(\tau(1)),1} + \cdots + E_{\sigma(\tau(n)),n} = \pi(\sigma\,\tau). \end{aligned}$$

(Popišite ovdje sve elemente grupe $\mathcal{S}_3$ i zatim elemente reprezentacije $\pi(\sigma)$, $\forall \sigma \in \mathcal{S}_3$.)

Osnovni problemi **Teorije Reprezentacija**:

(A) Za neku grupu G, na kojoj je još redovito zadana i topologija (diskretna grupa, algebarska grupa, Liejeva grupa, ...), opisati skup svih *ireducibilnih* reprezentacija π; sa eventualno još nekim dodatnim svojstvima (npr., π unitarna reprezentacija).

(B) Opisati neke "dobre" *reducibilne* reprezentacije pomoću ireducibilnih reprezentacija.

POGLAVLJE 2

Prsteni, polja i algebre

5. Osnovni pojmovi i primjeri

Pored grupa, prsteni su druge osnovne algebarska strukture u matematici. Kao i grupe, i prsteni se pojavljuju u analizi, u algebri, u teoriji brojeva, u algebarskoj geometriji i u mnogim drugim granama matematike.

5.1. Definicije prstena i polja; osnovna terminologija.

Za razliku od grupa gdje imamo samo jednu "unutarnju operaciju", kod prstena imamo dvije operacije; imajući na umu prsten $(\mathbb{Z}, +, \cdot)$, kao prvi "pravi" i osnovni primjer, te se operacije zovu i sada "*zbrajanje*" i "*množenje*". Preciznije, imamo ovu definiciju.

Definicija 5.1. Neprazan skup $R = (R, +, \cdot)$ zovemo **prsten** ukoliko je za operacije zbrajanja $+ : R \times R \to R$ i množenja $\cdot : R \times R \to R$ ispunjeno sljedeće:

(**1**) $(R, +)$ je komutativna grupa, sa neutralom $0 = 0_R$;
(**2**) $(R, \cdot)$ je *polugrupa*, tj. množenje je asocijativno;
(**3**) Vrijedi *distributivnost* "množenja prema zbrajanju", tj.

$$x \cdot (y + z) = x \cdot y + x \cdot z, \quad \forall x, y, z \in R,$$
$$(x + y) \cdot z = x \cdot z + y \cdot z, \quad \forall x, y, z \in R.$$

Element $0 = 0_R$, neutral u grupi $(R, +)$, zvat ćemo **nula** prstena R.

Ako postoji **jedinični element**, ili kraće **jedinica**, $1 = 1_R \in R$ takav da je

$$1 \cdot x = x \cdot 1 = x, \qquad \forall x \in R,$$

onda kažemo da je R **prsten s jedinicom**.

Prsten R je **komutativan prsten** ako je

$$x \cdot y = y \cdot x, \qquad \forall x, y \in R;$$

inače govorimo o **nekomutativnom prstenu**.

Napomena 5.2. Primjetimo da u svakom prstenu R, s jedinicom ili bez, njegova nula 0 zadovoljava

$$0 \cdot x = x \cdot 0 = 0, \qquad \forall x \in R;$$

naime, po distributivnosti je $x \cdot 0 = x \cdot (0 + 0) = x \cdot 0 + x \cdot 0$, iz čega slijedi $x \cdot 0 = 0$.

Osnovna podjela prstena je na komutativne i nekomutativne. Napomenimo, isto kao i kod grupa, da je u pravilu proučavanje strukture nekomutativnih prstena puno kompliciranije nego kod onih koji su komutativni. (No to nipošto ne znači da su svi komutativni prsteni jednostavni objekti za proučavanje. Naprotiv, često baš komutativnost u određenom smislu daje "bogatstvo strukture", tj. u mnogim komutativnim prstenima će biti cijelo mnoštvo potprstena i ideala; o tomu ćemo kasnije puno više govoriti.)

Sada uvodimo pojam "potstrukture" za prstene, tj. pojam potprstena.

Definicija 5.3. Skup $S \subseteq R$, gdje je R neki prsten, je **potprsten** od R ako je $S = (S, +, \cdot)$ i sam prsten. Drugim riječima, S je potprsten od R ako vrijede sljedeća dva uvjeta:

(**1**) $(\forall x, y \in S):\quad x - y \in S \qquad$ (tj., $(S,+)$ je grupa);
(**2**) $(\forall x, y \in S):\quad x \cdot y \in S \qquad$ (tj., $(S,\cdot)$ je grupoid).

Činjenicu da je S potprsten od R označavamo, analogno kao i kod grupa, sa

$$S \leq R.$$

NAPOMENA. (1) Od sada nadalje, kada je riječ o nekom prstenu $R = (R,+,\cdot)$, mi pri množenju elemenata u tom prstenu uglavnom nećemo pisati simbol "$\cdot$"; tj., ako su $x, y \in R$, onda najčešće

$$\text{pišemo} \quad x\,y \quad \text{namjesto} \quad x \cdot y.$$

(2) U daljnjem, za neke $n \in \mathbb{Z}$ i $x \in R$, koristit ćemo oznaku

$$n\,x = \begin{cases} x + \cdots + x \quad (n \text{ puta po } x) & \text{ako je } n > 0, \\ (-x) + \cdots + (-x) \quad (n \text{ puta po } -x) & \text{ako je } n < 0; \end{cases}$$

jasno, $0\,x = 0$.

Sljedeći je pojam direktni analogon odgovarajućeg pojma u teoriji grupa.

Definicija 5.4. Ako je dan prsten R, onda njegov **centar** definiramo kao

$$\mathcal{Z}(R) := \{x \in R \mid xr = rx, \ \ \forall r \in R\}.$$

Zadatak 36. Dokažite da je centar $\mathcal{Z}(R)$ potprsten od R.

Prije nego što počnemo ozbiljnije proučavati prstene, uvest ćemo najprije neke pojmove koje ćemo u daljnjem često trebati.

Definicija 5.5. Element $0 \neq \lambda \in R$ (tj., $0 \neq \rho \in R$) takav da je

$$\lambda\,x = 0 \qquad (\text{tj. } x\,\rho = 0), \qquad \text{za neki } 0 \neq x \in R$$

zove se **lijevi** (tj. **desni**) **djelitelj nule**.

R je **integralna domena**, ili kraće **domena**, ako nema ni lijevih ni desnih djelitelja nule.

Element $\omega \in R$, gdje je R prsten s jedinicom 1, je **invertibilan**, ako $\exists \omega' \in R$ takav da je

$$\omega\,\omega' = \omega'\,\omega = 1;$$

koristit ćemo oznaku

$$R^{\times} := \text{grupa invertibilnih elemenata u } R.$$

Napomena 5.6. Primjetimo da je $R^{\times}$ doista grupa; jasno, s obzirom na operaciju množenja u prstenu. Naime, ako su $u, v \in R^{\times}$, onda postoje neki $u', v' \in R$ takvi da je $u\,u' = u'u = 1$ i $v\,v' = v'v = 1$. Ali onda je

$$(u\,v)(v'u') = 1 = (v'u')(uv);$$

slijedi, $u\,v \in R^{\times}$. Isto tako, ako je $u \in R^{\times}$, onda je i njegov inverz u' također u $R^{\times}$; to je po definiciji od $R^{\times}$. Dakle, doista je riječ o grupi, kako smo i tvrdili.

Podsjetimo se ovdje i na dobro poznatu definiciju polja; poljima, koja čine važnu klasu prstena, bavit ćemo se na kraju ovog poglavlja.

Definicija 5.7. Prsten R je **tijelo**, ili **prsten s dijeljenjem**, ako je svaki ne-nul element u R invertibilan; tj., ukoliko je

$$R^{\times} = R \setminus \{0\}.$$

Komutativno tijelo zove se **polje**.

Sljedeći pojam, *karakteristika prstena*, posebno je važan u teoriji polja.

Definicija 5.8. Neka je R prsten i pretpostavimo da postoji $m \in \mathbb{N}$ takav da je

$$m\,x = 0, \qquad \forall x \in R.$$

Definirajmo **karakteristiku prstena** R sa

$$\operatorname{char} R := \text{minimalan takav } m;$$

jasno, ako m uopće postoji. U suprotnom govorimo da je R *karakteristike nula*, i pišemo

$$\operatorname{char} R = 0.$$

5.2. Primjeri prstena i polja.

Pogledajmo sada neke prve primjere prstena; kako komutativnih, tako i nekih nekomutativnih. Posebno, dati ćemo i neke osnovne primjere polja.

Primjer 5.9. (***I***) *PRSTENI.*

(1) Prsten $\mathbb{Z}$; $\mathbb{Z}$ je integralna domena, $\operatorname{char} \mathbb{Z} = 0$ i $\mathbb{Z}^{\times} = \{\pm 1\}$.

(2) Prsten $\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \dots, \overline{n-1}\}$, tzv. *prsten ostataka modulo* n. (To je specijalan slučaj *kvocijentnog prstena* R/I, gdje je R neki prsten, a I je neki ideal u R; o toj konstrukciji, koja je direktni analogon pojma kvocijentne grupe, u Teoriji grupa, govorit ćemo kasnije.) Primjetimo,

$$\mathbb{Z}/n\mathbb{Z} \text{ je integralna domena} \quad \Longleftrightarrow \quad n \text{ je prim broj};$$

npr., u $\mathbb{Z}/6\mathbb{Z}$ je $\overline{2}\,\overline{3} = \overline{0}$. Nadalje,

$$\operatorname{char}(\mathbb{Z}/n\mathbb{Z}) = n;$$

posebno ovdje primjetimo da za svaki $n \in \mathbb{N}_0$, postoji neki prsten čija je karakteristika baš n. (Kasnije ćemo pokazati da karakteristika polja može biti ili 0 ili neki prim broj $p \in \mathbb{N}$.) Za invertibilne elemente imamo

$$(\mathbb{Z}/n\mathbb{Z})^{\times} = \{\overline{k} \mid k \in \{1, \dots, n-1\} \text{ takav da } (n,k) = 1\}.$$

(3) *Prsteni polinoma*

$$\mathbb{K}[X], \quad \mathbb{K}[X_1, \dots, X_n], \qquad \text{za } \mathbb{K} = \mathbb{R}, \mathbb{C}, \mathbb{Q}, \dots$$

Općenitije, mogu se gledati $\mathcal{A}[X]$ i $\mathcal{A}[X_1,\ldots,X_n]$, prsteni polinoma u jednoj i više varijabli sa koeficijentima iz nekog komutativnog prstena $\mathcal{A}$; tako je npr. za teoriju brojeva, ali isto tako i za komutativnu algebru, vrlo interesantan primjer prstena $\mathbb{Z}[X_1,\ldots,X_n]$, prstena polinoma u n varijabli sa cijelim koeficijentima. (Mi ćemo u daljnjem još proučavati prstene polinoma, posebno u Odjeljku 8.)

(4) *Prsteni formalnih redova* sa koeficijentima iz nekog polja; ili, općenitije, prsteni formalnih redova

$$\mathcal{A}[[X]], \quad \mathcal{A}[[X_1,\ldots,X_n]],$$

sa koeficijentima iz nekog komutativnog prstena $\mathcal{A}$. Imamo općenito, za svaki $n\in\mathbb{N}$,

$$\mathcal{A}[X_1,\ldots,X_n] \leq \mathcal{A}[[X_1,\ldots,X_n]];$$

tj., prsten polinoma je potprsten prstena formalnih redova.

(5) *Prsteni neprekidnih funkcija*

$$C(\Delta) := \{f : \Delta \to \mathbb{R} \mid f \text{ je neprekidna funkcija}\}, \qquad \Delta \subseteq \mathbb{R}^n.$$

Da bismo vidjeli kako se doista radi o prstenu moramo se samo podsjetiti, dobro poznatih činjenica iz Analize, da su i zbroj i produkt dvije neprekidne funkcije također neprekidne funkcije. Jasno, ovdje su zbrajanje i množenje funkcija definirani "po točkama", tj. za dvije funkcije $f,g:\Delta\to\mathbb{R}$ definiramo njihov *zbroj* $f+g$, odnosno *produkt* $f\,g$, kao

$$\begin{aligned}(f+g)(x) &:= f(x)+g(x),\\ (f\,g)(x) &:= f(x)\,g(x), \qquad x\in\Delta.\end{aligned}$$

(6) *Prsteni cijelih funkcija*

$$\mathcal{H}(\mathbb{C}) := \{f : \mathbb{C}\to\mathbb{C} \mid f \text{ je cijela funkcija}\};$$

podsjetimo se da je $f:\mathbb{C}\to\mathbb{C}$ *cijela funkcija* ukoliko je ona derivabilna u svakom $z\in\mathbb{C}$. Sada, jasno, i ovdje se radi o prstenu budući su dobro poznate činjenice da je i zbroj i produkt od dvije derivabilne funkcije ponovo derivabilna funkcija; jedinica u $\mathcal{H}(\mathbb{C})$ je funkcija $f:\mathbb{C}\to\mathbb{C}$, $f(z):=1$ za svaki $z\in\mathbb{C}$, tj. konstanta 1.

U sljedećim važnim primjerima promatramo nekomutativne prstene.

(7) *Prsten matrica*

$$M_n(\mathbb{K}) := \{(x_{ij}) \mid x_{ij}\in\mathbb{K}\},$$

reda n-puta-n sa koeficijentima iz nekog polja $\mathbb{K}=\mathbb{R},\mathbb{C},\mathbb{Q},\ldots$; to je prsten uz standardno zbrajanje i množenje matrica. Jedinica u tom prstenu je $\boldsymbol{I}=\boldsymbol{I}_n$, dok je neutral za zbrajanje *nul-matrica* $\mathbf{0}$, matrica koja svuda ima 0. Nadalje,

$$M_n(\mathbb{K}) \text{ je integralna domena} \quad\Longleftrightarrow\quad n=1.$$

Primjetimo ovdje još da je karakteristika

$$\operatorname{char} M_n(\mathbb{K}) = \operatorname{char}\mathbb{K},$$

te da je skup invertibilnih elemenata u prstenu $M_n(\mathbb{K})$ jednak

$$M_n(\mathbb{K})^\times = \mathrm{GL}_n(\mathbb{K}),$$

tj. jednak dobro nam poznatoj općoj lineranoj grupi.

Napomenimo ovdje kako se ponekad promatraju i prsteni $M_n(R)$, n-puta-n matrica sa koeficijentima iz nekog, ne nužno komutativnog, prstena s jedinicom R.

(8) Promatrajmo sada neku abelovu grupu $\mathcal{A} = (\mathcal{A}, +)$, i onda skup $\operatorname{End}\mathcal{A}$, svih endomorfizama od $\mathcal{A}$. Ako na tom skupu definiramo *zbrajanje* "po točkama"

$$(f+g)(a) := f(a) + g(a), \qquad \forall f, g \in \operatorname{End}\mathcal{A},$$

te *"množenje"* kao kompoziciju funkcija

$$\operatorname{End}\mathcal{A} \times \operatorname{End}\mathcal{A} \ni (f, g) \longmapsto f\,g := f \circ g \in \operatorname{End}\mathcal{A},$$

onda je $\operatorname{End}\mathcal{A}$ (nekomutativan) prsten. Neutral za zbrajanje u tom prstenu je nul-endomorfizam $\mathcal{A} \ni a \mapsto 0 = 0_{\mathcal{A}}$, dok je jedinica toga prstena *identiteta*

$$\imath : \mathcal{A} \to \mathcal{A}, \qquad \imath(a) := a \quad \forall a \in \mathcal{A}.$$

(9) Neka je G proizvoljna grupa i neka je R proizvoljan prsten s jedinicom 1. Definirajmo skup

$$\begin{aligned} R[G] &:= \{\varphi : G \to R \mid \varphi(g) \neq 0 \text{ za konačno mnogo } g \in G\} \\ &= \Big\{\sum_{i=1}^{n} r_i g_i \mid r_i \in R,\ \ g_i \in G\Big\}, \end{aligned}$$

te na njemu promatrajmo operaciju *zbrajanja* "po komponentama"

$$(\varphi + \psi)(g) := \varphi(g) + \psi(g), \qquad \forall g \in G.$$

Tako je zapravo $(R[G], +)$ aditivna grupa izomorfna direktnoj sumi od $\operatorname{card} G$ primjeraka aditivne grupe $(R, +)$, tj.

$$(R[G], +) \cong \bigoplus_{g \in G} (R, +).$$

Sada na $R[G]$ definirajmo i operaciju množenja ovako:

$$\Big(\sum_{i=1}^{m} r_i g_i\Big) * \Big(\sum_{j=1}^{n} s_j h_j\Big) := \sum_i \sum_j (r_i s_j)\, g_i h_j.$$

Tojest, ako elemente koje množimo zapišemo kao funkcije $\varphi = \sum_{g \in G} r_g g$ i $\psi = \sum_{h \in G} s_h h$, gdje je samo konačno mnogo $r_g, s_h \in R$ različito od nule, onda je

$$(\varphi * \psi)(x) := \sum_{\substack{(g,h) \in G \times G \\ g\,h = x}} \varphi(g)\psi(h) = \sum_{\substack{(g,h) \in G \times G \\ g\,h = x}} r_g\, s_h;$$

množenje $(\varphi, \psi) \mapsto \varphi * \psi$, za $\varphi, \psi : G \to R$, zove se **konvolucijsko množenje**. Sada je lako provjeriti da je

$$R[G] = (R[G], +, *)$$

prsten; on se zove **grupni prsten**, za G i R. Jedinica u tom prstenu je $\varepsilon := 1\,e$, tj. funkcija

$$\varepsilon : G \to R, \qquad \varepsilon(x) := \begin{cases} 1, & x = e, \\ 0, & \text{inače;} \end{cases}$$

jasno, e je neutral u grupi G.

Primjetimo da za grupu G, te prstene R i $R[G]$, imamo:

$$R[G] \text{ komutativan} \iff G \text{ komutativna} \quad i \quad R \text{ komutativan}.$$

(***II***) *POLJA.*

(1) Prvi i osnovni primjeri polja, koji su fundamentalni objekti u svim granama matematike, su **polje racionalnih brojeva** $\mathbb{Q}$, **polje realnih brojeva** $\mathbb{R}$ i **polje kompleksnih brojeva** $\mathbb{C}$; operacije zbrajanja i množenja standardno su definirane. Jasno, imamo $\mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$.

(2) Kao prve primjere *konačnih polja* imamo prstene ostataka modulo p, kada je taj $p \in \mathbb{N}$ prim broj; tj.,

$$\mathbb{Z}/p\mathbb{Z} \text{ je polje} \iff p \text{ je prim broj.}$$

Primjetimo ovdje (vidi primjer (2) u (***I***)) da za prstene ostataka modulo n vrijedi ekvivalencija: $\mathbb{Z}/n\mathbb{Z}$ je polje akko je $\mathbb{Z}/n\mathbb{Z}$ integralna domena akko je n prim broj. (Ta je činjenica zapravo samo specijalan slučaj općenitog fenomena koji govori da je *svaka konačna integralna domena polje.* Taj se rezultat dokazuje u dva koraka. Prvi je vrlo jednostavan i govori da je svaka konačna integralna domena tijelo (vidi Propoziciju 10.5). Drugi korak, koji je dosta kompliciraniji, predmet je tzv. *Wedderburnovog teorema* koji kaže da je svako konačno tijelo štoviše i polje; tj., čim imamo konačnost imamo i komutativnost.)

(3) Pretpostavimo da je $d \in \mathbb{Z} \setminus \{0, 1\}$ *kvadratno slobodan*, tj. da je $d = -1$ ili $|d| = p_1 p_2 \cdots p_k$, gdje su $p_i \in \mathbb{N}$ u parovima međusobno različiti prim brojevi. Definirajmo skup brojeva

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

na kojem promatramo standardne operacije zbrajanja i množenja, naslijeđene iz $\mathbb{C}$. Lako je provjeriti da je to onda polje, koje se zove **kvadratno proširenje** od $\mathbb{Q}$ određeno sa d (vidi Zadatak 41). Napomenimo ovdje kako su kvadratna proširenja od $\mathbb{Q}$ tek (važan) dio klase tzv. polja algebarskih brojeva, gdje je polje $\mathbb{Q} \subseteq \mathbb{K} \subseteq \mathbb{C}$ tzv. **polje algebarskih brojeva** ukoliko je $\mathbb{K}$, gledan kao vektorski prostor nad $\mathbb{Q}$, konačnodimenzionalan (vidi Odjeljak 10).

Zadatak 37. Dokažite, kao što je rečeno u (***I***)-(9) u Primjeru 5.9, da je za proizvoljnu grupu G i proizvoljan prsten R skup $R[G] = (R[G], +, *)$ doista prsten s jedinicom.

Zadatak 38. Dokažite da je svaka konačna integralna domena tijelo.

U vezi sa prethodnim zadatkom, i u (***II***)-(2) u Primjeru 5.9 spomenutom Wedderburnovom teoremu, primjetimo kako ne postoji konačno tijelo koje nije polje. Sad je prirodno pitanje: *Postoje li uopće tijela koja nisu polja?* Odgovor je potvrdan, i kao najvažnije primjere takvih struktura imamo tzv. *kvaternione.* O njima će biti riječi u Pododjeljku 10.2

5.3. Definicije homomorfizma i direktnog produkta prstena.

NAPOMENA. (1) Ako ne kažemo drukčije, od sada nadalje, u cijelom ovom poglavlju, smatramo

$$\underline{Prsten} \equiv \text{Prsten s jedinicom } 1.$$

(2) U cijelom poglavlju, ako ne naglasimo drugačije, kada kažemo da je "A prsten" smatramo da je to *komutativan* prsten. (Jasno, "A" asocira da je prsten *abelov.*) S druge strane, ako je riječ o prstenima $R, S, \ldots$, oni će biti bilo komutativni ili ne.

Sada, kao i kod grupa, sljedeće osnovno pitanje je kakova preslikavanja među prstenima treba gledati. Sasvim analogno, kao i za grupe, i ovdje ćemo gledati ona preslikavanja koja "čuvaju strukturu"; tj., preslikavanja među prstenima koja respektiraju obje operacije, i zbrajanje i množenje u prstenu.

Definicija 5.10. Neka su R i S dva prstena. Preslikavanje $f : R \to S$ je **homomorfizam** prstena ukoliko je i aditivno i multiplikativno, tj. ako vrijedi

$$f(x+y) = f(x) + f(y) \quad \& \quad f(x\,y) = f(x)\,f(y), \qquad \forall x, y \in R,$$

te ako je

$$f(1_R) = 1_S,$$

tj. ako "f šalje jedinicu u jedinicu". Sa $\mathrm{Hom}(R, S)$ označavamo skup svih homomorfizama iz R u S. Homomorfizam f koji je još i injekcija naziva se **monomorfizam**, f koji je i surjekcija zovemo **epimorfizam**, a homomorfizam koji je i mono- i epi-, tj. bijektivan homomorfizam, zovemo **izomorfizam**. Za dva prstena R i S reći ćemo da su *izomorfni*, ako postoji neki izomorfizam f među njima; tu činjenicu označavamo sa

$$R \cong S.$$

(Jasno, kao i kod grupa, i ovdje je relacija "biti izomorfan" relacija ekvivalencije na skupu svih prstena.)

Posebno, ako je $R = S$, tj. ako imamo homomorfizam $f : R \to R$, onda kažemo da je f **endomorfizam** od R. Sa $\mathrm{End}\, R$ označavat ćemo skup svih endomorfizama od R. Endomorfizam koji je još i bijekcija zove se **automorfizam** od R. Sa $\mathrm{Aut}\, R$ označavamo skup svih automorfizama od R.

Za proizvoljan homomorfizam $f : R \to S$ definirajmo njegovu **jezgru**

$$\mathrm{Ker}\, f := f^{-1}(\{0_S\}) = \{x \in R \mid f(x) = 0\},$$

i njegovu **sliku**

$$\mathrm{Im}\, f := f(R) = \{f(x) \mid x \in R\}.$$

Napomena 5.11. Primjetimo ovdje kako smo u gornjoj definiciji homomorfizma prstena mogli ispustiti uvjet "$f(1_R) = 1_S$"; zapravo, ukoliko su R i S prsteni bez jedinice, onda je taj uvjet i besmislen. No s druge strane, primjetimo da u slučaju kad su R i S prsteni s jedinicom, a S je štoviše i integralna domena, onda za svako multiplikativno preslikavanje $f : R \to S$ imamo jednu i samo jednu od ove dvije mogućnosti: ili f šalje 1_R u 1_S, ili je f trivijalan homomorfizam, tj. imamo $f(r) = 0_S$ za svaki $r \in R$. Naime, ako u uvjet multiplikativnosti $f(x\,y) = f(x)f(y)$ stavimo $x = y = 1_R$, dobivamo

$$f(1_R) = f(1_R)f(1_R) \quad \Longleftrightarrow \quad f(1_R)\big(1_S - f(1_R)\big) = 0_S.$$

No kako je S domena, to iz zadnje jednakosti slijedi da je: ili $f(1_R) = 1_S$, ili $f(1_R) = 0_S$. Ali za drugu od te dvije mogućnosti imamo

$$f(r) = f(r\,1_R) = f(r)f(1_R) = f(r)0_S = 0_S \qquad \forall r \in R.$$

Sljedeća je jednostavna lema direktan analogon odgovarajućeg rezultata za grupe; i dokaz je potpuno isti kao tamo.

Lema 5.12. *Ako su $f : R \to S$ i $g : S \to T$ homomorfizmi prstena, onda je i njihova kompozicija $g \circ f : R \to T$ također homomorfizam prstena. Štoviše, ako su f i g oba monomorfizmi (tj. epimorfizmi, izomorfizmi), onda je i $g \circ f$ monomorfizam (tj. epimorfizam, izomorfizam).*

Neka su sada R i S dva prstena. Na Kartezijevom produktu $R\times S$ definirajmo zbrajanje i množenje "po komponentama"; tj.

$$\begin{aligned}(r_1, s_1) + (r_2, s_2) &:= (r_1 + r_2, s_1 + s_2),\\ (r_1, s_1)\,(r_2, s_2) &:= (r_1 s_1, r_2 s_2), \qquad \forall (r_1, s_1), (r_2, s_2) \in R \times S.\end{aligned}$$

Tada $R\times S$, sa tim operacijama, ima strukturu prstena; element $(0, 0) = (0_R, 0_S)$ je neutral za zbrajanje, a element $(1, 1) = (1_R, 1_S)$ je jedinica. Prsten $R \times S$ zove se *produkt prstena* R i S. (Kao jedan od prvih primjera možemo promatrati $\mathbb{Z}\times\mathbb{Z}$, skup parova cijelih brojeva u kojem zbrajamo i množimo "po komponentama".) Zapravo, produkt prstena nije ništa drugo nego direktan produkt aditivnih grupa $(R, +)$ i $(S, +)$, na kojem je još definirana i operacija množenja. Sasvim općenito, imamo ovu definiciju.

Definicija 5.13. Ako su $(R_\lambda, \lambda \in \Lambda)$ prsteni, definiramo

$$\prod_{\lambda\in\Lambda} R_\lambda := \{f : \Lambda \to \bigcup_{\Lambda} R_\lambda \mid f(\lambda) \in R_\lambda\},$$

sa zbrajanjem i množenjem "po komponentama"

$$(f + g)(\lambda) := f(\lambda) + g(\lambda) \quad \& \quad (f \cdot g)(\lambda) := f(\lambda) \cdot g(\lambda);$$

tako je dobiven prsten $(\prod_{\lambda\in\Lambda} R_\lambda, +, \cdot)$, koji se zove **direktan produkt prstena** $(R_\lambda)_\Lambda$.

Potprsten

$$\bigoplus_{\lambda\in\Lambda} R_\lambda := \{f \in \prod_{\lambda\in\Lambda} R_\lambda \mid f(\lambda) \neq 0_\lambda \text{ za konačno mnogo } \lambda \in \Lambda\},$$

od direktnog produkta $\prod_{\lambda\in\Lambda} R_\lambda$, zove se **direktna suma prstena** $(R_\lambda)_\Lambda$; jasno, ovdje je sa 0_λ označen neutral za zbrajanje u grupi $(R_\lambda, +)$.

