Matej Brešar

UVOD V ALGEBRO

DMFA – založništvo
Ljubljana 2018

CIP – Kataložni zapis o publikaciji
Narodna in univerzitetna knjižnica, Ljubljana

Prostor za CIP.

Predgovor

Knjiga je nastala iz mojih predavanj pri predmetu *Algebra 2* za študente drugega letnika matematike na Fakulteti za matematiko in fiziko Univerze v Ljubljani. V prvi vrsti naj bi tako služila kot učbenik pri tem in morda še sorodnih predmetih na slovenskih univerzah. Nekateri deli pa bi lahko bili zanimivi tudi za širše občinstvo.

Besedo *algebra* uporabljamo v različnih pomenih. V srednji šoli se srečamo z elementarno algebro, na začetku študija matematike pa z linearno algebro. Algebri, ki jo obravnava ta knjiga, bolj natančno pravimo *abstraktna algebra*. In res je abstraktna. Algebraične pojme si sicer znamo predstaviti s konkretnimi zgledi in kmalu se navadimo z njimi tudi rokovati. Toda kaj je njihov smisel? Čemu služijo? Tovrstna vprašanja začetnika pogosto begajo. Osnovne definicije so tako splošne, da si je najprej težko predstavljati, kako bi lahko koristile. Toda dejstvo je, da so algebraične metode izjemno učinkovito orodje za reševanje najrazličnejših matematičnih problemov. Preden jih lahko pričnemo uporabljati, pa jih moramo dobro razumeti – in to terja svoj čas. Z nekaj primeri uporabe se bomo seznanili tudi v tej knjigi, toda šele v zadnjih poglavjih. Algebro razumemo, ko uzremo celotno sliko: vpeljava vrste abstraktnih pojmov in njihova elementarna obravnava zlagoma vodita do rešitev zahtevnih konkretnih problemov. Dokazi so pogosto kratki in v svojem bistvu enostavni. Računanja je malo, nadomesti ga preplet dozdevno preprostih idej. Algebra je čudovito lepa.

Študenti matematike po vsem svetu se slej ko prej seznanijo z osnovami algebre. Nabor tem, ki sodijo v uvodni tečaj, je po nepisanih pravilih bolj ali manj določen. V tem pogledu ta knjiga ni nobena izjema. Kljub temu se od standardnih učbenikov precej razlikuje. Drugačna je razvrstitev tem po poglavjih. Ne gre le za vrstni red, po katerem so teme obravnavane; drugačna organizacija knjige bralcu podaja tudi nekoliko drugačno sliko o osnovnih algebraičnih pojmih. V standardnih učbenikih sta teorija grup in teorija kolobarjev, dve osnovni področji algebre, obravnavani ločeno. Vendar obe teoriji temeljita na istih idejah. Razlikujeta se okvirja, vsebini pa sta si podobni. To sicer velja le za osnovna poglavja, kmalu se teoriji odlepita druga od druge. Zakaj ne bi teh osnov o grupah in kolobarjih (ter drugih algebrskih strukturah) spoznavali hkrati in s tem bolj jasno poudarili ključne ideje, na katerih

algebra sloni? To vprašanje sem si zastavljal skozi leta, ko sem pri predavanjih sledil tradicionalni delitvi tem. V študijskem letu 2015/16 sem naposled prvič, takrat še poskusno, snov podal na način, kot je zdaj predstavljena v knjigi. Izšlo se je dobro: glavne ideje so res prišle bolj do izraza in na izpitih sem imel občutek, da jih študenti razumejo bolje in znajo povezovati. To me je vzpodbudilo k pisanju te knjige.

Knjiga ima sedem poglavij. Prvo je namenjeno vpeljavi osnovnih pojmov. Podanih je nekaj primerov, a le toliko, da si je abstraktne pojme laže predstavljati. Zato pa je drugo poglavje posvečeno izključno primerom. Tretje poglavje obravnava homomorfizme, četrto pa kvocientne strukture. Nestandarden pristop, pri katerem se različne algebrske strukture (grupe, kolobarji itd.) obravnava hkrati ali pa v zaporednih razdelkih, je značilen za ta štiri poglavja. Zadnja tri poglavja so bolj tradicionalna. Peto obravnava končne grupe, šesto deljivost v komutativnih kolobarjih, sedmo pa razširitve polj v povezavi z ničlami polinomov.

Prva štiri poglavja so namenjena učenju jezika algebre. Ta jezik morajo poznati vsi matematiki, tudi tisti, ki pri svojem delu le redko pridejo v stik z globljimi algebraičnimi rezultati. Matematična spoznanja je namreč pogosto najlaže opisati prav v jeziku algebre, zato ga potrebujejo za sporazumevanje z drugimi matematiki. Ta poglavja so tako s praktičnega vidika bistveni del knjige. Vendar v njih le malo izvemo o pomenu in globini algebre. Matematično so razmeroma nezahtevna. Veliko rezultatov je skoraj očitnih. Nekateri bralci bodo njihove dokaze uspeli poiskati sami in jih šele zatem primerjali z zapisanimi, kar je gotovo najbolj učinkovit in tudi najbolj kratkočasen način študija. Z matematičnega vidika so zadnja tri poglavja veliko bolj vznemirljiva. Dokazi postanejo zanimivi in izreki presenetljivi. Občuti se moč abstraktnega načina razmišljanja. Šele tu razumemo smisel vpeljave algebraičnega jezika iz prvega dela knjige.

Vsak razdelek se zaključi z nalogami. Poskušal sem jih urediti tako, da od lažjih prehajajo k težjim. Ker pa so združene tudi po tematskih sklopih, se tega nisem mogel držati povsem dosledno. V vsakem primeru pa priporočam, da se naloge rešujejo v danem vrstnem redu. Rešitve nekaterih se namreč lahko uporabijo pri reševanju naslednjih.

Za razumevanje knjige je potrebno poznavanje osnovnih številskih množic (vključno s kompleksnimi števili) in elementarna teorija množic. S slednjim imam v mislih predvsem operacije z množicami, osnovne pojme v zvezi s preslikavami med množicami in pojem ekvivalenčne relacije. Oznake, ki jih v zvezi s števili in množicami uporabljam, so tako standardne, da se mi jih ni zdelo potrebno pojasnjevati. Nekaj primerov: $\mathbb{N}$ označuje množico naravnih števil (brez 0), $\emptyset$ prazno množico, $|A|$ kardinalno število množice A, $A \times B$ kartezični produkt množic A in B, $f : A \to B$ preslikavo iz A v B, $x \mapsto f(x)$ preslikavo, ki element x preslika v $f(x)$ itd.

Predpostavlja se tudi predznanje osnov linearne algebre. Kljub temu so v knjigi, resda na zgoščen način, vključene vse potrebne podrobnosti v zvezi z vektorskimi prostori, matrikami in linearnimi preslikavami. Želel sem namreč opozoriti na vlogo temeljnih pojmov linearne algebre v okviru abstraktne algebre.

Kolegoma Petru Šemrlu in Igorju Klepu sem hvaležen za dragocene pogovore o konceptu knjige in koristne pripombe. Imel sem srečo, da je zadnji dve leti vaje pri Algebri 2 vodil Klemen Šivic. Osnutek knjige je skrbno prebral in odkril več napak ter predlagal razne izboljšave. V posebno veselje mi je, da se lahko zahvalim tudi številnim študentkam in študentom, ki so me opozorili na različne napake, od tipkarskih do sicer drobnih, a zato toliko težje izsledljivih matematičnih spodrsljajev.

Junij 2018 *Matej Brešar*

Kazalo

POGLAVJE 1

Osnovne algebrske strukture

Uvodno poglavje je namenjeno seznanitvi z osnovnimi algebrskimi strukturami. Poleg najosnovnejših – grup, kolobarjev in polj – bomo spoznali tudi polgrupe, monoide, vektorske prostore in algebre. Iz definicij bomo izpeljali nekaj preprostih dejstev, globljih rezultatov pa v tem poglavju ne bo. Primerov bo za vzorec, le toliko, da bodo pomagali razumeti definicije. Celotno poglavje je tako nekakšen slovar temeljnih pojmov algebre. Z njihovim preučevanjem bomo pričeli kasneje.

1.1. Binarne operacije

V algebri obravnavamo množice, opremljene z vsaj eno binarno operacijo.

Definicija 1.1. **Binarna (**ali **dvočlena) operacija** na neprazni množici S je preslikava iz $S \times S$ v S.

Seveda si lahko na množicah izmislimo najrazličnejše binarne operacije, vendar nas praviloma zanimajo tiste, ki se v matematiki naravno pojavljajo.

Primer 1.2. *Seštevanje* na množici celih števil $\mathbb{Z}$, torej preslikava

$$(m, n) \mapsto m + n,$$

je binarna operacija na $\mathbb{Z}$.

Primer 1.3. Tudi *množenje*, torej preslikava

$$(m, n) \mapsto m \cdot n,$$

je binarna operacija na množici $\mathbb{Z}$.

Seštevanje in množenje sta binarni operaciji tudi na marsikateri drugi množici. Cela števila smo izbrali zato, ker nam v algebri pogosto služijo kot osnovni model.

Primer 1.4. Naj $\mathcal{F}(X)$ označuje množico vseh preslikav iz neprazne množice X vase. S predpisom

$$(f, g) \mapsto f \circ g,$$

kjer $\circ$ označuje *kompozitum* preslikav, je definirana binarna operacija na $\mathcal{F}(X)$.

Primeri niso bili izbrani naključno. Seštevanje, množenje in komponiranje so najosnovnejše in tudi najpomembnejše binarne operacije.

V tem in v naslednjem razdelku bomo binarno operacijo na množici S označevali s simbolom $\star$. Torej je $\star$ predpis, ki vsakemu paru elementov x in y iz S priredi element

$$x \star y,$$

ki prav tako pripada množici S. Tako na primer skalarni produkt vektorjev v prostoru $\mathbb{R}^n$ ne definira binarne operacije na $\mathbb{R}^n$, saj je rezultat operacije realno število (skalar) in ne vektor. Vektorski produkt, po drugi strani, pa je binarna operacija na $\mathbb{R}^3$.

Prištevanje števila 0 in množenje s številom 1 imata očitno skupno lastnost; opredelimo jo v splošnem.

Definicija 1.5. Naj bo $\star$ binarna operacija na S. Element $e \in S$ se imenuje **nevtralni element** za $\star$, če za vsak $x \in S$ velja

$$x \star e = e \star x = x.$$

Primer 1.6. Nevtralni element za operacijo seštevanja v $\mathbb{Z}$ je število 0.

Primer 1.7. Nevtralni element za operacijo množenja v $\mathbb{Z}$ je število 1.

Primer 1.8. Nevtralni element za operacijo komponiranja preslikav na množici $\mathcal{F}(X)$ (primer 1.4) je identična preslikava id_X.

Nevtralni element ne obstaja vselej. Na primer, operacija seštevanja na množici *naravnih števil* ga nima, prav tako operacija množenja na množici vseh *sodih* celih števil.

Trditev 1.9. *Če nevtralni element za binarno operacijo na množici obstaja, potem je en sam.*

Dokaz. Denimo, da sta e in f nevtralna elementa za $\star$. Ker je e nevtralni element, je $e \star f = f$. Po drugi strani pa je $e \star f = e$, saj je tudi f nevtralni element. Torej je $e = f$. □

Elementu $e' \in S$, za katerega velja le $e' \star x = x$ za vse $x \in S$, pravimo **levi nevtralni element**. Teh je lahko več.

Primer 1.10. Če definiramo $\star$ s predpisom $x \star y = y$ za vse $x, y \in S$, je vsak element iz S levi nevtralni element.

Podobno definiramo **desni nevtralni element**, torej kot element $e'' \in S$ z lastnostjo $x \star e'' = x$ za vse $x \in S$.

Trditev 1.11. *Če za binarno operacijo $\star$ na S obstajata tako levi nevtralni element e' kot desni nevtralni element e'', potem sta enaka: $e' = e''$.*

Dokaz. Kot v dokazu trditve 1.9 sklepamo, da je $e' = e' \star e'' = e''$. □

Trditev 1.11 je pravzaprav splošnejša od trditve 1.9. Ker pa ima slednja drugačen poudarek, smo zapisali obe.

O splošnih binarnih operacijah je težko povedati veliko zanimivega. Ponavadi zahtevamo, da imajo naše binarne operacije neke lastnosti.

Definicija 1.12. Binarna operacija $\star$ na S je **asociativna**, če za vse $x, y, z \in S$ velja

$$(x \star y) \star z = x \star (y \star z). \tag{1.1}$$

Enakost (1.1) imenujemo **asociativnostni zakon**. Skoraj brez izjeme se bomo ukvarjali le z asociativnimi binarnimi operacijami. Sicer imajo tudi nekatere neasociativne binarne operacije pomembno mesto v matematiki, vendar se običajno ne obravnavajo v uvodnih poglavjih algebre. Vsaj ne sistematično. Na konkretne primere neasociativnih operacij namreč hitro naletimo. Prej omenjeni vektorski produkt na $\mathbb{R}^3$ je že tak.

Definicija 1.13. Naj bo $\star$ binarna operacija na S. Pravimo, da elementa x in y iz S **komutirata**, če velja

$$x \star y = y \star x. \tag{1.2}$$

Če je enakost (1.2) izpolnjena za vse $x, y \in S$, pravimo, da je $\star$ **komutativna** binarna operacija.

Kadar ni dvoma, katero binarno operacijo $\star$ na množici S imamo v mislih, namesto »$\star$ je komutativna« rečemo tudi »S je komutativna«. Podobno rečemo, da je »S asociativna« ipd.

Primer 1.14. Binarni operaciji seštevanje in množenje na $\mathbb{Z}$ sta asociativni in komutativni, binarna operacija odštevanje, torej $(m, n) \mapsto m - n$, pa, kot zlahka preverimo, ni niti asociativna niti komutativna. Odštevanje pravzaprav redkokdaj obravnavamo kot binarno operacijo. Tu nimamo v mislih le odštevanja celih števil, ampak odštevanje elementov v različnih množicah. Seveda se odštevanju ne moremo izogniti, toda vpeljali ga bomo preko seštevanja in pojma nasprotni element (gl. razdelek 1.3). Obravnavamo ga torej kot »izpeljano« in ne »samostojno« operacijo. Podobno velja za deljenje, ki ga lahko obravnavamo kot binarno operacijo na nekaterih množicah (na primer na množici neničelnih realnih števil). Vpeljemo ga preko množenja in pojma inverzni element.

Primer 1.15. Vzemimo $f, g, h \in \mathcal{F}(X)$ (gl. primer 1.4). Za poljuben $x \in X$ je

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

in

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

Preslikavi $(f \circ g) \circ h$ in $f \circ (g \circ h)$ sta torej enaki in operacija $\circ$ je asociativna. Komutativna pa je le tedaj, ko ima X (in s tem tudi $\mathcal{F}(X)$) en sam element. Namreč, če sta a in b različna elementa iz X, potem za konstantni preslikavi $f : x \mapsto a$ in $g : x \mapsto b$ velja $f \circ g = f \neq g = g \circ f$.

Komponiranje preslikav je izredno pomembna binarna operacija. Nekomutativnim operacijam se zato ne bomo tako zlahka odrekli kot neasociativnim.

Naj bo T podmnožica množice S z binarno operacijo $\star$. Denimo, da je za vse $t, t' \in T$ tudi $t \star t' \in T$. V tem primeru rečemo, da je množica T **zaprta za operacijo** $\star$ ali da je $\star$ **notranja operacija** na T. Če $T \neq \emptyset$, je torej tedaj zožitev $\star$ na $T \times T$ binarna operacija na T.

Primer 1.16. Seštevanje in množenje sta notranji operaciji na množici $\mathbb{N}$, odštevanje in deljenje pa nista.

Binarna operacija na množici S je seveda notranja operacija na S. Včasih tako namesto o »binarni operaciji« govorimo o »notranji binarni operaciji«. Res je pridevnik »notranji« s formalnega vidika tu odveč. Lahko pa je koristen že zato, da ne pride do zmešnjave s pojmom **zunanje binarne operacije**. To je preslikava iz $K \times S$ v S, kjer sta K in S različni množici.

Primer 1.17. Množenje vektorjev s skalarji v prostoru $\mathbb{R}^3$ je zunanja binarna operacija. To je preslikava, ki skalarju $\lambda \in \mathbb{R}$ in vektorju

$$\vec{x} = (x_1, x_2, x_3) \in \mathbb{R}^3$$

priredi vektor

$$\lambda\vec{x} = (\lambda x_1, \lambda x_2, \lambda x_3) \in \mathbb{R}^3.$$

Na nekaterih področjih algebre se srečamo tudi z drugačnimi, ne le (notranjimi in zunanjimi) binarnimi operacijami. Toda v tej knjigi se z njimi ne bomo ukvarjali.

Naloge

1. Naj bo S potenčna množica neprazne množice A. Unijo, presek in razliko množic lahko obravnavamo kot binarne operacije na S. Ugotovi, katere izmed njih so asociativne, katere komutativne in katere imajo levi ali desni nevtralni element.
2. Ugotovi, katere izmed naslednjih binarnih operacij na množici $\mathbb{N}$ so asociativne, katere imajo levi ali desni nevtralni element in v katerih lahko med seboj različna elementa komutirata:
   (a) $m * n = m + 2n$.
   (b) $m * n = m^2 n$.
   (c) $m * n = m$.
   (d) $m * n = m^n$.

3. Poišči vse končne neprazne podmnožice množice $\mathbb{Z}$, ki so zaprte za seštevanje.
4. Pokaži, da je podmnožica množice $\mathbb{Z}$, ki je zaprta za odštevanje, zaprta tudi za seštevanje in množenje. S primeroma pokaži, da iz zaprtosti za seštevanje ne sledi zaprtost za množenje in da iz zaprtosti za množenje ne sledi zaprtost za seštevanje. Poišči še nekaj primerov (ali pa kar vse!) podmnožic $\mathbb{Z}$, ki so zaprte za odštevanje.

   Komentar. Kasneje bomo dejstvo, da iz zaprtosti za odštevanje sledi zaprtost za seštevanje, izpeljali za veliko bolj splošne množice.
5. Naj bo S množica z binarno operacijo $\star$. Če sta njeni podmnožici T in T' zaprti za $\star$, potem je očitno taka tudi množica $T \cap T'$. S primerom pokaži, da za množico $T \cup T'$ to v splošnem ne velja.

   Komentar. Primera ne bi smelo biti težko poiskati; če $T \not\subseteq T'$ in $T' \not\subseteq T$, potem vsaj za standardne primere binarnih operacij bolj kot ne le izjemoma velja, da je $T \cup T'$ zaprta za $\star$. Nasploh se algebraične lastnosti praviloma lepo prenašajo na preseke množic, ne pa tudi na unije.
6. Označimo z $\mathcal{I}(X)$ množico vseh injektivnih preslikav iz $\mathcal{F}(X)$ (oznaka je iz primera 1.4), s $\mathcal{S}(X)$ množico vseh surjektivnih preslikav iz $\mathcal{F}(X)$ in z $\mathcal{B}(X)$ množico vseh bijektivnih preslikav iz $\mathcal{F}(X)$.
   (a) Pokaži, da so množice $\mathcal{I}(X)$, $\mathcal{S}(X)$, $\mathcal{B}(X)$, $\mathcal{F}(X) \setminus \mathcal{I}(X)$ in $\mathcal{F}(X) \setminus \mathcal{S}(X)$ zaprte za operacijo $\circ$.
   (b) Pokaži, da je $\mathcal{I}(X) = \mathcal{S}(X) = \mathcal{B}(X)$, če je X končna množica. V tem primeru je zato tudi množica $\mathcal{F}(X) \setminus \mathcal{B}(X)$ zaprta za $\circ$.
   (c) Pokaži, da množica $\mathcal{F}(X) \setminus \mathcal{B}(X)$ ni zaprta za $\circ$, če je X števna neskončna množica.
   (d) Znano je, da vsaka neskončna množica vsebuje števno neskončno podmnožico. S pomočjo tega dejstva pokaži, da množica $\mathcal{F}(X) \setminus \mathcal{B}(X)$ ni zaprta za $\circ$ za poljubno neskončno množico X.

   Komentar. Čeprav zapisana v algebraičnem jeziku, je to pravzaprav naloga iz teorije množic. Z algebraičnega vidika je pomemben predvsem detajl, ki sledi iz (a): $\circ$ je binarna operacija na množici $\mathcal{B}(X)$. Kmalu bomo videli, da je množica $\mathcal{B}(X)$ precej bolj naraven okvir za obravnavo komponiranja kot (»prevelika«) množica $\mathcal{F}(X)$. Oznako $\mathcal{B}(X)$ bomo sicer zamenjali s $\mathrm{Sim}(X)$ (gl. primer 1.36).

1.2. Polgrupe in monoidi

Množice, opremljene z eno ali več (notranjimi ali zunanjimi) binarnimi operacijami, za katere veljajo določene lastnosti (aksiomi), imenujemo **algebrske strukture**. Algebra je študij algebrskih struktur. Osnovni algebrski

strukturi sta grupa in kolobar. Pred definicijo grupe se bomo v tem razdelku seznanili z dvema splošnejšima strukturama.

Definicija 1.18. Neprazna množica S skupaj z asociativno binarno operacijo $\star$ na S se imenuje **polgrupa**.

Polgrupo torej sestavljata tako množica S kot operacija $\star$. Zato jo označujemo kot par

$$(S, \star).$$

Kadar je iz vsebine razvidno, katero operacijo imamo v mislih, smo lahko manj formalni in govorimo kar o polgrupi S. Podoben dogovor velja za druge algebrske strukture.

Primer 1.19. Preprost primer polgrupe je $(\mathbb{N}, +)$, torej množica naravnih števil skupaj z operacijo seštevanja. Seveda so polgrupe tudi $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$ in $(\mathbb{C}, +)$. Vendar so le-te, kot bomo kmalu videli, celo grupe, zato jih običajno ne navajamo kot značilne primere polgrup.

Asociativnost operacije v polgrupi S pomeni, da za poljubne $x_1, x_2, x_3 \in S$ velja

$$(x_1 \star x_2) \star x_3 = x_1 \star (x_2 \star x_3).$$

Zato oklepaje lahko izpustimo in ta element pišemo kot

$$x_1 \star x_2 \star x_3.$$

Ali lahko oklepaje odpravimo tudi, kadar nastopa več elementov? Torej, ali veljajo formule, kot sta na primer

$$(x_1 \star x_2) \star (x_3 \star x_4) = (x_1 \star (x_2 \star x_3)) \star x_4$$

in

$$(x_1 \star x_2) \star ((x_3 \star x_4) \star x_5) = x_1 \star (((x_2 \star x_3) \star x_4) \star x_5)?$$

Z večkratnim upoštevanjem asociativnostnega zakona se ni težko prepričati, da ti formuli res veljata. Seveda ne gre za naključna primera, oklepaje v polgrupi lahko vedno odpravimo. Tega ni težko dokazati, le označevanje povzroča nekaj sitnosti. Zato dokaz podajmo malce manj formalno, kot je v navadi, in tudi natančni formulaciji rezultata se raje izognimo.

Vzemimo $x_1, \ldots, x_n \in S$, $n \geq 2$, in vpeljimo

$$x := x_1 \star (x_2 \star (x_3 \star (\cdots \star x_n))).$$

Naj bo y katerikoli element, ki ga dobimo iz zaporedja elementov $x_1, \ldots, x_n$ (v tem vrstnem redu) z uporabo operacije $\star$; y je torej definiran podobno kot x, le oklepaji so lahko postavljeni drugače. Naš cilj je pokazati, da je $y = x$. Dokažimo to z indukcijo na n. Za $n = 2$ je trditev očitna, zato naj bo $n > 2$. Glede na zadnjo uporabo $\star$ (zadnji oklepaj) lahko y zapišemo kot $y = u \star v$, kjer v zapisu u nastopajo $x_1, \ldots, x_k$ za neki $k < n$, v zapisu v pa $x_{k+1}, \ldots, x_n$.

Po indukcijski predpostavki je $u = x_1 \star z$, kjer je $z = x_2 \star (x_3 \star (\cdots \star x_k))$. Iz asociativnosti $\star$ sledi $y = x_1 \star (z \star v)$. Za izraz $z \star v$ ponovno uporabimo indukcijsko predpostavko in dobimo $y = x$.

V polgrupi zato lahko oklepaje izpuščamo in izraze, kot sta x in y, pišemo v obliki

$$x_1 \star x_2 \star \cdots \star x_n.$$

Na podlagi tega dogovora lahko vpeljemo **potenco** elementa polgrupe S na enak način kot pri številih. Torej, za $x \in S$ in $n \in \mathbb{N}$ naj bo

$$x^n := x \star x \star \cdots \star x,$$

kjer x na desni strani nastopa n-krat. Očitno veljata formuli

$$x^{m+n} = x^m \star x^n \quad \text{in} \quad (x^m)^n = x^{mn}.$$

Poudarimo, da smo potenco x^n lahko nedvoumno definirali zaradi privzetka, da je operacija $\star$ asociativna. Brez tega bi imeli težave že z definicijo x^3, saj bi to lahko pomenilo $(x^2) \star x$ ali $x \star (x^2)$.

Pomembni primeri polgrup pogosto vsebujejo nevtralni element.

Definicija 1.20. Polgrupa z nevtralnim elementom se imenuje **monoid**.

(Nevtralni element je po definiciji hkrati levi in desni nevtralni element; polgrupa, ki ima samo levi ali samo desni nevtralni element, še ni monoid.)

Primer 1.21. Polgrupa $(\mathbb{N}, +)$ nima nevtralnega elementa in zato ni monoid. Monoid dobimo, če naravnim številom dodamo število 0. Torej, $(\mathbb{N} \cup \{0\}, +)$ je monoid z nevtralnim elementom 0. Monoida sta tudi $(\mathbb{N}, \cdot)$ in $(\mathbb{Z}, \cdot)$. Pri obeh je nevtralni element število 1.

Primer 1.22. Množica $\mathcal{F}(X)$ vseh preslikav iz neprazne množice X vase, opremljena z operacijo kompozitum, je monoid z nevtralnim elementom id_X (gl. primera 1.8 in 1.15).

Obstoj nevtralnega elementa omogoča vpeljavo naslednjih pojmov, ki v algebri igrajo izredno pomembne vloge. Še posebej to velja za pojem inverza.

Definicija 1.23. Naj bo $(S, \star)$ monoid z nevtralnim elementom e.

(a) Elementu $\ell \in S$ pravimo **levi inverz** elementa $x \in S$, če je $\ell \star x = e$.
(b) Elementu $d \in S$ pravimo **desni inverz** elementa $x \in S$, če je $x \star d = e$.
(c) Elementu $y \in S$ pravimo **inverz** elementa $x \in S$, če je hkrati njegov levi in desni inverz, torej če velja $y \star x = x \star y = e$. Elementu, ki ima inverz, pravimo **obrnljiv element**.

Vsak monoid ima vsaj en obrnljiv element, namreč nevtralni element, ki je očitno inverz samemu sebi. Lahko se zgodi, da drugih obrnljivih elementov ni. Možna je tudi druga skrajnost, da so obrnljivi prav vsi elementi. Toda o tem bomo spregovorili v naslednjem razdelku, zato se zdaj posvetimo le primerom,

ko to ne velja. V naslednjem primeru bomo obravnavali monoide, v katerih je operacija komutativna. V takih pojmi levi inverz, desni inverz in inverz seveda sovpadajo. Pridevnika »levi« in »desni« zato tedaj izpuščamo.

PRIMER 1.24. Edini obrnljiv element monoida $(\mathbb{N} \cup \{0\}, +)$ je 0, edini obrnljiv element monoida $(\mathbb{N}, \cdot)$ je 1, monoid $(\mathbb{Z}, \cdot)$ pa ima dva obrnljiva elementa: 1 in -1. Oba sta sama sebi inverz. V monoidih $(\mathbb{Q}, \cdot)$, $(\mathbb{R}, \cdot)$ in $(\mathbb{C}, \cdot)$ pa so obrnljivi vsi elementi razen elementa 0.

Oglejmo si še primer, ko je ločitev med levimi in desnimi inverzi potrebna.

PRIMER 1.25. Naj bo f preslikava iz množice X vase, torej element monoida $\mathcal{F}(X)$ (gl. primer 1.22). Če ima f levi inverz, torej če je $g \circ f = \mathrm{id}_X$ za neko preslikavo $g : X \to X$, potem je f injektivna. Iz $f(x) = f(y)$ namreč sledi $g(f(x)) = g(f(y))$ in zato $x = y$. Velja pa tudi obratno: če je f injektivna, potem ima (vsaj en) levi inverz g. Definiramo ga takole. Vzemimo $y \in X$. Če y leži v zalogi vrednosti f, ga lahko zapišemo kot $y = f(x)$ za neki $x \in X$. V tem primeru definiramo $g(y) := x$. Zaradi injektivnosti f je namreč x enolično določen in ta definicija je nedvoumna. Če pa y ne leži v zalogi vrednosti f, lahko $g(y)$ definiramo kakorkoli – v vsakem primeru velja $g \circ f = \mathrm{id}_X$. Če f ni surjektivna, potem taki elementi y res obstajajo in tako ima f več levih inverzov. Povzemimo:

(a) $f \in \mathcal{F}(X)$ ima levi inverz natanko tedaj, ko je f injektivna preslikava. Če f ni tudi surjektivna, ima več levih inverzov.

Slednje pride v poštev le v primeru, ko je množica X neskončna. Če je X končna, je namreč preslikava $f : X \to X$ injektivna natanko tedaj, ko je surjektivna (zakaj?).

Podobno velja:

(b) $f \in \mathcal{F}(X)$ ima desni inverz natanko tedaj, ko je f surjektivna preslikava. Če f ni tudi injektivna, ima več desnih inverzov.

Res, iz obstoja desnega inverza, torej preslikave $h : X \to X$ z lastnostjo $f \circ h = \mathrm{id}_X$, očitno sledi surjektivnost f. Obratno, naj bo f surjektivna in poiščimo njen desni inverz h. Zaradi surjektivnosti za poljuben $y \in X$ obstajajo taki elementi $x \in X$, da je $f(x) = y$. Za vsak y izberimo en tak x in definirajmo $h(y) := x$ (tu smo uporabili aksiom izbire). Potem je h desni inverz f. Če f ni tudi injektivna, je očitno desnih inverzov več.

Tako iz dokaza trditve (a) kot iz dokaza trditve (b) izluščimo še zadnjo trditev, ki jo bralec gotovo pozna iz elementarne teorije množic:

(c) $f \in \mathcal{F}(X)$ ima inverz natanko tedaj, ko je f bijektivna preslikava. Inverz je en sam. (Označujemo ga s f^{-1} in mu pravimo inverzna preslikava preslikave f.)

Nekateri elementi monoida imajo torej lahko več levih inverzov in nekateri več desnih inverzov. Ali imajo v kakem monoidu lahko tudi več inverzov? Odgovor je negativen. Sledil bo iz naslednje trditve, ki pove več kot le to.

TRDITEV 1.26. *Naj bo $(S, \star)$ monoid. Če je $\ell \in S$ levi inverz elementa $x \in S$ in je $d \in S$ desni inverz istega elementa x, potem je $\ell = d$.*

DOKAZ. Element $\ell \star x \star d$ je po eni strani enak

$$(\ell \star x) \star d = e \star d = d$$

in po drugi strani enak

$$\ell \star (x \star d) = \ell \star e = \ell.$$

Torej je $\ell = d$. □

POSLEDICA 1.27. *Če je x obrnljiv element monoida $(S, \star)$, potem iz $x \star y = e$ sledi $y \star x = e$. Podobno, iz $y \star x = e$ sledi $x \star y = e$.*

DOKAZ. Po predpostavki obstaja tak $z \in S$, da je $x \star z = z \star x = e$. Po trditvi 1.26 zato iz kateregakoli izmed pogojev $x \star y = e$ in $y \star x = e$ sledi $y = z$ (in s tem $x \star y = y \star x = e$). □

POSLEDICA 1.28. *Obrnljiv element v monoidu ima natanko en inverz.*

DOKAZ. Če sta y in z inverza x, je y tudi levi inverz x in z desni inverz x. Iz trditve 1.26 sledi $y = z$. □

Inverz obrnljivega elementa x označujemo z x^{-1}. Torej je

$$x \star x^{-1} = x^{-1} \star x = e.$$

Seveda je tudi x^{-1} obrnljiv in velja

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

TRDITEV 1.29. *Če sta x in y obrnljiva elementa monoida $(S, \star)$, je obrnljiv tudi element $x \star y$ in velja $(x \star y)^{-1} = y^{-1} \star x^{-1}$.*

DOKAZ. Preveriti moramo, da je

$$(x \star y) \star (y^{-1} \star x^{-1}) = e \quad \text{in} \quad (y^{-1} \star x^{-1}) \star (x \star y) = e.$$

Oboje postane očitno, če primerno prestavimo oklepaje. Tako je izraz na levi strani prve formule enak

$$x \star (y \star y^{-1}) \star x^{-1} = x \star e \star x^{-1} = x \star x^{-1},$$

kar je seveda enako e. □

Trditev se zlahka posploši na več členov. Če so $x_1, \ldots, x_n$ obrnljivi, je tak tudi $x_1 \star x_2 \star \cdots \star x_n$ in velja

$$(x_1 \star x_2 \star \cdots \star x_n)^{-1} = x_n^{-1} \star \cdots \star x_2^{-1} \star x_1^{-1}.$$

V primeru, ko so vsi x_i med seboj enaki, tako dobimo $(x^n)^{-1} = (x^{-1})^n$ za vsak obrnljiv x in vsak $n \in \mathbb{N}$. Ta element pišemo krajše kot x^{-n}, torej

$$x^{-n} := (x^n)^{-1} = (x^{-1})^n.$$

Če vpeljemo še

$$x^0 := e,$$

smo tako potenco x^n definirali za vsa cela števila n. Formuli

$$x^{m+n} = x^m \star x^n \quad \text{in} \quad (x^m)^n = x^{mn}$$

sta za obrnljiv element x izpolnjeni za vsa *cela*, ne le za naravna števila m in n. Dokaz zahteva nekaj potrpežljivosti, ni pa težek. Prepuščamo ga bralcu.

Trditev 1.30. *Če je x obrnljiv element monoida $(S, \star)$, potem za poljubna $y, z \in S$ iz $x \star y = x \star z$ sledi $y = z$. Podobno, iz $y \star x = z \star x$ sledi $y = z$.*

Dokaz. Iz $x \star y = x \star z$ sledi $x^{-1} \star (x \star y) = x^{-1} \star (x \star z)$. Z upoštevanjem asociativnosti takoj dobimo $y = z$. □

Vrstni red elementov v trditvi je pomemben. Denimo, iz pogoja $x \star y = z \star x$ sledi $y = x^{-1} \star z \star x$. Če z ne komutira z x, ni enak y.

Naloge

1. Pokaži, da je množico $\mathbb{N}$ polgrupa tako za binarno operacijo $m \star n = \max\{m, n\}$ kot za binarno operacijo $m \star n = \min\{m, n\}$. Za katero je monoid?
2. Poišči vse binarne operacije na množici $S = \{e, a\}$, za katere je S polgrupa in je e levi nevtralni element.
3. Pokaži, da je množica $\mathbb{R}$ polgrupa za binarno operacijo $x * y = |x|y$. Ali ima levi ali desni nevtralni element? Za vsak $x \in \mathbb{R}$ poišči vse elemente, ki z x komutirajo.
4. Pokaži, da je množica $\mathbb{Z}$ monoid za binarno operacijo $m*n = m+n+mn$. Poišči vse obrnljive elemente.
5. Pokaži, da v vsakem monoidu z nevtralnim elementom e iz $x \star y \star x = e$ sledi, da sta x in y obrnljiva in je $y = x^{-2}$.
6. Ugotovi, iz katerih izmed naslednjih pogojev sledi, da je element x monoida S obrnljiv:
   (a) Obstaja tak $y \in S$, da je $x \star y$ obrnljiv.
   (b) Obstaja tak $y \in S$, da y komutira z x in je $x \star y$ obrnljiv.
   (c) Obstaja tak $n \in \mathbb{N}$, da je x^n obrnljiv.

7. V monoidu $\mathcal{F}(\mathbb{N})$ poišči element, ki ima levi inverz in nima desnega (gl. primer 1.25). Poišči vsaj dva leva inverza.
8. Pokaži, da je v monoidu s končnim številom elementov levi inverz elementa x vselej tudi desni inverz (in tako inverz) in je oblike x^n za neki $n \in \mathbb{N}$.

   Namig. Množica $\{x^n \mid n \in \mathbb{N}\}$ je končna, zato je $x^k = x^\ell$ za neki različni naravni števili k in ℓ.

1.3. Grupe

Že v imenu polgrupe je namig na nepopolnost. Preidimo na (»prave«) grupe.

Definicija 1.31. Monoid, v katerem je vsak element obrnljiv, se imenuje **grupa**. Grupa, v kateri je operacija komutativna, se imenuje **Abelova grupa**.

Abelovim grupam rečemo tudi **komutativne grupe**. Ime so dobile po norveškem matematiku *Nielsu Henriku Abelu* (1802–1829), ki se je kljub kratkemu življenju v zgodovino zapisal kot eden največjih matematikov. Abel se sicer ni ukvarjal z grupami v modernem pomenu besede, vendar so se nekatere posebne grupe pojavljale v njegovem delu. Samo ime grupa je skoval francoski matematik *Évariste Galois* (1811–1832), ki mu je bilo dano še krajše življenje. Čeprav njegova definicija ni povsem enaka naši, se Galois šteje za utemeljitelja teorije grup. Abela je pokopala bolezen, Galois pa je umrl v dvoboju. Še v noči pred dvobojem naj bi, prepričan v svojo smrt, zapisoval svoj matematični testament. Morda je to predvsem legenda, ki se je spletla okoli nenavadne smrti znamenite osebnosti. Dejstvo pa je, da je bilo Galoisovo delo priznano šele veliko let po njegovi smrti in da so imele genialne ideje mladeniča pri dvajsetih izjemen vpliv na razvoj matematike. Omenimo še, da sta Abel in Galois neke posebne grupe uporabljala le kot orodje pri reševanju problema, povezanega z ničlami polinoma pete stopnje. O tem bomo nekoliko bolj podrobno spregovorili v razdelku 7.1. Nasploh se abstraktni matematični koncepti velikokrat vpeljujejo z namenom rešiti kak konkreten problem. Žal pri poučevanju matematike največkrat nimamo časa za pojasnjevanje ozadja in pojme uvedemo, kot bi bili dani z neba.

Poleg delitve na komutativne (Abelove) in nekomutativne je osnovna delitev grup na končne in neskončne grupe. Grupa je **končna**, če ima končno število elementov. Številu elementov končne grupe pravimo **red grupe**.

Grupe srečujemo na najrazličnejših področjih matematike. V tem uvodnem razdelku bomo omenili le nekaj enostavnih zgledov.

Primer 1.32. Preprosti primeri Abelovih grup so $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$ in $(\mathbb{C}, +)$. Pri vseh je nevtralni element število 0, inverz elementa a pa je

njegov nasprotni element, torej $-a$. Ker nasprotno število naravnega števila ni naravno število, monoid $(\mathbb{N} \cup \{0\}, +)$ ni grupa.

Vsak monoid v sebi skriva grupo. Označimo s S^* množico vseh obrnljivih elementov monoida S.

TRDITEV 1.33. *Če je $(S, \star)$ monoid, je $(S^*, \star)$ grupa.*

DOKAZ. Če $x, y \in S^*$, potem po trditvi 1.29 tudi $x \star y \in S^*$, torej je $\star$ notranja operacija na S^*. Ker je $\star$ asociativna na S, je asociativna tudi na S^*. Nevtralni element e je sam sebi inverz in zato pripada S^*. Vsak element iz S^* je obrnljiv po definiciji, njegov inverz pa seveda prav tako leži v S^*. □

PRIMER 1.34. Edini obrnljiv element monoidov $(\mathbb{N} \cup \{0\}, +)$ in $(\mathbb{N}, \cdot)$ je nevtralni element. Ustrezni grupi sta zato $(\{0\}, +)$ in $(\{1\}, \cdot)$. Vsaki grupi z enim samim elementom pravimo **trivialna grupa**.

PRIMER 1.35. Množice $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ in $\mathbb{C}$ so monoidi za operacijo množenja. Zato so

$$\mathbb{Z}^* = \{1, -1\}$$

in

$$\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}, \quad \mathbb{R}^* = \mathbb{R} \setminus \{0\} \quad \text{in} \quad \mathbb{C}^* = \mathbb{C} \setminus \{0\}$$

grupe za množenje. Seveda so tudi te grupe Abelove. Končna je le prva izmed njih.

PRIMER 1.36. Obrnljivi elementi monoida $\mathcal{F}(X)$ so natanko bijektivne preslikave (primer 1.25). Torej je

$$\mathrm{Sim}(X) := \mathcal{F}(X)^* = \{f : X \to X \mid f \text{ je bijektivna preslikava}\}$$

grupa za operacijo kompozitum. Bijektivni preslikavi iz množice X vase pravimo tudi **permutacija** množice X. Izraz permutacija se sicer pogosteje uporablja za končne množice X in še posebej za $X = \{1, \ldots, n\}$, a načeloma je ga lahko uporabimo tudi za neskončne množice. Grupi $\mathrm{Sim}(X)$, torej grupi permutacij množice X, pravimo **simetrična grupa** množice X. Ni se težko prepričati, da je ta grupa Abelova samo tedaj, ko je $|X| \leq 2$. Dokaz zaenkrat prepuščamo bralcu, sicer pa se bomo na simetrične grupe še vračali. V primeru, ko je $X = \{1, \ldots, n\}$, grupo $\mathrm{Sim}(X)$ označujemo s S_n.

Doslej smo splošno binarno operacijo označevali z $\star$, v konkretnih zgledih pa je bila enaka $+$, $\cdot$ ali $\circ$. Kot smo že omenili, so nasploh seštevanje, množenje in komponiranje najpomembnejši primeri binarnih operacij. Komponiramo seveda preslikave, seštevamo in množimo med seboj pa različne matematične objekte, ne le števila kot v zgornjih primerih. Oznako $\star$ smo uporabljali kot nevtralen simbol, ki lahko pomeni $+$, $\cdot$, $\circ$ ali kaj drugega. To označevanje pa zna biti naporno in pri daljših formulah se kar malo izgubimo. Zato bomo v

splošnih grupah oznako $\star$ zamenjali z oznako za množenje $\cdot$. Namesto $x \cdot y$ bomo ponavadi pisali kar xy, nevtralni element pa bomo namesto z e označevali z 1. Po dogovoru je tako

$$x^0 = 1$$

za vsak element x. Element xy bomo imenovali **produkt** elementov x in y in nasploh uporabljali terminologijo, ki se pri množenju ponuja sama od sebe. Izraza operacija in množenje bomo pri delu z grupami tako uporabljali kot sopomenki. Zaradi novih oznak, pa tudi zato, da bodo vsi aksiomi pregledno zbrani na enem mestu, sedaj ponovno zapišimo definicijo grupe.

Definicija grupe. Množica G skupaj z binarno operacijo $(x, y) \mapsto xy$ je **grupa**, če velja:

(G1) Za vse $x, y, z \in G$ je $(xy)z = x(yz)$.
(G2) Obstaja tak element $1 \in G$, da za vsak $x \in G$ velja $1x = x1 = x$. Element 1 imenujemo **enota** grupe G.
(G3) Za vsak $x \in G$ obstaja tak $x^{-1} \in G$, da je $xx^{-1} = x^{-1}x = 1$. Element x^{-1} imenujemo **inverz** elementa x.

Če velja tudi $xy = yx$ za vse $x, y \in G$, grupi G pravimo **Abelova grupa**.

Poudarimo, da aksiom (G2) pravi »... obstaja $1 \in G$, da za vsak $x \in G$ velja ... « in ne »... za vsak $x \in G$ obstaja $1 \in G$, da velja ... «. Opozorilo se morda zdi odveč, a napaka ni tako redka pri začetnikih.

Povzemimo nekaj izsledkov prejšnjega razdelka:

(a) Grupa G ima natanko eno enoto.
(b) Vsak element iz G ima natanko en inverz.
(c) Za vse $x \in G$ je $(x^{-1})^{-1} = x$.
(d) Za vse $x, y \in G$ je $(xy)^{-1} = y^{-1}x^{-1}$.
(e) Za vse $m, n \in \mathbb{Z}$ in $x \in G$ je $x^{m+n} = x^m x^n$ in $(x^m)^n = x^{mn}$.
(f) Za vse $x, y, z \in G$ iz $xy = xz$ sledi $y = z$.
(g) Za vse $x, y, z \in G$ iz $yx = zx$ sledi $y = z$.
(h) Za vse $x, y \in G$ iz $xy = 1$ sledi $yx = 1$, tj. $y = x^{-1}$.

Trditvi (f) in (g) imenujemo **pravili krajšanja** v grupi. Posebej omenimo njuna posebna primera: če je $xy = x$ ali $yx = x$, potem je $y = 1$. Iz $x^2 = x$ tako sledi $x = 1$.

Novo označevanje je enostavnejše in preglednejše. Vendarle pa bomo v posebnih grupah oznako za množenje včasih zamenjali z oznako, ki je v dani situaciji primernejša. Posebej oznaka za seštevanje $+$ bo pogosto uporabljena. Grupi s tako označeno operacijo pravimo **aditivna grupa**. Običajno so aditivne grupe Abelove. V literaturi najdemo tudi izjeme, a le poredko. Da se izognemo zapletom in vsakokratnim pojasnjevanjem, sprejmimo to kot pravilo:

Dogovor. V tej knjigi bodo vse aditivne grupe Abelove.

Kadarkoli bomo operacijo označevali s $+$, se bo torej razumelo, da za vse elemente x in y velja

$$x + y = y + x.$$

V aditivni grupi nevtralni element označujemo z 0 in mu rečemo **ničelni element** ali kar **ničla**. Elementu $x + y$ seveda pravimo **vsota** elementov x in y. Inverzni element elementa x označujemo z $-x$ in ga imenujemo **nasprotni element** elementa x. To je torej element, za katerega velja

$$x + (-x) = (-x) + x = 0.$$

V aditivni grupi definiramo **odštevanje** elementov na znani način, kot ga poznamo pri številih:

$$x - y := x + (-y).$$

Element $x - y$ imenujemo **razlika elementov** x in y. Nadalje, v aditivni grupi namesto x^n pišemo nx. Če je n naravno število, je torej

$$nx = x + \cdots + x \quad \text{in} \quad (-n)x = -x - \cdots - x,$$

kjer element x na desni strani obeh enakosti nastopa n-krat. Enakost $x^0 = 1$ se v aditivni grupi seveda zapiše kot

$$0x = 0.$$

Element 0 na levi strani je celo število, element na desni pa je ničelni element grupe. Za vsako celo število n in vsak element x aditivne grupe velja

$$(-n)x = n(-x) = -(nx).$$

Trditve (a)-(f) se za aditivno grupo glasijo takole:

(a') Aditivna grupa G ima natanko en ničelni element.
(b') Vsak element iz G ima natanko en nasprotni element.
(c') $-(-x) = x$ za vse $x \in G$.
(d') $-(x + y) = -x - y$ za vse $x, y \in G$.
(e') Za vse $m, n \in \mathbb{Z}$ in $x \in G$ je $(m+n)x = mx + nx$ in $n(mx) = (nm)x$.
(f') Za vse $x, y, z \in G$ iz $x + y = x + z$ sledi $y = z$.

Naloge

1. Ugotovi, katere izmed naslednjih množic so grupe za običajno seštevanje števil:
   (a) $\{\frac{n}{2} \mid n \in \mathbb{Z}\}$.
   (b) $\{x \in \mathbb{R} \mid x \geq 0\}$.
   (c) $\{x \in \mathbb{R} \mid x \notin \mathbb{Q}\} \cup \{0\}$.
   (d) $\{z \in \mathbb{C} \mid \mathrm{Im}(z) \in \mathbb{Z}\}$.
   (e) $\{z \in \mathbb{C} \mid \mathrm{Re}(z) \cdot \mathrm{Im}(z) = 0\}$.
   (f) $\{p + q\sqrt{2} \mid p, q \in \mathbb{Q}\}$.

2. Ugotovi, katere izmed naslednjih množic so grupe za običajno množenje števil:
   (a) $\{2^n \mid n \in \mathbb{Z}\}$.
   (b) $\{x \in \mathbb{R} \mid x > 0\}$.
   (c) $\{x \in \mathbb{R} \mid x < 0\}$.
   (d) $\{x \in \mathbb{R} \mid 0 < x < 1\}$.
   (e) $\{z \in \mathbb{C} \mid |z| \geq 1\}$.
   (f) $\{p + q\sqrt{2} \mid p, q \in \mathbb{Q}\} \setminus \{0\}$.
3. Poišči taka med seboj različna kompleksna števila u, z, w, da bo množica $\{u, z, w\}$ grupa za množenje.
4. Naj bo G množica vseh nekonstantnih linearnih funkcij, torej funkcij $f : \mathbb{R} \to \mathbb{R}$ oblike $f(x) = ax + b$, kjer sta $a, b \in \mathbb{R}$ in $a \neq 0$. Pokaži, da je G grupa za komponiranje. Ali je Abelova?
5. Pokaži, da je odprt interval realnih števil $(-1, 1)$ grupa za binarno operacijo $x * y = \frac{x+y}{1+xy}$.
6. S pomočjo trditve 1.33 poišči primer končne in primer neskončne množice števil, ki je za binarno operacijo $x \star y = x + y + xy$ grupa.
7. Pokaži, da za vsak element x *končne* grupe G obstaja tak $n \in \mathbb{N}$, da je $x^n = 1$.

   Komentar. Najmanjšemu naravnemu številu n s to lastnostjo pravimo **red elementa** x. Kot bomo videli kasneje, je ta pojem v teoriji grup zelo pomemben.
8. V vsaki grupi iz $xy = 1$ sledi $yx = 1$. Dokaži, da le v Abelovi grupi iz $xyz = 1$ sledi $zyx = 1$.
9. Pokaži, da je grupa, v kateri za vsak element x velja $x^2 = 1$, Abelova.
10. Pokaži, da je vsaka grupa s štirimi elementi Abelova.

    Komentar. Kasneje bomo videli, da je vsaka grupa z manj kot šest elementi Abelova. Lahko pa že zdaj to poskusiš dokazati sam.
11. Naj bo x produkt vseh elementov končne Abelove grupe. Pokaži, da je $x^2 = 1$.
12. Naj bo $(S, \star)$ polgrupa. Dokaži, da je S grupa natanko tedaj, ko sta za vsak par $a, b \in S$ rešljivi enačbi $a \star x = b$ in $y \star a = b$.

1.4. Kolobarji in polja

Aditivne grupe $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ in $\mathbb{C}$ smo navedli kot osnovne zglede Abelovih grup. Na teh množicah imamo definirano tudi množenje, ki je prav tako notranja (binarna) operacija. Vendar zanjo množice niso grupe, pač pa le monoidi. Seštevanje in množenje sta povezana preko zakona distributivnosti. Tako $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ in $\mathbb{C}$ ustrezajo pogojem naslednje definicije, so torej primeri kolobarjev.

DEFINICIJA 1.37. Množica K skupaj z binarnima operacijama seštevanje $(x, y) \mapsto x + y$ in množenje $(x, y) \mapsto xy$ se imenuje **kolobar**, če velja:

(K1) Za seštevanje je K Abelova grupa.
[Torej velja $(x+y)+z = x+(y+z)$ za vse $x, y, z \in K$, $x+y = y+x$ za vse $x, y \in K$, obstaja tak element $0 \in K$, da je $x + 0 = x$ za vsak $x \in K$, in za vsak $x \in K$ obstaja tak $-x \in K$, da je $x + (-x) = 0$.]

(K2) Za množenje je K monoid.
[Torej velja $(xy)z = x(yz)$ za vse $x, y, z \in K$ in obstaja tak element $1 \in K$, da za vsak $x \in K$ velja $1x = x1 = x$. Imenujemo ga **enota** kolobarja K.]

(K3) Izpolnjena sta **distributivnostna zakona**:

$$(x + y)z = xz + yz, \quad z(x + y) = zx + zy$$

za vse $x, y, z \in K$.

Kolobar je torej trojica

$$(K, +, \cdot).$$

Sestavlja ga množica K in operaciji $+$ in $\cdot$. Toda ponavadi manj formalno govorimo kar o kolobarju K. Kadar na primer omenjamo kolobar $\mathbb{Z}$, imamo v mislih običajno seštevanje in množenje celih števil. Zapis s trojico je potreben, kadar ni povsem jasno, kateri operaciji imamo v mislih.

Včasih med aksiome za kolobar ne uvrščamo zahteve o obstoju enote za množenje. Z drugimi besedami, v (K2) besedo monoid zamenjamo s polgrupa. To ima svoje prednosti. Obravnava **kolobarjev brez enote** pogosto ni bistveno zahtevnejša, pokrije pa veliko več primerov. Preprost zgled je množica sodih celih števil, opremljena z običajnim seštevanjem in množenjem. Vendar pa se pri delu s kolobarji brez enote včasih ne moremo izogniti sitnim podrobnostim, ki lahko odvrnejo pozornost od bistva. Zato smo obstoj enote vključili med aksiome.

Podobno kot za grupe tudi za kolobarje iz aksiomov izpeljemo nekaj enostavnih lastnosti. Ker je kolobar aditivna grupa, za seštevanje seveda veljajo vse ugotovitve iz prejšnjega razdelka. Podobno v zvezi z množenjem veljajo splošne ugotovitve o monoidih. Naslednja trditev opisuje lastnosti, ki povezujejo seštevanje in množenje. Poleg distributivnosti bomo v dokazu uporabljali tudi pravilo krajšanja v aditivni grupi.

TRDITEV 1.38. *V poljubnem kolobarju K velja:*

(a) $0x = x0 = 0$ *za vse* $x \in K$.
(b) $(-x)y = x(-y) = -(xy)$ *za vse* $x, y \in K$.
(c) $(x - y)z = xz - yz$ *in* $z(x - y) = zx - zy$ *za vse* $x, y, z \in K$.
(d) $(-x)(-y) = xy$ *za vse* $x, y \in K$.
(e) $(-1)x = x(-1) = -x$ *za vse* $x \in K$.

Dokaz. Iz

$$0x = (0 + 0)x = 0x + 0x$$

sledi $0x = 0$. Podobno izpeljemo $x0 = 0$. Iz

$$0 = x0 = x(y + (-y)) = xy + x(-y)$$

razberemo, da je $x(-y) = -(xy)$. Podobno dokažemo drugo formulo v (b). S pomočjo distributivnosti iz (b) izpeljemo (c). Iz (b) sledi tudi (d), saj je

$$(-x)(-y) = -(x(-y)) = -(-(xy)) = xy.$$

Prav tako je (e) takojšnja posledica (b). □

Primer 1.39. Najenostavnejši primer kolobarja je kolobar z enim samim elementom. Označevali ga bomo z $\{0\}$ in imenovali **ničelni** ali **trivialni kolobar**. V tem kolobarju elementa 0 in 1 sovpadata. Kolobar je **neničeln**, če vsebuje več kot en element. Ekvivalentno, to je kolobar, v katerem $1 \neq 0$. Namreč, iz $1 = 0$ sledi, da je $x = 1x = 0x = 0$ za vsak $x \in K$.

V aksiomu (K3) smo zahtevali veljavnost dveh zakonov distributivnosti. Če bi bilo množenje komutativno, bi seveda zadoščal en sam zakon.

Definicija 1.40. Kolobar, v katerem je množenje komutativno, imenujemo **komutativen kolobar**.

Primer 1.41. Kolobarji $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ in $\mathbb{C}$ so komutativni.

Teoriji komutativnih in nekomutativnih kolobarjev sta precej različni, vsaka ima svoje cilje in metode. Vendarle pa imata skupno osnovo, s katero se bomo v prihodnjih poglavjih seznanili. Tako kot grupe tudi kolobarje lahko delimo na končne in neskončne, vendar pa končni kolobarji v matematiki ne igrajo tako izrazito pomembne vloge kot končne grupe. Zato je ta delitev pri kolobarjih manj poudarjena. To pa ne pomeni, da se ne bomo srečevali s končnimi kolobarji. Kolobarji ostankov, s katerimi se bomo seznanili v razdelku 2.2, so navsezadnje eni ključnih primerov kolobarjev. Tudi zadnji razdelek knjige bo posvečen posebnim končnim kolobarjem.

Pri študiju matematike se z nekomutativnim množenjem običajno prvič srečamo pri množenju matrik. Če želimo neko množico matrik opremiti s strukturo kolobarja, se moramo omejiti na kvadratne matrike, da bo množenje notranja operacija. Zaradi enostavnosti in preglednosti si sedaj oglejmo le primer z matrikami velikosti 2×2. S splošnejšimi kolobarji matrik se bomo podrobneje ukvarjali kasneje.

Primer 1.42. Naj $M_2(\mathbb{R})$ označuje množico vseh realnih matrik velikosti 2×2. Njeni elementi so torej matrike $\begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}$, kjer so a_{ij} realna števila.

Seštevanje in množenje v $M_2(\mathbb{R})$ vpeljemo na standarden način:

$$\begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} + \begin{bmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{bmatrix} := \begin{bmatrix} a_{11}+b_{11} & a_{12}+b_{12} \\ a_{21}+b_{21} & a_{22}+b_{22} \end{bmatrix}$$

in

$$\begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} \begin{bmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{bmatrix} := \begin{bmatrix} a_{11}b_{11}+a_{12}b_{21} & a_{11}b_{12}+a_{12}b_{22} \\ a_{21}b_{11}+a_{22}b_{21} & a_{21}b_{12}+a_{22}b_{22} \end{bmatrix}.$$

Kot je dobro znano in se zlahka prepričamo, sta obe operaciji asociativni in izpolnjena sta distributivnostna zakona. Nevtralni element za seštevanje je ničelna matrika $0 = \left[\begin{smallmatrix} 0 & 0 \\ 0 & 0 \end{smallmatrix}\right]$, nevtralni element za množenje pa identična matrika $I = \left[\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right]$. Nasprotni element matrike $\left[\begin{smallmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{smallmatrix}\right]$ je matrika $\begin{bmatrix} -a_{11} & -a_{12} \\ -a_{21} & -a_{22} \end{bmatrix}$. Torej je $M_2(\mathbb{R})$ kolobar.

Za matriki

$$A = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \quad \text{in} \quad B = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$$

velja $AB = B$ in $BA = 0$. Kolobar $M_2(\mathbb{R})$ torej ni komutativen.

Zadnji primer pokaže še nekaj: produkt neničelnih elementov v kolobarju je lahko enak nič. Računanje je v kolobarjih torej vendarle nekoliko drugačno od računanja s števili.

Definicija 1.43. Element x kolobarja K je **delitelj niča**, če $x \neq 0$ in če obstaja tak $y \neq 0$ iz K, da je $xy = 0$ ali $yx = 0$.

V primeru, ko je $xy = 0$, elementu x natančneje pravimo **levi delitelj niča**, v primeru, ko je $yx = 0$, pa **desni delitelj niča**. Delitelj niča je tako element, ki je levi delitelj niča ali desni delitelj niča. V komutativnih kolobarjih sta pridevnika »levi« in »desni« seveda odveč.

Kolobar brez deliteljev niča je torej kolobar, v katerem iz $xy = 0$ sledi $x = 0$ ali $y = 0$. Taki so na primer kolobarji $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ in $\mathbb{C}$. V kolobarju brez deliteljev niča velja **pravilo krajšanja** v naslednjem smislu: če so elementi x, y, z taki, da $x \neq 0$ in je $xy = xz$ (ali pa $yx = zx$), potem je $y = z$. Enakost $xy = xz$ namreč lahko zapišemo v obliki $x(y - z) = 0$.

Kolobar je monoid za operacijo množenja, zato lahko govorimo o njegovih obrnljivih elementih. Množica K^* obrnljivih elementov kolobarja K je grupa za množenje (trditev 1.33). Lahko je razmeroma majhna (npr. $\mathbb{Z}^* = \{1, -1\}$), lahko pa vsebuje prav vse elemente razen seveda elementa 0 (npr. $\mathbb{R}^* = \mathbb{R}\backslash\{0\}$). Kolobarji s to zadnjo lastnostjo so posebej zanimivi.

Definicija 1.44. Neničeln kolobar je **obseg**, če je vsak njegov neničeln element obrnljiv. Komutativen obseg imenujemo **polje**.

Primer nekomutativnega obsega bomo spoznali kasneje. Šolski primeri polj so $\mathbb{Q}$, $\mathbb{R}$ in $\mathbb{C}$. Do nadaljnjega si pod poljem predstavljajmo enega izmed teh treh polj, kasneje pa bomo spoznali še številne druge primere.

Bralca naj ne moti, če bomo v nadaljevanju enkrat govorili o polju realnih (ali katerih drugih) števil, drugič pa o kolobarju teh števil. Z izbiro izraza včasih želimo nakazati smer razmišljanja, včasih pa je ta izbira preprosto naključna.

TRDITEV 1.45. *Obrnljiv element kolobarja ni delitelj niča.*

DOKAZ. Naj za elementa x in y iz kolobarja K velja $xy = 0$. Denimo, da je x obrnljiv. Enakost $xy = 0$ z leve pomnožimo z x^{-1} in dobimo $y = 0$. Podobno vidimo, da iz obrnljivosti y sledi $x = 0$. □

POSLEDICA 1.46. *Obseg je kolobar brez deliteljev niča.*

Obrat te ugotovitve ne velja. Veliko kolobarjev brez deliteljev niča ni obsegov. Omenimo le najpreprostejši primer.

PRIMER 1.47. Kolobar $\mathbb{Z}$ nima deliteljev niča, a ni obseg.

Čeprav so polja posebni primeri kolobarjev, je teorija polj v veliki meri neodvisna od teorije splošnih kolobarjev. Tudi globoki rezultati o kolobarjih so pogosto za polja očitni. Čeprav smo jih omenili kot primere tik ob definiciji kolobarja, so $\mathbb{Q}$, $\mathbb{R}$ in $\mathbb{C}$ preveč »popolni«, da bi bili zanimivi s stališča teorije kolobarjev. Drugače je s kolobarjem $\mathbb{Z}$, ki ga lahko štejemo za osnovni zgled ali kar prototip kolobarja.

Naloge

1. Ugotovi, katere izmed naslednjih množic so kolobarji za običajno seštevanje in običajno množenje števil:
   (a) $\{\frac{m}{2n+1} \mid m, n \in \mathbb{Z}\}$.
   (b) $\{\frac{2n+1}{m} \mid m, n \in \mathbb{Z}, m \neq 0\}$.
   (c) $\{m + 2ni \mid m, n \in \mathbb{Z}\}$.
   (d) $\{2m + ni \mid m, n \in \mathbb{Z}\}$.
   (e) $\{m + n\sqrt{2} \mid m, n \in \mathbb{Z}\}$.
   (f) $\{p + q\sqrt{2} \mid p, q \in \mathbb{Q}\}$.
   Kateri izmed teh kolobarjev so polja?
2. Naj bo K kolobar brez enote. Pokaži, da množica $\mathbb{Z} \times K$ postane kolobar (z enoto!), če jo opremimo z binarnima operacijama seštevanja in množenja takole:
$$(m, x) + (n, y) := (m + n, x + y),$$
$$(m, x) \cdot (n, y) := (mn, nx + my + xy)$$
   (tu je mn produkt celih števil m in n, xy produkt elementov x in y v K ipd.).