Napomena 5.14. (1) Za skup indeksa Λ konačan, tj. kada je $\Lambda = \{1, \ldots, n\}$, onda je

$$R_1 \times \cdots \times R_n = \prod_{i=1}^{n} R_i = \bigoplus_{i=1}^{n} R_i = R_1 \oplus \cdots \oplus R_n.$$

Sada elemente produkta, tj. sume prstena R_i, zapisujemo kao n-torke $(r_1, \ldots, r_n)$, $r_i \in R_i$, i onda su zbrajanje i množenje doista "uobičajeno" zbrajanje i množenje po komponentama.

(2) Primjetimo da je direktan produkt prstena s jedinicom ponovo prsten s jedinicom; sasvim precizno, ako sa 1_λ označimo jedinicu u prstenu R_λ, onda je sa $\mathbf{1}$, $\mathbf{1}(\lambda) := 1_\lambda$ za

svaki $\lambda \in \Lambda$, definirana jedinica u produktu. S druge pak strane, jasno je da će direktna suma prstena s jedinicom imati jedinicu akko je skup indeksa Λ konačan.

(* * *)

Na kraju ovog uvodnog odjeljka dajemo još nekoliko instruktivnih zadataka.

Zadatak 39. (i) Dokažite, kao što je navedeno u ($\boldsymbol{I}$)-(8) Primjera 5.9, da je za proizvoljnu abelovu grupu $\mathcal{A} = (\mathcal{A}, +)$ skup $\operatorname{End} \mathcal{A}$ doista prsten s jedinicom $\imath$.

(ii) Dokažite da je u slučaju $\mathcal{A} = \mathbb{Q}^n = \mathbb{Q} \times \cdots \times \mathbb{Q}$, n primjeraka od $\mathbb{Q} = (\mathbb{Q}, +)$, prsten $\operatorname{End} \mathcal{A}$ izomorfan prstenu $M_n(\mathbb{Q})$, n-puta-n matrica sa koeficijentima iz $\mathbb{Q}$.

(iii) Dokažite da se prsten $M_n(\mathbb{R})$ može shvatiti kao potprsten od $\operatorname{End} \mathbb{R}^n$. Jesu li prsteni $M_n(\mathbb{R})$ i $\operatorname{End} \mathbb{R}^n$ izomorfni?

Zadatak 40. Dokažite da su polja $\mathbb{Q}$, $\mathbb{R}$ i $\mathbb{C}$ međusobno neizomorfna.

Zadatak 41. (i) Dokažite da je za $d \in \mathbb{Z} \backslash \{0, 1\}$ kvadratno slobodan, skup $\mathbb{Q}(\sqrt{d})$ doista potpolje od $\mathbb{C}$.

(ii) Dokažite da se $\mathbb{Q}(\sqrt{d})$ može shvatiti kao $\mathbb{Q}$-vektorski prostor, te da je dimenzija $\dim_{\mathbb{Q}} \mathbb{Q}(\sqrt{d}) = 2$.

(iii) Za $d_1, d_2 \in \mathbb{Z} \setminus \{0, 1\}$ kvadratno slobodne vrijedi: $d_1 = d_2$ akko su polja $\mathbb{Q}(\sqrt{d_1})$ i $\mathbb{Q}(\sqrt{d_2})$ međusobno izomorfna.

Napomena 5.15. Podsjetimo se da za bilo koje brojeve $a, b \in \mathbb{R}$ i $n \in \mathbb{N}$ vrijedi tzv. *Binomni teorem* o razvoju $(a + b)^n$, n-te potencije binoma $a + b$. No taj se rezultat direktno poopćava na slučaj kada se polje $\mathbb{R}$ zamijeni proizvoljnim komutativnim prstenom. Preciznije, imamo ovaj teorem.

Teorem. (Binomni teorem)
Neka je A komutativan prsten. Tada za proizvoljne $x, y \in A$ i $n \in \mathbb{N}$ imamo

$$(x + y)^n = \sum_{k=0}^{n} \binom{n}{k} x^{n-k} y^k = x^n + \binom{n}{1} x^{n-1} y + \cdots + \binom{n}{n-1} x y^{n-1} + y^n.$$

Naravno, ovdje su $\binom{n}{k} \in \mathbb{N}$ *binomni koeficijenti*, definirani na uobičajen način.

Zadatak 42. (i) Dokažite gore navedeni Binomni teorem; preciznije rečeno, uvjerite se da je njegov dokaz *potpuno isti* kao i dokaz "klasičnog" Binomnog teorema za slučaj $A = \mathbb{R}$.

(ii) Dokažite da za $A = \mathbb{Z}/p\mathbb{Z}$, gdje je $p \in \mathbb{N}$ prim broj, i proizvoljne $x, y \in A$ vrijedi

$$(x + y)^p = x^p + y^p.$$

(*Uputa:* Pokažite da je svaki binomni koeficijent $\binom{p}{k}$ djeljiv prim brojem p, a zatim iskoristite činjenicu da je $\operatorname{char} A = p$.)

6. Ideali

Za bolje razumijevanje strukture grupa, te da bismo dobivali nove grupe iz već poznatih, promatrali smo njihove podgrupe i posebno normalne podgrupe. U Teoriji prstena centralno mjesto pripada tzv. *idealima.* Malo ležernije govoreći, ideali su za prstene ono što su normalne podgrupe za grupe.

6.1. Definicija ideala, operacije na idealima i kvocijentni prsten.

U ovom pododjeljku najprije uvodimo pojam (dvostranog) ideala u prstenu. Zatim na skupu $\mathrm{Id}\, R$, svih ideala nekog prstena R, uočavamo tri "prirodne" binarne operacije. To su *presjek* $I \cap J$, *zbroj* $I + J$ i *produkt* IJ; gdje su $I, J \in \mathrm{Id}\, R$ proizvoljni.

Definicija 6.1. Neka je R prsten. Podskup $I \subseteq R$ je **lijevi** (tj. **desni**) **ideal** u R ako su ispunjena sljedeća dva uvjeta:

(**1**) I je potprsten od R;

(**2**) Za sve $r \in R$ i $x \in I$ je $r\,x \in I$ (tj. $x\,r \in I$).

Gornji uvjet (**2**) često se simbolički piše kao

$$R\,I \subseteq I \qquad (\text{tj. } I\,R \subseteq I).$$

Podskup $I \subseteq R$ je (*dvostrani*) **ideal** ako je on istovremeni i lijevi i desni ideal. Činjenicu da je I ideal u prstenu R označavamo sa

$$I \trianglelefteq R.$$

Isto tako, koristit ćemo oznaku

$$\mathrm{Id}\, R := \text{skup svih ideala u } R.$$

Nadalje, reći ćemo da je ideal I od R **pravi ideal** ako je $I \neq R$ i $I \neq (0)$; ovdje je sa (0) označen **nul-ideal** $\{0\}$.

Napomena 6.2. (1) Primjetimo da nul-ideal doista je ideal; to je trivijalna posljedica činjenice da u svakom prstenu R njegova nula 0 zadovoljava $0\,x = x\,0 = 0$, za sve $x \in R$; vidi Napomenu 5.2.

(2) Lijevi, odnosno desni, ideali u prstenima zovu se i jednostranim idealima; za razliku od (dvostranih) ideala. Iako je, u nekomutativnoj teoriji, često potreba gledati razne jednostrane ideale, naglasimo da su ipak "pravi" objekti od interesa u algebri upravo ideali. Primjetimo još da je u slučaju *komutativnog* prstena R,

$$\text{ideal} \quad \equiv \quad \text{lijevi ideal} \quad \equiv \quad \text{desni ideal};$$

tj., u komutativnoj teoriji nema smisla govoriti o jednostranim idealima.

Primjer 6.3. (1) Svaki ideal $I \trianglelefteq \mathbb{Z}$ je oblika $I = n\mathbb{Z}$, $n \in \mathbb{N}_0$.

(2) Svaki ideal $I \trianglelefteq \mathbb{C}[X]$ je oblika $I = \mathbb{C}[X]\,f = \{\varphi\, f \mid \varphi \in \mathbb{C}[X]\}$, za neki polinom $f \in \mathbb{C}[X]$.

Sljedeća je lema sasvim jasna; jedino što treba iskoristiti je činjenica, koju smo dokazali, da je presjek neke familije podgrupa neke grupe ponovo podgrupa te grupe, te definiciju ideala.

Lema 6.4. *Neka je R proizvoljan prsten. Tada imamo:*

(i) *Ako je $\{R_\gamma;\ \gamma \in \Gamma\}$ neka familija potprstena od R, tada je i njihov skupovni presjek*
$$\bigcap_\Gamma R_\gamma$$
također potprsten od R.

(ii) *Ako je $\{I_\gamma;\ \gamma \in \Gamma\}$ neka familija ideala od R, tada je i njihov skupovni presjek*
$$\bigcap_\Gamma I_\gamma$$
također ideal od R.

Zadatak 43. Ako je $f : R \to S$ homomorfizam prstena, onda je jezgra $\operatorname{Ker} f \trianglelefteq R$ ideal, a slika $\operatorname{Im} f \leq S$ je potprsten.

Imajući na umu prethodnu lemu, uvodimo sljedeće pojmove.

Definicija 6.5. Neka je R prsten i $I \trianglelefteq R$ neki ideal. Skup $S \subseteq R$ je **skup generatora** od I ako je
$$I = \langle S \rangle = (S) := \bigcap_{\substack{J \trianglelefteq R \\ S \subseteq J}} J;$$
tj., I je najmanji ideal u R koji sadrži skup S. Ideal I je **konačno generiran** ako postoji konačan podskup $S \subseteq R$ takav da je $I = \langle S \rangle$. Ideal I je **glavni ideal** ako postoji neki element $r \in R$ takav da je $I = \langle r \rangle$. Kažemo da je R **prsten glavnih ideala**, ili kraće PGI, ako je svaki ideal u R glavni.

Napomena 6.6. (1) Pojmovi *konačno generiranih ideala* i *glavnih ideala* su fundamentalni u Algebri. Naime, grubo govoreći, ideali u prstenu koji su konačno generirani su pogodni za razna "računanja". Vezano uz to, u općenitoj je situaciji vrlo zanimljivo pitanje da se za dani konkretni ideal I u nekom prstenu R, ako znamo da je taj ideal konačno generiran, nađe neki skup generatora S. Štoviše, dobro je naći "minimalan" takav S; tj., takav S da je $\operatorname{card} S$ minimalan mogući. (Naravno, takav minimalan S "gotovo nikad" neće biti jedinstveno određen.)

(2) Klasa prstena R koji imaju svojstvo da je svaki ideal u R konačno generiran je vrlo velika, i moglo bi se reći da su "gotovo svi zanimljivi prsteni" takvi; posebno su takvi tzv. Noetherini prsteni (vidi Napomenu 9.17). S druge pak strane, PGI su "vrlo rijetki"; kao glavne reprezentante u toj potklasi navedimo prstene $\mathbb{Z}$ i $\mathbb{K}[X]$, za $\mathbb{K}$ proizvoljno polje (vidi Primjer 6.3). Kao primjere Noetherinih prstena, ali koji nisu PGI, navedimo prstene polinoma $\mathbb{K}[X_1, \ldots, X_n]$ u $n \geq 2$ varijabli, sa koeficijentima iz polja $\mathbb{K}$, te prsten polinoma $\mathbb{Z}[X]$; kasnije u ovom poglavlju dat ćemo dokaze rečenih tvrdnji.

Sada ćemo, pored presjeka, uvesti još dvije "prirodne" operacije na idealima, koje će nam, između ostalog, omogućiti da od ideala koje imamo dobijemo neke nove ideale.

Definicija 6.7. Za ideale $I, J \trianglelefteq R$ definirajmo njihov **zbroj** $I + J$ kao najmanji ideal u R koji sadrži $I \cup J$, te njihov **produkt** IJ kao najmanji ideal koji sadrži sve produkte elemenata $x\,y$, gdje su $x \in I$ i $y \in J$; tj.,

$$I + J := \langle I \cup J \rangle,$$
$$I\,J := \langle x\,y \mid x \in I,\ \ y \in J \rangle.$$

Analogno, ako su $I_1, \ldots, I_n \trianglelefteq R$ ideali, definiramo

$$I_1 + \cdots + I_n := \langle I_1 \cup \cdots \cup I_n \rangle,$$
$$I_1 \cdots I_n := \langle x_1 \cdots x_n \mid x_j \in I_j \rangle.$$

Sljedeća propozicija daje osnovna svojstva koja zadovoljavaju te dvije novouvedene operacije; osim toga, ta svojstva opravdavaju i uvedene nazive *zbroj ideala* i *produkt ideala.*

Propozicija 6.8. *Neka je R proizvoljan prsten, i neka su $I, J, K \trianglelefteq R$ ideali. Tada imamo:*

(i) $I + J = \{x + y \mid x \in I,\ \ y \in J\}$.

(ii) $IJ = \left\{\sum_{i=1}^{n} x_i y_i \mid x_i \in I,\ \ y_i \in J\ \ \&\ n \in \mathbb{N}\right\} \cup \{\,0\}$.

(iii) $(I + J) + K = I + (J + K) = I + J + K,$
$(I\,J)K = I(J\,K) = I\,J\,K.$

(iv) $I(J + K) = I\,J + I\,K,$
$(I + J)K = I\,K + J\,K.$

Dokaz. (i) Definirajmo skup

$$A := \{x + y \mid x \in I,\ \ y \in J\}.$$

Mi moramo pokazati da je taj skup A zapravo ideal, te da je $A = I + J$.

Sada, očito je $(A, +)$ abelova grupa; naime, za $x_1, x_2 \in I$ i $y_1, y_2 \in J$, te $x_1 + y_1, x_2 + y_2 \in A$ je

$$(x_1 + y_1) + (x_2 + y_2) = (x_1 + x_2) + (y_1 + y_2)\ \in A,$$

budući su posebno $(I, +)$ i $(J, +)$ abelove grupe. Isto tako, za bilo koje $r \in R$ i $a = x + y \in A$, gdje su $x \in I$ i $y \in J$, imamo

$$r\,a = r\,x\ +\ r\,y\ \in A;$$

tu naravno koristimo da su I i J posebno lijevi ideali pa su onda elementi $r\,x \in I$ i $r\,y \in J$. To znači da je A lijevi ideal u R. Ali sasvim analogno slijedi da je A i desni ideal; dakle, A je ideal, kako smo i tvrdili.

Nadalje, jer je posebno $0 \in J$ to imamo $I \ni x = x + 0 \in A$; tj., imamo inkluziju $I \subseteq A$. Analogno, imamo i inkluziju $J \subseteq A$; dakle, imamo i $I \cup J \subseteq A$. No to znači da *ideal* A sadrži uniju $I \cup J$; po definiciju zbroja ideala onda immao $I + J \subseteq A$. Za obratnu inkluziju, neka je $K \trianglelefteq R$ bilo koji ideal koji sadrži $I \cup J$. Onda je posebno

$$x + y \in K, \quad \forall x \in I,\ \forall y \in J;$$

tj., imamo $A \subseteq K$. Budući je K uzet proizvoljno, slijedi

$$A \subseteq \bigcap_{\substack{K \trianglelefteq R \\ I \cup J \subseteq K}} K = \langle I \cup J \rangle = I + J;$$

tako smo dokazali $I + J = A$, kako smo i tvrdili.

(ii) Analogno kao u (i), definirajmo skup

$$A := \{\sum_{i=1}^{n} x_i y_i \mid x_i \in I, \;\; y_i \in J \;\; \& \, n \in \mathbb{N}\} \cup \{0\}.$$

Jasno je da je $(A, +)$ abelova grupa; naime kad zbrojimo dvije konačne sume oblika $\sum x_i y_i$, ponovo dobijemo *konačnu* sumu istog oblika. Isto tako, za $r \in R$ i konačnu sumu $\sum x_i y_i \in A$ je

$$r \left(\sum x_i y_i\right) = \sum (r\, x_i) y_i \in A;$$

ovdje koristimo da je I ideal, pa onda imamo $r\, x_i \in I$ za sve i. Slijedi, A je lijevi ideal. Analogno, A je i desni ideal, tj. on je ideal. Za drugi korak, treba najprije primjetiti da A sadrži sve generatore $x\, y$ od ideala $I\, J$. Slijedi, $I\, J \subseteq A$. Za obratnu inkluziju, uzmemo proizvoljan ideal $K \trianglelefteq R$ koji sadrži skup $S := \{x\, y \mid x \in I, \;\; y \in J\}$. No onda, jer je posebno K zatvoren za zbrajanje, imamo da K sadrži i ideal A. Zbog proizvoljnosti od K, slijedi, po istom argumentu kao u (i), da je $A \subseteq I\, J$.

(iii) i (iv) Te su tvrdnje sada, kada imamo (i) i (ii), sasvim jasne. (Ako osjećate potrebu, detalje napišite sami!) □

Zadatak 44. Dokažite, da za svaka dva ideala I i J u proizvoljnom prstenu R vrijedi

$$I\, J \subseteq I \cap J.$$

Pokažite primjerima da su gore moguće i jednakost, ali isto tako i stroga inkluzija.

Sada, u potpunoj analogiji sa pojmom kvocijentne grupe, definiramo i pojam *kvocijentnog prstena.* Jedine su razlike te što kod prstena ono po čemu "cijepamo" je ideal (a sjetimo se da smo rekli da ideali u Teoriji prstena korespondiraju normalnim podgrupama u Teoriji grupa), te da sada imamo dvije "unutarnje" operacije, zbrajanje i množenje, za razliku od grupa gdje imamo samo jednu operaciju "u igri".

Najprije, ako je R neki prsten i I neki njegov ideal, onda je posebno $(R, +)$ aditivna, komutativna, grupa i posebno je $(I, +)$ normalna podgrupa. Tako ima smisla definirati kvocijentnu, aditivnu, grupu

$$R/I = (R, +)/(I, +).$$

Cilj nam je tu aditivnu, komutativnu, grupu štoviše "organizirati" u prsten.

Teorem 6.9. *Neka je R prsten i $I \trianglelefteq R$ bilo koji ideal. Ako na kvocijentnoj, aditivnoj, grupi R/I definiramo množenje iz $R/I \times R/I$ u R/I sa*

$$(x + I)\,(y + I) := x\, y + I, \qquad x, y \in R,$$

onda R/I ima strukturu prstena; zove se **kvocijentni prsten** *od R po I. Nadalje, preslikavanje*

$$\pi = \pi_I : R \to R/I, \qquad x \mapsto x + I,$$

je epimorfizam prstena; zove se **kanonski epimorfizam**, *ili* **kanonska surjekcija**.

Napomena 6.10. Primjetimo da je jezgra kanonske surjekcije π jednaka

$$\mathrm{Ker}\, \pi = I.$$

Dokaz. Ono što treba vidjeti je to da je gornje množenje dobro definirano; tj., da ne ovisi o uzetim reprezentantima. Pa neka su x, x' i y, y' elementi iz R takvi da je $x + I = x' + I$ i $y + I = y' + I$. Mi moramo pokazati da je

$$(x + I)(y + I) = x\,y + I = \ ? \ = x'\,y' + I = (x' + I)(y' + I).$$

U tu svrhu, primjetimo da je

$$x\,y + I = x'\,y' + I \quad \Longleftrightarrow \quad x\,y - x'y' = x(y - y') + (x - x')y' \in I.$$

Ali, kako je $x + I = x' + I$ ekvivalentno $x - x' \in I$, te $y + I = y' + I$ ekvivalentno $y - y' \in I$, to je doista $x(y - y') + (x - x')y' \in I$; tu koristimo da je I ideal, tj. i lijevi i desni.

Konačno, da vidimo kako se radi o prstenu, treba samo primjetiti da se i asocijativnost množenja i distributivnost množenja prema zbrajanju "naslijeđuju" iz R. Jasno, $0_{R/I} = 0 + I = I$ je nula u R/I, a $1_{R/I} = 1_R + I = 1 + I$ je jedinica. □

Ovaj pododjeljak završavamo dvama jednostavnim zadacima. Posebno u drugom zadatku pretpostavljamo da se znaju osnovne stvari o polinomima; za više detalja vidite Odjeljak 8.

Zadatak 45. Neka je $\mathcal{A} := \{a + b\sqrt{6} \mid a, b \in \mathbb{Z}\}$ i $\mathcal{B} := \{2a + 3b\sqrt{6} \mid a, b \in \mathbb{Z}\}$. Da li je $\mathcal{A}$ prsten? Da li je $\mathcal{B}$ potprsten od $\mathcal{A}$? Da li je $\mathcal{B}$ ideal u $\mathcal{A}$?

Zadatak 46.

(i) U prstenu polinoma $\mathcal{A} := \mathbb{Z}[X]$ definiramo podskup
$$\mathcal{B} := \{f(X) = a_0 + 5a_1X + a_2X^2 + \cdots + a_nX^n \mid a_i \in \mathbb{Z}\};$$
tj., $\mathcal{B}$ je skup onih polinoma iz $\mathcal{A}$ kojima je koeficijent uz X cijeli broj djeljiv s 5. Da li je $\mathcal{B}$ potprsten od $\mathcal{A}$? Da li je $\mathcal{B}$ ideal u $\mathcal{A}$?

(ii) U prstenu polinoma $\mathcal{A} := \mathbb{Z}[X]$ definiramo podskup
$$\mathcal{B} := \{f(X) = a_0 + 3a_1X + 3a_2X^2 + \cdots + 3a_nX^n \mid a_i \in \mathbb{Z}\};$$
tj., $\mathcal{B}$ je skup onih polinoma iz $\mathcal{A}$ kojima su svi koeficijenti, osim slobodnog, cijeli brojevi djeljivi s 3. Da li je $\mathcal{B}$ potprsten od $\mathcal{A}$? Da li je $\mathcal{B}$ ideal u $\mathcal{A}$?

6.2. Prosti i maksimalni ideali; spektar i maksimalni spektar.

Kao što smo već rekli, da bismo bolje razumijeli strukturu nekog prstena R, trebaju nam razne informacije o skupu $\operatorname{Id} R$. No taj će skup u pravilu biti "prevelik", pa se onda namjesto svih ideala u R gledaju neke zanimljive potklase ideala. Tu prvenstvenu ulogu imaju tzv. *spektar* $\operatorname{Spec} R$ i *maksimalni spektar* $\operatorname{Max} R$; iste ćemo sada definirati.

Definicija 6.11. Ideal $P \trianglelefteq R$ je **prost ideal** ako je $P \neq R$ i ako vrijedi sljedeći uvjet:

Ako su $I, J \trianglelefteq R$ ideali takvi da je $I\,J \subseteq P$, onda je ili $I \subseteq P$ ili $J \subseteq P$.

Skup svih prostih ideala u R označavamo sa

$$\operatorname{Spec} R,$$

i zovemo **spektar** prstena R.

Ideal $P \trianglelefteq R$ je **potpuno prost ideal** ako je $P \neq R$ i ako vrijedi sljedeći uvjet:

Ako su elementi $x, y \in R$ takvi da je $x\,y \in P$, onda je ili $x \in P$ ili $y \in P$.

Skup svih potpuno prostih ideala u R označavamo sa

$$\operatorname{Spec}_c R.$$

(Indeks "c" u gornjoj oznaci dolazi od engl. naziva "*completely prime*" za potpuno proste ideale.)

Ideal $M \trianglelefteq R$ je **maksimalan ideal** ako je $M \neq R$ i ako vrijedi sljedeći uvjet:

Ako je $I \trianglelefteq R$ ideal takav da je $M \subseteq I \subset R$, onda je $M = I$;

tj., ako je M maksimalan element u skupu $\operatorname{Id} R$, s obzirom na inkluziju $\subseteq$. Skup svih maksimalnih ideala u R označavamo sa

$$\operatorname{Max} R,$$

i zovemo **maksimalni spektar**, ili kraće **max-spektar**, prstena R; u upotrebi je još i oznaka $\operatorname{Spm} R$ za maksimalni spektar.

Ideal $S \trianglelefteq R$ je **poluprost ideal** ako je S presjek neke familije prostih ideala; tj., ako postoji neki podskup $\Omega \subseteq \operatorname{Spec} R$ takav da je $S = \bigcap_{P \in \Omega} P$. Posebno, smatramo da je i sam prsten R poluprost ideal (to zapravo "odgovara" slučaju $\Omega = \emptyset$).

Sljedeća propozicija daje *karakterizaciju prostih ideala* u prstenu.

Propozicija 6.12. *Za ideal $P \trianglelefteq R$ sljedeće su tvrdnje međusobno ekvivalentne.*

(a) *P je prost ideal.*
(b) *Ako su $P \subset I, J \trianglelefteq R$ ideali, onda $I\,J \not\subseteq P$.*
(c) *U kvocijentu R/P je produkt bilo koja dva $\neq (0)$ ideala i sam $\neq (0)$ ideal.*
(d) *Ako su $x, y \in R$ takvi da je $xRy \subseteq P$, onda je ili $x \in P$ ili $y \in P$.*
(e) *Za proizvoljne $x, y \in R \setminus P$ postoji neki element $w \in R$ takav da $x\,w\,y \notin P$.*

Dokaz. Dokazat ćemo: (a)$\Rightarrow$(b)$\Rightarrow$(c)$\Rightarrow$(d)$\Rightarrow$(e)$\Rightarrow$(a).

(a)$\Rightarrow$(b) To je zapravo direktna posljedica definicije prostih ideala. (Neka je (a) i pretpostavimo da ne vrijedi (b); tj., pretpostavimo da postoje neki ideali I, J u R koji strogo sadrže P, ali je $IJ \subseteq P$. Jer je, po (a), P prost ideal, onda iz $IJ \subseteq P$ slijedi da je ili $I \subseteq P$ ili $J \subseteq P$. No, koja god od te dvije mogućnosti nastupila, imat ćemo kontradikciju sa činjenicom da "I i J strogo sadrže P".)

(b)$\Rightarrow$(c) Označimo $\overline{R} := R/P$, i onda pretpostavimo da su $\overline{I}$ i $\overline{J}$ dva ne-nul ideala od $\overline{R}$ čiji je produkt $\overline{I}\,\overline{J}$ nul-ideal. Za kanonski epimorfizam $\pi : R \to \overline{R}$ definirajmo podskupove $I, J \subseteq R$ kao praslike po π od ideala $\overline{I}, \overline{J} \trianglelefteq \overline{R}$; tj., $I := \pi^{-1}(\overline{I})$ i $J := \pi^{-1}(\overline{J})$. Sada se odmah vidi (vidi Propoziciju 7.2) da su I i J zapravo ideali od R, koji strogo sadrže P, te da je $IJ \subseteq P$ (jer je $\pi(IJ) = \pi(I)\pi(J) = \overline{I}\,\overline{J} = (0_{\overline{R}})$, i onda $IJ \subseteq \operatorname{Ker} \pi = P$; vidi Napomenu 6.10). Drugim riječima, dokazali smo $\neg$(c)$\Rightarrow \neg$(b).

(c)$\Rightarrow$(d) Pretpostavimo $\neg$(d), tj. da postoje neki elementi $x, y \in R$ takvi da je $xRy \subseteq P$, ali istovremeno $x \notin P$ i $y \notin P$. No onda, posebno, ideali $P + \langle x \rangle$ i $P + \langle y \rangle$ strogo sadrže P, i kao posljedicu toga imamo da su

$$\overline{X} := (P + \langle x \rangle)/P \qquad \& \qquad \overline{Y} := (P + \langle y \rangle)/P$$

ne-nul ideali u $\overline{R} = R/P$. S druge strane, koristeći Propoziciju 6.8, imamo

$$(P + \langle x\rangle)(P + \langle y\rangle) = PP + P\langle y\rangle + \langle x\rangle P + \langle x\rangle\langle y\rangle \subseteq P + \langle x\rangle\langle y\rangle \subseteq P;$$

tu smo najprije koristili činjenicu da je $PK \subseteq P$ i $KP \subseteq P$ za bilo koji ideal $K \trianglelefteq R$ (vidi Zadatak 44), a zatim činjenicu da iz $xRy \subseteq P$ slijedi $\langle x\rangle\langle y\rangle \subseteq P$. (Sasvim precizno, u vezi sa zadnjom implikacijom, ako je $xRy \subseteq P$, onda je $RxR\,RyR = RxRyR \subseteq RPR \subseteq P$, tj. $\langle x\rangle\langle y\rangle \subseteq P$.) Kao posljedicu svega, imamo očito da je $\overline{X}\,\overline{Y} = (0_{\overline{R}})$. Tako smo zapravo dokazali $\neg$(c).

(d)$\Rightarrow$(e) Pretpostavimo $\neg$(e), tj. da za neke $x, y \notin P$ *ne postoji* $w \in R$ takav da $x\,w\,y \notin P$. Znači, *za svaki* $w \in R$ je $x\,w\,y \in P$; tj., imamo $xRy \subseteq P$. Drugim riječima, pokazali smo $\neg$(d).

(e)$\Rightarrow$(a) Pretpostavimo da P nije prost ideal, tj. da postoje neka dva ideala $I, J \trianglelefteq R$ takva da je $IJ \subseteq P$, ali istovremeno $I \not\subseteq P$ i $J \not\subseteq P$. No onda za bilo koje elemente $x \in I \setminus P$ i $y \in J \setminus P$ *nije moguće naći* neki $w \in R$ takav da $x\,w\,y \notin P$; naime, $x\,w\,y = (x\,w)y \in IJ \subseteq P$, jer je $y \in J$, a $x \in I$ povlači $x\,w \in I$. □

Korolar 6.13. (i) *U proizvoljnom prstenu R je svaki potpuno prost ideal ujedno i prost; tj., imamo*

$$\operatorname{Spec}_c R \subseteq \operatorname{Spec} R.$$

(ii) *U proizvoljnom komutativnom prstenu A je ideal prost akko je on potpuno prost, tj. imamo*

$$\operatorname{Spec} A = \operatorname{Spec}_c A;$$

drugim riječima, u komutativnoj teoriji govorimo samo o prostim idealima.

Dokaz. (i) Doista, neka je P neki potpuno prost ideal, te pretpostavimo da su $x, y \in R$ neki elementi takvi da je $xRy \subseteq P$. Onda je posebno $x\,y = x\,1\,y \in P$. Ali P je potpuno prost, pa imamo da je $x \in P$ ili $y \in P$. Tako smo dokazali da P zadovoljava uvjet (d) iz prethodne propozicije; znači, to je prost ideal.

(ii) Jedino što treba primjetiti je ovo: Za ideal P u komutativnom prstenu A i za bilo koje $x, y \in A$, budući je $xAy = x\,yA$, imamo

$$x\,y \in P \quad\Longleftrightarrow\quad xAy \subseteq P.$$

□

Napomena 6.14. Budući su u komutativnoj teoriji potpuno prosti ideali isto što i prosti ideali, u mnogim se knjigama koje se bave komutativnim prstenima prosti ideali definiraju upravo uvjetom kojim smo mi definirali potpuno proste ideale; tj., *Ideal P u (komutativnom) prstenu A je prost ukoliko za $x, y \in A$ iz $x\,y \in P$ slijedi da je ili $x \in P$ ili $y \in P$.* (Napomenimo da se, općenito, dio neke algebarske teorije u kojoj se proučavaju samo *komutativne strukture* uobičajeno zove "komutativna teorija"; tako govorimo o "komutativnoj teoriji za grupe", o "komutativnoj teoriji za prstene", itd.)

Sljedeći nam je korak dokazati važan teorem o egzistenciji maksimalnih, a onda i prostih, ideala u proizvoljnom *prstenu s jedinicom*. No prije nego sam teorem dokažemo, načinimo malu digresiju; naime, u samom dokazu koristimo jedan fundamentalan rezultat Teorije skupova, tzv. *Zornovu lemu*.

Digresija. Pretpostavimo da je $(\Omega, \preceq)$ neki neprazan *parcijalno uređen skup.* Podskup $\mathcal{L} \subseteq \Omega$ zove se *lanac* u Ω, ako za svaka dva elementa $x, y \in \mathcal{L}$ imamo ili $x \preceq y$ ili $y \preceq x$; drugim riječima, u lancu su svaka dva elementa usporediva. Nadalje, element $\mu \in \Omega$ je *maksimalan element* u Ω ako vrijedi:

$$\textit{Za } a \in \Omega \textit{ takav da je } \mu \preceq a, \textit{ nužno je } \mu = a.$$

Ako je sada $\emptyset \neq \Omega' \subseteq \Omega$ i ako postoji neki $g \in \Omega$ takav da je $\omega' \preceq g$, $\forall \omega' \in \Omega'$, onda kažemo da je *g gornja međa*, ili *gornja ograda*, od Ω'. Sada možemo iskazati najavljeni rezultat.

Teorem. (Zornova lema)
Neka je $(\Omega, \preceq)$ neprazan parcijalno uredjen skup. Ako svaki *lanac u Ω ima gornju među, onda u Ω postoji* barem jedan *maksimalan element.*

Mi, naravno, nećemo dokazivati netrivijalnu činjenicu da je Zornova lema ekvivalentna Aksiomu izbora; dokaz se može vidjeti npr. u...

Teorem 6.15. *Neka je R prsten (s jedinicom).*

(i) *Ako je $I \neq R$ neki ideal u R, onda postoji barem jedan maksimalan ideal $M \trianglelefteq R$ takav da $I \subseteq M$. Kao posljedicu imamo da je skup* $\operatorname{Max} R$ *neprazan, tj. u R postoji barem jedan maksimalan ideal.*

(ii) *Ako je $M \trianglelefteq R$ maksimalan ideal, onda je on posebno i prost ideal. Drugim riječima, imamo*
$$\operatorname{Max} R \subseteq \operatorname{Spec} R;$$
kao posljedicu imamo da i prosti ideali postoje.

Napomena 6.16. Ako je R neki prsten i $R \neq I \trianglelefteq R$ ideal, može se dogoditi da nad I "sjedi" *beskonačno* mnogo (međusobno različitih) maksimalnih ideala; naravno, takav I sam ne može biti maksimalan. Mi ćemo kasnije vidjeti da se to npr. događa u prstenima polinoma. Ali isto tako, kao "ekstrem na drugu stranu", može se dogoditi da nad *svakim* $R \neq I \trianglelefteq R$ sjedi *samo jedan* maksimalan ideal. To će se npr. događati u komutativnim prstenima A kod kojih je skup $\operatorname{Max} A$ jednočlan. Iako to na prvi mah možda zvuči iznenađujuće, pokazuje se da postoji cijelo mnoštvo takovih prstena. Zbog svoje važnosti za (komutativnu) Algebru imaju posebno ime, *lokalni prsteni*; i predmet su proučavanja tzv. *Lokalne algebre.* Kao evidentne predstavnike lokalnih prstena imamo polja (vidi Propoziciju 6.20), no ona su zapravo nezanimljivi reprezentanti za Lokalnu algebru. Pravi se primjeri lokalnih prstena dobivaju kao "derivati" tzv. *lokalizacije* prstena...

Dokaz Teorema 6.15. (i) Definirajmo skup
$$\Omega = \Omega_I := \text{skup svih ideala } J \neq R \text{ takvih da je } I \subseteq J.$$
Budući je i sam I u Ω, jasno je da je to neprazan skup. Isto tako, taj je skup parcijalno uređen; naravno, uređaj je "obična" skupovna inkluzija $\subseteq$. Neka je sada $\mathcal{L}$ neki lanac u Ω, pa definirajmo
$$\Gamma := \bigcup_{J \in \mathcal{L}} J.$$
Jer, po definiciji skupa Ω, svaki $J \in \mathcal{L}$ sadrži ideal I, to onda i sam Γ sadrži I. Drugo, očito je taj Γ i sam ideal u R. I treće, $\Gamma \neq R$. (Naime, kad bi bilo $\Gamma = R$, onda bi bilo

posebno $1 \in \Gamma$, a onda $1 \in J$ za neki J, što povlači $J = R$; ali to proturiječi da je $J \in \Omega$.) Zaključak je da

$$\Gamma \in \Omega.$$

Još samo treba primjetiti da je taj Γ gornja međa od $\mathcal{L}$. Sada, budući je lanac $\mathcal{L}$ bio proizvoljan, po Zornovoj lemi slijedi da u Ω postoji barem jedan element M; tj., da nad I "sjedi" barem jedan maksimalan ideal M.

(ii) Pretpostavimo da je M neki maksimalan ideal u R, ali da on *nije prost*. To znači da postoje neka dva ideala $I, J \trianglelefteq R$ takva da je $IJ \subseteq M$, ali istovremeno $I \not\subseteq M$ i $J \not\subseteq M$. No onda je posebno $M \subset M + I$, što zbog maksimalnosti od M povlači da je $M + I = R$. Sasvim analogno, imamo i $M + J = R$. Slijedi

$$R = RR = (M + I)(M + J) = MM + MJ + IM + IJ \subseteq M.$$

No kako je i, jasno, $M \subseteq R$, proizlazi da je $M = R$; no to je kontradikcija s tim da je M maksimalan ideal. Tako je tvrdnja (ii) dokazana. $\square$

Napomena 6.17. Neka dosadašnja razmatranja o idealima možemo zorno ilustrirati sljedećom sličicom, u kojoj "$XY \longrightarrow UV$" znači da "XY povlači UV":

$$\begin{tikzcd} & I \text{ potpuno prost} \arrow[d] & \\ I \text{ maksimalan} \arrow[r] & I \text{ prost} \arrow[r] & I \text{ poluprost} \end{tikzcd}$$

Naglasimo ovdje kako između "I potpuno prost" i "I maksimalan" nije moguće, u potpunoj općenitosti, staviti niti jednu implikaciju. Preciznije rečeno, postoje prsteni R u kojima je neki ideal I maksimalan, ali on nije potpuno prost (vidi Primjer 6.18(4) i Zadatak 48). Isto tako, postoje prsteni u kojima mnogi potpuno prosti ideali nisu maksimalni; npr., to ćemo imati u komutativnim prstenima kad god budemo gledali neki prost ($\equiv$potpuno prost) ne-maksimalan ideal.

Zadatak 47. Dokažite da su u prstenima $A = \mathbb{Z}$ ili $\mathbb{C}[X]$ svi prosti ne-nul ideali ujedno i maksimalni ideali. (Kasnije ćemo vidjeti da su gornja dva prstena tzv. *Euklidove domene*; pokazat ćemo da je svaka Euklidova domena PGI.)

Primjer 6.18. U ovom primjeru izračunat ćemo $\operatorname{Spec} R$ i $\operatorname{Max} R$, za neke konkretne prstene R.

(1) Neka je $R = \mathbb{Z}$. Kako smo već prije rekli, sada je svaki ideal glavni, tj. oblika $\langle n \rangle = n\mathbb{Z}$, $n \in \mathbb{N}_0$. Pritom je

$$\operatorname{Max} \mathbb{Z} = \{\langle 2 \rangle, \langle 3 \rangle, \langle 5 \rangle, \ldots \langle p \rangle, \ldots \mid p \text{ prim broj}\},$$

i

$$\operatorname{Spec} \mathbb{Z} = \operatorname{Max} \mathbb{Z} \cup \{(0)\}.$$

Primjetimo kako je spektar $\operatorname{Spec} \mathbb{Z}$ parametriziran skupom $\mathcal{P}$, svih prim brojeva u $\mathbb{N}$. Nadalje, primjetimo da je nul-ideal jedini *minimalan ideal*; preciznije rečeno, svi ostali ideali su maksimalni i "sjede" nad nul-idealom.

(2) Neka je $R = \mathbb{C}[X]$. I ovdje je svaki ideal glavni, tj. oblika $\langle f\rangle = \mathbb{C}[X]f$, $f \in \mathbb{C}[X]$. Lako se može pokazati da vrijedi sljedeća ekvivalencija:

$$\langle f\rangle \text{ prost ideal} \quad \Longleftrightarrow \quad f \text{ ireducibilan polinom.}$$

(Podsjetimo se da je neki polinom f *ireducibilan*, ako se ne može napisati kao produkt $f_1 f_2$ dvaju polinoma f_1 i f_2 koji su svaki stupnja barem 1.) Kao posljedicu imamo

$$\operatorname{Max}\mathbb{C}[X] = \{\langle X - c\rangle \mid c \in \mathbb{C}\}$$

i

$$\operatorname{Spec}\mathbb{C}[X] = \operatorname{Max}\mathbb{C}[X] \cup \{(0)\}.$$

Primjetimo kako je ovdje spektar $\operatorname{Spec}\mathbb{C}[X]$ parametriziran skupom $\mathbb{C}$, svih kompleksnih brojeva. Nadalje, primjetimo da je i sada nul-ideal jedini *minimalan ideal.* (Zapravo, situacija je vrlo slična kao kod prstena $\mathbb{Z}$.)

(3) Neka je $R = \mathbb{C}[X_1, \ldots, X_n]$, $n \geq 2$. U ovom prstenu, za razliku od polinoma u jednoj varijabli, postoje ideali koji nisu glavni; npr., svaki maksimalan ideal je takav. Pritom se može pokazati da imamo

$$\operatorname{Max} R = \{\langle X_1 - c_1, \ldots, X_n - c_n\rangle \mid c_i \in \mathbb{C}\}.$$

Napomenimo kako je lako pokazati da je svaki ideal $\langle X_1 - c_1, \ldots, X_n - c_n\rangle$ doista maksimalan. No teže je vidjeti da svaki maksimalan ideal u R ima upravo taj oblik; to je predmet slavnog Hilbertovog rezultata, tzv. "slabog teorema o nulama".

Isto tako naglasimo kako je spektar $\operatorname{Spec} R$ puno kompliciraniji skup nego $\operatorname{Max} R$. Bolje rečeno, uopće ne postoji neki dobar opis toga skupa, za sve n-ove. Štoviše, općeniti je problem vidjeti da li je neki ideal $I = \langle S\rangle$, gdje je S konkretan zadani konačan podskup polinoma, prost ili nije. (Spomenimo kako se rečeni problemi najbolje tretiraju u okviru Algebarske Geometrije, jedne od glavnih i najviše proučavanih matematičkih disciplina, koja povezuje algebarske metode i geometrijsku percepciju.)

(4) Neka je $R = M_n(\mathbb{R})$, $n \geq 2$. Ovo je, na neki način, "patološki" primjer nekomutativnog prstena. Naime, za razliku od mnogih zanimljivih nekomutativnih prstena $\mathcal{R}$ u kojima su skupovi $\operatorname{Max}\mathcal{R}$, $\operatorname{Spec}\mathcal{R}$ i $\operatorname{Spec}_c\mathcal{R}$ vrlo "veliki" i komplicirani za proučavati, ovdje je situacija vrlo jednostavna i specifična. Sasvim precizno, imamo:

$$\operatorname{Max} R = \operatorname{Spec} R = \{(\mathbf{0})\} \qquad \& \qquad \operatorname{Id} R = \{(\mathbf{0}), R\};$$

R je primjer tzv. **prostog prstena**, prstena koji nema netrivijalnih ideala.

(Budući da mi u ovom kolegiju Algebarske Strukture, zbog vrlo male materije koja se obrađuje, nismo u stanju čak niti definirati neke "zanimljive" nekomutativne prstene o čijim se spektrima i max-spektrima može nešto "pametno" reći, tek spomenimo da su npr. takvi zanimljivi objekti tzv. *omotačke algebre Liejevih algebri.*)

Zadatak 48. (i) Dokažite detaljno sve pomoćne tvrdnje iz gornjih primjera navedenih u (1), (2) i (3).

(ii) Dokažite detaljno sve tvrdnje iz (4); o $\operatorname{Id} R$, o spektru i o max-spektru. (*Uputa.* Probajte najprije uzeti $n = 2$. Da biste pokazali da R nema netrivijalnih (dvostranih) ideala, pretpostavite da je I neki ne-nul ideal, i onda množenjem sa tzv. *standardnim matricama* E_{ij} i slijeva i zdesna "napušite" I do cijelog R.)

(iii) Dokažite da ima (nekomutativnih) prstena R u kojima postoje ideali $I \trianglelefteq R$ koji su maksimalni, ali nisu potpuno prosti. (Specijalno, takvi su ideali ujedno i primjeri prostih, ali ne potpuno prostih, ideala.)

6.3. O idealima u komutativnim prstenima.

Cilj ovog kratkog pododjeljka je reći nešto o idealima u komutativnim prstenima. Najprije dajemo važan teorem koji karakterizira proste, odnosno maksimalne, ideale u takvim prstenima. Zatim dokazujemo propoziciju o karakterizaciji polja.

Najprije spomenuti teorem o karakterizaciji prostih/maksimalnih ideala.

Teorem 6.19. *Neka je A komutativan prsten.*

(i) *Ideal $P \trianglelefteq A$ je prost* akko *je kvocijentni prsten A/P integralna domena.*
(ii) *Ideal $M \trianglelefteq A$ je maksimalan* akko *je kvocijentni prsten A/M polje.*

Dokaz. (i) To je zapravo tvrdnja (a)$\Leftrightarrow$(c) u Propoziciji 6.12, za slučaj komutativnog prstena; mi ćemo ipak dati i direktan (jednostavniji) dokaz.

($\Rightarrow$) Pretpostavimo da su elementi $\overline{x} := x+P$ i $\overline{y} := y+P$ takvi da je $\overline{x}\,\overline{y} = \overline{0} := 0+P$, tj. $x\,y + P = 0 + P = P \;\Leftrightarrow\; x\,y \in P$. No kako je P prost ideal, to iz $x\,y \in P$ slijedi da je ili $x \in P$ ili $y \in P$, što je dalje ekvivalentno sa: ili $\overline{x} = \overline{0}$ ili $\overline{y} = \overline{0}$. Znači, A/P je integralna domena.

($\Leftarrow$) Pretpostavimo sada da je A/P integralna domena, ali da P *nije* prost ideal. Ali to da P nije prost znači da postoje neki $x, y \in A \setminus P$ takvi da je $x\,y \in P$. Onda imamo

$$x\,y \in P \quad\Longleftrightarrow\quad (x+P)(y+P) = 0 + P \quad\Longleftrightarrow\quad \overline{x}\,\overline{y} = \overline{0}.$$

No isto tako imamo $x \in A \setminus P \;\Leftrightarrow\; \overline{x} \neq \overline{0}$, ali i $y \in A \setminus P \;\Leftrightarrow\; \overline{y} \neq \overline{0}$. Slijedi da onda kvocijent A/P nije integralna domena, što je kontradikcija.

(ii) ($\Rightarrow$) Pretpostavimo da je M maksimalan ideal, pa onda pokažimo da je svaki ne-nul element u kvocijentu A/M invertibilan; onda, po definiciji polja, slijedi da je A/M polje. Pa neka je $\overline{0} \neq \overline{x} := x + M \in \overline{A} := A/M$ proizvoljan element. Sada, $\overline{0} \neq \overline{x}$ je ekvivalentno $x \in A \setminus M$. Slijedi da imamo strogu inkluziju $M \subset M + Ax$, no kako je M maksimalan ideal, slijedi dalje da je $M + Ax = A$. Specijalno se onda jedinica $1 \in A$ može napisati kao zbroj $1 = m + ax$, za neke $m \in M$ i $a \in A$. No onda, budući je "potez" $\alpha \mapsto \overline{\alpha}$ (kanonski) homomorfizam prstena, imamo

$$\overline{m + ax} = \overline{m} + \overline{a}\,\overline{x} = \overline{a}\,\overline{x} = \overline{1},$$

tj. $\overline{a} = (\overline{x})^{-1}$; tu smo koristili da je $\overline{m} = \overline{0}$. Time smo pokazali da doista svaki ne-nul $\overline{x}$ ima inverz.

($\Leftarrow$) Pretpostavimo sada da je A/M polje, ali da ideal M nije maksimalan, tj. da postoji neki ideal $I \trianglelefteq A$, $I \neq A$, takav da je $M \subset I$. No onda za proizvoljan element

$x \in I \setminus M$ imamo $\overline{x} \neq \overline{0}$. Ali kako je $\overline{A} = A/M$ polje, to (ne-nul) element $\overline{x}$ ima inverz. Znači, postoji neki $y \in A \setminus M$ takav da je $\overline{x}\,\overline{y} = \overline{1}$. Ali imamo

$$\overline{x}\,\overline{y} = \overline{1} \quad \Longleftrightarrow \quad x\,y - 1 \in M \quad \Longleftrightarrow \quad x\,y - 1 = m \text{ za neki } m \in M.$$

Slijedi

$$1 = x\,y - m \in I \quad \Longrightarrow \quad I = A;$$

gore smo koristili $x \in I \;\Rightarrow\; x\,y \in I$, te $m \in M \subset I$. No $I = A$ je kontradikcija; time je tvrdnja (ii) dokazana. □

Dokažimo sada i spomenutu propoziciju koja karakterizira polja.

Propozicija 6.20. *Neka je A komutativan prsten. Sljedeće su tvrdnje međusobno ekvivalentne.*

(a) *A je polje.*
(b) $\operatorname{Id} A = \{(0), A\}$.
(c) *Ako je B bilo koji (komutativan) prsten i $\varphi : A \to B$ bilo koji homomorfizam, onda je φ monomorfizam. (Tojest, svaki homomorfizam iz polja u prsten je nužno injekcija!)*

Dokaz. (a)⇒(b) Neka je $(0) \neq I \trianglelefteq A$ neki ne-nul ideal. Pokažimo da je onda nužno $I = A$. U tu svrhu uzmimo bilo koji element $0 \neq x \in I$. Budući je, po pretpostavci (a), A polje, to posebno x ima inverz $x^{-1} \in A$. Onda imamo, jer je I ideal,

$$x \in I \quad \Longrightarrow \quad 1 = x\,x^{-1} \in I\,A \subseteq I \quad \Longrightarrow \quad I = A,$$

kako smo i tvrdili.

(b)⇒(c) Budući je jezgra $\operatorname{Ker}\varphi$ ideal u A, to je, koristeći (b), ili $\operatorname{Ker}\varphi = (0)$ ili $\operatorname{Ker}\varphi = A$. Ali $\operatorname{Ker}\varphi = A$ je zapravo nemoguće; naime, imamo $\varphi(1_A) = 1_B \neq 0_B$. Znači, mora biti $\operatorname{Ker}\varphi = (0)$, što je ekvivalentno tomu da je φ monomorfizam.

(c)⇒(a) Neka (c) vrijedi, i pretpostavimo da A nije polje. To onda znači da postoji neki $0 \neq x \in A$ koji nema inverz; tj.,

$$1 \notin \{x\,y \mid y \in A\} = xA \quad (= Ax = \langle x \rangle).$$

Dakle, ideal Ax zadovoljava $(0) \neq Ax \neq A$. Slijedi da je kvocijentni prsten $B := A/Ax$ netrivijalan i s jedinicom $\overline{1} = 1 + Ax$. Nadalje, (kanonski epimorfizam) $\varphi : A \to B$, $\varphi(a) := a + Ax$ za $a \in A$, je homomorfizam koji nije monomorfizam; naime, jezgra mu je $\operatorname{Ker}\varphi = Ax \neq (0)$. Ali to je $\neg(c)$. □

(* * *)

Na kraju ovog odjeljka dajemo još neke zadatke.

Zadatak 49. (i) Kako izgledaju prosti ideali u prstenu $\mathbb{R}[X]$? Što je kvocijent $\mathbb{R}[X]/\langle X^2 + a^2 \rangle$, za $a \in \mathbb{R}\setminus\{0\}$; tj., hoće li to za neke a-ove biti integralna domena, ili čak polje?

(ii) Kakvu strukturu ima kvocijentni prsten $\mathbb{Q}[X]/\langle X^3 + 3 \rangle$?

Zadatak 50. Neka je $(a,b) \subseteq \mathbb{R}$. Sa $\mathcal{C}(a,b)$ i $\mathcal{C}^\infty(a,b)$ označimo skup svih neprekidnih i skup svih *glatkih* funkcija $f : (a,b) \to \mathbb{R}$, redom. (Funkcija f je "glatka na (a,b)" ako ima derivacije svakog reda na cijelom (a,b).) Fiksirajmo $z \in (a,b)$, i onda definirajmo skupove

$$I_z := \{f \in \mathcal{C}(a,b) \mid f(z) = 0\},$$
$$J_z := \{f \in \mathcal{C}^\infty(a,b) \mid f(z) = f'(z) = 0\}.$$

Dokažite:

(i) $\mathcal{C}(a,b)$ je prsten, za uobičajeno zbrajanje i množenje funkcija; I_z je maksimalan ideal. Što je $\mathcal{C}(a,b)/I_z$?

(ii) $\mathcal{C}^\infty(a,b)$ je prsten, i J_z je ideal. Da li je J_z maksimalan ideal? (*Uputa:* BSO pretpostavimo $z \neq 0$, i onda pokažite da je $J_z + \langle X - z\rangle \neq \mathcal{C}^\infty(a,b)$.)

Zadatak 51. Neka je A komutativan prsten.

(i) Definirajmo

$$\mathfrak{N}(A) := \{x \in A \mid x \text{ je nilpotentan}\};$$

element x je *nilpotentan* ako postoji $n = n(x) \in \mathbb{N}$ (n ovisi o x) takav da je $x^n = 0$. Dokažite da je $\mathfrak{N}(A) \trianglelefteq A$, ideal; taj se ideal zove **nilradikal** od A. (*Uputa:* Iskoristite Binomni teorem da biste pokazali: Ako su $x, y \in \mathfrak{N}(A)$, onda je i $x + y \in \mathfrak{N}(A)$.)

(ii) Dokažite da je

$$\mathfrak{N}\big(A/\mathfrak{N}(A)\big) = \{0\};$$

tj., u kvocijentu $A/\mathfrak{N}(A)$ nema nilpotentnih elemenata $\neq 0$.

Napomena 6.21. Može se dokazati da vrijedi sljedeći važan rezultat.

Teorem. *U komutativnom prstenu A imamo*

$$\mathfrak{N}(A) = \bigcap_{P \in \operatorname{Spec} A} P.$$

Zadatak 52. Neka je $A = \mathbb{Z}$, te neka su $I = \langle x\rangle$ i $J = \langle y\rangle$ ideali. Dokažite da vrijedi:

$$I + J = \langle M(x,y)\rangle,$$
$$I \cap J = \langle V(x,y)\rangle,$$
$$I\,J = \langle x\,y\rangle;$$

ovdje su sa $M(x,y)$ i $V(x,y)$ označeni NZM, *najveća zajednička mjera* i NZV, *najmanji zajednički višekratnik*, od x i y, redom.

Zadatak 53. Dokažite da za proizvoljne ideale $I, J \trianglelefteq \mathbb{Z}$ vrijedi

$$(I + J)(I \cap J) = I\,J.$$

U proizvoljnom (komutativnom) prstenu A, za ideale $I, J \trianglelefteq A$, vrijedi uvijek $(I+J)(I \cap J) \subseteq I\,J$, ali je moguća i stroga inkluzija; dokažite to.

Definicija 6.22. Za ideale I i J u proizvoljnom prstenu R kažemo da su **relativno prosti**, ako je

$$I + J = R.$$

Zadatak 54. (i) Dokažite: Ako su cijeli brojevi $x, y \in \mathbb{Z}$ relativno prosti u "klasičnom smislu" (tj., njihova je NZM jednaka 1), onda su ideali $\langle x \rangle$ i $\langle y \rangle$ relativno prosti u smislu gornje definicije; i obratno.