Komentar. To je pomembna konstrukcija, s katero lahko nekatere probleme o kolobarjih brez enote prevedemo na probleme o kolobarjih v našem smislu. Običajno elemente x iz K identificiramo z elementi $(0, x)$ iz $\mathbb{Z} \times K$ in v tem smislu obravnavamo K kot podmnožico $\mathbb{Z} \times K$. To ima smisel, ker sta potem operaciji v $\mathbb{Z} \times K$ razširitvi operacij v K.

3. Pokaži, da bi lahko kolobar ekvivalentno definirali brez zahteve o komutativnosti seštevanja (da torej enakost $x + y = y + x$ sledi iz ostalih aksiomov).
4. Naj bo K kolobar. Kateri izmed naslednjih pogojev so ekvivalentni pogoju, da je K komutativen?
   (a) $(x + y)^2 = x^2 + 2xy + y^2$ za vse $x, y \in K$.
   (b) $x^2 - y^2 = (x - y)(x + y)$ za vse $x, y \in K$.
   (c) Za vse $x, y \in K$ iz $xy = 1$ sledi $yx = 1$.
   (d) Za vse $x, y, z, w \in K$ iz $xy = zw$ sledi $yx = wz$.
5. Naj bo $\mathcal{P}(X)$ potenčna množica neprazne množice X. Pokaži, da $\mathcal{P}(X)$ postane komutativen kolobar, če vpeljemo vsoto elementov kot simetrično razliko množic, torej $A + B := (A \setminus B) \cup (B \setminus A)$, in produkt elementov kot presek množic, torej $A \cdot B := A \cap B$.
6. Element x kolobarja K imenujemo **idempotent**, če je $x^2 = x$. Kolobar imenujemo **Boolov kolobar**, če je vsak njegov element idempotent. Tak je na primer kolobar iz prejšnje naloge. Pokaži, da je vsak Boolov kolobar komutativen in da je vsak element x Boolovega kolobarja enak svojemu nasprotnemu elementu (torej zadošča $x + x = 0$).

   Komentar. Izkaže se, da je komutativen celo vsak kolobar, v katerem za vsak element x velja $x^n = x$ za neki $n \geq 2$. Toda dokaz ni enostaven in zahteva določeno predznanje. Za male n, na primer za $n = 3$ in $n = 4$, pa je dokazovanje lahko zabavna naloga.
7. Pokaži, da vsak kolobar z delitelji niča vsebuje taka neničelna elementa x in y, da je $xy = yx = 0$.
8. Pokaži, da v kolobarju brez deliteljev niča iz $x^2 = 1$ sledi $x = 1$ ali $x = -1$. S primerom pokaži, da to ne velja v vseh kolobarjih.
9. Pokaži, da je kolobar obseg, če ima vsak njegov neničeln element levi inverz.
10. Naj bosta x in y elementa kolobarja. Pokaži, da je element $1 - xy$ obrnljiv natanko tedaj, ko je obrnljiv element $1 - yx$.

    Namig. Rešitev je enostavna – a najbrž šele potem, ko jo vidiš. Inverz elementa $1 - yx$ poskusi izraziti s pomočjo inverza elementa $1 - xy$. Formulo lahko uganeš s pomočjo znane formule za vsoto geometrijske vrste, torej $(1-q)^{-1} = 1+q+q^2+\ldots$ (z vprašanjem konvergence vrste se tu ne obremenjuj). Zatem seveda preveri, da je formula prava. Tu

namreč ne gre za izpeljavo, temveč res za ugibanje – in za lep zgled, kako si lahko na enem matematičnem področju pomagamo z znanjem z drugega.

1.5. Vektorski prostori in algebre

Vektorski prostor je temeljni pojem linearne algebre. Njegova definicija je bralcu zato gotovo znana. Kljub temu jo zapišimo.

Definicija 1.48. Naj bo F polje. Množica V skupaj z (notranjo) binarno operacijo seštevanje $(u, v) \mapsto u + v$ in zunanjo binarno operacijo iz $F \times V$ v V, imenovano **množenje s skalarji** in označeno z $(\lambda, v) \mapsto \lambda v$, se imenuje **vektorski prostor nad** F, če velja:

(V1) Za seštevanje je V Abelova grupa.
(V2) Za vse $\lambda \in F$ in $u, v \in V$ je $\lambda(u + v) = \lambda u + \lambda v$.
(V3) Za vse $\lambda, \mu \in F$ in $v \in V$ je $(\lambda + \mu)v = \lambda v + \mu v$.
(V4) Za vse $\lambda, \mu \in F$ in $v \in V$ je $\lambda(\mu v) = (\lambda\mu)v$.
(V5) Za vse $v \in V$ je $1v = v$.

Namesto vektorski prostor pogosto rečemo kar **prostor**. Elemente (vektorskega) prostora imenujemo **vektorji**, elemente pripadajočega polja pa **skalarji**. Vektorju oblike λv pravimo **skalarni večkratnik** vektorja v.

Vektorski prostori se pojavljajo na različnih matematičnih področjih, a največkrat samo tisti nad poljem $\mathbb{R}$ ali nad poljem $\mathbb{C}$. Prvim pravimo **realni vektorski prostori**, drugim pa **kompleksni vektorski prostori**. Kasneje bomo videli, da je vendarle koristno obravnavati vektorske prostore nad poljubnimi polji.

Dodajmo nekaj pojasnil k definiciji. Tako seštevanje v V kot seštevanje v F smo označili z istim simbolom $+$. V (V3) obe seštevanji tudi nastopata. Podobno v (V4) nastopata dve množenji: množenje vektorjev s skalarji in množenje skalarjev med seboj, torej množenje v polju F. Simbol 1 v (V5) označuje enoto v F, torej element z lastnostjo $1\lambda = \lambda$ za vse $\lambda \in F$. Za ta element torej zahtevamo, da je tudi $1v = v$ za vsak vektor v.

V vsakem vektorskem prostoru V nad poljem F veljajo naslednje trditve:

(a) Za vsak $\lambda \in F$ je $\lambda 0 = 0$, kjer 0 označuje ničelni element iz V.
(b) Za vsak $v \in V$ je $0v = 0$, kjer 0 na levi strani označuje ničelni element polja F, 0 na desni pa ničelni element prostora V.
(c) Za vsak $\lambda \in F$ in vsak $v \in V$ iz $\lambda v = 0$ sledi $\lambda = 0$ ali $v = 0$.
(d) Za vsak $\lambda \in F$ in vsak $v \in V$ je $(-\lambda)v = -(\lambda v) = \lambda(-v)$.

Dokazi so enostavni. Prepuščamo jih bralcu.

Zapišimo nekaj primerov vektorskih prostorov. Najprej najbolj standarden primer.

PRIMER 1.49. Za vsako naravno število n množica F^n, tj. kartezični produkt n kopij polja F, postane vektorski prostor, če definiramo operaciji, kot temu pravimo, »po komponentah«:

$$(u_1, u_2, \ldots, u_n) + (v_1, v_2, \ldots, v_n) := (u_1 + v_1, u_2 + v_2, \ldots, u_n + v_n),$$
$$\lambda(v_1, v_2, \ldots, v_n) := (\lambda v_1, \lambda v_2, \ldots, \lambda v_n).$$

To zlahka preverimo. Kot poseben primer je $F = F^1$ vektorski prostor nad samim seboj. Če je $n = 2$ ali $n = 3$ in je $F = \mathbb{R}$, dobimo vektorska prostora $\mathbb{R}^2$ oziroma $\mathbb{R}^3$, ki si ju lahko predstavljamo geometrijsko. Ta ponazoritev včasih pride prav, tudi kadar se ukvarjamo z abstraktnimi vektorskimi prostori nad poljubnimi polji.

PRIMER 1.50. Vektorskemu prostoru, ki vsebuje samo vektor 0, pravimo **trivialni vektorski prostor**.

PRIMER 1.51. Polje $\mathbb{C}$ lahko obravnavamo kot vektorski prostor nad samim seboj. Po drugi strani pa je $\mathbb{C}$ tudi vektorski prostor nad $\mathbb{R}$, če za množenje s skalarji vzamemo kar običajno množenje: za $t \in \mathbb{R}$ in $z = x + yi \in \mathbb{C}$ je $tz = tx + tyi \in \mathbb{C}$. Podobno lahko $\mathbb{C}$ ali $\mathbb{R}$ interpretiramo kot vektorski prostor nad $\mathbb{Q}$.

PRIMER 1.52. Funkcijo $f : \mathbb{R} \to \mathbb{R}$, ki se da zapisati v obliki

$$f(x) = a_0 + a_1 x + \cdots + a_n x^n, \ x \in \mathbb{R},$$

za neke $a_i \in \mathbb{R}$, imenujemo **realni polinom**. Množica $\mathcal{P}$ vseh realnih polinomov je vektorski prostor za običajno seštevanje polinomov in množenje polinomov s skalarji, torej množenje z realnimi konstantami.

OPOMBA 1.53. Naj bo G poljubna aditivna grupa. Za vsako celo število n in element $x \in G$ smo definirali element $nx \in G$. Na preslikavo $(n, x) \mapsto nx$ lahko gledamo kot na zunanjo binarno operacijo iz $\mathbb{Z} \times G$ v G. Ima prav take lastnosti, kot jih zahtevamo za vektorski prostor:

$$n(x + y) = nx + ny, \ (m + n)x = mx + nx, \ n(mx) = (nm)x \text{ in } 1x = x.$$

Kljub temu ne rečemo, da je G vektorski prostor nad $\mathbb{Z}$. Kolobar $\mathbb{Z}$ namreč ni polje. Prav tako celim številom v tem kontekstu ne rečemo skalarji. Ta izraz je rezerviran za elemente polja, nad katerim je zgrajen vektorski prostor.

Mnogi pomembni primeri kolobarjev so hkrati vektorski prostori. Če je (in ponavadi je) njihovo množenje primerno usklajeno z množenjem s skalarji, potem namesto o kolobarju govorimo o algebri.

DEFINICIJA 1.54. Naj bo F polje. Množica A skupaj z (notranjima) binarnima operacijama seštevanje $(x, y) \mapsto x + y$ in množenje $(x, y) \mapsto xy$ ter zunanjo binarno operacijo množenje s skalarji $(\lambda, x) \mapsto \lambda x$ iz $F \times A$ v A se imenuje **algebra nad** F, če velja:

(A1) Za seštevanje in množenje s skalarji je A vektorski prostor nad F.
(A2) Za seštevanje in množenje je A kolobar.
(A3) Za vse $\lambda \in F$ in vse $x, y \in A$ je $\lambda(xy) = (\lambda x)y = x(\lambda y)$.

Vektorske prostore iz primerov 1.49-1.52 lahko na naraven način opremimo še z množenjem, s katerim postanejo algebre.

PRIMER 1.55. Vektorski prostor F^n postane algebra nad F, če tudi množenje definiramo po komponentah:

$$(u_1, u_2, \ldots, u_n)(v_1, v_2, \ldots, v_n) := (u_1v_1, u_2v_2, \ldots, u_nv_n).$$

Očitno je enota element $(1, 1, \ldots, 1)$. Tudi veljavnost ostalih aksiomov zlahka preverimo. Posebej omenimo najenostavnejši primer, ko je $n = 1$: vsako polje F je torej algebra nad samim seboj.

PRIMER 1.56. **Ničelna** ali **trivialna algebra** je seveda algebra, ki vsebuje le element 0.

Algebri nad poljem $\mathbb{R}$ pravimo **realna algebra**, algebri nad poljem $\mathbb{C}$ pa **kompleksna algebra**. Tako je na primer $\mathbb{R}^n$ realna in $\mathbb{C}^n$ kompleksna algebra.

PRIMER 1.57. Vemo že, da je $\mathbb{C}$ kolobar in realni vektorski prostor. Seveda je tudi realna algebra.

PRIMER 1.58. Če vektorski prostor realnih polinomov $\mathcal{P}$ opremimo še z običajnim množenjem polinomov, postane realna algebra.

PRIMER 1.59. Tudi kolobar matrik $M_2(\mathbb{R})$ iz primera 1.42 postane realna algebra, če vpeljemo množenje matrik s skalarji na običajen način:

$$\lambda \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} := \begin{bmatrix} \lambda a_{11} & \lambda a_{12} \\ \lambda a_{21} & \lambda a_{22} \end{bmatrix}$$

za vse $\lambda, a_{ij} \in \mathbb{R}$. Podobno je $M_2(\mathbb{C})$, množica vseh kompleksnih matrik velikosti 2×2, kompleksna algebra.

Algebre pogosto omenjamo v isti sapi kot kolobarje. Obravnavamo jih kot kolobarje, obogatene z dodatno operacijo množenja s skalarji. Pojma »teorija kolobarjev« in »teorija kolobarjev in algeber« se razlikujeta le v poudarku.

Naloge

1. Ugotovi, katere izmed naslednjih množic so vektorski prostori nad poljem $\mathbb{R}$ za običajno seštevanje vektorjev in običajno množenje vektorjev s skalarji:
   (a) $\{(x, y) \in \mathbb{R}^2 \mid x \geq 0,\ y \geq 0\}$.
   (b) $\{(x, y) \in \mathbb{R}^2 \mid x \in \mathbb{Q}\}$.

(c) $\{(x,y) \in \mathbb{R}^2 \mid x = y\}$.
(d) $\{(x,y,z) \in \mathbb{R}^3 \mid x = y = -z\}$.
(e) $\{(x,y,z) \in \mathbb{R}^3 \mid x = y = z^2\}$.
(f) $\{(x,y,z,w) \in \mathbb{R}^4 \mid x = w,\ y = z\}$.

Kateri izmed teh vektorskih prostorov so algebre nad $\mathbb{R}$, če vzamemo množenje iz primera 1.55?

V primerih (c)-(f) lahko vlogo polja $\mathbb{R}$ zamenjamo s katerimkoli poljem F. Ali so odgovori na zgornji vprašanji potem vselej enaki?

2. Naj bo $\mathcal{P}$ množica vseh realnih polinomov. Za vsak $f \in \mathcal{P}$ naj f' označuje odvod f. Ugotovi, katere izmed naslednjih množic so realni vektorski prostori za običajno seštevanje polinomov in običajno množenje polinomov s skalarji:
   (a) $\{f \in \mathcal{P} \mid f(0) = 0\}$.
   (b) $\{f \in \mathcal{P} \mid f'(0) = 0\}$.
   (c) $\{f \in \mathcal{P} \mid |f(0)| = |f'(0)|\}$.
   (d) $\{f \in \mathcal{P} \mid f(-x) = f(x) \text{ za vsak } x \in \mathbb{R}\}$.
   (e) $\{f \in \mathcal{P} \mid f(-x) = -f(x) \text{ za vsak } x \in \mathbb{R}\}$.
   (f) $\{f \in \mathcal{P} \mid |f(-x)| = |f(x)| \text{ za vsak } x \in \mathbb{R}\}$.

   Kateri izmed teh vektorskih prostorov so realne algebre za običajno množenje polinomov?
3. Pokaži, da je množica obrnljivih elementov algebre zaprta za množenje z neničelnimi skalarji.
4. Kateri elementi algebre realnih polinomov so obrnljivi? Ali ta algebra ima delitelje niča?
5. Pokaži, da je vsak neničeln element algebre F^n iz primera 1.55 bodisi obrnljiv bodisi delitelj niča.
6. Naj matrika $A \in M_2(\mathbb{C})$ ne bo skalarni večkratnik identične matrike. Pokaži, da matrika $B \in M_2(\mathbb{C})$ komutira z A natanko tedaj, ko je B oblike $B = \alpha A + \beta I$ za neka skalarja $\alpha, \beta \in \mathbb{C}$.

   Nasvet. Pomagaj si z izrekom o Jordanovi obliki matrike. Izrek pove, da za vsako matriko A obstaja taka obrnljiva matrika P, da je matrika PAP^{-1} bodisi oblike $\left[\begin{smallmatrix} \lambda & 0 \\ 0 & \mu \end{smallmatrix}\right]$ za neka $\lambda, \mu \in \mathbb{C}$ bodisi oblike $\left[\begin{smallmatrix} \lambda & 1 \\ 0 & \lambda \end{smallmatrix}\right]$ za neki $\lambda \in \mathbb{C}$.

   (V nalogi bi lahko kompleksna števila zamenjali z realnimi, a bi jo s tem za malenkost otežili.)
7. Naj bo $A \in M_2(\mathbb{R})$ taka matrika, da matrika A^2 ni skalarni večkratnik identične matrike. Pokaži, da poljubna matrika $B \in M_2(\mathbb{R})$ komutira z A natanko tedaj, ko komutira z A^2.

   Namig. S pomočjo znanega izreka iz linearne algebre se lahko izogneš računanju!

1.6. Podstrukture

Grupi $(\mathbb{R}, +)$ in $(\mathbb{C}, +)$ sta seveda različni, a očitno povezani. Obe imata isto operacijo, množica $\mathbb{R}$ pa je podmnožica množice $\mathbb{C}$. Pravimo, da je $(\mathbb{R}, +)$ podgrupa grupe $(\mathbb{C}, +)$. Podobno je $(\mathbb{R}, +, \cdot)$ podkolobar kolobarja $(\mathbb{C}, +, \cdot)$. Ker pa sta kolobarja $\mathbb{R}$ in $\mathbb{C}$ polji, rečemo tudi, da je $(\mathbb{R}, +, \cdot)$ podpolje $(\mathbb{C}, +, \cdot)$. Toda pojdimo po vrsti in natančno.

1.6.1. Podgrupe. V naslednji definiciji bomo govorili o »isti operaciji« na podmnožici H grupe G. Ta izraz je intuitivno razumljiv, a nekoliko sporen s formalnega vidika. Povsem natančno bi morali reči »zožitev operacije v grupi G na $H \times H$«. Toda tovrstnim zapletenim formulacijam se bomo v veri, da to ne bo vodilo do nesporazumov, raje izognili.

Definicija 1.60. Podmnožica H grupe G je **podgrupa** grupe G, če je za isto operacijo tudi sama grupa.

Oznaka

$$H \leq G$$

pomeni, da je H podgrupa G. Toda ponavadi bomo dali besedam prednost pred oznakami. Še opozorilo glede terminologije. Podgrupa H je sama grupa, zato ji bomo včasih rekli *grupa* H, drugič pa *podgrupa* H. Izbira poimenovanja je načeloma odvisna od konteksta, povsem jasnih pravil glede te izbire pa pravzaprav ni.

Vsaka grupa G ima vsaj dve podgrupi: G in $\{1\}$. Vsaki podgrupi, ki ni enaka G, pravimo **prava podgrupa**. Podgrupi $\{1\}$ pravimo **trivialna podgrupa**. (Če je G aditivna grupa, jo seveda označujemo z $\{0\}$.) Vsaka podgrupa grupe G očitno vsebuje enoto grupe G. Povedano drugače, trivialna podgrupa je vsebovana v vsaki drugi podgrupi.

Kako preveriti, ali je podmnožica H grupe G podgrupa? Naslednja trditev podaja dva odgovora. Seveda odgovor daje tudi definicija, vendar pri preverjanju ni treba slepo slediti aksiomom. Asociativnost množenja na H denimo takoj sledi iz asociativnosti množenja na G. Po drugi strani pa ne smemo pozabiti, da mora biti H zaprta za množenje, torej, da mora iz $x, y \in H$ slediti $xy \in H$.

Trditev 1.61. *Za neprazno podmnožico H grupe G so naslednje trditve ekvivalentne:*

(i) *H je podgrupa G.*
(ii) *Za vse $x, y \in H$ je $xy^{-1} \in H$.*
(iii) *H je zaprta za množenje in za vsak $x \in H$ je tudi $x^{-1} \in H$.*

Dokaz. (i)⇒(ii). Ker je H sama grupa, je ta implikacija očitna.

(ii)⇒(iii). Vzemimo $x \in H$. Iz (ii) najprej sledi $1 = xx^{-1} \in H$ in od tod $x^{-1} = 1x^{-1} \in H$. Za poljubna $x, y \in H$ je zato $xy = x(y^{-1})^{-1} \in H$.

(iii)⇒(i). Zaprtost za množenje pomeni, da je množenje binarna operacija na H. Asociativna je, saj je G grupa. Za poljuben $x \in H$ je tudi $x^{-1} \in H$ in zato $1 = xx^{-1}$ pripada H zaradi zaprtosti H za množenje. Inverz vsakega elementa iz H leži v H po predpostavki. □

Očitna prednost uporabe (ii) pred (iii) je, da moramo preveriti samo en pogoj. Ponavadi sicer ni posebej pomembno, katerega izmed obeh kriterijev izberemo. Dokaz, da je podmnožica grupe podgrupa, je le redkokdaj zamuden. Omenimo še alternativno inačico drugega pogoja:

(ii') za vse $x, y \in H$ je $x^{-1}y \in H$.

Tudi ta pogoj je ekvivalenten ostalim.

Primer 1.62. Množica neničelnih kompleksnih števil $\mathbb{C} \setminus \{0\}$ je grupa za množenje. S pomočjo zadnje trditve zlahka preverimo, da so naslednje množice njene podgrupe:

$$\mathbb{R} \setminus \{0\},\ \{x \in \mathbb{R} \,|\, x > 0\},\ \{z \in \mathbb{C} \,|\, |z| = 1\} \text{ in } \{1, -1, i, -i\}. \tag{1.3}$$

Množici

$$\{x \in \mathbb{R} \,|\, x > 1\} \text{ in } \{z \in \mathbb{C} \setminus \{0\} \,|\, |z| \leq 1\}$$

sta sicer zaprti za množenje, a nista podgrupi. Prva ne vsebuje niti enote, druga pa ne vsebuje inverzov vseh svojih elementov.

Druga podgrupa iz (1.3) je seveda tudi podgrupa prve grupe, zadnja podgrupa pa je podgrupa tretje grupe. Nasploh, če je $H \leq G$ in je K podmnožica H, sta si pogoja $K \leq H$ in $K \leq G$ ekvivalentna.

V aditivni grupi se pogoj (ii) glasi

$$x - y \in H \quad \text{za vse } x, y \in H,$$

pogoj (iii) pa

$$x + y, -x \in H \quad \text{za vse } x, y \in H.$$

Primer 1.63. Množica sodih celih števil $2\mathbb{Z}$ je podgrupa grupe $(\mathbb{Z}, +)$, množica lihih celih števil pa ni. Pravzaprav ni težko poiskati vseh podgrup $(\mathbb{Z}, +)$. To bomo naredili na začetku naslednjega poglavja, bralec pa lahko že sedaj do rezultata poskusi priti sam.

Primer 1.64. Naj bo G poljubna grupa. Množici

$$Z(G) := \{c \in G \,|\, cx = xc \text{ za vsak } x \in G\}$$

pravimo **center grupe** G. Očitno vsebuje enoto 1 in je zaprta za množenje. Če formulo $cx = xc$ z leve in z desne pomnožimo s c^{-1}, vidimo, da iz $c \in Z(G)$ sledi $c^{-1} \in Z(G)$. Torej je $Z(G)$ podgrupa G. Če je G Abelova, je seveda $Z(G) = G$, sicer pa je $Z(G)$ prava podgrupa G. S konkretnimi primeri se bomo srečavali v nalogah, predvsem v naslednjem poglavju.

Pravimo, da sta si elementa x in y iz grupe G **konjugirana**, če obstaja tak $a \in G$, da je $y = axa^{-1}$; to lahko zapišemo kot $x = a^{-1}ya$, torej x in y v tej definiciji nastopata simetrično. Konjugirana elementa imata vse lastnosti, ki nas v grupah zanimajo, enake. Toda več o tem kasneje. Vrnimo se k podgrupam. Če je H podgrupa grupe G in je a poljuben element iz G, je podgrupa tudi množica

$$aHa^{-1} := \{aha^{-1} \mid h \in H\}.$$

S pomočjo trditve 1.61 je dokaz enostaven in ga prepuščamo bralcu. Vsaki podgrupi oblike aHa^{-1} pravimo **konjugirana podgrupa** podgrupe H. Ta pojem je zanimiv v nekomutativnih grupah, saj v Abelovi grupi očitno velja $aHa^{-1} = H$. Podobno kot za elemente tudi za podgrupi H in K rečemo, da sta si konjugirani, če je K konjugirana podgrupa H (v tem primeru je tudi H konjugirana podgrupa K – zakaj?).

1.6.2. Podkolobarji. Podobno kot podgrupe vpeljemo **podstrukture** drugih algebrskih struktur. V kolobarjih moramo posebno pozornost nameniti enoti za množenje.

Definicija 1.65. Podmnožica L kolobarja K je **podkolobar** kolobarja K, če vsebuje enoto 1 kolobarja K in je za isti operaciji tudi sama kolobar.

Podkolobar L vsebuje tudi element 0 iz K, ne le enote 1. Namreč, L je podgrupa za seštevanje in njegov nevtralni element za seštevanje je lahko le ničla kolobarja K. Zato v definiciji ne zahtevamo posebej, da $0 \in L$. Zahtevi, da $1 \in L$, pa se ne moremo izogniti. Na primer množica vseh matrik oblike $\left[\begin{smallmatrix} x & 0 \\ 0 & 0 \end{smallmatrix}\right]$, kjer je $x \in \mathbb{R}$, je kolobar, ima isti operaciji kot kolobar $M_2(\mathbb{R})$, vendar pa njegova enota, to je matrika $\left[\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right]$, ne sovpada z enoto kolobarja $M_2(\mathbb{R})$, torej z matriko $\left[\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right]$. Zato ni podkolobar $M_2(\mathbb{R})$.

Trditev 1.66. *Podmnožica L kolobarja K je podkolobar natanko tedaj, ko $1 \in L$ in ko je za vse $x, y \in L$ tudi $x - y, xy \in L$.*

Dokaz. Vsak podkolobar seveda vsebuje enoto ter razlike in produkte svojih elementov. Dokažimo obratno implikacijo. Ker je $x - y \in L$ za vse $x, y \in L$, nam trditev 1.61 pove, da je L podgrupa za seštevanje. Po predpostavki je L zaprta tudi za množenje in vsebuje enoto 1. Ker je množenje v K asociativno in ker v K veljata distributivnostna zakona, je oboje izpolnjeno tudi v podmnožici L. Zato je L podkolobar. □

Seveda lahko pogoj $x - y \in L$ za vse $x, y \in L$ zamenjamo s pogojem $x + y, -x \in L$ za vse $x, y \in L$. Z besedami lahko trditev 1.66 povemo takole: podmnožica kolobarja K je podkolobar natanko tedaj, ko vsebuje enoto, je podgrupa za seštevanje in je zaprta za množenje.

Primer 1.67. Kolobar celih števil $\mathbb{Z}$ je podkolobar kolobarja racionalnih števil $\mathbb{Q}$. Podobno je $\mathbb{Z}$ podkolobar kolobarjev $\mathbb{R}$ in $\mathbb{C}$, $\mathbb{Q}$ je podkolobar $\mathbb{R}$ in $\mathbb{C}$, in $\mathbb{R}$ je podkolobar $\mathbb{C}$.

Primer 1.68. **Center kolobarja** K definiramo enako kot center grupe, torej kot množico

$$Z(K) := \{c \in K \mid cx = xc \text{ za vsak } x \in K\}.$$

Zlahka se prepričamo, da je $Z(K)$ podkolobar K. S konkretnimi primeri se bomo srečevali kasneje.

1.6.3. Podprostori. Preskočimo polja in preidimo k vektorskim prostorom.

Definicija 1.69. Podmnožica U vektorskega prostora V je **podprostor** prostora V, če je za isti operaciji tudi sama vektorski prostor.

Trditev 1.70. *Za neprazno podmnožico U vektorskega prostora V nad poljem F so naslednje trditve ekvivalente:*

(i) *U je podprostor V.*
(ii) *Za vse $u, w \in U$ in $\lambda, \mu \in F$ je $\lambda u + \mu w \in U$.*
(iii) *Za vse $u, w \in U$ je $u + w \in U$ in za vse $\lambda \in F$ in $u \in U$ je $\lambda u \in U$.*

Dokaz. (i)⇒(ii). To je očitno, saj je podprostor sam vektorski prostor.
(ii)⇒(iii). Če v pogoju (ii) izberemo $\lambda = \mu = 1$ oziroma $\mu = 0$, dobimo pogoj (iii).
(iii)⇒(i). Z izbiro $\lambda = -1$ v (iii) vidimo, da so nasprotni elementi iz U vsebovani v U. Zato je U podgrupa za seštevanje. Po predpostavki je množenje s skalarji operacija iz $F \times U$ v U. Ker je V vektorski prostor, tudi njegova podmnožica U zadošča vsem aksiomom vektorskega prostora. □

Primer 1.71. Poleg $\{0\}$ in $\mathbb{R}^2$ so edini podprostori $\mathbb{R}^2$ premice, ki potekajo skozi izhodišče. Podobno, podprostori $\mathbb{R}^3$ so $\{0\}$, $\mathbb{R}^3$ ter vse premice in ravnine, ki potekajo skozi izhodišče. Bralec ti dejstvi najbrž pozna, sicer pa se lahko z enostavnim geometrijskim razmislekom ponovno prepriča.

1.6.4. Podalgebre. Definicija podalgebre bi sedaj morala biti samoumevna.

Definicija 1.72. Podmnožica B algebre A je **podalgebra** algebre A, če vsebuje enoto 1 algebre A in če je za iste operacije tudi sama algebra.

Z drugimi besedami, podalgebra je podprostor, ki je hkrati podkolobar. Naslednja trditev zato ne potrebuje dokaza.

Trditev 1.73. *Podmnožica B algebre A je podalgebra natanko tedaj, ko $1 \in B$, za vse $x, y \in B$ je $x + y, xy \in B$ in za vse $\lambda \in F$ in $x \in B$ je $\lambda x \in B$.*

Če $\mathbb{C}$ obravnavamo kot realno algebro, je seveda $\mathbb{R}$ njena podalgebra. **Center algebre** definiramo enako kot center kolobarja (ali grupe); očitno ni le podkolobar, temveč podalgebra.

Dodajmo še malce bolj slikovit primer.

PRIMER 1.74. Množica vseh zgoraj trikotnih realnih matrik, torej matrik oblike $\begin{bmatrix} a_{11} & a_{12} \\ 0 & a_{22} \end{bmatrix}$, kjer so a_{ij} realna števila, je podalgebra algebre $M_2(\mathbb{R})$. Vsebuje namreč identično matriko in je zaprta za vse tri operacije: seštevanje, množenje in množenje s skalarji.

1.6.5. Podpolja. Definicija podpolj je sicer skladna z definicijami ostalih podstruktur, a obravnavamo jih nekoliko drugače. Zato smo to temo prihranili za konec.

DEFINICIJA 1.75. Podmnožica F polja E je **podpolje** polja E, če je za isti operaciji tudi sama polje.

Zahtevo, da podpolje vsebuje enoto polja, smo v definiciji izpustili, saj je enota e podpolja F nujno enaka enoti 1 polja E. Namreč, $e^2 = e$ in zato $e(1-e) = 0$; ker polja nimajo deliteljev niča in $e \neq 0$, sledi $e = 1$.

Dokaz naslednje trditve je podoben dokazu analognih zgornjih trditev, zato ga izpustimo.

TRDITEV 1.76. *Podmnožica F polja E je podpolje natanko tedaj, ko $1 \in F$, za vse $x, y \in F$ je $x - y, xy \in F$ in za vsak $x \neq 0$ iz F je $x^{-1} \in F$.*

Pogoj, da F vsebuje 1, lahko nadomestimo s pogojem, da F vsebuje vsaj en neničeln element.

Na pojem podpolja največkrat gledamo z zornega kota naslednje definicije.

DEFINICIJA 1.77. Polje E je **razširitev polja** F, če je F podpolje E.

Tako je na primer polje $\mathbb{C}$ razširitev polja $\mathbb{R}$. Ker realna števila spoznamo pred kompleksnimi oziroma slednja iz prvih celo konstruiramo, zveni to bolj naravno, kot pa reči, da je $\mathbb{R}$ podpolje $\mathbb{C}$. Podobno lahko opredelimo odnos med poljema $\mathbb{Q}$ in $\mathbb{R}$. Nasploh v teoriji polj običajno izhajamo s stališča, da dano polje poznamo, a ker iz tega ali onega razloga z njim nismo povsem zadovoljni, ga želimo razširiti. Pri drugih algebrskih strukturah je običajnejši drugačen pristop. Na primer v teoriji grup ponavadi podgrupe študiramo zato, da bi razumeli dano grupo.

Na koncu omenimo še skupne značilnosti vseh podstruktur, ki se tičejo operacij preseka in unije. Pričnimo s tole ugotovitvijo:

(a) Presek podgrup je podgrupa.

To ne velja le za presek dveh podgrup, pač pa za presek poljubne, lahko tudi neskončne družine podgrup. S pomočjo trditve 1.61 se o tem zlahka prepričamo. Namreč, če sta x in y elementa iz preseka družine podgrup, potem sta vsebovana v vsaki izmed teh podgrup, zato isto velja za element xy^{-1}, ki je torej vsebovan v preseku te družine podgrup. Podobno razmislimo:

(b) Presek podkolobarjev je podkolobar.
(c) Presek podprostorov je podprostor.
(d) Presek podalgeber je podalgebra.
(e) Presek podpolj je podpolje.

Nasprotno pa je unija podgrup le izjemoma spet podgrupa (gl. nalogo 6). Isto velja za unijo podkolobarjev, podprostorov, podalgeber in podpolj.

Naloge

1. Poišči podgrupo simetrične grupe S_3 z dvema elementoma.
2. Poišči podgrupo simetrične grupe S_3 s tremi elementi.
3. Začetne naloge prejšnjih treh razdelkov zdaj lahko interpretiramo drugače. Tako na primer naloga 1.3/1 sprašuje, katere izmed danih množic so podgrupe grupe $(\mathbb{C}, +)$. Poišči še sam kak primer podgrupe te grupe, kot tudi primer njene podmnožice, ki sicer ima katero od lastnosti podgrup, a ni podgrupa. Zastavi si podobne probleme v zvezi z nalogami 1.3/2, 1.4/1, 1.5/1 in 1.5/2.
4. Poišči primer grupe G in njene neprazne podmnožice X, ki ni podgrupa, ima pa tole lastnost: za vse $x \in X$ in vse $n \in \mathbb{Z}$ je $x^n \in X$.
5. Naj bo H *končna* neprazna podmnožica grupe G. Pokaži, da že iz predpostavke, da je H zaprta za množenje, sledi, da je H podgrupa. S primerom pokaži, da za neskončne množice H ta sklep v splošnem ne velja.

   Namig. Glej nalogo 1.2/8.
6. Naj bosta H in K taki podgrupi grupe G, da je tudi njuna unija $H \cup K$ podgrupa. Pokaži, da je potem $H \subseteq K$ ali $K \subseteq H$.
7. Poišči grupo G s štirimi elementi, ki vsebuje take podgrupe H_1,H_2,H_3, da je $G = H_1 \cup H_2 \cup H_3$ in $H_i \cap H_j = \{1\}$ za vse $i \neq j$.
8. Naj bo A grupa ali kolobar. Za poljuben $a \in A$ naj bo $C(a)$ množica vseh elementov iz A, ki komutirajo z a. Imenujemo jo **centralizator elementa** a. (V posebnem primeru je bil ta pojem obravnavan že v nalogah 1.5/6 in 1.5/7.)
   (a) Pokaži, da je $C(a)$ podgrupa oziroma podkolobar (in podalgebra, če je A algebra).
   (b) Pokaži, da je $C(a) \subseteq C(a^2)$.

(c) Pokaži, da je $C(a) = C(a^2)$, če je $a^{2k+1} = 1$ za kak $k \in \mathbb{N}$.
(d) Poišči kako grupo oziroma kolobar A in njen (njegov) element a, za katerega velja $C(a) \subsetneq C(a^2)$.

Komentar. Poleg centralizatorja elementa poznamo tudi **centralizator podmnožice** $S \subseteq A$. Definiramo jo kot $C(S) := \bigcap_{a \in S} C(a)$, torej kot množico elementov iz A, ki komutirajo z vsemi elementi iz S. Seveda je tudi $C(S)$ podgrupa oziroma podkolobar (podalgebra). Očitno je $C(A)$ enak centru A. Tradicionalno sicer center raje kot s $C(A)$ označujemo z $Z(A)$.

9. Pokaži, da je množica K^* obrnljivih elementov kolobarja K podkolobar le tedaj, ko je K ničelni kolobar.
10. Poišči primer podmnožice vektorskega prostora $\mathbb{R}^2$, ki je za seštevanje podgrupa, a ni podprostor.
11. Poišči primer podmnožice algebre $M_2(\mathbb{R})$, ki je podkolobar, a ni podalgebra.
12. Za vsak $a \in \mathbb{R}$ naj bo A_a množica vseh matrik oblike $\left[\begin{smallmatrix} x & y \\ ay & x \end{smallmatrix}\right]$, kjer sta $x, y \in \mathbb{R}$. Pokaži, da je A_a komutativna podalgebra algebre $M_2(\mathbb{R})$. Za katera števila a ima A_a delitelje niča? Pokaži, da ima v primeru, ko A_a nima deliteljev niča, vsaka neničelna matrika iz A_a inverz, ki leži v A_a. Torej je tedaj A_a polje!
13. Poišči primer komutativne podalgebre algebre $M_2(\mathbb{R})$, ki ima delitelje niča in ni podalgebra oblike A_a iz prejšnje naloge.
14. Naj bo K podkolobar kolobarja $\mathbb{R}$. Pokaži, da je $K[i] := \{x + yi \mid x, y \in K\}$ podkolobar kolobarja $\mathbb{C}$. Še več, $K[i]$ je podpolje $\mathbb{C}$, če je K podpolje $\mathbb{R}$. Ali lahko sedaj najdeš primer pravega podpolja polja $\mathbb{C}$, ki vsebuje število $\sqrt{2}i$?

1.7. Generatorji

Pričnimo s primerom, za katerega domnevamo, da je bralcu znan in tudi lahko razumljiv zaradi geometrijske ponazoritve. Vzemimo vektorski prostor $\mathbb{R}^3$. Edini podprostor, ki vsebuje vektorje $(1,0,0)$, $(0,1,0)$ in $(0,0,1)$, je prostor $\mathbb{R}^3$ sam. Zato rečemo, da ti trije vektorji generirajo prostor $\mathbb{R}^3$. Seveda to niso edini taki vektorji. Denimo, tudi za vektorje $(1,0,0)$, $(1,1,0)$ in $(1,1,1)$ velja isto. Vektorja $(1,0,0)$ in $(0,1,0)$ sama pa generirata ravnino $z = 0$, torej podprostor $\{(x,y,0) \mid x, y \in \mathbb{R}\}$. Namreč, ta ravnina je najmanjši podprostor $\mathbb{R}^3$, ki oba vektorja vsebuje.

Na podoben način lahko govorimo o generatorjih drugih algebrskih struktur. Začnimo z grupami.

1.7.1. Generatorji grup. Naj bo X neprazna podmnožica grupe G. Množico vseh elementov v G, ki jih lahko zapišemo v obliki

$$y_1 y_2 \cdots y_n, \text{ kjer je } y_i \in X \text{ ali } y_i^{-1} \in X,$$

označimo z $\langle X \rangle$. Če je $X = \{x_1, \ldots, x_n\}$, lahko pišemo tudi $\langle x_1, \ldots, x_n \rangle$. V zapisu $y_1 y_2 \cdots y_n$ so nekateri izmed elementov y_i lahko med seboj enaki. Tako na primer množica $\langle x, y \rangle$ vsebuje elemente, kot so

$$1,\ x,\ y,\ yx^{-1},\ x^2y^{-1}x,\ y^{-3}xy^5x^{-4}, \ldots$$

Množica $\langle X \rangle$ je očitno zaprta za množenje. Iz formule

$$(y_1 y_2 \cdots y_n)^{-1} = y_n^{-1} \cdots y_2^{-1} y_1^{-1}$$

razberemo, da vsebuje tudi inverze vseh svojih elementov. Po trditvi 1.61 je $\langle X \rangle$ podgrupa. Seveda je množica X njena podmnožica. Vsaka podgrupa grupe G, ki vsebuje množico X, očitno vsebuje tudi vsak element oblike $y_1 y_2 \cdots y_n$, kjer je $y_i \in X$ ali $y_i^{-1} \in X$. Torej je $\langle X \rangle$ izmed vseh podgrup, ki vsebujejo X, najmanjša; natančneje, vsebovana je v vsaki podgrupi, ki vsebuje X. Zato $\langle X \rangle$ imenujemo **podgrupa, generirana z množico** X. Če množica X sestoji iz elementov x_i, $\langle X \rangle$ imenujemo tudi **podgrupa, generirana z elementi** x_i. V primeru, ko je $\langle X \rangle = G$, rečemo, da je grupa G **generirana z množico** X. Elementom množice X v tem primeru pravimo **generatorji** grupe G, množici X pa **množica generatorjev** grupe G.

Primer 1.78. Množica pozitivnih racionalnih števil $\mathbb{Q}^+$ je grupa za množenje. Očitno je generirana s podmnožico naravnih števil, tj. $\langle \mathbb{N} \rangle = \mathbb{Q}^+$. Podgrupa $\langle 2, 3 \rangle$ sestoji iz vseh števil oblike $2^i 3^j$, kjer sta $i, j \in \mathbb{Z}$.

V aditivni grupi element v $\langle X \rangle$ zapišemo kot $x_1 + \cdots + x_n$, kjer $x_i \in X$ ali $-x_i \in X$. Morda je jasnejši ekvivalenten zapis $k_1 x_1 + \cdots + k_n x_n$, kjer je $x_i \in X$ in $k_i \in \mathbb{Z}$.

Primer 1.79. V grupi $(\mathbb{Z}, +)$ je $\langle 1 \rangle = \langle -1 \rangle = \mathbb{Z}$. Ta grupa ima torej lastnost, da jo generira že en sam element. Take grupe so zelo izjemne. Imenujemo jih ciklične grupe, a o tem več kasneje. Sta pa 1 in -1 edina elementa, ki generirata celo grupo $\mathbb{Z}$. Podgrupa $\langle 2 \rangle$ je na primer enaka $2\mathbb{Z}$, torej grupi sodih števil. Tudi podgrupa $\langle 4, 6 \rangle$ je enaka $2\mathbb{Z}$. Množica generatorjev (pod)grupe seveda ni enolično določena.

Vsaka grupa G očitno zadošča $\langle G \rangle = G$, kar pa ni ravno koristna informacija. Praviloma nas zanimajo čim manjše množice generatorjev. Če je grupa G generirana s kako končno množico X, rečemo, da je **končno generirana**. Vsaka končna grupa je seveda končno generirana. Grupa $(\mathbb{Z}, +)$ je neskončna, a je, kot smo pravkar videli, končno generirana, saj jo generira že en sam element. Študij končno generiranih grup je zahtevnejši kot študij končnih grup, a manj zahteven kot študij splošnih grup.

1.7.2. Generatorji kolobarjev. Naj bo sedaj X neprazna podmnožica kolobarja K. Označimo z $\overline{X}$ podgrupo za seštevanje, generirano z vsemi produkti elementov iz $X \cup \{1\}$. Element iz $\overline{X}$ torej lahko zapišemo v obliki

$$k_1 x_{11} \cdots x_{1m_1} + k_2 x_{21} \cdots x_{2m_2} + \cdots + k_n x_{n1} \cdots x_{nm_n},$$

kjer $x_{ij} \in X \cup \{1\}$ in $k_i \in \mathbb{Z}$. S pomočjo trditve 1.66 vidimo, da je $\overline{X}$ podkolobar. Očitno $\overline{X}$ vsebuje množico X in je vsebovan v vsakem drugem podkolobarju, ki vsebuje X. Zato rečemo, da je $\overline{X}$ **podkolobar, generiran z množico** X**.** Pojme kot **generatorji kolobarja**, **končno generiran kolobar** ipd. definiramo tako kot analogne pojme v grupah.

Primer 1.80. Naj bo K kolobar kompleksnih števil $\mathbb{C}$.

(a) Podkolobar, generiran z elementom 1, je kolobar celih števil $\mathbb{Z}$. Ker vsak podkolobar vsebuje 1, torej vsebuje tudi vsa cela števila. Z drugimi besedami, $\mathbb{Z}$ je najmanjši podkolobar kolobarja $\mathbb{C}$.

(b) Podkolobar, generiran z elementom i, sestoji iz kompleksnih števil oblike $m + ni$, kjer sta $m, n \in \mathbb{Z}$. Označujemo ga z $\mathbb{Z}[i]$ in imenujemo kolobar **Gaussovih celih števil**.

1.7.3. Generatorji vektorskih prostorov. Bralec je z osnovami teorije vektorskih prostorov predvidoma že seznanjen. Naslednji pojmi in dejstva zanj tako ne bodo novi, kratka ponovitev pa vseeno ne bo odveč.

Naj bo V vektorski prostor nad poljem F. Vsakemu vektorju oblike

$$\lambda_1 v_1 + \lambda_2 v_2 + \cdots + \lambda_n v_n, \text{ kjer } \lambda_i \in F,$$

pravimo **linearna kombinacija** vektorjev $v_1, v_2, \ldots, v_n \in V$. Če je X neprazna podmnožica V, je množica $\mathcal{L}(X)$ vseh linearnih kombinacij vektorjev iz X podprostor, ki vsebuje X in je vsebovan v vsakem podprostoru, ki vsebuje X. Torej je $\mathcal{L}(X)$ **podprostor, generiran z** X. Pravimo mu tudi **linearna lupina množice** X, množici generatorjev X pa pravimo **ogrodje** prostora $\mathcal{L}(X)$. Končno generiranemu vektorskemu prostoru V, torej vektorskemu prostoru, ki ima kako končno ogrodje, pravimo **končno-razsežen vektorski prostor**. V takem prostoru torej obstajajo končne množice, katerih linearna lupina je cel prostor.

Pojmi iz prejšnjega odstavka so podobni tistim, ki smo jih vpeljali za grupe in kolobarje. Le poimenovali smo jih na svojstven način. Pojmi, ki so zdaj pred nami, pa so posebnost vektorskih prostorov.

Za podmnožico S vektorskega prostora V rečemo, da je **linearno odvisna**, če obstajajo taki različni vektorji $v_1, v_2, \ldots, v_n \in S$, da je

$$\lambda_1 v_1 + \lambda_2 v_2 + \cdots + \lambda_n v_n = 0$$

za neke skalarje $\lambda_1, \lambda_2, \ldots, \lambda_n \in F$, ki niso vsi enaki 0. Če S ni linearno odvisna, rečemo, da je **linearno neodvisna**. Neskončna množica je torej linearno neodvisna, če je vsaka njena končna podmnožica linearno neodvisna.

Če je $S = \{v_1, \ldots, v_n\}$ in so vsi v_i med seboj različni, namesto o linearni odvisnosti ali neodvisnosti množice S govorimo tudi o linearni odvisnosti ali neodvisnosti vektorjev $v_1, \ldots, v_n$.

Naslednja trditev je ključ za razumevanje končno-razsežnih vektorskih prostorov.

TRDITEV 1.81. *Če vektorji $u_1, \ldots, u_m$ sestavljajo ogrodje končno-razsežnega prostora V, vektorji $v_1, \ldots, v_n \in V$ pa so linearno neodvisni, je $m \geq n$.*

DOKAZ. Po predpostavki je $v_1 = \lambda_1 u_1 + \cdots + \lambda_m u_m$ za neke skalarje λ_i. Ker v_1 ne more biti enak 0, smemo brez škode za splošnost privzeti, da je $\lambda_1 \neq 0$. Zgornjo enakost pomnožimo z λ_1^{-1}. Tako vidimo, da je u_1 linearna kombinacija vektorjev $v_1, u_2, \ldots, u_m$. Od tod hitro sledi, da je tudi množica $\{v_1, u_2, \ldots, u_m\}$ ogrodje. Zato je $v_2 = \nu v_1 + \mu_2 u_2 + \cdots + \mu_m v_m$ za neke skalarje ν in μ_i. Ker sta vektorja v_1 in v_2 linearno neodvisna, vsi μ_i ne morejo biti enaki 0. Privzeti smemo, da je $\mu_2 \neq 0$. Potem je u_2 linearna kombinacija vektorjev $v_1, v_2, u_3, \ldots, u_m$, iz česar sledi, da je tudi množica $\{v_1, v_2, u_3, \ldots, u_m\}$ ogrodje. S postopkom nadaljujemo. Na vsakem koraku eden izmed vektorjev v_i izpodrine enega izmed vektorjev u_j. Naposled pridemo do ogrodja z m vektorji, ki vsebuje vse vektorje $v_1, \ldots, v_n$. Torej je res $m \geq n$. □

Podmnožica B prostora V je **baza** prostora V, če je hkrati linearno neodvisna in ogrodje. Vsak vektor iz V lahko na en sam način zapišemo kot linearno kombinacijo vektorjev iz baze. Baze v vektorskih prostorih vselej obstajajo. Za splošne prostore je dokaz podan v dodatku A. Za končno-razsežne prostore pa je to skoraj očitno. Vsako ogrodje z najmanjšim možnim številom elementov je namreč linearno neodvisna množica (zakaj?) in zato baza. Končno-razsežen prostor V ima torej končno bazo. Iz trditve 1.81 sledi, da imajo vse njegove baze isto število elementov. Pravimo mu **dimenzija** ali **razsežnost** prostora V in ga označujemo z $\dim_F V$ ali kar $\dim V$. Če je $\dim_F V = n$, rečemo, da je V **n-razsežen**. V takem prostoru je *vsaka* linearno neodvisna množica B z n elementi baza. Namreč, če vzamemo katerikoli vektor $v \in V \setminus B$, iz trditve 1.81 razberemo, da je množica $B \cup \{v\}$ linearno odvisna. Od tod takoj sledi, da v leži v linearni lupini B. Zato je B ogrodje in tako baza.

PRIMER 1.82. Vektorski prostor F^n je n-razsežen. Njegovo najenostavnejšo, t. i. standardno bazo sestavljajo vektorji

$$e_1 := (1, 0, \ldots, 0),\ e_2 := (0, 1, 0, \ldots, 0), \ldots, e_n := (0, \ldots, 0, 1).$$

PRIMER 1.83. Kot vektorski prostor nad poljem $\mathbb{R}$ je prostor kompleksnih števil $\mathbb{C}$ 2-razsežen, kot vektorski prostor nad samim seboj pa 1-razsežen.

PRIMER 1.84. Realni vektorski prostor matrik $M_2(\mathbb{R})$ je 4-razsežen. Njegova standardna baza sestoji iz matrik

$$E_{11} := \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix},\ E_{12} := \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix},\ E_{21} := \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix},\ E_{22} := \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}.$$

PRIMER 1.85. Vektorski prostor vseh realnih polinomov $\mathcal{P}$ je neskončno-razsežen. Njegovo standardno bazo sestavljajo polinomi

$$1,\ x,\ x^2,\ x^3, \ldots$$

Vsak polinom namreč lahko na en sam način zapišemo kot linearno kombinacijo teh polinomov.

1.7.4. Generatorji algeber. Naj bo A algebra nad poljem F in naj bo X neprazna podmnožica A. Podobno kot pri obravnavi generatorjev kolobarjev razmislimo, da je **podalgebra, generirana z** X množica vseh elementov oblike

$$\lambda_1 x_{11} \cdots x_{1m_1} + \lambda_2 x_{21} \cdots x_{2m_2} + \cdots + \lambda_n x_{n1} \cdots x_{nm_n},$$

kjer $x_{ij} \in X \cup \{1\}$ in $\lambda_i \in F$. To je torej linearna lupina podkolobarja, generiranega z X.

PRIMER 1.86. Algebra realnih polinomov $\mathcal{P}$ je generirana z enim samim elementom, namreč s polinomom x (kot tudi z vsakim njegovim neničelnim skalarnim večkratnikom).

Za algebro rečemo, da je **končno-razsežna**, če je končno-razsežna kot vektorski prostor.

PRIMER 1.87. Algebra matrik $M_2(\mathbb{R})$ je končno-razsežna, njena dimenzija je 4 (gl. primer 1.84). Generirana pa je že z dvema elementoma, na primer z matrikama E_{12} in E_{21}. Ker je $E_{11} = E_{12}E_{21}$ in $E_{22} = E_{21}E_{12}$, lahko namreč vsako matriko zapišemo kot linearno kombinacijo matrik E_{12},E_{21}, $E_{12}E_{21}$ in $E_{21}E_{12}$. Za primerjavo pa matriki E_{11} in E_{22} generirata »samo« podalgebro vseh diagonalnih matrik, torej matrik oblike $\left[\begin{smallmatrix} \lambda & 0 \\ 0 & \mu \end{smallmatrix}\right]$, kjer sta $\lambda, \mu \in \mathbb{R}$.

Seveda lahko $M_2(\mathbb{R})$ obravnavamo tudi kot (zgolj) kolobar. Podkolobar, generiran z elementoma E_{12} in E_{21}, je potem kolobar vseh matrik s celoštevilskimi členi.

1.7.5. Generatorji polj. Naj bo X neprazna podmnožica polja F. Kot prej označimo z $\overline{X}$ podkolobar kolobarja F, generiran z X. Ni razloga, da bi bil ta podkolobar že polje. Trdimo, da je **podpolje, generirano z** X, torej najmanjše podpolje, ki X vsebuje, enako množici vseh elementov oblike uv^{-1}, kjer sta $u, v \in \overline{X}$ in $v \neq 0$. Vsako podpolje, ki vsebuje X, očitno mora vsebovati vse take elemente. Zato moramo le preveriti, da je ta množica res podpolje. Iz enakosti

$$uv^{-1} - wz^{-1} = (uz - vw)(vz)^{-1} \tag{1.4}$$

vidimo, da je razlika dveh elementov te množice spet element množice. Ostale lastnosti, ki jih po trditvi 1.76 podpolje mora imeti, preverimo brez težav.

Še majhen komentar. Bralcu se je morda zazdelo, da se formule (1.4) ne bi domislil sam. Toda če pišemo $\frac{u}{v}$ namesto namesto uv^{-1} in $\frac{w}{z}$ namesto wz^{-1} ter nato uporabimo znana pravila za računanje z ulomki, se formula prikaže sama. Sicer ni v navadi, da bi zapis z ulomki uporabljali v abstraktnih poljih. Lahko pa »goljufamo«, če nam je tako računanje lažje.

V primeru 1.80 smo kompleksna števila obravnavali kot kolobar. Zdaj jih obravnavajmo kot polje.

Primer 1.88. Naj bo F polje kompleksnih števil $\mathbb{C}$.

(a) Podpolje, generirano z elementom 1, je polje racionalnih števil $\mathbb{Q}$. Vsako podpolje $\mathbb{C}$ torej vsebuje vsa racionalna števila.

(b) Podpolje, generirano z elementom i, sestoji iz kompleksnih števil oblike $p+qi$, kjer sta p in q racionalni števili. O tem se zlahka prepričamo neposredno, tj. preverimo, da je ta množica podpolje, vsebovano v vsakem podpolju, ki vsebuje i. Seveda pa lahko sledimo zgornjemu razmisleku in do istega zaključka pridemo preko kolobarja Gaussovih celih števil $\mathbb{Z}[i]$. To podpolje označujemo s $\mathbb{Q}(i)$ in mu pravimo razširitev polja $\mathbb{Q}$ s priključitvijo elementa i. Ta terminologija je skladna z duhom teorije polj (gl. konec prejšnjega razdelka).

Iz zgornjih razmislekov med drugim sledi, da najmanjša podgrupa (podkolobar itd.), ki vsebuje neprazno podmnožico X, res obstaja. Z »najmanjša« seveda mislimo na to, da je vsebovana v vsaki drugi podgrupi (podkolobarju itd.), ki vsebuje X. Do tega zaključka lahko pridemo tudi hitreje. Podgrupa, generirana z X je očitno enaka preseku vseh podgrup, ki X vsebujejo. To sledi iz dejstva, omenjenega na koncu prejšnjega razdelka, da je presek podgrup spet podgrupa. Isto velja za podkolobarje, podprostore, podalgebre in podpolja. Vendar pa s tem nič ne izvemo o tem, kako izgledajo podgrupe (podkolobarji itd.), generirane z X.

Doslej smo privzemali, da je množica X neprazna. Podgrupa, generirana s prazno množico $\emptyset$, je trivialna podgrupa $\{1\}$. Enaka je namreč preseku vseh podgrup grupe in je torej najmanjša podgrupa v grupi. Podobno je trivialni podprostor $\{0\}$ podprostor, generiran s $\emptyset$ (zato je $\emptyset$ baza prostora $\{0\}$). Podkolobar, generiran s $\emptyset$ pa je enak podkolobarju, generiranemu z elementoma, vsebovanima v vsakem podkolobarju, torej elementoma 0 in 1. Podobno velja za podalgebre in podpolja, generirane s $\emptyset$.

Naloge

1. Naj bo X podmnožica grupe G. Označimo z X^{-1} množico inverzov elementov iz X. Ali je $\langle X\rangle = \langle X^{-1}\rangle$?

2. Poišči dva elementa simetrične grupe S_3, ki grupo generirata. Ali to grupo generira že en sam element?
3. Naj bosta H in K podgrupi aditivne grupe G. Pokaži, da podgrupa, generirana z njuno unijo $H \cup K$, sestoji iz vseh elementov oblike $h + k$, kjer je $h \in H$ in $k \in K$.

   Komentar. Tej podgrupi pravimo vsota podgrup H in K in jo označujemo s $H + K$. O tem bomo še spregovorili.
4. Pokaži, da grupa $(\mathbb{Q}, +)$ ni končno generirana. Kaj pa grupa $(\mathbb{Q}^*, \cdot)$?
5. Določi podgrupe grupe $(\mathbb{Z}, +)$, generirane z množicami $\{6, 9\}$, $\{63, 90\}$ in $\{28, 99\}$. Ali lahko sedaj določiš podgrupo, generirano s poljubnim parom naravnih števil m in n?

   Komentar. Morda je odgovor na zadnje vprašanje laže uganiti, kot pa dokazati njegovo pravilnost. Po razdelku 2.1 pa bi tudi dokazovanje moralo biti enostavno!
6. Pokaži, da je grupa $(\mathbb{R}^*, \cdot)$ generirana z intervalom $[-2, -1]$.
7. Za vsako naravno število n določi podgrupo grupe $(\mathbb{C}^*, \cdot)$, generirano z elementom
$$z_n := \cos \frac{2\pi}{n} + i \sin \frac{2\pi}{n}.$$
   Določi tudi podgrupo, generirano z vsemi z_n, $n \in \mathbb{N}$.
8. Množico vseh realnih polinomov $\mathcal{P}$ lahko obravnavamo kot aditivno grupo, kolobar, realni vektorski prostor ali realno algebro. Opiši podgrupo, podkolobar, podprostor in podalgebro, generirano s polinomoma x^2 in $2x^3$.
9. Tudi $M_2(\mathbb{R})$, množico vseh realnih matrik velikosti 2×2, lahko obravnavamo kot aditivno grupo, kolobar, realni vektorski prostor ali realno algebro. Določi podgrupo, podkolobar, podprostor in podalgebro, generirano z matrikama $\left[\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right]$ in $\left[\begin{smallmatrix} 0 & 0 \\ 3 & 0 \end{smallmatrix}\right]$.
10. Določi podkolobar kolobarja $\mathbb{C}$, generiran z elementom $3i$.
11. Določi podkolobar kolobarja $\mathbb{C}$, generiran z elementoma $5-6i$ in $2+15i$.
12. Pokaži, da je množica vseh realnih polinomov p z lastnostjo $p(0) = p(1)$ podalgebra algebre vseh realnih polinomov $\mathcal{P}$. Poišči kako končno množico, ki jo generira.
13. Pokaži, da je vsak neničeln element x končno-razsežne algebre A bodisi delitelj niča bodisi obrnljiv. Pokaži tudi, da obrnljivost x sledi že iz obstoja levega ali desnega inverza.

    Namig. Če je dimenzija A enaka n, so elementi $1, x, \ldots, x^n$ linearno odvisni.
14. Določi podpolje polja $\mathbb{R}$, generirano z elementoma $\sqrt{2}$ in $\sqrt{3}$.

15. Določi podpolje polja $\mathbb{R}$, generirano z elementom $\sqrt[3]{2}$.

Komentar. Z znanjem iz poglavja 7 bi zadnji nalogi rešili brez računanja. Toda zaenkrat se naslanjamo le na definicije in elementarna opažanja.

1.8. Direktni produkti in vsote

V algebri poznamo veliko konstrukcij, s katerimi iz danih grup, kolobarjev itd. dobimo nove. V tem razdelku se bomo seznanili z najenostavnejšimi izmed njih, nekakšnimi konstrukcijami »na prvo žogo«.

1.8.1. Direktni produkt grup. Naj bodo $G_1, \ldots, G_m$ grupe. Njihov kartezični produkt $G_1 \times \cdots \times G_m$ postane grupa, če definiramo operacijo (množenje) na naraven način:

$$(x_1, \ldots, x_m)(y_1, \ldots, y_m) := (x_1 y_1, \ldots, x_m y_m)$$

za vse $x_i, y_i \in G_i$, $i = 1, \ldots, m$. Res: asociativnost vpeljanega množenja sledi iz asociativnosti množenj v posameznih grupah, element $(1, \ldots, 1)$ je enota, inverz elementa $(x_1, \ldots, x_m)$ pa element $(x_1^{-1}, \ldots, x_m^{-1})$. Morda opozorimo, da smo z istim simbolom 1 označili enote različnih grup. Če bi enoto grupe G bolj nedvoumno označili z 1_G, bi zapisali

$$1_{G_1 \times \cdots \times G_m} = (1_{G_1}, \ldots, 1_{G_m}).$$

Je pa tako označevanje precej zamudno in včasih nepregledno, zato se mu raje odpovejmo. Le zavedati se moramo, da simbol 1 v algebri lahko označuje različne stvari. Podobno je s simbolom 0. Pomen moramo razbrati iz konteksta.

Množico $G_1 \times \cdots \times G_m$, opremljeno z vpeljano operacijo (torej z množenjem »po komponentah«) imenujemo **direktni produkt grup** $G_1, \ldots, G_m$. Kadar govorimo o grupi $G_1 \times \cdots \times G_m$, imamo praviloma v mislih to operacijo.

Direktni produkti grup ohranjajo različne lastnosti grup. Denimo, direktni produkt Abelovih grup je očitno Abelova grupa, direktni produkt končnih grup je končna grupa.