(ii) Ako je A komutativan prsten i ako su $I, J \trianglelefteq A$ relativno prosti ideali, onda je

$$I \cap J = I\,J.$$

7. Homomorfizmi prstena

Podsjetimo: Za prstene R i S, preslikavanje $f : R \to S$ je homomorfizam prstena ukoliko je f aditivno i multiplikativno preslikavanje koje "šalje 1_R u 1_S". U ovom odjeljku najprije navodimo tri osnovna rezultata o homomorfizmima prstena; to su tzv. *Teoremi o izomorfizmima.* Naglasimo kako će njihovi dokazi biti zapravo jednostavne posljedice triju Teorema o izomorfizmima za grupe. Na kraju odjeljka dokazujemo još jedan vrlo koristan rezultat; to je tzv. *Kineski teorem o ostacima* za prstene. Kao što mu i samo ime govori, taj je rezultat direktna generalizacija "klasičnog" Kineskog teorema o ostacima iz elementarne Teorije brojeva; naime, "klasična verzija" se odnosi na prsten $\mathbb{Z}$, dok je njegova generalizacija dana za proizvoljan prsten R.

7.1. Teoremi o izomorfizmima.

Sada ćemo dokazati prvi od triju teorema o izomorfizmima.

Teorem 7.1. (Prvi teorem o izomorfizmu)
Neka je $f : R \to S$ proizvoljan homomorfizam prstena. Tada je $\operatorname{Ker} f \trianglelefteq R$ *ideal,* $\operatorname{Im} f \leq S$ *je potprsten, a preslikavanje*

$$\overline{f} : R/\operatorname{Ker} f \to \operatorname{Im} f, \qquad \overline{f}(r + \operatorname{Ker} f) := f(r),$$

je (dobro definiran) izomorfizam prstena; tj.,

$$R/\operatorname{Ker} f \cong \operatorname{Im} f.$$

Dokaz. Najprije primjetimo da je f homomorfizam iz aditivne grupe $(R, +)$ u grupu $(S, +)$, pa su onda $\operatorname{Ker} f \leq (R, +)$ i $\operatorname{Im} f \leq (S, +)$ podgrupe. No, štoviše, za proizvoljne $r \in R$ i $n \in \operatorname{Ker} f$ ($\Leftrightarrow f(n) = 0$) imamo

$$f(rn) = f(r)f(n) = f(r)\,0 = 0 \quad \text{i} \quad f(nr) = \cdots = 0;$$

znači, $\operatorname{Ker} f$ je ideal u R. Isto tako, ako su $s_1, s_2 \in \operatorname{Im} f$, onda postoje neki $r_1, r_2 \in R$ takvi da je $f(r_i) = s_i$, za $i = 1, 2$. Ali onda je $s_1 s_2 = f(r_1 r_2) \in \operatorname{Im} f$; tj., $\operatorname{Im} f$ je skup zatvoren za množenje, pa je to potprsten od S.

Sada znamo da su $R/\operatorname{Ker} f$ i $\operatorname{Im} f$ prsteni. Nadalje, po Prvom teoremu o izomorfizmu za grupe, znamo da je $\overline{f}$ (dobro definiran) izomorfizam iz aditivne grupe $(R, +)/(\operatorname{Ker} f, +)$ na grupu $(\operatorname{Im} f, +)$. Da bismo dokazali teorem, još samo treba primjetiti da, za $\overline{r_i} := r_i + \operatorname{Ker} f$, imamo

$$\overline{f}(\overline{r_1}\,\overline{r_2}) = \overline{f}(r_1 r_2 + \operatorname{Ker} f) = f(r_1 r_2) = f(r_1)f(r_2) = \overline{f}(\overline{r_1})\overline{f}(\overline{r_2});$$

ovdje smo koristili definiciju množenja u kvocijentnom prstenu, zatim definiciju preslikavanja $\overline{f}$, i konačno činjenicu da f je homomorfizam prstena. Tako imamo da je $\overline{f}$ i multiplikativno preslikavanje; dakle je to izomorfizam prstena. $\square$

Sljedeća je propozicija analogon Propozicije 2.9 u Poglavlju 1.

Propozicija 7.2. *Neka je $f : R \to S$ homomorfizam prstena, te neka su $I \trianglelefteq R$ i $J \trianglelefteq S$ ideali takvi da je $f(I) \subseteq J$. Tada je preslikavanje*

$$\overline{f} : R/I \to S/J, \qquad r + I \mapsto f(r) + J,$$

homomorfizam prstena.

Zadatak 55. Dokažite detaljno prethodnu propoziciju. (*Uputa:* "Kopirajte" dokaz gore spomenute propozicije.)

Sada ćemo dokazati tzv. Drugi teorem o izomorfizmu.

Teorem 7.3. (Drugi teorem o izomorfizmu)
Neka je R prsten, $S \leq R$ neki potprsten i $I \trianglelefteq R$ neki ideal. Tada je $S + I \leq R$ potprsten, i $S \cap I \trianglelefteq S$ ideal. Nadalje, vrijedi

$$S/S \cap I \cong S + I/I.$$

Dokaz. Prvo, lako je provjeriti da je $S + I$ potprsten od R. Naime, ako su $s_1, s_2 \in S$ i $x_1, x_2 \in I$, onda imamo

$$(s_1 + x_1) - (s_2 + x_2) = (s_1 - s_2) + (x_1 - x_2) \in S + I$$

i

$$(s_1 + x_1)(s_2 + x_2) = s_1 s_2 + (s_1 x_2 + x_1 s_2 + x_1 x_2) \in S + I;$$

ovdje koristimo da je I ideal pa je sumand $(\cdots)$ iz I. Dalje, isto je tako jasno da je $S \cap I$ ideal u S, te da je I ideal u $S + I$.

Sada, definirajmo preslikavanje

$$\phi : S \to S + I/I, \qquad \phi(x) := x + I.$$

Po Drugom teoremu o izomorfizmu za grupe, taj ϕ je epimorfizam aditivnih grupa, sa jezgrom $\operatorname{Ker} \phi = S \cap I$. No očito je ϕ štoviše i homomorfizam prstena, tj. epimorfizam prstena. Još samo treba primjeniti Prvi teorem o izomorfizmu za prstene. $\square$

Sljedeća je propozicija potrebna za dokaz tzv. Trećeg teorema o izomorfizmu, ali je i sama za sebe vrlo važna i korisna. Ona daje preciznu vezu između ideala (tj. prostih ideala) u R, te ideala (tj. prostih ideala) u kvocijentu R/I; ovdje je $I \trianglelefteq R$ fiksirani ideal.

Propozicija 7.4. *Neka je R proizvoljan prsten, $I \trianglelefteq R$ neki ideal, i onda $\pi : R \to R/I$ kanonski epimorfizam. Na skupu svih ideala u R koji sadrže ideal I definirajmo preslikavanje Θ ovako:*

$$\Theta : \{K \mid I \subseteq K \in \operatorname{Id} R\} \longrightarrow \operatorname{Id}(R/I),$$
$$K \longmapsto \pi(K) = K/I.$$

Tada je Θ monotona *bijekcija, čije je inverzno preslikavanje dano sa*

$$\Theta^{-1}(\overline{K}) = \pi^{-1}(\overline{K}), \qquad \overline{K} \trianglelefteq R/I.$$

Nadalje, preslikavanje

$$\theta : \{P \mid I \subseteq P \in \operatorname{Spec} R\} \longrightarrow \operatorname{Spec}(R/I),$$
$$\theta(P) = \Theta(P),$$

je također monotona bijekcija. (Primjetimo da je zapravo θ restrikcija od Θ na "manju" domenu $\{P \mid I \subseteq P \in \operatorname{Spec} R\}$, tj. skup svih prostih ideala u R koji sadrže I.)

Dokaz. Označimo kvocijent od R po I sa

$$\overline{R} := R/I.$$

Jasno, ako je $K \trianglelefteq R$ ideal takav da sadrži I, onda je K/I ideal u $\overline{R}$; znači, preslikavanje Θ doista "završava" u kodomeni $\mathrm{Id}(R/I)$, tj. dobro je definirano. Nadalje, očito je Θ monotono preslikavanje; tj., ako su $K_1 \subseteq K_2$ dva ideala u R koja oba sadrže I, onda je $K_1/I \subseteq K_2/I$.

(Θ injekcija)
Neka su $K_1, K_2 \trianglelefteq R$ ideali i pretpostavimo da je

$$\Theta(K_1) = \Theta(K_2) \qquad \Longleftrightarrow \qquad K_1/I = K_2/I.$$

Onda, za proizvoljan element $k_1 \in K_1$ je $k_1 + I \in K_1/I = K_2/I$. Znači, postoji neki $k_2 \in K_2$ takav da je $k_1 + I = k_2 + I$, što je ekvivalentno sa $k_1 - k_2 \in I$. Ali onda, jer je posebno $I \subseteq K_2$, slijedi $k_1 - k_2 \in K_2$, tj. $k_1 \in K_2$. Zbog proizvoljnosti izbora za k_1, imamo $K_1 \subseteq K_2$; jasno, sasvim analogno slijedi i obratna inkluzija, pa tako imamo i $K_1 = K_2$. Time je pokazano da je Θ injekcija.

(Θ surjekcija)
Za proizvoljan ideal $\overline{K} \trianglelefteq \overline{R}$, definirajmo

$$K := \pi^{-1}(\overline{K});$$

tj., K je praslika od $\overline{K}$ po π. Sada se lako provjeri da je K ideal u R i da sadrži I. Nadalje, imamo $\pi(K) = \overline{K}$; znači, Θ je stvarno i surjekcija.

Kada imamo dokazane gornje činjenice, onda je evidentno da je doista sa

$$\Theta^{-1} : \overline{K} \longmapsto \pi^{-1}(\overline{K})$$

definiran inverz od Θ.

Dokažimo sada da je i θ bijekcija. U tu svrhu neka je $P \in \operatorname{Spec} R$ neki prost ideal i označimo

$$\overline{P} := \pi(P) = P/I.$$

Tvrdimo da je $\overline{P}$ prost ideal u prstenu $\overline{R}$. Pa neka su $\overline{J_1}, \overline{J_2} \trianglelefteq \overline{R}$ dva ideala takva da je produkt $\overline{J_1}\,\overline{J_2} \subseteq \overline{P}$. Ali po prvom dijelu propozicije, znamo da su ideali $\overline{J_i}$ oblika $\overline{J_i} = J_i/I$, za neke ideale $J_i \trianglelefteq R$ koji sadrže I. Ali onda inkluzija $\overline{J_1}\,\overline{J_2} \subseteq \overline{P}$ povlači $J_1 J_2 \subseteq P$. (Naime, ako su $x \in J_1$ i $y \in J_2$, onda je $(x+I)(y+I) = x\,y + I \in \overline{P}$. To znači da postoji neki $p \in P$ takav da je $x\,y - p \in I$. Slijedi da je $x\,y \in p + I \subseteq P$. No, kako produkti $x\,y$ generiraju $J_1 J_2$, zaključujemo da je doista $J_1 J_2 \subseteq P$.) Sada, inkluzija $J_1 J_2 \subseteq P$ i činjenica da je P prost daju da je ili $J_1 \subseteq P$ ili $J_2 \subseteq P$. Ali

$$J_i \subseteq P \quad \Longrightarrow \quad \overline{J_i} = J_i/I \subseteq P/I = \overline{P}.$$

Tako smo dokazali da je

$$\overline{P} \in \operatorname{Spec} \overline{R},$$

što smo i tvrdili. Obratno, ako je $\overline{P} \in \operatorname{Spec} \overline{R}$, definirajmo $P := \pi^{-1}(\overline{P})$. Idući 'obratnim putem' u gornjem dokazu, vidi se da je P prost ideal; i jasno, sadrži I. Zaključak je da je θ doista bijekcija između navedena dva skupa prostih ideala. Time je propozicija dokazana. $\square$

Zadatak 56. Neka je $f : R \to S$ epimorfizam prstena. Definirajmo preslikavanje na idealima

$$\Theta : K \longmapsto f(K).$$

(i) Dokažite: $\Theta : \{K \mid \operatorname{Ker} f \subseteq K \in \operatorname{Id}(R)\} \to \operatorname{Id} S$ je monotona bijekcija.
(ii) Vrijedi li analogon gornje propozicije za proste ideale?

Sada dokazujemo i tzv. Treći teorem o izomorfizmu.

Teorem 7.5. (Treći teorem o izomorfizmu)
Neka je R prsten, te neka su $I, J \trianglelefteq R$ ideali takvi da je $I \subseteq J$. Tada je $J/I \trianglelefteq R/I$ ideal i vrijedi

$$(R/I)/(J/I) \cong R/J.$$

Dokaz. Da je J/I ideal u kvocijentu R/I slijedi po prethodnoj propoziciji. Nadalje, preslikavanje

$$\phi : R/I \to R/J, \qquad \phi(r + I) := r + J,$$

je dobro definiran epimorfizam aditivnih grupa (usp. Propoziciju 7.2). Štoviše, to je i (surjektivan) homomorfizam prstena. Po Prvom teoremu o izomorfizmu za prstene, slijedi

$$(R/I)/\operatorname{Ker}\phi \cong \operatorname{Im}\phi = R/J.$$

Još samo treba primjetiti, ponovo po gornjoj propoziciji, da je jezgra $\operatorname{Ker}\phi$ ideal oblika K/I za neki ideal $K \trianglelefteq R$ koji sadrži I. No očito je $K = I$. Tako je teorem dokazan. $\square$

7.2. Kineski teorem o ostacima za prstene.

Sada ćemo dokazati najavljeni Kineski teorem o ostacima za prstene. No prije toga podsjetimo se nekih dobro poznatih stvari iz elementarne teorije brojeva.

Za brojeve $m \in \mathbb{N}$ i $a, b \in \mathbb{Z}$ definiramo pojam "kongruencije modulo m" ovako: Kažemo da su a i b *kongruentni modulo* m, i pišemo

$$b \equiv a \pmod{m},$$

ako m dijeli $b - a$, tj. $m \mid b - a$. Ovdje primjetimo, što je sasvim očito, da *kongruencijska jednadžba*

$$X \equiv a \pmod{m},$$

po X, ima rješenja

$$X = m\,k + a, \qquad k \in \mathbb{Z}.$$

Sada, ako su $m_1, m_2 \in \mathbb{N}$ i $a_1, a_2 \in \mathbb{Z}$, gledajmo *sustav kongruencijskih jednadžbi*

$$X \equiv a_1 \pmod{m_1},$$
$$X \equiv a_2 \pmod{m_2}.$$

I općenito, za n prirodnih brojeva $m_1, \dots, m_n \in \mathbb{N}$ i n cijelih brojeva $a_1, \dots, a_n \in \mathbb{Z}$, možemo pitati ako postoji rješenje sustava kongruencijskih jednadžbi

$$(\Sigma) \qquad \begin{aligned} X &\equiv a_1 \pmod{m_1}, \\ &\dots \qquad \dots \\ X &\equiv a_n \pmod{m_n}. \end{aligned}$$

(Naravno, zanimljivo je i pitanje kako, ukoliko znamo da rješenje postoji, isto naći. No mi se tim pitanjem ovdje nećemo baviti; za više detalja vidi npr. [A. Dujella, *Uvod u teoriju brojeva*, Pogl. 2].)

Sada ćemo iskazati, te radi potpunosti ali i u cilju komparacije dokaza sa "općenitom verzijom", dokazati tzv. "klasični" Kineski teorem o ostacima.

Teorem. (Kineski teorem o ostacima)
Neka su $m_1, \dots, m_n \in \mathbb{N}$ u parovima relativno prosti brojevi, tj. najveća je zajednička mjera $(m_i, m_j) = 1$, za sve $i \neq j$. (Ili ekvivalentno rečeno: $\langle m_i \rangle + \langle m_j \rangle = \mathbb{Z}$.) Onda za proizvoljne $a_1, \dots, a_n \in \mathbb{Z}$, sustav (Σ) ima rješenja.

Štoviše, ako je x_0 jedno rješenje od (Σ), onda su sva ostala rješenja x dana sa $x \equiv x_0 \pmod{m_1 \cdots m_n}$.

Dokaz. Označimo

$$m := m_1 \cdots m_n \qquad \& \qquad u_i := m/m_i, \quad \text{za } i = 1, \dots, n.$$

Budući je mjera $(m_i, u_i) = 1$, za svaki i, onda

$$(3) \qquad \exists x_i \in \mathbb{Z} \qquad \text{tako da} \quad u_i x_i \equiv a_i \pmod{m_i}, \quad \forall i.$$

[[Da bismo to vidjeli, primjetimo da za $k \in \{1, \dots, m_i\}$ i neke $c_k \in \{1, \dots, m_i\}$, takve da je $k\, u_i \equiv c_k \pmod{m_i}$, imamo

$$\{c_1, \dots, c_{m_i}\} = \{1, \dots, m_i\};$$

tj., to je tzv. *potpun sistem ostataka*. Naime, $c_k = c_l$ povlači $k\, u_i - l\, u_i \equiv 0 \pmod{m_i}$, a to dalje $m_i \mid (k-l)u_i$. Jer su m_i i u_i relativno prosti, slijedi da $m_i \mid k - l$, i onda $k = l$.]]

Sada, definirajmo

$$x_0 := u_1 x_1 + \cdots + u_n x_n.$$

Sasvim je jasno da je onda $x_0 \equiv u_i x_i \pmod{m_i}$, iz čega, koristeći (3), slijedi

$$x_0 \equiv a_i \pmod{m_i} \qquad \forall i = 1, \dots, n.$$

Konačno, ako je x proizvoljno rješenje od (Σ), onda je posebno $x \equiv x_o \pmod{m_i}$, za svaki i. No to je ekvivalentno sa $m_i \mid x - x_0$, iz čega slijedi

$$m = m_1 \cdots m_n \mid x - x_0;$$

tj., $x \equiv x_0 \pmod{m}$. $\square$

Definicija 7.6. Neka je R prsten i $I \trianglelefteq R$ neki ideal. Za elemente $a, b \in R$ kažemo da su **kongruentni modulo** I, i pišemo

$$b \equiv a \pmod{I},$$

ukoliko je $b - a \in I$.

Napomena 7.7. Primjetimo da u slučaju $R = \mathbb{Z}$ i $I = \langle m \rangle$, imamo ekvivalentnost uvjeta

$$b - a \in I \qquad \Longleftrightarrow \qquad m \mid b - a;$$

drugim riječima, gornja je definicija doista generalizacija 'klasičnog' pojma kongruencije za cijele brojeve.

Teorem 7.8. (Kineski teorem o ostacima za prstene)
Neka su $I_1, \ldots, I_n \trianglelefteq R$ ideali takvi da su I_i i I_j relativno prosti za $i \neq j$; tj., $I_i + I_j = R$. Tada za proizvoljne $a_1, \ldots, a_n \in R$ sustav kongruencija

$$X \equiv a_i \pmod{I_i}, \qquad i = 1, \ldots, n,$$

ima rješenja u R; tj., postoji barem jedan $x \in R$ takav da je za $X = x$ ispunjeno svih n gornjih kongruencija.

Zapravo, dokazat ćemo ovaj malo jači rezultat; tvrdnja (i) sljedećeg teorema je točno gornji teorem.

Teorem 7.9. *Neka su $I_1, \ldots, I_n \trianglelefteq R$ ideali. Definirajmo preslikavanje*

$$\varphi : R \to \prod_{i=1}^{n} R/I_i, \qquad \varphi(x) := (x + I_1, \ldots, x + I_n).$$

Tada je φ homomorfizam prstena za koji vrijedi sljedeće:

(i) *Preslikavanje φ je epimorfizam* akko *su ideali I_i, I_j u parovima relativno prosti.*
(ii) *Preslikavanje φ je monomorfizam* akko *je $I_1 \cap \cdots \cap I_n = (0)$.*

Dokaz. Jasno je da je φ doista homomorfizam prstena.

(i) ($\Rightarrow$) Pretpostavimo da je φ surjekcija, ali da je $I_i + I_j \neq R$, za neke $i < j$. Uzmimo bilo koji element $\omega \in R \setminus (I_i + I_j)$. Onda, zbog surjektivnosti, za n-torku

$$\Omega := (I_1, \ldots, I_{i-1}, \omega + I_i, I_{i+1}, \ldots, I_j, \ldots, I_n) \in \prod_i R/I_i$$

postoji neki $x \in R$ takav da je

$$\varphi(x) = \Omega.$$

No onda je posebno $x + I_i = \omega + I_i$ i $x + I_j = I_j$, što je ekvivalentno sa $\omega - x \in I_i$ i $x \in I_j$. Slijedi

$$\omega = (\omega - x) + x \in I_i + I_j;$$

no to je u kontradikciji sa izborom od ω.

($\Leftarrow$) Pretpostavimo dakle da je $I_i + I_j = R$, za sve $i \neq j$; tj., da su ideali I_i međusobno, u parovima, relativno prosti. Sada, za proizvoljan $1 \leq i \leq n$ i element $a_i \in R$, naći ćemo $x_i \in R$ takav da je

$$\varphi(x_i) = (I_1, \ldots, I_{i-1}, a_i + I_i, I_{i+1}, \ldots, I_n).$$

Naime, tada će za

$$x := x_1 + \cdots + x_n$$

biti

$$\varphi(x) = \sum_i \varphi(x_i) = (a_1 + I_1, \ldots, a_n + I_n);$$

tj., imat ćemo surjektivnost od φ.

Da bismo pokazali gornju tvrdnju, najprije BSO možemo pretpostaviti da je $i = 1$; tj., da imamo $a_1 \in R$, pa tražimo $x_1 \in R$ takav da je $\varphi(x_1) = (a_1 + I_1, I_2, \ldots, I_n)$. (Jedini razlog za ovu pretpostavku je da sada "sve radimo na prvim koordinatama u n-torkama", što će nam biti lakše za zapisivati!)

Najprije, činjenica da su ideali I_1 i I_i, za $i = 2, \ldots, n$, relativno prosti znači da imamo

$$I_1 + I_2 = R, \qquad I_1 + I_3 = R, \qquad \cdots \quad \cdots \qquad I_1 + I_n = R.$$

Množenjem tih jednakosti, te korištenjem distributivnosti množenja prema zbrajanju, za ideale, dobijemo

$$R = R \cdots R = \prod_{j=2}^{n} (I_1 + I_j) \subseteq I_1 + I_2 \cdots I_n \subseteq R.$$

$\big($Kada u gornjem produktu $\prod_{j=2}^{n}(I_1 + I_j)$ "izmnožimo" sve izraze u zagradama dobit ćemo ukupno 2^n sumanada oblika $J_2 \cdots J_n$, gdje je za svaki $i = 2, \ldots, n$ ili $J_i = I_1$ ili $J_i = I_i$. No, kako su I_i-ovi ideali, a posebno je I_1 ideal, to je očito $J_2 \cdots J_n \subseteq I_1$, za svaki sumand $J_2 \cdots J_n$ u kojem se na bar jednom mjestu J_k pojavi upravo I_1. Preciznije rečeno, to će se dogoditi uvijek osim u jednom jedinom slučaju; to je kada budemo uzeli "posljednji" sumand, tj. sumand $I_2 \cdots I_n$. Zato je

$$\prod_{j=2}^{n} (I_1 + I_j) \subseteq I_1 + I_2 \cdots I_n,$$

kako smo gore i napisali.$\big)$ Dakle, vrijedi

$$I_1 + I_2 \cdots I_n = R. \tag{4}$$

Odavde, koristeći činjenicu da je $I\,J \subseteq I \cap J$ za bilo koja dva ideala $I, J \trianglelefteq R$, dobivamo

$$I_1 + I_2 \cap \cdots \cap I_n = R.$$

Sada slijedi da postoje neki $\alpha \in I_1$ i $\beta \in I_2 \cap \cdots \cap I_n$ takvi da je

$$\alpha + \beta = a_1.$$

Pokažimo da je $x_1 := \beta$ element koji tražimo. Doista, jer je $\beta \in I_2, \ldots, I_n$, to imamo

$$\begin{aligned} \varphi(\beta) &= \big(\beta + I_1, \beta + I_2, \ldots, \beta + I_n\big) = \big(\beta + I_1, I_2, \ldots, I_n\big) \\ &= \big(a_1 + I_1, I_2, \ldots, I_n\big); \end{aligned}$$

gore smo koristili da je $\beta + I_i = I_i$, za $2 \le i \le n$, te da je $\beta + I_1 = a_1 - \alpha + I_1 = a_1 + I_1$. Time je tvrdnja (i) u potpunosti dokazana.

(ii) ($\Rightarrow$) Pretpostavimo da je φ injekcija, pa neka je onda $a \in I_1 \cap \cdots \cap I_n$. No tada je, po definiciji preslikavanja φ,

$$\varphi(a) = (I_1, \ldots, I_n) = 0 = 0_{\prod_i R/I_i},$$

i onda, jer je φ injekcija, $a = 0$; tu koristimo dobro poznatu činjenicu da je homomorfizam injektivan akko mu je jezgra trivijalna.

($\Leftarrow$) Ako je $a \in R$ takav da je $\varphi(a) = 0$, onda po definiciji preslikavanja φ slijedi da je $a \in I_1 \cap \cdots \cap I_n$. Ali, po pretpostavci je $I_1 \cap \cdots \cap I_n = (0)$, pa slijedi $a = 0$. Tako smo pokazali da je φ injekcija. $\square$

Napomena 7.10. U vezi sa prethodnim teoremom primjetimo da ako je A komutativan prsten, a ideali $I_1, \dots, I_n \trianglelefteq A$ su u parovima relativno prosti, onda je

$$I_1 \cdots I_n = I_1 \cap \cdots \cap I_n.$$

[[*Dokaz.* Da bismo to pokazali, prvo primjetimo da jednakost (4), naravno sa potpuno istim argumentom dokaza, vrijedi za bilo kojih ≥ 2 ideala koji su u parovima relativno prosti. Posebno, ako to primjenimo na ideale $I_m, I_{m+1}, \dots, I_n$, za $1 \leq m \leq n-1$, dobit ćemo

$$\begin{aligned} I_{n-1} + I_n &= R, \\ I_{n-2} + I_{n-1}I_n &= R, \\ \cdots \quad & \quad \cdots \\ I_1 + I_2 \cdots I_n &= R. \end{aligned}$$

Primjenom činjenice da za relativno proste ideale $I, J \trianglelefteq A$ vrijedi $I\,J = I \cap J$ (vidi Zadatak 54), imamo sljedeće jednakosti među idealima:

$$\begin{aligned} I_{n-1} \cap I_n &= I_{n-1}I_n \\ I_{n-2} \cap I_{n-1}I_n &= I_{n-2}I_{n-1}I_n \\ \cdots \quad & \quad \cdots \\ I_1 \cap I_2 \cdots I_n &= I_1 I_2 \cdots I_n. \end{aligned}$$

Iz gornjih jednakosti, pomoću induktivnog argumenta, slijedi

$$I_j \cap \cdots \cap I_n = I_j \cdots I_n, \qquad \text{za } j = 1, 2, \dots, n;$$

što je i trebalo pokazati.]]

8. Prsteni polinoma

U cijelom ovom odjeljku:

$$A = \text{komutativan prsten s jedinicom } 1.$$

Polinomi su osnovne funkcije u matematici. Posebno, polinomi nad $\mathbb{R}$ ili $\mathbb{C}$, tj. sa realnim ili kompleksnim koeficijentima, su objekti bez kojih je npr. nemoguće zamisliti Matematičku analizu. Za potrebe Algebre, standardno se pojam polinoma generalizira uzevši namjesto $\mathbb{R}$ ili $\mathbb{C}$ bilo koji komutativan prsten s jedinicom.

Definicija 8.1. Izraz oblika

$$p(X) := a_0 + a_1 X + \ldots + a_i X^i + \ldots + a_k X^k, \qquad k \in \mathbb{N}_0, \ \ a_i \in A,$$

zove se **polinom** u X. Drugi način zapisa polinoma je u obliku

$$p(X) = \sum_i a_i X^i,$$

s tim da se onda podrazumijeva da je gornja suma zapravo konačna; tj., da sumacija "ide" od $i = 0$ do nekog $k \geq 0$. Skup svih polinoma nad A, tj. polinoma sa koeficijentima iz prstena A, označava se sa $A[X]$; tj.

$$A[X] := \text{skup svih polinoma } p(X) \text{ sa koeficijentima iz } A.$$

Ovdje je X (*formalna*) **varijabla**, a simbol X^i je tzv. i-ta *potencija* od X. Elementi a_i zovu se **koeficijenti** polinoma $p(X)$; posebno, kažemo da je a_i i-ti koeficijent. Koeficijent a_0 zove se **slobodni koeficijent**, a a_k se zove **vodeći koeficijent**; kada govorimo o vodećem koeficijentu, mi zapravo pretpostavljamo da je $a_k \neq 0$.

Posebno definiramo **nul-polinom** kao

$$0 = 0 + 0\,X + 0\,X^2 + \cdots;$$

drugim riječima, nul-polinom je polinom koji je konstanta, i to baš konstanta $0 = 0_A$.

Za polinom $p(X)$ kao gore, kojemu je vodeći koeficijent $a_k \neq 0$, definiramo **stupanj** polinoma $p(X)$ kao

$$\deg p(X) := k;$$

tako govorimo da je $p(X)$ *polinom stupnja* k. Nadalje, dogovorno se uzima da je stupanj nul-polinoma jednak -1.

Za polinome $p_1(X) = \sum_i a_i X^i$ i $p_2(X) = \sum_i b_i X^i$ standardno se definira *zbroj polinoma*

$$p_1(X) + p_2(X) := \sum_i (a_i + b_i) X^i;$$

tj., polinome zbrajamo tako da im "zbrojimo koeficijente uz iste potencije".

Isto tako, za polinome $p_1(X)$ i $p_2(X)$ kao gore, definira se *produkt polinoma*

$$p_1(X) \cdot p_2(X) = p_1(X)\, p_2(X) := \sum_i c_i X^i,$$

gdje su koeficijenti c_i dobiveni "konvolucijskim množenjem", tj., dani su kao $c_0 := a_0 b_0$, $c_1 := a_0 b_1 + a_1 b_0$, i općenito

$$c_i := a_0 b_i + a_1 b_{i-1} + \cdots + a_i b_0;$$

ovdje se naravno podrazumijeva da su koeficijenti $a_l = 0$, ukoliko je $l > k_1 = \deg p_1(X)$, odnosno da je $b_l = 0$, ukoliko je $l > k_2 = \deg p_2(X)$.

Napomena 8.2. Sada kada smo na skupu $A[X]$ definirali operacije zbrajanja "+" i množenja "·" polinoma, lako je provjeriti da

$$A[X] = (A[X], +, \cdot)$$

ima strukturu komutativnog prstena s jedinicom; tako govorimo da je $A[X]$ **prsten polinoma u** X **sa koeficijentima iz** A. Naravno, nula u tom prstenu je nul-polinom. Jedinica u $A[X]$ je konstanta $1 = 1_A$.

Sasvim analogno, definiraju se polinomi u više varijabli.

Definicija 8.3. Izraz oblika

$$p(X_1, \ldots, X_n) := \sum_{(i_1,\ldots,i_n)\in\mathbb{N}_0^n} a_{i_1\cdots i_n} X_1^{i_1} \cdots X_n^{i_n} \qquad a_{i_1\cdots i_n} \in A,$$

zove se *polinom u varijablama* $X_1, \ldots, X_n$; naravno i sada se podrazumijeva da je gornja suma konačna. I ovdje se $a_{i_1\cdots i_n}$-ovi zovu *koeficijenti* polinoma. Oznaka za skup svih polinoma nad A u varijablama X_i je

$$A[X_1, \ldots, X_n].$$

Pojam stupnja polinoma više varijabli dan je na sljedeći način. Za $p = p(X_1, \ldots, X_n)$, kao gore, stavimo

$$\deg p := \max\{i_1 + \cdots + i_n \mid a_{i_1\cdots i_n} \neq 0\};$$

tj., ako za *monom*

$$a_{i_1\cdots i_n} X_1^{i_1} \cdots X_n^{i_n}$$

definiramo njegov stupanj kao zbroj $i_1 + \cdots + i_n$ svih potencija od varijabli $X_1, \ldots, X_n$, onda je stupanj polinoma p jednak najvećem stupnju njegovih monoma.

Na skupu $A[X_1, \ldots, X_n]$ definiraju se operacije zbrajanja i množenja polinoma analogno kao što je to načinjeno za polinome u jednoj varijabli. Naime, za polinom $p(X_1, \ldots, X_n)$ kao gore, i neki $q(X_1, \ldots, X_n)$ sa koeficijentima $b_{i_1\cdots i_n}$, imamo zbroj

$$p(X_1, \ldots, X_n) + q(X_1, \ldots, X_n) = \sum_{(i_1,\ldots,i_n)} (a_{i_1\cdots i_n} + b_{i_1\cdots i_n}) X_1^{i_1} \cdots X_n^{i_n}.$$

Isto tako, produkt polinoma p i q dobivamo tako da polinome 'izmnožimo po linearnosti'; tj., množimo svaki monom od p sa svakim monomom od q, i onda dobiveno sredimo tako da "pokupimo" sve koeficijente koji stoje uz neki konkretan produkt varijabli $X_1^{k_1} \cdots X_n^{k_n}$. Jasno, monome množimo po pravilu

$$(a_{i_1\cdots i_n} X_1^{i_1} \cdots X_n^{i_n})\,(b_{j_1\cdots j_n} X_1^{j_1} \cdots X_n^{j_n}) := (a_{i_1\cdots i_n}\, b_{j_1\cdots j_n}) X_1^{i_1+j_1} \cdots X_n^{i_n+j_n}.$$

Napomena 8.4. (1) Kao i za $A[X]$, imamo da i $A[X_1, \ldots, X_n]$, uz definirane operacije zbrajanja i množenja polinoma, ima strukturu komutativnog prstena s jedinicom; tako govorimo da je $A[X_1, \ldots, X_n]$ **prsten polinoma u** $X_1, \ldots, X_n$ **sa koeficijentima iz** A. Nula u tom prstenu je ponovo **nul-polinom**, tj. nula $0 = 0_A$ u A, a jedinica je konstanta $1 = 1_A$.

(2) Primjetimo da se prsten polinoma $A[X_1, \ldots, X_n]$, u n varijabli, zapravo može shvatiti kao

$$A[X_1, \ldots, X_n] \equiv A[X_1, \ldots, X_{n-1}]\big[X_n\big];$$

tj., kao prsten u varijabli X_n sa koeficijentima iz prstena polinoma u prvih $n-1$ varijabli. Tu zapravo mi "sredimo svaki polinom u varijablama X_i po potencijama od X_n". Zapravo, sasvim analogno imamo

$$A[X_1, \ldots, X_n] \equiv A[X_{u_1}, \ldots, X_{u_k}]\big[X_{v_1}, \ldots, X_{v_m}\big],$$

gdje je $k + m = n$, $1 \leq u_1 < \cdots < u_k \leq n$, $1 \leq v_1 < \cdots < v_m \leq n$ i imamo disjunktnu uniju

$$\{u_1, \ldots, u_k\} \cup \{v_1, \ldots, v_m\} = \{1, 2, \ldots, n\};$$

tj., načinimo particiju skupa $\{1, 2, \ldots, n\}$ na u_i-ove i v_j-ove, a zatim svaki polinom iz $A[X_1, \ldots, X_n]$ sređujemo po potencijama od $X_{v_1}, \ldots, X_{v_m}$.

Zadatak 57. Neka je element $\alpha \in A$ fiksiran, i onda definirajmo preslikavanje

$$\mathcal{E}_\alpha : A[X] \to A, \qquad p(X) \mapsto p(\alpha);$$

preslikavanje $\mathcal{E}_\alpha$ zove se *evaluacija* u α. Dokažite da je to preslikavanje homomorfizam prstena. Kada će to biti epimorfizam? Odredite jezgru $\operatorname{Ker} \mathcal{E}_\alpha$. Kada će $\mathcal{E}_\alpha$ biti monomorfizam?

Analogno, za $\boldsymbol{\alpha} := (\alpha_1, \ldots, \alpha_n) \in A^n$, definiramo evaluaciju u $\boldsymbol{\alpha}$ kao

$$\mathcal{E}_{\boldsymbol{\alpha}} : A[X_1, \ldots, X_n] \to A, \qquad p(X_1, \ldots, X_n) \mapsto p(\boldsymbol{\alpha}).$$

Što se sada može reći o tomu da li je to preslikavanje epimorfizam i/ili monomorfizam?

Sljedeća jednostavna lema zapravo karakterizira integralne domene među prstenima polinoma.

Lema 8.5. *Ako je prsten koeficijenata A integralna domena, onda je i prsten polinoma $A[X_1, \ldots, X_n]$ također integralna domena; naravno, i obratno.*

Dokaz. Budući je, kako smo vidjeli gore, $A[X_1, \ldots, X_n] = A[X_1, \ldots, X_{n-1}]\big[X_n\big]$, to je jasno da BSO možemo uzeti da je $n = 1$. (Naime, tako iz činjenice da je A domena dobijemo da je i $B := A[X_1]$ domena. Zatim slijedi da je i $A[X_1, X_2] = B[X_2]$ također domena. Nastavljamo indukcijom!)

Pa neka je sada $n = 1$, i neka su dani polinomi

$$p_1 = p_1(X) = a_0 + a_1 X + \cdots + a_{k_1} X^{k_1}, \qquad p_2 = p_2(X) = b_0 + b_1 X + \cdots + b_{k_2} X^{k_2},$$

gdje su njihovi vodeći koeficijenti a_{k_1} i b_{k_2} različiti od nule. Drugim riječima, stupnjevi su $\deg p_i = k_i \geq 0$, za $i = 1, 2$; i, posebno, to nisu nul-polinomi. Ali onda je stupanj produkta tih dvaju polinoma jednak

$$\deg(p_1 p_2) = \deg p_1 + \deg p_2,$$

što je posebno ≥ 0. Slijedi da $p_1 p_2$ nije nul-polinom; time je lema dokazana. $\square$

Napomena 8.6. Primjetimo da za proizvoljan A, u prstenu polinoma $A[X_1, \dots, X_n]$ vrijedi sljedeće za stupnjeve: Ako su $p_1 = p_1(X_1, \dots, X_n)$ i $p_2 = p_2(X_1, \dots, X_n)$ polinomi, onda je

$$\deg(p_1 + p_2) \leq \max\{\deg p_1, \deg p_2\},$$
$$\deg(p_1 p_2) \leq \deg p_1 + \deg p_2;$$

i posebno ćemo za stupanj produkta imati jednakost, ako je A domena. Nadalje, za *kompoziciju polinoma*

$$(p_2 \circ p_1)(X) := p_2(p_1(X)),$$

gdje su $p_1, p_2 \in A[X]$ polinomi u jednoj varijabli, imamo za stupanj kompozicije

$$\deg(p_2 \circ p_1) \leq (\deg p_1)(\deg p_2);$$

ponovo, za slučaj da je A štoviše integralna domena, imamo jednakost.

Zadatak 58. Dokažite detaljno sve tvrdnje iz gornje Napomene, i primjerima pokažite da se rečene tvrdnje ne mogu poboljšati; barem u slučaju prstena polinoma u jednoj varijabli. (Tojest, u gornjem izrazu za stupanj zbroja možemo imati znak "$<$" čak iako je A polje; u izrazima za produkt i kompoziciju možemo imati znak "$<$" ukoliko A nije domena; itd..)

Sljedeći je važan rezultat tzv. "Teorem o dijeljenju s ostatkom"; on je direktna generalizacija dobro poznatih rezultata o dijeljenju s ostatkom u $\mathbb{Z}$ i u prstenima polinoma u jednoj varijabli sa koeficijentima iz $\mathbb{R}$ ili $\mathbb{C}$. Taj se teorem ponekad zove i *Euklidov algoritam*; jer u važnom slučaju kada je A polje, prsten polinoma $A[X]$ jest tzv. Euklidova domena. Za više detalja vidite Definiciju 9.1 i Napomenu 9.19(2).

Teorem 8.7. (Teorem o dijeljenju s ostatkom)
Neka su $f(X)$ i $g(X)$ iz $A[X]$ polinomi, različiti od nul-polinoma, i pretpostavimo da je vodeći koeficijent u polinomu $g(X)$ iz $A^\times$, grupe invertibilnih elemenata u A. Tada postoje, *i* jedinstveni *su, polinomi $q(X)$ i $r(X)$ iz $A[X]$ takvi da je*

$$f(X) = g(X)\, q(X) + r(X) \qquad \& \qquad \deg r(X) < \deg g(X).$$

Dokaz. (*Egzistencija*)
Dokaz ćemo dati indukcijom po stupnju polinoma kojeg dijelimo, tj. polinoma $f(X)$. Za to, napišimo polinome

$$f(X) = a_0 + a_1 X + \cdots + a_n X^n, \qquad g(X) = b_0 + b_1 X + \cdots + b_m X^m,$$

pri čemu je $a_n \neq 0$ i $b_m \in A^\times$. Kao što smo rekli, dokaz egzistencije od $q(X)$ i $r(X)$ provodimo indukcijom po n, tj. stupnju od $f(X)$. Najprije pogledajmo bazu indukcije; tj. $n = 0$. Tu imamo dvije mogućnosti:

(1) $\deg g(X) = 0$.
Sada je $g(X) = b_0 \in A^\times$, pa onda uzmemo za r i q polinome konstante $r(X) := 0$ i $q(X) := b_0^{-1} a_0$.

(2) $\deg g(X) > 0$.
Sada uzmemo $r(X) := f(X)$ i $q(X) := 0$, nul-polinom.

Sada prelazimo na korak indukcije. Preciznije rečeno, pretpostavimo da teorem vrijedi za sve polinome $f(X)$ stupnja $< n$, pa pokažimo da onda vrijedi i za sve polinome stupnja $= n$. Za to BSO pretpostavimo da je

$$\deg g(X) = m \leq n = \deg f(X);$$

naime, ukoliko je $\deg g(X) > \deg f(X)$, onda uzmemo $q(X) := 0$ i $r(X) := f(X)$. Dalje definirajmo "pomoćni" polinom $f_1(X)$ sa

$$f_1(X) := f(X) - a_n b_m^{-1} X^{n-m} g(X);$$

tu koristimo činjenicu da je vodeći koeficijent b_m od $g(X)$ invertibilan u A. Primjetimo da je zapravo

$$f_1(X) = \big(a_n X^n + \text{ niže potencije od } f\big) \ - \big(a_n b_m^{-1} X^{n-m}(b_m X^m + \text{ niže potencije od } g)\big),$$

pa se gore član $a_n X^n$ "pokrati". Slijedi da je

$$\deg f_1(X) < \deg f(X) = n.$$

No onda primjena pretpostavke indukcije, sada na polinom $f_1(X)$, daje da postoje neki polinomi $\widetilde{q}(X)$ i $r(X)$ takvi da je

$$f_1(X) = \widetilde{q}(X)g(X) + r(X) \qquad \& \qquad \deg r(X) < \deg g(X).$$

No onda slijedi da je

$$f(X) = q(X)g(X) + r(X),$$

gdje polinom $q(X)$ definiramo kao

$$q(X) := a_n b_m^{-1} X^{n-m} + \widetilde{q}(X);$$

time je eqzistencija rastava dokazana.

(*Jedinstvenost*)

Pretpostavimo da imamo neke $q_i(X)$ i $r_i(X)$, za $i = 1, 2$, takve da je

$$q_1(X)g(X) + r_1(X) = f(X) = q_2(X)g(X) + r_2(X)$$

i $\deg r_i(X) < \deg g(X)$, za $i = 1, 2$. Onda slijedi

$$(q_1(X) - q_2(X))g(X) = r_2(X) - r_1(X).$$

Tvrdimo da odavde slijedi da je $q_1(X) - q_2(X) = 0$, a onda naravno imamo i $r_2(X) - r_1(X) = 0$; što i moramo vidjeti. Naime, kad bi bilo $q_1(X) - q_2(X) \neq 0$, onda bismo imali

$$\deg((q_1(X) - q_2(X))g(X)) \geq m = \deg g(X);$$

tu ponovo koristimo činjenicu da je vodeći koeficijent b_m od $g(X)$ invertibilan u A, pa posebno on nije djelitelj nule. Ali kako isto tako imamo (vidi Napomenu 8.6) da je $\deg(r_2(X) - r_1(X)) < m = \deg g(X)$, dolazimo do kontradikcije.

Tako je teorem u potpunosti dokazan. $\square$

Napomena 8.8. (1) Primjetimo kako je pretpostavka $b_m \in A^\times$, u teoremu, doista nužna. Kao ilustraciju za to pogledajmo $A = \mathbb{Z}$ i onda prsten polinoma $\mathbb{Z}[X]$, te onda npr. polinome $f(X) = 2X$ i $g(X) = 3$. Očito je da onda ne postoje neki $q(X), r(X) \in \mathbb{Z}[X]$ takvi da je $2X = 3q(X) + r(X)$ i još $\deg r(X) < 0 = \deg g(X)$; zapravo, tu bi moralo biti $r(X) = 0$ i onda $2X = 3q(X)$, što je očito nemoguće.

(2) Gornji se teorem ne može generalizirati na slučaj polinoma u dvije ili više varijabli; čak iako je A npr. polje. (Nađite npr. u $\mathbb{R}[X_1, X_2]$ dva polinoma $f = f(X_1, X_2)$ i $g = g(X_1, X_2)$ takve da ne postoje q i r iz $\mathbb{R}[X]$ za koje vrijedi $f = gq + r$ i $\deg r < \deg g$.)

Sljedeći je važan teorem samo specijalan slučaj nešto općenitijeg rezultata (vidi Teorem 9.7).

Teorem 8.9. *Ako je* $\mathbb{F}$ *polje, onda je prsten polinoma* $\mathbb{F}[X]$ PGI*, prsten glavnih ideala.*

DOKAZ. Neka je $(0) \neq I \trianglelefteq \mathbb{F}[X]$ neki ideal; moramo pokazati da je onda on glavni. U tu svrhu, uzmimo polinom $g = g(X)$ takav da $g \neq 0$, $g \in I$ i stupanj $\deg g$ je minimalan mogući; tj. $\deg g = \min\{\deg \gamma \mid \gamma \in I\}$. (Takav g sigurno postoji; to je zapravo posljedica elementarne činjenice da svaki neprazan podskup od $\mathbb{N}$ ima najmanji element!) Tvrdimo da je

$$I = \langle g \rangle.$$

Doista, očita je inkluzija $I \supseteq \langle g \rangle$. Za obratno, uzmimo proizvoljan $f \in I$. Po Teoremu o dijeljenju s ostatkom, postoje neki q i r takvi da je $f = qg + r$ i $\deg r < \deg g$. Ali kako su $f, g \in I$, to slijedi da je također $r = f - qg \in I$. No, zbog "minimalnosti stupnja" od g, zaključujemo da je nužno $r = 0$, dakle $f = qg \in \langle g \rangle$. □

Već smo prije rekli da zapravo prstena koji su PGI ima vrlo malo, u odnosu na sve (komutativne) prstene. Posebno, prsteni

$$\mathbb{Z}[X] \qquad \text{i} \qquad A[X_1, \dots, X_n], \quad \text{za } n \geq 2,$$

<u>nisu</u> PGI. Sljedeći je zadatak u vezi s tim (vidi i Zadatak 62).

Zadatak 59. Gledajmo prsten $A := \mathbb{R}[X, Y]$, prsten polinoma u varijablama X i Y sa realnim koeficijentima. Definirajmo ideal

$$I := \langle X, Y \rangle.$$

Dokažite da je I maksimalan ideal, i nije glavni ideal. Koju strukturu ima kvocijent A/I? (*Uputa:* Pretpostavite da je $I = \langle p \rangle$, za neki polinom $p \in \mathbb{R}[X, Y]$; jasno, moralo bi biti $\deg p \geq 1$. Onda iz $X, Y \in I$ imamo da postoje neki f, g takvi da je $X = p\,f$ i $Y = p\,g$. Zaključite da su f i g konstante...)

Zadatak 60. Dokažite da su invertibilni elementi u prstenu polinoma samo konstante iz prstena koeficijenata koje su još i invertibilne; tj, imamo

$$A[X_1, \dots, X_n]^{\times} = A^{\times}.$$

9. Domene glavnih ideala i faktorijalni prsteni

U cijelom ovom odjeljku:

$$\mathcal{A} = \text{komutativan prsten s jedinicom } 1.$$

Kao što smo već puno puta spomenuli, prsten $\mathbb{Z}$ je prvi zanimljivi primjer (komutativnog) prstena. Iako je, gledano s jedne strane, vrlo jednostavan za razumijevanje, u njemu možemo uočiti mnoge fenomene koji će se u većoj ili manjoj mjeri ponekad generalizirati na mnoge druge prstene; takvi su, recimo, tzv. *prsteni cijelih polja algebarskih brojeva* koji su glavni objekti jedne jako proučavane grane Teorije brojeva, a koja se zove *Algebarska teorija brojeva.* (No naglasimo kako su i mnoga pitanja vezana i uz sam $\mathbb{Z}$ vrlo teška i trenutno vrlo daleko od nekog zadovoljavajućeg odgovora; ali isto tako, tu su mnogi duboki i fundamentalni rezultati dobiveni u proteklih cca 200 godina. Naprimjer, centralni je problem u matematici *Problem distribucije prim brojeva*; tu bismo željeli razumijeti kako su zapravo prim brojevi "razmješteni" u skupu svih cijelih brojeva.) Jedno od glavnih svojstava koje ima $\mathbb{Z}$ je predmet tzv. *Osnovnog teorema aritmetike* koji govori da se svaki cijeli broj $x \in \mathbb{Z}$, $|x| > 1$, može napisati u obliku

$$x = \pm p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k},$$

gdje je $\{p_1, p_2, \ldots, p_k\} \subseteq \mathbb{N}$ skup svih prim brojeva koji dijele x, a α_i-ovi su najveće potencije s kojom p_i "ulazi" u x, tj. najveće potencije takve da $p_i^{\alpha_i}$ dijeli x. Jasno, ako nam poredak p_i-ova u gornjem rastavu nije bitan, možemo reći da je rastav zapravo jedinstven. Upravo navedeno svojstvo o "faktorizaciji cijelih brojeva preko prim brojeva" zapravo je gotovo sasvim očito, ali u isto vrijeme apsolutno fundamentalno za proučavanje prstena $\mathbb{Z}$. I sada, prirodno je pitati ima li još nekih zanimljivih prstena $\mathcal{A}$ koji će imati to svojstvo. Naravno, tu bismo onda morali najprije vidjeti koji bi objekti u takovom prstenu $\mathcal{A}$ "preuzeli ulogu" koju imaju prim brojevi u $\mathbb{Z}$. Drugo, moramo vidjeti kako formulirati navedeno svojstvo, za te prstene $\mathcal{A}$; prstene sa tim svojstvom zvat ćemo *faktorijalnim prstenima.* Glavni zadatak ovog odjeljka je dati neke osnovne rezultate u vezi odgovora na spomenuto pitanje.

Glavni rezultat ovog odjeljka je Teorem 9.23:

Svaka DGI, domena glavnih ideala, je faktorijalan prsten.

Tako ćemo, pored samog $\mathbb{Z}$, dobiti još dosta drugih prstena sa "svojstvom jedinstvene faktorizacije". Ali naglasimo ovdje da postoje i drugi vrlo zanimljivi primjeri prstena koji će biti faktorijalni, ali neće biti prsteni glavnih ideala. Zapravo, jedan od najvažnijih rezultata o faktorijalnim prstenima, koji mi nećemo ovdje dokazivati, je sljedeći teorem; u vezi s njim primjetimo kako su polja "trivijalni" primjeri faktorijalnih prstena. Isto tako, podsjetimo se da prsteni polinoma u dvije ili više varijabli nisu *PGI*.

Teorem. *Ako je $\mathcal{A}$ faktorijalan prsten, onda je prsten polinoma $\mathcal{A}[X_1, \ldots, X_n]$, za bilo koji $n \in \mathbb{N}$, također faktorijalan. Posebno, prsten polinoma $\mathbb{F}[X_1, \ldots, X_n]$ je faktorijalan, za bilo koje polje $\mathbb{F}$.*

Drugi važan cilj ovoga odjeljka je prepoznati svojstvo o kojemu govore Teoremi o dijeljenju s ostatkom u $\mathbb{Z}$ i u $\mathbb{F}[X]$, za $\mathbb{F}$ polje, kao svojstvo koje zapravo karakterizira jednu zanimljivu klasu prstena koji su još i domene; takve će se zvati *Euklidove domene.*

Zatim ćemo dokazati Teorem 9.7:

Svaka Euklidova domena je DGI.

Kao trivijalnu posljedicu navedenih dvaju teorema dobivamo i ovu činjenicu:

Svaka Euklidova domena je faktorijalan prsten.

NAPOMENA. Na kraju ovog uvodnog dijela odjeljka, naglasimo još jednom, kako su PGI, a onda još i više Euklidove domene, zapravo dosta rijetki objekti u skupu npr. svih (komutativnih) domena. Tako da dobivene rezultate treba shvatiti kao "mali fragment" studiranja komutativnih domena s jedinicom, gdje su u izvjesnom smislu i promatrani objekti i dobiveni rezultati "lijepi i jednostavni". No to nipošto ne znači da su u "komplementu tog fragmenta" stvari isto tako "lijepe i jednostavne".

9.1. Euklidove domene.

Definicija 9.1. Prsten $\mathcal{A}$ je **Euklidova domena** ako je to integralna domena i ako postoji neka funkcija $\lambda : \mathcal{A} \setminus \{0\} \to \mathbb{N}_0$ takva da za nju vrijedi sljedeće:

Ako su elementi $A, B \in \mathcal{A}$, gdje je $B \neq 0$, onda postoje neki elementi $C, D \in \mathcal{A}$ takvi da je

$$A = BC + D,$$

gdje je $D = 0$ ili $\lambda(D) < \lambda(B)$.

Primjer 9.2. (1) Prsten $\mathcal{A} = \mathbb{Z}$, sa funkcijom $\lambda(x) := |x|$, je Euklidova domena. Naime, podsjetimo se da Teorem o dijeljenju s ostatkom u $\mathbb{Z}$ glasi: *Ako su $a \in \mathbb{Z}$ i $b \in \mathbb{N}$, onda postoje jedinstveni $q \in \mathbb{Z}$ i $r \in \mathbb{N}_0$, takvi da je $a = qb + r$, pri čemu je $0 \leq r < b$.* Sada, ako su $A \in \mathbb{Z}$ i $B \in \mathbb{N}$, onda postojanje elemenata C i D, sa svojstvom kao u gornjoj definiciji, slijedi iz navedenog teorema. S druge strane, ako je pak B negativan, onda je $-B \in \mathbb{N}$, pa ponovo po teoremu postoje neki q, r takvi da je

$$A = q(-B) + r, \qquad 0 \leq r < -B = |B|.$$

Stavimo $C := -q$ i $D := r$.

(2) Prsten $\mathcal{A} = \mathbb{F}[X]$, gdje je $\mathbb{F}$ proizvoljno polje, sa funkcijom $\lambda(p(X)) := \deg p(X)$ je Euklidova domena. Naime, to slijedi direktno iz Teorema o dijeljenju s ostatkom za polinome.

Sada ćemo dati još dva primjera prstena koji su Euklidove domene. Prvi je *prsten Gaussovih cijelih brojeva*; napomenimo da je taj prsten zapravo tzv. *prsten cijelih* za polje $\mathbb{Q}(\imath) := \{a + b\imath \mid a, b \in \mathbb{Q}\}$. Drugi je prsten također prsten cijelih jednog polja; sada je to primjer tzv. *ciklotomskog polja*, dobivenog kao proširenje od $\mathbb{Q}$ trećim korijenima iz jedinice.