Če so G_i aditivne grupe, spremenimo tako oznake kot terminologijo. Namesto izraza direktni produkt grup uporabljamo izraz **direktna vsota grup**, namesto $G_1 \times \cdots \times G_m$ pišemo $G_1 \oplus \cdots \oplus G_m$, operacijo pa seveda označujemo s $+$. Zgornja definicija se tako glasi

$$(x_1, \ldots, x_m) + (y_1, \ldots, y_m) := (x_1 + y_1, \ldots, x_m + y_m).$$

Za tak zapis in tako terminologijo se pač dogovorimo v tej knjigi. Navade so namreč različne. Nekateri oznako $G_1 \oplus \cdots \oplus G_m$ uporabljajo tudi za direktni produkt nekomutativnih grup, drugi pa tudi za aditivne grupe uporabljajo oznako $G_1 \times \cdots \times G_m$.

Vpeljanim direktnim produktom oziroma vsotam grup bolj natančno pravimo **zunanji** direktni produkti oziroma vsote. Kasneje, v razdelku 4.5, bomo spoznali še notranje. Kot bomo videli, pa je razlika med obema pojmoma predvsem formalna.

1.8.2. Direktni produkt kolobarjev. Po vpeljavi direktnega produkta grup ni težko uganiti, kako definiramo direktne produkte (ali vsote) drugih algebrskih struktur. **Direktni produkt kolobarjev** $K_1, \ldots, K_m$ je tako množica $K_1 \times \cdots \times K_m$ skupaj z operacijama

$$(x_1, \ldots, x_m) + (y_1, \ldots, y_m) := (x_1 + y_1, \ldots, x_m + y_m)$$

in

$$(x_1, \ldots, x_m)(y_1, \ldots, y_m) := (x_1 y_1, \ldots, x_m y_m).$$

Zlahka preverimo, da je to kolobar z ničelnim elementom $0 = (0, \ldots, 0)$ in enoto $1 = (1, \ldots, 1)$. Podobno kot pri grupah so tudi pri kolobarjih različne navade glede oznak in terminologije. Nekateri vpeljani kolobar označujejo s $K_1 \oplus \cdots \oplus K_m$ in mu pravijo direktna vsota kolobarjev $K_1, \ldots, K_m$. A raje ostanimo pri izrazu direktni produkt.

Če so K_i neničelni kolobarji, ima $K_1 \times \cdots \times K_m$ delitelje niča. Na primer produkt elementov $(x_1, 0, \ldots, 0)$ in $(0, x_2, 0, \ldots, 0)$ je enak 0.

1.8.3. Direktna vsota vektorskih prostorov. Naj bodo $V_1, \ldots, V_m$ vektorski prostori nad poljem F. Njihov kartezični produkt $V_1 \times \cdots \times V_m$ skupaj z operacijama

$$\begin{aligned}(u_1, \ldots, u_m) + (v_1, \ldots, v_m) &:= (u_1 + v_1, \ldots, u_m + v_m),\\ \lambda(v_1, \ldots, v_m) &:= (\lambda v_1, \ldots, \lambda v_m)\end{aligned}$$

je vektorski prostor nad F. Imenujemo ga **(zunanja) direktna vsota prostorov** $V_1, \ldots, V_m$ in ga označujemo z $V_1 \oplus \cdots \oplus V_m$. Vektorski prostor F^m torej lahko opredelimo kot direktno vsoto m kopij prostora F.

1.8.4. Direktni produkt algeber. Algebre so hkrati kolobarji in vektorski prostori. **Direktni produkt algeber** $A_1, \ldots, A_m$ nad poljem F tako definiramo kot množico $A_1 \times \cdots \times A_m$ skupaj z operacijami

$$\begin{aligned}(x_1, \ldots, x_m) + (y_1, \ldots, y_m) &:= (x_1 + y_1, \ldots, x_m + y_m),\\ (x_1, \ldots, x_m)(y_1, \ldots, y_m) &:= (x_1 y_1, \ldots, x_m y_m),\\ \lambda(x_1, \ldots, x_m) &:= (\lambda x_1, \ldots, \lambda x_m).\end{aligned}$$

Seveda s tem $A_1 \times \cdots \times A_m$ postane algebra nad F.

In direktni produkt polj? Polja so kolobarji, zato o njihovem direktnem produktu seveda lahko govorimo. Vendar pa dobljeni kolobar ni polje, saj ima delitelje niča. Zato direktni produkt polj vsaj v teoriji polj nima pomena.

Kot smo že nekajkrat omenili, je le-ta v marsičem drugačna od teorij drugih algebrskih struktur.

V zgornjih definicijah smo se zaradi enostavnosti omejili na direktne produkte in vsote končnega števila objektov. Lahko bi vzeli tudi neskončno družino grup, kolobarjev itd. in v njihov kartezični produkt vpeljali operacije tako kot zgoraj. Za zgled si oglejmo tale primer.

PRIMER 1.89. Polje $\mathbb{R}$ interpretirajmo kot algebro nad samim seboj. Direktni produkt štev no neskončno mnogo kopij algebre $\mathbb{R}$ je kot množica kartezični produkt $\mathbb{R}\times\mathbb{R}\times\dots$, ki jo lahko poistovetimo z množico vseh realnih zaporedij. Operacije v tej algebri so definirane takole:

$$\begin{aligned}(x_1, x_2, \dots) + (y_1, y_2, \dots) &:= (x_1 + y_1, x_2 + y_2, \dots),\\ (x_1, x_2, \dots)(y_1, y_2, \dots) &:= (x_1y_1, x_2y_2, \dots),\\ \lambda(x_1, x_2, \dots) &:= (\lambda x_1, \lambda x_2, \dots).\end{aligned}$$

Torej gre za običajno računanje z zaporedji, ki ga poznamo iz matematične analize.

Naloge

1. Naj bodo $G_1, \dots, G_m$ končno generirane grupe. Pokaži, da je tudi njihov direktni produkt $G_1 \times \cdots \times G_m$ končno generirana grupa.
2. Pokaži, da za poljubne grupe $G_1, \dots, G_m$ velja
$$Z(G_1 \times \cdots \times G_m) = Z(G_1) \times \cdots \times Z(G_m),$$
torej da je center direktnega produkta enak direktnemu produktu centrov. Podobno za poljubne kolobarje $K_1, \dots, K_m$ velja
$$Z(K_1 \times \cdots \times K_m) = Z(K_1) \times \cdots \times Z(K_m).$$
3. Množico B imenujemo **baza** Abelove grupe $(G, +)$, če ima naslednji lastnosti:
   - za vsak $x \in G$ obstajajo taki elementi $b_1, \dots, b_k \in B$ in taka cela števila $n_1, \dots, n_k$, da je $x = n_1b_1 + \cdots + n_kb_k$,
   - za vse (različne) $b_1, \dots, b_k \in B$ in vsa cela števila $n_1, \dots, n_k$ iz $n_1b_1 + \cdots + n_kb_k = 0$ sledi $n_i = 0$ za vse i.

   Definicija je torej enaka definiciji baze vektorskih prostorov, le vlogo polja skalarjev nadomesti kolobar celih števil $\mathbb{Z}$. Vendar pa imajo le redke Abelove grupe bazo. Takim pravimo **proste Abelove grupe**.
   (a) Pokaži, da je grupa $\mathbb{Z}^m := \mathbb{Z} \oplus \cdots \oplus \mathbb{Z}$, tj. direktna vsota m kopij grupe $(\mathbb{Z}, +)$, prosta in poišči vse njene baze.
   (b) Pokaži, da končna Abelova grupa ne more biti prosta.
   (c) Ali je grupa $(\mathbb{Q}, +)$ prosta?

4. Naj bosta G_1 in G_2 grupi in naj bo p praštevilo. Pokaži, da grupa $G_1 \times G_2$ vsebuje element reda p (gl. nalogo 1.3/7) natanko tedaj, ko vsaj ena izmed grup G_1 in G_2 vsebuje element reda p. Ali to velja tudi, kadar p ni praštevilo?
5. Naj bo H_i podgrupa grupe G_i, $i = 1, \ldots, m$. Hitro vidimo, da je potem $H_1 \times \cdots \times H_m$ podgrupa grupe $G_1 \times \cdots \times G_m$. Ni pa nujno vsaka podgrupa grupe $G_1 \times \cdots \times G_m$ take oblike. Poišči drugačen primer (za kake konkretne grupe G_i).
6. Določi podkolobar kolobarja $\mathbb{Z} \times \mathbb{Z}$, generiran z elementom $(1, -1)$.
7. Določi podkolobar kolobarja $\mathbb{R} \times \mathbb{Z}$, generiran z elementom $(\sqrt{2}, 0)$.
8. Naj bo F polje. Opiši vse podprostore algebre $F^2 := F \times F$. Kateri izmed njih so podalgebre? Morda je še laže odgovoriti na splošnejše vprašanje: katere podmnožice 2-razsežne algebre so podalgebre?
9. Označimo z e konstantno zaporedje samih enic, z e_n, kjer je $n \in \mathbb{N}$, pa zaporedje, katerega n-ti člen je enak 1, vsi drugi členi pa so enaki 0. Pokaži, da je linearna lupina množice $\{e, e_1, e_2, \ldots\}$ – torej množica vseh zaporedij, ki so od nekega člena dalje konstantna – podalgebra algebre vseh zaporedij iz primera 1.89. Ali je kot algebra končno generirana?

POGLAVJE 2

Primeri grup in kolobarjev

Primeri v matematiki in še posebej v algebri niso pomembni le zato, ker nam pomagajo razumeti teorijo. Abstraktno teorijo praviloma razvijamo zaradi različnih primerov, ki bi jih radi bolje razumeli in jih obravnavali na poenoten način. Resda se matematična teorija čez čas lahko oddalji od izvora, se osamosvoji in začnemo jo dojemati kot zanimivo in dragoceno samo po sebi. Toda tudi takrat je eden izmed njenih bistvenih ciljev uporabnost na konkretnih primerih; morda ne le teh, iz katerih se je porodila.

To poglavje je namenjeno pregledu nekaterih najpomembnejših primerov grup in kolobarjev ter algeber. Tudi vektorski prostori in polja se bodo naravno vpletali v našo razpravo.

Če za izhodišče postavimo števila, se primeri kolobarjev ponujajo prej kot primeri grup. Seveda pa je vsak kolobar tudi grupa za seštevanje, grupo pa tvori tudi množica njegovih obrnljivih elementov. Tako se bodo primeri grup in kolobarjev med seboj prepletali. Primerom grup, ki niso neposredno povezane s kolobarji, se bomo posvetili na koncu poglavja.

Eden izmed ciljev poglavja je pokazati, da se grupe in kolobarji pojavljajo vsepovsod v matematiki. Srečati jih ni težko, le prepoznati jih moramo.

2.1. Grupa in kolobar celih števil

Z naravnimi števili se seznanimo zelo zgodaj in na intuitivni ravni z njihovim razumevanjem nimamo težav. Zato njihovo formalno definicijo izpustimo. Tudi za *načelo matematične indukcije* domnevamo, da ne potrebuje razlage. Omenimo še *načelo dobre urejenosti*, ki pravi, da vsaka neprazna podmnožica množice $\mathbb{N}$ vsebuje najmanjše število. Povejmo drugače: če je S podmnožica $\mathbb{N}$, v kateri nobeno število ni najmanjše, potem je S prazna množica, torej $n \notin S$ za vsako naravno število n. Dokaz z indukcijo na n je enostaven. Res, S očitno ne vsebuje 1, in iz predpostavke, da S ne vsebuje števil $1, 2, \ldots n$, očitno sledi, da S ne vsebuje števila $n+1$. Načelo dobre urejenosti seveda velja tudi za neprazne podmnožice $\mathbb{N} \cup \{0\}$. V dokazu moramo samo 1 zamenjati z 0. Prav tako velja za neprazne podmnožice

$$\mathbb{N} \cup \{-1, 0\},\ \mathbb{N} \cup \{-2, -1, 0\}\ \text{ itd.}$$

Kako bi jasneje opredelili vse take podmnožice? To so natanko tiste podmnožice množice $\mathbb{Z}$, ki so *navzdol omejene*. Bralec ta pojem najbrž pozna: za množico $S \subseteq \mathbb{Z}$ rečemo, da je navzdol omejena, če obstaja tak $a \in \mathbb{Z}$, da je $a \leq s$ za vse $s \in S$. Z obratno neenakostjo definiramo *navzgor omejeno* podmnožico, ki ima seveda analogne lastnosti. Zapišimo načelo dobre urejenosti za oba tipa množic:

(a) vsaka neprazna navzdol omejena podmnožica množice $\mathbb{Z}$ vsebuje najmanjše število;
(b) vsaka neprazna navzgor omejena podmnožica množice $\mathbb{Z}$ vsebuje največje število.

Množica naravnih števil je za seštevanje »samo« polgrupa. Zato v algebri raje obravnavamo množico celih števil, ki je za seštevanje grupa, če jo opremimo še z množenjem, pa postane kolobar. Tudi če nas zanima problem o naravnih številih, ga je z algebraičnimi sredstvi pogosto bolj udobno reševati za cela števila.

Opozorimo, da bomo skozi vso knjigo cela števila včasih obravnavali kot grupo za seštevanje, včasih kot kolobar, ponekod pa tudi samo kot množico brez algebraičnega pomena. Morebitnim dvoumnostim se sicer lahko izognemo z uporabo oznak $(\mathbb{Z}, +)$ oziroma $(\mathbb{Z}, +, \cdot)$. Vendar bomo največkrat pisali samo $\mathbb{Z}$ in razbrali iz vsebine, katero vlogo celih števil imamo v mislih.

Pričnimo z izrekom, iz katerega bodo vsi drugi sledili. Imenuje se **osnovni izrek o deljenju**.

Izrek 2.1. *Za vsaki števili $m \in \mathbb{Z}$ in $n \in \mathbb{N}$ obstajata taki števili $q, r \in \mathbb{Z}$, da je*

$$m = qn + r \quad in \quad 0 \leq r < n.$$

Dokaz. Za dovolj veliko število ℓ je $\ell n > m$. Tako število ℓ je večje od vsakega števila iz množice

$$S := \{k \in \mathbb{Z} \mid kn \leq m\}.$$

To pomeni, da je množica S navzgor omejena. Seveda je tudi neprazna, saj bi sicer $kn > m$ veljalo za vsa, tudi negativna cela števila k. Zato v S obstaja največje število q (gl. (b) zgoraj). Število $q + 1$ potem ni v S. Torej je

$$qn \leq m < (q + 1)n = qn + n.$$

Število $r := m - qn$ tako zadošča $0 \leq r < n$. □

Število r imenujemo **ostanek** pri deljenju m z n. Omenimo še, da sta števili q in r enolično določeni. Dokaz je enostaven in ga prepuščamo bralcu.

S pomočjo izreka 2.1 ni težko poiskati vseh podgrup grupe $(\mathbb{Z}, +)$. Najprej vpeljimo oznako

$$n\mathbb{Z} := \{nx \mid x \in \mathbb{Z}\}.$$

Tu je n poljubno celo število. Ker pa je $n\mathbb{Z} = (-n)\mathbb{Z}$, običajno izberemo nenegativno število.

Posledica 2.2. *Podmnožica H grupe $\mathbb{Z}$ je podgrupa za seštevanje natanko tedaj, ko je $H = n\mathbb{Z}$ za neki $n \in \mathbb{N} \cup \{0\}$.*

Dokaz. Množica $n\mathbb{Z}$ je očitno zaprta za seštevanje in vsebuje nasprotne elemente svojih elementov. Torej je podgrupa.

Pri dokazovanju obratne trditve imejmo v mislih, da je izmed vseh naravnih števil v $n\mathbb{Z}$, kjer je $n \geq 1$, najmanjše prav število n. Vzemimo poljubno podgrupo H grupe $\mathbb{Z}$. Če je $H = \{0\}$, jo zapišemo kot $H = n\mathbb{Z}$ za $n = 0$. Naj bo torej $H \neq \{0\}$. Ker H vsebuje nasprotne elemente svojih elementov, je

$$H \cap \mathbb{N} \neq \emptyset.$$

Označimo z n najmanjše število v $H \cap \mathbb{N}$ (gl. (a) zgoraj). Iz $n \in H$ sledi $-n \in H$, iz obojega pa zlahka izpeljemo $n\mathbb{Z} \subseteq H$. Dokazati moramo še obratno inkluzijo. Vzemimo $m \in H$. Po izreku 2.1 obstajata taka $q, r \in \mathbb{Z}$, da je

$$r = m - qn \text{ in } 0 \leq r < n.$$

Ker sta m in qn elementa podgrupe H, v H leži tudi r. Iz $r < n$ zato sledi, da r ni naravno število, saj smo n izbrali kot najmanjše naravno število iz H. Torej je $r = 0$ in zato $m = qn \in n\mathbb{Z}$. □

Trivialno podgrupo $\{0\}$ dobimo pri $n = 0$, celo grupo $\mathbb{Z}$ pa pri $n = 1$. Vsaka prava netrivialna podgrupa $(\mathbb{Z}, +)$ torej sestoji iz celoštevilskih večkratnikov nekega naravnega števila $n \geq 2$. Denimo,

$$2\mathbb{Z} = \{0, \pm 2, \pm 4, \dots\}$$

vsebuje vse večkratnike števila 2, torej vsa soda cela števila. Podgrupa $n\mathbb{Z}$ je očitno generirana s številom n. Zato lahko posledico 2.2 povemo tudi takole: vse podgrupe grupe $(\mathbb{Z}, +)$ so generirane z enim samim elementom. V nadaljevanju bomo ilustrirali uporabnost tega rezultata, in s tem abstraktnega algebraičnega pristopa, pri temi iz elementarne matematike.

Pravimo, da celo število $k \neq 0$ **deli** celo število n, če je $n = qk$ za neko celo število q. V tem primeru pišemo

$$k \mid n.$$

Rečemo tudi, da je k **delitelj** n ali da je n **deljiv** s k. Če k ne deli n, pišemo $k \nmid n$. Seveda $k \mid 0$ za vsak $k \neq 0$, medtem ko $k \nmid 1$, razen če je $k = 1$ ali $k = -1$. Očitno $1 \mid n$ in $-1 \mid n$ za vsak $n \in \mathbb{Z}$.

Naj bosta m in n celi števili. Vsaj eno naj bo različno od 0. Številu $k \neq 0$, ki deli tako m kot n, pravimo **skupni delitelj** m in n. Naravno število d, ki je skupni delitelj števil m in n in je deljivo z vsakim drugim skupnim deliteljem m in n, se imenuje **največji skupni delitelj** m in n. Očitno je s temi pogoji

d enolično določen. Toda ali sploh obstaja? Na to vprašanje bomo odgovorili s pomočjo posledice 2.2 in naslednjega razmisleka o podgrupah Abelovih grup.

Naj bosta H in K podgrupi aditivne (in zato po našem dogovoru Abelove) grupe G. Potem je tudi množica

$$H + K := \{h + k \mid h \in H, k \in K\}$$

podgrupa G. Res, iz zapisa

$$(h + k) - (h' + k') = (h - h') + (k - k')$$

vidimo, da razlika dveh elementov iz $H + K$ leži v $H + K$. Tako je

$$m\mathbb{Z} + n\mathbb{Z} = \{mx + ny \mid x, y \in \mathbb{Z}\}$$

podgrupa $\mathbb{Z}$.

Posledica 2.3. *Vsak par celih števil m in n, od katerih vsaj eno ni enako 0, ima največji skupni delitelj d. Lahko ga zapišemo v obliki $d = mx + ny$ za neka $x, y \in \mathbb{Z}$.*

Dokaz. Ker je $m\mathbb{Z} + n\mathbb{Z}$ podgrupa grupe $(\mathbb{Z}, +)$, po posledici 2.2 obstaja tak $d \in \mathbb{N} \cup \{0\}$, da je

$$d\mathbb{Z} = m\mathbb{Z} + n\mathbb{Z}.$$

Seveda $d \neq 0$, saj $m \neq 0$ ali $n \neq 0$. Ker $d \in d\mathbb{Z}$, ga torej lahko zapišemo kot $d = mx + ny$ za neka $x, y \in \mathbb{Z}$. Od tod vidimo, da je d deljiv z vsakim skupnim deliteljem c števil m in n; namreč, iz $m = cz$ in $n = cw$ sledi $d = c(zx + wy)$. Toda zakaj je d skupni delitelj? Iz

$$m \in m\mathbb{Z} \subseteq m\mathbb{Z} + n\mathbb{Z} = d\mathbb{Z}$$

sledi, da $d \mid m$. Podobno vidimo, da $d \mid n$. □

Posledico 2.3 lahko dokažemo tudi brez omembe grup. Navsezadnje jo lahko izluščimo iz slovite *Evklidove* knjige *Elementi* izpred treh stoletij pred našim štetjem, torej dobri dve tisočletji pred vpeljavo pojma grupe. Naš glavni namen je bil na preprostem primeru ponazoriti učinkovitost abstraktne algebre. Kasneje bomo isto metodo dokazovanja uporabili v bistveno splošnejši situaciji.

Opomba 2.4. Vzemimo naravni števili m in n. Z zaporedno uporabo izreka 2.1 dobimo

$$\begin{aligned} m &= q_1 n + r_1, & 0 < r_1 < n, \\ n &= q_2 r_1 + r_2, & 0 < r_2 < r_1, \\ r_1 &= q_3 r_2 + r_3, & 0 < r_3 < r_2, \\ &\vdots \\ r_{k-2} &= q_k r_{k-1} + r_k, & 0 < r_k < r_{k-1}, \\ r_{k-1} &= q_{k+1} r_k + 0. \end{aligned}$$

Slej ko prej se namreč deljenje mora iziti, saj vsak naslednji ostanek r_i manjši od prejšnjega. Zadnja enakost pove, da $r_k \mid r_{k-1}$, iz predzadnje tako sledi $r_k \mid r_{k-2}$ itd. Na koncu ugotovimo, da $r_k \mid n$ in $r_k \mid m$, torej je r_k skupni delitelj m in n. Naj bo sedaj r poljuben skupni delitelj teh dveh števil. Iz prve enakosti razberemo, da $r \mid r_1$, iz druge sledi $r \mid r_2$ itd. Naposled ugotovimo, da $r \mid r_k$. Torej je r_k največji skupni delitelj števil m in n.

Tudi ta postopek za iskanje največjega skupnega delitelja para števil je predstavljen že v Evklidovih *Elementih*. Imenujemo ga **Evklidov algoritem**.

Za celi števili m in n, ne obe enaki 0, pravimo, da sta si **tuji**, če je njun največji skupni delitelj enak 1.

Posledica 2.5. *Celi števili m in n sta si tuji natanko tedaj, ko obstajata taki celi števili x in y, da je $mx + ny = 1$.*

Dokaz. Iz $mx + ny = 1$ očitno sledi, da nobeno naravno število večje od 1 ni skupni delitelj m in n, torej je 1 njun največji skupni delitelj. Obrat razberemo iz posledice 2.3. □

Opomba 2.6. Na enak način kot za dve števili definiramo največji skupni delitelj več celih števil $n_1, \ldots, n_k \in \mathbb{Z}$, ki niso vsa 0. Za dokaz obstoja moramo samo slediti dokazu posledice 2.3. Ob tem ugotovimo, da lahko največji skupni delitelj d zapišemo v obliki $d = n_1 x_1 + \cdots + n_k x_k$ za neke $x_i \in \mathbb{Z}$. Kadar je $d = 1$, rečemo, da so si števila $n_1, \ldots, n_k$ tuja. Kot v dokazu posledice 2.5 vidimo, da so si ta števila tuja natanko tedaj, ko je $n_1 x_1 + \cdots + n_k x_k = 1$ za neke $x_i \in \mathbb{Z}$. Omenimo še, da iz tujosti $n_1, \ldots, n_k$ še ne sledi, da so si ta števila paroma tuja. Na primer, števila $2, 3, 6$ so si tuja, a ne paroma tuja.

Naravno število p je **praštevilo**, če $p \neq 1$ in če sta 1 in p edini naravni števili, ki ga delita. Tudi naslednja posledica je bila znana že Evklidu.

Posledica 2.7. *Naj bo p praštevilo in m, n naravni števili. Če $p \mid mn$, potem $p \mid m$ ali $p \mid n$.*

Dokaz. Denimo, da $p \nmid m$. Ker je p praštevilo, sta si potem števili p in m tuji. Posledica 2.5 pove, da je $px + my = 1$ za neki celi števili x in y. Z množenjem te enakosti z n dobimo $pxn + mny = n$. Ker je po predpostavki $mn = cp$ za neki $c \in \mathbb{N}$, sledi $p(xn + cy) = n$ in zato $p \mid n$. □

Naslednjemu izreku pravimo **osnovni izrek aritmetike**. Bralcu gotovo ni neznan. Svetujemo mu, da se pred branjem dokaza vpraša, ali zna vsaj prvo trditev izreka, tj. da je vsako od 1 različno naravno število produkt praštevil, dokazati sam. Še pojasnilo: po dogovoru tudi za vsako praštevilo p rečemo, da je enako produktu praštevil. V tem produktu pač nastopa en sam faktor, praštevilo p samo.

Izrek 2.8. *Vsako naravno število $n > 1$ lahko zapišemo kot produkt praštevil. Ta zapis je enoličen do vrstnega reda faktorjev natančno.*

Dokaz. Prvo trditev dokažimo z indukcijo na n. Za $n = 2$ je očitna, zato smemo privzeti, da je $n > 2$ in da je vsako naravno število, ki je večje od 1 in manjše od n, enako produktu praštevil. Če je n samo praštevilo, ni kaj dokazovati. Naj bo torej $n = rs$, kjer je $1 < r, s < n$. Po predpostavki sta števili r in s enaki produktu praštevil. Potem pa isto velja za n.

Dokažimo še enoličnost. Zapišimo n kot produkt praštevil na dva načina,

$$n = p_1 p_2 \cdots p_s \quad \text{in} \quad n = q_1 q_2 \cdots q_t.$$

Ker je p_1 praštevilo in deli $q_1 q_2 \cdots q_t$, iz posledice 2.7 sledi, da p_1 deli q_1 ali $q_2 \cdots q_t$. V drugem primeru deli q_2 ali $q_3 \cdots q_t$ itd. Naposled ugotovimo, da p_1 deli vsaj eno izmed števil q_i. Ker je vrstni red faktorjev za nas nepomemben, smemo privzeti, da p_1 deli q_1. Toda tudi q_1 je praštevilo, zato je to možno le tedaj, ko je $p_1 = q_1$. Torej je

$$p_1 p_2 \cdots p_s = p_1 q_2 \cdots q_t.$$

S krajšanjem p_1 dobimo

$$p_2 \cdots p_s = q_2 \cdots q_t.$$

Zgornji razmislek lahko zdaj ponovimo in ugotovimo, da smemo brez škode za splošnost privzeti, da je $p_2 = q_2$. Tako nadaljujemo. Če bi bila s in t različna, npr. če bi bil s večji kot t, bi na koncu prišli do enakosti $p_{t+1} \cdots p_s = 1$, kar je protislovje. Torej je $s = t$ in oba zapisa sta enaka. □

V zapisu $n = p_1 p_2 \cdots p_s$ so nekatera izmed praštevil p_i seveda lahko med seboj enaka (npr. $4 = 2 \cdot 2$). Lahko pišemo tudi takole:

$$n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r},$$

kjer so p_i različna praštevila, k_i pa (enolično določena) naravna števila.

V algebri pogosto poskušamo objekte, ki jih obravnavamo, razstaviti na nerazstavljive objekte. Osnovni izrek aritmetike pove, da se to da doseči za elemente kolobarja celih števil. Kasneje bomo izrek razširili na precej splošnejše kolobarje.

Zaključimo razdelek s še enim klasičnim izrekom in Evklidovem brezčasnim dokazom.

Izrek 2.9. *Praštevil je neskončno mnogo.*

Dokaz. Denimo, da je praštevil končno mnogo. Označimo njihovo število z n. Naj bodo $p_1, p_2, \ldots, p_n$ edina praštevila. Oglejmo si število

$$p_1 p_2 \cdots p_n + 1.$$

Po izreku 2.8 obstaja praštevilo p_j, ki ga deli. Torej je

$$p_j q = p_1 p_2 \cdots p_n + 1$$

za neko naravno število q. Zapišemo to enakost v obliki

$$p_j(q - p_1 \cdots p_{j-1} p_{j+1} \cdots p_n) = 1.$$

Toda to je protislovje, saj število 1 ne more biti deljivo s praštevilom p_j. □

Ljudje se s praštevili ukvarjamo že zelo dolgo. Kljub temu je več problemov o praštevilih z zelo enostavno formulacijo, razumljivo že srednješolcem, še vedno odprtih. Omenimo dva posebej znamenita. **Goldbachova domneva** pravi, da lahko z izjemo števila 2 vsako sodo naravno število zapišemo kot vsoto dveh praštevil. **Domneva o praštevilskih dvojčkih** pravi, da obstaja neskončno mnogo takih praštevil p, da je tudi $p+2$ praštevilo. Morda pa bomo še za časa naših življenj izvedeli, če je katera izmed teh domnev resnična.

Naloge

1. Vrni se k nalogi 1.7/5. Jo je sedaj laže rešiti?
2. Naj bosta m in n naravni števili. Po osnovnem izreku aritmetike obstajajo taka različna praštevila $p_1, \ldots, p_r$ in taka nenegativna cela števila $k_1, \ldots, k_r$ in $\ell_1, \ldots, \ell_r$, da je $m = p_1^{k_1} \cdots p_r^{k_r}$ in $n = p_1^{\ell_1} \cdots p_r^{\ell_r}$. Izrazi največji skupni delitelj števil m in n s pomočjo p_i, k_i in ℓ_i. Podobno izrazi *najmanjši skupni večkratnik* števil m in n, torej najmanjše naravno število, ki je deljivo tako z m kot z n.
3. Izpelji posledico 2.3 s pomočjo Evklidovega algoritma.
4. Naj bo a element grupe G. Denimo, da obstajata taki tuji si celi števili m in n, da je $a^m = a^n = 1$. Pokaži, da je $a = 1$.
5. Naj bo G grupa, H njena podgrupa in a element iz G. Denimo, da je $a^m = 1$ za neki $m \in \mathbb{Z}$ in da je n najmanjše naravno število z lastnostjo $a^n \in H$. Pokaži, da $n \mid m$.

6. Poišči vsa taka praštevila p, da je število $7p + 4$ kvadrat kakega naravnega števila.
7. Praštevilo se imenuje **Mersennovo praštevilo**, če je oblike $2^p - 1$ za neko naravno število p. Pokaži, da je tedaj tudi p praštevilo in da ima število $n = 2^{p-1}(2^p - 1)$ lastnost, da je vsota vseh njegovih deliteljev enaka $2n$.
8. Označimo s P_m množico vseh praštevil, ki so kvečjemu manjša od števila $m \geq 2$. Dokaži, da je

$$\prod_{p \in P_m} \frac{1}{1 - \frac{1}{p}} \geq \sum_{n=1}^{m} \frac{1}{n}$$

in od tod izpelji, da je praštevil neskončno mnogo (tu je $\prod$ znak za produkt).

Namig. Geometrijska vrsta.

9. Pokaži, da obstaja neskončno praštevil, ki imajo pri deljenju s 4 ostanek 3.

Namig. Predpostavi, da so $p_1, \ldots, p_n$ edina taka števila in opazuj število $4p_1 \cdots p_n - 1$.

10. Pokaži, da za vsako naravno število n obstaja n zaporednih naravnih števil, od katerih nobeno ni praštevilo.

Namig. Za katero število a nobeno izmed števil $a+2, a+3, \ldots, a+(n+1)$ ni praštevilo?

2.2. Grupa in kolobar ostankov

Zamislimo si večer, ura je odbila sedem. Koliko bo čez štiri ure? Odgovor je seveda enajst, saj je $7 + 4 = 11$. Koliko pa bo čez šest ur? Takrat bo ura ena in do odgovora smo prav tako prišli s seštevanjem, čeprav vsota celih števil 7 in 6 ni enaka 1. Seštevali namreč nismo v grupi $\mathbb{Z}$, pač pa v grupi $\mathbb{Z}_{12}$. Pojasnimo!

Naj bo n naravno število. Pravimo, da sta celi števili a in b **kongruentni po modulu** n, če $n \mid (a - b)$. V tem primeru pišemo

$$a \equiv b \pmod{n}.$$

Na primer, $13 \equiv 1 \pmod{12}$ in $21 \equiv -3 \pmod{12}$. Definicijo lahko povemo tudi takole: a in b sta kongruentni po modulu n, če imata pri deljenju z n isti ostanek.

Na kongruentnost lahko gledamo kot na relacijo na množici celih števil. Števili a in b sta v relaciji, če je $a \equiv b \pmod{n}$. Refleksivnost in simetričnost

te relacije sta očitni, pa tudi tranzitivnost zlahka preverimo: če n deli $a-b$ in $b-c$, potem n deli tudi

$$a-c=(a-b)+(b-c).$$

Kongruentnost po modulu n je torej *ekvivalenčna relacija*. Označimo z $[a]$ ekvivalenčni razred, ki mu pripada $a\in\mathbb{Z}$. Seveda je

$$[a]=[a']\iff a\equiv a' \pmod{n}.$$

V ekvivalenčnem razredu $[0]$ so vsa cela števila, ki so z n deljiva, v $[1]$ so cela števila, ki imajo pri deljenju z n ostanek 1 itd. Množico vseh ekvivalenčnih razredov označimo z $\mathbb{Z}_n$. Ima n elementov, namreč

$$\mathbb{Z}_n=\{[0],[1],\dots,[n-1]\}.$$

Množico $\mathbb{Z}_n$ bomo sedaj opremili z operacijama seštevanja in množenja. Pri tem se bomo prvič soočili s problemom **dobre definiranosti**. Ta problem se pojavi, kadar definiramo preslikavo ali operacijo na množici, v kateri lahko elemente zapisujemo na različne načine. Pojasnimo s primerom.

Primer 2.10. Definirajmo preslikavo $f:\mathbb{Q}\to\mathbb{Q}$ s predpisom

$$f\Big(\frac{r}{s}\Big)=\frac{r^2}{s^2}.$$

To je seveda preslikava, ki vsakem številu priredi njegov kvadrat, torej $f(x)=x^2$ za vse $x\in\mathbb{Q}$. Malce spremenimo predpis in definirajmo

$$\mathcal{F}\Big(\frac{r}{s}\Big)=\frac{r^2}{s}.$$

Če nismo pozorni, se nam tudi ta definicija zdi nedvoumna. Toda koliko je na primer $\mathcal{F}(0.5)$? Ker je $0.5=\frac{1}{2}$, se kot odgovor ponuja $\mathcal{F}(0.5)=\frac{1^2}{2}=0.5$. Toda 0.5 lahko zapišemo na primer tudi kot $\frac{-3}{-6}$, kar vodi do odgovora $\mathcal{F}(0.5)=\frac{(-3)^2}{-6}=-1.5$. Predpis $\mathcal{F}(\frac{r}{s})=\frac{r^2}{s}$ je torej nesmiseln ali, kot rečemo, ni dobro definiran. Z začetnim predpisom $f(\frac{r}{s})=\frac{r^2}{s^2}$ pa ni nič narobe. Če namreč racionalno število x zapišemo na dva načina, enkrat kot $\frac{r}{s}$ in drugič kot $\frac{r'}{s'}$, potem je $rs'=sr'$, iz česar sledi $(rs')^2=(sr')^2$ in zato $\frac{r^2}{s^2}=\frac{r'^2}{s'^2}=x^2$. Za vsako racionalno število x je torej $f(x)=x^2$, neodvisno od izbire zapisa števila x v obliki ulomka.

Tako kot lahko isto racionalno število predstavimo z različnimi ulomki, lahko isti element iz $\mathbb{Z}_n$ (torej ekvivalenčni razred) predstavimo z različnimi celimi števili; velja namreč

$$\dots=[a-n]=[a]=[a+n]=[a+2n]=\dots$$

Če je podano pravilo, ki domnevno definira funkcijo f na $\mathbb{Z}_n$, se moramo prepričati, da iz $[a]=[a']$ sledi $f([a])=f([a'])$. Potem rečemo, da je f

dobro definirana. Podobno mora za binarno operacijo $\star$ na $\mathbb{Z}_n$ veljati, da je $[a] \star [b] = [a'] \star [b']$, kadarkoli je $[a] = [a']$ in $[b] = [b']$.

TRDITEV 2.11. *Če v množico $\mathbb{Z}_n$ vpeljemo seštevanje s predpisom*

$$[a] + [b] := [a + b],$$

postane $\mathbb{Z}_n$ Abelova grupa.

DOKAZ. Najprej moramo preveriti dobro definiranost vpeljane operacije. Dokazati moramo, da iz $[a] = [a']$ in $[b] = [b']$ sledi $[a+b] = [a'+b']$. Z drugimi besedami, iz predpostavk $n \mid a - a'$ in $n \mid b - b'$ moramo izpeljati zaključek

$$n \mid (a + b) - (a' + b').$$

Ker je

$$(a + b) - (a' + b') = (a - a') + (b - b'),$$

to očitno velja.

Asociativnost seštevanja v $\mathbb{Z}_n$ sledi iz asociativnosti seštevanja v $\mathbb{Z}$. Res,

$$\begin{aligned}([a] + [b]) + [c] &= [a + b] + [c] = [(a + b) + c] \\ &= [a + (b + c)] = [a] + [b + c] = [a] + ([b] + [c]).\end{aligned}$$

Podobno velja za komutativnost. Ničelni element v $\mathbb{Z}_n$ je $[0]$, nasprotni element elementa $[a]$ pa je element $[-a]$. □

Grupa $(\mathbb{Z}_n, +)$ je generirana z enim samim elementom, namreč z $[1]$. Torej je tako kot $(\mathbb{Z}, +)$ tudi ta grupa ciklična (gl. primer 1.79). Kasneje bomo videli, da v bistvu ni drugih cikličnih grup kot te.

Aditivna grupa $(\mathbb{Z}_n, +)$ na naraven način postane kolobar.

TRDITEV 2.12. *Če v aditivno grupo $\mathbb{Z}_n$ vpeljemo množenje s predpisom*

$$[a] \cdot [b] := [ab],$$

postane $\mathbb{Z}_n$ komutativen kolobar.

DOKAZ. Tudi sedaj moramo preveriti dobro definiranost operacije. Dokazati moramo, da iz $[a] = [a']$ in $[b] = [b']$ (torej iz $n \mid a - a'$ in $n \mid b - b'$) sledi $[ab] = [a'b']$ (torej $n \mid ab - a'b'$). To pa jasno sledi iz enakosti

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

Asociativnost in komutativnost množenja ter distributivnostni zakon dokažemo podobno, kot smo dokazali asociativnost seštevanja v dokazu trditve 2.11. Enota je element $[1]$. □

Kolobarju $(\mathbb{Z}_n, +, \cdot)$ pravimo **kolobar ostankov po modulu** n, grupi $(\mathbb{Z}_n, +)$ pa **grupa ostankov po modulu** n. Poenostavimo označevanje elementov iz $\mathbb{Z}_n$; namesto $[a]$, kjer je $0 \leq a < n$, bomo pisali kar a. Torej je

$$\mathbb{Z}_n = \{0, 1, \ldots, n-1\}.$$

Čeprav bomo torej elemente $\mathbb{Z}_n$ zapisovali enako kot cela števila, ne smemo pozabiti, da je računanje z njimi drugačno od običajnega. Vsota elementov $a + b$ v $\mathbb{Z}_n$ je ostanek pri deljenju običajne vsote števil $a + b$ z n. Denimo, v $\mathbb{Z}_{12}$ je $7 + 6 = 1$. Podobno je produkt elementov ab v $\mathbb{Z}_n$ enak ostanku pri deljenju običajnega produkta števil ab z n. Na primer, v $\mathbb{Z}_{12}$ je $5 \cdot 7 = 11$ in $3 \cdot 8 = 0$. Kolobar $\mathbb{Z}_n$ ima torej lahko delitelje niča. Če n ni praštevilo, jih pravzaprav zanesljivo ima (zakaj?). In če n je praštevilo? Za začetek si oglejmo najenostavnejši primer, ko je $n = 2$. Kolobar $\mathbb{Z}_2$ ima le dva elementa, 0 in 1. Z njima računamo takole:

$$0 + 0 = 0,\ \ 0 + 1 = 1,\ \ 1 + 0 = 1,\ \ 1 + 1 = 0,$$
$$0 \cdot 0 = 0,\ \ 0 \cdot 1 = 0,\ \ 1 \cdot 0 = 0,\ \ 1 \cdot 1 = 1.$$

V oči bode formula $1 + 1 = 0$, vse drugo je enako kot pri številih. Edini neničelni element je enota 1, ki seveda ni delitelj niča. Še več, ta element je obrnljiv. To pomeni, da je $\mathbb{Z}_2$ polje. Pokazali bomo, da je $\mathbb{Z}_p$ polje za vsako praštevilo p. Pri tem si bomo pomagali z naslednjo lemo, ki je zanimiva sama po sebi. Najprej pa definicija, ki nam bo pomagala pri enostavnejši formulaciji.

Definicija 2.13. Neničeln komutativen kolobar brez deliteljev niča se imenuje **cel kolobar**.

Očiten primer celega kolobarja je vsako polje. Med končnimi kolobarji drugačnih tudi ni.

Lema 2.14. *Končen cel kolobar K je polje.*

Dokaz. Vzemimo poljuben element $a \neq 0$ iz K. Naš cilj je pokazati, da ima enačba $ax = 1$ rešitev. V ta namen si oglejmo preslikavo $x \mapsto ax$ iz K v K. Ker K nima deliteljev niča in zato v K velja pravilo krajšanja, iz $ax = ay$ sledi $x = y$. To pomeni, da je ta preslikava injektivna. Zaradi končnosti množice K je zato tudi surjektivna. V njeni zalogi vrednosti je torej tudi 1, kar dokazuje želeno. □

Kolobar celih števil $\mathbb{Z}$ je najenostavnejši primer neskončnega celega kolobarja, ki ni polje. Več primerov bomo srečali kasneje.

Izkaže se, da lema 2.14 velja tudi brez privzetka o komutativnosti K, vendar bi za dokaz potrebovali več predznanja. S primerno predelavo zgornjega dokaza sicer brez težav ugotovimo, da je neničeln končen kolobar brez deliteljev niča vselej obseg. Bistveno težje pa je dokazati *Wedderburnov izrek* iz leta 1905, ki pravi, da so vsi končni obsegi komutativni.

TRDITEV 2.15. *Naravno število p je praštevilo natanko tedaj, ko je kolobar $\mathbb{Z}_p$ polje.*

DOKAZ. Če p ni praštevilo, je bodisi $\mathbb{Z}_p$ ničelni kolobar (za $p = 1$) bodisi ima $\mathbb{Z}_p$ delitelje niča in zato ni polje. Naj bo p praštevilo. Po lemi 2.14 zadošča dokazati, da $\mathbb{Z}_p$ nima deliteljev niča. Denimo, da $a, b \in \mathbb{Z}_p$ zadoščata $ab = 0$. Če a in b obravnavamo kot celi števili, to pomeni, da je njun običajni produkt (v $\mathbb{Z}$) večkratnik praštevila p. Toda potem $p \mid a$ ali $p \mid b$ (gl. posledico 2.7). Od tod jasno sledi $a = 0$ ali $b = 0$. □

V tem dokazu smo a in b najprej obravnavali kot elementa kolobarja $\mathbb{Z}_p$, nato kot celi števili, na koncu pa spet kot elementa $\mathbb{Z}_p$. Če je bralca to zmedlo, naj na ustreznih mestih a in b zamenja z $[a]$ in $[b]$.

Seznam doslej znanih polj torej lahko dopolnimo z bistveno drugačnimi primeri, končnimi polji $\mathbb{Z}_p$. V razdelku 7.7 bomo opisali vsa končna polja.

Podobno kot $\mathbb{Z}$ bomo tudi $\mathbb{Z}_n$ včasih obravnavali le kot Abelovo grupo, včasih pa kot kolobar. Ker bomo vsakič uporabljali isto oznako in ker povrh elemente iz $\mathbb{Z}_n$ označujemo enako kot cela števila, bo potrebno nekaj pozornosti.

Naloge

1. Določi vsa naravna števila n, za katere je $f : \mathbb{Z}_n \to \mathbb{Z}_n$, $f([a]) = [|a|]$, dobro definirana preslikava.
2. Določi vsa naravna števila n, za katere je $[a] \star [b] = [|ab|]$ dobro definirana binarna operacija na množici $\mathbb{Z}_n$.
3. Poišči vse podgrupe grupe $\mathbb{Z}_6$.
4. Red elementa $a \in \mathbb{Z}_n$ je najmanjše naravno število r, za katerega je $ra = 0$ (gl. nalogo 1.3/7). Poišči red vseh elementov grup $\mathbb{Z}_5$ in $\mathbb{Z}_6$.
5. Za vsak $a \in \mathbb{Z}_{12}$ opiši podgrupo $\langle a \rangle$, tj. podgrupo, generirano z a.
6. Naj $k \mid n$. Pokaži, da ima grupa $\mathbb{Z}_n$ podgrupo s k elementi.

   Komentar. Taka podgrupa je ena sama. Dokazati to dejstvo je ena izmed nalog v razdelku 3.1. Lahko pa poskusiš že sedaj!
7. Za katere $n \geq 2$ je vsota vseh elementov grupe $\mathbb{Z}_n$ enaka 0?
8. Iz dokaza leme 2.14 razberemo, da je v končnem komutativnem kolobarju vsak neničeln element, ki ni delitelj niča, obrnljiv. Dokaži nekoliko splošnejšo trditev: če je K poljuben kolobar in je a tak element iz K, da je množica $\{a^n \mid n = 0, 1, 2, \dots\}$ končna, potem je a bodisi delitelj niča bodisi je obrnljiv, njegov inverz pa je tedaj enak neki njegovi potenci.

   Namig. Glej nalogo 1.2/8.

9. Pokaži, da kolobar Z_n vsebuje tak neničeln element a, da je $a^2 = 0$ natanko tedaj, ko je n deljiv s kvadratom kakega praštevila.
10. Pokaži, da je element $[a]$ kolobarja $\mathbb{Z}_n$ obrnljiv natanko tedaj, ko sta si števili a in n tuji.

    Komentar. Ponovno smo uporabili oznako $[a]$ za element iz $\mathbb{Z}_n$, da smo lahko oznako a prihranili za celo število. Na prvi pogled morda naloga deluje dvoumno, saj je $[a] = [a + kn]$ za vsak $k \in \mathbb{Z}$. Toda tujost a in n je ekvivalentna tujosti $a + kn$ in n za katerikoli $k \in \mathbb{Z}$.

    Omenimo še zvezo s t. i. **Eulerjevo funkcijo** φ. To je funkcija iz množice $\mathbb{N}$ vase, definirana takole: $\varphi(n)$ je število vseh od n kvečjemu manjših naravnih števil, ki so si tuja z n. Tako je na primer $\varphi(6) = 2$, saj sta od števil $1, 2, 3, 4, 5, 6$ edino 1 in 5 tuji s 6. Očitno je $\varphi(1) = 1$, za vsako praštevilo p pa je $\varphi(p) = p - 1$. Iz trditve naloge sledi, da je število $\varphi(n)$ enako redu grupe obrnljivih elementov kolobarja $\mathbb{Z}_n$, torej da je

    $$\varphi(n) = |\mathbb{Z}_n^*|.$$

    Če te veseli elementarna teorija števil, dokaži še, da za vsaki tuji si števili k in ℓ velja $\varphi(k\ell) = \varphi(k)\varphi(\ell)$ in tod izpelji **Eulerjevo formulo**

    $$\varphi(n) = n \prod_{p|n} \Big(1 - \frac{1}{p}\Big),$$

    kjer produkt teče po vseh praštevilih, ki delijo n.
11. Za katere n ima kolobar $\mathbb{Z}_n$ natanko en delitelj niča in za katere ima natanko dva delitelja niča?
12. Poišči primer neskončnega kolobarja, ki ima natanko 24 obrnljivih elementov in primer neskončnega kolobarja, ki ima natanko 40 obrnljivih elementov.

    Namig. Direktni produkt kolobarjev.

2.3. Obseg kvaternionov

Z zaporedjem številskih množic

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

se postopoma seznanjamo v procesu šolanja. Vsak člen zaporedja je izredno pomemben, a v nekem smislu nepopoln, kar nas vodi do njegovega naslednika. Bi lahko to zaporedje smiselno nadaljevali? Je s kompleksnimi števili res konec vsega zanimivega?

Vprašanje zastavimo natančneje. Kompleksna števila $\mathbb{C}$ so realna algebra (gl. primer 1.57). Standardna baza vektorskega prostora $\mathbb{C}$ nad poljem $\mathbb{R}$ je množica $\{1, i\}$. Dimenzija $\mathbb{C}$ nad $\mathbb{R}$ je torej enaka 2. Prvo vprašanje, ki se

naravno poraja, je, ali bi lahko razširili množenje kompleksnih števil na 3-razsežen realni vektorski prostor. Poskusimo. Dodajmo množici $\{1, i\}$ tretji vektor, ki ga označimo z j. Obravnavajmo torej realni vektorski prostor A z bazo $\{1, i, j\}$ in se vprašajmo, ali lahko razširimo množenje kompleksnih števil na A tako, da bo postala A realna algebra z enoto 1. Element i seveda zadošča $i^2 = -1$, elemente ij, ji, j^2 pa šele moramo določiti. Kot element prostora A je ij oblike

$$ij = \lambda + \mu i + \nu j$$

za neke $\lambda, \mu, \nu \in \mathbb{R}$ (namesto $\lambda 1$ pišemo kar λ, kot je v navadi tudi pri kompleksnih številih). To enakost pomnožimo z leve z i in upoštevajmo, da je $i^2 = -1$ in da je množenje asociativno. Sledi

$$-j = \lambda i - \mu + \nu ij.$$

Če tu namesto ij pišemo $\lambda + \mu i + \nu j$ in združimo skalarje pri baznih vektorjih, dobimo

$$(\nu\lambda - \mu) + (\nu\mu + \lambda)i + (\nu^2 + 1)j = 0.$$

Ker so $1, i, j$ linearno neodvisni, število $\nu^2 + 1$ pa za noben $\nu \in \mathbb{R}$ ni enako 0, smo prišli v protislovje. Kompleksnih števil torej ne moremo smiselno razširiti na 3-razsežni prostor.

Ne obupajmo. Videli smo, da ij ne more ležati v linearni lupini 1, i in j. Torej potrebujemo vsaj štiri dimenzije. Označimo četrti bazni vektor s k. Naj $\mathbb{H}$ označuje realni vektorski prostor z bazo $\{1, i, j, k\}$ (razlog za to oznako bo pojasnjen na koncu). Vsak element iz $\mathbb{H}$ torej lahko zapišemo kot

$$\lambda_0 + \lambda_1 i + \lambda_2 j + \lambda_3 k, \tag{2.1}$$

kjer so λ_i enolično določena realna števila. Seštevanje in množenje s skalarji v $\mathbb{H}$ je seveda definirano takole:

$$\begin{aligned}(\lambda_0 + \lambda_1 i + \lambda_2 j + \lambda_3 k) + (\mu_0 + \mu_1 i + \mu_2 j + \mu_3 k)\\ := (\lambda_0 + \mu_0) + (\lambda_1 + \mu_1)i + (\lambda_2 + \mu_2)j + (\lambda_3 + \mu_3)k\end{aligned}$$

in

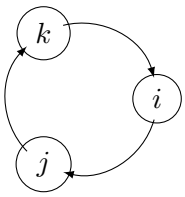
$$\lambda(\lambda_0 + \lambda_1 i + \lambda_2 j + \lambda_3 k) := (\lambda\lambda_0) + (\lambda\lambda_1)i + (\lambda\lambda_2)j + (\lambda\lambda_3)k.$$

Vektorski prostor $\mathbb{H}$ bomo sedaj opremili še z množenjem, s katerim bo postal algebra. Dovolj je, če povemo, kako se med seboj množijo bazni vektorji $1, i, j, k$. Iz aksiomov za algebro namreč vidimo, da bo s tem množenje poljubnih dveh elementov iz $\mathbb{H}$ nedvoumno določeno. Natančneje, v mislih imamo distributivnostna zakona in zvezo med množenjem elementov in množenjem elementov s skalarji, torej pravilo $\lambda(xy) = (\lambda x)y = x(\lambda y)$. Element 1 seveda igra vlogo enote za množenje, zato zadošča podati naslednja pravila za množenje:

$$\begin{aligned}i^2 = j^2 = k^2 = -1,\\ ij = -ji = k,\end{aligned}$$

$$jk = -kj = i,$$
$$ki = -ik = j.$$

Formule si najlažje zapomnimo s pomočjo slike:



Če se pomikamo v smeri urinega kazalca, je produkt zaporednih elementov naslednji element; če se pomikamo v obratni smeri, dobimo nasprotni element naslednjega elementa. Tako je na primer

$$(2 + i - k)(i + \frac{1}{2}j) = 2i + 2\frac{1}{2}j + i^2 + \frac{1}{2}ij - ki - \frac{1}{2}kj = -1 + \frac{5}{2}i + \frac{1}{2}k.$$

Zakaj prav ta pravila za množenje? Z malce daljšim razmislekom bi do njih prišli po naravni poti. Toda to izpustimo in se posvetimo vprašanju, kaj iz pravil sledi. Najprej bi morali preveriti, da je $\mathbb{H}$ res algebra. To ni prav nič težko, a precej sitno opravilo. V dokazu asociativnosti množenja zadošča obravnavati le bazne elemente (zakaj?), torej moramo preveriti enakosti, kot so $(ij)k = i(jk)$, $(i^2)j = i(ij)$ itd. Izpustimo podrobnosti – seveda je $\mathbb{H}$ res 4-*razsežna realna algebra*. Elemente $\mathbb{H}$ imenujemo **kvaternioni**. Kvaternione oblike $\lambda_0 + \lambda_1 i$ lahko poistovetimo s kompleksnimi števili in tako $\mathbb{C}$ obravnavamo kot podalgebro $\mathbb{H}$. (Elementi i, j, k nastopajo simetrično in zato bi lahko i nadomestili tudi z j ali k, seveda pa je zaradi skladnosti oznak izbira i naravnejša.) Podobno tudi $\mathbb{R}$ obravnavamo kot podalgebro $\mathbb{H}$. Kvaternionu oblike λ_0 $(= \lambda_0 1)$ ponavadi pravimo kar realno število. Za razliko od $\mathbb{R}$ in $\mathbb{C}$ je algebra $\mathbb{H}$ nekomutativna, saj je denimo $ij \neq ji$.

Podobno kot konjugiranje kompleksnih števil vpeljemo konjugiranje kvaternionov. Vzemimo kvaternion $h = \lambda_0 + \lambda_1 i + \lambda_2 j + \lambda_3 k$. **Konjugirani kvaternion** $\overline{h}$ definiramo kot

$$\overline{h} := \lambda_0 - \lambda_1 i - \lambda_2 j - \lambda_3 k.$$

Neposredni račun pokaže, da je

$$h\overline{h} = \overline{h}h = \lambda_0^2 + \lambda_1^2 + \lambda_2^2 + \lambda_3^2.$$

Torej je $h\overline{h} = \overline{h}h$ realno število (skalar), ki je enako 0 le tedaj, ko je $h = 0$. Od tod vidimo, da je vsak od 0 različen kvaternion h obrnljiv; njegov inverz je namreč

$$h^{-1} = \frac{1}{h\overline{h}}\overline{h}.$$

Na primer, $(3-i+2k)^{-1} = \frac{1}{14}(3+i-2k)$. S tem smo dokazali, da je $\mathbb{H}$ obseg. Povzemimo:

TRDITEV 2.16. *Algebra kvaternionov $\mathbb{H}$ je nekomutativen obseg.*

V primeru 1.62 smo omenili, da kompleksna števila $1, -1, i, -i$ tvorijo grupo za množenje. Zdaj ji lahko dodamo še kvaternione $j, -j, k, -k$. Res je

$$Q := \{\pm 1, \pm i, \pm j, \pm k\}$$

grupa za množenje. Imenujemo jo **kvaternionska grupa**. S svojimi osmimi elementi je ena najmanjših nekomutativnih grup. Simetrična grupa S_3 ima sicer še manj, namreč 6 elementov. V razdelku 2.8 bomo spoznali diedrsko grupo D_8, ki ima prav tako 8 elementov in ni komutativna.

Formule za množenje kvaternionov i, j, k spominjajo na formule za vektorski produkt vektorjev $\vec{i}, \vec{j}, \vec{k}$ v $\mathbb{R}^3$. Če kvaternion $\lambda_0+\lambda_1 i+\lambda_2 j+\lambda_3 k$ pišemo kot par $(\lambda_0, \vec{u})$, kjer je $\vec{u} = (\lambda_1, \lambda_2, \lambda_3) \in \mathbb{R}^3$, se pravilo za množenje kvaternionov glasi takole:

$$(\lambda_0, \vec{u})(\mu_0, \vec{v}) = (\lambda_0\mu_0 - \vec{u}\cdot\vec{v}, \lambda_0\vec{v} + \mu_0\vec{u} + \vec{u}\times\vec{v}). \tag{2.2}$$

Tu je $\vec{u}\cdot\vec{v}$ skalarni in $\vec{u}\times\vec{v}$ vektorski produkt vektorjev $\vec{u}$ in $\vec{v}$. V množenju kvaternionov sta torej skriti obe osnovni računski operaciji z vektorji.

Čeprav na kvaternione ne gledamo kot na števila, lahko imamo $\mathbb{H}$ za naslednika v zaporedju $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$. Ta ugledni status mu dajejo številne lepe lastnosti in še posebej dejstvo, da je obseg. Kako naprej? Izkaže se, da so $\mathbb{R}$, $\mathbb{C}$ in $\mathbb{H}$ edine končno-razsežne realne algebre, ki so obsegi. Njihove dimenzije so 1, 2 in 4. Naslednja pomembna dimenzija je 8. Tu imamo t. i. *oktonione*, ki imajo prav tako več lepih lastnosti, vendar pa njihovo množenje ni asociativno. Zato to sicer zanimivo temo izpustimo.

Oznaka $\mathbb{H}$ je v čast odkritelju kvaternionov, irskemu matematiku *Williamu R. Hamiltonu*. Po dolgem, neuspešnem iskanju množenja vektorjev v 3-razsežnem realnem prostoru, ki bi imelo podobno lepe lastnosti kot množenje kompleksnih števil, se mu je 16. oktobra 1843 na poti ob dublinskem kanalu Royal Canal utrnila zamisel o 4-razsežnih kvaternionih. V navalu navdušenja je na most Broom Bridge vrezal formulo

$$i^2 = j^2 = k^2 = ijk = -1. \tag{2.3}$$

Ta svojevrstni »vandalizem« je zapisan v zgodovino podobno kot Arhimedov *Heureka*.

Naloge

1. Pokaži, da iz formul (2.3) sledijo vse druge formule za množenje elementov i, j in k.
2. V obsegu $\mathbb{H}$ reši enačbi $(i+j)x = 1+k$ in $y(i+j) = 1+k$.

3. Poišči vse rešitve enačbe $ix - xi = j$ v $\mathbb{H}$.
4. Poišči $Z(\mathbb{H})$, center algebre $\mathbb{H}$.
5. Poišči $Z(Q)$, center grupe Q.
6. Poišči vse rešitve enačbe $x^2 = -1$ v $\mathbb{H}$.

   Nasvet. Računanje bo preglednejše, če kvaternion zapišemo v obliki $(\lambda_0, \vec{u})$ in uporabimo formulo (2.2).
7. Pokaži, da za vse $h, h' \in \mathbb{H}$ in $\lambda \in \mathbb{R}$ velja
$$\overline{\lambda h} = \lambda \overline{h}, \ \ \overline{h + h'} = \overline{h} + \overline{h'} \ \text{ in } \ \overline{hh'} = \overline{h'} \cdot \overline{h}.$$
8. Normo kvaterniona $h = \lambda_0 + \lambda_1 i + \lambda_2 j + \lambda_3 k$ definiramo kot nenegativno realno število
$$\|h\| := \sqrt{\lambda_0^2 + \lambda_1^2 + \lambda_2^2 + \lambda_3^2}.$$
   Pokaži, da za vse $h, h' \in \mathbb{H}$ velja $\|hh'\| = \|h\|\|h'\|$.

   Nasvet. S pomočjo ugotovitev prejšnje naloge in enakosti $\|h\|^2 = h\overline{h}$ je račun kratek.
9. Pokaži, da za vsak kvaternion $h \in \mathbb{H}$ obstajata taki realni števili α in β, da je $h^2 + \alpha h + \beta = 0$. Števili α in β izrazi s h in $\overline{h}$.
10. Naj bo $h \in \mathbb{H} \setminus \mathbb{R}$. Dokaži, da je $h + \overline{h} = 0$ natanko tedaj, ko obstaja tak $x \in \mathbb{H}$, da je $hx \neq xh$ in $h^2 x = xh^2$.
11. V definiciji algebre $\mathbb{H}$ lahko vlogo realnih števil nadomestimo z elementi kateregakoli polja F. Elementi so še vedno oblike (2.1), le da so vsi λ_i iz F. Računske operacije definiramo enako kot zgoraj in s tem dobimo 4-razsežno algebro nad poljem F. Označimo jo s $\mathbb{H}_F$. Pokaži, da je algebra $\mathbb{H}_{\mathbb{Q}}$ obseg, algebra $\mathbb{H}_{\mathbb{C}}$ pa ima delitelje niča.
12. Pokaži, da je končno-razsežna kompleksna algebra A brez deliteljev niča 1-razsežna.

    Namig. Za vsak $a \in A$ je $x \mapsto ax$ linearna preslikava iz A v A. Kaj vemo o linearnih preslikavah iz končno-razsežnega *kompleksnega* vektorskega prostora vase?
13. Naj bosta x in y taka neničelna elementa obsega O, da $x \neq y^{-1}$. Pokaži, da velja t. i. **Huajeva identiteta**
$$xyx = x - \left(x^{-1} + (y^{-1} - x)^{-1}\right)^{-1}.$$
14. Pokaži, da je obseg O komutativen, če za vse $x, y \in O$ velja $(xy)^2 = (yx)^2$.

    Namig. Elementa x in y lahko nadomestiš z vsoto drugih elementov. Ne pozabi na primer, ko za vsak $x \in O$ velja $x + x = 0$ (taki obsegi res obstajajo, najpreprostejši primer je polje $\mathbb{Z}_2$).

15. Pokaži, da nekomutativna grupa G, v kateri za vse elemente x in y velja $(xy)^2 = (yx)^2$, vsebuje tak element a, da $a \neq 1$ in je $a^2 = 1$. Preveri tudi, da je primer take grupe kvaternionska grupa Q.

2.4. Kolobarji matrik in linearne grupe

Z matrikami se ponavadi najprej seznanimo pri linearni algebri. Zelo pomembno vlogo pa imajo tudi v abstraktni algebri.

2.4.1. Kolobarji matrik. Kolobar matrik velikosti 2×2 s členi iz $\mathbb{R}$ smo že večkrat omenili. Naj bo zdaj n poljubno naravno število in K poljuben kolobar. Kvadratni tabeli

$$\begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{bmatrix},$$

kjer so a_{ij} elementi iz K, pravimo **matrika** velikosti $n \times n$ s členi iz K. Temu precej dolgemu zapisu se težko izognemo, kadar imamo opravka s konkretnimi matrikami. Dokler obravnavamo splošne matrike, pa ga raje zamenjajmo z enostavnim zapisom

$$(a_{ij}).$$

Množico vseh $n \times n$ matrik, tj. matrik velikosti $n \times n$, s členi iz K označimo z

$$M_n(K).$$

Seštevanje v $M_n(K)$ je definirano takole:

$$(a_{ij}) + (b_{ij}) := (a_{ij} + b_{ij}).$$

S tem $M_n(K)$ postane Abelova grupa. To zlahka preverimo. Ničelni element je seveda ničelna matrika, torej matrika, v kateri so vsi členi enaki 0. Če vpeljemo še množenje matrik s predpisom

$$(a_{ij})(b_{ij}) := (c_{ij}), \text{ kjer je } c_{ij} = \textstyle\sum_{k=1}^{n} a_{ik} b_{kj},$$

postane $M_n(K)$ kolobar. Najbrž se bralec ne srečuje z matričnim množenjem prvič in tako že ve, da je asociativno, da sta izpolnjena distributivnostna zakona, in da je identična matrika I, tj. matrika z enicami na diagonali in ničlami izven diagonale ($a_{ii} = 1$ in $a_{ij} = 0$, če $i \neq j$), enota za množenje. Dejstvo, da so členi matrike zdaj elementi poljubnega, lahko celo nekomutativnega kolobarja K in ne števila, kot smo vajeni v linearni algebri, v ničemer ne spremeni računov, ki te lastnosti dokazujejo. V vsakem primeru pa se bralec lahko o tem prepriča z računi (morda zaradi lažje preglednosti le za matrike velikosti 2×2).

Kolobar $M_1(K)$ je seveda v bistvu kar kolobar K. Ko govorimo o matrikah, imamo praviloma v mislih, da je $n \geq 2$. Kolobar $M_n(K)$ je tedaj nekomutativen in ima delitelje niča (gl. primer 1.42).

Matrika (a_{ij}) se imenuje **diagonalna matrika**, če je $a_{ij} = 0$ za vse $i \neq j$. Če je $a_{ij} = 0$ za vse $i > j$, potem matriki (a_{ij}) pravimo **zgoraj trikotna matrika**. Če hkrati velja, da je tudi $a_{ii} = 0$ za vse i, potem ji rečemo **strogo zgoraj trikotna matrika**. Analogno vpeljemo (strogo) spodaj trikotne matrike. Vsaka matrika je očitno enaka vsoti strogo spodaj trikotne, diagonalne in strogo zgoraj trikotne matrike.

Kot smo že omenili, elementu e nekega kolobarja pravimo **idempotent**, če je enak svojemu kvadratu, torej če je $e^2 = e$. V tem primeru je tudi $1 - e$ idempotent, saj je $(1-e)^2 = 1-2e+e^2 = 1-e$. Očitna primera idempotentov sta elementa 0 in 1. V kolobarjih brez deliteljev niča sta tudi edina, saj lahko formulo $e^2 = e$ zapišemo kot $e(1 - e) = 0$. Primer idempotenta v kolobarju $M_n(K)$ je vsaka diagonalna matrika, ki ima na diagonali samo ničle in enice.

Element a iz kolobarja se imenuje **nilpotenten element** ali **nilpotent**, če je $a^n = 0$ za neki $n \in \mathbb{N}$. V kolobarjih brez deliteljev niča je element 0 očitno edini nilpotent. Primer nilpotentnega elementa v $M_n(K)$ je vsaka strogo zgoraj (ali spodaj) trikotna matrika. Dokaz je enostavna vaja iz računanja z matrikami.

Če je K algebra nad poljem F, postane tudi $M_n(K)$ *algebra nad* F, če definiramo množenje matrik s skalarji takole:

$$\lambda(a_{ij}) := (\lambda a_{ij}).$$

Kot poseben primer je tako $M_n(F)$ algebra nad F. Na primer, $M_n(\mathbb{R})$ je realna algebra in $M_n(\mathbb{C})$ je kompleksna algebra. Bralec se verjetno spomni iz linearne algebre, da je algebra $M_n(F)$ povezana z algebro vseh linearnih preslikav na n-razsežnem vektorskem prostoru nad F. Toda to temo prihranimo za naslednje poglavje, ko bomo govorili o homomorfizmih algebrskih struktur.

2.4.2. Linearne grupe. Od matričnih kolobarjev prehajamo k matričnim grupam. Ogledali si bomo primere grup, katerih elementi so matrike nad poljem, operacija pa je množenje. Seveda množica vseh $n \times n$ matrik nad poljem F ni grupa, pač pa le monoid. Spomnimo se, da množica vseh obrnljivih elementov poljubnega monoida S tvori grupo, ki jo označujemo s S^* (trditev 1.33). Torej je množica

$$\mathrm{GL}_n(F) := M_n(F)^*,$$

tj. množica vseh obrnljivih $n \times n$ matrik nad F, grupa. Imenujemo jo **splošna linearna grupa**. Ni težko videti, da je nekomutativna, če je le $n > 1$. Druge t. i. **linearne grupe** so podgrupe grupe $\mathrm{GL}_n(F)$. Navedimo nekaj primerov. Prvega vpeljemo preko pojma **determinanta matrike**. Predvidevamo, da se je bralec z determinanto in njenimi lastnostmi seznanil pri linearni algebri

(morda sicer le v primeru, ko je $F = \mathbb{R}$ in $F = \mathbb{C}$, toda osnovna teorija je enaka za vsako polje F). Ponovimo definicijo in nekaj za nas pomembnih dejstev. Determinanto matrike $A = (a_{ij}) \in M_n(F)$ definiramo s formulo

$$\det(A) := \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) a_{1\sigma(1)} \cdots a_{n\sigma(n)};$$

tu S_n označuje množico vseh permutacij (gl. primer 1.36), $\operatorname{sgn}(\sigma)$ pa predznak permutacije σ. Bralec pojem predznaka gotovo pozna, sicer pa ga bomo vpeljali v razdelku 2.7.

Če je $n = 2$, je torej

$$\det\left(\begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}\right) = a_{11}a_{22} - a_{12}a_{21}.$$

Z naraščajočim n je členov v formuli čedalje več in izračun determinante samo s svinčnikom in papirjem po zgornji formuli je praktično neizvedljiv. Za matrike z veliko ničlami je ta naloga lahko neprimerno lažja. Na primer, determinanta zgoraj (ali spodaj) trikotne matrike je enaka kar produktu vseh diagonalnih členov. Za tako matriko je namreč vsaj eden izmed členov $a_{1\sigma(1)}, \ldots, a_{n\sigma(n)}$ enak 0 pri vsaki permutaciji σ, ki je različna od identitete. Sicer pa se ne bomo ukvarjali z računanjem determinant. Potrebujemo le naslednje lastnosti:

(a) $\det(I) = 1$.
(b) $\det(AB) = \det(A)\det(B)$ za vse $A, B \in M_n(F)$.
(c) Matrika $A \in M_n(F)$ je obrnljiva natanko tedaj, ko $\det(A) \neq 0$.

Trditev (a) je očitna, trditvi (b) in (c) pa se izpeljeta z nekaj truda. Če ju bralec ne pozna, naj (b) preveri vsaj za $n = 2$ in za zgoraj trikotne matrike, v zvezi s (c) pa naj preveri, da za matriko $A = \left[\begin{smallmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{smallmatrix}\right] \in M_2(F)$ z neničelno determinanto velja

$$A^{-1} = \frac{1}{\det(A)} \begin{bmatrix} a_{22} & -a_{12} \\ -a_{21} & a_{11} \end{bmatrix}.$$

Dokazi (b) in (c) za poljuben n so v vseh standardnih učbenikih linearne algebre.

Opomba 2.17. Morda se je bralec vprašal, ali polje F lahko nadomestimo s poljubnim kolobarjem K. Če je K komutativen kolobar, je to do neke mere res: (a) in (b) veljata, v (c) pa moramo pogoj $\det(A) \neq 0$ zamenjati s pogojem, da je $\det(A)$ obrnljiv element kolobarja K. Dokazi niso bistveno drugačni kot za polja. Če pa je K nekomutativen, zgornja definicija determinante nima pravega smisla.

V luči trditve (c) lahko splošno linearno grupo opišemo takole:

$$\mathrm{GL}_n(F) = \{A \in M_n(F) \mid \det(A) \neq 0\}.$$

Oglejmo si množico

$$\mathrm{SL}_n(F) := \{A \in M_n(F) \mid \det(A) = 1\}.$$

Iz trditve (b) vidimo, da je $\mathrm{SL}_n(F)$ zaprta za množenje. Iz (a) in (b) sledi, da je

$$\det(A)\det(A^{-1}) = \det(I) = 1$$

za vsako obrnljivo matriko A. Zato inverz matrike iz $\mathrm{SL}_n(F)$ spet leži v $\mathrm{SL}_n(F)$. Torej je $\mathrm{SL}_n(F)$ podgrupa grupe $\mathrm{GL}_n(F)$. Pravimo ji **posebna** (ali **specialna**) **linearna grupa**.

V nadaljevanju bomo uporabljali nekatere pojme iz linearne algebre. Če jih bralec ne pozna, naj ta del preskoči. Z A^t označimo transponirano matriko matrike A. Množica

$$\mathrm{O}_n(F) := \{A \in M_n(F) \mid AA^t = I\},$$

torej množica vseh ortogonalnih matrik, je podgrupa $\mathrm{GL}_n(F)$. Imenuje se **ortogonalna grupa**. Podobno vpeljemo **unitarno grupo**

$$\mathrm{U}_n := \{A \in M_n(\mathbb{C}) \mid AA^* = I\}.$$

Tu A^* označuje adjungirano matriko matrike A. Grupama

$$\mathrm{SO}_n(F) := \mathrm{O}_n(F) \cap \mathrm{SL}_n(F) \quad \text{in} \quad \mathrm{SU}_n := \mathrm{U}_n \cap \mathrm{SL}_n(\mathbb{C})$$

pravimo **posebna ortogonalna grupa** in **posebna unitarna grupa**. Nazadnje omenimo še **simplektično grupo**

$$\mathrm{Sp}_{2n}(F) := \{A \in M_{2n}(F) \mid A^t J A = J\},$$

kjer je

$$J = \begin{bmatrix} 0 & I_n \\ -I_n & 0 \end{bmatrix} \in M_{2n}(F).$$

Tu je I_n identična matrika velikosti $n \times n$.

Za vse navedene grupe je seveda potrebno preveriti, da so res podgrupe splošne linearne grupe. Dokazi so enostavni in jih prepuščamo bralcu. Lahko bi se domislili še veliko primerov podgrup $\mathrm{GL}_n(F)$, vendar smo se omejili na pomembne, klasične zglede.

Naloge

1. Ugotovi, katere izmed naslednjih množic so podgrupe grupe $\mathrm{GL}_n(\mathbb{R})$:
   (a) $\{(a_{ij}) \in \mathrm{GL}_n(\mathbb{R}) \mid a_{ij} \in \mathbb{Z}\}$.
   (b) $\{(a_{ij}) \in \mathrm{SL}_n(\mathbb{R}) \mid a_{ij} \in \mathbb{Z}\}$.
   (c) $\{(a_{ij}) \in \mathrm{O}_n(\mathbb{R}) \mid a_{ij} \in \mathbb{Z}\}$.
   (d) $\{A \in \mathrm{GL}_n(\mathbb{R}) \mid A = A^t\}$.
   (e) $\{A \in \mathrm{GL}_n(\mathbb{R}) \mid |\det(A)| = 1\}$.
   (f) $\{A \in \mathrm{GL}_n(\mathbb{R}) \mid A^2 = I\}$.

Nasvet. To in tudi naslednje naloge, v katerih nastopajo matrike velikosti $n \times n$, reši vsaj za $n = 2$. Računanje z večjimi matrikami je včasih nepregledno in zamudno, kar nas lahko odvrne od bistva problema. Sicer pa so lahko že z matrikami velikosti 2×2 računi dolgi. Kadar lahko izbereš poljubno matriko, vzemi tako s čim več ničlami!

2. Koliko elementov ima grupa $\mathrm{GL}_2(\mathbb{Z}_2)$?

   Komentar. V nalogah v razdelku 3.1 bomo to grupo in tudi grupi iz naslednjih dveh nalog opredelili jasneje.

3. Opiši podgrupo grupe $\mathrm{GL}_2(\mathbb{R})$, generirano z matriko $\left[\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right]$.

4. Opiši podgrupo grupe $\mathrm{GL}_2(\mathbb{C})$, generirano z matrikama $\left[\begin{smallmatrix} i & 0 \\ 0 & -i \end{smallmatrix}\right]$ in $\left[\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right]$.

5. Poišči $Z(\mathrm{GL}_n(F))$, center grupe $\mathrm{GL}_n(F)$.

6. Opiši $Z(M_n(K))$, center kolobarja $M_n(K)$, s pomočjo centra kolobarja K.

7. Kolobar K imenujemo **prakolobar**, če za vsaka neničelna elementa $a, b \in K$ obstaja tak $x \in K$, da $axb \neq 0$. Kolobarji brez deliteljev ničа seveda so prakolobarji, niso pa edini: pokaži, da je kolobar $M_n(K)$ prakolobar natanko tedaj, ko je K prakolobar.

8. Pokaži, da prakolobar z delitelji ničа vsebuje neničeln nilpotent.

   Komentar. Obstoj neničelnega nilpotenta je ekvivalenten obstoju neničelnega elementa s kvadratom nič. Namreč, za vsak $n \geq 2$ iz $a^n = 0$ sledi $(a^{n-1})^2 = 0$.

9. Naj bo $A \in M_n(F)$ matrika, v kateri sta katerikoli vrstici linearni odvisni (matrika z rangom največ 1). Pokaži, da je $A^2 = \lambda A$ za neki $\lambda \in F$. Poišči sedaj kak nilpotent v kolobarju $M_n(F)$, ki ni strogo zgoraj trikotna ali strogo spodaj trikotna matrika, in kak idempotent v $M_n(F)$, ki ni diagonalna matrika.

10. Naj bo e idempotent kolobarja K. Pokaži, da je potem za vsak $x \in K$ tudi element $e + ex(1 - e)$ idempotent. Poišči sedaj še kak idempotent kolobarja $M_3(F)$, ki ni diagonalna matrika in nima ranga 1.

11. Naj bo K kolobar, v katerem je element $1 + 1$ obrnljiv. Pokaži, da K vsebuje idempotent e, različen od 0 in 1, natanko tedaj, ko K vsebuje tak element u, da $u \neq 1$, $u \neq -1$ in $u^2 = 1$.

    Namig. Če najprej obravnavaš primer, ko sta e in u diagonalni matriki velikosti 2×2, lahko dobiš idejo, kako se lotiti v splošnem.

12. Za matriko $A \in M_n(F)$ rečemo, da se da *diagonalizirati*, če obstaja taka obrnljiva matrika $P \in M_n(F)$, da je $P^{-1}AP$ diagonalna matrika. Pokaži, da lahko tako matriko zapišemo kot $A = \sum_{i=1}^{r} \lambda_i E_i$ za neke $\lambda_i \in F$ in take idempotentne matrike $E_1, \ldots, E_r \in M_n(F)$, da je $E_i E_j = 0$ za vse $i \neq j$.

13. Če je $T \in M_n(F)$ strogo zgoraj trikotna matrika, ima matrika $I - T$ determinanto enako 1 in je zato obrnljiva. Dokaži naslednjo veliko splošnejšo trditev: če je x nilpotenten element poljubnega kolobarja K, je element $1 - x$ obrnljiv.

    Namig. S pomočjo geometrijske vrste ugani, kako izraziti $(1 - x)^{-1}$ (podobno kot v nalogi 1.4/10).

14. Pokaži, da je v kolobarju brez enote, ki nima deliteljev niča, edini idempotent element 0.

15. Naj bo M množica vseh takih neskončnih matrik

$$\begin{bmatrix} a_{11} & a_{12} & a_{13} & \dots \\ a_{21} & a_{22} & a_{23} & \dots \\ a_{31} & a_{32} & a_{33} & \dots \\ \vdots & \vdots & \vdots & \ddots \end{bmatrix},$$

    kjer so $a_{ij} \in \mathbb{R}$, da ima vsak stolpec le končno mnogo neničelnih členov. Pokaži, da je M kolobar za običajno seštevanje in množenje matrik. Pokaži tudi, da ima matrika

$$\begin{bmatrix} 0 & 1 & 0 & 0 & \dots \\ 0 & 0 & 1 & 0 & \dots \\ 0 & 0 & 0 & 1 & \dots \\ \vdots & \vdots & \vdots & \vdots & \ddots \end{bmatrix}$$

    desni inverz, ne pa tudi levega.

16. Pokaži, da kolobar K vsebuje element, ki ima desni inverz in nima levega inverza natanko tedaj, ko kolobar $M_2(K)$ vsebuje obrnljivo zgoraj trikotno matriko, katere inverz ni zgoraj trikotna matrika.

    Namig. Če je $ab = 1$, potem je $e := 1 - ba$ idempotent in $ae = eb = 0$.

2.5. Kolobarji funkcij

Naj bo X neprazna množica. *Vsoto* in *produkt funkcij* $f : X \to \mathbb{R}$ in $g : X \to \mathbb{R}$ definiramo kot funkciji $f + g : X \to \mathbb{R}$ in $fg : X \to \mathbb{R}$, podani s predpisoma

$$(f + g)(x) := f(x) + g(x) \text{ za vse } x \in X$$

in

$$(fg)(x) := f(x)g(x) \text{ za vse } x \in X.$$

To je običajno seštevanje in množenje funkcij, s katerim se srečamo pri matematični analizi. Za ti operaciji je množica vseh funkcij iz X v $\mathbb{R}$ *komutativen kolobar*. To je lahko preveriti. Asociativnost obeh operacij sledi iz asociativnosti seštevanja in množenja realnih števil. Podobno je s komutativnostjo in distributivnostjo. Ničelni element je konstantna funkcija 0, torej funkcija,

ki vsak $x \in X$ preslika v število 0. Nasprotni element funkcije f je funkcija $x \mapsto -f(x)$. Enota je konstantna funkcija 1.

Vlogo realnih števil v definiciji lahko nadomestimo s kompleksnimi. Še več, polje $\mathbb{R}$ lahko zamenjamo s poljubnim poljem F. Toda raje se izognimo pretirani splošnosti in ostanimo pri realnih številih.

Kolobar vseh funkcij iz X v $\mathbb{R}$ je morda prevelik, da bi bil zanimiv za obravnavo. Običajno nas zanimajo podkolobarji, ki jih sestavljajo kake posebne funkcije. Lep primer je $C(X)$, kolobar vseh zveznih funkcij iz X v $\mathbb{R}$. Tu seveda X ni več poljubna množica; lahko je na primer $X = \mathbb{R}$ ali pa je X interval realnih števil $[a, b]$ (namesto $C([a, b])$ lahko pišemo $C[a, b]$). Da je $C(X)$ res podkolobar, sledi iz dejstva, da sta razlika in produkt *zveznih funkcij* spet zvezni funkciji. Podobno lahko govorimo o kolobarju *omejenih funkcij* $B(X)$, *zvezno odvedljivih funkcij* $C^1(X)$, *gladkih funkcij* $C^\infty(X)$ itd. Na različnih področjih matematike srečamo izreke, ki pravijo, da je neki razred funkcij zaprt za vsoto, razliko in produkt. To lahko povemo tako, da je ta razred kolobar. Z vidika algebre je posebej zanimiv *kolobar polinomov*, s katerim smo se že srečevali v primerih in nalogah. V naslednjem razdelku se bomo študija polinomov lotili sistematično.

Funkcije lahko množimo tudi s skalarji. Za $\lambda \in \mathbb{R}$ in $f : X \to \mathbb{R}$ definiramo funkcijo $\lambda f : X \to \mathbb{R}$ s predpisom

$$(\lambda f)(x) := \lambda f(x) \text{ za vse } x \in X.$$

S tem postane kolobar vseh funkcij iz X v $\mathbb{R}$ algebra. Prav tako so algebre tudi vsi zgoraj omenjeni kolobarji posebnih funkcij. Včasih je res pomembno, da te kolobarje obravnavamo kot algebre, drugič spet ne. Zato včasih govorimo o kolobarjih funkcij in drugič o algebrah funkcij.

Primer 2.18. Algebro realnih polinomov lahko opišemo kot podalgebro algebre vseh funkcij iz $\mathbb{R}$ v $\mathbb{R}$, generirano z identično funkcijo $\mathrm{id}_{\mathbb{R}}$. V tej izjavi ne moremo besed algebra in podalgebra nadomestiti s kolobar in podkolobar.

Posebej omenimo še primer, ko je $X = \mathbb{N}$. Funkcije iz X v $\mathbb{R}$ so tedaj realna zaporedja. Funkcijo $f : \mathbb{N} \to \mathbb{R}$ namreč pišemo kot zaporedje $(x_n) = (x_1, x_2, \dots)$, kjer je $x_i = f(i)$. Z algebro vseh realnih zaporedij smo se že srečali v primeru 1.89. Hitro ugotovimo, da operacije iz tega primera sovpadajo z operacijami, ki smo jih definirali v tem razdelku. Tako imamo dva različna pogleda na isto algebro. Zanimiv primer podalgebre je množica vseh konvergentnih zaporedij c. Res je podalgebra, saj so vsota, produkt in produkt s skalarjem konvergentnih zaporedij spet konvergentna zaporedja. Pomemben primer podalgebre vseh zaporedij je tudi algebra vseh omejenih zaporedij. Namesto z $B(\mathbb{N})$ jo označujemo z ℓ^∞.

Oznake $C(X)$, $B(X)$, $C^1(X)$, $C^\infty(X)$, c in ℓ^∞ prihajajo iz matematične analize. V analizi sicer te množice obravnavamo kot algebre ali pa zgolj vektorske prostore, opremljene še z dodatno topološko strukturo. Mi smo seveda izpostavili le algebraični vidik.

Nazadnje še beseda o primeru, ko je množica X končna. Če je $|X| = n$, lahko funkcijo $f : X \to \mathbb{R}$ predstavimo kot n-terico $(x_1, \ldots, x_n)$, kjer je $x_i = f(i)$. Algebro vseh funkcij iz X v $\mathbb{R}$ tako identificiramo z algebro $\mathbb{R}^n$ iz primera 1.55.

Naloge

1. Naj bo $\mathcal{F}$ množica vseh funkcij iz $\mathbb{R}$ iz $\mathbb{R}$. Kot vemo, je $\mathcal{F}$ Abelova grupa za običajno seštevanje funkcij. Denimo, da za drugo binarno operacijo v $\mathcal{F}$ namesto običajnega množenja vzamemo komponiranje. Pokaži, da v $\mathcal{F}$ potem veljajo vsi aksiomi za kolobar z izjemo enega izmed obeh distributivnostnih zakonov (katerega?).
2. Pokaži, da ima kolobar $C[a, b]$ delitelje niča. Ali ima delitelje niča tudi kolobar realnih polinomov?
3. Katera izmed naslednjih trditev je pravilna:
   (a) Funkcija $f \in C[a, b]$ je obrnljiv element kolobarja $C[a, b]$ natanko tedaj, ko f nima ničel.
   (b) Funkcija $f \in C[a, b]$ je delitelj niča v kolobarju $C[a, b]$ natanko tedaj, ko ima f kako ničlo.
4. Ali kolobar $C[a, b]$ vsebuje idempotente, različne od 0 in 1? Ali vsebuje neničelne nilpotente?
5. Pokaži, da je za vsako nekonstantno funkcijo $f \in C[a, b]$ podalgebra, generirana s f, neskončno-razsežna.
6. Znano je, da je vsako konvergentno zaporedje realnih števil omejeno. Torej je $c \subseteq \ell^\infty$. Poišči kako tako zaporedje iz $\ell^\infty \setminus c$, da njegov kvadrat leži v c.
7. Ali je algebra vseh realnih zaporedij generirana z množico vseh svojih idempotentov?

2.6. Kolobarji polinomov

V prejšnjem razdelku smo kolobar polinomov omenili kot primer podkolobarja kolobarja vseh funkcij iz $\mathbb{R}$ v $\mathbb{R}$. Pogled na polinom kot na funkcijo je bralcu gotovo domač. Toda v abstraktni algebri polinome obravnavamo nekoliko drugače.

2.6.1. Kolobarji polinomov ene spremenljivke. Polinom bo za nas formalna vsota

$$f(X) = a_0 + a_1X + \cdots + a_nX^n,$$

kjer a_i niso nujno realna ali kaka druga števila, pač pa elementi nekega kolobarja K. Imenujemo jih **koeficienti** polinoma $f(X)$. Koeficientu a_0 pravimo **prosti** ali **konstantni člen**, koeficientu a_n pa **vodilni koeficient**, a le kadar ni enak 0. Člene z ničelnim koeficientom lahko v zapisu izpustimo in tudi sicer uporabljamo nekatere bolj ali manj samoumevne poenostavitve. Tako na primer namesto

$$0 + 1X + 0X^2 + (-2)X^3 + 0X^4$$

pišemo

$$X - 2X^3.$$

Če so vsi a_k enaki 0, polinom $f(X)$ pišemo kot 0.

Na polinom ne gledamo kot na funkcijo in simbol X ne predstavlja elementa iz K. Potenca X^k ima predvsem vlogo indeksa, označuje k-to mesto. Polinom $f(X)$ bi lahko vpeljali tudi kot zaporedje

$$(a_0, a_1, \dots, a_n, 0, 0, \dots),$$

torej kot zaporedje elementov iz K, v katerem so od nekega mesta dalje vsi členi enaki 0. Vendar bi bil ta zapis manj prikladen za množenje polinomov. Zato ostanimo pri našem zapisu, ki pa ga bomo včasih zamenjali z

$$f(X) = \sum_{k\geq 0} a_kX^k.$$

Tu razumemo, da je $a_k = 0$ za vse indekse k, ki so večji od nekega števila $n \geq 0$. S tem zapisom bo laže podati naslednje definicije. Za polinoma $f(X) = \sum_{k\geq 0} a_kX^k$ in $\bar{f}(X) = \sum_{k\geq 0} \bar{a}_kX^k$ rečemo, da sta **enaka**, če je $a_k = \bar{a}_k$ za vse $k \geq 0$. **Vsoto** polinomov

$$f(X) = \sum_{k\geq 0} a_kX^k \text{ in } g(X) = \sum_{k\geq 0} b_kX^k$$

definiramo kot polinom

$$f(X) + g(X) := \sum_{k\geq 0} (a_k + b_k)X^k,$$

njun **produkt** pa kot polinom

$$f(X)g(X) := \sum_{k\geq 0} c_kX^k,$$

kjer je

$$c_k = a_0b_k + a_1b_{k-1} + \cdots + a_{k-1}b_1 + a_kb_0.$$

Povedano drugače, c_k je vsota vseh produktov oblike $a_i b_j$, kjer je $i + j = k$. Na prvi pogled formula za množenje morda zgleda zapletena, a v ozadju ni nič drugega kot formula

$$a_i X^i \cdot b_j X^j = (a_i b_j) X^{i+j}$$

skupaj z distributivnostnima zakonoma. Če je $a_k = 0$ za $k > n$ in $b_k = 0$ za $k > m$, potem je $c_k = 0$ za $k > n + m$. Formulo za produkt lahko zapišemo tudi takole:

$$\begin{aligned}&(a_0 + a_1 X + \cdots + a_m X^m) \cdot (b_0 + b_1 X + \cdots + b_n X^n)\\ =&a_0 b_0 + (a_0 b_1 + a_1 b_0) X + \cdots + (a_{m-1} b_n + a_m b_{n-1}) X^{m+n-1} + a_m b_n X^{m+n}.\end{aligned}$$

Računanje s polinomi je torej tako, kot bi ga sami uganili.

S tema operacijama postane množica vseh polinomov s koeficienti iz kolobarja K kolobar. Dokaz izpustimo, saj gre le za rutinsko preverjanje. Bralcu vseeno svetujemo, naj razmisli, kaj sta ničelni element in enota ter kako bi morali preveriti asociativnost množenja. Kolobar polinomov s koeficienti iz K, ali, kot mu krajše rečemo, **kolobar polinomov nad** K, označujemo s

$$K[X].$$

Čeprav simbol X igra le formalno vlogo, ga imenujemo **spremenljivka**. V tem ne gre iskati kakega skritega pomena. Gre za navado, ki izvira iz obravnave polinomov kot funkcij. Na spremenljivko X seveda lahko gledamo kot na polinom, torej kot element kolobarja $K[X]$. Očitno komutira z vsemi drugimi elementi iz $K[X]$. V kasnejših poglavjih se bomo sicer omejili na primer, ko je kolobar K komutativen. Takrat je očitno komutativen tudi kolobar $K[X]$.

Omenimo, da imata vsota in produkt izrazov oblike $f(X) = \sum_{k\geq 0} a_k X^k$ in $g(X) = \sum_{k\geq 0} b_k X^k$ smisel tudi takrat, ko koeficienti a_k in b_k niso nujno od nekega indeksa dalje vsi enaki 0. Takim izrazom pravimo **formalne potenčne vrste**. Tudi zanje so izpolnjeni aksiomi za kolobar. To preverimo enako kot za polinome. **Kolobar formalnih potenčnih vrst** označujemo s $K[[X]]$. Kolobar polinomov $K[X]$ je njegov podkolobar.

Če je K algebra nad poljem F, tudi kolobar $K[X]$ postane algebra nad F, če definiramo množenje s skalarji takole:

$$\lambda \cdot (a_0 + a_1 X + \cdots + a_n X^n) := (\lambda a_0) + (\lambda a_1) X + \cdots + (\lambda a_n) X^n$$

za vse $\lambda \in F$ in $a_i \in K$. Kot poseben primer je tako kolobar $F[X]$ algebra nad F. Ta vidik sicer za nas ne bo zelo pomemben. Ponavadi bomo govorili kar o kolobarju $F[X]$. Ti kolobarji, torej kolobarji polinomov nad polji, bodo ena osrednjih tem poglavij 6 in 7.

Vrnimo se h kolobarju polinomov nad poljubnim kolobarjem K. Pravimo, da ima polinom $f(X) = a_0 + a_1 X + \cdots + a_n X^n$ **stopnjo** n, če je $a_n \neq 0$. Tedaj pišemo

$$\mathrm{st}(f(X)) = n.$$

Polinom 0 nima definirane stopnje. Polinomom stopnje 0 ter tudi polinomu 0 pravimo **konstantni polinomi**. To so torej polinomi, ki so enaki svojemu konstantnemu členu. Običajno jih kar identificiramo z elementi kolobarja in v tem smislu obravnavamo K kot podkolobar $K[X]$. Polinomom stopnje vsaj 1 tako rečemo tudi **nekonstantni polinomi**. Polinomi stopnje 1 se imenujejo **linearni polinomi**, polinomi stopnje 2 **kvadratni polinomi**, in polinomi stopnje 3 **kubični polinomi**.

TRDITEV 2.19. *Če je K kolobar brez deliteljev niča, potem za poljubna neničelna polinoma $f(X), g(X) \in K[X]$ velja*

$$\mathrm{st}(f(X)g(X)) = \mathrm{st}(f(X)) + \mathrm{st}(g(X)).$$

Zato je tedaj tudi $K[X]$ kolobar brez deliteljev niča.

DOKAZ. Naj bo $f(X)$ polinom stopnje m z vodilnim koeficientom a_m in $g(X)$ polinom stopnje n z vodilnim koeficientom b_n. Iz formule za produkt polinomov razberemo, da je potem $f(X)g(X)$ polinom stopnje $m+n$ z vodilnim koeficientom $a_m b_n$. To dokazuje trditev. □

Pri naslednjih definicijah se ponavadi omejimo na primer, ko je kolobar K komutativen (gl. nalogo 8). **Vrednost polinoma**

$$f(X) = a_0 + a_1 X + \cdots + a_n X^n$$

v elementu $x \in K$ definiramo tako, da enostavno zamenjamo simbol X z x, torej kot

$$f(x) := a_0 + a_1 x + \cdots + a_n x^n.$$

Torej je $f(x)$ element kolobarja K. Definicija ima smisel tudi takrat, ko je x element kakega (komutativnega) kolobarja K', ki vsebuje K kot svoj podkolobar. Potem je seveda $f(x) \in K'$. Če je $f(x) = 0$, element x imenujemo **ničla** (ali **koren**) polinoma $f(X)$.

PRIMER 2.20. Polinom $X^2 + 1 \in \mathbb{R}[X]$ nima ničle v $\mathbb{R}$. Ima pa dve ničli v $\mathbb{C}$, namreč števili i in $-i$.

Vsakemu polinomu $f(X) \in K[X]$ priredimo **polinomsko funkcijo**

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

To je preslikava iz K v K, ki jo seveda določa polinom $f(X)$. Ali velja tudi obratno, je polinom določen s svojo polinomsko funkcijo? V splošnem je odgovor negativen.

PRIMER 2.21. Polinoma 0 in $X + X^2$ imata kot elementa $\mathbb{Z}_2[X]$ isto polinomsko funkcijo, namreč ničelno funkcijo $x \mapsto 0$ za vsak $x \in \mathbb{Z}_2$.

Ta primer pojasni, zakaj polinomov ne moremo definirati kot funkcij. Res pa takega primera ne moremo najti na primer v kolobarju $\mathbb{R}[X]$. Za polinome z realnimi ali kompleksnimi koeficienti je razlika med polinomom in polinomsko funkcijo bolj kot ne le formalna.

2.6.2. Kolobarji polinomov več spremenljivk. Doslej smo obravnavali polinome ene spremenljivke, ki smo jo označili z X. S temi polinomi se bomo pogosto srečevali tudi v nadaljevanju, med drugim v povezavi z razširitvami polj. Polinomi več spremenljivk so nekoliko zahtevnejša tema in ne sodijo povsem v uvodna poglavja algebre. Ker pa imajo v matematiki tako pomembno vlogo, se jih vsaj dotaknimo.

Kaj je kolobar polinomov več spremenljivk? Odgovorimo najprej neformalno, z zgledi. Primer polinoma v dveh spremenljivkah X in Y z realnimi koeficienti je

$$f(X,Y) = 5X^2Y^4 - \sqrt{2}X^8Y + \frac{3}{2}X^6 + 7.$$

Njegovi **koeficienti** so 5, $-\sqrt{2}$, $\frac{3}{2}$ in 7. Sestavljajo ga štirje členi, ki jim pravimo **monomi**. Prvi monom ima stopnjo $2+4=6$, drugi stopnjo 9, tretji spet stopnjo 6, in zadnji stopnjo 0. Polinom $f(X,Y)$ ima **stopnjo** 9, ker je to najvišja izmed stopenj mononomov, ki ga sestavljajo. Polinome v dveh (ali več) spremenljivkah seštevamo na naraven, samoumeven način. Na primer,

$$(X^2Y + X^2 - 5) + (-4X^2Y + XY - X^2 + 6) = -3X^2Y + XY + 1.$$

Definicija množenja sloni na pravilu

$$(aX^pY^q)\cdot(bX^rY^s) = (ab)X^{p+r}Y^{q+s}$$

in distributivnosti. Tako je na primer

$$(XY+2)(X^2Y^3 - XY^2) = X^3Y^4 + X^2Y^3 - 2XY^2,$$

kot lahko bralec hitro preveri.

In zdaj k formalni definiciji. Že definicija kolobarja polinomov ene spremenljivke je bila nekoliko zamudna. Morda se zato zdi, da je pred nami malce nadležna naloga. K sreči pa do definicije vodi bližnjica. **Kolobar polinomov v dveh spremenljivkah** nad kolobarjem K definiramo kot

$$K[X,Y] := \big(K[X]\big)[Y],$$

torej kot kolobar polinomov v spremenljivki Y nad kolobarjem polinomov v spremenljivki X. Polinom v spremenljivkah X in Y tako zapišemo kot

$$\sum_{j\geq 0}\Big(\sum_{i\geq 0} a_{ij}X^i\Big)Y^j,$$

kjer je le končno mnogo elementov $a_{ij} \in K$ različnih od 0. Če upoštevamo distributivnost in opustimo pisanje oklepajev, pridemo do zapisa

$$\sum_{j\geq 0}\sum_{i\geq 0} a_{ij}X^iY^j$$

kot v zgornjih zgledih. Tudi seštevanje in množenje iz zgledov se ujemata s seštevanjem in množenjem iz formalne definicije. Bralec se lahko o tem prepriča s kratkim računom. Omenimo še, da spremenljivki X in Y nastopata enakovredno, zato bi lahko $K[X,Y]$ vpeljali tudi kot $(K[Y])[X]$. S tem bi najprej prišli do malce drugačnega zapisa, vsebinskih razlik pa ne bi bilo. Spremenljivki X in Y namreč komutirata.

Kolobar polinomov v n spremenljivkah vpeljemo iterativno:

$$K[X_1,\ldots,X_{n-1},X_n] := (K[X_1,\ldots,X_{n-1}])[X_n].$$

Na podlagi zgornjega zgleda bo bralec gotovo pravilno uganil, kako za te polinome definiramo pojme monom, koeficient in stopnja. Če je K komutativen kolobar in so $x_1,\ldots,x_n$ elementi iz K, definiramo **vrednost**

$$f(x_1,\ldots,x_n)$$

polinoma $f(X_1,\ldots,X_n)$ v $(x_1,\ldots,x_n)$ tako, da vsak X_i zamenjamo z x_i. Vsaki taki n-terici $(x_1,\ldots,x_n)$, da je

$$f(x_1,\ldots,x_n) = 0,$$

pravimo **ničla** tega polinoma. Če je K algebra nad poljem F, na naraven način tudi $K[X_1,\ldots,X_n]$ postane algebra nad F.

Polinomi v n spremenljivkah niso pomemembni le v abstraktni algebri. Pojavljajo se na različnih matematičnih področjih, predvsem v *algebraični geometriji*. Kaj bi lahko bilo geometrijskega na primer na polinomu

$$f(X_1,X_2,X_3) = X_1^2 + X_2^2 + X_3^2 - 1 \in \mathbb{R}[X_1,X_2,X_3]?$$

Njegove ničle! Množica njegovih ničel je enotska sfera v prostoru $\mathbb{R}^3$. Klasična algebraična geometrija se ukvarja z ničlami polinomov več spremenljivk.

Oglejmo si še en primer. Naj bo n naravno število, večje od 1. Množica ničel polinoma

$$g(X_1,X_2,X_3) = X_1^n + X_2^n - X_3^n \in \mathbb{R}[X_1,X_2,X_3]$$

je ploskev v prostoru $\mathbb{R}^3$. Ali vsebuje kako tako točko (a,b,c), da so vse komponente naravna števila? Ali torej obstajajo taki $a,b,c \in \mathbb{N}$, da je

$$a^n + b^n = c^n?$$

Za $n = 2$ je odgovor pozitiven. Rešitvam pravimo pitagorejske trojice; preprost primer je $(3,4,5)$. Francoski pravnik in ljubiteljski matematik *Pierre de Fermat* je leta 1637 na robu strani v Diofantovi knjigi *Aritmetika* napisal, da je našel čudovit dokaz, da za noben $n \geq 3$ takih naravnih števil a,b,c ni, le na

robu strani je premalo prostora za njegov zapis. Fermatove trditve se je prijelo ime *Fermatov zadnji izrek*. Glede dokaza se je Fermat skoraj zanesljivo zmotil, čeprav resnice seveda nikoli ne bomo izvedeli. Problem, ali ta izrek res velja, je bil namreč zatem odprt več kot 350 let. Z njim so se spopadali nekateri največji matematiki, popularen pa je bil tudi med matematičnimi amaterji, saj se je zdelo, da je za rešitev morda potreben le genialen preblisk. Šele leta 1995 je angleški matematik *Andrew Wiles* objavil popoln dokaz Fermatovega zadnjega izreka. V njem se uporabljajo različna matematična orodja, tudi geometrijska in algebraična. Dolg je čez 100 strani in je v celoti razumljiv le redkim matematikom, ki premorejo potrebno tehnično znanje. Sama formulacija Fermatovega zadnjega izreka je seveda povsem elementarna in ne terja vpeljave polinoma $g(X_1, X_2, X_3)$. Glavna tema Wilesovega dokaza je pravzaprav t. i. eliptična krivulja, podana z enačbo $y^2 = x(x - a^n)(x + b^n)$, torej množica ničel nekega drugega polinoma. Z omembo polinoma $g(X_1, X_2, X_3)$ smo želeli dati le droben namig o tem, kako se različna matematična področja prepletajo in kako se problemov lahko lotimo z različnih zornih kotov.

Naloge

1. Za vsako naravno število n poišči tak polinom $f(X) \in \mathbb{Z}_2[X]$, da je $f(X)(1 + X) = 1 + X^{n+1}$.
2. Ugotovi, za katera naravna števila n obstaja tak polinom $f(X) \in \mathbb{Z}_3[X]$, da je $f(X)(1 + X) = 1 + X^{n+1}$ in ga poišči.
3. Naj bo K kolobar brez deliteljev niča. Pokaži, da so v kolobarju $K[X]$ lahko obrnljivi le konstantni polinomi (kateri?). Poišči nekonstanten polinom, ki je obrnljiv element kolobarja $\mathbb{Z}_4[X]$.
4. Naj bo K komutativen kolobar in naj bo $a \in K$ tak, da je element $2a$ obrnljiv. Pokaži, da ima polinom $aX^2 + bX + c \in K[X]$ kako ničlo v K natanko tedaj, ko obstaja tak $d \in K$, da je $d^2 = b^2 - 4ac$. V tem primeru sta tako $x_1 := (2a)^{-1}(-b + d)$ kot $x_2 := (2a)^{-1}(-b - d)$ ničli. Če K nima deliteljev niča, drugih ničel v K ta polinom nima.
5. Pokaži, da zadnja ugotovitev prejšnje naloge v kolobarjih z delitelji niča ne velja vedno. Poišči na primer komutativen kolobar K, v katerem je element $2 := 1 + 1$ obrnljiv, polinom X^2 pa ima vsaj tri ničle v K.
6. Poišči vse ničle polinoma $f(X) = 1+X+X^2$ v $\mathbb{Z}_{19}$. Za katero praštevilo p ima $f(X)$ natanko eno ničlo v $\mathbb{Z}_p$? Poišči kako še tako praštevilo $p \neq 2$, da $f(X)$ v $\mathbb{Z}_p$ nima ničle.
7. Pokaži, da za vsak končen komutativen kolobar K z n elementi obstaja tak polinom $f(X) \in K[X]$ stopnje n, da je pripadajoča polinomska funkcija ničelna.

8. Naj bo K komutativen kolobar in naj bodo $f(X), g(X), h(X) \in K[X]$ taki polinomi, da je $f(X) = g(X)h(X)$. Pokaži, da potem za vsak $x \in K$ velja $f(x) = g(x)h(x)$.

   Komentar. Pojem vrednosti polinoma s koeficienti iz kolobarja K bi sicer načeloma lahko definirali tudi v primeru, ko kolobar K ni komutativen. Toda potem trditev naloge ne bi veljala. Zato je ta pojem za nekomutativne kolobarje nekoliko nenaraven.

9. Pokaži, da imata različna polinoma iz $\mathbb{R}[X]$ različni polinomski funkciji. Posploši na realne polinome več spremenljivk.

10. Polinomu v n spremenljivkah pravimo **homogen polinom**, če imajo vsi njegovi monomi isto stopnjo. Pokaži, da je $0 \neq f(X_1, \ldots, X_n) \in \mathbb{R}[X_1, \ldots, X_n]$ homogen polinom stopnje d natanko tedaj, ko za vse $\lambda, x_1, \ldots, x_n \in \mathbb{R}$ velja $f(\lambda x_1, \ldots, \lambda x_n) = \lambda^d f(x_1, \ldots, x_n)$.

11. Naj bo F polje. Za vsak polinom $f(X, Y) \in F[X, Y]$ naj $f(Y, X)$ označuje polinom, ki ga dobimo tako, da v polinomu $f(X, Y)$ zamenjamo vlogo spremenljivk X in Y (monom aX^kY^ℓ se pri tem preoblikuje v monom $aX^\ell Y^k$). Če je $f(Y, X) = f(X, Y)$, rečemo, da je $f(X, Y)$ **simetričen polinom**. Kot se hitro prepričamo, je množica vseh simetričnih polinomov podalgebra algebre $F[X, Y]$. Pokaži, da je generirana s polinomoma $s_1(X, Y) := X + Y$ in $s_2(X, Y) := XY$.

    Komentar. Na polinome v dveh spremenljivkah smo se omejili samo zaradi enostavnosti. Polinom $f(X_1, \ldots, X_n)$ v n spremenljivkah je simetričen, če za vsako permutacijo σ množice $\{1, \ldots, n\}$ velja

    $$f(X_{\sigma(1)}, \ldots, X_{\sigma(n)}) = f(X_1, \ldots, X_n).$$

    Simetrični polinomi sestavljajo podalgebro algebre $F[X_1, \ldots, X_n]$. **Osnovni izrek o simetričnih polinomih** pravi, da je ta podalgebra generirana s polinomi

    $$\begin{aligned} s_1(X_1, \ldots, X_n) &:= X_1 + X_2 + \cdots + X_n, \\ s_2(X_1, \ldots, X_n) &:= X_1X_2 + X_1X_3 + \cdots + X_{n-1}X_n, \\ &\vdots \\ s_n(X_1, \ldots, X_n) &:= X_1X_2 \cdots X_n. \end{aligned}$$

    Imenujemo jih **elementarni simetrični polinomi**.

12. Naj bo F polje. Algebra $F[X, Y]$ je očitno generirana z dvema elementoma, namreč z X in Y. Ali je generirana z enim samim elementom?

13. **Odvod** formalne potenčne vrste $f(X) = \sum_{k \geq 0} a_k X^k \in \mathbb{R}[X]$ definiramo kot $f'(X) = \sum_{k \geq 1} k a_k X^{k-1} \in \mathbb{R}[X]$. Kdaj je $f'(X) = f(X)$?

14. Naj bo K poljuben kolobar. Pokaži, da je $1 - X$ obrnljiv element kolobarja $K[[X]]$ in izračunaj njegov inverz.
15. Pokaži, da je formalna potenčna vrsta $\sum_{k\geq 0} a_k X^k$ obrnljiv element kolobarja $K[[X]]$ natanko tedaj, ko je a_0 obrnljiv element kolobarja K.
16. Korak naprej od kolobarja formalnih potenčnih vrst $K[[X]]$ je **kolobar Laurentovih vrst** $K((X))$. Njegovi elementi so formalne vrste $\sum_{k\in\mathbb{Z}} a_k X^k$, kjer je lahko samo končno mnogo elementov $a_{-1}, a_{-2}, \ldots$ različnih od 0. Seštevanje in množenje v $K((X))$ definiramo na samoumeven način (tako da je $K[[X]]$ podkolobar $K((X))$). Pokaži, da je $K((X))$ obseg, če je K obseg.

   Komentar. Iz danih obsegov tako gradimo nove. Če je K polje, je tudi $K((X))$ polje. Če pa je K nekomutativen obseg, je tak tudi obseg $K((X))$. Obseg kvaternionov $\mathbb{H}$ tako zdaj ni več edini nekomutativen obseg, ki ga poznamo!

2.7. Simetrična grupa

Povedali smo že, da grupo vseh permutacij množice

$$\mathbb{N}_n := \{1, \ldots, n\}$$

označujemo s S_n in ji pravimo **simetrična grupa** (gl. primer 1.36). Čeprav je operacija v S_n komponiranje, bomo namesto $\sigma \circ \pi$ pisali $\sigma\pi$ in temu rekli **produkt permutacij** σ in π. Enota v S_n je identična preslikava $\mathrm{id}_{\mathbb{N}_n}$, ki jo bomo označevali kar z 1. Permutacijo $\sigma \in S_n$, ki $k \in \mathbb{N}_n$ preslika v $i_k \in \mathbb{N}_n$, $1 \leq k \leq n$, označujemo z dvovrstičnim simbolom

$$\sigma = \begin{pmatrix} 1 & 2 & \ldots & n \\ i_1 & i_2 & \ldots & i_n \end{pmatrix}.$$

Tako na primer $\left(\begin{smallmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 1 & 3 \end{smallmatrix}\right)$ označuje permutacijo, ki 1 slika v 4, 2 ohrani (torej preslika vase), 3 slika v 1, 4 pa v 3.

Koliko je vseh permutacij? Preslikava iz končne množice vase je bijektivna natanko tedaj, ko je injektivna. Vprašanje si zato lahko zastavimo takole: koliko je injektivnih preslikav iz množice $\mathbb{N}_n$ vase? Vsaka taka preslikava, imenujmo jo σ, lahko preslika element 1 na n različnih načinov. Element 2 lahko preslika kamorkoli, razen v $\sigma(1)$; število možnih izbir je torej $n - 1$. Za element 3 imamo $n - 2$ možnosti itd. Vseh injektivnih preslikav je tako $n \cdot (n-1) \cdots 2 \cdot 1$. Torej je

$$|S_n| = n!,$$

kar si velja zapomniti.

Permutaciji, ki med seboj zamenja elementa i in j iz $\mathbb{N}_n$, vse druge elemente pa preslika vase, pravimo **transpozicija**. Označujemo jo z $(i\,j)$. Očitno je $(i\,j)^2 = 1$, torej je transpozicija sama sebi inverz. Hitro preverimo, da na

primer transpoziciji $(1\,2)$ in $(1\,3)$ ne komutirata. Zato je grupa S_n *nekomutativna*, brž ko je $n \geq 3$.

Pokažimo, da množica vseh transpozicij generira grupo S_n. Po dogovoru je produkt prazne množice elementov enak 1 (to potrebujemo zaradi primera, ko je $n = 1$).

TRDITEV 2.22. *Vsaka permutacija $\sigma \in S_n$ se da zapisati kot produkt transpozicij.*

DOKAZ. Dokazali bomo z indukcijo na n. Za $n = 1$ ni kaj dokazovati. Naj bo torej $n > 1$ in privzemimo, da trditev velja za $n-1$. Če je $\sigma(n) = n$, lahko σ interpretiramo kot element S_{n-1} in želeni zaključek velja. Če je $\sigma(n) = k \neq n$, pa produkt $(k\,n)\sigma$ slika n v n. Zato je $(k\,n)\sigma = \tau_1 \cdots \tau_r$ za neke transpozicije τ_i. Če pomnožimo to formulo z leve s $(k\,n)$ in upoštevamo, da je $(k\,n)^2 = 1$, dobimo zapis σ v obliki produkta transpozicij. □

Zapis permutacije v obliki produkta transpozicij žal ni enoličen. Na primer, $(1\,2)(1\,3) = (1\,3)(2\,3)$, $(2\,3) = (1\,2)(1\,3)(1\,2)$, $1 = (1\,2)(1\,2)$ ipd. V naslednji lemi bomo pokazali, da imajo vsi zapisi vendarle nekaj skupnega. Pred tem naredimo majhen razmislek, ki ga bomo potrebovali v dokazu.

Naj bo $f(X_1, \ldots, X_n)$ polinom v n spremenljivkah nad nekim kolobarjem. Za vsako permutacijo $\sigma \in S_n$ vpeljimo polinom $(\sigma f)(X_1, \ldots, X_n)$ takole:

$$(\sigma f)(X_1, \ldots, X_n) := f(X_{\sigma(1)}, \ldots, X_{\sigma(n)}).$$

Naj bo π neka nadaljnja permutacija. Če uporabimo zgornjo definicijo za π in polinom $(\sigma f)(X_1, \ldots, X_n)$, dobimo

$$(\pi(\sigma f))(X_1, \ldots, X_n) = (\sigma f)(X_{\pi(1)}, \ldots, X_{\pi(n)}). \tag{2.4}$$

Da bomo naslednji korak laže razumeli, uvedimo oznako $Y_i := X_{\pi(i)}$ za vsak $i \in \mathbb{N}_n$. Po definiciji je

$$(\sigma f)(Y_1, \ldots, Y_n) = f(Y_{\sigma(1)}, \ldots, Y_{\sigma(n)}) \text{ in } Y_{\sigma(i)} = X_{(\pi\sigma)(i)}.$$

Zato je desna stran v (2.4) enaka $f(X_{(\pi\sigma)(1)}, \ldots, X_{(\pi\sigma)(n)})$. S ponovno uporabe definicije vidimo, da lahko (2.4) zapišemo takole:

$$(\pi(\sigma f))(X_1, \ldots, X_n) = ((\pi\sigma)f)(X_1, \ldots, X_n). \tag{2.5}$$

TRDITEV 2.23. *Če permutacijo $\sigma \in S_n$ lahko zapišemo kot produkt sodega (oz. lihega) števila transpozicij, potem ima tudi vsak drug zapis σ v obliki produkta transpozicij sodo (oz. liho) število faktorjev.*

DOKAZ. Najprej pojasnimo idejo dokaza. Poiskali bomo tak neničeln polinom

$$f(X_1, \ldots, X_n) \in \mathbb{Z}[X_1, \ldots, X_n],$$

da bo za vsako transpozicijo τ veljalo

$$(\tau f)(X_1, \ldots, X_n) = -f(X_1, \ldots, X_n). \tag{2.6}$$

Iz te formule in iz (2.5) sledi, da je

$$((\tau_1 \cdots \tau_k)f)(X_1, \ldots, X_n) = (-1)^k f(X_1, \ldots, X_n)$$

za poljubne transpozicije $\tau_1, \ldots, \tau_k$. S tem bo dokazano, da σ ne moremo zapisati kot produkt sodega števila transpozicij in hkrati kot produkt lihega števila transpozicij.

Poiščimo torej tak polinom $f(X_1, \ldots, X_n)$. Če je $n = 2$, je izbira očitna: $f(X_1, X_2) = X_1 - X_2$. Za $n = 3$ je tak polinom

$$f(X_1, X_2, X_3) := (X_1 - X_2)(X_1 - X_3)(X_2 - X_3).$$

Res, v S_3 so tri transpozicije, $(1\,2), (1\,3)$ in $(2\,3)$, in za vsako izmed njih velja (2.6). Bralcu svetujemo, da se o tem prepriča. Zdaj lahko uganemo, da je v splošnem iskani polinom

$$f(X_1, \ldots, X_n) := \prod_{i<j}(X_i - X_j) = (X_1 - X_2)(X_1 - X_3)\ldots(X_{n-1} - X_n).$$

Vzemimo transpozicijo $\tau = (p\,q)$, $p < q$, in preverimo, da velja (2.6). Faktorji v polinomu $(\tau f)(X_1, \ldots, X_n)$ so do predznaka natančno enaki faktorjem v polinomu $f(X_1, \ldots, X_n)$. Tisti z drugačnim predznakom so poleg $X_q - X_p$ še $X_q - X_\ell$ in $X_\ell - X_p$, kjer je $p < \ell < q$. Slednji nastopajo v parih, zato je število vseh faktorjev z drugačnim predznakom liho. To dokazuje (2.6). □

Permutaciji pravimo **soda permutacija**, če jo lahko zapišemo kot produkt sodega števila transpozicij. Če jo lahko zapišemo kot produkt lihega števila transpozicij, pa ji pravimo **liha permutacija**. Zgornji trditvi povesta, da je vsaka permutacija soda ali liha, ne more pa biti oboje hkrati. Število

$$\operatorname{sgn}(\sigma) := \begin{cases} 1\,; & \sigma \text{ je soda permutacija} \\ -1\,; & \sigma \text{ je liha permutacija} \end{cases}$$

imenujemo **predznak** permutacije σ. Očitno je produkt dveh sodih permutacij soda permutacija, produkt sode permutacije z liho permutacijo je liha permutacija, produkt dveh lihih permutacij pa je soda permutacija. Te ugotovitve lahko povzamemo s formulo

$$\operatorname{sgn}(\pi\sigma) = \operatorname{sgn}(\pi)\operatorname{sgn}(\sigma) \quad \text{za vse } \pi, \sigma \in S_n.$$

Z izbiro $\pi = \sigma^{-1}$ dobimo

$$\operatorname{sgn}(\sigma^{-1}) = \operatorname{sgn}(\sigma)^{-1} \quad \text{za vse } \sigma \in S_n.$$

To pomeni, da je inverz sode permutacije soda permutacija, inverz lihe pa liha. Ker je množica sodih permutacij tudi zaprta za množenje, je podgrupa grupe S_n. Imenujemo jo **alternirajoča grupa** in označujemo z A_n.

Vsaka permutacija je torej zgrajena iz transpozicij. Oglejmo si še nekoliko drugačne gradnike permutacij. Permutaciji σ pravimo **cikel**, če obstajajo taki različni elementi $i_1, \ldots, i_k \in \mathbb{N}_n$, da σ preslika i_1 v i_2, i_2 v i_3 itd., i_k preslika v začetni element i_1, vse ostale elemente iz $\mathbb{N}_n$ pa ohrani. Opisani cikel je določen s k elementi, zato mu bolj natančno rečemo **cikel dolžine** k ali kar **k-cikel**. Označujemo ga z

$$(i_1\, i_2 \ldots i_k).$$

Denimo, permutacija $\left(\begin{smallmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 1 & 3 \end{smallmatrix}\right)$ je 3-cikel $(1\,4\,3)$. Lahko ga zapišemo tudi kot $(3\,1\,4)$ ali $(4\,3\,1)$, medtem ko je na primer $(1\,3\,4)$ drug 3-cikel. Transpozija ni nič drugega kot 2-cikel, vsak 1-cikel (i_1) pa je identiteta 1.

Vsaka permutacija je seveda enaka produktu ciklov, saj se jo da zapisati celo kot produkt transpozicij. Vendar pa se da pri razcepu permutacije na cikle povedati več. Najlažje je to razložiti na primeru. Vzemimo permutacijo

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 7 & 1 & 3 & 8 & 9 & 4 & 2 & 6 & 5 \end{pmatrix}.$$

Element 3 se s to permutacijo ohranja in v nekem smislu lahko nanj pozabimo. Opazujmo tole zaporedje slik:

$$1 \mapsto 7,\ 7 \mapsto 2,\ 2 \mapsto 1.$$

Znotraj σ smo torej našli 3-cikel $(1\,7\,2)$. Opazimo, da σ lahko zapišemo kot produkt $\sigma = (1\,7\,2)\sigma'$, kjer je

$$\sigma' = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 1 & 2 & 3 & 8 & 9 & 4 & 7 & 6 & 5 \end{pmatrix}.$$

Permutacija σ' poleg 3 ohranja tudi 1, 7 in 2. Zato se osredotočimo na preostalih pet elementov. Iz zaporedij slik

$$4 \mapsto 8,\ 8 \mapsto 6,\ 6 \mapsto 4 \quad \text{in} \quad 5 \mapsto 9,\ 9 \mapsto 5$$

razberemo, da je $\sigma' = (4\,8\,6)(5\,9)$. Torej lahko σ zapišemo kot produkt treh ciklov,

$$\sigma = (1\,7\,2)(4\,8\,6)(5\,9),$$

ki so drug od drugega popolnoma neodvisni v smislu, da nimajo skupnih elementov. V tem zapisu se nikjer ne pojavi številka 3. Lahko pišemo tudi

$$\sigma = (1\,7\,2)(4\,8\,6)(5\,9)(3),$$

saj je 1-cikel (3) enak identiteti.

Enako kot v tem primeru lahko obravnavamo poljubno permutacijo σ. Pričnimo z elementom 1 in si oglejmo zaporedje elementov

$$1, \sigma(1), \sigma^2(1), \ldots$$

iz $\mathbb{N}_n$. Ker je množica $\mathbb{N}_n$ končna, obstaja tako število $r \geq 1$, da so elementi

$$1, \sigma(1), \ldots, \sigma^{r-1}(1)$$

med seboj različni, $\sigma^r(1)$ pa je eden izmed njih. Dejansko je edina možnost, da je $\sigma^r(1) = 1$. Namreč, iz $\sigma^r(1) = \sigma^p(1)$, $0 \leq p < r$, sledi $\sigma^{r-p}(1) = 1$, zato je p lahko le 0. Tako pridemo do r-cikla

$$(1\,\sigma(1)\ldots\sigma^{r-1}(1))$$

in, kot v primeru, razcepa

$$\sigma = (1\,\sigma(1)\ldots\sigma^{r-1}(1))\sigma',$$

kjer permutacija σ' ohranja

$$1, \sigma(1), \ldots, \sigma^{r-1}(1).$$

Zatem nadaljujemo z obravnavo σ'. S ponavljanjem postopka na koncu pridemo do zapisa σ kot produkta takih ciklov, da nobena dva ne vsebujeta skupnega elementa. Takim ciklom pravimo **disjunktni cikli**. Povzetek razmisleka je torej tale trditev.

TRDITEV 2.24. *Vsaka permutacija $\sigma \in S_n$ se da zapisati kot produkt disjunktnih ciklov.*

Hitro se prepričamo, da disjunktni cikli med seboj komutirajo. Trditev 2.24 tako pove, da lahko vsak element grupe S_n zapišemo kot produkt razmeroma enostavnih elementov, ki povrh komutirajo drug z drugim. Trditev 2.22 pa pove, da ga lahko zapišemo kot produkt še enostavnejših elementov, vendar brez zaključka o komutiranju.

Zapis permutacije v obliki produkta disjunktnih ciklov je enoličen. To gotovo ni presenetljivo že zaradi načina, kako smo do tega zapisa prišli. Zato natančen dokaz izpustimo. Bolj previdno bi se izrazili takole: zapis je enoličen do vrstnega reda faktorjev natančno. Ker ti faktorji komutirajo, je njihov vrstni red seveda nepomemben.

Naloge

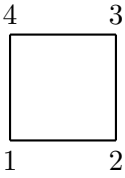
1. Naj bo $\sigma = \left(\begin{smallmatrix}1&2&3&4\\4&2&1&3\end{smallmatrix}\right)$ in $\pi = \left(\begin{smallmatrix}1&2&3&4\\3&4&1&2\end{smallmatrix}\right)$. Določi $\sigma\pi$, $\pi\sigma$, σ^{-1}, in π^{-1}.
2. Permutacijo
$$\sigma = \begin{pmatrix}1&2&3&4&5&6&7&8&9\\5&1&6&8&7&3&9&4&2\end{pmatrix}$$
zapiši kot produkt disjunktnih ciklov. Koliko je dolžina najdaljšega cikla? V spodnji vrstici med seboj zamenjaj dve številki tako, da bo v zapisu nove permutacije kot produkta disjunktnih ciklov nastopal kak cikel z daljšo dolžino.
3. Permutacijo $\sigma = (3\,5\,2)(5\,7\,1)(1\,3) \in S_7$ zapiši kot produkt disjunktnih ciklov. Poišči tudi permutacijo σ^{-1} in jo zapiši kot produkt disjunktnih ciklov.