Definicija 9.3. Podskup $\mathbb{Z}[\imath] \subseteq \mathbb{C}$ definiran kao

$$\mathbb{Z}[\imath] := \{a + b\imath \mid a, b \in \mathbb{Z}\}$$

zove se skup **Gaussovih cijelih brojeva**.

Neka je

$$\omega := -1/2 + \imath\sqrt{3}/2;$$

ω je tzv. *primitivni treći korijen jedinice*. Definirajmo skup

$$\mathbb{Z}[\omega] := \{a + b\omega \mid a, b \in \mathbb{Z}\}.$$

Primjetimo kako je $\mathbb{Z}[\imath]$ očito prsten, a kako je on potprsten od polja $\mathbb{C}$, to sa radi o integralnoj domeni; tako govorimo o prstenu, tj. domeni, Gaussovih cijelih brojeva. Cilj sljedećeg jednostavnog zadatka je pokazati da je i $\mathbb{Z}[\omega]$ također prsten; dakle, budući je i sada $\mathbb{Z}[\omega] \subseteq \mathbb{C}$, ponovo je riječ o domeni.

Zadatak 61. Dokažite da je $\mathbb{Z}[\omega]$ prsten. Nadalje, u vezi s gore navedenim, opišite kako izgleda najmanje potpolje od $\mathbb{C}$ koje sadrži $\mathbb{Q}$ i broj ω. (*Uputa:* Primjetite da je $1 + \omega + \omega^2 = 0$.)

Propozicija 9.4. (i) *Prsten $\mathbb{Z}[\imath]$, sa funkcijom*

$$\lambda(a + b\imath) := |a + b\imath|^2 = a^2 + b^2,$$

je Euklidova domena.

(ii) *Prsten $\mathbb{Z}[\omega]$, sa funkcijom*

$$\lambda(a + b\omega) := a^2 - ab + b^2,$$

je Euklidova domena.

Napomena 9.5. Zapravo, kao što ćemo vidjeti u dokazu propozicije, u oba slučaja je funkcija λ dana kao

$$\lambda(z) = |z|^2;$$

samo što prvi put uzimamo $z \in \mathbb{Z}[\imath] \subseteq \mathbb{C}$, a drugi put $z \in \mathbb{Z}[\omega] \subseteq \mathbb{C}$.

Dokaz. (i) Neka su $A = a + b\imath$ i $B = c + d\imath$ iz $\mathbb{Z}[\imath]$ zadani, te neka je $B \neq 0$. Tada je

$$A/B = r + s\imath \qquad \text{za neke } r, s \in \mathbb{Q}.$$

(Napišite r i s kao funkcije od a i b!) Sada odaberimo $m, n \in \mathbb{Z}$ takve da je

$$|r - m| \leq 1/2 \qquad \& \qquad |s - n| \leq 1/2.$$

Takvi m i n sigurno postoje. (U kompleksnoj ravnini gledajmo 'mrežu' $\mathbb{Z}[\imath]$; tu mrežu čine kvadratići stranica duljine 1. Sada pogledamo onaj kvadratić u koji 'padne' naš broj r/s; vodoravni pravci u kompleksnoj ravnini koji određuju taj kvadratić prolaze kroz brojeve $l\imath$ i $(l+1)\imath$, za neki $l \in \mathbb{Z}$, dok okomiti pravci koji ga određuju prolaze kroz brojeve k i $k+1$, za neki $k \in \mathbb{Z}$. Sada, ako je $r - k < k + 1 - r$, tj. ako je r bliže broju k nego broju $k+1$, uzmimo $r = k$; ako je pak r bliže broju $k+1$ nego broju k, uzmimo $r = k+1$. Jasno, ako je r "na pola puta", tj. ako je $r - k = k + 1 - r$, onda je svejedno hoćemo li za r uzeti k ili $k+1$. Analogno izaberemo $s \in \{l, l+1\}$. Nacrtajte sliku!) Sada definirajmo

$$C := m + n\imath \in \mathbb{Z}[\imath].$$

Za funkciju λ, proširenu sa $\mathbb{Z}[\imath]$ na $\mathbb{Q}[\imath]$, tj. za funkciju

$$\lambda : \mathbb{Q}[\imath] \to \mathbb{Q}_+, \qquad \lambda(x + y\imath) := x^2 + y^2,$$

onda imamo

$$\lambda(A/B - C) = (r - m)^2 + (s - n)^2 \leq 1/4 + 1/4 = 1/2.$$

Dalje, definirajmo

$$D := A - BC \in \mathbb{Z}[\imath].$$

Tvrdimo da su gore definirani C i D takvi da zadovoljavaju uvjet iz definicije Euklidove domene. Doista, ako je $D = 0$, onda je $A = BC$, pa smo gotovi. A ako je $D \neq 0$, koristeći da je

$$\lambda(XY) = \lambda(X)\lambda(Y), \qquad \forall\, X, Y \in \mathbb{Z}[\imath],$$

(to zato jer je $\lambda(z) = |z|^2$ i $|z_1 z_2| = |z_1|\,|z_2|$) imamo

$$\lambda(D) = \lambda(B(A/B - C)) = \lambda(B)\lambda(A/B - C) \leq \lambda(B) \cdot 1/2 < \lambda(B);$$

i ponovo smo gotovi.

(ii) Najprije primjetimo da za *konjugiranje* $z \mapsto \overline{z}$ u $\mathbb{C}$ imamo posebno $\overline{\omega} = \omega^2$. Slijedi, koristeći $1 + \omega + \omega^2 = 0$, da je za $X \in \mathbb{Z}[\omega]$ također i $\overline{X} \in \mathbb{Z}[\omega]$; sasvim precizno, lako se provjeri da je

$$\overline{a + b\omega} = (a - b) - b\omega.$$

Primjetimo da je onda

$$\lambda(X) = X\,\overline{X} = |X|, \qquad X \in \mathbb{Z}[\omega].$$

Neka su sada $A, B \in \mathbb{Z}[\omega]$ i pretpostavimo $B \neq 0$. Tada je

$$A/B = (A\overline{B})/(B\overline{B}) = r + s\omega \qquad \text{za neke } r, s \in \mathbb{Q};$$

ovdje je $B\overline{B} = \lambda(B) \in \mathbb{N}$. Kao i u (i), odaberimo $m, n \in \mathbb{Z}$ takve da je $|r - m| \leq 1/2$ i $|s - n| \leq 1/2$. Onda definiramo

$$C := m + n\omega.$$

Tada je

$$\lambda(A/B - C) = (r - m)^2 - (r - m)(s - n) + (s - n)^2 \leq 3 \cdot 1/4 < 1.$$

Definirajmo i

$$D := A - BC.$$

Sada, kao i u (i), možemo uzeti da je $D \neq 0$; inače $A = BC$. Ali onda je

$$\lambda(D) = \lambda(B)\lambda(A/B - C) < \lambda(B);$$

i gotovi smo. Tako je propozicija dokazana. $\square$

Napomena 9.6. Jedan od osnovnih problema u Komutativnoj algebri, i posebno Algebarskoj teoriji brojeva, je za zadani prsten $\mathcal{A}$ odrediti strukturu od $\mathcal{A}^\times$, grupe invertibilnih elemenata u $\mathcal{A}$, te posebno konkretno računati (neke) invertibilne elemente. Npr., u prstenu $\mathcal{A} = \mathbb{Z}$ je situacija "super-jednostavna", jer je tu $\mathbb{Z} = \{\pm 1\}$. Ali već u prstenu

$$\mathcal{A} = \mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}$$

je grupa $\mathcal{A}^\times$ kompliciranija. Naime, može se pokazati (!probajte probati!) da je neki $a + b\sqrt{2}$ iz $\mathcal{A}^\times$, tj. invertibilni element, akko je $N(a + b\sqrt{2}) := a^2 - 2b^2 \in \{\pm 1\}$. (To je samo specijalan slučaj općenitog i netrivijalnog teorema iz Algebarske teorije brojeva koji glasi: Ako je $K/\mathbb{Q}$ polje algebarskih brojeva i ako je $\mathcal{O}_K$ prsten cijelih u K, onda za tzv. *normu* $N_{K/\mathbb{Q}} : \mathcal{O}_K \to \mathbb{Z}$ imamo da je neki $u \in \mathcal{O}_K$ invertibilan element akko je $N_{K/\mathbb{Q}}(u) \in \{\pm 1\}$.) Posebno, za $\mathcal{A}$ se dobije da je grupa invertibilnih elemenata

$$\mathcal{A}^\times = \{\pm a_n \pm b_n\sqrt{2} \mid n \in \mathbb{N}_0\},$$

gdje su a_n-ovi i b_n-ovi dani rekurzivno

$$a_{n+1} = a_n + 2b_n, \quad b_{n+1} = a_n + b_n \qquad \& \qquad a_0 = b_0 = 1.$$

U vezi sa gornjom Napomenom navedimo ovdje dva jednostavna zadatka o invertibilnim elementima.

Zadatak 62. Neka je $\mathcal{A}$ prsten i pretpostavimo da postoji neka funkcija $\psi : \mathcal{A}\backslash\{0\} \to \mathbb{Z}$ takva da je $\psi(1) = 1$ i $\psi(x\,y) = \psi(x)\psi(y)$ za sve $x, y \in \mathcal{A} \setminus \{0\}$. Dokažite: Ako je element $u \in \mathcal{A} \setminus \{0\}$ invertibilan, onda je $\psi(u) \in \{\pm 1\}$. Vrijedi li nužno i obratno; tj., da li je svaki element $u \in \mathcal{A} \setminus \{0\}$ takav da je $\psi(u) \in \{\pm 1\}$ nužno invertibilan?

Zadatak 63. (i) Odredite grupu invertibilnih elemenata $\mathbb{Z}[\imath]^\times$. (*Uputa:* Pokažite da za funkciju λ, kao u Propoziciji 9.4, vrijedi $\lambda(u) = 1$ akko je u invertibilan, $u \in \mathbb{Z}[\imath]$.)

(ii) Odredite grupu invertibilnih elemenata $\mathbb{Z}[\omega]^\times$.

Dokažimo sada ovaj najavljeni teorem; iako je njegov dokaz zapravo "kopija" dokaza Teorema 8.9, ipak ćemo ga dati.

Teorem 9.7. *Svaka Euklidova domena je* PGI*; tj.,* DGI.

Dokaz. Neka je $\mathcal{A}$, sa funkcijom λ, Euklidova domena i $I \trianglelefteq \mathcal{A}$ ideal. Neka je $0 \neq B \in I$ takav da je

$$\lambda(B) \leq \lambda(X), \qquad \forall\, 0 \neq X \in I.$$

(To možemo. Zašto!?) Tvrdimo da je

$$I = \langle B \rangle.$$

[[Inkluzija ($\supseteq$) je očita. Za ($\subseteq$), neka je $0 \neq A \in I$. Znamo: Postoje C i D iz $\mathcal{A}$ takvi da je $A = BC + D$, gdje je $D = 0$ ili $\lambda(D) < \lambda(B)$. Sada, jer su $A, B \in I$, je $D = A - BC \in I$, a onda, koristeći "minimalnost" od B, slijedi $D = 0$.]] Time je teorem dokazan. $\square$

Korolar 9.8. *Prsteni* $\mathbb{Z}$*,* $\mathbb{F}[X]$*,* $\mathbb{Z}[\imath]$ *i* $\mathbb{Z}[\omega]$ *su* DGI*, domene glavnih ideala.*

Napomena 9.9. Korisno je primjetiti da obrat gornjeg teorema *nije istinit*; tj., *postoje* PGI-ovi koji nisu Euklidove domene! Kao primjer za to imamo potprsten $\mathcal{A}$ od $\mathbb{C}$, definiran kao

$$\mathcal{A} := \{a + b(1 + \imath\sqrt{19}/2 \mid a, b \in \mathbb{Z}\}.$$

Zadatak 64. Dokažite da prsten $\mathcal{A}$, iz gornje Napomene, doista jest DGI, ali nije Euklidova domena.

U vezi sa Euklidovim domenama, dajemo još dva zadatka.

Zadatak 65. (i) Prsten $\mathbb{Z}[X]$ nije Euklidova domena. (*Uputa:* Pokažite da npr. ideal $\langle 2X, 3\rangle$ nije glavni ideal u $\mathbb{Z}[X]$.)
(ii) Ako je $\mathbb{F}$ polje i $n \geq 2$, onda prsten polinoma $\mathbb{F}[X_1, \dots, X_n]$ nije Euklidova domena.
(iii) Da li je svako polje Euklidova domena?
(iv) Da li je potprsten Euklidove domene i sam nužno Euklidova domena?

Zadatak 66. Neka je $\mathcal{A}$ Euklidova domena, i neka je $P \in \operatorname{Spec} \mathcal{A}$ neki prost ideal. Da li je nužno kvocijent $\mathcal{A}/P$ Euklidova domena?

9.2. Prosti i ireducibilni elementi.

Podsjetimo da je $\mathcal{A}$ komutativan prsten, ali ne nužno integralna domena. Isto tako, podsjetimo se:

$$\mathcal{A}^\times := \text{grupa invertibilnih elemenata.}$$

Najprije, uvedimo pojam *djeljivosti* u komutativnim prstenima; to je direktna generalizacija djeljivosti u $\mathbb{Z}$.

Definicija 9.10. Za elemente $x, y \in \mathcal{A}$, gdje je $y \neq 0$, kažemo da "y **dijeli** x", i pišemo $y \mid x$, ako

$$\exists\, c \in \mathcal{A} \ : \qquad x = y\, c.$$

Sada definirajmo neke pojmove koje ćemo u daljnjem promatrati.

Definicija 9.11. Kažemo da su elementi $a, b \in \mathcal{A}$ **asocirani**, i koristimo oznaku $a \sim b$, ako

$$\exists\, u \in \mathcal{A}^\times \ : \qquad a = u\, b.$$

Element $c \in \mathcal{A}$ je **ireducibilan** ako su ispunjena sljedeća dva uvjeta:
(**I1**) $0 \neq c \notin \mathcal{A}^\times$;
(**I2**) Ako je $c = a\, b$, onda je ili $a \in \mathcal{A}^\times$ ili $b \in \mathcal{A}^\times$.

Drugim riječima, element je ireducibilan ako je to nenul neinvertibilan element koji se ne može napisati kao produkt dva neinvertibilna elementa. Skup svih ireducibilnih elemenata u $\mathcal{A}$ označavat ćemo sa

$$\operatorname{Irr} \mathcal{A}.$$

Element $p \in \mathcal{A}$ je **prost** ako su ispunjena sljedeća dva uvjeta:
(**P1**) $0 \neq p \notin \mathcal{A}^\times$;
(**P2**) Ako $p \mid a\, b$, onda ili $p \mid a$ ili $p \mid b$.

Drugim riječima, element je prost ako je to nenul neinvertibilan element koji ima svojstvo da ako dijeli produkt dva elementa, onda on dijeli barem jedan od faktora.

Napomena 9.12. Sasvim je jasno da je relacija "*biti asociran*" relacija ekvivalencije na skupu $\mathcal{A}$. Posljedica toga je da se $\mathcal{A}$, po relaciji $\sim$, raspada na klase. Ako za proizvoljan $a \in \mathcal{A}$ označimo klasu tog elementa

$$[a] := \{x \in \mathcal{A} \mid x \sim a\} \quad (= \{u\, a \mid u \in \mathcal{A}^\times\}),$$

onda se skup svih klasa označava na standardan način, tj., sa $\mathcal{A}/\sim$.

Primjetimo, što je očito iz definicije ireducibilnog elementa, da ako je u nekoj klasi $[a]$ neki element ireducibilan, onda su svi elementi u toj klasi ireducibilni. Ili malo drugačije rečeno: Element a je ireducibilan akko su svi elementi u njegovoj klasi $[a]$ ireducibilni. Sada, u $\mathcal{A}/\sim$ možemo promatrati samo "ireducibilne klase", tj., klase čiji su reprezentanti ireducibilni elementi iz $\mathcal{A}$. Često se za neki pogodno izabran skup reprezentanata svih ireducibilnih klasa koristi oznaka $\operatorname{Irr}\mathcal{A}$; tj., ista oznaka kao za skup *svih* ireducibilnih elemenata (vidi Primjer 9.22).

Sada pogledajmo neke primjere prstena, i u njima neke ireducibilne, odnosno proste, elemente.

Primjer 9.13. (1) Očito je da u prstenu $\mathbb{Z}$, za element $n \in \mathbb{Z}$, imamo:

$$n \text{ je prost} \quad \Longleftrightarrow \quad n = \pm p, \quad p \in \mathbb{N} \text{ prim broj} \quad \Longleftrightarrow \quad n \text{ je ireducibilan.}$$

(2) U prstenu $\mathbb{Z}/6\mathbb{Z}$, prstenu ostataka modulo 6, je element $\overline{2}$ prost; podsjetimo da u prstenu $\mathbb{Z}/n\mathbb{Z}$ elemente označavamo sa $\overline{k} := k + n\mathbb{Z}$. Ali kako je $\overline{2} = \overline{2} \cdot \overline{4}$, te kako elementi $\overline{2}$ i $\overline{4}$ *nisu* invertibilni, to po definiciji ireducibilnog elementa slijedi da $\overline{2}$ nije ireducibilan. Dakle, ovdje posebno vidimo da, za razliku od $\mathbb{Z}$-a, u prstenu $\mathbb{Z}/6\mathbb{Z}$ prosti elementi nisu isto što i ireducibilni elementi. Naravno, sasvim analogno razmatranje vrijedi u bilo kojem prstenu oblika $\mathbb{Z}/n\mathbb{Z}$, kada je n *složen* broj.

(3) Neka je

$$\mathcal{A} := \mathbb{Z}[\sqrt{10}] = \{a + b\sqrt{10} \mid a, b \in \mathbb{Z}\};$$

jasno je da je $\mathcal{A}$ integralna domena. Definirajmo **normu** (usp. Napomenu 9.6)

$$N : \mathcal{A} \to \mathbb{Z}, \qquad N(a + b\sqrt{10}) := a^2 - 10b^2.$$

Lako je provjeriti da za normu N vrijedi sljedeće:

($\circ$) N je (potpuno) *multiplikativna*; tj., imamo $N(x\,y) = N(x)N(y)$, za sve $x, y \in \mathcal{A}$.
($\circ\circ$) Za $x \in \mathcal{A}$ imamo: $x = 0$ akko $N(x) = 0$.

Nadalje, imamo sljedeću tvrdnju.

Tvrdnja. (i) $u \in \mathcal{A}^\times \quad \Longleftrightarrow \quad N(u) = \pm 1$.
(ii) Elementi $2, 3, 4 \pm \sqrt{10}$ su ireducibilni u $\mathcal{A}$.
(iii) Elementi $2, 3, 4 \pm \sqrt{10}$ nisu prosti u $\mathcal{A}$.

[[(ii) Naprimjer, kad bi se 2 mogao napisati u obliku $2 = x\,y$, za neke $x, y \in \mathcal{A}$, onda bi bilo $4 = N(2) = N(x)N(y)$. Ali lako je pokazati da za bilo koji $\alpha \in \mathcal{A}$ imamo $N(\alpha) \neq \pm 2, \pm 3$. Slijedi da je ili $N(x) = \pm 1$ ili $N(y) = \pm 1$; tj., po (i), ili je x invertibilan ili je y invertibilan. Sasvim se analogno pokaže da su i ostala tri elementa ireducibilna.

(iii) Primjetimo da je $3 \cdot 2 = 6 = (4 + \sqrt{10})(4 - \sqrt{10})$. Sada, kad bismo u $\mathcal{A}$ imali da $3 \mid 4 + \sqrt{10}$ ili $3 \mid 4 - \sqrt{10}$, onda bi bilo $4 \pm \sqrt{10} = 3\,c$, za neki $c \in \mathcal{A}$. No onda (u oba slučaja) slijedi

$$6 = N(4 \pm \sqrt{10}) = N(3)N(c) = 9N(c);$$

što je nemoguće, jer mora biti $N(c) \in \mathbb{Z}$.]]

Napomena 9.14. Primjetimo ovdje da prsten $\mathbb{Z}[\sqrt{10}]$ nije DGI; vidi Propoziciju 9.16(ii) dolje.

Zadatak 67. Dokažite detaljno sve tvrdnje navedene u prethodnom primjeru. Probajte naći neki drugi broj $d \neq 10$ tako da u prstenu $\mathbb{Z}[\sqrt{d}] := \{a + b\sqrt{d} \mid a, b \in \mathbb{Z}\}$ postoje neki elementi koji su ireducibilni, ali nisu prosti. U vezi s gornjom napomenom, nađite neki konkretni ideal $I \trianglelefteq \mathbb{Z}[\sqrt{10}]$ koji nije glavni.

Prije nego što iskažemo i dokažemo najavljenu propoziciju, uvedimo pojam *najveće zajedničke mjere* za proizvoljan komutativan prsten $\mathcal{A}$; primjetimo da je definicija potpuno ista kako se to definira u prstenu $\mathbb{Z}$.

Definicija 9.15. Neka je $\mathcal{A}$ prsten i neka su $a, b \in \mathcal{A}$ dva elementa. Element $d \in \mathcal{A}$ zove se **najveća zajednička mjera** od a i b, ili kraće NZM, ako vrijedi:

(**M1**) $d \mid a \quad \& \quad d \mid b$;

(**M2**) Ako je d' neki element iz $\mathcal{A}$ takav da $d' \mid a$ i $d' \mid b$, onda $d' \mid d$.

Oznaka za NZM od a i b je

$$d = (a, b).$$

Propozicija 9.16. *Neka je $\mathcal{A}$ integralna domena. Tada vrijede sljedeće tvrdnje.*

(i) *Za element $p \in \mathcal{A}$ imamo:*

$$p \text{ je prost} \quad \Longrightarrow \quad p \text{ je ireducibilan.}$$

(ii) *Ako je $\mathcal{A}$* DGI*, onda je element u $\mathcal{A}$ ireducibilan akko je on prost. Drugim riječima, u svakoj* DGI *je*

$$\textit{prost element} \equiv \textit{ireducibilan element.}$$

(iii) *Ako je $\mathcal{A}$* DGI*, onda je to* Noetherin *prsten; tj., ima sljedeće svojstvo:*
Ako je $I_1 \subseteq I_2 \subseteq \cdots$ rastući niz ideala u $\mathcal{A}$, onda postoji $k \in \mathbb{N}$ takav da je

$$I_k = I_{k+n} \qquad \forall\, n \in \mathbb{N}.$$

Napomena 9.17. Za prsten R, komutativan ili ne, kažemo da je **Noetherin** ukoliko je on i lijevo i desno Noetherin. Pritom je R **lijevo Noetherin** ukoliko vrijedi da svaki rastući niz

$$L_1 \subseteq L_2 \subseteq \cdots$$

lijevih ideala L_i u R "stabilizira", tj., da postoji neki indeks k takav da je

$$L_k = L_{k+n} \qquad \forall\, n \in \mathbb{N}.$$

Analogno se definira i **desno Noetherin** prsten, samo što sada namjesto L_i-ova gledamo *desne* ideale D_i u R.

Naglasimo kako je "svojstvo Noetherinosti" fundamentalan pojam u algebri. Naime, kako u komutativnoj, tako i u nekomutativnoj teoriji, ima cijelo mnoštvo prstena koji su Noetherini. Tako su zapravo (gotovo) svi prsteni koje smo mi u ovom kolegiju spominjali Noetherini. No to nije lako dokazati. Naprimjer, sljedeći je rezultat slavni "Hilbertov teorem o bazi"; to je na koncu 19. stoljeća bila fundamentalna opservacija koja je kao posljedicu imala "smrt" tzv. teorije invarijanata. (Precizno rečeno, u modernoj terminologiji, tim je rezultatom pokazano da je svaki ideal, u prstenu polinoma u konačno varijabli sa koeficijentima iz nekog polja, konačnogeneriran.) Istini za volju, naglasimo da je originalni Hilbertov teorem imao, namjesto $\mathcal{A}$, polje $\mathbb{C}$; korak da se od tog originalnog rezultata dobije niže navedeni općenitiji rezultat je u biti jednostavan.

Teorem. (Hilbertov teorem o bazi)
Pretpostavimo da je $\mathcal{A}$ komutativan Noetherin prsten. Tada je i prsten polinoma $\mathcal{A}[X_1, \ldots, X_n]$, za proizvoljan $n \in \mathbb{N}$, također Noetherin. Posebno, budući je svako polje $\mathbb{F}$ Noetherin prsten (jedini ideali u polju su trivijalni ideali), to je $\mathbb{F}[X_1, \ldots, X_n]$ Noetherin prsten.

Prije same propozicije, dokažimo ovu jednostavnu lemu.

Lema 9.18. *Ako je $\mathcal{A}$* DGI*, onda za svake $a, b \in \mathcal{A}$ postoji* NZM $d = (a, b)$*, i vrijedi*

$$\langle a, b\rangle = \langle d\rangle; \qquad \textit{tj.} \;\; \mathcal{A}\, d = \mathcal{A}\, a + \mathcal{A}\, b.$$

Dokaz. Definirajmo ideal $I := \langle a, b\rangle$. Budući je $\mathcal{A}$ DGI, onda je posebno i ideal I glavni; dakle, $I = \langle d\rangle$, za neki $d \in \mathcal{A}$. Sada, jer su $a, b \in I$, to je onda $\langle a\rangle \subseteq \langle d\rangle$ i $\langle b\rangle \subseteq \langle d\rangle$. Slijedi da je $a = d\,x$, za neki $x \in \mathcal{A}$, a odavde da $d \mid a$; i analogno, $d \mid b$. Tako imamo da d zadovoljava uvjet (**M1**) iz definicije NZM. Ako je sada d' neki element takav da $d' \mid a$ i $d' \mid b$, onda je $\langle a\rangle \subseteq \langle d'\rangle$ i $\langle b\rangle \subseteq \langle d'\rangle$. Dakle,

$$\langle d\rangle = I = \langle a\rangle + \langle b\rangle \subseteq \langle d'\rangle \qquad \Longrightarrow \qquad d' \mid d.$$

Znači, imamo i uvjet (**M2**), pa je d, po definiciji, NZM od a i b. □

Napomena 9.19. (1) Gornja je lema poopćenje sa $\mathbb{Z}$ na proizvoljnu DGI $\mathcal{A}$. Naime, za $a, b \in \mathbb{Z}$ dobro je poznato da postoji NZM $d = (a, b)$, i onda postoje $X, Y \in \mathbb{Z}$ takvi da je

$$d = Xa + Yb;$$

npr., za $a = 24$ i $b = 34$ je $d = 2$, i onda $2 = -7 \cdot 24 + 5 \cdot 34$.