4. Permutacijo $(1\,2)(2\,3)\cdots(k-1\,k)$ zapiši kot k-cikel.
5. Permutacijo $(1\,2)(1\,3)\cdots(1\,k)$ zapiši kot k-cikel.
6. Poišči inverz k-cikla $(i_1\,i_2\ldots i_k)$.
7. Pokaži, da ima k-cikel predznak $(-1)^{k-1}$.
8. Denimo, da je permutacija $\sigma \in S_n$ enaka produktu s disjunktnih ciklov, v katerih nastopajo vse številke iz $\mathbb{N}_n$ (tak zapis vedno obstaja, saj lahko dodajamo 1-cikle $(i) = 1$). S pomočjo prejšnje naloge pokaži, da je $\operatorname{sgn}(\sigma) = (-1)^{n-s}$.
9. Spomnimo se, da je red elementa a grupe G najmanjše naravno število r z lastnostjo $a^r = 1$. Pokaži, da je red k-cikla enak k.
10. Pokaži, da je red vsake permutacije enak najmanjšemu skupnemu večkratniku dolžin disjunktnih ciklov, ki sestavljajo permutacijo.
11. V grupi S_{10} poišči kako permutacijo z maksimalnim redom. Ali v grupah S_{11} in S_{12} obstajajo elementi z višjim redom?
12. Naj bo σ k-cikel, $k \geq 3$. Pokaži, da je σ^2 cikel natanko tedaj, ko je k lih.
13. Pokaži, da za vsako permutacijo $\pi \in S_n$ in vsak k-cikel $(i_1\,i_2\ldots i_k) \in S_n$ velja $\pi(i_1\,i_2\ldots i_k) = (\pi(i_1)\,\pi(i_2)\ldots\pi(i_k))\pi$.
14. Naj bo permutacija $\sigma \in S_n$ enaka produktu disjunktnih ciklov dolžin $k_1, \ldots, k_r$. Če je permutacija $\sigma' \in S_n$ prav tako enaka produktu disjunktnih ciklov dolžin $k_1, \ldots, k_r$, bomo rekli, da ima σ' *enako zgradbo disjunktnih ciklov* kot σ. Na primer, permutaciji $(1\,2\,3)(4\,5\,6)(7\,8)$ in $(4\,2\,5)(8\,1)(6\,3\,7)$ imata enako zgradbo disjunktnih ciklov. Še ena definicija, ki pa pravzaprav ni nova (gl. razdelek 1.6): za permutaciji $\sigma, \sigma' \in S_n$ rečemo, da sta si *konjugirani*, če obstaja taka permutacija $\pi \in S_n$, da je $\sigma' = \pi\sigma\pi^{-1}$. S pomočjo prejšnje naloge pokaži:
   (a) Vsaka permutacija, ki je konjugirana k-ciklu, je sama k-cikel.
   (b) Poljubna k-cikla v S_n sta si konjugirana.
   (c) Permutaciji σ in σ' sta si konjugirani natanko tedaj, ko imata enako zgradbo disjunktnih ciklov.
15. Pokaži, da je grupa S_n generirana s transpozicijami $(1\,2)$, $(2\,3)$, $\ldots$, $(n-1\,n)$.
16. Pokaži, da je grupa S_n generirana s transpozicijo $(1\,2)$ in n-ciklom $(1\,2\ldots n)$.
17. Pokaži, da je $Z(S_n)$, center grupe S_n, enak $\{1\}$ za vsak $n \geq 3$.
18. Pokaži, da je $Z(A_n) = \{1\}$ za vsak $n \geq 4$.
19. Pokaži, da je $|A_n| = \frac{n!}{2}$, če je $n > 1$.

20. Pokaži, da je za vsak $n \geq 3$ grupa A_n generirana z množico vseh 3-ciklov.

2.8. Diedrska grupa

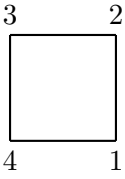
Zamislimo si kvadrat v ravnini. Njegova oglišča označimo z 1, 2, 3 in 4 kot na sliki.



Kvadrat iz ravnine premaknimo v prostor in zatem spet vrnimo na izpraznjeno mesto v ravnini. Pred tem ga lahko v prostoru poljubno premikamo, med drugim tudi obrnemo na glavo. Zato oglišča morda zamenjajo mesto. Vsaki taki transformaciji kvadrata pravimo **simetrija**. Pri tem nas zanima samo končna lega kvadrata, ne pa gibanje v prostoru, ki je do nje vodilo.

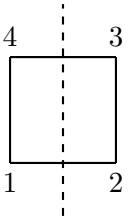
Na simetrijo lahko gledamo kot na permutacijo oglišč. V tem smislu produkt dveh simetrij geometrijsko ustreza zaporedni izvedbi ene simetrije za drugo. Kar je seveda spet simetrija. Identiteta 1 je simetrija (lege kvadrata ne spremenimo). Prav tako je inverz simetrije spet simetrija (prestavljeni kvadrat lahko vrnemo v začetno lego). Množica vseh simetrij je torej podgrupa simetrične grupe S_4. Imenujemo jo **diedrska grupa reda 8** in označujemo z D_8. Kot bomo videli, je njen red, torej število elementov, res 8. Kateri so ti elementi?

Če naš kvadrat zavrtimo (rotiramo) za kot 90^o v nasprotni smeri urinega kazalca, preide v tole lego:

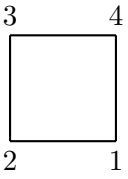


Označimo to simetrijo z r. Kot permutacijo jo lahko opredelimo kot 4-cikel $(1\,2\,3\,4)$, a raje nadaljujmo z geometrijskim razmišljanjem. Simetrija r^2 ustreza vrtenju za kot 180^o, simetrija r^3 vrtenju za kot 270^o, medtem ko je $r^4 = 1$. Tako smo našli štiri elemente grupe D_8: $1, r, r^2$ in r^3. Do preostalih pridemo tako, da kvadrat najprej obrnemo na glavo in ga potem zavrtimo. Obračanje

lahko izvedemo na različne načine. Enega izmed njih lahko opredelimo kot zrcaljenje preko premice:



S tem kvadrat preide v tole lego:



Označimo to simetrijo z z; kot permutacija je z produkt transpozicij $(1\,2)$ in $(3\,4)$. (Lahko bi izbrali tudi zrcaljenje preko vertikalne premice ali preko ene izmed diagonal; odločili smo se pač za eno izmed možnosti.)

Zdaj lahko navedemo vse elemente naše grupe:

$$D_8 = \{1, r, r^2, r^3, z, rz, r^2z, r^3z\}.$$

Ni se težko prepričati, da je vseh osem elementov med seboj različnih. Več kot osem pa simetrij kvadrata ne more biti. Namreč, vsaka simetrija je določena z dvema podatkoma. Prvi je, na katero od štirih mest preide prvo oglišče. Drugi pa je, ali kvadrat obrnemo na glavo ali ne. Torej je vseh simetrij (največ) $4 \times 2 = 8$.

Elementa r in z očitno generirata grupo D_8. Ker je $rz \neq zr$ (zakaj?), grupa ni Abelova. Omenimo še zveze

$$r^4 = 1, \;\; z^2 = 1, \;\; (rz)^2 = 1.$$

Izpeljemo jih lahko geometrijsko ali pa z računanjem v simetrični grupi S_4.

Na enak način obravnavamo simetrije pravilnega n-kotnika za poljuben $n \geq 3$. Na primer, ko je $n = 4$, smo se omejili le zaradi lažje predstave. Grupi simetrij pravilnega n-kotnika pravimo **diedrska grupa reda** $2n$. Označevali jo bomo z D_{2n} (navade so sicer različne, nekateri to grupo označujejo z D_n). Generirana je z rotacijo r (za kot $\frac{360^\circ}{n}$) in zrcaljenjem z, ki ne komutirata. Pri tem veljajo enakosti

$$r^n = 1, \;\; z^2 = 1, \;\; (rz)^2 = 1$$

in

$$D_{2n} = \{1, r, \ldots, r^{n-1}, z, rz, \ldots r^{n-1}z\}.$$

Diedrsko grupo lahko obravnavamo kot podgrupo simetrične grupe. Za velike n je D_{2n} razmeroma majhna podgrupa S_n, saj je $|D_{2n}| = 2n$ in $S_n = n!$. Za $n = 3$ pa je red obeh grup enak 6, zato je $D_6 = S_3$.

Doslej smo privzemali, da je $n \geq 3$. Za $n = 2$ definiramo D_4 kot grupo simetrij pravotnika, ki ni kvadrat. Sestavljajo jo identiteta 1, rotacija r za kot 180^o, zrcaljenje z in produkt rz. Pri tem je $zr = rz$, zato je grupa D_4 Abelova. Diedrsko grupo D_2 pa sestavljata elementa 1 in r, pri čemer je $r^2 = 1$. Diedrskih grup D_2 in D_4 ne moremo obravnavnati kot podgrupi simetričnih grup S_1 in S_2, saj imata slednji le en oziroma dva elementa.

Besedo simetrija v matematiki uporabljamo tudi v drugih situacijah. Običajno imamo s tem v mislih preslikave, ki ohranjajo neke matematične objekte. Simetrije množice $\{1, \ldots, n\}$ so tako kar permutacije, torej elementi simetrične grupe S_n. Pogled lahko obrnemo in obravnavamo simetrične objekte, torej objekte, ki jih neke preslikave ohranjajo. Na različne načine se s simetričnimi objekti srečujemo tudi v umetnosti. Študij simetrij je tako eno tistih področij, kjer se matematika najbolj približa umetnosti – ali, bolje rečeno, njenim drugim zvrstem, saj tudi matematiko lahko prištevamo med oblike umetnosti.

Naloge

1. Poišči vse take elemente $x \in D_{2n}$, da je $x^2 = 1$.
2. Poišči vse take elemente $x \in D_{2n}$, da je $rxr = x$.
3. Poišči vse take elemente $x \in D_{2n}$, da je $xzx = z$.
4. Poišči $C(r)$, centralizator elementa $r \in D_{2n}$ (gl. nalogo 1.6/8).
5. Poišči $C(z)$, centralizator elementa $z \in D_{2n}$.
6. Naj bo $n \geq 3$. Pokaži, da je $Z(D_{2n})$, center grupe D_{2n}, enak $\{1\}$, če je n lih, in $\{1, r^{\frac{n}{2}}\}$, če je n sod.
7. Elementu k grupe G pravimo **komutator**, če obstajata taka $x, y \in G$, da je $k = xyx^{-1}y^{-1}$ (očitno je $k = 1$ natanko tedaj, ko x in y komutirata – od tod ime). Pokaži, da je množica vseh komutatorjev v D_{2n}, kjer je $n \geq 3$, enaka podgrupi, generirani z r^2.

   Komentar. V splošnem množica vseh komutatorjev grupe ni podgrupa.
8. Poleg končnih diedrskih grup D_{2n} poznamo tudi **neskončno diedrsko grupo** D_∞. Definiramo jo kot podgrupo grupe $\mathrm{Sim}(\mathbb{R})$, torej grupe vseh bijektivnih preslikav iz $\mathbb{R}$ v $\mathbb{R}$, generirano s preslikavama $r, z : \mathbb{R} \to \mathbb{R}$, $r(x) = x + 1$, $z(x) = -x$. Pokaži, da je $r^n \neq 1$ za vse $n \in \mathbb{Z} \setminus \{0\}$, $z^2 = 1$, $(rz)^2 = 1$ in $D_\infty = \{r^n, r^n z \mid n \in \mathbb{Z}\}$.

9. Pokaži, da je vsaka izmed grup D_{2n} in D_∞ generirana s takim parom elementov u in w, da je $u^2 = w^2 = 1$.

   Komentar. Najbrž ni težko uganiti, katera elementa u in w izbrati. Sporočilo naloge pa je vseeno zanimivo, še posebej v luči naloge 3.1/22.

POGLAVJE 3

Homomorfizmi

V matematiki so nam včasih kake stvari intuitivno sicer razumljive, a jih ne znamo izraziti v besedah. Zato moramo zgraditi jezik, ki omogoča jasen opis. Jezik algebre v veliki meri sloni na pojmu homomorfizma.

Homomorfizmi so preslikave med algebrskimi strukturami (torej grupami, kolobarji itd.), ki ohranjajo operacije in s tem značilnosti struktur. Potrebujemo jih, da grupe (kolobarje itd.) med seboj primerjamo in prehajamo iz ene v drugo.

3.1. Izomorfnost grup in ciklične grupe

V matematiki pogosto ne ločujemo med sicer različnimi objekti, če imajo ključne lastnosti enake. Kdaj ni treba razlikovati med dvema grupama?

3.1.1. Izomorfnost grup. Do odgovora na zastavljeno vprašanje nas bo vodil naslednji primer.

Primer 3.1. Končno grupo lahko predstavimo s **Cayleyevo tabelo**. Na primer, Cayleyeva tabela grupe $(\mathbb{Z}_4, +)$ je

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

Vsota dveh elementov leži na križišču vrstice in stolpca, ki ju ta elementa začenjata. Oglejmo si še grupo kompleksnih števil

$$U_4 := \{1, i, -1, -i\}.$$

Operacija v tej grupi je seveda množenje. Na prvi pogled se morda zdi, da razen istega števila elementov grupi $\mathbb{Z}_4$ in U_4 nimata veliko skupnega. Toda zapišimo Cayleyevo tabelo grupe U_4:

$\cdot$	1	i	-1	$-i$
1	1	i	-1	$-i$
i	i	-1	$-i$	1
-1	-1	$-i$	1	i
$-i$	$-i$	1	i	-1

Oznake so sicer različne, toda zgradbi obeh tabel sta enaki. Element 0 v prvi tabeli se pojavlja na istih elementih kot element 1 v drugi tabeli. Prav tako se na istih mestih pojavljata elementa 1 in i, 2 in -1, in 3 in $-i$. Čeprav sta formalno različni, se ti grupi v bistvu ne razlikujeta. S stališča teorije grup ju lahko imamo za enaki.

Zgornje opažanje bomo bolje razumeli, če si ogledamo splošnejši primer.

PRIMER 3.2. Števila iz U_4 lahko opišemo kot rešitve enačbe $z^4 = 1$ v množici kompleksnih števil. Vzemimo zdaj poljubno naravno število n in vpeljimo

$$U_n := \{z \in \mathbb{C} \mid z^n = 1\}.$$

Zlahka preverimo, da je U_n grupa za množenje. Iz elementarne teorije kompleksnih števil vemo, da je $|U_n| = n$ in da so vsi elementi iz U_n potence števila

$$a := \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}.$$

Natančneje, če označimo $z_k := a^k$, $k = 0, 1, \ldots, n-1$, je

$$U_n = \{z_0, z_1, \ldots, z_{n-1}\}.$$

Očitno je

$$z_k z_\ell = \begin{cases} z_{k+\ell} & ; \ k+\ell < n \\ z_{k+\ell-n} & ; \ k+\ell \geq n \end{cases}$$

To lahko zapišemo bolj enostavno kot

$$z_k z_\ell = z_{k+\ell},$$

kjer je $k + \ell$ vsota k in ℓ v grupi $\mathbb{Z}_n$. Množenje elementov z_k iz U_n torej ustreza seštevanju njihovih indeksov v grupi $\mathbb{Z}_n$. Grupi U_n in $\mathbb{Z}_n$ se v bistvu razlikujeta le v oznakah. Bolj natančno to lahko opredelimo s preslikavo

$$\varphi : U_n \to \mathbb{Z}_n, \ \ \varphi(z_k) = k,$$

ki prevede grupo U_n v grupo $\mathbb{Z}_n$; je namreč bijektivna in povezuje množenje v U_n s seštevanjem v $\mathbb{Z}_n$ preko formule

$$\varphi(z_k z_\ell) = \varphi(z_k) + \varphi(z_\ell) \ \text{ za vse } k, \ell = 0, 1, \ldots, n-1. \tag{3.1}$$

Kako torej prepoznati »enakost« dveh grup? Seveda ne gre za enakost v dobesednem pomenu. Izraz, ki ga uporabljamo, je **izomorfnost**. Pravimo, da sta si **grupi** G in G' **izomorfni**, če obstaja taka bijektivna preslikava $\varphi : G \to G'$, da velja

$$\varphi(xy) = \varphi(x)\varphi(y) \text{ za vse } x, y \in G.$$

Vsaki taki preslikavi φ pravimo **izomorfizem grup**. Izomorfnost grup G in G' označimo z

$$G \cong G'.$$

V definiciji smo obe operaciji označili kot množenje. Če je katera izmed operacij seštevanje, zapis pač ustrezno spremenimo. Iz formule (3.1) tako razberemo, da sta si grupi U_n in $\mathbb{Z}_n$ izomorfni, torej $U_n \cong \mathbb{Z}_n$.

Izomorfizem grup pretvori operacijo v prvi grupi v operacijo v drugi grupi. Zaradi lažje predstave si zamislimo, da je G končna grupa. Če ji je grupa G' izomorfna, imata G in G' enaki, le drugače označeni Cayleyevi tabeli. Res, če označimo elemente iz G z $g_1, \ldots, g_n$ in zapišemo ustrezno Cayleyevo tabelo, potem je Cayleyeva tabela grupe G' prav taka, le da je povsod na mestu g_i zapisan $\varphi(g_i)$, kjer je φ izomorfizem iz G v G'.

Na prvi pogled v definiciji izomorfnosti grupi G in G' ne nastopata simetrično. Govorili smo o izomorfizmu iz G v G' in ne iz G' v G. Toda iz naslednje trditve sledi, da izomorfizem grup iz G v G' obstaja natanko tedaj, ko obstaja izomorfizem grup iz G' v G. S φ^{-1} bomo označili inverzno preslikavo preslikave φ, ki zaradi bijektivnosti φ res obstaja.

Trditev 3.3. *Če je $\varphi : G \to G'$ izomorfizem grup, je tudi $\varphi^{-1} : G' \to G$ izomorfizem grup.*

Dokaz. Seveda je preslikava φ^{-1} bijektivna. Dokazati moramo, da je

$$\varphi^{-1}(uv) = \varphi^{-1}(u)\varphi^{-1}(v)$$

za poljubna $u, v \in G'$. Zaradi injektivnosti φ je dovolj pokazati, da je

$$\varphi(\varphi^{-1}(uv)) = \varphi(\varphi^{-1}(u)\varphi^{-1}(v)).$$

To pa je res, saj sta obe strani enaki uv. Za levo stran je to očitno, za desno stran pa moramo uporabiti predpostavko, da je φ izomorfizem. □

Oglejmo si še nekaj primerov. Prvi je trivialen.

Primer 3.4. Za vsako grupo G velja

$$G \cong G.$$

Najenostavnejši primer izomorfizma iz G v G je identična preslikava id_G.

PRIMER 3.5. Znana lastnost eksponentne funkcije $x \mapsto e^x$ je $e^{x+y} = e^x e^y$. Kako to interpretirati v jeziku algebre? Eksponentna funkcija je izomorfizem iz grupe realnih števil za seštevanje v grupo pozitivnih realnih števil za množenje. Torej je

$$(\mathbb{R}, +) \cong (\mathbb{R}^+, \cdot).$$

PRIMER 3.6. Grupa $(\mathbb{Z}, +)$ je izomorfna vsaki svoji netrivialni podgrupi. Res, po posledici 2.2 je vsaka netrivialna podgrupa oblike $n\mathbb{Z}$ za neki $n \in \mathbb{N}$, in $x \mapsto nx$ je izomorfizem iz $\mathbb{Z}$ v $n\mathbb{Z}$.

Končna grupa pa ne more biti izomorfna svoji pravi podgrupi. Izomorfni grupi imata namreč isti red, saj je izomorfizem bijektivna preslikava.

3.1.2. Ciklične grupe in red elementa. Grupe iz primerov 3.1 in 3.6 imajo skupno lastnost, ki jo opisuje naslednja definicija.

DEFINICIJA 3.7. Grupi, ki je generirana z enim samim elementom, pravimo **ciklična grupa**.

Ciklično grupo, generirano z elementom a, označujemo z $\langle a \rangle$ (gl. razdelek 1.7). Vsak element v $\langle a \rangle$ je oblike a^k za neki $k \in \mathbb{Z}$, in obratno, vsak element oblike a^k leži v $\langle a \rangle$. Torej je

$$\langle a \rangle = \{a^k \mid k \in \mathbb{Z}\}.$$

Na primer, $U_4 = \langle i \rangle = \langle -i \rangle$.

V aditivni grupi namesto a^k seveda pišemo ka. Grupa $(\mathbb{Z}, +)$ je generirana z elementom 1 (kot tudi z -1) in je torej ciklična. Tudi grupa $(\mathbb{Z}_n, +)$, kjer je n poljubno naravno število, je ciklična. Generirana je z elementom 1, če je le $n > 1$. Za $n = 1$ je to trivialna grupa, generirana z elementom 0.

Vsaka ciklična grupa je Abelova, saj je

$$a^k \cdot a^\ell = a^{k+\ell} = a^\ell \cdot a^k.$$

Naslednji izrek bo povedal veliko več: v bistvu so edine ciklične grupe te, ki smo jih omenili v prejšnjem odstavku. V dokazu bomo ponovili nekatere razmisleke, ki smo jih naredili prej, med drugim v primeru 3.1.

IZREK 3.8. *Ciklična grupa G je izomorfna bodisi grupi $(\mathbb{Z}, +)$ bodisi grupi $(\mathbb{Z}_n, +)$ za neki $n \in \mathbb{N}$.*

DOKAZ. Naj bo a element, ki generira G. Torej je $G = \langle a \rangle$.

Privzemimo najprej, da so vsi elementi a^k med seboj različni, torej da iz $a^k = a^\ell$ sledi $k = \ell$. To pomeni, da je preslikava

$$\varphi : \mathbb{Z} \to G,\ \varphi(k) = a^k,$$

injektivna. Ker je $G = \langle a \rangle$, je φ tudi surjektivna. Očitno tudi velja

$$\varphi(k + \ell) = a^{k+\ell} = a^k a^\ell = \varphi(k)\varphi(\ell).$$

Torej je φ izomorfizem grup.

Obravnavajmo drugo možnost, ko obstajata taki celi števili k in ℓ, da je $k < \ell$ in je $a^k = a^\ell$. Slednjo enakost lahko zapišemo kot $a^{\ell-k} = 1$. Torej obstajajo taka naravna števila s, da je $a^s = 1$. Naj bo n najmanjše izmed njih. Trdimo, da je tedaj

$$|G| = n \text{ in } G = \{1, a, \dots, a^{n-1}\}. \tag{3.2}$$

Če je $0 \le p < q < n$, sta elementa a^p in a^q res različna, saj bi sicer za naravno število $q - p$ veljalo $a^{q-p} = 1$ in $q - p < n$. Torej je $|G| \ge n$. Vzemimo zdaj poljuben element $a^k \in G$. Po osnovnem izreku o deljenju (izrek 2.1) obstajata taki celi števili q in r, da je $k = qn + r$ in je $0 \le r < n$. Zato je

$$a^k = a^{qn+r} = (a^n)^q a^r = a^r,$$

kar dokazuje (3.2). Kot v primeru 3.1 označimo $z_k := a^k$, $k = 0, 1, \dots, n-1$. Očitno je $z_k z_\ell = z_{k+\ell}$, kjer je $k + \ell$ vsota k in ℓ v grupi $\mathbb{Z}_n$. Zato je

$$\varphi : G \to \mathbb{Z}_n,\ \varphi(z_k) = k,$$

izomorfizem grup. □

Ker imata izomorfni grupi isti red, je torej vsaka končna ciklična grupa reda n izomorfna grupi $(\mathbb{Z}_n, +)$, vsaka neskončna ciklična grupa pa grupi $(\mathbb{Z}, +)$.

Ciklične grupe so pomembne, ker jih najdemo znotraj vsake grupe G. Namreč, vsak element $a \in G$ generira **ciklično podgrupo** $\langle a \rangle$. Ta podgrupa je tesno povezana z naslednjim pomembnim pojmom, s katerim smo se srečevali že v nalogah.

Definicija 3.9. Naj bo a element grupe G. Če obstaja kako tako naravno število s, da je $a^s = 1$, potem rečemo, da ima element a **končen red**. Najmanjšemu naravnemu številu s to lastnostjo pravimo **red elementa** a. Če je $a^s \ne 1$ za vsa naravna števila s, pa rečemo, da ima a **neskončen red**.

Element a ima končen red natanko tedaj, ko je ciklična podgrupa $\langle a \rangle$ končna. Če ima a red n, potem je $\langle a \rangle = \{1, a, \dots, a^{n-1}\}$ in $|\langle a \rangle| = n$. Torej je

$$\text{red } a = |\langle a \rangle|. \tag{3.3}$$

Z besedami: red elementa a je enak redu ciklične podgrupe, ki jo a generira.

Končna grupa seveda ne more vsebovati neskončne ciklične podgrupe, zato ima v njej vsak element končen red. V grupi $(\mathbb{Z}, +)$, denimo, pa imajo z izjemo ničelnega vsi elementi neskončen red. V aditivni grupi je seveda red elementa a najmanjše naravno število n, za katero velja $na = 0$.

Primer 3.10. V grupi $(\mathbb{Z}_4, +)$ ima element 0 red 1, element 2 ima red 2, elementa 1 in 3 pa red 4. Diedrska grupa D_4 (gl. razdelek 2.8) ima prav tako 4 elemente, vendar imajo razen enote vsi njeni elementi red enak 2. Ker

izomorfizem grup očitno ohranja red vsakega elementa, grupi $\mathbb{Z}_4$ in D_4 nista izomorfni. Bralec naj se prepriča, da je grupa D_4 izomorfna grupi $(\mathbb{Z}_2 \oplus \mathbb{Z}_2, +)$.

Naloge

1. Pokaži, da je v vsaki grupi red elementa x enak redu elementa x^{-1}.
2. Pokaži, da je v vsaki grupi red elementa xy enak redu elementa yx.
3. Naj bo G netrivialna ciklična grupa. Denimo, da ima en sam generator, da torej le za en element $a \in G$ velja $G = \langle a \rangle$. Pokaži, da je $G \cong \mathbb{Z}_2$.
4. Pokaži, da grupa $(\mathbb{Z}_2 \oplus \mathbb{Z}_2, +)$ ni ciklična, grupa $(\mathbb{Z}_3 \oplus \mathbb{Z}_2, +)$ pa je (in je zato izomorfna grupi $(\mathbb{Z}_6, +)$).

   Komentar. Odgovor na splošno vprašanje, za katere $m, n \in \mathbb{N}$ je grupa $(\mathbb{Z}_m \oplus \mathbb{Z}_n, +)$ ciklična, je podan v nalogi 8. Pot do nje vodi preko naslednjih treh nalog.
5. Naj bo a element grupe G. Pokaži:
   (a) Če je $a^m = 1$, kjer je $m \in \mathbb{Z}$, je m deljiv z redom elementa a.
   (b) Če $a \neq 1$ in je $a^p = 1$ za neko praštevilo p, je p red elementa a.

   Namig. Osnovni izrek o deljenju.
6. Naj bo red elementa a grupe G naravno število m, red elementa $b \in G$ pa naravno število n. Denimo, da a in b komutirata. Pokaži, da red elementa ab deli najmanjši skupni večkratnik števil m in n. S primerom pokaži, da mu ni nujno enak.
7. Naj bo m red elementa a grupe G, n pa red elementa b grupe H. Pokaži, da je red elementa $(a, b) \in G \times H$ najmanjši skupni večkratnik števil m in n.
8. Naj bosta G in H končni ciklični grupi. Pokaži, da je grupa $G \times H$ ciklična natanko tedaj, ko sta si števili $|G|$ in $|H|$ tuji.

   Namig. Končna grupa K je ciklična natanko tedaj, ko vsebuje element reda $|K|$.
9. Naj bo $G = \langle a \rangle$ končna ciklična grupa reda n. Pokaži, da element a^k generira G natanko tedaj, ko sta si števili k in n tuji.

   Komentar. Število vseh generatorjev grupe $(\mathbb{Z}_n, +)$ torej sovpada s številom obrnljivih elementov kolobarja $(\mathbb{Z}_n, +, \cdot)$ in je enako $\varphi(n)$, kjer je φ Eulerjeva funkcija – glej nalogo 2.2/10.
10. Pokaži, da končna ciklična grupa G reda n vsebuje podgrupo reda d natanko tedaj, ko $d \mid n$. Pokaži tudi, da je taka podgrupa ena sama.

    Komentar. Kot vidimo iz komentarja k prejšnji nalogi, ima ta podgrupa $\varphi(d)$ različnih generatorjev. Vsak izmed njih ima red d, in obratno,

vsak element reda d generira to (edino) podgrupo reda d. Torej ima grupa G natanko $\varphi(d)$ elementov reda d. Če v mislih G razbijemo na podmnožice, v katerih imajo vsi elementi isti red, tako dobimo formulo

$$n = \sum_{d \mid n} \varphi(d).$$

11. Naj ima element a grupe G red 5. Koliko je red elementa $b \in G$, če $b \neq 1$ in je $bab = a$? Koliko je red elementa $c \in G$, če $c \neq 1$ in je $ac = c^2a$?

    Namig. Oglej si $a^j b a^{-j}$ in $a^j c a^{-j}$, $j = 1, 2, \ldots$, in uporabi nalogo 5.

12. Pokaži, da je vsaka podgrupa ciklične grupe ciklična.

    Namig. Za neskončno ciklično grupo $\mathbb{Z}$ to pove posledica 2.2. Za splošne ciklične grupe je treba samo preurediti dokaz.

13. Pokaži, da ima neskončna grupa neskončno mnogo podgrup.

    Namig. Loči med primeroma, ko imajo vsi elementi grupe končen red in ko obstaja element z neskončnim redom.

14. Naj bo G končna Abelova grupa, ki vsebuje kak element reda 2. Pokaži, da je produkt vseh elementov v G enak produktu vseh elementov v G, ki imajo red 2 (zato ima ta produkt red 1 ali 2).

    Namig. Če red elementa x ni 1 ali 2, je $x \neq x^{-1}$.

15. Pokaži, da za vsak element x iz polja F iz $x^2 = 1$ sledi $x = 1$ ali $x = -1$. Z uporabo ugotovitve prejšnje naloge za grupo $\mathbb{Z}_p^*$, tj. grupo vseh obrnljivih elementov polja $\mathbb{Z}_p$, od tod izpelji **Wilsonov izrek**: naravno število p je praštevilo natanko tedaj, ko je

$$(p-1)! \equiv -1 \pmod{p}.$$

16. Pokaži, da je podgrupa grupe $\mathrm{GL}_2(\mathbb{R})$, generirana z matriko $\left[\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right]$, izomorfna grupi $(\mathbb{Z}, +)$.

17. Pokaži, da je podgrupo grupe $\mathrm{GL}_2(\mathbb{C})$, generirana z matrikama $\left[\begin{smallmatrix} i & 0 \\ 0 & -i \end{smallmatrix}\right]$ in $\left[\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right]$, izomorfna kvaternionski grupi Q.

    Komentar. Nasploh imamo pri iskanju izomorfizmov nekaj svobode, možnosti je več. Res se včasih kak izomorfizem zdi naraven in ga opazimo takoj (tako naj bi bilo v nalogi 16). V kvaternionski grupi Q pa ima več elementov povsem enake lastnosti, zato ima tudi naloga več »naravnih« rešitev.

18. Pokaži, da je diedrska grupa D_8 izomorfna podgrupi ortogonalne grupe $\mathrm{O}_2(\mathbb{R})$, generirani z matrikama $R = \left[\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right]$ in $Z = \left[\begin{smallmatrix} -1 & 0 \\ 0 & 1 \end{smallmatrix}\right]$.

    Komentar. Bralec, ki pozna pomen ortogonalnih matrik, bo rešitev znal pojasniti tudi geometrijsko.

19. Pokaži, da je grupa $\mathrm{GL}_2(\mathbb{Z}_2)$ izomorfna simetrični grupi S_3.

    Namig. Izomorfizem ohranja red elementov.

20. Diedrska grupa D_8 in kvaternionska grupa Q imata obe red 8 in sta obe nekomutativni. Kljub temu si nista izomorfni. Zakaj?

21. Pokaži, da si nobeni izmed grup $(\mathbb{R}^+, \cdot)$, $(\mathbb{R} \setminus \{0\}, \cdot)$ in $(\mathbb{C} \setminus \{0\}, \cdot)$ nista izomorfni.

    Komentar. Prva grupa je prava podgrupa druge grupe, druga pa tretje. Toda to še ni razlog za to, da si grupe niso izomorfne – glej primer 3.6.

22. Naj bo grupa G generirana z elementoma u in w, ki imata oba red enak 2. Označimo uw^{-1} s s. Dokaži:
    (a) Če ima s končen red n, je G izomorfna diedrski grupi D_{2n}.
    (b) Če ima s neskončen red, je G izomorfna neskončni diedrski grupi D_∞.

    Nasvet. Najprej pokaži, da lahko vsak element v G zapišemo kot s^i ali $s^j w$ za neki celi števili i in j, in da element oblike s^i ne more biti enak elementu oblike $s^j w$.

3.2. Izomorfnost vektorskih prostorov

Podobno kot izomorfnost grup vpeljemo izomorfnost drugih algebrskih struktur. Naj bosta zdaj V in V' vektorska prostora nad poljem F. Pravimo, da je preslikava $\varphi : V \to V'$ **linearna**, če velja

$$\varphi(x+y) = \varphi(x) + \varphi(y) \text{ in } \varphi(\lambda x) = \lambda\varphi(x) \text{ za vse } x, y \in V,\ \lambda \in F.$$

Ta pogoja lahko nadomestimo z enim samim, ekvivalentnim pogojem, da je

$$\varphi(\lambda x + \mu y) = \lambda\varphi(x) + \mu\varphi(y) \text{ za vse } x, y \in V,\ \lambda, \mu \in F.$$

Najbrž je to bralcu znano iz linearne algebre, v vsakem primeru pa je dokaz enostaven in mu ga prepuščamo. Bijektivni linearni preslikavi iz V v V' pravimo **izomorfizem vektorskih prostorov**. Če taka preslikava obstaja, pravimo, da sta si prostora V in V' **izomorfna**.

V naslednjem izreku se omejimo na končno-razsežne vektorske prostore. Dejansko izrek velja tudi za neskončno-razsežne prostore, če definiramo dimenzijo prostora kot kardinalno število njegove baze (ki vedno obstaja, gl. dodatek A). Toda v to se ne bomo spuščali.

Izrek 3.11. *Končno-razsežna vektorska prostora V in V' nad poljem F sta si izomorfna natanko tedaj, ko imata enako dimenzijo.*

Dokaz. Naj bo φ izomorfizem iz V v V'. Vzemimo bazo $\{b_1, \ldots, b_n\}$ prostora V in dokažimo, da je potem $\{\varphi(b_1), \ldots, \varphi(b_n)\}$ baza prostora V'.

S tem bomo pokazali, da imata oba prostora enako dimenzijo n. Vzemimo poljubne skalarje λ_i, $i = 1, \ldots, n$. Potem je

$$\varphi(\lambda_1 b_1 + \cdots + \lambda_n b_n) = \lambda_1 \varphi(b_1) + \cdots + \lambda_n \varphi(b_n).$$

Ker je $\{b_1, \ldots, b_n\}$ ogrodje V in je φ surjektivna, od tod sledi, da je množica $\{\varphi(b_1), \ldots, \varphi(b_n)\}$ ogrodje V'. Pokažimo še, da je linearno neodvisna. Če za neke skalarje λ_i velja

$$\lambda_1 \varphi(b_1) + \cdots + \lambda_n \varphi(b_n) = 0,$$

je po zgornji formuli tudi

$$\varphi(\lambda_1 b_1 + \cdots + \lambda_n b_n) = 0.$$

Ker je tudi $\varphi(0) = 0$ (to sledi iz $\varphi(0) = \varphi(0 + 0) = 2\varphi(0)$) in je φ injektivna, lahko zaključimo, da je

$$\lambda_1 b_1 + \cdots + \lambda_n b_n = 0.$$

Toda množica $\{b_1, \ldots, b_n\}$ je linearno neodvisna, zato so vsi skalarji λ_i enaki 0. Prav to smo želeli dokazati.

Izrek moramo dokazati še v drugo smer. Predpostavimo, da imata oba prostora dimenzijo n. Vzemimo neko bazo $\{b_1, \ldots, b_n\}$ prostora V in bazo $\{b'_1, \ldots, b'_n\}$ prostora V'. Vsak vektor iz V lahko na en sam način zapišemo kot $\lambda_1 b_1 + \cdots + \lambda_n b_n$ za neke skalarje $\lambda_i \in F$. Preslikavo $\varphi : V \to V'$ definirajmo takole:

$$\varphi(\lambda_1 b_1 + \cdots + \lambda_n b_n) = \lambda_1 b'_1 + \cdots + \lambda_n b'_n$$

za poljubne $\lambda_i \in F$. Brez težav se prepričamo, da je φ izomorfizem vektorskih prostorov. □

Posledica 3.12. *Netrivialen končno-razsežen vektorski prostor nad poljem F je izomorfen prostoru F^n za neki $n \in \mathbb{N}$.*

Z izrekom 3.11 se je v taki ali drugačni obliki bralec že srečal pri linearni algebri. Kljub temu smo ga zapisali in dokazali, ker se lepo umešča v kontekst naše razprave. V algebri poskušamo objekte, ki jih obravnavamo, klasificirati »do izomorfnosti natančno«. S tem mislimo, da želimo opisati vse, le da med izomorfnimi ne ločimo. V tem smislu je študij vektorskih prostorov (nad danim poljem) silno enostaven. Izrek 3.11 nam da dokončen odgovor o njihovi zgradbi. Za vsako naravno število n obstaja vektorski prostor dimenzije n (na primer F^n) in poljubna prostora enake dimenzije sta si izomorfna. Za druge algebrske strukture, ki jih obravnavamo v tej knjigi, ne velja nič podobnega. V primeru 3.10 smo denimo našli dve neizomorfni grupi s štirimi elementi. Zgradba grup, kolobarjev, polj in algeber je bistveno bolj zapletena kot zgradba vektorskih prostorov. V prejšnjem razdelku smo sicer izpeljali podobno enostavno klasifikacijo cikličnih grup, a te grupe so zelo posebne.

Naloge

1. Poišči tak izomorfizem φ iz 2-razsežnega realnega vektorskega prostora $V = \{(x, y, z) \in \mathbb{R}^3 \mid x+y+z = 0\}$ v 2-razsežen realni vektorski prostor $\mathbb{C}$, da je $\varphi((1, -2, 1)) = 1 + i$ in $\varphi^{-1}(i) = (0, 1, -1)$.
2. Zapiši predpis za poljuben izomorfizem med prostoroma V in $\mathbb{C}$ iz prejšnje naloge.
3. Naj bosta V in V' 2-razsežna vektorska prostora nad poljem $\mathbb{Z}_2$. Koliko je izomorfizmov iz V v V'?
4. Naj bo p praštevilo. Pokaži, da sta si končno-razsežna prostora V in V' nad poljem $\mathbb{Z}_p$ izomorfna natanko tedaj, ko je $|V| = |V'|$.

   Namig. Koliko elementov ima n-razsežen vektorski prostor nad $\mathbb{Z}_p$?
5. Množici kvadratnih matrik nad kompleksnimi števili $M_m(\mathbb{C})$ in kvadratnih matrik nad kvaternioni $M_n(\mathbb{H})$ lahko obravnavamo kot vektorska prostora nad poljem $\mathbb{R}$. Ali sta si za kak par naravnih števil m in n ta prostora izomorfna?
6. Množico kvaternionov oblike $\alpha_0 + \alpha_1 i$ lahko identificiramo s kompleksnimi števili. Preveri, da aditivna grupa $(\mathbb{H}, +)$ postane vektorski prostor nad poljem $\mathbb{C}$, če produkt kvaternionov λh, kjer je $\lambda \in \mathbb{C} \subseteq \mathbb{H}$ in $h \in \mathbb{H}$, interpretiramo kot množenje vektorjev s skalarji. Koliko je dimenzija $\mathbb{H}$ nad $\mathbb{C}$? Ali je $\mathbb{H}$ tudi algebra nad $\mathbb{C}$?
7. Realni algebri kvaternionov $\mathbb{H}$ in matrik $M_2(\mathbb{R})$ imata obe dimenzijo 4, zato sta si kot vektorska prostora izomorfni. Ali za kak izomorfizem vektorskih prostorov $\varphi : \mathbb{H} \to M_2(\mathbb{R})$ lahko velja, da je $\varphi(h^2) = \varphi(h)^2$ za vse $h \in \mathbb{H}$?

3.3. Pojem homomorfizma

Homomorfizem lahko opišemo kot preslikavo, ki ohranja operacije, značilne za obravnavano algebrsko strukturo. Prejšnja razdelka smo posvetili bijektivnim homomorfizmom grup in vektorskih prostorov. Namen je bil delno motivacijski, želeli smo pokazati, da je ta pojem naraven. Sedaj bomo študij homomorfizmov postavili na trdnejše temelje. Opozorimo, da bomo drugače kot ponavadi tako grupe, kolobarje, vektorske prostore kot algebre označevali z istima simboloma A in A'. Večina lastnosti, ki jih bomo spoznali, je namreč skupna vsem algebrskim strukturam. Zato bo tako označevanje priročno.

Definicija 3.13. Preslikava $\varphi : A \to A'$ je

- **homomorfizem grup**, če sta A in A' grupi in velja
$$\varphi(xy) = \varphi(x)\varphi(y)$$
za vse $x, y \in A$;

- **homomorfizem kolobarjev**, če sta A in A' kolobarja in velja
$$\varphi(1) = 1,\ \ \varphi(x+y) = \varphi(x) + \varphi(y)\ \text{ in }\ \varphi(xy) = \varphi(x)\varphi(y)$$
za vse $x, y \in A$;
- **homomorfizem vektorskih prostorov** (ali **linearna preslikava**), če sta A in A' vektorska prostora nad istim poljem F in velja
$$\varphi(x+y) = \varphi(x) + \varphi(y)\ \text{ in }\ \varphi(\lambda x) = \lambda\varphi(x)$$
za vse $x, y \in A$ in $\lambda \in F$;
- **homomorfizem algeber**, če sta A in A' algebri nad istim poljem F in velja
$$\varphi(1) = 1,\ \ \varphi(x+y) = \varphi(x) + \varphi(y),\ \ \varphi(xy) = \varphi(x)\varphi(y)\ \text{ in}$$
$$\varphi(\lambda x) = \lambda\varphi(x)$$
za vse $x, y \in A$ in $\lambda \in F$.

Največkrat je iz konteksta razvidno, ali imamo v mislih homomorfizem grup, kolobarjev, prostorov ali algeber. Zato ga ponavadi imenujemo kar **homomorfizem**. Bijektivnemu homomorfizmu pravimo **izomorfizem**, surjektivnemu homomorfizmu **epimorfizem**, injektivnemu homomorfizmu pa **monomorfizem** ali **vložitev**. Homomorfizmu iz A v A pravimo **endomorfizem**, bijektivnemu endomorfizmu pa **avtomorfizem** (z drugimi besedami, avtomorfizem je endomorfizem, ki je izomorfizem).

K tem definicijam dodajmo nekaj komentarjev.

Opomba 3.14. Formulo, s katero je definiran homomorfizem grup, moramo ustrezno spremeniti, če je katera izmed grup A in A' aditivna (gl. razdelek 3.1). Če sta obe grupi aditivni, se formula glasi
$$\varphi(x+y) = \varphi(x) + \varphi(y)\ \text{ za vse } x, y \in A.$$
Preslikavi s to lastnostjo pravimo tudi **aditivna preslikava**. Homomorfizmi kolobarjev, vektorskih prostorov in algeber so torej med drugim aditivne preslikave.

Opomba 3.15. Za homomorfizme kolobarjev in algeber smo zahtevali, da slikajo enoto 1 kolobarja (algebre) A v enoto 1 kolobarja (algebre) A'. Tako na primer preslikava $\varphi : \mathbb{R} \to M_2(\mathbb{R})$, $\varphi(x) = \left[\begin{smallmatrix} x & 0 \\ 0 & 0 \end{smallmatrix}\right]$, ni homomorfizem, čeprav ohranja tako vsoto kot produkt.

Opomba 3.16. Homomorfizmov polj ne definiramo posebej. To so kar homomorfizmi kolobarjev. Polja se sicer od »navadnih« kolobarjev razlikujejo po komutativnosti in obrnljivosti neničelnih elementov, toda homomorfizmi kolobarjev očitno ohranjajo komutativnost, pa tudi inverze elementov slikajo v inverze njihovih slik (gl. trditev 3.23). Zato ni potrebe, da bi za homomorfizme polj zahtevali kaj več kot za homomorfizme kolobarjev.

Opomba 3.17. Izraz *vložitev* za injektiven homomorfizem $\varphi : A \to A'$ običajno uporabimo takrat, ko A identificiramo z zalogo vrednosti φ znotraj A'. Denimo, v razdelku 2.6 smo zapisali, da z identifikacijo elementov kolobarja K s konstantnimi polinomi lahko K obravnavamo kot podkolobar kolobarja polinomov $K[X]$. Zdaj to lahko povemo formalno korektno: kolobar K vložimo v kolobar $K[X]$ s predpisom

$$a \mapsto a + 0X + 0X^2 + \dots.$$

Še enostavnejši zgled: polje realnih števil s predpisom

$$x \mapsto x + i0$$

vložimo v polje kompleksnih števil. Podobno polji realnih in kompleksnih števil vložimo v obseg kvaternionov.

V naslednjih trditvah bomo zbrali nekaj dejstev, ki jih hitro izpeljemo iz definicij.

Trditev 3.18. *Kompozitum homomorfizmov je homomorfizem.*

Dokaz. Naj bosta $\varphi : A \to A'$ in $\psi : A' \to A''$ homomorfizma grup. Potem je

$$\begin{aligned}(\psi \circ \varphi)(xy) &= \psi(\varphi(xy)) = \psi(\varphi(x) \cdot \varphi(y)) \\ &= \psi(\varphi(x)) \cdot \psi(\varphi(y)) = (\psi \circ \varphi)(x) \cdot (\psi \circ \varphi)(y).\end{aligned}$$

Torej je $\psi \circ \varphi : A \to A''$ homomorfizem grup. Podobno preverimo, da je kompozitum homomorfizmov kolobarjev, vektorskih prostorov in algeber spet homomorfizem. □

Naslednjo trditev za izomorfizme grup že poznamo (trditev 3.3). Za izomorfizme kolobarjev, vektorskih prostorov in algeber je dokaz podoben, zato ga izpustimo.

Trditev 3.19. *Inverzna preslikava izomorfizma je izomorfizem.*

Če obstaja izomorfizem iz A v A', pravimo, da sta si A in A' **izomorfni**, in pišemo

$$A \cong A'.$$

Tu sta A in A' lahko grupi, kolobarja, vektorska prostora ali algebri. Iz trditve 3.19 sledi, da je relacija izomorfnosti $\cong$ simetrična, tj. iz $A \cong A'$ sledi $A' \cong A$. Ker je kompozitum bijektivnih preslikav bijektivna preslikava, trditev 3.18 pove, da je kompozitum izomorfizmov izomorfizem. Zato je relacija $\cong$ tranzitivna: iz $A \cong A'$ in $A' \cong A''$ sledi $A \cong A''$. Tudi $A \cong A$ velja tako za grupe, kolobarje, vektorske prostore, kot za algebre. V vseh primerih je namreč identiteta id_A avtomorfizem A. Torej je $\cong$ *ekvivalenčna relacija.*

Kot posledico zadnjih dveh trditev dobimo nove zanimive primere grup.

Posledica 3.20. *Množica vseh avtomorfizmov grupe (kolobarja, vektorskega prostora, algebre) A je grupa za komponiranje.*

Dokaz. Ker je kompozitum bijektivnih preslikav bijektivna preslikava, iz trditve 3.18 sledi, da je kompozitum avtomorfizmov avtomorfizem. Komponiranje je seveda asociativna operacija, identiteta id_A je avtomorfizem in je nevtralni element za komponiranje, po trditvi 3.19 pa je inverz avtomorfizma spet avtomorfizem. □

Trditev 3.21. *Če je $\varphi : A \to A'$ homomorfizem grup, je $\varphi(1) = 1$ in $\varphi(x^{-1}) = \varphi(x)^{-1}$ za vse $x \in A$.*

Dokaz. Iz

$$\varphi(1) = \varphi(1^2) = \varphi(1)^2$$

po pravilu krajšanja v grupi sledi $\varphi(1) = 1$. Zato je

$$\varphi(x)\varphi(x^{-1}) = \varphi(xx^{-1}) = \varphi(1) = 1,$$

iz česar sledi $\varphi(x^{-1}) = \varphi(x)^{-1}$. □

Za aditivne grupe trditev 3.21 dobi tole obliko.

Trditev 3.22. *Če je $\varphi : A \to A'$ homomorfizem aditivnih grup, je $\varphi(0) = 0$ in $\varphi(-x) = -\varphi(x)$ za vse $x \in A$.*

Trditev 3.22 seveda velja za homomorfizme kolobarjev, vektorskih prostorov in algeber. Za homomorfizme kolobarjev in algeber torej velja tako $\varphi(1) = 1$ kot $\varphi(0) = 0$. Prva formula je del definicije, druga pa iz definicije sledi.

Nekoliko splošnejša inačica obeh formul iz trditve 3.21 je formula

$$\varphi(x^n) = \varphi(x)^n$$

za vse $x \in A$ in vsa cela (ne le naravna) števila n. Dokaz prepuščamo bralcu. Če sta grupi aditivni, se ta formula glasi

$$\varphi(nx) = n\varphi(x).$$

Tudi homomorfizmi kolobarjev na obrnljivih elementih delujejo tako kot homomorfizmi grup.

Trditev 3.23. *Če je $\varphi : A \to A'$ homomorfizem kolobarjev in je element $x \in A$ obrnljiv, je obrnljiv tudi $\varphi(x)$ in velja $\varphi(x^{-1}) = \varphi(x)^{-1}$.*

Dokaz. Dokaz se od dokaza trditve 3.21 razlikuje v dveh podrobnostih. Prva je, da je enakost $\varphi(1) = 1$ zdaj predpostavka in je ni treba dokazovati. Druga pa, da moramo poleg $\varphi(x)\varphi(x^{-1}) = 1$ izpeljati tudi $\varphi(x^{-1})\varphi(x) = 1$ (kar je seveda zelo lahko). V kolobarjih namreč iz $ab = 1$ v splošnem ne sledi $ba = 1$. □

Pri homomorfizmih, ki niso izomorfizmi, ponavadi veliko pozornost posvečamo pojmoma slike in jedra. Vpeljimo ju.

Definicija 3.24. Zalogi vrednosti homomorfizma $\varphi : A \to A'$ pravimo **slika homomorfizma** in jo označujemo z $\operatorname{im}\varphi$. Torej je

$$\operatorname{im}\varphi = \{\varphi(x) \mid x \in A\}.$$

Trditev 3.25. *Slika homomorfizma grup (oz. kolobarjev, vektorskih prostorov, algeber) je podgrupa (oz. podkolobar, podprostor, podalgebra).*

Dokaz. Naj bo $\varphi : A \to A'$ homomorfizem grup. Iz $\varphi(x)\varphi(y) = \varphi(xy)$ sledi, da je množica $\operatorname{im}\varphi$ zaprta za množenje, iz $\varphi(x)^{-1} = \varphi(x^{-1})$ pa sledi, da vsebuje inverze vseh svojih elementov. Torej je podgrupa grupe A'. Na podoben način pokažemo, da je slika homomorfizma kolobarjev podkolobar, slika homomorfizma vektorskih prostorov podprostor in slika homomorfizma algeber podalgebra. □

Vsak homomorfizem $\varphi : A \to A'$ torej postane epimorfizem, če skrčimo kodomeno A' in ga obravnavamo kot homomorfizem iz A v $\operatorname{im}\varphi$. Vložitev pri tem postane izomorfizem.

Definicija 3.26. **Jedro homomorfizma grup** $\varphi : A \to A'$ je množica

$$\ker\varphi := \{x \in A \mid \varphi(x) = 1\}.$$

Če je A' aditivna grupa, se definicija seveda glasi takole:

$$\ker\varphi := \{x \in A \mid \varphi(x) = 0\}. \tag{3.4}$$

Kolobarji, vektorski prostori in algebre so med drugim aditivne grupe. Zato s (3.4) definiramo tudi **jedro homomorfizma kolobarjev, vektorskih prostorov** in **algeber**.

Trditev 3.21 pove, da jedro homomorfizma grup vsebuje enoto 1. Če je 1 edini element v jedru, pravimo, da je **jedro trivialno**. Za homomorfizme aditivnih grup, kolobarjev, prostorov in algeber seveda rečemo, da je njihovo jedro trivialno, če vsebuje le ničelni element.

Trditev 3.27. *Homomorfizem $\varphi : A \to A'$ je injektiven natanko tedaj, ko je njegovo jedro trivialno.*

Dokaz. Privzeti smemo, da sta A in A' grupi za množenje, saj v drugih primerih samo spremenimo oznake. Če je homomorfizem φ injektiven, v njegovem jedru razen 1 ne more biti noben drug element x, saj bi sicer veljalo $\varphi(x) = \varphi(1)$. Obratno, če je jedro trivialno in za neka elementa $x, y \in A$ velja $\varphi(x) = \varphi(y)$, potem je

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

in zato $xy^{-1} \in \ker\varphi = \{1\}$, tj. $x = y$. □

Morda ne bo odveč, če trditev ponovimo v manj zgoščeni obliki. Če je $\varphi : A \to A'$ homomorfizem grup in operacijo v A označujemo kot množenje, potem velja

$$\varphi \text{ je injektiven} \iff \ker \varphi = \{1\}.$$

Če pa operacijo v A označujemo kot seštevanje, torej če je A aditivna grupa, velja

$$\varphi \text{ je injektiven} \iff \ker \varphi = \{0\}.$$

Slednje torej velja tudi za homomorfizme kolobarjev, vektorskih prostorov in algeber, saj so vsi (med drugim) aditivne preslikave, torej homomorfizmi aditivnih grup.

Bralcu svetujemo, da zapiše dokaz trditve 3.27 tudi za primer, ko sta grupi A in A' aditivni. Brez razumevanja tovrstnih osnovnih dejstev in njihovih dokazov bo namreč težko slediti nadaljevanju.

Slika homomorfizma je nekakšna mera za surjektivnost. Večja kot je slika, bližje smo surjektivnosti. Jedro homomorfizma pa je mera za injektivnost. Manjše kot je jedro, bližje smo injektivnosti. »Najpopolnejši« homomorfizmi so izomorfizmi, ki imajo trivialno jedro in največjo možno sliko. Njihovo nasprotje, torej homomorfizmi z največjim možnim jedrom in najmanjšo možno sliko, so **trivialni homomorfizmi**. Trivialni homomorfizem grup je preslikava, ki vse elemente prve grupe preslika v enoto 1 druge grupe. Pri drugih strukturah enoto zamenjamo z ničelnim elementom. Iz formalnih razlogov lahko pri kolobarjih in algebrah trivialni homomorfizem slika le v ničelni kolobar $\{0\}$. Homomorfizmi namreč ohranjajo enoto (slikajo 1 v 1), kar vodi do pogoja $1 = 0$, ki je izpolnjen le v ničelnem kolobarju.

Slika homomorfizma $\varphi : A \to A'$ je podmnožica A', jedro pa je podmnožica A. O strukturi slike govori trditev 3.25. Kaj lahko rečemo o jedru? To vprašanje je zanimivejše, kot bi morda pričakovali. S preprostim računom sicer takoj preverimo, da je jedro homomorfizma grup podgrupa, jedro homomorfizma vektorskih prostorov podprostor in da ima jedro homomorfizma kolobarjev (oz. algeber) vse lastnosti podkolobarja (oz. podalgebre), razen da ne vsebuje (nujno) enote 1. Toda povedati se da še več. Vendar počakajmo do razdelkov 4.2 in 4.3.

Naloge

1. Pokaži, da iz $A_1 \cong B_1$ in $A_2 \cong B_2$ sledi $A_1 \times A_2 \cong B_1 \times B_2$. Tu so A_1, A_2, B_1 in B_2 lahko grupe, kolobarji ali algebre.
2. Pokaži, da je $A_1 \times A_2 \cong A_2 \times A_1$. Tudi tu sta A_1 in A_2 lahko grupi, kolobarja ali algebri.

3. Naj bo $\varphi : A \to A'$ homomorfizem grup in naj bo $\varphi(a) = b$ za neka $a \in A$, $b \in A'$. Pokaži, da je množica vseh rešitev enačbe $\varphi(x) = b$ enaka množici

$$a \ker \varphi := \{au \mid u \in \ker \varphi\}.$$

Komentar. Če je φ homomorfizem aditivnih grup, torej če je aditivna preslikava, to množico seveda zapišemo kot $a + \ker \varphi := \{a + u \mid u \in \ker \varphi\}$. To vključuje homomorfizme kolobarjev, vektorskih prostorov in algeber, saj so vsi med drugim aditivne preslikave.

4. Naj bo $\varphi : A \to A'$ homomorfizem grup in naj ima element $a \in A$ končen red. Pokaži, da red $\varphi(a)$ deli red a. Če je φ vložitev, sta oba reda enaka.

   Komentar. V splošnem reda nista enaka; glej na primer nalogo 5 v naslednjem razdelku.

5. Homomorfizem polgrup definiramo enako kot homomorfizem grup, za homomorfizme monoidov pa dodatno zahtevamo, da slikajo nevtralni element v nevtralni element. Za operacijo množenja po komponentah je množica $\mathbb{Z} \times \mathbb{Z}$ monoid. Poišči preslikavo $\varphi : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z} \times \mathbb{Z}$, ki je endomorfizem polgrup, ni pa endomorfizem monoidov.

6. Naj bosta A in A' vektorska prostora nad poljem $\mathbb{Q}$. Pokaži, da je vsak homomorfizem aditivnih grup $\varphi : A \to A'$ tudi homomorfizem vektorskih prostorov. Z drugimi besedami, pokaži, da iz $\varphi(x + y) = \varphi(x) + \varphi(y)$ za vse $x, y \in A$ sledi $\varphi(qx) = q\varphi(x)$ za vse $q \in \mathbb{Q}$ in $x \in A$.

   Komentar. To je posebnost polja racionalnih števil. V tej nalogi ne moremo $\mathbb{Q}$ zamenjati z $\mathbb{R}$ ali $\mathbb{C}$.

7. Pokaži, da jedro netrivialnega homomorfizma kolobarjev ne vsebuje obrnljivih elementov.

8. Ugotovi, katere tri izmed naslednjih trditev so pravilne za vsak netrivialen homomorfizem kolobarjev $\varphi : A \to A'$:
   (a) Če je A komutativen, je tudi $\operatorname{im} \varphi$ komutativen.
   (b) Če A nima deliteljev niča, tudi $\operatorname{im} \varphi$ nima deliteljev niča.
   (c) Če ima A delitelje niča, ima tudi $\operatorname{im} \varphi$ delitelje niča.
   (d) Če je A obseg, je tudi $\operatorname{im} \varphi$ obseg.
   (e) Če je A polje, je tudi $\operatorname{im} \varphi$ polje.

   Nepravilni trditvi ovrzi s primeroma.

   Komentar. Morda je iskanje primerov kar precejšen izziv, saj se s konkretnimi primeri homomorfizmov kolobarjev še nismo srečali. Po naslednjem razdelku bo naloga bistveno lažja. Kljub temu poskusi že zdaj! Nič hudega, če ne uspeš. Iz neuspelih poskusov se včasih naučimo še več.

3.4. Primeri homomorfizmov

Namen tega razdelka je predstaviti raznovrstne primere homomorfizmov. Nekaj primerov smo srečali že v prejšnjih razdelkih. Spomnimo se na primer eksponentne funkcije, ki jo lahko interpretiramo kot izomorfizem grup (gl. primer 3.5). Tudi logaritemska funkcija kot njej inverzna funkcija je zato izomorfizem grup. Nasploh pomembne preslikave, ki jih srečujemo na različnih področjih matematike, pogosto ohranjajo kako algebrsko lastnost in so zato homomorfizmi kake algebrske strukture. Nekaj takih preslikav bomo srečali tudi v tem razdelku.

3.4.1. Primeri homomorfizmov grup. Pričnemo s tremi primeri v Abelovih grupah.

Primer 3.28. Preslikava, ki vsakemu elementu x Abelove grupe G priredi njegov inverz x^{-1}, je avtomorfizem grupe G. Splošneje, za vsako celo število m je preslikava

$$x \mapsto x^m$$

endomorfizem Abelove grupe G. (V aditivni grupi bi seveda pisali $x \mapsto mx$).

Primer 3.29. Preslikava

$$z \mapsto |z|$$

je epimorfizem iz grupe neničelnih kompleksnih števil $\mathbb{C}^*$ v grupo pozitivnih realnih števil $\mathbb{R}^+$. Operacija v obeh grupah je seveda množenje. Jedro tega epimorfizma je enotska krožnica

$$\mathbb{T} := \{z \in \mathbb{C} \,|\, |z| = 1\},$$

imenovana tudi **krožna grupa**.

Primer 3.30. Preslikava

$$x \mapsto \cos x + i \sin x$$

je epimorfizem iz grupe $(\mathbb{R}, +)$ v krožno grupo $(\mathbb{T}, \cdot)$ (zakaj?). Njeno jedro je množica $\{2k\pi \,|\, k \in \mathbb{Z}\}$.

Primer 3.31. Formula $\operatorname{sgn}(\pi\sigma) = \operatorname{sgn}(\pi)\operatorname{sgn}(\sigma)$, ki velja za vse elemente π in σ simetrične grupe S_n, pove, da je preslikava

$$\sigma \mapsto \operatorname{sgn}(\sigma)$$

epimorfizem iz grupe S_n v grupo $(\{1, -1\}, \cdot)$. Njeno jedro je alternirajoča grupa A_n.

Primer 3.32. Podobno lastnost kot predznak permutacije ima determinanta matrike: determinanta produkta matrik je enaka produktu determinant. Torej je preslikava

$$A \mapsto \det(A)$$

epimorfizem iz splošne linearne grupe $\mathrm{GL}_n(F)$ v grupo $(F^*, \cdot)$, tj. grupo neničelnih skalarjev za množenje. Njeno jedro je posebna linearna grupa $\mathrm{SL}_n(F)$.

PRIMER 3.33. Naj bosta G_1 in G_2 poljubni grupi. Preslikava

$$\pi : G_1 \times G_2 \to G_1,\ \pi\big((x_1, x_2)\big) = x_1,$$

je epimorfizem z jedrom $\{1\} \times G_2$, preslikava

$$\iota : G_1 \to G_1 \times G_2,\ \iota(x_1) = (x_1, 1)$$

pa vložitev grupe G_1 v direktni produkt $G_1 \times G_2$. Očitno je $\pi \circ \iota = \mathrm{id}_{G_1}$, medtem ko je $\iota \circ \pi\big((x_1, x_2)\big) = (x_1, 1)$.

PRIMER 3.34. Naj bo G poljubna grupa. Za vsak $a \in G$ definirajmo preslikavo $\varphi_a : G \to G$ s predpisom

$$\varphi_a(x) = axa^{-1}.$$

Hitro preverimo, da je φ_a bijektivna. Ker je

$$\varphi_a(xy) = axya^{-1} = (axa^{-1})(aya^{-1}) = \varphi_a(x)\varphi_a(y),$$

je φ_a avtomorfizem grupe G. Take avtomorfizme imenujemo **notranji avtomorfizmi grupe** G. Zanimivi so v nekomutativnih grupah. Edini notranji avtomorfizem Abelove grupe je namreč identiteta.

Elementa x in $\varphi_a(x)$ sta si seveda konjugirana. Če je H podgrupa grupe G, jo avtomorfizem φ_a preslika v podgrupo aHa^{-1}. Poljubni konjugirani podgrupi sta si torej izomorfni.