(2) Podsjetimo se da je svaka Euklidova domena ujedno i DGI; ali postoje DGI koje nisu Euklidove domene. Drugim riječima, klasa komutativnih prstena koji su DGI je nešto veća nego klasa komutativnih prstena koji su Euklidove domene. U vezi s prethodnom lemom, koja je rezultat "egzistencijalne naravi", naglasimo da u slučaju da je naš prsten $\mathcal{A}$ Euklidova domena, postoji "konstruktivna metoda" za nalaženje NZM $d = (a, b)$, za dva elementa $a, b \in \mathcal{A}$. To je poznati *Euklidov algoritam.*

Teorem. (Euklidov algoritam)
Neka je $\mathcal{A}$ Euklidova domena, sa pripadnom funkcijom λ, te neka su $a, b \in \mathcal{A}$ dva elementa gdje je $b \neq 0$. Višestrukom primjenom Definicije 9.1 imamo:

$$\begin{aligned}
a &= q_0 b + r_1, && \textit{gdje je} \quad r_1 = 0 \;\; \textit{ili} \;\; \lambda(r_1) < \lambda(b);\\
b &= q_1 r_1 + r_2, && \textit{gdje je} \quad r_2 = 0 \;\; \textit{ili} \;\; \lambda(r_2) < \lambda(r_1);\\
r_1 &= q_2 r_2 + r_3, && \textit{gdje je} \quad r_3 = 0 \;\; \textit{ili} \;\; \lambda(r_3) < \lambda(r_2);\\
&\cdots && \cdots \qquad\qquad \cdots\\
r_k &= q_{k+1} r_{k+1} + r_{k+2}, && \textit{gdje je} \quad r_{k+2} = 0 \;\; \textit{ili} \;\; \lambda(r_{k+2}) < \lambda(r_{k+1});\\
&\cdots && \cdots \qquad\qquad \cdots
\end{aligned}$$

Neka je sada n najmanji *takav da je ostatak* $r_{n+1} = 0$*; ovdje je* $r_0 = b$*. Tada za* NZM (a, b) *imamo:*

$$r_n = (a, b).$$

Zadatak 68. (i) Dokažite prethodni teorem; o Euklidovom algoritmu.

(ii) Ako je $\mathcal{A}$ Euklidova domena, onda Euklidov algoritam i Lemma 9.18 osiguravaju da za $a, b \in \mathcal{A}$ postoje elementi $\alpha, \beta \in \mathcal{A}$ takvi da je NZM $(a, b) = \alpha a + \beta b$. Moraju li ti α i β biti jedinstveno određeni? (*Uputa:* Gledajte npr. slučaj $\mathcal{A} = \mathbb{R}[X]$, i onda polinome $a = a(X) := X$ i $b = b(X) := X + 1$.)

Dokaz Propozicije 9.16. (i) Neka je p prost element, ali pretpostavimo da on nije ireducubilan. Znači da postoje neki $a, b \notin \mathcal{A}^\times$ takvi da je $p = a\,b$. Ali $p = a\,b$ posebno povlači da $p \mid a\,b$, a kako je p prost, slijedi $p \mid a$ ili $p \mid b$. BSO pretpostavimo da $p \mid a$; dakle je $a = p\,x$, za neki $x \in \mathcal{A}$. Sada, iz $p = a\,b$ i $a = p\,x$ slijedi $p = p\,x\,b$, što je dalje ekvivalentno $p(1 - x\,b) = 0$. Kako je $\mathcal{A}$ integralna domena, a element $p \neq 0$, slijedi da je $1 = x\,b$. No to znači da je b invertibilan; kontradikcija.

(ii) Pretpostavimo sada da je $\mathcal{A}$ DGI, i da je $p \in \mathcal{A}$ neki ireducibilan element. Pokazat ćemo da je on i prost. U tu svrhu, pretpostavimo da postoje neki $a, b \in \mathcal{A}$ takvi da $p \mid a\,b$, ali $p \nmid a$. (Mi moramo pokazati da $p \mid b$!) Pokažimo najprije ovu pomoćnu tvrdnju:

Tvrdnja. Ako je $d := (a, p)$, onda je $d \in \mathcal{A}^\times$.

[[Naime, po prvom uvjetu u definiciji NZM, imamo $d \mid a$ i $d \mid p$; i onda, posebno, $p = d\,\omega$, za neki $\omega \in \mathcal{A}$. Ali p je ireducibilan, pa onda slijedi da je ili $d \in \mathcal{A}^\times$ ili $d \sim p$. No, $d \sim p$ je, po definiciji relacije "$\sim$", ekvivalentno tomu da je $u\,p = d$, za neki $u \in \mathcal{A}^\times$; i posebno, onda $p \mid d$. Konačno, iz $p \mid d$ i $d \mid a$ slijedi da $p \mid a$, što je kontradikcija; dakle, mogućnost $d \sim p$ otpada, pa tvrdnja slijedi.]]

Sada, koristeći gornju Tvrdnju i Lemu 9.18, imamo da je

$$\mathcal{A} = \langle 1 \rangle = \langle d \rangle = \langle a, p \rangle \quad \Longrightarrow \quad \langle b \rangle = \langle a\,b, p\,b \rangle;$$

posljednja je implikacija jasna. Konačno, jer $p \mid a\,b$, imamo $a\,b \in \langle p \rangle$. Ali kako je očito i $p\,b \in \langle p \rangle$, to po gornjoj jednakosti slijedi

$$\langle b \rangle \subseteq \langle p \rangle \quad \Longrightarrow \quad p \mid b,$$

što smo i morali pokazati.

(iii) Budući je $\mathcal{A}$ PGI, onda je posebno $I_j = \langle a_j \rangle$, za neke elemente $a_j \in \mathcal{A}$. Definirajmo $I := \bigcup_{j=1}^{\infty} I_j = \bigcup_j \langle a_j \rangle$. Očito je $I \trianglelefteq \mathcal{A}$ ideal. No, ponovo jer je $\mathcal{A}$ PGI, imamo da je $I = \langle a \rangle$, za neki $a \in \mathcal{A}$. Ali $a \in I$ povlači da je posebno $a \in I_k$, za neki $k \in \mathbb{N}$; to po definiciji unije skupova. Dakle je $\langle a \rangle \subseteq I_k$, a onda je jasno da je

$$I = I_k = I_{k+1} = \cdots$$

Tako je propozicija dokazana. $\square$

9.3. Faktorijalni prsteni.

Sada ćemo definirati pojam *faktorijalnog prstena.*

Definicija 9.20. Integralna domena $\mathcal{A}$ je **faktorijalan prsten**, ili *faktorizacijski prsten*, ako vrijedi sljedeće:

(FP1) (*Egzistencija rastava*)
Za svaki $a \in \mathcal{A}$ takav da je $0 \neq a \notin \mathcal{A}^\times$, postoji rastav

$$a = c_1 \cdots c_n,$$

gdje su $c_i \in \mathcal{A}$ ireducibilni elementi.

(FP2) (*Jedinstvenost rastava*)
Ako imamo dva rastava $a = c_1 \cdots c_n = e_1 \cdots e_m$, onda je $m = n$, i postoji neka permutacija $\sigma \in \mathcal{S}_n$ tako da je $c_i \sim e_{\sigma(i)}$.

Napomena 9.21. Primjetimo kako je uvjet (**FP2**) zapravo 'jedinstvenost rastava do na elemente iz $\mathcal{A}^\times$'. Sasvim precizno, rastav $a = c_1 \cdots c_n$, nekog elementa a, nećemo razlikovati od rastava $a = e_1 \cdots e_n$, ako je $e_i = u_i \, c_{\sigma(i)}$ za neke invertibilne elemente $u_i \in \mathcal{A}^\times$ i neku permutaciju $\sigma \in \mathcal{S}_n$. Konkretno, npr. u prstenu $\mathbb{Z}$ rastave $2 \cdot 2 \cdot 5 \cdot 5 \cdot 5 \cdot 7$ i $(-7) \cdot 2 \cdot (-5) \cdot (-5) \cdot 2 \cdot 5$, broja 3500, ne razlikujemo.

Primjer 9.22. (1) Prsten $\mathbb{Z}$ je faktorijalan, u smislu gornje definicije. Dokaz te činjenice je ništa drugo nego dobro poznati *Osnovni teorem aritmetike*; to je detaljno objašnjeno na početku ovog odjeljka. Napomenimo kako se za "istaknuti" skup reprezentanata ireducibilnih klasa standardno uzima skup $\mathcal{P}$, skup svih prim brojeva u $\mathbb{N}$. Tojest,

$$\operatorname{Irr} \mathbb{Z} = \{2, 3, 5, 7, \ldots\}$$

(2) Kao što ćemo pokazati u teoremu koji slijedi, skup polinoma $\mathbb{F}[X]$, sa koeficijentima iz nekog polja $\mathbb{F}$, je faktorijalan prsten. U vezi s tim, zanimljivo je pitanje kako u tom prstenu izgledaju ireducibilni elementi. Pokazuje se da je odgovor na to pitanje, u punoj općenitosti, vrlo kompliciran, i usko je vezan s tim kakovo je polje $\mathbb{F}$. (Tek naglasimo da je problem nalaženja ireducibilnih polinoma već u $\mathbb{Q}[X]$ neočekivano težak; tu su razvijene brojne metode i dokazani mnogi rezultati koji pomažu odgovoriti da li je neki konkretan polinom $p(X) \in \mathbb{Q}[X]$ ireducibilan ili ne.) Za ilustraciju, podsjetimo se kako smo u *Elementarnoj matematici 1* odgovorili na to pitanje u slučaju $\mathbb{F} = \mathbb{C}$ ili $\mathbb{R}$. Imamo

$$\operatorname{Irr} \mathbb{C}[X] = \{X - \alpha \mid \alpha \in \mathbb{C}\}$$

i

$$\operatorname{Irr} \mathbb{R}[X] = \{X - \alpha \mid \alpha \in \mathbb{R}\} \cup \{X^2 + pX + q \mid p, q \in \mathbb{R} \ \& \ p^2 - 4q < 0\}.$$

Ovdje su sa Irr? označeni "pogodno uzeti" reprezentanti ireducibilnih klasa; to su tzv. *normirani polinomi*, polinomi čiji su vodeći koeficijenti jednaki 1. (Podsjetimo se da su u prstenu $\mathcal{A}[X]$, gdje je $\mathcal{A}$ neki prsten, invertibilni elementi $\mathcal{A}[X]^\times = \mathcal{A}^\times$; posebno je onda $\mathbb{F}[X]^\times = \mathbb{F}^\times = \mathbb{F} \setminus \{0\}$ (vidi Zadatak 60). Zato su u prstenu $\mathbb{F}[X]$ dva polinoma $p(X)$ i $q(X)$ asocirana akko postoji neki $0 \neq \alpha \in \mathbb{F}$ takav da je $q(X) = \alpha p(X)$.) Primjetimo kako je ovdje odgovor na postavljeno pitanje bio zapravo vrlo jednostavan. Jedan od odgovora mogao bi biti i taj da su na neki način polja $\mathbb{C}$ i $\mathbb{R}$ dosta jednostavna, ili bolje rečeno "dosta specifična"; svakako, što se tiče aritmetike, polje $\mathbb{Q}$ sa "svim svojim pratećim objektima" je neusporedivo zanimljivije i "misterioznije" nego li polja $\mathbb{C}$ i $\mathbb{R}$.

Zadatak 69. Dokažite da su doista $\operatorname{Irr}\mathbb{C}[X]$ i $\operatorname{Irr}\mathbb{R}[X]$ kao što je navedeno u prethodnom Primjeru.

Sada ćemo iskazati i dokazati najavljeni teorem, koji je glavni rezultat ovog odjeljka.

Teorem 9.23. *Svaka* DGI *je faktorijalan prsten.*

Najprije dokazujemo ovu propoziciju.

Propozicija 9.24. *Ako je $\mathcal{A}$* DGI*, onda se svaki element $0 \neq a \notin \mathcal{A}^\times$ može (općenito nejedinstveno!) napisati kao*

$$a = c_1 \cdots c_n,$$

gdje su c_i neki ireducibilni elementi u $\mathcal{A}$.

Dokaz. BSO pretpostavimo da a nije ireducibilan; inače nemamo što dokazivati. Tada se, po definiciji ireducibilnih elemenata, a može rastaviti kao

$$a = a_1 b_1, \qquad a_1, b_1 \notin \mathcal{A}^\times.$$

Sada, ako a_1 nije ireducibilan, onda njega rastavimo, analogno kao i sam a, na $a_1 = a_2 b_2$, gdje $a_2, b_2 \notin \mathcal{A}^\times$. Ako ni a_2 nije ireducibilan, postupak nastavimo, tj., rastavimo $a_2 = a_3 b_3$, itd. Tako dobivamo niz elemenata $a_1, a_2, \ldots$, za koje vrijedi

$$\langle a \rangle \subset \langle a_1 \rangle \subset \langle a_2 \rangle \subset \cdots$$

[[Naime, kako je $a_i = a_{i+1} b_{i+1}$ ze neke *neinvertibilne* elemente a_{i+1} i b_{i+1}, to za ideale generirane sa a_i i a_{i+1} imamo $\langle a_i \rangle \subseteq \langle a_{i+1} \rangle$. Ali, kao što smo gore i označili, štoviše imamo i strogu inkluziju. Da to vidimo pretpostavimo suprotno, tj., da imamo jednakost $\langle a_i \rangle = \langle a_{i+1} \rangle$. To posebno znači da je $a_{i+1} \in \langle a_i \rangle$, tj., $a_{i+1} = a_i x$, za neki $x \in \mathcal{A}$. Sada iz $a_{i+1} = a_i x$ i $a_i = a_{i+1} b_{i+1}$ dobivamo

$$a_{i+1} = (a_{i+1} b_{i+1}) x \qquad \Longleftrightarrow \qquad a_{i+1}(1 - b_{i+1} x) = 0.$$

No kako je $\mathcal{A}$ integralna domena, iz posljednje jednakosti slijedi da je $1 = b_{i+1} x$, tj., b_{i+1} je invertibilan; kontradikcija.]]

Ali sada se sjetimo da smo u Propoziciji 9.16(iii) dokazali da je svaka DGI Noetherin prsten. To konkretno znači da gore napisan niz ideala $\langle a \rangle \subset \langle a_1 \rangle \subset \langle a_2 \rangle \subset \cdots$ ne može biti beskonačan. No to zapravo znači da smo mi, počevši od $a_0 = a$, nakon nekog k-tog koraka došli do elementa a_k koji **je** ireducibilan. Tako smo mi zapravo dokazali da postoji neki ireducibilan element, označimo ga sa α_1 (zapravo je taj α_1 jednak gornjem a_k!), takav da je

$$a = \alpha_1 \beta_1 \qquad \text{za neki } \beta_1 \in \mathcal{A}.$$

Ako je sada taj β_1 ireducibilan, onda smo gotovi. A ako nije, onda se i on može napisati, na sasvim isti način kao što smo to napravili za a, u obliku $\beta_1 = \alpha_2 \beta_2$, gdje je α_2 ireducibilan. Postupak nastavljamo, i dobivamo niz elemenata $\beta_1, \beta_2, \ldots$. Sasvim isto kao i za a_i-ove, imamo

$$\langle \beta_1 \rangle \subset \langle \beta_2 \rangle \subset \langle \beta_3 \rangle \subset \cdots$$

No isti razlog kao i prije osigurava da taj niz ideala nije beskonačan. Drugim riječima, neki je β_l ireducibilan. Tako zapravo imamo rastav

$$a = \alpha_1 \alpha_2 \cdots \alpha_l \beta_l,$$

rastav od a na ireducibilne elemente. Time je dokaz propozicije gotov. $\square$

Treba nam još jedan novi pojam; i on je, kao što ćemo vidjeti u sljedećem primjeru, direktna generalizacija dobro poznate situacije u $\mathbb{Z}$.

Definicija 9.25. Neka je $\mathcal{A}$ DGI i neka je $p \in \mathcal{A}$ neki prost element ($\equiv$ ireducibilan element). Definirajmo **red od** p, kao funkciju

$$\mathrm{ord}_p : \mathcal{A} \to \mathbb{N}_0, \qquad \mathrm{ord}_p(a) := n, \quad \text{gdje je } n \text{ t.d. } p^n | \, a \quad \& \quad p^{n+1} \nmid a.$$

Napomena 9.26. Primjetimo kako broj n u gornjoj definiciji uvijek postoji. Naime, kad on ne bi postojao, to bi značilo da mi za svaki $k \in \mathbb{N}$ imamo $p^k \mid a$, tj., da imamo neke b_k takve da je $a = p^k b_k$. Ali onda bismo imali beskonačan niz strogo rastućih ideala $\langle b_1 \rangle \subset \langle b_2 \rangle \subset \langle b_3 \rangle \subset \cdots$; što je nemoguće.

Primjer 9.27. (1) U prstenu $\mathbb{Z}$, za neki prim broj p, jasno je da za svaki element $a \in \mathbb{Z}$ postoji jedinstven $n \in \mathbb{N}_0$ takav da $p^n | \, a$, ali $p^{n+1} \nmid a$; sada definiramo $\mathrm{ord}_p(a) := n$.

(2) Neka je sada $\mathcal{A} = \mathbb{C}[X]$. Vidjeli smo da je $\mathrm{Irr}\, \mathbb{C}[X] = \{X - \alpha \mid \alpha \in \mathbb{C}\}$. S druge strane, kao posljedicu *Osnovnog teorema algebre*, imamo da se svaki polinom $F \in \mathbb{C}[X]$ može na jedinstven način napisati u obliku

$$F(X) = c \prod_{i=1}^{t} (X - \alpha_i)^{s_i}, \qquad c, \alpha_i \in \mathbb{C}, \quad s_i \in \mathbb{N}.$$

Sada se definira red od $X - \alpha_i$ kao

$$\mathrm{ord}_{X-\alpha_i}(F) := s_i.$$

Lema 9.28. *Neka je* $\mathcal{A}$ DGI *i neka su* $0 \neq a, b \in \mathcal{A}$. *Tada za bilo koji prost element* p *imamo*

$$\mathrm{ord}_p(a\, b) = \mathrm{ord}_p(a) + \mathrm{ord}_p(b)$$

Dokaz. Označimo $\alpha := \mathrm{ord}_p(a)$ i $\beta := \mathrm{ord}_p(b)$. Tada je $a = p^\alpha c$ i $b = p^\beta e$, gdje su elementi c i e takvi da $p \nmid c$ i $p \nmid e$. Slijedi da je $a\, b = p^{\alpha+\beta} c\, e$. Ali p je prost, pa onda $p \nmid c\, e$. Iz posljednje dvije činjenice zaključujemo da je $\mathrm{ord}_p(a\, b) = \alpha + \beta$. Time je lema dokazana. $\square$

Neka je sada $\mathfrak{P} \subseteq \mathcal{A}$ neki podskup koji se sastoji od prostih elemenata i takav je da vrijede sljedeća dva uvjeta:

(**I**) Svaki prost element $p \in \mathcal{A}$ je asociran nekom elementu $\pi \in \mathfrak{P}$.

(**II**) Nikoja dva elementa $\pi_1, \pi_2 \in \mathfrak{P}$ nisu asocirana.

Primjetimo da u $\mathbb{Z}$ možemo uzeti za $\mathfrak{P}$ skup svih prim brojeva u $\mathbb{N}$. U slučaju $\mathbb{F}[X]$, za $\mathbb{F}$ polje, za $\mathfrak{P}$ možemo uzeti skup svih normiranih ireducibilnih polinoma.

Sada dajemo malo precizniju formulaciju Teorema 9.23.

Teorem 5.22.′ *Neka je* $\mathcal{A}$ DGI *i neka je skup* $\mathfrak{P} \subseteq \mathcal{A}$ *izabran kao gore. Tada svaki element* $0 \neq a \in \mathcal{A}$ *možemo na* jedinstven *način napisati u obliku*

$$a = u \prod_{p \in \mathfrak{P}} p^{l(p)}, \qquad u \in \mathcal{A}^{\times}, \quad l(p) = \mathrm{ord}_p(a).$$

(Tu su u *i* $l(p)$*-ovi jedinstveni!)*

Dokaz. (*Egzistencija*) To je Propozicija 9.24.

(*Jedinstvenost*) Primjenom funkcije ord_q, za $q \in \mathfrak{P}$, na jednakost $a = u \prod_{p \in \mathfrak{P}} p^{l(p)}$ dobijemo

$$\mathrm{ord}_q(a) = \mathrm{ord}_q(u) + \sum_p l(p)\,\mathrm{ord}_q(p);$$

tu koristimo i Lemu 9.28. Ali očito je da $\mathrm{ord}_q(u) = 0$ i $\mathrm{ord}_q(p) = 1$ ako je $q = p$, odnosno $\mathrm{ord}_q(p) = 0$ ako je $q \neq p$. Znači da je $l(p) = \mathrm{ord}_p(a)$; tj., brojevi $l(p)$ su doista jedinstveni. No onda je očito da je i u jedinstven. Time je teorem dokazan. □

(* * *)

Ovaj odjeljak završavamo sa tri zadatka od kojih prva dva donose dvije vrlo korisne informacije o domenama glavnih ideala.

Zadatak 70. Ako je $\mathcal{A}$ DGI, onda je svaki nenul prost ideal u $\mathcal{A}$ štoviše i maksimalan ideal, tj., imamo

$$\mathrm{Spec}\,\mathcal{A} \setminus \{(0)\} \subseteq \mathrm{Max}\,\mathcal{A}.$$

Zadatak 71. Dokažite: Ako je $\mathcal{A}$ PGI i ako je $I \trianglelefteq \mathcal{A}$ bilo koji ideal, onda je i kvocijentni prsten $\mathcal{A}/I$ također PGI.

U vezi s idućim zadatkom podsjetimo se da pojmovi invertibilnog, ireducibilnog i prostog elementa ne pretpostavljaju da je neki prsten $\mathcal{A}$, koji gledamo, nužno integralna domena.

Zadatak 72. Neka je $n \in \mathbb{N}$ takav da postoji neki prim broj p takav da p^2 dijeli n. Dokažite da onda element $\overline{p} = p + n\mathbb{Z}$ je ireducibilan, u prstenu $\mathbb{Z}/n\mathbb{Z}$.

10. Polja

U ovom se odjeljku, u vrlo kratkim crtama, bavimo poljima. Cilj nam je prvenstveno uvesti tek neke osnovne pojmove iz Teorije polja; kao što su pojmovi: *potpolje*, *proširenje polja*, *prosto polje*, *konačno proširenje*, *algebarsko proširenje*, *algebarsko zatvorenje*, *algebraski zatvarač*, itd. Pored toga, navodimo još neke primjere polja, te dokazujemo dva osnovna rezultata (Propozicija 10.5 i Teorem 10.9). To radimo u prvom pododjeljku. U drugom se pododjeljku, uz ponešt detalja, ukratko bavimo *kvaternionima*; kao primjerima (nekomutativnih) tijela.

10.1. Osnovni pojmovi i neki primjeri.

Podsjetimo se da je prsten R s jedinicom *tijelo* ako je $R^\times = R \setminus \{0\}$, tj., ako je svaki nenul element invertibilan. Komutativno tijelo je *polje*. Od dobro poznatih primjera polja spomenimo $\mathbb{Q}$, $\mathbb{R}$ i $\mathbb{C}$. Još smo imali i polja $\mathbb{Z}/p\mathbb{Z}$, za $p \in \mathbb{N}$ prim broj, kao primjere konačnih polja. Definirali smo i tzv. *kvadratna proširenja* od $\mathbb{Q}$, $\mathbb{Q}(\sqrt{d}) = \{a + b\sqrt{d} \mid a, b \in \mathbb{Q}\}$; vidi dolje.

Polja ćemo označavati slovima

$$\mathbb{K},\ \mathbb{L}\ ,\mathbb{E}\ ,\mathbb{F}\ \ldots$$

Za neki element x nekog polja $\mathbb{K}$, njegov inverz x^{-1} često označavamo i sa $1/x$. Zato, isto tako, pišemo često x/y namjesto $x\,y^{-1}$.

Definicija 10.1. Ako su $\mathbb{K}$, $\mathbb{L}$ polja takva da je $\mathbb{K} \subseteq \mathbb{L}$, onda kažemo da je $\mathbb{K}$ **potpolje** od $\mathbb{L}$, ili da je $\mathbb{L}$ **proširenje** od $\mathbb{K}$. Oznaka za to će biti

$$\mathbb{L} \mid \mathbb{K};$$

analogno, za polja $\mathbb{K}_1 \subseteq \mathbb{K}_2 \subseteq \cdots \subseteq \mathbb{K}_n$, pišemo

$$\mathbb{K}_n \mid \mathbb{K}_{n-1} \mid \cdots \mid \mathbb{K}_1.$$

Ako posebno imamo $\mathbb{L} \mid \mathbb{M} \mid \mathbb{K}$, onda ćemo reći da je $\mathbb{M}$ **međupolje** koje sadrži $\mathbb{K}$ i sadržano je u $\mathbb{L}$; ili kraće, da je $\mathbb{M}$ međupolje za $\mathbb{L} \mid \mathbb{K}$.

Napomena 10.2. Ako imamo $\mathbb{L} \mid \mathbb{E}_i \mid \mathbb{K}$, za neka međupolja $(\mathbb{E}_i;\ i \in I)$, onda je sasvim jasno da je

$$\mathbb{E} := \bigcap_I \mathbb{E}_i$$

također polje. (Naime, znamo od prije da je presjek $\Pi := \bigcap_{\mathcal{F}} P$, bilo koje familije $\mathcal{F}$ potprstena nekog "velikog" prstena R, ponovo potprsten od R. Nadalje, ako su svi $P \in \mathcal{F}$ štoviše i polja, onda je i Π također polje. Za to vidjeti treba samo primjetiti da ako je $0 \neq x \in \Pi$, onda je, po definiciji presjeka, i inverz x^{-1} također iz Π.) Za polje $\mathbb{E}$ imamo $\mathbb{L} \mid \mathbb{E} \mid \mathbb{K}$; tj., $\mathbb{E}$ je međupolje za $\mathbb{L} \mid \mathbb{K}$.

Sada, analogno kao što smo to napravili i za grupe i za ideale, definiramo pojam polja generiranog nekim skupom.

Definicija 10.3. Neka je $\mathbb{L} \mid \mathbb{K}$ i $S \subseteq \mathbb{L}$ neki podskup. Definirajmo onda polje $\mathbb{K}(S)$ kao *najmanje potpolje od* $\mathbb{L}$ *koje sadrži i polje* $\mathbb{K}$ *i skup* S, tj.,

$$\mathbb{K}(S) := \bigcap_{\substack{\mathbb{L}|\mathbb{E}|\mathbb{K} \\ \mathbb{K}\cup S\subseteq \mathbb{E}}} \mathbb{E};$$

polje $\mathbb{K}(S)$ zovemo **proširenje** od $\mathbb{K}$ u $\mathbb{L}$ **generirano** sa S. Posebno, ako je skup $S = \{a\}$ jednočlan, pišemo $\mathbb{K}(a)$ namjesto $\mathbb{K}(\{a\})$; analogno, za $S = \{a_1, a_2, \ldots, a_n\}$ pišemo $\mathbb{K}(a_1, \ldots, a_n)$.

Primjer 10.4. (1) Neka je $\mathbb{L} = \mathbb{R}$, $\mathbb{K} = \mathbb{Q}$ i $a = \sqrt{n}$, za neki $n \in \mathbb{N}$. Definirajmo polje

$$\mathbb{E}_n := \mathbb{Q}(\sqrt{n}) \overset{\text{tv.}}{=} \{a + b\sqrt{n} \mid a, b \in \mathbb{Q}\}.$$

Ovdje mi definiramo polje $\mathbb{E}_n := \mathbb{Q}(\sqrt{n})$ i tvrdimo da je ono jednako $\mathbb{F}_n := \{a + b\sqrt{n} \mid a, b \in \mathbb{Q}\}$. Da to vidimo treba samo pokazati da je $\mathbb{F}_n$ doista polje; jer je tada jasno da svako drugo polje $\mathbb{E}$, koje sadrži $\mathbb{K} \cup \{\sqrt{n}\}$, nužno sadrži i $\mathbb{F}_n$. Ali, kao prvo, očito je skup $\mathbb{F}_n$ grupa s obzirom na zbrajanje, i zatvoren je za množenje. Jedino još treba vidjeti da svaki nenul element $a + b\sqrt{n} \in \mathbb{F}_n$ ima inverz u $\mathbb{F}_n$. No, imamo

$$(a + b\sqrt{n})^{-1} = \frac{1}{a + b\sqrt{n}} = \frac{1}{a + b\sqrt{n}}\,\frac{a - b\sqrt{n}}{a - b\sqrt{n}} = \frac{a}{a^2 - nb^2} - \frac{b}{a^2 - nb^2}\sqrt{n};$$

tj., $(a + b\sqrt{n})^{-1} = x + y\sqrt{n}$, gdje su $x := a/(a^2 - nb^2)$ i $y := b/(a^2 - nb^2)$ oba iz $\mathbb{Q}$. Tako je doista $(a + b\sqrt{n})^{-1} \in \mathbb{F}_n$.