Omenimo še, da je množica vseh notranjih avtomorfizmov grupe G podgrupa grupe vseh avtomorfizmov. To sledi iz formul

$$\varphi_a\varphi_b = \varphi_{ab} \ \text{ in } \ \varphi_a^{-1} = \varphi_{a^{-1}}.$$

(Pod)grupo vseh notranjih avtomorfizmov označujemo z

$$\mathrm{Inn}(G),$$

grupo vseh avtomorfizmov pa z

$$\mathrm{Aut}(G).$$

Formula $\varphi_a\varphi_b = \varphi_{ab}$ pove, da je preslikava $a \mapsto \varphi_a$ epimorfizem iz grupe G v grupo $\mathrm{Inn}(G)$.

S homomorfizmi vektorskih prostorov, torej z linearnimi preslikavami, se ne bomo podrobneje ukvarjali, saj so le-ti tema linearne algebre. Preidimo na kolobarje in algebre.

3.4.2. Primeri homomorfizmov kolobarjev in algeber. Pričnimo tam, kjer smo pri grupah končali.

PRIMER 3.35. **Notranji avtomorfizem kolobarja** K definiramo enako kot notranji avtomorfizem grupe. Element $a \in K$ zdaj sicer ni povsem poljuben, privzeti moramo, da je obrnljiv. Kot smo videli, preslikava $\varphi_a(x) = axa^{-1}$ ohranja produkt, očitno pa je tudi aditivna in ohranja enoto.

PRIMER 3.36. Ali je preslikava $f : \mathbb{Z}_2 \to \mathbb{Z}$, definirana s predpisom $f(0) = 0$ in $f(1) = 1$, homomorfizem kolobarjev? Vse zahteve iz definicije homomorfizma so izpolnjene, z izjemo ene: $f(1+1) \neq f(1) + f(1)$. Torej f ni niti homomorfizem aditivnih grup. Zato pa je homomorfizem kolobarjev preslikava $\varphi : \mathbb{Z} \to \mathbb{Z}_2$,

$$\varphi(a) = \begin{cases} 1 & ; \ a \text{ je lih} \\ 0 & ; \ a \text{ je sod} \end{cases} .$$

Splošneje, za vsak $n \in \mathbb{N}$ je s predpisom

$$\varphi(a) = [a]$$

definiran epimorfizem iz $\mathbb{Z}$ v $\mathbb{Z}_n$; tu smo uporabili oznako $[a]$ iz definicije kolobarja ostankov po modulu n (gl. razdelek 2.2). Njegovo jedro je množica $n\mathbb{Z}$.

PRIMER 3.37. V prejšnjem razdelku smo omenili, da lahko vsak kolobar K vložimo v kolobar polinomov $K[X]$, tako da vsakemu elementu priredimo ustrezni konstantni polinom. Neke vrste obrat tega primera je epimorfizem

$$\varphi : K[X] \to K, \ \ \varphi(a_0 + a_1X + \cdots + a_nX^n) = a_0.$$

Njegovo jedro je množica vseh polinomov s konstantnim členom 0. Če je K komutativen, lahko epimorfizem φ opišemo tudi kot preslikavo, ki vsakemu polinomu $f(X)$ priredi element $f(0)$ iz K, torej vrednost $f(X)$ v 0. Element 0 lahko tu zamenjamo s katerimkoli elementom x iz K in dobimo epimorfizem

$$f(X) \mapsto f(x)$$

iz kolobarja $K[X]$ v kolobar K. Njegovo jedro je množica vseh polinomov, katerih ničla je x.

PRIMER 3.38. Podoben primer si lahko zamislimo v kolobarjih funkcij. Denimo, za poljubno število $x \in [0,1]$ je preslikava

$$f \mapsto f(x),$$

ki vsaki zvezni funkciji $f \in C[0,1]$ priredi funkcijsko vrednost v točki x, epimorfizem iz kolobarja $C[0,1]$ v kolobar $\mathbb{R}$. Pravzaprav je homomorfizem algeber, ne le kolobarjev.

PRIMER 3.39. Naj bo V vektorski prostor nad poljem F. Z

$$\mathrm{End}_F(V)$$

označimo množico vseh endomorfizmov prostora V, torej vseh linearnih preslikav iz V v V. V to množico vpeljimo seštevanje, množenje in množenje s skalarjem takole: vsota endomorfizmov $f, g \in \mathrm{End}_F(V)$ naj bo preslikava $f + g : V \to V$, definirana s predpisom

$$(f + g)(v) := f(v) + g(v),$$

produkt fg naj bo kompozitum teh dveh endomorfizmov, torej

$$(fg)(v) := f(g(v)),$$

produkt λf, kjer je $\lambda \in F$ in $f \in \mathrm{End}_F(V)$, pa definiramo z

$$(\lambda f)(v) := \lambda f(v).$$

Tudi $f + g, fg, \lambda f$ so spet endomorfizmi in še več, s temi operacijami postane množica $\mathrm{End}_F(V)$ algebra nad F. Dokaz je rutinski in ga izpustimo. Bralec morda to dejstvo sicer pozna iz linearne algebre, kot tudi dejstvo, da je ta algebra v primeru, ko je $\dim_F V = n$, izomorfna matrični algebri $M_n(F)$, torej

$$\mathrm{End}_F(V) \cong M_n(F).$$

Skicirajmo dokaz. Omejimo se na primer, ko je $n = 2$. Splošni primer ni težji, le označevanje je bolj zapleteno. Vzemimo neko bazo $\{b_1, b_2\}$ prostora V. Za vsak $f \in \mathrm{End}_F(V)$ obstajajo taki skalarji $f_{ij} \in F$, da je

$$f(b_1) = f_{11}b_1 + f_{21}b_2 \text{ in } f(b_2) = f_{12}b_1 + f_{22}b_2.$$

Endomorfizmu f sedaj priredimo matriko

$$A_f := \begin{bmatrix} f_{11} & f_{12} \\ f_{21} & f_{22} \end{bmatrix} \in M_2(F).$$

Z računom preverimo, da velja

$$A_{\mathrm{id}_V} = I, \ A_{f+g} = A_f + A_g, \ A_{fg} = A_f A_g \text{ in } A_{\lambda f} = \lambda A_f$$

za vse $f, g \in \mathrm{End}_F(V)$ in $\lambda \in F$. To pomeni, da je preslikava $f \mapsto A_f$ homomorfizem iz algebre $\mathrm{End}_F(V)$ v algebro $M_2(F)$. Hitro se prepričamo, da je bijektivna in zato izomorfizem.

Zaključimo z daljšim primerom, v katerem se bomo spopadli z značilnim algebraičnim problemom. Podani bodo objekti, v tem primeru kolobarji, in v njih bomo poskušali prepoznati »znane« objekte – v tem primeru kolobarje, s katerimi smo se že srečali.

PRIMER 3.40. Oglejmo si štiri primere podkolobarjev kolobarja realnih oziroma, v zadnjem primeru, kompleksnih matrik velikosti 2×2. To so

$$K_1 := \left\{ \begin{bmatrix} x & 0 \\ 0 & x \end{bmatrix} \mid x \in \mathbb{R} \right\},$$

$$K_2 := \left\{ \begin{bmatrix} x & 0 \\ 0 & y \end{bmatrix} \mid x, y \in \mathbb{R} \right\},$$

$$K_3 := \left\{ \begin{bmatrix} x & y \\ -y & x \end{bmatrix} \mid x, y \in \mathbb{R} \right\},$$

$$K_4 := \left\{ \begin{bmatrix} z & w \\ -\overline{w} & \overline{z} \end{bmatrix} \mid z, w \in \mathbb{C} \right\}.$$

Poskusimo »razkrinkati«, za katere kolobarje gre. Poiščimo torej znane kolobarje, ki so jim ti kolobarji izomorfni.

1. Iz enakosti

$$\begin{bmatrix} x & 0 \\ 0 & x \end{bmatrix} \pm \begin{bmatrix} x' & 0 \\ 0 & x' \end{bmatrix} = \begin{bmatrix} x \pm x' & 0 \\ 0 & x \pm x' \end{bmatrix} \quad \text{in} \quad \begin{bmatrix} x & 0 \\ 0 & x \end{bmatrix} \begin{bmatrix} x' & 0 \\ 0 & x' \end{bmatrix} = \begin{bmatrix} xx' & 0 \\ 0 & xx' \end{bmatrix}$$

vidimo, da je K_1 podkolobar kolobarja $M_2(\mathbb{R})$. Razberemo pa še več: operaciji v K_1 sta v bistvu enaki operacijama v kolobarju $\mathbb{R}$. Res je

$$K_1 \cong \mathbb{R};$$

izomorfizem je preslikava

$$\left[\begin{smallmatrix} x & 0 \\ 0 & x \end{smallmatrix} \right] \mapsto x.$$

2. Matrike iz K_2 seštejemo in množimo tako, da seštejemo in množimo diagonalne člene. Računanje je v bistvu enako kot v direktnem produktu dveh kopij kolobarja $\mathbb{R}$. Torej je

$$K_2 \cong \mathbb{R} \times \mathbb{R}.$$

Izomorfizem je podan z

$$\left[\begin{smallmatrix} x & 0 \\ 0 & y \end{smallmatrix} \right] \mapsto (x, y).$$

3. Seštevanje v kolobarju K_3 je podobno enostavno kot v K_1 in K_2. Zanimivejše je množenje:

$$\begin{bmatrix} x & y \\ -y & x \end{bmatrix} \begin{bmatrix} x' & y' \\ -y' & x' \end{bmatrix} = \begin{bmatrix} xx' - yy' & xy' + x'y \\ -(xy' + x'y) & xx' - yy' \end{bmatrix}.$$

Produkt res leži v K_3, ki torej je podkolobar $M_2(\mathbb{R})$. Na kaj spominja rezultat? Množenje kompleksnih števil je definirano s podobno formulo

$$(x + yi)(x' + y'i) = (xx' - yy') + (xy' + x'y)i.$$

Zato je

$$K_3 \cong \mathbb{C}.$$

Izomorfizem je preslikava

$$\left[\begin{smallmatrix} x & y \\ -y & x \end{smallmatrix} \right] \mapsto x + yi.$$

4. Kot v prejšnjih primerih se z računom prepričamo, da je K_4 podkolobar $M_2(\mathbb{C})$. To je lahka računska naloga, ki pa nam tokrat morda ne pomaga takoj pri »razkritju« kolobarja K_4. Zato opozorimo na tole lastnost elementov iz K_4: vsaka neničelna matrika

$$\begin{bmatrix} z & w \\ -\overline{w} & \overline{z} \end{bmatrix} \in K_4$$

ima neničelno determinanto $z\overline{z}+w\overline{w}$ in je zato obrnljiva v $M_2(\mathbb{C})$. Njen inverz pravzaprav leži v K_4:

$$\begin{bmatrix} z & w \\ -\overline{w} & \overline{z} \end{bmatrix}^{-1} = \frac{1}{z\overline{z}+w\overline{w}} \begin{bmatrix} \overline{z} & -w \\ \overline{w} & z \end{bmatrix} \in K_4.$$

Torej je K_4 obseg! Zato ne bi smelo biti presenečenje, da je K_4 izomorfen obsegu kvaternionov, torej

$$K_4 \cong \mathbb{H}.$$

Izomorfizem je podan z

$$\begin{bmatrix} z & w \\ -\overline{w} & \overline{z} \end{bmatrix} \mapsto x + yi + uj + vk,$$

kjer je $z = x + yi$ in $w = u + vi$. To se pač preveri. Toda bralec naj se vpraša, kako bi do tega ali kakega drugega izomorfizma prišel sam.

Vsi štirje kolobarji iz primera 3.40 so tudi realne algebre in vse zgornje preslikave so izomorfizmi algeber, ne le kolobarjev. Tako je algebra matrik K_4 izomorfna algebri kvaternionov $\mathbb{H}$. V razdelku 2.3 smo zapisali, da so $\mathbb{R}$, $\mathbb{C}$ in $\mathbb{H}$ edine končno-razsežne realne algebre, ki so obsegi. Izrazili smo se malce površno. Natančno bi rekli, da je vsaka končno-razsežna realna algebra, ki je obseg, izomorfna eni izmed algeber $\mathbb{R}$, $\mathbb{C}$ ali $\mathbb{H}$. Vendar take površnosti v algebri niso neobičajne. Izomorfne objekte med seboj enačimo in tako včasih »pozabimo« na njihovo različnost. Začetnika to lahko zmede. Zgodi se, da v enem stavku med dvema kolobarjema ne ločujemo, že v naslednjem pa ju imamo za različna. Čez čas nas to neha motiti, še kasneje pa tega niti ne opazimo več.

Naloge

1. Denimo, da se homomorfizma grup (kolobarjev, vektorskih prostorov, algeber) $\varphi, \psi : A \to A'$ ujemata na neki množici generatorjev X grupe (kolobarja, vektorskega prostora, algebre) A. Pokaži, da je $\varphi = \psi$.

   Komentar. Homomorfizmi so torej povsem določeni z vrednostmi na *katerikoli* množici generatorjev. Več naslednjih nalog obravnava vprašanje, ali obstaja homomorfizem, ki ima na *neki* množici generatorjev vnaprej predpisane vrednosti.

2. Naj bo G poljubna grupa. Pokaži, da za vsak $a \in G$ obstaja tak homomorfizem grup $\varphi : \mathbb{Z} \to G$, da je $\varphi(1) = a$.
3. Poišči vse endomorfizme aditivne grupe $\mathbb{Z}$. Kateri izmed njih so avtomorfizmi? Pokaži, da je grupa $\mathrm{Aut}(\mathbb{Z})$ izomorfna grupi $\mathbb{Z}_2$.
4. Poišči vse endomorfizme kolobarja $\mathbb{Z}$.
5. Naj bo G poljubna grupa in naj $a \in G$. Pokaži, da obstaja tak homomorfizem $\varphi : \mathbb{Z}_n \to G$, da je $\varphi(1) = a$ natanko tedaj, ko je $a^n = 1$.

   Komentar. Število n ni nujno red elementa a, lahko je njegov večkratnik. V tem primeru je red elementa $\varphi(1)$ manjši od reda elementa 1.
6. Opiši avtomorfizme aditivne grupe $\mathbb{Z}_n$ in pokaži, da je grupa $\mathrm{Aut}(\mathbb{Z}_n)$ izomorfna grupi $\mathbb{Z}_n^*$, tj. grupi obrnljivih elementov kolobarja $\mathbb{Z}_n$.

   Namig. Vsak endomorfizem $\mathbb{Z}_n$ je povsem določen z vrednostjo na generatorju 1. Avtomorfizem lahko ta generator preslika samo v ta ali kateri drugi generator.
7. Naj bo G grupa s trivialnim centrom. Pokaži, da ima potem tudi grupa $\mathrm{Aut}(G)$ trivialen center.
8. Poišči tri različne vložitve netrivialne grupe G v grupo $G \times G$.

   Namig. Dva načina razbereš iz primera 3.33.
9. Naj bo K poljuben kolobar. Pokaži, da za vsak $a \in K$ obstaja tak homomorfizem kolobarjev $\varphi : \mathbb{Z}[X] \to K$, da je $\varphi(X) = a$.
10. Ali obstaja tak endomorfizem φ kolobarja $\mathbb{Z}[X]$, da je $\varphi(X^2) = X^3$?
11. Poišči vse avtomorfizme kolobarja $\mathbb{Z}[X]$.
12. Naj bo A poljubna algebra nad poljem F. Pokaži, da za vsak $a \in A$ obstaja tak homomorfizem algeber $\varphi : F[X] \to A$, da je $\varphi(X) = a$.
13. Poišči vse avtomorfizme algebre $F[X]$.
14. Naj bo A poljubna realna algebra in naj bosta $a, b \in A$. Pokaži, da obstaja tak homomorfizem algeber $\varphi : \mathbb{H} \to A$, da je $\varphi(i) = a$ in $\varphi(j) = b$ natanko tedaj, ko je $a^2 = b^2 = -1$ in $ab = -ba$.
15. Pojasni, zakaj endomorfizem algebre $M_2(\mathbb{R})$ ne more preslikati matrike E_{11} v matriko E_{12}. Poišči kak tak endomorfizem φ, da je $\varphi(E_{11}) = E_{22}$.
16. Naj bosta V in V' poljubna vektorska prostora nad poljem F. Pokaži, da za poljubno bazo $\{b_i \mid i \in I\}$ prostora V in poljubno množico vektorjev $\{a_i \mid i \in I\}$ iz V' obstaja tak homomorfizem vektorskih prostorov $\varphi : V \to V'$, da je $\varphi(b_i) = a_i$ za vse $i \in I$.

    Komentar. Ponovno vidimo, da so vektorski prostori drugačni in v nekem smislu enostavnejši od ostalih algebrskih struktur. V tej nalogi je bil vektorski prostor V povsem poljuben, v nalogah 2, 9 in 12 pa

smo se morali omejiti na posebno grupo, kolobar oziroma algebro. Ob tem, da je bil tudi zaključek bistveno skromnejši, saj je zadeval le en element a. Naloge bi sicer lahko modificirali, tako da bi vključevale več elementov. Vendar bi morali vpeljati več novih pojmov, zato se temu raje izognimo.

Še komentar o reševanju naloge. Nekateri bralci se morda počutijo negotovo pri obravnavi neskončnih baz. Lahko se tudi omejijo na primer, ko je prostor V končno-razsežen in je torej množica I končna. Neskončno-razsežni primer je sicer zahtevnejši le pojmovno, ne vsebinsko. V poljubnem vektorskem prostoru se da namreč vsak vektor zapisati kot *končna* linearna kombinacija nekih baznih vektorjev.

17. Preveri, da je konjugiranje $z \mapsto \overline{z}$ avtomorfizem kolobarja $\mathbb{C}$. Še več, je avtomorfizem realne algebre $\mathbb{C}$. Pokaži, da je poleg identitete $\mathrm{id}_{\mathbb{C}}$ tudi edini avtomorfizem realne algebre $\mathbb{C}$.

18. Če identificiramo kvaternione oblike $\lambda_0 + \lambda_1 i$ s kompleksnimi števili, lahko realno algebro $\mathbb{C}$ obravnavamo kot podalgebro realne algebre $\mathbb{H}$. Poišči kako razširitev avtomorfizma algebre kompleksnih števil $z \mapsto \overline{z}$ iz prejšnje naloge na avtomorfizem cele algebre $\mathbb{H}$. Ali je ta avtomorfizem notranji?

Komentar. Konjugiranje kvaternionov $h \mapsto \overline{h}$ ni pravi odgovor. Ta preslikava sicer je linearna in bijektivna, vendar obrne vrstni red faktorjev, tj. zadošča $\overline{hh'} = \overline{h'} \cdot \overline{h}$. Takim preslikavam pravimo *antiavtomorfizmi*. Najbolj znan primer antiavtomorfizma je transponiranje $A \mapsto A^t$ na algebri matrik $M_n(F)$.

19. Poišči podkolobar kolobarja $M_2(\mathbb{Z})$, ki je izomorfen kolobarju Gaussovih celih števil $\mathbb{Z}[i]$.

Namig. Primer 3.40.

20. Poišči kako tako neničelno preslikavo $\delta : \mathbb{R}[X] \to \mathbb{R}[X]$, da bo s predpisom

$$f(X) \mapsto \begin{bmatrix} f(X) & \delta(f(X)) \\ 0 & f(X) \end{bmatrix}$$

definirana vložitev algebre $\mathbb{R}[X]$ v algebro $M_2(\mathbb{R}[X])$.

21. Pokaži, da je algebra $\mathbb{H}_{\mathbb{C}}$ iz naloge 2.3/11 izomorfna algebri $M_2(\mathbb{C})$.

22. Označimo z A množico vseh matrik oblike $\left[\begin{smallmatrix} a & b & d \\ 0 & a & c \\ 0 & 0 & a \end{smallmatrix}\right]$ in z A' množico vseh matrik oblike $\left[\begin{smallmatrix} a & 0 & 0 \\ b & a & 0 \\ d & c & a \end{smallmatrix}\right]$, kjer so $a, b, c, d \in \mathbb{R}$. Preveri, da sta A in A' 4-razsežni realni algebri za običajne operacije z matrikami. Pokaži, da sta si A in A' izomorfni, nista pa izomorfni algebri $M_2(\mathbb{R})$.

3.5. Cayleyev izrek in drugi izreki o vložitvah

Sporočilo prvega izreka, ki ga bomo dokazali, je na prvi pogled presenetljivo: »edine« grupe so simetrične grupe in njihove podgrupe. Podobna izreka bomo zatem dokazali za kolobarje in algebre. Resnici na ljubo ti izreki nimajo tako velike uporabne vrednosti, kot bi morda najprej pričakovali. Imajo pa filozofsko poanto, ki ima vpliv na naše razumevanje in obravnavo grup, kolobarjev in algeber.

3.5.1. Vložitev grupe v simetrično grupo. Spomnimo se, da $\mathrm{Sim}(X)$ označuje simetrično grupo množice X, torej grupo vseh permutacij množice X (primer 1.36). Naslednji izrek se imenuje po angleškem matematiku *Arthurju Cayleyu* iz devetnajstega stoletja.

Izrek 3.41. ***(Cayleyev izrek)*** *Vsako grupo G lahko vložimo v neko simetrično grupo.*

Dokaz. Za vsak $a \in G$ definirajmo preslikavo

$$\ell_a : G \to G, \;\; \ell_a(x) = ax.$$

Iz $\ell_a(x) = \ell_a(y)$ sledi $ax = ay$ in zato $x = y$. Torej je preslikava ℓ_a injektivna. Ker je $\ell_a(a^{-1}x) = x$ za vsak $x \in G$, je tudi surjektivna. Zato je $\ell_a \in \mathrm{Sim}(G)$; v tem dokazu bomo za množico X izbrali kar G.

Oglejmo si sedaj preslikavo

$$\varphi : G \to \mathrm{Sim}(G), \;\; \varphi(a) = \ell_a.$$

Iz

$$\ell_{ab}(x) = (ab)x = a(bx) = \ell_a(\ell_b(x)) = (\ell_a \circ \ell_b)(x)$$

sledi, da je $\ell_{ab} = \ell_a \circ \ell_b$. To lahko zapišemo kot $\varphi(ab) = \varphi(a) \circ \varphi(b)$, kar pomeni, da je φ homomorfizem grup. Če $a \in \ker \varphi$, je $\ell_a = \mathrm{id}_G$ in zato $a = \ell_a(1) = \mathrm{id}_G(1) = 1$. Torej ima φ trivialno jedro in je vložitev. □

Izrek pove, da bi lahko brez škode za splošnost grupo definirali kot bolj konkreten pojem, tj. kot množico permutacij, ki je zaprta za množenje in vsebuje inverze vseh svojih elementov. Zgodovinsko je bila slednja definicija pravzaprav prva. Prehod je bil torej naraven, od konkretnega k abstraktnemu in ne obratno.

Kot je razvidno iz dokaza, bi lahko izrek formulirali bolj natančno: grupo G lahko vložimo v simetrično grupo $\mathrm{Sim}(G)$. Toda namerno smo želeli poudariti predvsem to, da se G da vložiti v simetrično grupo neke množice. Zanesljivo lahko za to množico izberemo kar G, toda morda so možne tudi bolj posrečene izbire (za katere bi se bilo treba bolj potruditi). Če je, denimo, G že sama simetrična grupa, je nima smisla vlagati v neprimerno večjo simetrično grupo $\mathrm{Sim}(G)$.

Vendarle pa ima ugotovitev, da vsako grupo G lahko vložimo prav v grupo $\mathrm{Sim}(G)$, tudi dobro plat. Če je G končna grupa, je $\mathrm{Sim}(G)$ grupa permutacij končne množice, torej simetrična grupa S_n za neki $n \in \mathbb{N}$. Tako velja tale posledica.

Posledica 3.42. *Vsako končno grupo G lahko vložimo v simetrično grupo S_n za neki $n \in \mathbb{N}$.*

Izkaže se, da so zanimivi tudi poljubni homomorfizmi iz grup v simetrične grupe, ne le vložitve. Ponavadi pa v zvezi s tem uporabljamo malce drugačen jezik in s tem povezane enostavnejše oznake. Pravimo, da grupa G **deluje na množici** X, če obstaja preslikava iz $G \times X$ v X, ki vsakemu paru (a, x) priredi element $a \cdot x \in X$, tako da velja:

(a) $(ab) \cdot x = a \cdot (b \cdot x)$ za vse $a, b \in G$ in vse $x \in X$.
(b) $1 \cdot x = x$ za vse $x \in X$.

Tej preslikavi potem pravimo **delovanje grupe G na množici X**. Pojem delovanja grupe na množici je ekvivalenten pojmu homomorfizma iz grupe v simetrično grupo. Res, če je φ homomorfizem iz grupe G v simetrično grupo $\mathrm{Sim}(X)$, potem je s predpisom

$$a \cdot x := \varphi(a)(x)$$

definirano delovanje G na X. Obratno, če je dano delovanje grupe G na množici X, potem lahko definiramo homomorfizem $\varphi : G \to \mathrm{Sim}(X)$ takole: $\varphi(a)$ je permutacija množice X, definirana s predpisom

$$\varphi(a)(x) := a \cdot x.$$

Bralcu svetujemo, da se o obojem prepriča. Prav nič težko ni, le slediti je treba definicijam. V dokazu, da je $\varphi(a)$ permutacija, se lahko naslonimo na formulo $a \cdot (a^{-1} \cdot x) = x$, ki sledi iz (a) in (b).

Grupa G deluje na sami sebi z običajnim množenjem. Prav to je delovanje, ki se uporabi v dokazu Cayleyevega izreka. Pri bolj poglobljenem študiju grup se srečamo z raznovrstnimi delovanji, ki včasih vodijo do presenetljivih rezultatov.

3.5.2. Vložitev kolobarja v kolobar endomorfizmov. Naj bo M aditivna (in zato Abelova) grupa. Označimo z

$$\mathrm{End}(M)$$

množico vseh njenih endomorfizmov, torej vseh aditivnih preslikav iz M vase. Vsoto $f + g$ in produkt fg endomorfizmov $f, g \in \mathrm{End}(M)$ definiramo enako kot v primeru 3.39, tj.

$$(f + g)(m) := f(m) + g(m),$$
$$(fg)(m) := f(g(m)).$$

Za tako definirani operaciji je $\mathrm{End}(M)$ kolobar. To preverimo rutinsko, podobno oziroma še laže kot preverimo v primeru 3.39, da je $\mathrm{End}_F(V)$ algebra. Naslednji izrek pokaže, da ima kolobar endomorfizmov aditivne grupe v teoriji kolobarjev podobno vlogo, kot jo ima simetrična grupa v teoriji grup.

Izrek 3.43. *Vsak kolobar K lahko vložimo v kolobar endomorfizmov neke aditivne grupe.*

Dokaz. Dokaz je podoben dokazu Cayleyevega izreka. Vlogo aditivne grupe M ima kar kolobar K. Za vsak $a \in K$ definirajmo $\ell_a : K \to K$, $\ell_a(x) = ax$. Očitno je ℓ_a aditivna preslikava, torej $\ell_a \in \mathrm{End}(K)$. Kot v dokazu Cayleyevega izreka vidimo, da je $\ell_{ab} = \ell_a \circ \ell_b$. Zlahka tudi preverimo, da je $\ell_{a+b} = \ell_a + \ell_b$ in $\ell_1 = \mathrm{id}_K$. Preslikava

$$\varphi : K \to \mathrm{End}(K),\ \varphi(a) = \ell_a,$$

je torej homomorfizem kolobarjev. Če je $a \in K$ tak, da je $\ell_a = 0$, je $a = \ell_a(1) = 0$. To pomeni, da ima φ trivialno jedro. Torej je vložitev. □

V dokazu Cayleyevega izreka smo pri obravnavi grupe $\mathrm{Sim}(G)$ »pozabili«, da je G grupa in smo jo obravnavali samo kot množico. Podobno v zadnjem dokazu pri obravnavi kolobarja $\mathrm{End}(K)$ zanemarimo množenje v kolobarju K in K obravnavamo le še kot aditivno grupo.

Podobna pot kot do pojma delovanja grupe na množici nas vodi do pojma modula M nad kolobarjem K. Aditivna grupa M skupaj z zunanjo binarno operacijo $(a, m) \mapsto am$ iz $K \times M$ v M je **modul nad kolobarjem** K, če velja:

(a) $(a + b)m = am + bm$ za vse $a, b \in K$ in vse $m \in M$.
(b) $a(m + n) = am + an$ za vse $a \in K$ in vse $m, n \in M$.
(c) $(ab)m = a(bm)$ za vse $a, b \in K$ in vse $m \in M$.
(d) $1m = m$ za vse $m \in M$.

Pojem modula je ekvivalenten pojmu homomorfizma iz kolobarja K v kolobar endomorfizmov aditivne grupe M. Če je $\varphi : K \to \mathrm{End}(M)$ homomorfizem, s predpisom

$$am := \varphi(a)(m)$$

postane M modul nad K. Obratno, če je M modul nad K, lahko definiramo homomorfizem $\varphi : K \to \mathrm{End}(M)$ s predpisom

$$\varphi(a)(m) := am.$$

Dokaz je preprosta vaja iz razumevanja definicij.

Definicije modula si ni težko zapomniti, saj je povsem enaka definiciji vektorskega prostora, le da namesto skalarjev, torej elementov nekega polja F, nastopajo elementi poljubnega kolobarja K. Lahko pa obrnemo pogled in rečemo, da je vektorski prostor modul nad poljem. Opažanja iz opombe

1.53 sedaj lahko strnemo v stavek, da je vsaka aditivna grupa modul nad kolobarjem $\mathbb{Z}$. Vsak kolobar K je modul nad samim seboj, če množenje v K interpretiramo kot modulsko operacijo (kot smo to posredno naredili v dokazu izreka 3.43).

Bolj natančno se modulu, ki smo ga definirali, reče *levi* modul nad K. Desni modul definiramo analogno, le elemente iz kolobarja pišemo na desni namesto na levi; natančneje, namesto am pišemo ma in (c) se glasi $m(ab) = (ma)b$.

Kot enega pomembnejših pojmov v algebri se je spodobilo modul vsaj omeniti. Podrobneje pa se z moduli v tej knjigi ne bomo ukvarjali.

3.5.3. Vložitev algebre v algebro linearnih preslikav. Če je A algebra nad poljem F, dokaz izreka 3.43 na očiten način lahko preoblikujemo tako, da namesto kolobarja endomorfizmov aditivne grupe dobimo algebro endomorfizmov vektorskega prostora. Zato rezultat, ki ga dobimo, zapišimo brez podrobnejše razlage.

Izrek 3.44. *Vsako algebro A lahko vložimo v algebro endomorfizmov nekega vektorskega prostora.*

(Levi) modul nad algebro A definiramo kot vektorski prostor M, v katerem poleg zahtev (a)-(d) iz definicije modula nad kolobarjem dodamo še zahtevo, da je

$$\lambda(am) = (\lambda a)m = a(\lambda m)$$

za vse $\lambda \in F$, $a \in A$, $m \in M$. Pojem modula nad algebro je ekvivalenten pojmu homomorfizma iz algebre v algebro endomorfizmov vektorskega prostora.

V izreku 3.44 za vektorski prostor seveda lahko izberemo kar A. Če je A končno-razsežna, lahko torej A vložimo v algebro endomorfizmov končno-razsežnega vektorskega prostora. Le-ta pa je izomorfna matrični algebri $M_n(F)$ (primer 3.39). Zato velja naslednja posledica.

Posledica 3.45. *Vsako končno-razsežno algebro lahko vložimo v matrično algebro $M_n(F)$ za neki $n \in \mathbb{N}$.*

Elemente grup si torej lahko vselej predstavimo kot permutacije, elemente kolobarjev (algeber) pa kot endomorfizme aditivnih grup (vektorskih prostorov). S tem sicer zanimivim dejstvom si največkrat ne moremo veliko pomagati – včasih pa vendarle. Ilustrirajmo s primerom.

Primer 3.46. Ali lahko končno-razsežna algebra A nad (denimo) poljem $\mathbb{R}$ vsebuje taka elementa s in t, da je

$$st - ts = 1?$$

Ker je algebra poljubna, se nam morda najprej zazdi, da se tega problema sploh ne znamo lotiti. S posledico 3.45 ga lahko pretvorimo v konkretnejši problem: ali obstajata taki matriki $S, T \in M_n(\mathbb{R})$, da je

$$ST - TS = I?$$

Z matrikami znamo računati in zdaj se rešitev ne zdi več nedosegljiva. Toda ne zaletimo se prehitro v dolge račune. Spomnimo se pojma *sled matrike*. Definirana je kot vsota diagonalnih elementov matrike. Kot je dobro znano in tudi ni težko preveriti, imata matriki ST in TS isto sled. Očitno je sled razlike matrik enaka razliki sledi. Zato je sled matrike $ST - TS$ enaka 0. Sled identične matrike I pa je seveda enaka n, torej je različna od 0. Matrika $ST - TS$ zato ne more biti enaka identiteti I in tudi odgovor na naše začetno vprašanje je negativen: za vsaka elementa $s, t \in A$ je $st - ts \neq 1$.

O vektorskih prostorih v tem razdelku nismo rekli nič. Ti imajo že v osnovi tako enostavno zgradbo, da jih nima smisla vlagati v kak drug prostor. Vsak netrivialen končno-razsežen vektorski prostor je izomorfen prostoru F^n (posledica 3.12) in temu ni kaj dodati.

Naloge

1. Preizkusi razumevanje dokaza Cayleyevega izreka in poišči podgrupi simetrične grupe S_4, izomorfni grupama $\mathbb{Z}_4$ in $\mathbb{Z}_2 \oplus \mathbb{Z}_2$.
2. Preizkusi razumevanje dokaza izreka 3.43 in poišči podkolobar kolobarja $\mathrm{End}(\mathbb{Z})$ (torej kolobarja endomorfizmov aditivne grupe $\mathbb{Z}$), izomorfnega kolobarju celih števil $\mathbb{Z}$.
3. Preizkusi razumevanje dokaza izreka 3.44 (in posledice 3.45) in poišči podalgebro realne algebre $M_4(\mathbb{R})$, izomorfno algebri kvaternionov $\mathbb{H}$.
4. Vsak element simetrične grupe S_n lahko zapišemo kot produkt takih elementov $a \in S_n$, da je $a^2 = 1$. To sledi iz dejstva, da je vsaka permutacija produkt transpozicij. Ker lahko vsako končno grupo G vložimo v simetrično grupo S_n za neki $n \in \mathbb{N}$, lahko tudi vsak element iz G zapišemo kot produkt takih elementov $a \in G$, da je $a^2 = 1$. Je to res? Ne more biti, saj denimo ciklična grupa z lihim redom razen enote sploh nima elementa a z lastnostjo $a^2 = 1$ (zakaj?). Kje v zgornjem razmisleku je napaka?
5. Naj grupa G deluje na množici X in naj bo $x \in X$. Množici

   $$G \cdot x = \{a \cdot x \mid a \in G\} \subseteq X$$

   pravimo **orbita** elementa x, množici

   $$G_x := \{a \in G \mid a \cdot x = x\} \subseteq G$$

pa **stabilizator** elementa x.

(a) Pokaži, da je s predpisom

$$x \sim y \iff y = a \cdot x \text{ za neki } a \in G$$

definirana ekvivalenčna relacija na množici X in da so ekvivalenčni razredi orbite elementov.

(b) Pokaži, da je stabilizator G_x podgrupa grupe G in da iz $x \sim y$ sledi, da sta si podgrupi G_x in G_y konjugirani.

6. Preveri, da so z naslednjimi predpisi podana delovanja grup na množicah in opiši orbite posameznih elementov:
   (a) Naj bo $G = \mathrm{GL}_n(\mathbb{R})$ in $X = \mathbb{R}^n$. Za $A \in G$ in $x \in X$ naj bo $A \cdot x$ običajni produkt matrike z vektorjem (ki ga pišemo kot stolpec).
   (b) Naj bo $G = S_3$ in $X = S_3$. Za $\sigma \in G$ in $\pi \in X$ naj bo $\sigma \cdot \pi = \sigma\pi\sigma^{-1}$.
   (c) Naj bo $G = \mathbb{R}$, torej grupa realnih števil za seštevanje, in naj bo X množica vseh linearnih funkcij iz $\mathbb{R}$ v $\mathbb{R}$. Za $t \in G$ in $f \in X$ naj bo $t \cdot f$ funkcija, definirana s predpisom $(t \cdot f)(x) = f(x) + t$.
   (d) Naj bosta G in X kot v (c). Za $t \in G$ in $f \in X$ naj bo $t \cdot f$ funkcija, definirana s predpisom $(t \cdot f)(x) = f(x + t)$.
7. Podmnožici N modula M nad kolobarjem K pravimo **podmodul**, če je za isti operaciji tudi sama modul. Razmisli, da je N podmodul natanko tedaj, ko je N podgrupa za seštevanje in ko je $an \in N$ za vse $a \in K$ in vse $n \in N$. Za modul $M \neq \{0\}$ rečemo, da je **enostaven**, če sta $\{0\}$ in M njegova edina podmodula. Pokaži, da je M enostaven natanko tedaj, ko za vsak $0 \neq m \in M$ velja $\{am \mid a \in K\} = M$.
8. Preveri, da so z naslednjimi operacijami definirani moduli nad kolobarji in ugotovi, ali so enostavni:
   (a) Naj bo K kolobar $M_n(\mathbb{R})$ in naj bo M aditivna grupa $\mathbb{R}^n$. Operacija iz $K \times M$ v M naj bo običajno množenje matrik z vektorji.
   (b) Naj bo K kolobar $\mathbb{Z}_8$ in naj bo M aditivna grupa $\{0, 2, 4, 6\} \leq \mathbb{Z}_8$. Operacija iz $K \times M$ v M naj bo običajno množenje v $\mathbb{Z}_8$.
   (c) Naj bo K kolobar zveznih funkcij $C[0, 1]$ in naj bo M aditivna grupa $\{f \in C[0, 1] \mid f(0) = 0\}$. Operacija iz $K \times M$ v M naj bo običajno množenje funkcij.
   (d) Naj bo K kolobar kvaternionov $\mathbb{H}$ in naj bo tudi $M = \mathbb{H}$ (le da M obravnavamo le kot aditivno grupo, ne kot kolobar). Operacija iz $K \times M$ v M naj bo običajno množenje kvaternionov.
9. Naj bo V vektorski prostor vseh polinomov z realnimi koeficienti in naj bo $T \in \mathrm{End}_{\mathbb{R}}(V)$ podan s predpisom $T(f(X)) = Xf(X)$. Poišči tak $S \in \mathrm{End}_{\mathbb{R}}(V)$, da je $ST - TS = I$.

   Komentar. Predpostavka v primeru 3.46, da je algebra A končnorazsežna, je torej potrebna.

10. Naj bo s obrnljiv element končno-razsežne realne algebre A. Pokaži, da je $sts^{-1} \neq t+1$ za vsak $t \in A$.
11. Prejšnja naloga pove, da za vsak notranji avtomorfizem φ končno-razsežne realne algebre A velja $\varphi(t) \neq t+1$ za vsak $t \in A$. Pokaži, da to velja za vse avtomorfizme φ, ne le za notranje.

    Namig. Z obravnavo preslikave $\varphi\ell_t\varphi^{-1} : A \to A$ problem prevedi na problem iz prejšnje naloge, s tem da vlogo algebre A prevzame algebra endomorfizmov vektorskega prostora A.

3.6. Vložitev celega kolobarja v polje ulomkov

V poljih imajo neničelni elementi inverze, kar je seveda velika prednost pred splošnimi kolobarji. Če lahko kolobar vložimo v polje, bodo imeli njegovi neničelni elementi inverze vsaj v tem polju, če jih že nimajo v kolobarju samem. Na primer, z izjemo števil 1 in -1 druga neničelna cela števila nimajo inverzov v kolobarju $\mathbb{Z}$, toda vsa so obrnljiva v polju $\mathbb{Q}$.

Kdaj lahko neničeln kolobar K vložimo v kako polje? Dve omejitvi sta očitni: K mora biti komutativen in ne sme imeti deliteljev niča (gl. posledico 1.46). Torej mora biti K *cel*. Pokazali bomo, da je ta pogoj tudi zadosten za obstoj vložitve v neko polje. Konstrukcija tega polja je glavna tema razdelka. Če povemo, da bomo samo sledili konstrukciji polja racionalnih števil, naloga pred nami ne bi smela biti težka. Toda kaj je formalna definicija racionalnih števil? Ker so nam ta števila tako domača, se s tem vprašanjem morda nismo obremenjevali. V definiciji gotovo moramo upoštevati, da na primer ulomki $\frac{1}{2}$, $\frac{2}{4}$, $\frac{-6}{-12}$ itd. predstavljajo isto racionalno število. S tem smo nakazali bistvo problema, s katerim se bomo soočili pri naši konstrukciji.

Do konca tega razdelka naj K *označuje poljuben cel kolobar*. Naš namen je konstruirati polje, ki bo v posebnem primeru, ko je K kolobar celih števil $\mathbb{Z}$, enako polju racionalnih števil $\mathbb{Q}$.

Lema 3.47. *S predpisom*

$$(a,b) \sim (a',b') \iff ab' = a'b$$

je definirana ekvivalenčna relacija na množici $K \times (K \setminus \{0\})$.

Dokaz. Refleksivnost in simetričnost relacije sta očitni. Dokažimo tranzitivnost. Privzemimo, da je $(a,b) \sim (a',b')$ in $(a',b') \sim (a'',b'')$, tj. $ab' = a'b$ in $a'b'' = a''b'$. Prvo enakost pomnožimo z b'' in drugo z b. Tako dobimo

$$ab'b'' = a'bb'' \quad \text{in} \quad a'bb'' = a''bb'.$$

Primerjava obeh enakosti da $ab'b'' = a''bb'$, tj. $(ab'' - a''b)b' = 0$. Ker $b' \in K \setminus \{0\}$ in ker K po predpostavki nima deliteljev niča, sledi $ab'' - a''b = 0$. Torej je $(a,b) \sim (a'',b'')$. □

Vpeljimo oznako

$$\frac{a}{b} := \text{ekvivalenčni razred elementa } (a,b).$$

Tu je a poljuben element iz K in b poljuben element iz $K \setminus \{0\}$. Ekvivalenčna razreda $\frac{a}{b}$ in $\frac{a'}{b'}$ sta seveda enaka natanko tedaj, ko je $(a,b) \sim (a',b')$. Torej velja

$$\frac{a}{b} = \frac{a'}{b'} \iff ab' = a'b.$$

LEMA 3.48. *Za poljubne $a, a', c, c' \in K$ in $b, b', d, d' \in K \setminus \{0\}$ iz*

$$\frac{a}{b} = \frac{a'}{b'} \quad \text{in} \quad \frac{c}{d} = \frac{c'}{d'}$$

sledi

$$\frac{ad+bc}{bd} = \frac{a'd'+b'c'}{b'd'} \quad \text{in} \quad \frac{ac}{bd} = \frac{a'c'}{b'd'}.$$

DOKAZ. Ker K nima deliteljev niča, sta elementa bd in $b'd'$ različna od 0. Zato imajo vsi nastopajoči izrazi smisel. Pokazati moramo, da iz

$$ab' = a'b \quad \text{in} \quad cd' = c'd$$

sledi

$$(ad+bc)b'd' = (a'd'+b'c')bd \quad \text{in} \quad (ac)(b'd') = (a'c')(bd).$$

S preureditvijo izrazov vidimo, da oboje res velja. □

Bralec je najbrž uganil pomen izrazov v lemi. V naslednjem izreku pridemo z besedo na dan.

IZREK 3.49. *Naj bo K cel klobar. Če v množico vseh ekvivalenčnih razredov*

$$F := \left\{ \frac{a}{b} \mid a, b \in K, b \neq 0 \right\}$$

vpeljemo seštevanje in množenje s predpisoma

$$\frac{a}{b} + \frac{c}{d} := \frac{ad+bc}{bd} \quad \text{in} \quad \frac{a}{b} \cdot \frac{c}{d} := \frac{ac}{bd},$$

postane F polje. Preslikava $\varphi : K \to F$, definirana z

$$\varphi(a) = \frac{a}{1},$$

je vložitev celega kolobarja K v polje F.

DOKAZ. Lema 3.48 pove, da sta operaciji seštevanja in množenja dobro definirani. Z neposrednim računom preverimo asociativnost in komutativnost obeh operacij ter veljavnost distributivnostnega zakona. Ničelni element je $\frac{0}{1}$, enota pa $\frac{1}{1}$. Nasprotni element elementa $\frac{a}{b}$ je element $\frac{-a}{b}$. Element $\frac{a}{b}$ je

različen od $0 = \frac{0}{1}$ natanko tedaj, ko $a \neq 0$. Njegov inverz je element $\frac{b}{a}$. Torej je F polje. Da je φ homomorfizem, sledi iz enakosti

$$\frac{a+b}{1} = \frac{a}{1} + \frac{b}{1} \quad \text{in} \quad \frac{ab}{1} = \frac{a}{1} \cdot \frac{b}{1}.$$

Če je $\varphi(a) = 0$, je očitno $a = 0$. To pomeni, da je φ vložitev. □

Definicija 3.50. Polje F iz izreka 3.49 se imenuje **polje ulomkov** celega kolobarja K.

Kolobar K obravnavamo kot podkolobar polja ulomkov F. Namesto $\frac{a}{1}$ pišemo kar a. Če je F_0 podpolje F, ki vsebuje K, potem vsebuje tudi inverz $\frac{1}{b}$ vsakega neničelnega elementa $b \in K$, iz česar jasno sledi, da je $F_0 = F$. To pomeni, da je polje ulomkov celega kolobarja K generirano z množico K.

Zabeležimo nekaj posebnih primerov.

Primer 3.51. Če je K že samo polje, je $F = K$.

Primer 3.52. Polje racionalnih števil $\mathbb{Q}$ je polje ulomkov kolobarja celih števil $\mathbb{Z}$.

Primer 3.53. Za vsako polje F je kolobar polinomov $F[X]$ cel kolobar (gl. trditev 2.19). Njegovo polje ulomkov imenujemo **polje racionalnih funkcij** v X in ga označujemo s $F(X)$. Splošneje, tudi kolobar polinomov več spremenljivk $F[X_1, \ldots, X_n]$ je cel in njegovemu polju ulomkov pravimo polje racionalnih funkcij v spremenljivkah $X_1, \ldots, X_n$. Označujemo ga s $F(X_1, \ldots, X_n)$.

Naslednja posledica izreka 3.49 povzema bistvo tega razdelka.

Posledica 3.54. *Vsak cel kolobar lahko vložimo v polje.*

Pri konstrukciji polja ulomkov smo večkrat uporabili predpostavko, da je kolobar K komutativen. Za nekomutativne kolobarje so podobne konstrukcije bistveno bolj zahtevne in tudi omejitve so strožje. Tako se izkaže, da ne moremo vsakega nekomutativnega kolobarja brez deliteljev niča vložiti v (nekomutativen) obseg.

Naloge

1. Naj bosta $f(X), g(X) \in \mathbb{R}[X]$ nekonstantna polinoma. Denimo, da sta v polju $\mathbb{R}(X)$ povezana z enakostjo

$$f(X) + \frac{1}{f(X)} = g(X) + \frac{1}{g(X)}.$$

Pokaži, da je potem $f(X) = g(X)$.

2. Naj bo $D : \mathbb{R}(X) \to \mathbb{R}(X)$ aditivna preslikava, ki slika konstantne polinome v 0 in zadošča
$$D\big(q(X)r(X)\big) = D\big(q(X)\big)r(X) + q(X)D\big(r(X)\big)$$
za vse $q(X), r(X) \in \mathbb{R}(X)$. Pokaži, da je
$$D\left(\frac{f(X)}{g(X)}\right) = u(X)\frac{f'(X)g(X) - f(X)g'(X)}{g(X)^2}$$
za vse $f(X), g(X) \in \mathbb{R}[X]$, kjer je $u(X) = D(X)$ in je $f'(X)$ odvod polinoma $f(X)$ (definiramo ga seveda takole: če je $f(X) = \sum_{k=0}^{n} a_k X^k$, je $f'(X) = \sum_{k=1}^{n} k a_k X^{k-1}$).
Nasvet. Najprej izračunaj $D(f(X))$.
3. Pokaži, da lahko vsak avtomorfizem celega kolobarja K razširimo na avtomorfizem njegovega polja ulomkov F.
Komentar. Pri tej in tudi naslednji nalogi ne pozabi preveriti dobre definiranosti preslikave.
4. Nak bo K podkolobar polja E. Pokaži, da je podpolje polja E, generirano s K, izomorfno polju ulomkov kolobarja K.
Komentar. Lep primer celega kolobarja je kolobar Gaussovih celih števil $\mathbb{Z}[i]$. Njegovo polje ulomkov je torej izomorfno polju $\mathbb{Q}(i) = \{p + qi \mid p, q \in \mathbb{Q}\}$ (gl. primer 1.88).

3.7. Karakteristika kolobarja in prapolja

V prejšnjih dveh razdelkih smo abstraktne grupe, kolobarje in algebre vložili v konkretnejše ali prikladnejše za študij. Kot ponavadi bomo polja obravnavali nekoliko drugače. Znotraj abstraktnega polja bomo poiskali konkretno polje.

Naj bo F polje. Ker vsebuje enoto 1, vsebuje tudi element $2 \cdot 1 = 1 + 1$. Zaradi enostavnosti ga označimo z 2. Podobno F vsebuje elemente
$$3 := 3 \cdot 1 = 1 + 1 + 1, \quad 4 := 4 \cdot 1 = 1 + 1 + 1 + 1 \text{ itn.}$$
Ker vsebuje tudi njihove nasprotne elemente in element 0, smo znotraj F našli kopijo celih števil. Toda F je polje, zato vsebuje tudi vse elemente oblike mn^{-1}, kjer sta m in n celi števili in $n \neq 0$. Torej F vsebuje kopijo racionalnih števil. Povedano drugače, polje racionalnih števil $\mathbb{Q}$ lahko vložimo v F. Res? Nekje smo se morali zmotiti. Za vsako praštevilo p je kolobar $\mathbb{Z}_p$ polje (trditev 2.15), ki kot končna množica ne more vsebovati neskončne množice $\mathbb{Q}$. Kje smo torej naredili napako? V $\mathbb{Z}_p$ je $p \cdot 1 = 0$, zato to polje ne vsebuje kopije celih števil. Če bi na začetku odstavka privzeli, da je $n \cdot 1 \neq 0$ za vsako naravno število n, pa v nadaljevanju ne bi bilo nič spornega.

Za nadaljnjo razpravo potrebujemo naslednjo definicijo.

Definicija 3.55. Naj bo K kolobar. Če obstajajo taka naravna števila n, da je $n \cdot 1 = 0$, potem najmanjšemu izmed njih pravimo **karakteristika kolobarja** K. Če takih naravnih števil ni, rečemo, da ima kolobar K **karakteristiko** 0.

Definicijo bi lahko povedali tudi drugače. Kolobar je aditivna grupa za seštevanje in njegova karakteristika je enaka redu enote (v smislu definicije 3.9), če je seveda le-ta končen. Sicer je karakteristika enaka 0.

Pogoj iz definicije se torej posredno tiče vseh elementov kolobarja, ne le enote 1. Namreč, ker je

$$n \cdot x = x + \cdots + x = (1 + \cdots + 1)x = (n \cdot 1)x,$$

v kolobarju K s karakteristiko n velja

$$n \cdot x = 0 \text{ za vse } x \in K.$$

Seveda bi lahko pojem karakteristike definirali tudi s pomočjo tega pogoja, ki pove več kot pogoj iz definicije. V nadaljevanju ga bomo uporabljali brez komentarja.

Primer 3.56. Večina kolobarjev, na katere najprej pomislimo, ima karakteristiko 0. Taki so npr. kolobarji $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ in $\mathbb{C}$.

Primer 3.57. Kolobar ostankov $\mathbb{Z}_n$ ima karakteristiko n. Tudi kolobar polinomov $\mathbb{Z}_n[X]$, kolobar matrik $M_k(\mathbb{Z}_n)$ in direktni produkt $\mathbb{Z}_n \times \mathbb{Z}_n$ imajo karakteristiko n.

Primer 3.58. Kolobar $\mathbb{Z}_3 \times \mathbb{Z}_2$ ima karakteristiko 6.

Pojem karakteristike je posebej pomemben za polja. Naslednjo trditev največkrat uporabljamo zanje, čeprav velja za širši razred kolobarjev.

Trditev 3.59. *Karakteristika neničelnega kolobarja K brez deliteljev niča je bodisi* 0 *bodisi praštevilo.*

Dokaz. Privzemimo, da je karakteristika K naravno število n. Dokazati moramo, da je n praštevilo. Denimo, da je $n = rs$ za neki naravni števili r in s. Potem je

$$(r \cdot 1)(s \cdot 1) = n \cdot 1 = 0.$$

Ker K nima deliteljev niča, mora biti eden izmed elementov $r \cdot 1$ in $s \cdot 1$ enak 0. Po predpostavki je n najmanjše naravno število, za katerega je $n \cdot 1 = 0$. Zato sledi $r = n$ ali $s = n$. Torej je n praštevilo. □

Polje ima torej lahko le ničelno ali praštevilsko karakteristiko.

Izrek 3.60. *Naj bo F polje.*

(a) *Če je karakteristika F enaka* 0*, lahko polje $\mathbb{Q}$ vložimo v F.*
(b) *Če je karakteristika F praštevilo p, lahko polje $\mathbb{Z}_p$ vložimo v F.*

Dokaz. (a) Ideja dokaza je bila že predstavljena na začetku razdelka. Samo formalizirati jo moramo. Definirajmo preslikavo $\varphi : \mathbb{Q} \to F$ s predpisom

$$\varphi\left(\frac{m}{n}\right) = (m \cdot 1)(n \cdot 1)^{-1}$$

za vse $m, n \in \mathbb{Z}$, $n \neq 0$. Dokazati moramo, da je ta preslikava dobro definirana. Privzemimo, da je $\frac{m}{n} = \frac{m'}{n'}$, kjer sta seveda n in n' različna od 0. Potem je $mn' = nm'$ in zato

$$(m \cdot 1)(n' \cdot 1) = (n \cdot 1)(m' \cdot 1).$$

Ker ima F karakteristiko 0, sta $n' \cdot 1$ in $n \cdot 1$ neničelna in zato obrnljiva elementa. Če zadnjo enakost pomnožimo z njunima inverzoma, dobimo

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

S tem smo dokazali, da je φ dobro definirana preslikava. Z neposrednim računom preverimo, da je φ homomorfizem. Njegovo jedro je očitno trivialno. Torej je φ vložitev.

(b) Da se izognemo dvoumnostim, bomo elemente iz $\mathbb{Z}_p$ označevali kot ob njihovi vpeljavi, torej s $[k]$, kjer je $k \in \mathbb{Z}$. Preslikavo $\varphi : \mathbb{Z}_p \to F$ definirajmo s predpisom

$$\varphi([k]) = k \cdot 1.$$

Iz $[k] = [\ell]$ sledi $k - \ell \in p\mathbb{Z}$ in zato $k \cdot 1 = \ell \cdot 1$. Torej je φ dobro definirana. Brez težav se prepričamo, da je φ vložitev. □

Vsako podpolje polja F vsebuje enoto 1. Podpolje, generirano z 1, je torej izmed vseh podpolj najmanjše; vsako drugo ga vsebuje. Imenujemo ga **prapolje** polja F. Kot vidimo iz dokaza izreka, je v obeh primerih $\operatorname{im}\varphi$ enak ravno prapolju F. Izrek lahko zato povemo tudi takole: če ima polje F karakteristiko 0, je njegovo prapolje izomorfno polju $\mathbb{Q}$, če pa ima karakteristiko p, je njegovo prapolje izomorfno polju $\mathbb{Z}_p$.

Naloge

1. Pokaži, da je karakteristika neničelnega komutativnega kolobarja K enaka 2 natanko tedaj, ko je $(x + y)^2 = x^2 + y^2$ za vse $x, y \in K$.
2. Naj ima kolobar K karakteristiko $n > 0$ in naj bo m poljubno celo število. Pokaži, da je $m \cdot 1 = 0$ natanko tedaj, ko n deli m.
3. Naj bo karakteristika kolobarja K praštevilo p. Pokaži, da element $a \in K$ zadošča $a^p = 1$ natanko tedaj, ko je $(a - 1)^p = 0$.

   Namig. Če ti ne uspe poiskati rešitve, si oglej dokaz leme 7.60.
4. Pokaži, da lahko polje $\mathbb{Q}$ vložimo v polje s karakteristiko 0 na natanko en način.

5. Pokaži, da lahko polje $\mathbb{Z}_p$ vložimo v polje s karakteristiko p na natanko en način.
6. Naj bosta K in K' kolobarja. Ugotovi, katera izmed naslednjih trditev je pravilna:
   (a) Če obstaja vložitev K v K', imata K in K' isto karakteristiko.
   (b) Če obstaja epimorfizem iz K v K', imata K in K' isto karakteristiko.

   Nepravilno trditev ovrzi s primerom.
7. Naj bo $n \in \mathbb{N}$. Za katere $k \in \mathbb{N}$ obstaja homomorfizem kolobarjev iz $\mathbb{Z}_n$ v $\mathbb{Z}_k$?
8. Kolobar $K \neq \{0\}$ imenujemo **enostaven kolobar**, če za vsak $a \neq 0$ iz K obstajajo taki elementi $x_i, y_i \in K$, $i = 1, \ldots, n$, da je $\sum_{i=1}^{n} x_i a y_i = 1$. Pokaži, da je karakteristika enostavnega kolobarja bodisi 0 bodisi praštevilo.

   Komentar. V naslednjem poglavju bomo podali definicijo enostavnega kolobarja na bolj standarden način, ki pa je tej ekvivalentna (gl. nalogo 4.3/3). Očitni primeri enostavnih kolobarjih so obsegi, še zdaleč pa niso edini.

   Omenimo, da je ugotovitev naloge neodvisna od trditve 3.59. Kolobar $\mathbb{Z}$ nima deliteljev niča, a ni enostaven (zakaj?), kolobar $M_n(\mathbb{R})$ pa ima delitelje niča, a je enostaven (gl. nalogo 4.3/5).
9. Pokaži, da ima algebra A nad poljem F isto karakteristiko kot F.
10. Naj bo A algebra nad poljem s karakteristiko različno od 2 in naj element $a \in A$ zadošča $a^2 = 1$. Pokaži, da je A direktna vsota svojih podprostorov $A_0 = \{x \in A \mid ax = xa\}$ in $A_1 = \{x \in A \mid ax = -xa\}$.

    Komentar. Izvzetje primera, ko je karakteristika polja enaka 2, je očitno potrebno, saj je tedaj $A_0 = A_1$. Karakteristika 2 je nasploh nekaj posebnega. Seštevanje in odštevanje se takrat ujemata, kar ima različne posledice.

POGLAVJE 4

Kvocientne strukture

V tem poglavju se bomo seznanili s posebnimi podgrupami grup, ki jim pravimo edinke. S pomočjo vsake edinke lahko iz grupe konstruiramo novo grupo, imenovano kvocientna grupa. Podobno iz posebnih podmnožic kolobarjev, imenovanih ideali, konstruiramo kvocientne kolobarje. Poseben primer teh konstrukcij smo srečali pri vpeljavi grupe oziroma kolobarja ostankov $\mathbb{Z}_n$, le da smo se takrat izrazoma kvocientna grupa oziroma kvocientni kolobar izognili.

Kvocientne strukture so tesno povezane s homomorfizmi. Vsak homomorfizem porodi kvocientno strukturo, in obratno, kvocientna struktura porodi homomorfizem. Preko te zveze bomo lahko bolje razumeli pomen homomorfizmov, ki niso injektivni. Pravi smisel in pomen tako homomorfizmov kot kvocientnih struktur pa bosta prišla do izraza v naslednjih poglavjih, ko bomo te pojme uporabljali kot orodja pri reševanju pomembnih problemov.

4.1. Odseki in Lagrangeov izrek

V tem poglavju se bo vse vrtelo okoli naslednjega pojma.

Definicija 4.1. Naj bo H podgrupa grupe G in naj bo $a \in G$. Množici

$$aH := \{ah \,|\, h \in H\}$$

pravimo **odsek** grupe G po podgrupi H.

Če je G aditivna grupa, odsek pišemo kot $a + H$. Torej je

$$a + H = \{a + h \,|\, h \in H\}.$$

Kasneje bomo ta zapis uporabljali tudi v vektorskih prostorih, kolobarjih in algebrah. Toda zdaj se vrnimo h grupi, opremljeni z množenjem.

Odseki v splošnem niso podgrupe. Če $a \notin H$, odsek aH ne vsebuje enote (zakaj?) in že zato ne more biti podgrupa. Primer, ko je $a \in H$, je drugačen. Velja namreč

$$aH = H \iff a \in H. \tag{4.1}$$

To kratko vajo iz razumevanja definicije prepuščamo bralcu. Sicer pa bomo kmalu dokazali lemo 4.6, ki obravnava splošnejšo situacijo.

Odsek aH natančneje imenujemo **levi odsek**. **Desni odsek** vpeljemo kot množico

$$Ha := \{ha \,|\, h \in H\}.$$

Ker pa bomo z redkimi izjemami obravnavali samo leve odseke, bomo pridevnik »levi« praviloma izpuščali. Lahko bi se odločili za obravnavo le desnih odsekov. Izbrali smo pač eno od enakovrednih možnosti.

Oglejmo si nekaj primerov. V prvih dveh bomo obravnavali aditivni grupi.

PRIMER 4.2. Naj bo $G = \mathbb{Z}$ in $H = n\mathbb{Z}$, $n \in \mathbb{N}$. Odseki, ki jih porodijo $0, 1, \ldots, n-1$, so

$$n\mathbb{Z},\ 1 + n\mathbb{Z},\ \ldots\ , (n-1) + n\mathbb{Z}.$$

V odseku $n\mathbb{Z}$ so vsa števila, ki so deljiva z n, v odseku $1 + n\mathbb{Z}$ so vsa števila, ki imajo pri deljenju z n ostanek 1 itd. To so tudi edini odseki, saj je

$$\begin{aligned} n + n\mathbb{Z} &= n\mathbb{Z}, \\ (n+1) + n\mathbb{Z} &= 1 + n\mathbb{Z}, \ \text{itd.} \end{aligned}$$

in podobno

$$\begin{aligned} -1 + n\mathbb{Z} &= (n-1) + n\mathbb{Z}, \\ -2 + n\mathbb{Z} &= (n-2) + n\mathbb{Z}, \ \text{itd.} \end{aligned}$$

S temi množicami smo se srečali že v razdelku 2.2 pri vpeljavi grupe (in kolobarja) ostankov $\mathbb{Z}_n$. Tam smo odsek $a + n\mathbb{Z}$ označevali z $[a]$ (in kasneje kar z a, če je $0 \leq a < n$).

PRIMER 4.3. Naj bo G aditivna grupa $\mathbb{R}^2$ in naj bo H abscisna os, torej premica $y = 0$. Odseki $a + H$ so horizontalne premice, tj. premice vzporedne premici H.

PRIMER 4.4. Naj bo $G = \mathbb{C}^*$, tj. grupa neničelnih kompleksnih števil z operacijo množenja. Za H vzemimo njeno podgrupo $\mathbb{T}$, torej krožno grupo. Odsek zH je množica vseh kompleksnih števil, ki imajo isto absolutno vrednost kot število $z \in \mathbb{C}^*$. Geometrijsko lahko odseke opišemo kot koncentrične krožnice.

PRIMER 4.5. Naj bo G simetrična grupa S_n in H alternirajoča grupa A_n. Če $\sigma \in H$, torej če je σ soda permutacija, je $\sigma H = H$. Če pa je σ liha permutacija, je, kot hitro razmislimo, σH množica vseh lihih permutacij. Odseka sta torej samo dva. Prvi sestoji iz vseh sodih permutacij, drugi pa iz vseh lihih permutacij.

V naslednjih lemah privzemimo, da je G poljubna grupa in H njena podgrupa. Prva lema odgovori na vprašanje, kdaj različna elementa porodita isti odsek.

LEMA 4.6. *Za poljubna $a, b \in G$ velja*

$$aH = bH \iff a^{-1}b \in H.$$

DOKAZ. Če je $aH = bH$, potem $b = b \cdot 1 \in bH = aH$. Torej je $b = ah_0$ za neki $h_0 \in H$. Če to enakost pomnožimo z leve z a^{-1}, dobimo $a^{-1}b = h_0 \in H$.

Za dokaz obratne trditve privzemimo, da je $h_0 := a^{-1}b \in H$. Potem je $b = ah_0$ in zato $bh = a(h_0h) \in aH$ za vsak $h \in H$. Torej je $bH \subseteq aH$. Ker je

$$b^{-1}a = (a^{-1}b)^{-1} = h_0^{-1} \in H,$$

na enak način vidimo, da je $aH \subseteq bH$. □

Pogoj $a^{-1}b \in H$ nas spomni na karakterizacijo pojma podgrupe: neprazna podmnožica H grupe G je podgrupa natanko tedaj, ko iz $a, b \in H$ sledi $a^{-1}b \in H$. Za razliko od leme 4.6 pa se tu obravnava le situacija, ko sta a in b elementa iz H. Podgrupo lahko karakteriziramo tudi z lastnostjo, da je $ab^{-1} \in H$ za vse $a, b \in H$. Če sta a in b elementa iz G (in ne nujno iz H), je pogoj $ab^{-1} \in H$ ekvivalenten enakosti *desnih* odsekov Ha in Hb. Pri obravnavi enakosti odsekov je torej potrebno nekaj previdnosti, pogoja $a^{-1}b \in H$, $a, b \in G$, in $ab^{-1} \in H$, $a, b \in G$, si nista ekvivalentna. Kako si zapomniti, kateri ustreza »našim«, torej levim odsekom? Enostavno! Formulo $aH = bH$ pomnožimo z leve z inverzom enega izmed obeh elementov, npr. z inverzom a, in dobimo $H = a^{-1}bH$. To pa je izpolnjeno tedaj (in le tedaj), ko je $a^{-1}b \in H$. V Abelovih grupah so ta opozorila seveda odveč. V aditivni grupi ugotovitev iz leme zapišemo takole:

$$a + H = b + H \iff b - a \in H \,(\iff a - b \in H).$$

V vseh zgornjih primerih različna odseka nista imela nobenega skupnega elementa. Ni šlo za naključja.

LEMA 4.7. *Za poljubna $a, b \in G$ sta odseka aH in bH bodisi enaka bodisi disjunktna.*

DOKAZ. Denimo, da je $aH \cap bH \neq \emptyset$. Naj bosta $h_1, h_2 \in H$ taka, da je $ah_1 = bh_2$. Če pomnožimo to enakost z leve z a^{-1} in z desne s h_2^{-1}, dobimo $a^{-1}b = h_1h_2^{-1} \in H$. Iz leme 4.6 sledi, da je $aH = bH$. □

Grupa G je torej disjunktna unija odsekov aH. Vsak element a iz G namreč leži v odseku aH, različna odseka pa sta disjunktna. Kadar je neka množica disjunktna unija svojih podmnožic, lahko v množico uvedemo ekvivalenčno relacijo, tako da so ekvivalenčni razredi ravno te podmnožice. V luči leme 4.6 je v našem primeru ta ekvivalenčna relacija definirana takole:

$$a \sim b \iff a^{-1}b \in H.$$

To omenjamo predvsem kot zanimivost. Za cilje tega poglavja sta ključni lemi 4.6 in 4.7 in z njima bi lahko ta razdelek tudi zaključili. Vendar smo le še korak

oddaljeni od temeljnega izreka teorije končnih grup, zato se je težko ustaviti. Potrebujemo samo še eno definicijo. Moči množice vseh odsekov $\{aH \mid a \in G\}$ grupe G po podgrupi H pravimo **indeks podgrupe** H in jo označujemo z

$$[G : H].$$

Če je G končna grupa, je seveda $[G : H] < \infty$ za vsako podgrupo H. Tudi podgrupe neskončnih grup imajo lahko končen indeks. Denimo, $[\mathbb{Z} : n\mathbb{Z}] = n$ (gl. primer 4.2).

Napovedani izrek se imenuje po *Joseph-Louisu Lagrangeu*, ki je leta 1771, še pred uvedbo pojma grupe, izpeljal njegov poseben primer.

Izrek 4.8. ***(Lagrangeov izrek)*** *Naj bo H podgrupa končne grupe G. Potem je*

$$|G| = [G : H] \cdot |H|.$$

Dokaz. Namesto $[G : H]$ pišimo r. Množico vseh odsekov tako lahko zapišemo kot $\{a_1H, \ldots, a_rH\}$ za neke $a_i \in G$. Po lemi 4.7 je grupa G disjunktna unija množic $a_1H, \ldots, a_rH$. Zato je

$$|G| = |a_1H| + \cdots + |a_rH|. \tag{4.2}$$

Vsako izmed števil $|a_iH|$ pa je kar enako $|H|$. Preslikava $h \mapsto a_ih$ iz H v a_iH je namreč bijektivna – ker iz $a_ih = a_ih'$ sledi $h = h'$, je injektivna, surjektivna pa je očitno. Zato iz (4.2) sledi $|G| = r|H|$. □

Primer 4.9. Ker ima grupa S_n red $n!$ in je $[S_n : A_n] = 2$ (gl. primer 4.5), ima grupa A_n red $\frac{n!}{2}$.

Glavno sporočilo izreka je, da je red končne grupe deljiv z redom vsake njene podgrupe. Od tod se hitro izpeljejo številna pomembna dejstva o končnih grupah. Toda s tem počakajmo do začetka naslednjega poglavja. V nadaljevanju tega se bomo posvetili odsekom nekaterih posebnih podgrup.

Naloge

1. Opiši odseke kvaternionske grupe Q po podgrupi $\{1, -1\}$.
2. Opiši odseke kvaternionske grupe Q po podgrupi $\{1, -1, i, -i\}$.
3. Opiši odseke grupe $(\mathbb{R}^3, +)$ po podgrupi $\{(x, 0, 0) \mid x \in \mathbb{R}\}$.
4. Opiši odseke grupe $(\mathbb{R}^3, +)$ po podgrupi $\{(x, y, 0) \mid x, y \in \mathbb{R}\}$.
5. Opiši odseke grupe $(\mathbb{C}^*, \cdot)$ po podgrupi $\{1, -1\}$.
6. Opiši odseke grupe $(\mathbb{C}^*, \cdot)$ po podgrupi $\mathbb{R}^+$.
7. Opiši odseke grupe $(\mathbb{C}^*, \cdot)$ po podgrupi $\mathbb{R}^*$.
8. Naj bo G končna grupa in $H \leq G$. Pokaži, da obstajata taka elementa $a, b \in G$, da $a \notin H$, $b \notin H$ in $ab \notin H$ natanko tedaj, ko je $|G| > 2|H|$.

9. Naj bo $H = \{1, (1\,2)\} \leq S_3$. Poišči vse leve odseke aH in vse desne odseke Ha, kjer $a \in S_3$. Pokaži, da iz $aH = bH$ ne sledi $Ha = Hb$.
10. Naj bo G poljubna grupa in $H \leq G$. Pokaži, da sta desna odseka Ha in Hb enaka natanko tedaj, ko je $ba^{-1} \in H$. Od tod izpelji še inačico leme 4.7 in izreka 4.8 za desne odseke.

    Komentar. Ker Lagrangeov izrek torej velja tako za leve kot za desne odseke, je moč množice vseh desnih odsekov končne grupe po njeni podgrupi enaka moči množice vseh levih odsekov. V naslednji nalogi je treba pokazati, da to velja tudi brez predpostavke o končnosti grupe.
11. Naj bo $H \leq G$. Poišči bijektivno preslikavo iz množice vseh levih odsekov $\mathcal{L} = \{aH \mid a \in G\}$ v množico vseh desnih odsekov $\mathcal{D} = \{Ha \mid a \in G\}$.

    Namig. Iz ugotovitve naloge 9 sledi, da predpis $aH \mapsto Ha$ ni smiseln (zakaj?). Pri iskanju preslikave ne pozabi na dobro definiranost!

4.2. Podgrupe edinke in kvocientne grupe

Kot smo omenili v primeru 4.2, smo se z odseki že srečali v razdelku 2.2. Elementi grupe ostankov $\mathbb{Z}_n$ so odseki $a + n\mathbb{Z}$, ki smo jih tedaj označevali z $[a]$. V spremenjenih oznakah se definicija seštevanja v $\mathbb{Z}_n$ glasi takole:

$$(a + n\mathbb{Z}) + (b + n\mathbb{Z}) = (a + b) + n\mathbb{Z}. \tag{4.3}$$

Množica vseh odsekov grupe $\mathbb{Z}$ glede na njeno podgrupo $n\mathbb{Z}$ torej na enostaven in naraven način postane grupa. Ali lahko tu $\mathbb{Z}$ in $n\mathbb{Z}$ zamenjamo s poljubno grupo in njeno podgrupo?

4.2.1. Definicija podgrupe edinke in kvocientne grupe. Naj bo G poljubna grupa. Njeno podgrupo bomo v tem razdelku označevali z N – razlog za tako oznako bo kmalu pojasnjen. Operacijo v abstraktni grupi pišemo kot množenje. V luči (4.3) se za definicijo operacije v množici vseh odsekov

$$G/N := \{aN \mid a \in G\}$$

zato ponuja predpis $aN \cdot bN := (ab)N$. Tu je seveda ab produkt elementov a in b v grupi G. Toda ali je to množenje dobro definirano? Naslednja lema pove, da le tedaj, ko podgrupa N izpolnjuje poseben pogoj.

Lema 4.10. *Naj bo N podgrupa grupe G. Naslednja pogoja sta ekvivalentna:*

(i) *Za vse $a, a', b, b' \in G$ iz $aN = a'N$ in $bN = b'N$ sledi $(ab)N = (a'b')N$.*
(ii) *Za vse $a \in G$ in $n \in N$ je $ana^{-1} \in N$.*

Dokaz. Iz leme 4.6 razberemo, da lahko pogoj (i) zapišemo tudi takole:

$$a^{-1}a' \in N \ \wedge \ b^{-1}b' \in N \implies b^{-1}a^{-1}a'b' = (ab)^{-1}(a'b') \in N. \tag{4.4}$$

(i)⇒(ii). Za poljubna elementa $n \in N$ in $a \in G$ je $1^{-1}n = n \in N$ in $aa^{-1} = 1 \in N$. Zato iz (4.4) sledi $ana^{-1} = (a^{-1})^{-1}1^{-1}na^{-1} \in N$.

(ii)⇒(i). Naj bodo $a, a', b, b' \in G$ taki, da je

$$n_1 := a^{-1}a' \in N \quad \text{in} \quad n_2 := b^{-1}b' \in N.$$

Iz zapisa

$$b^{-1}a^{-1}a'b' = b^{-1}n_1bb^{-1}b' = (b^{-1}n_1b)n_2$$

vidimo, da iz (ii) in iz predpostavke, da je N podgrupa, sledi $b^{-1}a^{-1}a'b' \in N$. Torej velja (4.4) in s tem (i). □

Pomembno sporočilo leme je, da iz pogoja (ii) sledi pogoj (i). Veljavnost obratne implikacije smo zabeleležili predvsem kot zanimivost in motivacijo za obravnavo podgrup, ki zadoščajo pogoju (ii). Dajmo jim ime.

Definicija 4.11. Če podgrupa N grupe G zadošča pogoju (ii) (in zato tudi (i)) iz leme 4.10, se imenuje **podgrupa edinka** ali kar **edinka**. V tem primeru pišemo $N \triangleleft G$.

V dobesednem prevodu iz angleškega jezika bi edinke imenovali normalne podgrupe. Od tod oznaka N. Čeprav se je v slovenščini zasidral drugačen izraz, se oklenimo standardnega označevanja podgrup edink.

Zapis $N \triangleleft G$ torej beremo kot »N je podgrupa edinka grupe G«. Spomnimo se še zapisa $H \leq G$, ki ga beremo kot »H je podgrupa grupe G«. Torej velja:

$$N \triangleleft G \iff N \leq G \text{ in } aNa^{-1} \subseteq N \text{ za vsak } a \in G.$$

Z aNa^{-1} smo seveda označili množico $\{ana^{-1} \mid n \in N\}$.

Podali smo eno izmed možnih definicij edinke. Naslednja trditev podaja tri pogoje, ki so ekvivalentni pogoju iz naše definicije.

Trditev 4.12. *Za podgrupo N grupe G so naslednji pogoji ekvivalentni:*

(i) *N je edinka (tj. $aNa^{-1} \subseteq N$ za vsak $a \in G$).*
(ii) *$aN \subseteq Na$ za vsak $a \in G$.*
(iii) *$aN = Na$ za vsak $a \in G$.*
(iv) *$aNa^{-1} = N$ za vsak $a \in G$.*

Dokaz. (i)⇒(ii). Če $aNa^{-1} \subseteq N$ z desne pomnožimo z a, dobimo $aN \subseteq Na$ (bralec naj razmisli, da tovrstno množenje elementa z množico res ohranja inkluzijo).

(ii)⇒(iii). Ker $aN \subseteq Na$ velja za vsak $a \in G$, je tudi $a^{-1}N \subseteq Na^{-1}$ za vsak $a \in G$. Če to inkluzijo pomnožimo z leve in hkrati z desne z a, dobimo $Na \subseteq aN$. Torej je $aN = Na$.

(iii)⇒(iv). Enakost $aN = Na$ pomnožimo z desne z a^{-1}.
(iv)⇒(i). To je očitno. □

Pogoj (iv) lahko izrazimo z besedami: edina *konjugirana podgrupa* podgrupe N je podgrupa N sama. Opozorimo, da to ne pomeni nujno, da je $ana^{-1} = n$ za vse $a \in G$ in $n \in N$. Prav tako pogoja (iii), ki pravi, da je levi odsek aN enak desnemu odseku Na, ne smemo razumeti kot $an = na$ za vse $a \in G$ in $n \in N$. Gre le za enakost množic aN in Na.

Vrnimo se k izhodiščnemu vprašanju.

Izrek 4.13. *Naj bo $N \triangleleft G$. Če v množico vseh odsekov G/N vpeljemo množenje s predpisom*

$$aN \cdot bN = (ab)N,$$

postane G/N grupa. Preslikava $\pi : G \to G/N$, definirana s

$$\pi(a) = aN$$

je epimorfizem in $\ker \pi = N$.

Dokaz. Dobra definiranost množenja sledi iz leme 4.10. Asociativnost je posledica asociativnosti množenja v G:

$$(aN \cdot bN) \cdot cN = (ab)N \cdot cN = ((ab)c)N = (a(bc))N = aN \cdot (bN \cdot cN)\,.$$

Enota je odsek $N(= 1N)$. Inverz odseka aN je odsek $a^{-1}N$. Torej je G/N grupa. Enakost $aN \cdot bN = (ab)N$ lahko prepišemo kot $\pi(a)\pi(b) = \pi(ab)$. To pomeni, da je π homomorfizem; očitno je surjektiven, torej epimorfizem. Element $a \in G$ pripada jedru π natanko tedaj, ko je $aN = N$, kar pa je po lemi 4.6 (ali po (4.1)) ekvivalentno pogoju, da je $a \in N$. □

Definicija 4.14. Grupi G/N iz izreka 4.13 pravimo **kvocientna** ali **faktorska grupa**, preslikavi π pa **kanonični epimorfizem**.

Beseda *kanonični* se v matematiki pogosto uporablja. Kot sopomenki se morda ponujata besedi *naravni* ali pa *standardni*, natančno pa ta pojem težko definiramo. Razumemo ga skozi primere.

Izrek 4.13 povezuje odseke in homomorfizme. Formula $\pi(ab) = \pi(a)\pi(b)$ je le drugačen zapis formule $aN \cdot bN = (ab)N$, enakost $\ker \pi = N$ pa je drugačen zapis ekvivalentnosti pogojev $aN = N$ in $a \in N$. Vsaka edinka je torej jedro kakega homomorfizma. Pokažimo, da velja tudi obratno, da torej pojma »podgrupa edinka« in »jedro homomorfizma grup« sovpadata.

Trditev 4.15. *Podmnožica N grupe G je podgrupa edinka natanko tedaj, ko je N jedro homomorfizma iz grupe G v neko grupo G'.*

Dokaz. Naj bo $N = \ker \varphi$ za neki homomorfizem $\varphi : G \to G'$. Če sta $m, n \in N$, je tudi $mn^{-1} \in N$, saj je

$$\varphi(mn^{-1}) = \varphi(m)\varphi(n)^{-1} = 1 \cdot 1^{-1} = 1.$$

Torej je N podgrupa. Za vsak $a \in G$ in vsak $n \in N$ je

$$\varphi(ana^{-1}) = \varphi(a)\varphi(n)\varphi(a)^{-1} = \varphi(a)1\varphi(a)^{-1} = 1,$$

tj. $ana^{-1} \in N$ in zato je N edinka. Obratno, vsaka podgrupa edinka je jedro kanoničnega epimorfizma. □

S primeri edink in kvocientnih grup počakajmo do razdelka 4.4, ko si bomo lahko pomagali s t. i. izrekom o izomorfizmu. Zaenkrat podajmo samo nekaj enostavnih opazk.

Vsaka netrivialna grupa G ima vsaj dve podgrupi edinki, to sta $\{1\}$ in G. Če sta to tudi edini edinki, G imenujemo **enostavna grupa**. O takih grupah bomo nekaj več spregovorili v poglavju o končnih grupah. Brez dokazov omenimo samo dva primera, ciklično grupo praštevilskega reda in alternirajočo grupo A_n, kjer je $n \geq 5$.

Če je G končna grupa in $N \triangleleft G$, je po Lagrangeovem izreku

$$|G/N| = \frac{|G|}{|N|}.$$

Od tod med drugim sledi, da red kvocientne grupe deli red grupe.

V Abelovi grupi je očitno kar vsaka podgrupa edinka. Če je G aditivna grupa in N njena poljubna podgrupa, je tako $G/N = \{a + N \mid a \in G\}$ grupa za seštevanje, definirano s predpisom

$$(a + N) + (b + N) = (a + b) + N.$$

Formula (4.3) je poseben primer. Kvocientna grupa $\mathbb{Z}/n\mathbb{Z}$ je torej grupa ostankov $\mathbb{Z}_n$.

4.2.2. Produkt podgrup. V različnih pogledih je delo z edinkami lažje kot delo s splošnimi podgrupami. Oglejmo si pojem **produkta dveh podgrup**. Če sta H in K podgrupi grupe G, njun produkt definiramo kot množico

$$HK := \{hk \mid h \in H, k \in K\}.$$

V splošnem ta množica ni podgrupa (gl. nalogo 15).

Trditev 4.16. *Naj bo G grupa.*

(a) *Če sta $H, K \leq G$ in je $HK = KH$, je $HK \leq G$.*
(b) *Če je $H \leq G$ in $N \triangleleft G$, je $HN = NH \leq G$.*
(c) *Če sta $M, N \triangleleft G$, je $MN = NM \triangleleft G$.*

Dokaz. (a) Vzemimo $h_1, h_2 \in H$ in $k_1, k_2 \in K$. Pokazati moramo, da

$$(h_1k_1)(h_2k_2)^{-1} = h_1k_1k_2^{-1}h_2^{-1}$$

leži v HK. Ker $k_1k_2^{-1} \in K$, $h_2^{-1} \in H$ in je $KH = HK$, lahko $k_1k_2^{-1}h_2^{-1}$ zapišemo kot h_3k_3 za neka $h_3 \in H$ in $k_3 \in K$. Zato je

$$h_1k_1k_2^{-1}h_2^{-1} = (h_1h_3)k_3 \in HK.$$

(b) Po trditvi 4.12 je $hN = Nh$ za vsak $h \in H$. Zato je $HN = NH$.
(c) Dokazati moramo le, da je $aMNa^{-1} \subseteq MN$ za vsak $a \in G$. To takoj sledi iz enakosti $a(mn)a^{-1} = (ama^{-1})(ana^{-1})$. □

Produkt podgrup Abelove grupe torej je podgrupa. V aditivnih grupah namesto o produktu seveda govorimo o vsoti. **Vsota podgrup**

$$H + K = \{h + k \mid h \in H, k \in K\}$$

aditivne grupe G torej je podgrupa. Ne glede na to, ali je grupa Abelova ali ni, je produkt edink spet edinka. Kot zlahka preverimo, je tudi **presek edink** M in N spet edinka, torej

$$M \cap N \lhd G.$$

Seveda je

$$M \cap N \subseteq N \subseteq MN = NM.$$

Slednja enakost je enakost množic in ne pomeni nujno, da elementi iz M komutirajo z elementi iz N. Navsezadnje lahko za M in N izberemo kar G. V luči tega je naslednja trditev zanimiva. Z njo bi radi opozorili tudi na koristnost pojma **komutator**. Spomnimo se (gl. nalogo 2.8/7), da je komutator elementov a in b element $aba^{-1}b^{-1}$. Označujemo ga z $[a, b]$. Očitno a in b komutirata natanko tedaj, ko je njun komutator enak 1.

Trditev 4.17. *Če sta $M, N \lhd G$, je $[m, n] \in M \cap N$ za vse $m \in M$ in $n \in N$. Iz $M \cap N = \{1\}$ tako sledi, da je je $mn = nm$ za vse $m \in M$ in $n \in N$.*

Dokaz. Če $[m, n]$ pišemo kot $m(nm^{-1}n^{-1})$ in upoštevamo, da je M podgrupa edinka, vidimo, da je $[m, n] \in M$. Podobno iz $[m, n] = (mnm^{-1})n^{-1}$ razberemo, da je $[m, n] \in N$. □

Nazadnje omenimo, da lahko govorimo tudi o produktu več, ne le dveh podgrup. **Produkt podgrup** $H_1, \ldots, H_m$ grupe G definiramo kot množico

$$H_1H_2 \cdots H_m := \{h_1h_2 \cdots h_m \mid h_i \in H_i, i = 1, \ldots, m\}.$$

Iz trditve 4.16 sledi, da je $N_1N_2 \cdots N_m$ edinka, če so $N_1, N_2, \ldots, N_m$ edinke.

4.2.3. Podgrupe kvocientne grupe. Kadar nas zanima zgradba neke grupe, se težko izognemo obravnavi njenih podgrup in posebej edink. Kaj lahko rečemo o podgrupah kvocientne grupe G/N? Kako so povezane s podgrupami grupe G? Do odgovorov nas bo vodila naslednja lema. Najprej se spomnimo dveh standardnih oznak. Če je f preslikava iz množice A v množico A', B podmnožica A in B' podmnožica A', potem pišemo

$$f(B) := \{f(b) \mid b \in B\}$$

in

$$f^{-1}(B') := \{a \in A \mid f(a) \in B'\}.$$

LEMA 4.18. *Naj bo $\varphi : G \to G'$ homomorfizem grup.*

(a) *Če je $H' \leq G'$, je $\varphi^{-1}(H') \leq G$.*
(b) *Če je $N' \lhd G'$, je $\varphi^{-1}(N') \lhd G$.*
(c) *Če je $H \leq G$, je $\varphi(H) \leq G'$.*
(d) *Če je $N \lhd G$ in je φ epimorfizem, je $\varphi(N) \lhd G'$.*

DOKAZ. (a) Vzemimo $h, k \in \varphi^{-1}(H')$. Potem $\varphi(h), \varphi(k) \in H'$. Pokazati moramo, da $hk^{-1} \in \varphi^{-1}(H')$, torej da $\varphi(hk^{-1}) \in H'$. Ker je $\varphi(hk^{-1}) = \varphi(h)\varphi(k)^{-1}$ in je H' podgrupa, to res velja.

(b) Ker po trditvi (a) vemo, da je $\varphi^{-1}(N')$ podgrupa, moramo pokazati le, da iz $a \in G$ in $n \in \varphi^{-1}(N')$, tj. $\varphi(n) \in N'$, sledi $ana^{-1} \in \varphi^{-1}(N')$. To pa je res, saj je

$$\varphi(ana^{-1}) = \varphi(a)\varphi(n)\varphi(a)^{-1}$$

in je N' edinka.

(c) Ker je podgrupa H sama grupa in je zožitev φ na H homomorfizem iz H v G', to sledi iz trditve 3.25 (seveda pa zlahka dokažemo tudi neposredno).

(d) Trditev (c) pove, da je $\varphi(N)$ podgrupa. Za vse $a \in G$ in $n \in N$ je $ana^{-1} \in N$ in zato

$$\varphi(a)\varphi(n)\varphi(a)^{-1} = \varphi(ana^{-1}) \in \varphi(N).$$

Ker je preslikava φ surjektivna, to pomeni, da je $\varphi(N)$ edinka. □

Vrnimo se k vprašanju, ki smo si ga zastavili. Naj bo $N \lhd G$. Če je H podgrupa grupe G, ki vsebuje N, potem je očitno N tudi podgrupa edinka grupe H. Zato lahko tvorimo kvocientno grupo H/N. Le-ta pa je podgrupa grupe G/N – to preverimo brez težav, sledi pa tudi iz trditve (c), če za φ izberemo kanonični epimorfizem $\pi : G \to G/N$. Podobno razmislimo, da je za vsako podgrupo edinko M grupe G, ki vsebuje N, grupa M/N podgrupa edinka grupe G/N. Naslednji izrek pove, da smo s tem opisali vse podgrupe oziroma podgrupe edinke grupe G/N.

IZREK 4.19. *Naj bo $N \lhd G$.*

(a) *Vsaka podgrupa grupe G/N je oblike H/N za neko podgrupo H grupe G, ki vsebuje N.*
(b) *Vsaka podgrupa edinka grupe G/N je oblike M/N za neko podgrupo edinko M grupe G, ki vsebuje N.*

DOKAZ. Označimo s π kanonični epimorfizem iz G v G/N.

(a) Naj bo H' podgrupa G/N. Po lemi 4.18 (a) je $H := \pi^{-1}(H')$ podgrupa grupe G. V H so taki elementi $h \in G$, da odsek $\pi(h) = hN$ leži v H'. Seveda je $N \subseteq H$, saj je $nN = N$ za vsak $n \in N$ in je N enota grupe H'. Ker je preslikava π surjektivna, je

$$\pi(\pi^{-1}(H')) = H'.$$

Zapisano drugače,

$$H' = \pi(H) = H/N.$$

(b) Dokaz druge trditve poteka po istem vzorcu. Vzemimo podgrupo edinko N' grupe G/N. Lema 4.18 (b) pove, da je $M := \pi^{-1}(N')$ podgrupa edinka grupe G. Seveda je $N \subseteq M$ in $N' = \pi(M) = M/N$. □

Površen povzetek izreka je, da obstaja enostavna zveza med podgrupami (edinkami) grupe G/N in tistimi podgrupami (edinkami) grupe G, ki vsebujejo N. Kvocientna grupa G/N ima torej kvečjemu manj podgrup (edink) kot originalna grupa G in bi tako vsaj načeloma lahko bila lažje obvladljiva.

Primer 4.20. Kot zgled uporabe izreka 4.19 opišimo podgrupe grupe $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$. Pričnimo z opazko: za poljubno naravno število k je $k\mathbb{Z}_n = \{kx \mid x \in \mathbb{Z}_n\}$ podgrupa $(\mathbb{Z}_n, +)$. Denimo $2\mathbb{Z}_4 = \{0, 2\}$ je prava netrivialna podgrupa grupe $\mathbb{Z}_4$, medtem ko je npr. $3\mathbb{Z}_4 = \mathbb{Z}_4$ in $4\mathbb{Z}_4 = \{0\}$. Trdimo, da vsako podgrupo $\mathbb{Z}_n$ lahko zapišemo kot

$$k\mathbb{Z}_n, \text{ kjer } k \in \mathbb{N} \text{ in } k|n.$$

Ker je vsaka podgrupa grupe $\mathbb{Z}$ oblike $k\mathbb{Z}$ za neki $k \geq 0$ (posledica 2.2), je po izreku 4.19 vsaka podgrupa grupe $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$ oblike $k\mathbb{Z}/n\mathbb{Z}$, kjer je $n\mathbb{Z} \subseteq k\mathbb{Z}$. Kot bo bralec zlahka preveril, je slednje izpolnjeno natanko tedaj, ko k deli n, grupo $k\mathbb{Z}/n\mathbb{Z}$ pa lahko zapišemo kot $k\mathbb{Z}_n$.

Naloge

1. Naj bo a tak element grupe G, da je $a^2 = 1$. Pokaži, da je podgrupa $\langle a \rangle = \{1, a\}$ edinka natanko tedaj, ko a leži v centru grupe G.
2. Ugotovi, katere podgrupe simetrične grupe S_3 so in katere niso edinke.
3. Pokaži, da so vse podgrupe kvaternionske grupe Q edinke.

   Komentar. Torej nimajo le Abelove grupe lastnost, da so vse njihove podgrupe edinke.
4. Katera izmed podgrup $\langle r \rangle$ in $\langle z \rangle$ diedrske grupe D_{2n} je edinka?
5. Pokaži, da je $\mathrm{Inn}(G)$, grupa notranjih avtomorfizmov grupe G, podgrupa edinka grupe vseh avtomorfizmov $\mathrm{Aut}(G)$.
6. Če je c element centra grupe G, je $aca^{-1} = c$ za vsak $a \in G$. Zato je center $Z(G)$, kot tudi vsaka njegova podgrupa, podgrupa edinka grupe G. Pokaži, da grupa $G/Z(G)$ ni ciklična, razen če je G Abelova grupa.
7. Podgrupo edinko grupe G lahko opišemo kot podgrupo N z lastnostjo, da je $\varphi(N) \subseteq N$ za vsak $\varphi \in \mathrm{Inn}(G)$. Podgrupi $K \leq G$ pravimo **karakteristična podgrupa**, če $\varphi(K) \subseteq K$ velja za vsak $\varphi \in \mathrm{Aut}(G)$. Take podgrupe so torej edinke. Pokaži:

(a) $\{1, -1, i, -i\}$ je podgrupa edinka kvaternionske grupe Q, ni pa njena karakteristična podgrupa.
(b) Za vsako netrivialno grupo G je $G \times \{1\}$ podgrupa edinka grupe $G \times G$, ni pa njena karakteristična podgrupa.
(c) Center $Z(G)$ poljubne grupe G je karakteristična podgrupa.

8. Naj bo $N \leq G$. Pokaži, da iz $[G : N] = 2$ sledi $N \triangleleft G$ in $G/N \cong \mathbb{Z}_2$.

   Namig. Če $a \notin N$, je G disjunktna unija levih odsekov N in aN, in tudi disjunktna unija desnih odsekov N in Na.

9. Naj bo N končna podgrupa grupe G. Denimo, da G ne vsebuje nobene druge podgrupe, ki bi imela isti red kot N. Pokaži, da je potem $N \triangleleft G$.

10. Pokaži, da je $\mathbb{Q}/\mathbb{Z}$ neskončna grupa, v kateri ima vsak element končen red.

11. Naj bo G Abelova grupa. Označimo z N množico vseh elementov iz G, ki imajo končen red. Pokaži, da je N podgrupa G in da je v grupi G/N enota edini element s končnim redom.

12. Naj bo X neprazna podmnožica grupe G. Pokaži, da je podgrupa, generirana z množico $\{gxg^{-1} \mid g \in G, x \in X\}$, enaka podgrupi edinki, generirani z množico X (torej edinki, ki vsebuje X in je vsebovana v vsaki drugi edinki, ki vsebuje X).

13. Pokaži, da lema 4.18 (d) v splošnem ne velja za homomorfizme, ki niso surjektivni.

    Namig. Podgrupa $H \leq G$ morda ni edinka v G, vselej pa je $H \triangleleft H$.

14. Naj bosta H in K taki podgrupi grupe G, da je $HK = H \cup K$. Pokaži, da je potem $H \subseteq K$ ali $K \subseteq H$.

    Komentar. To je inačica naloge 1.6/6.

15. Naj bosta a in b taka elementa grupe G, da je $a^2 = b^2 = 1$ in $ab \neq ba$. Pokaži, da produkt podgrup $H = \{1, a\}$ in $K = \{1, b\}$ ni podgrupa. Poišči še kak konkreten primer grupe s takima elementoma.

16. Produkt podmnožic X in Y grupe G definiramo enako kot produkt podgrup, torej kot $XY := \{xy \mid x \in X, y \in Y\}$. Pokaži, da je produkt odsekov aN in bN tudi po tej definiciji enak $(ab)N$, če je seveda $N \triangleleft G$.

17. Naj bo G poljubna grupa. Podgrupi, generirani z vsemi komutatorji $[a, b]$, kjer sta a in b poljubna elementa iz G, pravimo **komutatorska podgrupa** in jo označujemo z G'. Pokaži:
    (a) G je komutativna natanko tedaj, ko je $G' = \{1\}$.
    (b) Vsak element iz G' se da zapisati kot produkt komutatorjev.
    (c) $G' \triangleleft G$ in grupa G/G' je Abelova.
    (d) Če je $N \triangleleft G$, je grupa G/N Abelova natanko tedaj, ko je $G' \subseteq N$.

Komentar. Grupi G/G' pravimo **abelizacija** grupe G. Če je na primer G nekomutativna enostavna grupa, je G' kot njena edinka lahko enaka samo grupi G sami in zato je abelizacija G/G' trivialna grupa. Ni pa to najbolj značilen primer. Izkaže se, da ima veliko grup lastnost, da se zaporedje podgrup $G \supseteq G' \supseteq (G')' \supseteq \ldots$ izteče s trivialno grupo. Povejmo natančneje: če definiramo $G^{(0)} = G$ in $G^{(i+1)} = (G^{(i)})'$ za vsak $i \geq 0$, je $G^{(n)} = \{1\}$ za neki $n \geq 0$. Taki grupi pravimo **rešljiva grupa**. *William Burnside* je leta 1904 dokazal, da so rešljive vse končne grupe, katerih red je deljiv z največ dvema praštevilom, *Walter Feit* in *John G. Thompson* pa sta leta 1963 dokazala, da so rešljive vse končne grupe z lihim redom. Red končne nekomutativne enostavne grupe je torej nujno sodo število, deljivo z vsaj tremi praštevili. Denimo, red alternirajoče grupe A_5 je $60 = 2^2 \cdot 3 \cdot 5$; izkaže se, da je ta grupa enostavna in da ima izmed vseh nekomutativnih enostavnih grup najmanjši red.

18. Poišči Q', komutatorsko podgrupo kvaternionske grupe Q.
19. Pokaži, da je $S_n' = A_n$ za vse $n \geq 3$.
    Namig. Naloga 2.7/20.

4.3. Ideali in kvocientni kolobarji

V tem razdelku bomo izpeljali podobne rezultate za kolobarje, kot smo jih v prejšnjem razdelku za grupe. Dokazi bodo analogni, v precejšnji meri bomo samo posnemali zgornje razmisleke.

4.3.1. Definicija ideala in kvocientnega kolobarja. Naj bo K kolobar. Če je I njegova podgrupa za seštevanje, postane množica vseh odsekov

$$K/I = \{a + I \mid a \in K\}$$

aditivna grupa za operacijo

$$(a + I) + (b + I) = (a + b) + I.$$

To smo spoznali v prejšnjem razdelku. Seveda pa v kolobarjih ne moremo biti zadovoljni samo s seštevanjem. V aditivni grupi $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$ smo definirali množenje s predpisom $[a] \cdot [b] = [ab]$, ali, zapisano z običajnimi oznakami za odseke,

$$(a + n\mathbb{Z})(b + n\mathbb{Z}) = ab + n\mathbb{Z}.$$

Vprašajmo se torej, kakšna mora biti podgrupa I, da lahko v K/I vpeljemo množenje z naravnim predpisom

$$(a + I)(b + I) := ab + I?$$

Odgovor daje naslednja lema, ki je analogna lemi 4.10 iz prejšnjega razdelka.

LEMA 4.21. *Naj bo I podgrupa za seštevanje kolobarja K. Naslednja pogoja sta ekvivalentna:*

(i) *Za vse $a, a', b, b' \in K$ iz $a + I = a' + I$ in $b + I = b' + I$ sledi $ab + I = a'b' + I$.*
(ii) *Za vse $a \in K$ in $u \in I$ je $au \in I$ in $ua \in I$.*

DOKAZ. Spomnimo se, da sta odseka $a + I$ in $a' + I$ enaka natanko tedaj, ko je $a' - a \in I$. Zato lahko pogoj (i) zapišemo takole:

$$a' - a \in I \ \wedge \ b' - b \in I \implies a'b' - ab \in I. \tag{4.5}$$

(i)⇒(ii). Ker za vsak $a \in K$ in vsak $u \in I$ velja $a - a = 0 \in I$ in $u - 0 = u \in I$, iz (4.5) sledi $au = au - a0 \in I$ in podobno $ua = ua - 0a \in I$.

(ii)⇒(i). Denimo, da za $a, a', b, b' \in K$ velja $u_1 := a' - a \in I$ in $u_2 := b' - b \in I$. Ker je

$$a'b' - ab = (a + u_1)(b + u_2) - ab = u_1 b + a u_2 + u_1 u_2,$$

iz (ii) sledi $a'b' - ab \in I$. Torej (4.5) velja. □

DEFINICIJA 4.22. Naj bo I podgrupa kolobarja K za seštevanje. Če I zadošča pogoju (ii) (in zato tudi (i)) iz leme 4.21, se imenuje **ideal** kolobarja K. V tem primeru pišemo $I \triangleleft K$.

Morda si bo definicijo lažje vtisniti v spomin, če jo zapišemo v zgoščeni obliki:

$$I \triangleleft K \iff I \text{ je podgrupa za seštevanje, } KI \subseteq I \text{ in } IK \subseteq I.$$

Med drugim je torej ideal zaprt za množenje. Vendar pa praviloma ni podkolobar, saj ne vsebuje nujno enote 1 – če jo vsebuje, je pravzaprav enak celemu K (zakaj?).

PRIMER 4.23. Podmnožica kolobarja $\mathbb{Z}$ je ideal natanko tedaj, ko je oblike $n\mathbb{Z}$ za neki $n \in \mathbb{N} \cup \{0\}$. Posledica 2.2 namreč pove, da so množice $n\mathbb{Z}$ edine podgrupe za seštevanje v $\mathbb{Z}$; ker so očitno tudi ideali, so to hkrati edini ideali.

IZREK 4.24. *Naj bo $I \triangleleft K$. Če v množico vseh odsekov K/I vpeljemo seštevanje in množenje s predpisoma*

$$(a + I) + (b + I) = (a + b) + I,$$
$$(a + I)(b + I) = ab + I,$$

postane K/I kolobar. Preslikava $\pi : K \to K/I$, definirana s

$$\pi(a) = a + I$$

je epimorfizem in $\ker \pi = I$.

Dokaz. Iz prejšnjega razdelka vemo, da je K/I aditivna grupa. Množenje je dobro definirano po lemi 4.21. Kot v dokazu izreka 4.13 vidimo, da je asociativno, pa tudi distributivnostna zakona sledita takoj iz distributivnostnih zakonov v K. Enota za množenje je odsek $1 + I$. Torej je K/I kolobar. Iz definicij seštevanja in množenja vidimo, da je preslikava π epimorfizem. V njegovem jedru so tisti elementi $a \in K$, za katere je $a + I = I$. To pa so natanko elementi iz I. □

Definicija 4.25. Kolobarju K/I iz izreka 4.24 pravimo **kvocientni** ali **faktorski kolobar**, preslikavi π pa **kanonični epimorfizem**.

Kot osnovni zgled si oglejmo kolobar celih števil $\mathbb{Z}$. Kot vemo, so vsi njegovi ideali oblike $n\mathbb{Z}$ (primer 4.23), množenje v aditivni grupi $\mathbb{Z}/n\mathbb{Z}$ pa sovpada z množenjem, kot smo ga vpeljali v razdelku 2.2. Torej je

$$\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}_n$$

enakost kolobarjev, ne le aditivnih grup.

Omenimo še očitna primera idealov poljubnega kolobarja K. To sta ničelni ideal $\{0\}$ in cel kolobar K. Več primerov idealov in kvocientnih kolobarjev bomo srečali v naslednjem razdelku.

Trditev 4.15 pravi, da je podmnožica grupe podgrupa edinka natanko tedaj, ko je jedro homomorfizma grup. Analogna trditev velja za kolobarje.

Trditev 4.26. *Podmnožica I kolobarja K je ideal natanko tedaj, ko je I jedro homomorfizma iz kolobarja K v neki kolobar K'.*

Dokaz. Vsak ideal je jedro kanoničnega epimorfizma. Dokazati moramo obratno trditev. Denimo, da je $I = \ker \varphi$ za neki homomorfizem $\varphi : K \to K'$. Če sta $u, v \in I$, je

$$\varphi(u - v) = \varphi(u) - \varphi(v) = 0.$$

Torej je $u - v \in I$. Za vsak $u \in I$ in $a \in K$ je

$$\varphi(au) = \varphi(a)\varphi(u) = \varphi(a)0 = 0$$

in zato $au \in I$. Podobno vidimo, da je tudi $ua \in I$. Torej je I ideal. □

4.3.2. Operacije z ideali. Če sta I in J ideala kolobarja K, sta ideala tudi njun **presek**

$$I \cap J$$

in **vsota**

$$I + J := \{u + v \,|\, u \in I, v \in J\}.$$

Oboje takoj preverimo. Prav tako je ideal njun **produkt** IJ, ki ga definiramo kot podgrupo K za seštevanje, generirano z vsemi elementi oblike uv, $u \in I$, $v \in J$. Torej IJ sestoji iz vseh elementov oblike

$$u_1v_1 + \cdots + u_nv_n,$$

kjer $u_i \in I$ in $v_i \in J$. Tudi dokaze teh dejstev prepuščamo bralcu. Če je kolobar nekomutativen, sta lahko ideala IJ in JI med seboj različna. Oba pa sta, po definiciji ideala, vsebovana tako v I kot v J. Zato velja

$$IJ \subseteq I \cap J \subseteq I \subseteq I + J.$$

PRIMER 4.27. Za ideala $I = 4\mathbb{Z}$ in $J = 6\mathbb{Z}$ kolobarja $\mathbb{Z}$ velja $IJ = 24\mathbb{Z}$, $I \cap J = 12\mathbb{Z}$ in $I + J = 2\mathbb{Z}$. Kaj dobimo, če 4 in 6 zamenjamo s poljubnima številoma m in n? To vprašanje ne bi smelo biti pretežko.

4.3.3. Enostranski ideali in enostavni kolobarji. Naslednji pojem nima analogije v teoriji grup. Podmnožico L kolobarja K imenujemo **levi ideal**, če je podgrupa za seštevanje in če velja $KL \subseteq L$, torej $a\ell \in L$ za vse $a \in K$ in $\ell \in L$. Podobno definiramo **desni ideal**, le pogoj $KL \subseteq L$ zamenjamo s pogojem $LK \subseteq L$. Leve in desne ideale z eno besedo imenujemo **enostranski** ideali. Ideali so seveda hkrati levi in desni ideali. Zato jim včasih rečemo tudi **dvostranski** ideali. V komutativnih kolobarjih med enostranskimi in dvostranskimi ideali očitno ni razlike. V nekomutativnih kolobarjih pa tako eni kot drugi igrajo pomembno vlogo.

PRIMER 4.28. Množica vseh matrik oblike $\left[\begin{smallmatrix} a & 0 \\ b & 0 \end{smallmatrix}\right]$, $a, b \in \mathbb{R}$, je levi ideal kolobarja $M_2(\mathbb{R})$, ki ni desni ideal. Podobno je množica vseh matrik oblike $\left[\begin{smallmatrix} a & b \\ 0 & 0 \end{smallmatrix}\right]$ desni ideal, ki ni levi ideal.

Naslednji trditvi bomo formulirali za leve ideale. Iz dokazov je očitno, da veljata tudi za desne ideale.

TRDITEV 4.29. *Če levi ideal L kolobarja K vsebuje kak obrnljiv element, je $L = K$.*

DOKAZ. Označimo obrnljiv element iz L z ℓ. Potem je $1 = \ell^{-1}\ell \in KL \subseteq L$ in zato tudi $a = a1 \in KL \subseteq L$ za vsak $a \in K$. □

TRDITEV 4.30. *Neničeln kolobar K je obseg natanko tedaj, ko sta $\{0\}$ in K njegova edina leva ideala.*

DOKAZ. Naj bo K obseg in $L \neq K$ njegov levi ideal. Ker je vsak neničeln element iz K obrnljiv, je po prejšnji trditvi L lahko enak le $\{0\}$.

Za dokaz obratne trditve privzemimo, da sta $\{0\}$ in K edina leva ideala kolobarja K. Vzemimo $a \neq 0$ iz K in pokažimo, da je obrnljiv. Množica

$$Ka := \{xa \mid x \in K\}$$

je očitno levi ideal. Ker vsebuje $a\,(= 1a)$ in zato ni enak $\{0\}$, je $Ka = K$. Od tod sledi, da obstaja tak $b \in K$, da je $ba = 1$. Tudi b ni enak 0, zato za levi ideal Kb velja enak zaključek, torej $Kb = K$ in zato $cb = 1$ za neki $c \in K$. Ker pa je levi inverz vselej enak desnemu (trditev 1.26), sta elementa c in a enaka. Torej je $ab = ba = 1$, kar pomeni, da je element a obrnljiv. □

Neničeln kolobar K se imenuje **enostaven kolobar**, če sta $\{0\}$ in K njegova edina ideala. Iz trditve 4.30 sledi, da so obsegi enostavni kolobarji. Ni pa vsak enostaven kolobar obseg. Denimo, tudi kolobar $n \times n$ matrik nad obsegom je, kot se izkaže, enostaven, pa ni obseg. V komutativnih kolobarjih pa pojma obseg, torej v tem primeru polje, in enostaven kolobar sovpadata. To namreč sledi iz trditve 4.30. Zapišimo ta rezultat.

Posledica 4.31. *Komutativen kolobar K je enostaven natanko tedaj, ko je polje.*

4.3.4. Ideali kvocientnega kolobarja in maksimalni ideali. V razdelku 4.2 smo opisali podgrupe in podgrupe edinke kvocientne grupe G/N. Podobno lahko opišemo podkolobarje in ideale kvocientnega kolobarja K/I. Omejimo se le na opis idealov. V dokazu naslednje leme in izreka moramo samo slediti dokazoma leme 4.18 in izreka 4.19 in narediti nekaj očitnih prilagoditev. Podrobnosti prepuščamo bralcu kot koristno vajo, iz katere se bo naučil več, kot bi se iz branja dokaza.

Lema 4.32. *Naj bo $\varphi : K \to K'$ homomorfizem kolobarjev.*
(a) *Če je $I' \lhd K'$, je $\varphi^{-1}(I') \lhd K$.*
(b) *Če je $I \lhd K$ in je φ epimorfizem, je $\varphi(I) \lhd K'$.*

Izrek 4.33. *Naj bo $I \lhd K$. Vsak ideal kolobarja K/I je oblike J/I za neki ideal J kolobarja K, ki vsebuje I.*

Primer 4.34. Vse podgrupe aditivne grupe $\mathbb{Z}_n$ so oblike $k\mathbb{Z}_n$, kjer $k \mid n$ (primer 4.20). Vsaka izmed njih je tudi ideal kolobarja $\mathbb{Z}_n$, torej so te množice tudi edini ideali kolobarja $\mathbb{Z}_n$. To lahko izpeljemo tudi iz izreka 4.33.

Seveda velja tudi obrat izreka 4.33, tj. J/I je ideal K/I za vsak ideal J, ki vsebuje I. Če z izjemo I in K takih idealov J sploh ni, izrek dobi izredno enostavno obliko. Idealom s to lastnostjo najprej dajmo ime.

Definicija 4.35. Idealu I kolobarja K pravimo **maksimalen ideal**, če $I \neq K$ in če *ne* obstaja tak ideal J, da bi veljalo $I \subsetneq J \subsetneq K$.

Denimo, $2\mathbb{Z}$ je maksimalen ideal kolobarja $\mathbb{Z}$. Če namreč neki ideal kolobarja $\mathbb{Z}$ poleg vseh sodih števil vsebuje še kako liho število, je enak celemu kolobarju $\mathbb{Z}$ (zakaj?). Več primerov bomo spoznali v naslednjem razdelku.

Posledica 4.36. *Ideal I kolobarja K je maksimalen natanko tedaj, ko je kvocientni kolobar K/I enostaven.*

Dokaz. Če je I maksimalen, potem K/I ni ničelni kolobar (saj $I \neq K$) in po izreku 4.33 kolobar K/I nima drugih idealov kot I/I (torej $\{0\}$) in K/I. To pomeni, da je K/I enostaven kolobar. Obratno, če I ni maksimalen, potem obstaja tak ideal J, da je $I \subsetneq J \subsetneq K$. Tedaj je J/I ideal K/I, ki ni enak $\{0\}$ ali K/I. Zato kolobar K/I ni enostaven. □

Posledica 4.37. *Ideal I komutativnega kolobarja K je maksimalen natanko tedaj, ko je kvocientni kolobar K/I polje.*

Dokaz. Seveda je tudi kvocientni kolobar K/I komutativen. Zato ta posledica sledi iz posledic 4.31 in 4.36. □

V komutativnih kolobarjih torej maksimalni ideali porodijo polja. To se bo izkazalo za pomembno pri študiju razširitev polj.

Omenimo še izrek A.2 iz dodatka, ki pravi, da je vsak *pravi ideal* kolobarja – tj. ideal, ki ni enak celemu kolobarju – vsebovan v kakem maksimalnem idealu. Dokaz izreka sloni na Zornovi lemi.

4.3.5. Kvocientni prostori in algebre. Ideal algebre definiramo enako kot ideal kolobarja. Ker je za vsak skalar λ in element u iz ideala algebre tudi $\lambda u = \lambda(1u) = (\lambda 1)u$ element iz ideala, je ideal podprostor. Kako definiramo kvocientno algebro? Še prej moramo odgovoriti na vprašanje, kako definiramo kvocientni vektorski prostor. Na obe vprašanji sta odgovora taka, kot bi ju zdaj že morali pričakovati.

Izrek 4.38. *Naj bo U podprostor vektorskega prostora V. Če v množico vseh odsekov V/U vpeljemo seštevanje in množenje s skalarji s predpisoma*

$$(v+U)+(w+U) = (v+w)+U,$$
$$\lambda(v+U) = \lambda v + U,$$

postane V/U vektorski prostor. Preslikava $\pi : V \to V/U$, definirana s

$$\pi(v) = v + U$$

je epimorfizem in $\ker \pi = U$.

Dokaz. Kot vemo, je V/U aditivna grupa. Pokažimo, da je množenje s skalarji dobro definirano. Denimo, da je $v+U = v'+U$. Potem je $v - v' \in U$. Ker je U podprostor, je tudi

$$\lambda v - \lambda v' = \lambda(v - v') \in U$$

za vsak skalar λ. To pomeni, da je $\lambda v + U = \lambda v' + U$, kar smo želeli dokazati. Z računom zlahka preverimo, da so v V/U izpolnjeni aksiomi vektorskega prostora. Tudi o lastnostih epimorfizma π razmislimo brez težav. □

Vektorskemu prostoru V/U seveda pravimo **kvocientni** ali **faktorski vektorski prostor**, preslikavi π pa kanonični epimorfizem. V zadnjem izreku vpeljimo še **kvocientno** ali **faktorsko algebro** skupaj z ustreznim kanoničnim epimorfizmom.

IZREK 4.39. *Naj bo I ideal algebre A. Če v množico vseh odsekov A/I vpeljemo seštevanje, množenje in množenje s skalarji s predpisi*

$$\begin{aligned}(a+I)+(b+I) &= (a+b)+I,\\ (a+I)(b+I) &= ab+I,\\ \lambda(a+I) &= \lambda a+I,\end{aligned}$$

postane A/I algebra. Preslikava $\pi : A \to A/I$, definirana s

$$\pi(a) = a + I$$

je epimorfizem in $\ker \pi = I$.

DOKAZ. V luči izrekov 4.24 in 4.38 moramo dokazati le, da v A/I velja enakost $\lambda(xy) = (\lambda x)y = x(\lambda y)$. To pa zlahka preverimo. □

Naloge

1. Naj bo X neprazna podmnožica kolobarja K. Pokaži, da je množica vseh elementov oblike

   $$k_1x_1\ell_1 + k_2x_2\ell_2 + \cdots + k_nx_n\ell_n,$$

   kjer so $k_i, \ell_i \in K$ in $x_i \in X$, ideal, generiran z množico X (torej ideal kolobarja K, ki vsebuje X in je vsebovan v vsakem drugem idealu, ki vsebuje X).

   Komentar. Če je K komutativen, se ta opis seveda poenostavi (elemente ℓ_i lahko izpustimo). Tako je tedaj ideal, generiran z enim samim elementom x, enak kar množici vseh elementov oblike kx, $k \in K$. Označujemo ga z (x) in mu pravimo *glavni ideal*. Taki ideali bodo igrali pomembno vlogo v šestem poglavju.

2. V kolobarjih komutator definiramo drugače kot v grupah, čeprav ga označujemo enako. **Komutator** elementov x in y kolobarja K je element

   $$[x, y] := xy - yx.$$

   Označimo s C_K ideal, generiran z vsemi komutatorji $[x, y]$ kolobarja K. Pokaži, da je kvocientni kolobar K/C_K komutativen in da je C_K vsebovan v vsakem idealu I z lastnostjo, da je kolobar K/I komutativen. Opiši C_K v primeru, ko je K kolobar vseh zgoraj trikotnih $n \times n$ realnih matrik.

3. Pokaži, da je kolobar K enostaven natanko tedaj, ko za vsak $a \neq 0$ iz K obstajajo taki $x_i, y_i \in K$, $i = 1, \ldots, n$, da je $\sum_{i=1}^{n} x_i a y_i = 1$.

4. Pojasni, zakaj je neničeln homomorfizem iz enostavnega kolobarja v katerikoli kolobar vselej injektiven.

   Komentar. Kot poseben primer je tako homomorfizem polj vedno injektiven.

5. Naj bo O obseg. Pokaži, da je kolobar $M_n(O)$ enostaven.

   Nasvet. Pomagaj si z **matričnimi enotami**. To so matrike E_{ij}, ki imajo člen na križišču i-te vrstice in j-tega stolpca enak 1, vse druge člene pa enake 0. Posebej koristna je formula

   $$E_{ij}AE_{kl} = a_{jk}E_{il},$$

   ki velja za vsako matriko $A = (a_{ij})$.

6. Pokaži, da je center enostavnega kolobarja polje.

7. Naj bodo $I_1, \ldots, I_r$ taki ideali kolobarja K, da je $I_i + I_j = K$ za vse $i \neq j$. Pokaži, da je s predpisom

   $$\varphi(a) = (a + I_1, \ldots, a + I_r)$$

   definiran epimorfizem iz K v $K/I_1 \times \cdots \times K/I_r$ z jedrom $I_1 \cap \cdots \cap I_r$.

   Navodilo. Najprej preveri, da je φ homomorfizem in da je $I_1 \cap \cdots \cap I_r$ njegovo jedro. Preostane dokaz surjektivnosti φ. Ker je $I_1 + I_i = K$, $i \geq 2$, je $v_i + u_i = 1$ za neka $v_i \in I_1$ in $u_i \in I_i$. Zato je

   $$1 = (v_2 + u_2) \cdots (v_r + u_r) = v + u_2 \cdots u_r,$$

   kjer je $v \in I_1$, kar da $\varphi(u_2 \cdots u_r) = (1, 0, \ldots, 0)$ (tu 1 označuje enoto kolobarja K/I_1, torej odsek $1 + I_1$, 0 pa ničlo kolobarja K/I_j, torej odsek I_j). Podobno vidimo, da $\operatorname{im}\varphi$ vsebuje vse elemente oblike $(0, \ldots, 0, 1, 0, \ldots, 0)$. Od tod izpelji, da je φ surjektiven.

8. Poišči kak tak $x \in \mathbb{Z}$, da je

   $$x \equiv 2 \pmod 3, \;\; x \equiv 1 \pmod 4, \;\; x \equiv 3 \pmod 7.$$

   Ta naloga gotovo ni težka. Če ne drugače, jo rešimo s poskušanjem. Vsak tovrsten sistem enačb pa nima rešitve. Na primer, iz posledice 2.5 hitro sledi, da celo število x z lastnostjo

   $$x \equiv 1 \pmod{n_1} \text{ in } x \equiv 0 \pmod{n_2}$$

   obstaja le tedaj, ko sta si števili n_1 in n_2 tuji. Kaj velja v splošnem? Pokaži, da do odgovora vodi ugotovitev prejšnje naloge, če za K izberemo kolobar $\mathbb{Z}$. Natančneje, pokaži, da za vsaka paroma tuja si naravna števila $n_1, \ldots, n_r$ in poljubna cela števila $a_1, \ldots, a_r$ obstaja tako celo število x, da je

   $$x \equiv a_i \pmod{n_i} \text{ za vse } i = 1, \ldots, r.$$

Če je tudi $y \in \mathbb{Z}$ rešitev tega sistema enačb, je

$$x \equiv y \pmod{n_1 \cdots n_r}.$$

Komentar. To je klasičen rezultat teorije števil. Imenuje se **kitajski izrek o ostankih**. Kitajski matematiki so ga namreč v neki obliki poznali že pred skoraj dvema tisočletjema.

9. Ali ima kolobar $\mathbb{C}[X]/(X^2+1)$ delitelje niča?

   Pojasnilo. Z $(f(X))$ označujemo ideal, generiran s polinomom $f(X)$ (gl. nalogo 1).

10. Ali ima kolobar $\mathbb{R}[X]/(X^2+1)$ delitelje niča? Ali je izomorfen kolobarju $\mathbb{R}[X]/(X^2-1)$?

11. Poišči produkt, presek in vsoto idealov (X^2+X) in (X^2-X) kolobarja $\mathbb{R}[X]$.

12. Pokaži, da sta množici $I = \{f \in C(\mathbb{R}) \mid f(x) = 0 \text{ za vse } x < 0\}$ in $J = \{f \in C(\mathbb{R}) \mid f(x) = 0 \text{ za vse } x > 0\}$ ideala kolobarja zveznih funkcij $C(\mathbb{R})$ in da je $IJ = I \cap J = \{0\}$ ter $I + J = \{f \in C(\mathbb{R}) \mid f(0) = 0\}$.

13. Naj bosta I in J taka ideala komutativnega kolobarja K, da je $K = I + J$. Pokaži, da je $IJ = I \cap J$.

14. Naj bosta K_1 in K_2 poljubna kolobarja. Pokaži, da je vsak ideal direktnega produkta $K_1 \times K_2$ oblike $I_1 \times I_2$, kjer je I_1 ideal K_1 in I_2 ideal K_2.

    Komentar. Podgrupe edinke direktnega produkta grup $G_1 \times G_2$ niso nujno oblike $N_1 \times N_2$, kjer je N_1 edinka G_1 in N_2 edinka G_2. Denimo, za vsako grupo G je množica $\{(x, x) \mid x \in G\}$ je podgrupa grupe $G \times G$. Če je G Abelova, je seveda edinka.

15. Poišči vse ideale kolobarja $\mathbb{R} \times \mathbb{R} \times \mathbb{R}$. Kateri izmed njih so maksimalni?

16. Naj bo I množica vseh elementov neničelnega komutativnega kolobarja K, ki niso obrnljivi. Denimo, da je I zaprta za seštevanje. Pokaži, da je potem I ideal K in da je kolobar K/I polje (ali ekvivalentno, I je maksimalen ideal). Poišči kak konkreten primer takega kolobarja K, ki ni polje (npr. med kolobarji $\mathbb{Z}_n$).

17. Naj bo a element kolobarja K. Pokaži, da je množica $L = \{x \in K \mid xa = 0\}$ levi ideal K, množica $D = \{x \in K \mid ax = 0\}$ pa desni ideal K. S primerom pokaži (npr. v kolobarju $K = M_2(\mathbb{R})$), da $L \cap D$ ni nujno niti levi niti desni ideal.

18. Naj bo $L \neq \{0\}$ levi ideal in $D \neq \{0\}$ desni ideal kolobarja $M_2(\mathbb{R})$. Pokaži, da $d\ell = 0$ ne more veljati za vse $\ell \in L$, $d \in D$ in poišči primer, ko je $\ell d = 0$ za vse $\ell \in L$, $d \in D$.

19. Za (enostranski ali dvostranski) ideal I kolobarja K pravimo, da je **nilpotenten**, če obstaja tak $n \in \mathbb{N}$, da je $u_1 \cdots u_n = 0$ za vse $u_i \in I$. Pokaži, da je množica vseh strogo zgoraj trikotnih $n \times n$ realnih matrik nilpotenten ideal kolobarja zgoraj trikotnih $n \times n$ realnih matrik, ki vsebuje vse druge nilpotentne ideale tega kolobarja.
20. Pokaži, da je množica vseh nilpotentnih elementov komutativnega kolobarja ideal. S primerom pokaži, da za nekomutativne kolobarje to v splošnem ne velja.
21. Pokaži, da je vsota dveh nilpotentnih idealov nilpotenten ideal.
22. Ena izmed naslednjih izjav je pravilna in dokaz ni posebej težek. Druga izjava se imenuje **Köthejeva domneva**. Vprašanje, ali je pravilna ali ne, je odprto že od leta 1930. Ugotovi, katera je katera.
    (a) Če kolobar K vsebuje neničeln levi ideal, v katerem je vsak element nilpotenten, potem vsebuje tudi neničeln (dvostranski) ideal, v katerem je vsak element nilpotenten.
    (b) Če kolobar K vsebuje neničeln nilpotenten levi ideal, potem vsebuje tudi neničeln nilpotenten dvostranski ideal.

4.4. Izrek o izomorfizmu in primeri kvocientnih struktur

O pomenu izomorfizmov in vložitev smo že veliko govorili. Potrebujemo jih zato, da lahko identificiramo na pogled različne algebraične objekte oziroma zato, da lahko ene objekte vidimo znotraj drugih. Kaj pa je pomen homomorfizmov, ki niso injektivni?