Sada je, jasno,

$$\mathbb{R} \mid \mathbb{E}_n \mid \mathbb{Q}.$$

(Primjetimo da je npr. $\mathbb{E}_4 = \mathbb{Q}$, ali za n kvadratno slobodan je $\mathbb{Q} \subset \mathbb{E}_n$) .

(2) Neka je sada $\mathbb{L} = \mathbb{C}$, $\mathbb{K} = \mathbb{Q}$ i $a = \sqrt{-n}$, za neki $n \in \mathbb{N}$; možemo odmah pretpostaviti da je n kvadratno slobodan. Definirajmo polje

$$\mathbb{E}_n^- := \mathbb{Q}(\sqrt{-n}) \overset{\text{tv.}}{=} \{a + b\sqrt{-n} \mid a, b \in \mathbb{Q}\}.$$

Ovdje je $\mathbb{E}_n^- := \mathbb{Q}(\sqrt{-n})$ i tvrdimo da je $\mathbb{E}_n^- = \mathbb{F}_n^- := \{a + b\sqrt{-n} \mid a, b \in \mathbb{Q}\}$. Analogno kao i u (1) vidi se da je $\mathbb{F}_n^-$ doista polje. Isti argument kao i prije daje $\mathbb{E}_n^- = \mathbb{F}_n^-$.

Sada je, jasno,

$$\mathbb{C} \mid \mathbb{E}_n \mid \mathbb{Q}.$$

(3) Uzmimo ponovo $\mathbb{L} = \mathbb{R}$ i $\mathbb{K} = \mathbb{Q}$, ali sada $a = \pi$. (Podsjetimo se da je broj π transcendentan; taj fundamentalan i netrivijalan rezultat, koji je dokazao Lindemann, bio je jedan od najvećih uspjeha matematike 19. stoljeća. Inače, kažemo da je $\alpha \in \mathbb{C}$ *algebarski broj* ako postoji neki nenul polinom $f(X) \in \mathbb{Q}[X]$ takav da je $f(\alpha) = 0$; tj., α je algebarski ako je on nultočka nekog nenul polinoma sa racionalnim koeficijentima. Ako je pak $\tau \in \mathbb{C}$ broj takav da ne postoji nenul polinom sa racionalnim koeficijentima čija je τ nultočka, onda kažemo da je broj τ *transcendentan*.) Definirajmo polje

$$\mathbb{E} := \mathbb{Q}(\pi) \overset{\text{tv.}}{=} \Big\{\frac{f(\pi)}{g(\pi)} \mid f\ g \in \mathbb{Q}[X] \ \ \&\ \ g \neq 0\Big\}.$$

Zadatak 73. Dokažite da se gore definirana polja $\mathbb{E}_n^- := \mathbb{Q}(\sqrt{-n})$ ne mogu monomorfno "uroniti" u $\mathbb{R}$. Preciznije rečeno, dokažite da ne postoji homomorfizam $\varphi : \mathbb{Q}(\sqrt{-n}) \to \mathbb{R}$. (*Uputa:* Najprije, kao što znamo, svaki homomorfizam iz nekog polja u neki prsten je nužno monomorfizam; vidi dolje. Sada, kad bi takav φ postojao, onda bi moralo biti $\varphi(m) = m$ za svaki $m \in \mathbb{Z}$, i onda $\varphi(q) = q$ za svaki $q \in \mathbb{Q}$. Dalje, bilo bi $\varphi(\sqrt{-n}) = r$, za neki $r \in \mathbb{R}$. Ali, onda,

$$-n = \varphi(-n) = \varphi(\sqrt{-n}\,\sqrt{-n}) = \varphi(\sqrt{-n})\varphi(\sqrt{-n}) = r^2;$$

što je nemoguće.)

Podsjetimo se da smo dokazali sljedeći rezultat; to je bila Propozicija 6.20

Propozicija. *Neka je A komutativan prsten. Sljedeće su tvrdnje međusobno ekvivalentne.*

(a) *A je polje.*
(b) $\operatorname{Id} A = \{(0), A\}$.
(c) *Ako je B bilo koji (komutativan) prsten i $\varphi : A \to B$ bilo koji homomorfizam, onda je φ monomorfizam. (Tojest, svaki homomorfizam iz polja u prsten je nužno injekcija!)*

Zadatak 74. Neka je R (nekomut.) prsten s 1 takav da je $\operatorname{Id} R = \{(0), R\}$; tj., R je *prost prsten.* Da li je R nužno tijelo?

Sada ćemo dokazati ovaj najavljeni rezultat (vidi $(\boldsymbol{II})(2)$ u Primjeru 5.9).

Propozicija 10.5. *Konačna integralna domena je tijelo.*

Dokaz. Neka je R neka konačna integralna domena i neka je element $a \in R \setminus \{0\}$ proizvoljan. Definirajmo preslikavanja

$$\lambda_a, \rho_a : R \to R, \qquad \lambda_a(x) := a\,x, \quad \text{i} \quad \rho_a(x) := x\,a.$$

Jasno je da su oba ta preslikavanja bijekcije; naime, to su očito injekcije koje idu iz *konačnog* skupa R u njega samog. Onda posebno slijedi da se po tim preslikavanjima "pogodi" i jedinica 1; tj., postoje neki a_1 i a_2 takvi da je $\lambda_a(a_1) = a\,a_1 = 1$ i $\rho_a(a_2) = a_2\,a = 1$. No posljednje jednakosti govore da element a ima i lijevi i desni inverz, s obzirom na množenje; jasno, onda je $a_1 = a_2$ (jedinstven) inverz od a. Dakle, pokazali smo da je a invertibilan. Zbog proizvoljnosti izbora od a, slijedi da je R tijelo. □

Navedimo bez dokaza ovaj važan i netrivijalan rezultat, koji postrožuje prethodnu propoziciju; i njega smo spomenuli u Primjeru 5.9.

Teorem. (Wedderburn) *Konačna integralna domena je polje; tj., u integralnoj domeni 'konačnost povlači komutativnost'.*

U prvom odjeljku spomenuli smo kvaternione, kao primjere tijela koja nisu komutativna. Kvaternionima se bavimo u Pododjeljku 10.2.

Sada ćemo se sasvim kratko osvrnuti na morfizme među poljima. Najprije, podsjetimo se da je $f : \mathbb{K} \to \mathbb{L}$ homomorfizam polja ako je to homomorfizam prstena; naglasimo kako uvijek uzimamo da je $f(1) = 1$. Nadalje, po gore navedenoj Propoziciji 6.20, slijedi da je jezgra $\mathrm{Ker}\, f$ nekog homomorfizma među poljima nužno nulideal. No to onda znači da je f nužno injektivan; tj., f je monomorfizam. Dakle, homomorfizmi među poljima su uvijek i monomorfizmi; budući to znači da se za f kao gore polje $\mathbb{K}$ može injektivno preslikati, tj. "uložiti", u polje $\mathbb{L}$, uobičajeno je homomorfizme među poljima zvati i **ulaganja**.

Navedimo ovdje još jedan važan prateći objekt svakog polja, odnosno svakog proširenja polja. Najprije, ako je $\mathbb{K}$ polje, definirajmo

$$\mathrm{Aut}\,\mathbb{K} = \text{skup svih automorfizama polja } \mathbb{K}.$$

Jasno je da je taj skup, s obzirom na operaciju komponiranja, grupa; ta se grupa zove **grupa automorfizama** od $\mathbb{K}$. Nadalje, ako je $\mathbb{L} \mid \mathbb{K}$ neko proširenje polja, definirajmo skup

$$\mathrm{Aut}_{\mathbb{K}}\,\mathbb{L} := \text{skup svih automorfizama polja } \mathbb{L} \text{ koji fiksiraju polje } \mathbb{K};$$

precizno rečeno, taj skup sastoji se od onih automorfizama $f \in \mathrm{Aut}\,\mathbb{L}$, takvih da je $f(k) = k$ za *svaki* $k \in \mathbb{K}$. Jasno je da je i taj skup grupa; jasno, ponovo za operaciju kompozicije.

Zadatak 75. Dokažite da su polja $\mathbb{Q}$, $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\imath)$ i $\mathbb{Q}(\pi)$ međusobno neizomorfna. Štoviše, nema ulaganja među poljima $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\imath)$ i $\mathbb{Q}(\pi)$.

Karakteristika polja

Podsjetimo se još jednom na sljedeću jednostavnu činjenicu; to je specijalan slučaj gornje propozicije.

Lema 10.6. *Prsten $\mathbb{Z}/n\mathbb{Z}$ je polje akko je n prim broj.*

Sada definirajmo još jedan osnovni pojam.

Definicija 10.7. Polje je **prosto polje** ako ne sadrži niti jedno pravo potpolje.

Primjer 10.8. Polja $\mathbb{Q}$ i $\mathbb{Z}/p\mathbb{Z}$, za $p \in \mathbb{N}$ prim broj, su prosta polja.

(Naime, kad bi $\mathbb{K}$ bilo potpolje od $\mathbb{Q}$, onda iz $1 \in \mathbb{K}$ slijedi $1 + 1 = 2 \in \mathbb{K}$, $1 + 2 = 3 \in \mathbb{K}, \ldots$; tj., $\mathbb{N} \subseteq \mathbb{K}$. Jasno, isto tako, $1 \in \mathbb{K}$ povlači $-1 \in \mathbb{K}$, a onda i $-\mathbb{N} \subseteq \mathbb{K}$. Znači, $\mathbb{Z} \subseteq \mathbb{K}$. No onda, jer je $\mathbb{K}$ polje, i razlomci $a/b \in \mathbb{K}$, za $a, b \in \mathbb{Z}$ i $b \neq 0$. Znači, $\mathbb{Q} \subseteq \mathbb{K}$; tj., $\mathbb{Q} = \mathbb{K}$.

Za $\mathbb{Z}/p\mathbb{Z}$ je isto jasno da nema pravo potpolje.)

Sljedeći rezultat, između ostalog, govori da su zapravo $\mathbb{Q}$ i $\mathbb{Z}/p\mathbb{Z}$, do na izomorfizam, jedina prosta polja.

Teorem 10.9. *U svakom polju $\mathbb{K}$ sadržano je* jedinstveno *prosto potpolje $\mathbb{K}_0$. Nadalje, imamo točno jednu od sljedeće dvije mogućnosti: ili je*

$$\mathbb{K}_0 \cong \mathbb{Q}, \qquad \textit{i tada} \quad \mathrm{char}\,\mathbb{K} = 0;$$

ili je

$$\mathbb{K}_0 \cong \mathbb{Z}/p\mathbb{Z}, \qquad \textit{i tada} \quad \mathrm{char}\,\mathbb{K} = p \qquad (p \textit{ prim broj}).$$

Dokaz. Definirajmo

$$\mathbb{K}_0 := \text{presjek svih potpolja od } \mathbb{K}.$$

Jasno (v. Napomenu 10.2): $\mathbb{K}_0$ je potpolje od $\mathbb{K}$, prosto je, i jedinstveno je takvo. Sada definiramo preslikavanje

$$\varphi : \mathbb{Z} \to \mathbb{K}, \qquad z \mapsto z\,1.$$

Očito je φ homomorfizam prstena s jedinicom. Imamo dvije mogućnosti.

Slučaj 1. φ nije injekcija.
Sada, za jezgru $\operatorname{Ker}\varphi$ i sliku $\operatorname{Im}\varphi$, po Prvom teoremu o izomorfizmu, imamo

$$\mathbb{Z}/\operatorname{Ker}\varphi \cong \operatorname{Im}\varphi \subseteq \mathbb{K};$$

posebno, $\mathbb{Z}/\operatorname{Ker}\varphi$ je integralna domena. (Naime, $\mathbb{K}$ je polje, pa specijalno i domena, a $\mathbb{Z}/\operatorname{Ker}\varphi \cong \operatorname{Im}\varphi$ je potprsten od $\mathbb{K}$!) Kako je $\mathbb{Z}$ PGI, onda je $\operatorname{Ker}\varphi = p\mathbb{Z}$, za neki $p \in \mathbb{N}$. Znači, $\mathbb{Z}/p\mathbb{Z}$ je domena, a onda je jasno da je p prim broj. Dakle je $\mathbb{K}_0 \cong \mathbb{Z}/p\mathbb{Z}$.

Pokažimo:

$$\operatorname{char}\mathbb{K} = p.$$

Doista, za $1 = 1_{\mathbb{K}} \in \mathbb{K}_0 \subseteq \mathbb{K}$ je $p\,1 = 1 + \cdots + 1 = 0$ (p puta po 1). Sada, za proizvoljan $x \in \mathbb{K}$ je

$$p\,x = x\,1 + \cdots + x\,1 = x(1 + \cdots + 1) = x(p\,1) = x\,0 = 0.$$

Slučaj 2. φ injekcija.
Ako je φ injekcija, onda je

$$\phi : \mathbb{Q} \to \mathbb{K}, \qquad \phi(a/b) := \varphi(a)/\varphi(b),$$

također injektivni homomorfizam prstena; to se odmah vidi. Slijedi da je jezgra $\operatorname{Ker}\phi = (0)$, i onda $\mathbb{Q} \cong \operatorname{Im}\phi \subseteq \mathbb{K}$. Slijedi: $\mathbb{K}_0 \cong \mathbb{Q}$, i sada $\operatorname{char}\mathbb{K} = 0$. □

Algebarska proširenja polja

Ako imamo proširenje polja $\mathbb{L}/\mathbb{K}$, onda možemo gledati $\mathbb{L}$ kao vektorski prostor nad $\mathbb{K}$. Označimo

$$[\mathbb{L} : \mathbb{K}] := \dim_{\mathbb{K}} \mathbb{L}.$$

Definicija 10.10. Kažemo da je $\mathbb{L}/\mathbb{K}$ **konačno proširenje** ako je $[\mathbb{L} : \mathbb{K}] < \infty$.

Primjer 10.11. Kažemo da je polje $\mathbb{K}$ **kvadratno proširenje** od $\mathbb{Q}$, ili **kvadratno polje**, ako je $[\mathbb{K} : \mathbb{Q}] = 2$ (više o kvadratnim poljima vidite u [A. Dujella, *Uvod u teoriju brojeva*, Pogl. 8]. Lako se može pokazati da za takav $\mathbb{K}$ imamo

$$\mathbb{K} \cong \mathbb{Q}(\sqrt{n}) = \{a + b\sqrt{n} \mid a, b \in \mathbb{Q}\},$$

gdje je $\pm 1, 0 \neq n \in \mathbb{N}$ kvadratno slobodan. (Pokažite to, i napravite Zadatak 41!)

Zadatak 76. Označimo (v. Propoziciju 9.4):

$$\omega := -1/2 + \imath\sqrt{3}/2$$

(i) Pokažite da je $\mathbb{Q}(\omega)$ kvadratno polje, i nađite n takav da je $\mathbb{Q}(\omega) = \mathbb{Q}(\sqrt{n})$ (*Uputa:* $n = -3$.)

(ii) Izračunajte $[\mathbb{Q}(\sqrt[3]{5}, \omega) : \mathbb{Q}]$. (*Uputa:* Nađite bazu od $\mathbb{K} := \mathbb{Q}(\sqrt[3]{5}, \omega)$, kao $\mathbb{Q}$-vektorskog prostora.)

Zadatak 77. Označimo:

$$\vartheta := \sqrt{2} + \sqrt{3}$$

(i) Dokažite da je

$$\mathbb{Q}(\vartheta) = \{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} \mid a, b, c, d \in \mathbb{Q}\};$$

i onda $[\mathbb{Q}(\vartheta) : \mathbb{Q}] = 4$. (*Uputa:* Pokažite da su $1, \sqrt{2}, \sqrt{3}, \sqrt{6}$ $\mathbb{Q}$-linearno nezavisni.)

(ii) Opišite sva ulaganja među poljima: $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{6})$, $\mathbb{Q}(\vartheta)$ i $\mathbb{Q}(\pi)$.

Ponovo, neka je $\mathbb{L}/\mathbb{K}$ neko proširenje polja.

Definicija 10.12. Kažemo da je $\alpha \in \mathbb{L}$ **algebarski nad** $\mathbb{K}$, ako postoji polinom $0 \neq F \in \mathbb{K}[X]$ takav da je

$$F(\alpha) = 0 \qquad \text{(tj., } \alpha \text{ je nultočka od } F);$$

inače, kažemo da je α **transcendentan nad** $\mathbb{K}$.

Primjer 10.13. Neka je $\mathbb{L}/\mathbb{K} = \mathbb{R}/\mathbb{Q}$. Tada su npr. brojevi

$$\sqrt{p} \text{ za } p \text{ prim broj}, \quad \sqrt[7]{5}, \quad -\sqrt[19]{3}, \quad \sqrt[99]{1+\sqrt{6}}, \ldots$$

algebarski brojevi, nad $\mathbb{Q}$; dok su npr.

$$e, \quad \pi, \quad 2^{\sqrt{2}}, \ldots$$

transcendentni, nad $\mathbb{Q}$.

Definicija 10.14. Kažemo da je proširenje $\mathbb{L}/\mathbb{K}$ **algebarsko** (nad $\mathbb{K}$), ako je svaki $\alpha \in \mathbb{L}$ algebarski, nad $\mathbb{K}$. Općenito, ako imamo proširenje $\mathbb{L}/\mathbb{K}$, onda je

$$\mathbb{E} := \{\alpha \in \mathbb{L} \mid \alpha \text{ algebarski nad } \mathbb{K}\}$$

polje; tzv. **algebarsko zatvorenje** od $\mathbb{K}$ u $\mathbb{L}$.

Napomena 10.15. Kao ilustraciju za gore uvedeni pojam algebarskog zatvorenja, mogli bismo gledati algebarsko zatvorenje od $\mathbb{Q}$ u $\mathbb{R}$. Ali naglasimo da je to novo dobiveno polje zapravo vrlo kompliciran objekt.

Uvedimo još jedan osnovni pojam u Teoriji polja.

Definicija 10.16. Kažemo da je polje $\mathbb{K}$ **algebarski zatvoreno**, ako svaki nekonstantan polinom iz $\mathbb{K}[X]$ ima bar jednu nultočku u $\mathbb{K}$. (Lako se vidi da su onda sve nultočke, bilo kojeg nekonstantnog polinoma, iz $\mathbb{K}$.)

Bez dokaza navodimo ovaj važan, netrivijalan, teorem.

Teorem 10.17. *Za svako polje $\mathbb{K}$ postoji algebarsko proširenje $\mathbb{L}/\mathbb{K}$ takvo da je $\mathbb{L}$ algebarski zatvoreno polje. Nadalje, ako su $\mathbb{L}_1$ i $\mathbb{L}_2$ dva algebarska proširenja od $\mathbb{K}$, i oba su algebarski zatvorena, onda postoji izomorfizam polja $\sigma : \mathbb{L}_1 \to \mathbb{L}_2$ nad $\mathbb{K}$ (tj., $\sigma_{|\mathbb{K}} = 1_{\mathbb{K}}$).*

Polje $\mathbb{L}$ iz prethodnog teorema (koje je, do na izomorfizam, jedinstveno) zovemo **algebarski zatvarač** od $\mathbb{K}$, i označavamo sa $\overline{\mathbb{K}}$; tj.,

$$\overline{\mathbb{K}} := \text{algebarski zatvarač od } \mathbb{K}.$$

Naprimjer, $\overline{\mathbb{R}} = \mathbb{C}$.

10.2. Kvaternioni.

Neka je $\mathbb{F}$ neko polje karakteristike $\operatorname{char}\mathbb{F} \neq 2$, sa jedinicom $1 = 1_{\mathbb{F}}$, te neka su dani elementi $a, b \in \mathbb{F}^{\times}$. Definirajmo 4-dimenzionalan $\mathbb{F}$-vektorski prostor $\mathbb{K}$, čija je baza

$$\{1, \boldsymbol{i}, \boldsymbol{j}, \boldsymbol{k}\};$$

tj.,

$$\mathbb{K} := \mathbb{F} + \mathbb{F}\boldsymbol{i} + \mathbb{F}\boldsymbol{j} + \mathbb{F}\boldsymbol{k}.$$

Nadalje definirajmo $\mathbb{F}$-bilinearno množenje na $\mathbb{K}$ tako da vrijedi:

(1) 1 je jedinica od $\mathbb{K}$;
(2) $\boldsymbol{i}^2 = a$, $\boldsymbol{j}^2 = b$ i $\boldsymbol{ij} = -\boldsymbol{ji} = \boldsymbol{k}$;
(3) Množenje je asocijativno.

Zadatak 1. Dokažite da vrijedi sljedeće:

$$\boldsymbol{k}^2 = -ab, \qquad \boldsymbol{ik} = -\boldsymbol{ki} = a\boldsymbol{j}, \qquad \boldsymbol{jk} = -\boldsymbol{kj} = -b\boldsymbol{i}.$$

Sada je jasno da je $\mathbb{K}$ primjer prstena s jedinicom.

Definicija 10.18. Skup $\mathbb{K}$, uz gore definirano bilinearno množenje, označava se sa

$$\mathbb{K} = \left(\frac{a, b}{\mathbb{F}}\right),$$

i zove **prsten (generaliziranih) kvaterniona** nad $\mathbb{F}$. Elementi toga skupa zovu se **(generalizirani) kvaternioni**.

Sljedeća jednostavna lema, koju navodimo bez dokaza, daje prve daljnje infomacije o dobivenim prstenima.

Lema 10.19.
(i) *Centar $\mathcal{Z}(\mathbb{K}) = \mathbb{F}$.*
(ii) *Prsten $\mathbb{K}$ nema pravih ideala; tj., to je prost prsten.*

Sasvim je jasno da možemo pisati

$$\mathbb{K} = \mathbb{F} \oplus \mathbb{K}_+;$$

ovo je direktna suma $\mathbb{F}$-vektorskih prostora.

Definicija 10.20. Elementi iz $\mathbb{K}_+$ zovu se **čisti kvaternioni**; tj., *čisti generalizirani kvaternioni.*

Ako u skladu s gornjom dekompozicijom $\mathbb{K} = \mathbb{F} \oplus \mathbb{K}_+$, pišemo element $x \in \mathbb{K}$ kao

$$x = c_0 + z, \qquad c_0 \in \mathbb{F}, \;\; z \in \mathbb{K}_+,$$

onda definiramo **konjugirani** kvaternion

$$x^* := c_0 - z.$$

Sljedeći zadatak govori o nekim jednostavnim pravilima za konjugiranje kvaterniona.

Zadatak 2. Za kvaternione $x, y \in \mathbb{K}$, i $d \in \mathbb{F}$, vrijede sljedeće jednakosti:
(i) $(x + y)^* = x^* + y^*$;
(ii) $(xy)^* = y^* x^*$;
(iii) $x^{**} = x$;
(iv) $d^* = d$.

Za daljnje potrebe definiramo još jedan važan pojam.

Definicija 10.21. Za element $x \in \mathbb{K}$ definiramo **normu** od x kao

$$\nu(x) := xx^*.$$

Primjetimo da ako napišemo $x = c_0 + c_1\boldsymbol{i} + c_2\boldsymbol{j} + c_3\boldsymbol{k}$, onda je

$$\nu(x) = c_0^2 - ac_1^2 - bc_2^2 - abc_3^2.$$

Odavde posebno slijedi da je $\nu(x) \in \mathbb{F}$; tj.,

$$\nu : \mathbb{K} \to \mathbb{F}.$$

Isto tako, imamo

$$\nu(x) = \nu(x^*) = x^* x.$$

Ovaj jednostavni zadatak govori o još nekim važnim svojstvima norme. (*Uputa:* Za (i) napišite $\nu(xy)$, koristeći prethodne jednakosti, te uzmite u obzir tvrdnju (i) gornje Leme. Dio (ii) je očit.)

Zadatak 3. Za kvaternione $x, y \in \mathbb{K}$, i $d \in \mathbb{F}$, vrijede sljedeće jednakosti:
(i) $\nu(xy) = \nu(x)\nu(y)$,
(ii) $\nu(d) = d^2$.

Sljedeć korisna propozicija karakterizira one prstene generaliziranih kvaterniona koji su štoviše tijela. Dokaz ćemo ispustiti.

Propozicija 10.22. *Neka je $\mathbb{K}$ prsten generaliziranih kvaterniona, kao gore. Tada su međusobno ekvivalentne sljedeće tvrdnje:*
(a) *$\mathbb{K}$ je tijelo; tj., svaki $0 \neq x \in \mathbb{K}$ je invertibilan.*
(b) *$\nu(x) \neq 0$, za svaki $0 \neq x \in \mathbb{K}$.*
(c) *Ako trojka $(c_0, c_1, c_2) \in \mathbb{F}^3$ zadovoljava uvjet $c_0^2 = ac_1^2 + bc_2^2$, onda je*

$$c_0 = c_1 = c_2 = 0.$$

Gornja propozicija ima kao direktnu posljedicu sljedeći fundamentalan korolar. (Zašto?) No prije samog korolara, jedna definicija.

Definicija 10.23. Neka je $\mathbb{F} = \mathbb{R}$, te izaberimo $a = b = -1$. Prsten

$$\mathbb{H} := \left(\frac{-1, -1}{\mathbb{R}}\right)$$

zovemo prsten **Hamiltonovih kvaterniona**.

Korolar 10.24. *Prsten Hamiltonovih kvaterniona je štoviše tijelo; tako govorimo o* **tijelu Hamiltonovih kvaterniona**.

Napomena 10.25. Može se pokazati da su, do na izomorfizam, jedini prsteni kvaterniona nad $\mathbb{R}$ gore definirani Hamiltonovi kvaternioni $\mathbb{H}$, i prsten kvaterniona

$$\mathbb{M} := \left(\frac{1, 1}{\mathbb{R}}\right).$$

Nadalje, prema zadatku koji slijedi, imamo da je

$$\mathbb{M} \cong M_2(\mathbb{R}),$$

prsten 2-puta-2 realnih matrica. Jasno, $\mathbb{M}$ nije tijelo.

Zadatak 4. Neka je $\mathbb{F}$ polje, $\operatorname{char} \mathbb{F} \neq 2$, i neka je $a \in \mathbb{F}^{\times}$ proizvoljan. Tada je

$$\left(\frac{a, 1}{\mathbb{F}}\right) \cong M_2(\mathbb{F}),$$

(*Uputa:* Definirajte elemente

$$\varepsilon_{11} := \frac{1 - \boldsymbol{j}}{2}, \qquad \varepsilon_{22} := \frac{1 + \boldsymbol{j}}{2}, \qquad \varepsilon_{12} := \frac{\boldsymbol{i} + \boldsymbol{k}}{2}, \qquad \varepsilon_{21} := \frac{\boldsymbol{i} - \boldsymbol{k}}{2a}.$$

Zatim napravite "tablicu množenja" za te elemente; onda ćete lako definirati željeni izomorfizam.)

Sljedeća propozicija posebno pokazuje da kvaternionskih tijela, do na izomorfizam, ima beskonačno mnogo. (Tu, jasno, koristimo dobro poznatu činjenicu iz elementarne Teorije brojeva koja govori da p-ova, kao u propoziciji, ima beskonačno mnogo.) I dokaz ove propozicije ćemo ispustiti.

Propozicija 10.26. *Ako je $p \in \mathbb{N}$ prim broj takav da je $p \equiv 3 \pmod 4$, tada je prsten kvaterniona*

$$\mathbb{T}_p := \left(\frac{-1, p}{\mathbb{Q}}\right)$$

tijelo. Nadalje, ako su p i q dva međusobno različita prim broja, koji su oba kongruentni 3 modulo 4, onda su kvaternionska tijela $\mathbb{T}_p$ i $\mathbb{T}_q$ međusobno neizomorfna.

To be continued!!!