4.4.1. Izrek o izomorfizmu. Naslednji izrek pove, da vsak homomorfizem porodi izomorfizem.

Izrek 4.40. *Naj bo $\varphi : A \to A'$ homomorfizem (grup, kolobarjev, vektorskih prostorov ali algeber). Potem je*

$$A/\ker\varphi \cong \operatorname{im}\varphi.$$

Dokaz. Podrobno obravnavajmo primer, ko je φ homomorfizem grup. Kot vemo, je $\ker\varphi$ podgrupa edinka, zato lahko vpeljemo kvocientno grupo $A/\ker\varphi$. Za poljubna $a, a' \in A$ velja

$$a\ker\varphi = a'\ker\varphi \iff a^{-1}a' \in \ker\varphi \iff \varphi(a^{-1}a') = 1 \iff \varphi(a) = \varphi(a').$$

Od tod sledi, da je preslikava $\overline{\varphi} : A/\ker\varphi \to \operatorname{im}\varphi$,

$$\overline{\varphi}(a\ker\varphi) = \varphi(a)$$

dobro definirana (iz $a \ker \varphi = a' \ker \varphi$ sledi $\varphi(a) = \varphi(a')$) in injektivna (iz $\varphi(a) = \varphi(a')$ sledi $a \ker \varphi = a' \ker \varphi$). Ker je

$$\begin{aligned}\overline{\varphi}(a \ker \varphi \cdot b \ker \varphi) &= \overline{\varphi}((ab) \ker \varphi) = \varphi(ab) \\ &= \varphi(a)\varphi(b) = \overline{\varphi}(a \ker \varphi)\overline{\varphi}(b \ker \varphi),\end{aligned}$$

je $\overline{\varphi}$ homomorfizem. Očitno je tudi surjektiven, zato je izomorfizem.

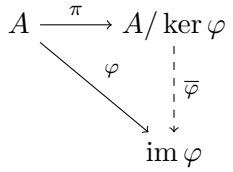
Za homomorfizme kolobarjev, vektorskih prostorov in algeber moramo samo slediti zgornjemu dokazu in ga primerno prikrojiti. Seveda so drugačne oznake, odsek pišemo kot $a + \ker \varphi$ in ne $a \ker \varphi$. Pri tem je $\ker \varphi$ ideal (če je φ homomorfizem kolobarjev ali algeber) oziroma podprostor (če je φ homomorfizem vektorskih prostorov). Vse spremembe, ki jih moramo narediti, pa so povsem očitne. Bralec naj se o tem res prepriča in razmisli o vseh podrobnostih! □

Izrek največkrat uporabljamo v primeru, ko je φ epimorfizem. Zaključek se takrat glasi

$$A/\ker \varphi \cong A'.$$

Izreku 4.40 bomo rekli **izrek o izomorfizmu**. V literaturi ga sicer večkrat srečamo pod imenom **prvi izrek o izomorfizmu**. Poznamo namreč še dva izreka s tem imenom, ki pa smo ju uvrstili med naloge. Izreki o izomorfizmu se v literaturi pogosto imenujejo po nemški matematičarki *Emmy Noether* (1882–1935), ki je imela izjemen vpliv na razvoj algebre.

Dokaz izreka 4.40 je eden tistih, ki si jih velja posebej dobro zapomniti. Pri takih dokazih ne gre samo za preverjanje pomembnih dejstev, ampak so del osnovnega razumevanja tematike. Morda si ga najlažje vtisnemo v spomin s pomočjo t. i. **komutativnega diagrama**:



Definicijo izomorfizma $\overline{\varphi}$ namreč lahko povemo tako, da je kompozitum $\overline{\varphi}$ s kanoničnim epimorfizmom π enak danemu homomorfizmu φ. Prav to pa iz diagrama razberemo, če sledimo smeri puščic. V algebri pogosto srečamo bolj zapletene komutativne diagrame z več množicami in preslikavami med njimi.

Če se povrnemo k izhodiščnemu razmišljanju, lahko zdaj rečemo, da se pojem homomorfizma razkrije s pomočjo kvocientnih struktur. Obratno lahko kvocientne strukture opišemo s pomočjo kanoničnih epimorfizmov. V nekaterih ozirih imamo tako lahko pojma homomorfizem in kvocientna struktura za ekvivalentna.

Kot enostaven zgled uporabnosti in učinkovitosti izreka o izomorfizmu si oglejmo alternativen dokaz osnovnega izreka o cikličnih grupah (izreka 3.8).

Primer 4.41. Naj bo G ciklična grupa in naj bo $a \in G$ tak element, da je $G = \langle a \rangle$. Preslikava

$$\varphi : \mathbb{Z} \to G, \;\; \varphi(n) = a^n,$$

je očitno epimorfizem grup. Če ima trivialno jedro, je injektivna in tako izomorfizem. V nasprotnem primeru je $\ker \varphi = n\mathbb{Z}$ za neki $n \in \mathbb{N}$ (posledica 2.2). Po izreku 4.40 je

$$\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z} \cong \operatorname{im} \varphi = G,$$

s čimer je izrek 3.8 dokazan. Dokaz je precej krajši od dokaza iz razdelka 3.1. Na izrek o izomorfizmu se moramo navaditi, potem je marsikaj laže.

V nadaljevanju si bomo ogledali konkretne primere podgrup edink in idealov ter pripadajočih kvocientnih struktur. Pri opisu slednjih si bomo v znatni meri pomagali z izrekom o izomorfizmu.

4.4.2. Primeri edink in kvocientnih grup. Pričnimo s trivialnim primerom.

Primer 4.42. Naj bo G poljubna grupa. Kot smo že omenili, sta podgrupi $\{1\}$ in G edinki. Za ustrezni kvocientni grupi velja $G/\{1\} \cong G$ in $G/G \cong \{1\}$. To je očitno iz definicije, lahko pa bi uporabili tudi izrek 4.40 za identiteto oziroma trivialni homomorfizem.

Primere 4.3-4.5 si zdaj lahko ogledamo v novi luči. Podgrupe iz vseh treh primerov so namreč edinke. Za prva primera je to očitno, saj obravnavata Abelovi grupi.

Primer 4.43. Naj bo G aditivna grupa $\mathbb{R}^2$, H pa premica $y = 0$, torej $H = \{(x_1, 0) \,|\, x_1 \in \mathbb{R}\}$. Odseki so horizontalne premice. Kako jih seštevamo? Odsek $(x_1, x_2) + H$ lahko zapišemo kot $(0, x_2) + H$, saj je

$$(x_1, x_2) - (0, x_2) = (x_1, 0) \in H.$$

Vsota odsekov $(0, x_2) + H$ in $(0, y_2) + H$ je odsek $(0, x_2 + y_2) + H$. Seštevanje odsekov torej ustreza seštevanju realnih števil x_2 in y_2. Zato uganemo, da je

$$G/H \cong \mathbb{R}.$$

Res, preslikava

$$(x_1, x_2) + H \mapsto x_2$$

je izomorfizem iz grupe G/H v grupo $\mathbb{R}$. O tem se zlahka prepričamo, vendar ne smemo pozabiti na preverjanje dobre definiranosti preslikave. Zato pa izrek 4.40 ponuja bližnjico do istega zaključka. Preslikava

$$\varphi : G \to \mathbb{R}, \quad \varphi(x_1, x_2) = x_2,$$

je epimorfizem aditivnih grup in $\ker\varphi = H$. Zato je po izreku $G/H \cong \mathbb{R}$.

PRIMER 4.44. Opišimo kvocientno grupo $\mathbb{C}^*/\mathbb{T}$. Za vsak $a \in \mathbb{C}^*$ lahko odsek $a\mathbb{T}$ zapišemo kot $|a|\mathbb{T}$, produkt odsekov $|a|\mathbb{T}$ in $|b|\mathbb{T}$ pa je odsek $|a||b|\mathbb{T}$. Množenje primerno zapisanih odsekov torej ustreza množenju pozitivnih realnih števil. To nas napelje k domnevi, da je

$$\mathbb{C}^*/\mathbb{T} \cong \mathbb{R}^+.$$

Res, preslikava $z \mapsto |z|$ je epimorfizem iz $\mathbb{C}^*$ v $\mathbb{R}^+$ in njegovo jedro je $\mathbb{T}$ (gl. primer 3.29), zato želeni zaključek sledi iz izreka 4.40.

PRIMER 4.45. Alternirajoča grupa A_n je podgrupa edinka simetrične grupe S_n. To hitro sledi iz definicije edinke, še hitreje pa iz dejstva, da je A_n jedro epimorfizma $\sigma \mapsto \operatorname{sgn}(\sigma)$ iz S_n v grupo $(\{1,-1\}, \cdot\,)$ (primer 3.31). Od tod tudi sledi, da je

$$S_n/A_n \cong \mathbb{Z}_2. \tag{4.6}$$

Namreč, po izreku 4.40 je $S_n/A_n \cong \{1,-1\}$, grupa $\{1,-1\}$ pa je – kot ciklična grupa reda 2 – izomorfna $\mathbb{Z}_2$. Sicer so si, kot se zlahka prepričamo, vse grupe reda 2 med seboj izomorfne. Zato (4.6) sledi že dejstva, da je $[S_n : A_n] = 2$ (gl. primer 4.5).

PRIMER 4.46. Posebna linearna grupa $\mathrm{SL}_n(F)$ je jedro epimorfizma $A \mapsto \det(A)$ iz splošne linearne grupe $\mathrm{GL}_n(F)$ v grupo $(F^*, \cdot\,)$ (primer 3.32). Zato je

$$\mathrm{GL}_n(F)/\mathrm{SL}_n(F) \cong F^*.$$

PRIMER 4.47. Center $Z(G)$ grupe G je očitno podgrupa edinka. Torej lahko govorimo o kvocientni grupi $G/Z(G)$. Ali je izomorfna kaki grupi, ki smo jo že srečali? V primeru 3.34 smo omenili, da je preslikava $a \mapsto \varphi_a$ epimorfizem iz grupe G v grupo vseh notranjih avtomorfizmov $\mathrm{Inn}(G)$. V jedru te preslikave so tisti $c \in G$, za katere je $\varphi_c = \mathrm{id}_G$, torej elementi c z lastnostjo, da je $cxc^{-1} = x$ za vse $x \in G$. To je očitno izpolnjeno natanko tedaj, ko je $c \in Z(G)$. Po izreku 4.40 je zato

$$G/Z(G) \cong \mathrm{Inn}(G).$$

4.4.3. Primeri idealov in kvocientnih kolobarjev (algeber). Omenimo najprej, da se pri pojmu centra teoriji grup in kolobarjev razideta v naslednjem smislu: center $Z(G)$ nekomutativne grupe G je edinka, center $Z(K)$ nekomutativnega kolobarja K pa ni ideal, saj vsebuje enoto (gl. trditev 4.29). Zdaj pa k primerom idealov in kvocientnih kolobarjev.

PRIMER 4.48. Očitna primera idealov poljubnega kolobarja K sta $\{0\}$ in K. Seveda je $K/\{0\} \cong K$ in $K/K \cong \{0\}$.

PRIMER 4.49. Omenili smo že, da je

$$\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}_n$$

za vsak $n \in \mathbb{N}$. Definiciji kolobarjev $\mathbb{Z}/n\mathbb{Z}$ in $\mathbb{Z}_n$ se namreč ujemata, čeprav zaradi različnih oznak to na prvi pogled ni očitno.

Kot zanimivost še tole. V primeru 3.36 smo omenili, da je preslikava $\varphi : \mathbb{Z} \to \mathbb{Z}_n$, defnirana s $\varphi(a) = [a]$, epimorfizem kolobarjev. Kaj je pravzaprav φ? Nič drugega kot kanonični epimorfizem iz $\mathbb{Z}$ v $\mathbb{Z}/n\mathbb{Z}$.

Kot vemo, je kolobar ostankov $\mathbb{Z}_p$ polje natanko tedaj, ko je p praštevilo (gl. trditev 2.15). To lahko zdaj povežemo s posledico 4.37. Za naravno število p so torej naslednje trditve ekvivalentne:

(i) p je praštevilo.
(ii) Kolobar $\mathbb{Z}_p\,(= \mathbb{Z}/p\mathbb{Z})$ je polje.
(iii) $p\mathbb{Z}$ je maksimalen ideal kolobarja $\mathbb{Z}$.

V naslednjih dveh primerih bomo ugotovitve iz primerov 3.37 in 3.38 interpretirali s pomočjo izreka 4.40.

PRIMER 4.50. Naj bo K poljuben kolobar. Z $XK[X]$ označimo množico vseh polinomov iz $K[X]$ s konstantnim členom 0. Potem je $XK[X]$ ideal $K[X]$ in

$$K[X]/XK[X] \cong K.$$

Če je K polje, je po posledici 4.37 ideal $XK[X]$ maksimalen.

PRIMER 4.51. Izberimo točko x iz intervala $[0, 1]$. Množica

$$I_x := \{f \in C[0,1] \mid f(x) = 0\}$$

je ideal kolobarja (oz. algebre) $C[0, 1]$ in

$$C[0,1]/I_x \cong \mathbb{R}.$$

Po posledici 4.37 je torej I_x maksimalen ideal.

PRIMER 4.52. Naj bo A končno generirana komutativna algebra nad poljem F. Če je $\{a_1, \ldots, a_n\}$ množica njenih generatorjev, je torej vsak element iz A linearna kombinacija izrazov oblike $a_1^{k_1} \cdots a_n^{k_n}$, $k_i \geq 0$. To lahko povemo tudi takole: vsak element iz A je oblike

$$f(a_1, \ldots, a_n), \text{ kjer je } f(X_1, \ldots, X_n) \in F[X_1, \ldots, X_n].$$

Tu seveda $f(a_1, \ldots, a_n)$ označuje vrednost polinoma v n-terici $(a_1, \ldots, a_n)$. Preslikava

$$\varphi : F[X_1, \ldots, X_n] \to A, \quad \varphi(f(X_1, \ldots, X_n)) = f(a_1, \ldots, a_n)$$

je torej surjektivna. Hitro se prepričamo, da je φ homomorfizem algeber. Njegovo jedro I je ideal. Po izreku 4.40 je

$$F[X_1, \ldots, X_n]/I \cong A.$$

Vsaka komutativna algebra, generirana z n elementi, je torej izomorfna kvocientni algebri algebre polinomov v n spremenljivkah z nekim njenim idealom.

Končno generiranost smo privzeli predvsem zaradi lažje razlage. Lahko govorimo tudi o algebri polinomov v neskončno spremenljivkah, le vsak posamezen polinom je odvisen le od končnega števila spremenljivk. Na enak način kot zgoraj razmislimo, da je *vsaka* komutativna algebra izomorfna kvocientni algebri algebre polinomov z nekim njenim idealom.

V teoriji komutativnih algeber ima torej algebra polinomov posebno vlogo. V teoriji splošnih, torej lahko tudi nekomutativnih algeber ima podobno vlogo **prosta algebra**, tj. algebra *nekomutativnih* polinomov. Le-te definiramo podobno kot običajne polinome, le da spremenljivke X_i med seboj ne komutirajo. Natančna definicija bi vzela preveč prostora. Upamo, da si tudi brez nje bralec lahko ustvari predstavo. Vsaka algebra je izomorfna kvocientni algebri proste algebre z nekim njenim idealom. V dokazu samo primerno prikrojimo zgornji razmislek o komutativnih algebrah. Podobno je vsaka grupa izomorfna kvocientni grupi **proste grupe** z neko njeno podgrupo edinko. Tudi strogi definiciji proste grupe se izognimo. Poskusimo predstaviti samo osnovno idejo. Da se ne izgubimo v oznakah, se omejimo na prosto grupo v dveh generatorjih. Označimo ju z x in y. Prosta grupa sestoji iz t. i. **besed**. To so formalni izrazi, ki jih pišemo kot zaporedja potenc x in y z neničelnimi celoštevilskimi eksponenti, denimo

$$x,\ xy,\ x^2y^{-1}x,\ y^{-4}x^{-2}y^3xy^{-1} \text{ ipd.}$$

Tem izrazom priključimo še enoto 1 (imenujemo jo tudi prazna beseda). Množenje besed definiramo na samoumeven način. Tako je denimo

$$x^3y^{-2} \cdot x^{-3}y = x^3y^{-2}x^{-3}y$$

in

$$yx^5y^{-2}x \cdot x^{-1}y^2x^{-2} = yx^3.$$

S tem res dobimo grupo.

Razumevanje prejšnjega odstavka ni ključno za nadaljevanje. Napisano je bilo v upanju, da bodo radovednejši bralci o podrobnostih razmislili sami ali pa poiskali dodatno literaturo.

Naloge

1. Naj bo G grupa vseh nekonstantnih linearnih funkcij (gl. nalogo 1.3/4). Označimo z N njeno podmnožico, ki sestoji iz vseh funkcij oblike $f(x) = x + b$, kjer je $b \in \mathbb{R}$. Pokaži, da je $N \triangleleft G$ in da je $G/N \cong \mathbb{R}^*$.
2. Pokaži, da je $\mathbb{R}/\mathbb{Z} \cong \mathbb{T}$.

   Namig. $\varphi(x) = \cos 2\pi x + i \sin 2\pi x$.

3. Kateri znani grupi je izomorfna grupa $\mathbb{R}^*/\{1,-1\}$?
4. Kateri znani grupi je izomorfna grupa $\mathbb{R}^*/\mathbb{R}^+$?
5. Kateri znani grupi je izomorfna grupa $\mathbb{C}^*/\mathbb{R}^+$?
6. Kateri znani grupi je izomorfna grupa U_n/SU_n?

   Namig. Kakšno število je determinanta unitarne matrike?
7. Preveri, da je množica matrik $G = \left\{ \left[\begin{smallmatrix} 1 & m \\ 0 & 1 \end{smallmatrix}\right] \mid m \in \mathbb{Z} \right\}$ Abelova grupa za običajno množenje matrik. Poišči tako podgrupo $N \leq G$, da je $G/N \cong \mathbb{Z}_3$.
8. Poišči tako netrivialno podgrupo N krožne grupe $\mathbb{T}$, da je $\mathbb{T}/N \cong \mathbb{T}$.

   Namig. Če je φ surjektiven endomorfizem grupe G, je $G/\ker\varphi \cong G$.
9. Poišči tako nekomutativno grupo G, da je grupa $\mathrm{Inn}(G)$ Abelova.
10. Naj bo K kolobar brez enote in naj bo $\mathbb{Z} \times K$ kolobar iz naloge 1.4/2. Pokaži, da je množica $I := \{0\} \times K$ njegov ideal in da je $(\mathbb{Z} \times K)/I \cong \mathbb{Z}$.
11. Pokaži, da je množica $I = \{f \in C[0,1] \mid f(0) = f(1) = 0\}$ ideal kolobarja $C[0,1]$ in da je $C[0,1]/I \cong \mathbb{R} \times \mathbb{R}$.
12. Naj bo c kolobar vseh konvergentnih realnih zaporedij (gl. razdelek 2.5) in naj bo c_0 množica vseh realnih zaporedij z limito 0. Pokaži, da je c_0 maksimalen ideal c in da je $c/c_0 \cong \mathbb{R}$.
13. Pokaži, da je kolobar $\mathbb{R}[X]/(X^2)$ izomorfen kolobarju vseh 2×2 matrik oblike $\left[\begin{smallmatrix} a & b \\ 0 & a \end{smallmatrix}\right]$, $a, b \in \mathbb{R}$. (Tu je $(X^2) = \{X^2 f(X) \mid f(X) \in \mathbb{R}[X]\}$.)
14. Pokaži, da je $M_2(2\mathbb{Z})$, množica vseh 2×2 matrik s členi iz $2\mathbb{Z}$, ideal kolobarja $M_2(\mathbb{Z})$ in da je $M_2(\mathbb{Z})/M_2(2\mathbb{Z}) \cong M_2(\mathbb{Z}_2)$. Splošneje, če je I ideal kolobarja K, je $M_n(I)$ ideal kolobarja $M_n(K)$. Kateremu kolobarju je izomorfen kolobar $M_n(K)/M_n(I)$?
15. Pokaži, da je $I = \left\{ \left[\begin{smallmatrix} 0 & k \\ 0 & 0 \end{smallmatrix}\right] \mid k \in \mathbb{Z} \right\}$ ideal kolobarja $K = \left\{ \left[\begin{smallmatrix} n & k \\ 0 & n \end{smallmatrix}\right] \mid n, k \in \mathbb{Z} \right\}$. Kateremu znanemu kolobarju je izomorfen kolobar K/I?
16. Poišči taka ideala I in J kolobarja $K = \left\{ \left[\begin{smallmatrix} m & k \\ 0 & n \end{smallmatrix}\right] \mid m, n, k \in \mathbb{Z} \right\}$, da je $|K/I| = |K/J| = 4$ in $K/I \ncong K/J$.
17. Poišči tak ideal I kolobarja $\mathbb{Z}[X]$, da je $\mathbb{Z}[X]/I \cong \mathbb{Z}_3[X]$.
18. Poišči tak ideal J kolobarja $\mathbb{Z}[X]$, da je $\mathbb{Z}[X]/J \cong \mathbb{Z}_3$.

    Komentar. Ker je $\mathbb{Z}_3$ polje, je J maksimalen ideal.
19. Naj bo U podprostor končno-razsežnega vektorskega prostora V. Pokaži, da je $\dim V/U = \dim V - \dim U$.
20. **(Drugi izrek o izomorfizmu)** Naj bo G grupa, $H \leq G$ in $N \lhd G$. Pokaži, da je $H \cap N \lhd H$, $N \lhd HN$ in da je

$$H/(H \cap N) \cong HN/N.$$

Navodilo. Uporabi (prvi) izrek o izomorfizmu za homomorfizem $\varphi : H \to HN/N$, $\varphi(h) = hN$.

21. Naj bosta U in W podprostora vektorskega prostora V. Pokaži, da je
$$U/(U \cap W) \cong (U + W)/W$$
in zato (gl. nalogo 19)
$$\dim(U + W) + \dim U \cap W = \dim U + \dim W,$$
če je V končno-razsežen.

Komentar. To je drugi izrek o izomorfizmu za vektorske prostore. Dokaže se v bistvu enako kot za grupe. To velja tudi za inačico izreka za kolobarje, ki se glasi takole: če je L podkolobar, I pa ideal kolobarja K, je $L/(L \cap I) \cong (L + I)/I$. Podoben izrek velja za algebre.

22. Naj bo $\varphi : G \to G'$ homomorfizem grup in naj bo N taka podgrupa edinka grupe G, da je $N \subseteq \ker \varphi$. Pokaži, da je s predpisom $\overline{\varphi}(aN) = \varphi(a)$ definiran homomorfizem $\overline{\varphi} : G/N \to G'$ z lastnostima $\operatorname{im} \overline{\varphi} = \operatorname{im} \varphi$ in $\ker \overline{\varphi} = \ker \varphi/N$.

Komentar. To je nekoliko splošnejša inačica izreka o izomorfizmu. Dokaz ni veliko zahtevnejši.

23. **(Tretji izrek o izomorfizmu)** Naj bo G grupa, $M, N \triangleleft G$ in $N \subseteq M$. Pokaži, da je
$$G/M \cong (G/N)/(M/N).$$

Navodilo. Iz zaključka prejšnje naloge sledi, da kanonični epimorfizem $\pi : G \to G/M$ porodi epimorfizem $\overline{\pi} : G/N \to G/M$ s $\ker \overline{\pi} = M/N$. Uporabi osnovni (prvi) izrek za $\overline{\pi}$ in želeni rezultat sledi.

Komentar. Podoben izrek s podobnim dokazom velja tudi za vektorske prostore, kolobarje in algebre (vlogo edink seveda prevzamejo podprostori oziroma ideali).

24. Naj bosta $\varphi : G \to G'$ in $\psi : G \to G''$ homomorfizma grup. Ugotovi, katera izmed naslednjih trditev je pravilna:
   (a) Če je $\ker \varphi = \ker \psi$, potem je $\operatorname{im} \varphi \cong \operatorname{im} \psi$.
   (b) Če je $\operatorname{im} \varphi \cong \operatorname{im} \psi$, potem $\ker \varphi = \ker \psi$.
   Nepravilno trditev ovrži s primerom.

4.5. Zunanji in notranji direktni produkti grup

V razdelku 1.8 smo vpeljali direktne produkte oziroma vsote grup, kolobarjev, vektorskih prostorov in algeber. Pri grupah smo omenili, da jih bolj natančno imenujemo *zunanji* direktni produkti (oziroma, kadar imamo opravka z aditivnimi grupami, zunanje direktne vsote). Zdaj bomo definirali še *notranje* direktne produkte oziroma vsote. Z zunanjimi iz danih objektov

zgradimo novega, z notranjimi pa dani objekt razgradimo na manjše. V bistvu pa obakrat opisujemo isti pojav.

Ponazorimo s primerom. Aditivno grupo $\mathbb{R}^2$ običajno vpeljemo kot *zunanjo* direktno vsoto dveh kopij aditivne grupe $\mathbb{R}$. Torej je grupa $\mathbb{R}^2$ množica $\mathbb{R} \times \mathbb{R}$ opremljena s komponentnim seštevanjem. Možen pa je tudi drugačen pogled. Zamislimo si ravnino v povsem geometrijskem smislu. Če v njej izberemo izhodišče, njene točke identificiramo s krajevnimi vektorji in nato vpeljemo seštevanje na geometrijski način, ta ravnina postane aditivna grupa. Šele sedaj vpeljimo koordinatni sistem, ki omogoča preglednejšo obravnavo. Vsak vektor potem lahko na en sam način zapišemo kot vsoto vektorja iz abscisne osi in vektorja iz ordinatne osi. Temu rečemo, da je ravnina *notranja* direktna vsota abscisne in ordinatne osi. V čem je torej v tem primeru razlika med zunanjo in notranjo direktno vsoto? Samo v pristopu, rezultat je v bistvu enak.

Primeri iz prejšnjega razdelka bi nas lahko napeljali k napačnemu sklepu, da so podgrupe grup praviloma edinke. V nekomutativnih grupah imamo pogosto opravka z »navadnimi« podgrupami, torej takimi, ki niso edinke. Resda pa so pomembni primeri podgrup velikokrat edinke. Tako imamo v zunanjem direktnem produktu $G := G_1 \times G_2$ grup G_1 in G_2 dve edinki, ki nosita vso informacijo o grupi. To sta

$$\widetilde{G}_1 := \{(x_1, 1) \,|\, x_1 \in G_1\} \text{ in } \widetilde{G}_2 := \{(1, x_2) \,|\, x_2 \in G_2\}.$$

Res sta očitno podgrupi. Iz

$$(a_1, a_2)(x_1, 1)(a_1, a_2)^{-1} = (a_1, a_2)(x_1, 1)(a_1^{-1}, a_2^{-1}) = (a_1 x_1 a_1^{-1}, 1) \in \widetilde{G}_1$$

sledi, da je $\widetilde{G}_1$ edinka. Podobno vidimo, da je tudi $\widetilde{G}_2$ edinka.

Podgrupa $\widetilde{G}_1$ se zgolj formalno razlikuje od grupe G_1. Običajno med tema grupama ne ločujemo in jih tudi označujemo enako. Dokler pa vztrajamo pri formalni obravnavi, lahko rečemo le, da je

$$G_1 \cong \widetilde{G}_1 \text{ in } G_2 \cong \widetilde{G}_2.$$

Izomorfizem iz G_1 v $\widetilde{G}_1$ je preslikava $x_1 \mapsto (x_1, 1)$.

Vsak element (x_1, x_2) iz G lahko zapišemo kot produkt $(x_1, 1)(1, x_2)$, torej kot produkt elementa iz $\widetilde{G}_1$ z elementom iz $\widetilde{G}_2$. To pomeni, da je

$$G = \widetilde{G}_1 \widetilde{G}_2,$$

ali z besedami, grupa G je enaka produktu svojih podgrup edink $\widetilde{G}_1$ in $\widetilde{G}_2$ (gl. razdelek 4.2). Njun presek je trivialen, torej

$$\widetilde{G}_1 \cap \widetilde{G}_2 = \{1\}.$$

Ta opažanja lahko posplošimo na direktne produkte več faktorjev. Naj bodo $G_1, \ldots, G_m$ grupe in naj bo

$$G := G_1 \times \cdots \times G_m$$

njihov zunanji direktni produkt. Potem so

$$\widetilde{G}_i := \{(1, \ldots, 1, x_i, 1, \ldots, 1) \mid x_i \in G_i\} \tag{4.7}$$

podgrupe edinke (ki so kot grupe izomorfne grupam G_i), grupa G je enaka njihovemu produktu,

$$G = \widetilde{G}_1 \cdots \widetilde{G}_m,$$

in presek vsake izmed teh edink s produktom ostalih je trivialen,

$$\widetilde{G}_i \cap \left(\widetilde{G}_1 \cdots \widetilde{G}_{i-1}\widetilde{G}_{i+1} \cdots \widetilde{G}_m\right) = \{1\}$$

za vse $i = 1, \ldots, m$. Te lastnosti podgrup edink $\widetilde{G}_i$ zunanjega direktnega produkta bomo uporabili v definiciji notranjega direktnega produkta.

Definicija 4.53. Grupa G je **notranji direktni produkt** svojih podgrup edink $N_1, \ldots, N_m$, če je G njihov produkt, torej

$$G = N_1 \cdots N_m, \tag{4.8}$$

in če je

$$N_i \cap (N_1 \cdots N_{i-1}N_{i+1} \cdots N_m) = \{1\} \tag{4.9}$$

za vse $i = 1, \ldots, m$.

Razmislek pred definicijo lahko povzamemo takole: če je grupa G zunanji direktni produkt grup $G_1, \ldots, G_m$, potem je G notranji direktni produkt podgrup edink $\widetilde{G}_i$, definiranih s (4.7). Poenostavljeno rečeno je torej vsak zunanji direktni produkt tudi notranji. Izrek 4.55 bo povedal, da v bistvu velja tudi obratno. Pred tem pa si poskusimo pojem notranjega direktnega produkta malce razjasniti.

Najprej omenimo, da iz (4.9) sledi $N_i \cap N_j = \{1\}$ za vse $i \neq j$, zato je po trditvi 4.17

$$n_i n_j = n_j n_i \text{ za vse } n_i \in N_i,\ n_j \in N_j,\ i \neq j. \tag{4.10}$$

Seveda ni razloga, da bi elementi iz N_i komutirali med seboj. Komutirajo pa torej z elementi iz drugih podgrup N_j.

Pogoj (4.8) pove, da lahko vsak element iz G zapišemo kot produkt elementov iz $N_1, \ldots, N_m$ na vsaj en način. Pokažimo, da je zaradi pogoja (4.9) ta način en sam, in da je ta lastnost za notranje direktne vsote celo karakteristična.

Trditev 4.54. *Grupa G je notranji direktni produkt svojih podgrup edink $N_1, \ldots, N_m$ natanko tedaj, ko lahko vsak element iz G na en sam način zapišemo kot $n_1 \cdots n_m$, kjer je $n_i \in N_i$.*

Dokaz. Naj bo G notranji direktni produkt podgrup edink $N_1, \ldots, N_m$. Denimo, da je

$$n_1 n_2 \cdots n_m = r_1 r_2 \cdots r_m$$

za neke $n_i, r_i \in N_i$, $i = 1, \ldots, m$. Če pomnožimo to enakost z leve z r_1^{-1} in z desne z $(n_2 \cdots n_m)^{-1}$, dobimo

$$r_1^{-1} n_1 = (r_2 \cdots r_m)(n_2 \cdots n_m)^{-1}.$$

Ker je $N_2 \cdots N_m$ podgrupa (gl. trditev 4.16), torej vsebuje element $r_1^{-1} n_1$. Seveda je ta element vsebovan tudi v N_1. Zato iz (4.9) sledi, da je $n_1 = r_1$. Začetno enakost tako lahko krajšamo z n_1 in dobimo

$$n_2 \cdots n_m = r_2 \cdots r_m.$$

Argument zdaj ponovimo in tako izpeljemo najprej $n_2 = r_2$, zatem $n_3 = r_3$ itd. Zapis elementa v obliki $n_1 n_2 \cdots n_m$ je torej res en sam.

Dokažimo še obratno trditev. Privzemimo torej, da vsak element iz G lahko na en sam način zapišemo v obliki $n_1 \cdots n_m$, kjer je $n_i \in N_i$. Očitno potem velja (4.8), zato moramo dokazati le (4.9). Vzemimo element

$$a \in N_i \cap (N_1 \cdots N_{i-1} N_{i+1} \cdots N_m).$$

Lahko ga zapišemo na dva načina:

$$a = 1 \cdots 1 \cdot n_i \cdot 1 \cdots 1 \quad \text{in} \quad a = n_1 \cdots n_{i-1} \cdot 1 \cdot n_{i+1} \cdots n_m$$

za neke $n_j \in N_j$. Iz predpostavke o enoličnosti zapisa sledi, da so vsi n_j enaki 1. Torej je $a = 1$ in (4.9) velja. □

Naslednji izrek pove, da je razlika med notranjim in zunanjim direktnim produktom nebistvena.

Izrek 4.55. *Če je grupa G notranji direktni produkt svojih podgrup edink $N_1 \ldots, N_m$, potem je G izomorfna njihovemu zunanjemu direktnemu produktu $N_1 \times \cdots \times N_m$.*

Dokaz. Vpeljimo preslikavo $\varphi : N_1 \times \cdots \times N_m \to G$ s predpisom

$$\varphi\big((n_1, \ldots, n_m)\big) = n_1 \cdots n_m.$$

Iz trditve 4.54 sledi, da je φ bijektivna. Pokažimo, da je homomorfizem. Vzemimo poljubne $n_i, r_i \in N_i$ in si oglejmo element

$$u := \varphi\big((n_1, \ldots, n_m) \cdot (r_1, \ldots, r_m)\big).$$

Dokazati moramo, da je u enak

$$\varphi\big((n_1, \ldots, n_m)\big) \cdot \varphi\big((r_1, \ldots, r_m)\big) = n_1 \cdots n_m r_1 \cdots r_m.$$

Ker je

$$(n_1, \ldots, n_m) \cdot (r_1, \ldots, r_m) = (n_1 r_1, \ldots, n_m r_m),$$

je u po definiciji preslikave φ enak

$$u = n_1 r_1 n_2 r_2 n_3 r_3 \cdots n_m r_m.$$

Iz (4.10) sledi, da n_2 komutira z r_1, n_3 komutira z r_2 in r_1, itn. S tem pridemo do želenega zapisa $u = n_1 \cdots n_m r_1 \cdots r_m$. □

Notranji direktni produkt označujemo enako kot zunanji, torej kot $N_1 \times \cdots \times N_m$. Pravzaprav med zunanjim in notranjim direktnim produktom pogosto sploh ne ločimo in tako pridevnika »zunanji« oziroma »notranji« izpuščamo.

Največkrat se srečamo s primerom, ko je $m = 2$. Pogoja iz definicije se tedaj glasita $G = N_1 N_2$ in $N_1 \cap N_2 = \{1\}$. Po trditvi 4.54 lahko ta pogoja nadomestimo s pogojem, da lahko vsak element iz G na en sam način zapišemo v obliki $n_1 n_2$, kjer je $n_1 \in N_1$ in $n_2 \in N_2$. Preslikava $\varphi : G \to N_2$, $\varphi(n_1 n_2) = n_2$, je zato dobro definirana. S pomočjo (4.10) se takoj prepričamo, da je φ epimorfizem. Ker je očitno $\ker \varphi = N_1$, iz izreka o izomorfizmu sledi

$$G/N_1 \cong N_2. \tag{4.11}$$

Seveda velja tudi $G/N_2 \cong N_1$.

Oglejmo si nekaj primerov. Prvi je trivialen.

Primer 4.56. Vsaka grupa G je notranji direktni produkt svojih edink G in $\{1\}$.

Primer 4.57. Diedrska grupa D_4 sestoji iz elementov $1, r, z, rz$. Ob tem velja $r^2 = z^2 = 1$ in $rz = zr$. Očitno je D_4 notranji direktni produkt svojih (cikličnih) podgrup $N_1 = \{1, r\}$ in $N_2 = \{1, z\}$. (Grupa D_4 je Abelova in zato za njene podgrupe ne omenjamo posebej, da so edinke.)

Primer 4.58. Grupa neničelnih kompleksnih števil $\mathbb{C}^*$ je notranji direktni produkt svojih podgrup $\mathbb{R}^+ = \{r \in \mathbb{R} \mid r > 0\}$ in $\mathbb{T} = \{z \in \mid |z| = 1\}$. Vsak $z \in \mathbb{C}^*$ namreč lahko zapišemo kot produkt števil $|z| \in \mathbb{R}^+$ in $\frac{z}{|z|} \in \mathbb{T}$, očitno pa velja tudi $\mathbb{R}^+ \cap \mathbb{T} = \{1\}$. Iz (4.11) sledi

$$\mathbb{C}^*/\mathbb{T} \cong \mathbb{R}^+,$$

kar smo že pokazali v primeru 4.44. Podobno velja tudi

$$\mathbb{C}^*/\mathbb{R}^+ \cong \mathbb{T}.$$

Primer 4.59. Posebna linearna grupa $\mathrm{SL}_n(F)$ je podgrupa edinka splošne linearne grupe $\mathrm{GL}_n(F)$ (primer 4.46). Ni se težko prepričati, da center Z grupe $\mathrm{GL}_n(F)$, ki je seveda tudi edinka, sestoji iz vseh skalarnih matrik λI, $\lambda \in F^*$. Pokažimo, da je v primeru, ko je $x \mapsto x^n$ bijektivna preslikava iz F v F (npr. ko je $F = \mathbb{R}$ in je n liho število), grupa $\mathrm{GL}_n(F)$ njun notranji direktni produkt. Vzemimo $A \in \mathrm{GL}_n(F)$. Po predpostavki obstaja tak $\lambda \in F^*$, da je $\lambda^n = \det(A)$. Determinanta matrike $\lambda^{-1} A$ je potem enaka 1, torej je

$\lambda^{-1}A \in \mathrm{SL}_n(F)$. Iz zapisa $A = \lambda I \cdot \lambda^{-1}A$ tako sledi, da je grupa $\mathrm{GL}_n(F)$ enaka produktu Z in $\mathrm{SL}_n(F)$. Skalarna matrika λI leži v $\mathrm{SL}_n(F)$ natanko tedaj, ko je $\lambda^n = 1$. Ker je preslikava $x \mapsto x^n$ injektivna, je to izpolnjeno le za $\lambda = 1$. Torej je $Z \cap \mathrm{SL}_n(F) = \{1\}$.

V aditivnih grupah izraz direktni produkt zamenjamo z **direktna vsota**, oznako $N_1 \times \cdots \times N_m$ pa z oznako $N_1 \oplus \cdots \oplus N_m$. Za aditivno grupo G in njene podgrupe N_i torej pišemo

$$G = N_1 \oplus \cdots \oplus N_m,$$

kadar je

$$G = N_1 + \cdots + N_m$$

in

$$N_i \cap (N_1 + \cdots + N_{i-1} + N_{i+1} + \cdots + N_m) = \{0\}$$

za vse $i = 1, \ldots, m$. Po trditvi 4.54 je to ekvivalentno pogoju, da lahko vsak element iz G na en sam način zapišemo v obliki $n_1 + \cdots + n_m$ za neke $n_i \in N_i$.

Primer 4.60. Hitro se prepričamo, da je grupa $\mathbb{Z}_6$ (notranja) direktna vsota svojih podgrup $\{0, 2, 4\}$ in $\{0, 3\}$. Prva je izomorfna $\mathbb{Z}_3$, druga pa $\mathbb{Z}_2$. Zato je grupa $\mathbb{Z}_6$ izomorfna (zunanji) direktni vsoti $\mathbb{Z}_3 \oplus \mathbb{Z}_2$. Grupe $\mathbb{Z}_4$ pa ne moremo zapisati kot direktne vsote pravih netrivialnih podgrup. Edina taka podgrupa je namreč $\{0, 2\}$. Tudi grup $\mathbb{Z}_2$, $\mathbb{Z}_3$ in $\mathbb{Z}_5$ ne moremo »razstaviti«, saj so celo brez pravih netrivialnih podgrup. Katere izmed grup $\mathbb{Z}_n$ so torej direktne vsote svojih pravih podgrup? Odgovor bomo podali v razdelku 5.4.

Direktne vsote v vektorskih prostorih obravnavamo enako kot direktne vsote v aditivnih grupah, le vlogo podgrup prevzamejo podprostori. Dodatna operacija množenja s skalarji v dokazovanjih ne povzroča preglavic. Tako brez težav izpeljemo inačico izreka 4.55 za vektorske prostore. Podrobnosti prepuščamo bralcu.

Če se vpeljava direktnih vsot v vektorskih prostorih le malo razlikuje od vpeljave direktnih vsot v aditivnih grupah, pa je bistvena razlika v eksistenci – glej nalogi 9 in 10.

Naloge

1. Denimo, da je grupa G notranji direktni produkt edink $N_1 \ldots, N_m$, ki so kot grupe vse Abelove. Pokaži, da je potem tudi G Abelova.
2. Pokaži, da je grupa $\mathbb{R}^*$ notranji direktni produkt podgrup $\mathbb{R}^+$ in $\{1, -1\}$.
3. Pokaži, da nekomutativna grupa z manj kot 12 elementi ni direktni produkt svojih pravih podgrup edink.

   Nasvet. Lahko si pomagaš z dejstvom, da so vse grupe z manj kot šest elementi Abelove. To bomo sicer pokazali šele v naslednjem poglavju,

ko bomo izpeljevali različne posledice Lagrangeovega izreka. Toda poskusi to pokazati že sedaj!

4. Pokaži, da je diedrska grupa D_{12} notranji direktni produkt edink $\langle r^2, z\rangle$ in $\langle r^3\rangle$.
5. Za katera naravna števila n je ortogonalna grupa $\mathrm{O}_n(\mathbb{R})$ notranji direktni produkt edink $\mathrm{SO}_n(\mathbb{R})$ in $\{-I, I\}$?
6. Naj bo $n \geq 3$. Ali je simetrična grupa S_n notranji direktni produkt edinke A_n in neke druge edinke N?
7. Pokaži, da grupa $\mathbb{Z}$ ni notranja direktna vsota dveh svojih pravih podgrup.
8. Naj bodo V_1, V_2, V_3 različni enorazsežni podprostori 2-razsežnega vektorskega prostora V. Pokaži, da je $V = V_1 + V_2 + V_3$ in $V_i \cap V_j = \{0\}$ za vse $i \neq j$, vendar pa V ni direktna vsota V_1, V_2 in V_3.

   Komentar. S to nalogo želimo opozoriti, da pogoja (4.9) ne moremo nadomestiti s pogojem, da je $N_i \cap N_j = \{1\}$ za vse $i \neq j$.
9. Naj bo V končno-razsežen vektorski prostor. Pokaži, da za vsak njegov podprostor U obstaja tak podprostor W, da je $V = U \oplus W$.

   Namig. Bazo prostora U lahko razširimo do baze prostora V.
10. Naj bo V končno-razsežen realni vektorski prostor. Pokaži, da za vsak njegov pravi neničeln podprostor U obstaja neskončno mnogo takih podprostorov W, da je $V = U \oplus W$.

    Komentar. Tako v tej kot v prejšnji nalogi je predpostavka, da je V končno-razsežen, nepotrebna. Tudi v neskončno-razsežnih prostorih lahko namreč vsako linearno neodvisno množico dopolnimo do baze.

4.6. Direktni produkti in vsote v kolobarjih

Študij direktnih produktov in vsot v kolobarjih je sicer idejno podoben kot v grupah, v podrobnostih pa vendarle nekoliko drugačen.

Kolobar K je aditivna grupa in zato lahko govorimo o zapisu K kot direktne vsote njegovih podgrup za seštevanje. Če so torej $I_1, \ldots, I_m$ podgrupe K, je K njihova direktna vsota, kar pišemo kot $K = I_1 \oplus \cdots \oplus I_m$, kadar lahko vsak element iz K na en sam način zapišemo kot vsoto $u_1 + \cdots + u_m$ za neke $u_i \in I_i$. Zanimala nas bo situacija, ko so te podgrupe I_i ideali. To je povezano s pojmom direktnega produkta kolobarjev. Namreč, če so $K_1, \ldots, K_m$ kolobarji in je $K = K_1 \times \cdots \times K_m$ njihov direktni produkt, potem so, kot se hitro prepričamo, množice

$$\widetilde{K_i} := \{(0, \ldots, 0, x_i, 0 \ldots, 0) \mid x_i \in K_i\} \tag{4.12}$$

ideali kolobarja K in K je njihova direktna vsota.

Za razumevanje in jasnejši opis direktnih vsot idealov si bomo pomagali z idempotenti. Spomnimo se, da se element e iz kolobarja K imenuje **idempotent**, če je $e^2 = e$. Idempotent, ki komutira z vsakim elementom iz kolobarja, torej idempotent iz centra kolobarja, se imenuje **centralen idempotent**. Če je e centralen idempotent, je

$$eK := \{ex \mid x \in K\}$$

očitno ideal kolobarja K (zgoraj definirani ideali $\widetilde{K_i}$ so take oblike za centralen idempotent $(0, \ldots, 0, 1, 0, \ldots, 0)$, kjer je 1 enota kolobarja K_i). Idempotenta e in f sta **ortogonalna**, če je $ef = fe = 0$. Na primer, za vsak idempotent e je tudi $1 - e$ idempotent in idempotenta e in $1 - e$ sta ortogonalna. Za idempotente $e_1, \ldots, e_m$ bomo rekli, da so **paroma ortogonalni**, če sta e_i in e_j ortogonalna za vse $i \neq j$. Vsota idempotentov nasploh ni idempotent, vsota paroma ortogonalnih idempotentov pa je.

Izrek 4.61. *Naj bodo $I_1, \ldots, I_m$ ideali kolobarja K. Potem je $K = I_1 \oplus \cdots \oplus I_m$ natanko tedaj, ko obstajajo taki paroma ortogonalni centralni idempotenti $e_1, \ldots, e_m \in K$, da je $e_1 + \cdots + e_m = 1$ in $I_i = e_i K$ za vse $i = 1, \ldots, m$.*

Dokaz. Najprej privzemimo, da je $K = I_1 \oplus \cdots \oplus I_m$. Enoto 1 kolobarja K potem lahko zapišemo kot $e_1 + \cdots + e_m$, kjer so $e_i \in I_i$. Za vse $i \neq j$ je $I_i I_j \subseteq I_i \cap I_j = \{0\}$. Če pomnožimo enakost $1 = e_1 + \cdots + e_m$ z leve z $u_i \in I_i$, tako dobimo $u_i = u_i e_i$. Podobno z množenjem z u_i z desne dobimo $u_i = e_i u_i$. Torej je

$$u_i = u_i e_i = e_i u_i \quad \text{za vse } u_i \in I_i. \tag{4.13}$$

To med drugim pove, da je $I_i \subseteq e_i K$. Ker je I_i ideal in je e_i njegov element, velja tudi obratna inkluzija $e_i K \subseteq I_i$. Torej je $I_i = e_i K$. Če za u_i v (4.13) izberemo kar e_i, dobimo $e_i^2 = e_i$. Enakost (4.13) tudi pove, da e_i komutira z vsemi elementi iz I_i. Če $j \neq i$, potem zaradi $I_i I_j = I_j I_i = \{0\}$ velja $e_i u_j = u_j e_i = 0$ za vse $u_j \in I_j$. Od tod sledi, da e_i komutira z vsemi elementi iz K in je torej centralen idempotent. Očitno so $e_1, \ldots, e_m$ paroma ortogonalni.

Dokažimo še obratno trditev. Če so idempotenti $e_1, \ldots, e_m$ paroma ortogonalni, je

$$e_i K \cap (e_1 K + \cdots + e_{i-1} K + e_{i+1} K + \cdots + e_m K) = \{0\}$$

za vsak $i = 1, \ldots, m$. Res, če enakost

$$e_i x_i = e_1 x_1 + \cdots + e_{i-1} x_{i-1} + e_{i+1} x_{i+1} + \cdots + e_m x_m$$

pomnožimo z leve z e_i, takoj dobimo $e_i x_i = 0$. Če velja še $e_1 + \cdots + e_m = 1$, je $e_1 x + \cdots + e_m x = x$ za vsak $x \in K$ in zato $K = e_1 K \oplus \cdots \oplus e_m K$. □

Primer 4.62. Za $e_1 = 1$ in $e_2 = 0$ dobimo trivialni primer: $I_1 = K$ in $I_2 = \{0\}$.

PRIMER 4.63. V primeru 4.60 smo omenili, da je grupa $(\mathbb{Z}_6, +)$ direktna vsota svojih podgrup $\{0, 2, 4\}$ in $\{0, 3\}$. Ti podgrupi sta tudi ideala kolobarja $(\mathbb{Z}_6, +, \cdot)$. Ustrezna idempotenta sta $e_1 = 4$ in $e_2 = 1 - e_1 = 3$.

V drugem delu dokaza, tj. v dokazu obratne trditve, nismo uporabili predpostavke, da so idempotenti e_i centralni. Tako smo dejansko dokazali, da je kolobar K direktna vsota svojih *desnih* idealov $e_1K, \ldots, e_mK$, če so e_i paroma ortogonalni idempotenti in je njihova vsota enaka 1.

Ideali I_i iz izreka niso podkolobarji K, saj ne vsebujejo enote 1 kolobarja K. So pa vendarle kolobarji, saj ima, kot vidimo iz (4.13), vsak izmed njih svojo enoto e_i. Nasploh ideali kolobarjev nimajo nujno svojih enot. Ideali I_i jih pač imajo, zato lahko govorimo o direktnem produktu kolobarjev $I_1, \ldots, I_m$, torej o kolobarju $I_1 \times \cdots \times I_m$.

IZREK 4.64. *Če je kolobar K enak direktni vsoti svojih idealov $I_1 \ldots, I_m$, potem je K izomorfen njihovemu direktnemu produktu $I_1 \times \cdots \times I_m$.*

DOKAZ. Pokažimo, da je preslikava $\varphi : I_1 \times \cdots \times I_m \to K$,

$$\varphi\big((u_1, \ldots, u_m)\big) = u_1 + \cdots + u_m,$$

izomorfizem kolobarjev. Ker lahko vsak element iz K na natanko en način zapišemo kot vsoto $u_1 + \cdots + u_m$, $u_i \in I_i$, je φ bijektivna. Dokažimo še, da je homomorfizem. Dokaz, da φ ohranja vsoto, je zelo enostaven in ga izpustimo. Naj bodo e_i idempotenti iz izreka 4.61. Potem je e_i enota kolobarja I_i, zato je $(e_1, \ldots, e_m)$ enota kolobarja $I_1 \times \cdots \times I_m$. Preslikava φ jo preslika v element $e_1 + \cdots + e_m$, ki je enota 1 kolobarja K. Dokazati moramo le še, da je za poljubne $u_i, v_i \in I_i$ element

$$\varphi\big((u_1, \ldots, u_m) \cdot (v_1, \ldots, v_m)\big) = \varphi\big((u_1v_1, \ldots, u_mv_m)\big) = u_1v_1 + \cdots + u_mv_m$$

enak elementu

$$\varphi\big((u_1, \ldots, u_m)\big) \cdot \varphi\big((v_1, \ldots, v_m)\big) = (u_1 + \cdots + u_m)(v_1 + \cdots + v_m).$$

To pa je takojšnja posledica dejstva, da je $u_iv_j = (u_ie_i)(e_jv_j) = 0$ za vse $i \neq j$. □

Vse, kar smo povedali za direktne produkte in vsote v kolobarjih, velja tudi za **direktne produkte in vsote v algebrah**. V zgornjih vrsticah moramo samo besedo »kolobar« zamenjati z »algebra«.

Na koncu omenimo, da se v literaturi ponekod direktnemu produktu končnega števila kolobarjev reče tudi *direktna vsota*. Oznaka $K_1 \times \cdots \times K_n$ se tedaj ponavadi zamenja z oznako $K_1 \oplus \cdots \oplus K_n$. Če bi se odločili za to terminologijo, bi morali tako kot pri grupah ločiti med zunanjo in notranjo direktno vsoto.

Tako pa smo se pridevnikoma »zunanji« in »notranji« pri kolobarjih lahko izognili.

Naloge

1. Naj bo $K = K_1 \times \cdots \times K_m$ in naj bo $\widetilde{K_i}$ kot v (4.12). Pokaži, da je
$$K/\widetilde{K_i} \cong K_1 \times \cdots \times K_{i-1} \times K_{i+1} \times \cdots \times K_m.$$
2. Pokaži, da ima kolobar, ki je enak direktni vsoti m neničelnih idealov $I_1, \ldots, I_m$, vsaj 2^m centralnih idempotentov.
3. Naj bo p praštevilo in k naravno število. Pokaži, da sta 0 in 1 edina idempotenta kolobarja $\mathbb{Z}_{p^k}$. Še več, vsak element v $\mathbb{Z}_{p^k}$ je bodisi obrnljiv bodisi nilpotenten.
4. Pokaži, da kolobar $\mathbb{Z}_n$ vsebuje idempotent, različen od 0 in 1, če je n deljiv z vsaj dvema praštevilomaa.

   Namig. Če sta si števili n_1 in n_2 tuji, po kitajskem izreku o ostankih (gl. nalogo 4.3/8) obstaja tak $x \in \mathbb{Z}$, da je $x \equiv 1 \pmod{n_1}$ in $x \equiv 0 \pmod{n_2}$.
5. Naj bo K množica vseh realnih zaporedij. Za običajno seštevanje in množenje zaporedij je K kolobar (gl. primer 1.89). Pokaži, da K vsebuje taka ideala I in J, da je $K = I \oplus J$ in $K \cong I \cong J$ (tako je $K \cong K \times K$ po izreku 4.64). Ali tudi kolobar vseh konvergentnih zaporedij vsebuje taka ideala?
6. Naj bo $G = \{g_1, \ldots, g_n\}$ poljubna množica. Množica vseh formalnih linearnih kombinacij $\sum_{i=1}^n \lambda_i g_i$, kjer so λ_i elementi nekega polja F, postane vektorski prostor nad F z bazo G, če definiramo seštevanje in množenje s skalarji na samoumeven način (kot bi ju definirali, če bi $\sum_{i=1}^n \lambda_i g_i$ pisali kot n-terico $(\lambda_1, \ldots, \lambda_n)$). Privzemimo sedaj, da je G grupa. Potem ta vektorski prostor postane algebra, če množenje elementov grupe razširimo na cel prostor na edini možni način, torej z upoštevanjem distributivnosti in enakosti $\lambda_i g_i \cdot \mu_j g_j = (\lambda_i \mu_j) g_i g_j$; tu je $g_i g_j$ produktov elementov v grupi G, $\lambda_i \mu_j$ pa produkt elementov v polju F. Imenujemo jo **grupna algebra** grupe G nad poljem F in označujemo s $F[G]$.
   (a) Pokaži, da element $u := \sum_{i=1}^n g_i$ zadošča $ug_j = g_j u = u$ za vsak $g_j \in G$.
   (b) Predpostavimo, da je karakteristika polja F enaka 0 ali pa ne deli $|G|$. Pokaži, da je $e := \frac{1}{|G|} u$ centralen idempotent algebre $F[G]$, dimenzija ideala $eF[G]$ je enaka 1, ideal $(1-e)F[G]$ pa sestoji iz vseh takih elementov $\sum_{i=1}^n \lambda_i g_i$, da je $\sum_{i=1}^n \lambda_i = 0$.
   (c) Naj bo $G = \{1, -1\}$, tj. ciklična grupa z dvema elementoma. Pokaži, da je $F[G] \cong F \times F$, razen če je karakteristika polja F enaka 2. V tem primeru je algebra $F[G]$ izomorfna algebri vseh matrik oblike $\left[\begin{smallmatrix} \alpha & \beta \\ 0 & \alpha \end{smallmatrix}\right]$, $\alpha, \beta \in F$.

POGLAVJE 5

Končne grupe

V prejšnjih poglavjih smo zgradili jezik, ki omogoča obravnavo algebraičnih problemov. Zdaj smo spet na začetku. Problemov se lahko lotimo.

V tem poglavju se bomo seznanili z osnovami teorije končnih grup. Zgradbo končne grupe poskušamo razumeti preko lastnosti posameznih elementov in podgrup. Učinkovitost takega pristopa se bo posebej izkazala v zadnjem razdelku, ko bomo klasificirali vse končne Abelove grupe. Naša obravnava bo slonela na pojmih in rezultatih prejšnjih poglavij. Homomorfizmi, odseki in kvocientne grupe bodo tako sedaj samo še orodje za dokazovanje ali pa jezik, v katerem lahko izrazimo izreke.

5.1. Posledice Lagrangeovega izreka

Katere posebnosti končnih grup že poznamo? Pravzaprav jih ni veliko, saj smo doslej le malokrat ločevali med končnimi in neskončnimi grupami. Omenimo lahko, da je vsaka končna ciklična grupa izomorfna grupi $(\mathbb{Z}_n, +)$ in da je red poljubnega elementa a končne grupe enak redu ciklične podgrupe $\langle a \rangle$. Toda oboje je skorajda očitno (gl. razdelek 3.1). Edini nekoliko globlji rezultat o končnih grupah, ki smo ga že spoznali, je Lagrangeov izrek (izrek 4.8). Spomnimo se ga.

Lagrangeov izrek. *Če je G končna grupa in H njena podgrupa, potem je*

$$|G| = [G : H] \cdot |H|.$$

Tu je $[G : H]$ indeks grupe G po podgrupi H, torej število vseh odsekov aH, $a \in G$. Največkrat uporabljamo samo naslednjo posledico izreka.

Posledica 5.1. *Red vsake podgrupe končne grupe deli red grupe.*

Tudi tej posledici pogosto rečemo kar Lagrangeov izrek. V nadaljevanju razdelka bomo iz te osnovne posledice izpeljali številne druge. Prve se tičejo redov elementov. Najprej zabeležimo nekaj enostavnih opazk o redih, ki jih bomo do konca poglavja pogosto potrebovali.

Opomba 5.2. Naj bo a element grupe G.
(a) Če ima a red n, potem za vsak $m \in \mathbb{Z}$ velja

$$a^m = 1 \iff n \mid m.$$

Dokaz je preprost. Iz $n \mid m$ očitno sledi $a^m = 1$. Obratno, naj bo $a^m = 1$. Po osnovnem izreku o deljenju zapišimo $m = qn + r$, kjer je $q \in \mathbb{Z}$ in $0 \leq r < n$. Iz

$$1 = a^m = (a^n)^q a^r = 1a^r = a^r$$

sledi $r = 0$, saj je n najmanjše naravno število z lastnostjo $a^n = 1$. Torej $n \mid m$.

(b) Če $a \neq 1$ in za neko praštevilo p velja $a^p = 1$, potem je p red elementa a. To sledi takoj iz (a).

(c) Če ima a red n in je $\varphi : G \to G'$ homomorfizem grup, potem red elementa $\varphi(a)$ deli n. Namreč, $\varphi(a)^n = \varphi(a^n) = 1$, zato tudi to sledi iz (a).

(d) Če je N edinka v G in ima a red n, potem red elementa $aN \in G/N$ deli n. To sledi iz (c), če za φ izberemo kanonični epimorfizem iz G v G/N.

Preidimo na posledice Lagrangeovega izreka.

Posledica 5.3. *Red vsakega elementa končne grupe deli red grupe.*

Dokaz. Red elementa a je enak redu ciklične podgrupe $\langle a \rangle$, le-ta pa po posledici 5.1 deli red grupe. □

Posledica 5.4. *Če je G končna grupa z n elementi, je $a^n = 1$ za vsak $a \in G$.*

Dokaz. Vzemimo $a \in G$ in označimo z r njegov red. Po posledici 5.3 je $n = rk$ za neki $k \in \mathbb{N}$. Zato je $a^n = (a^r)^k = 1^k = 1$. □

Kot zanimivost si poglejmo, kaj posledica 5.4 pove v posebnem primeru, ko za G izberemo grupo vseh neničelnih (torej obrnljivih) elementov polja $\mathbb{Z}_p$; tu je p seveda praštevilo (gl. trditev 2.15).

Posledica 5.5. *Za vsako praštevilo p in vsako naravno število a je*

$$a^p \equiv a \pmod{p}.$$

Dokaz. Elementi polja $\mathbb{Z}_p$ so odseki $x + p\mathbb{Z}$, kjer je $x \in \mathbb{Z}$. Očitno smemo privzeti, da $p \nmid a$. Zato je odsek $a + p\mathbb{Z}$ neničeln in kot tak element grupe $\mathbb{Z}_p^*$. Po posledici 5.4 je zato

$$(a + p\mathbb{Z})^{p-1} = 1 + p\mathbb{Z},$$

tj.

$$a^{p-1} + p\mathbb{Z} = 1 + p\mathbb{Z}.$$

Torej $p \mid a^{p-1} - 1$ in zato tudi $p \mid a^p - a$. □

Ta rezultat je Pierre de Fermat leta 1640 omenil v pismu prijatelju. Danes ga imenujemo *Fermatov mali izrek* (po globini je v primerjavi s Fermatovim zadnjim izrekom, o katerem smo spregovorili v razdelku 2.6, res »majhen«).

Presenetljivo se je ta sicer preprosta, ne pa tudi očitna ugotovitev o številih izkazala za uporabno v kriptografiji. To je veda, ki se ukvarja z varnim prenašanjem sporočil od pošiljatelja do prejemnika (kot je na primer bančno poslovanje na spletu). Eden najbolj razširjenih algoritmov v kriptografiji, imenovan RSA, sloni na dejstvu, da računalniki zmorejo tudi zelo velika števila med seboj množiti, ne pa tudi razstavljati. Njegov teoretični temelj je prav Fermatov mali izrek. Zamislimo si francoskega pravnika, po duši matematika, ki se sredi 17. stoletja zvečer ob svečah kratkočasi z dozdevno nekoristnim razmišljanjem o številih. Nakar neka njegova ugotovitev v 20. stoletju dobi široko uporabo v svetovnem spletu in še kje. Zveni neverjetno! Nasploh se rezultati teoretične matematike proti vsem pričakovanjem včasih izkažejo za uporabne v znanosti in tehnologiji. Praviloma šele čez desetletja ali stoletja po odkritju.

Vrnimo se h grupam. Za vsako naravno število n najdemo vsaj eno grupo z n elementi, namreč ciklično grupo. Če je n praštevilo, drugih ni.

Posledica 5.6. *Vsaka grupa G s praštevilskim redom je ciklična. Še več, za vsak od* 1 *različen element a iz G je $\langle a\rangle = G$.*

Dokaz. Naj bo red grupe G praštevilo p. Vzemimo $a \in G$, ki je različen od enote 1. Ciklična podgrupa $\langle a\rangle$ potem ni trivialna, njen red pa deli p po posledici 5.1. Zato je lahko enak le p. To pomeni, da je $\langle a\rangle = G$. □

Vsaka grupa G s p elementi je torej izomorfna grupi $(\mathbb{Z}_p, +)$ (gl. izrek 3.8). Naslednja posledica podaja še eno karakterizacijo takih grup.

Posledica 5.7. *Netrivialna grupa nima pravih netrivialnih podgrup natanko tedaj, ko je ciklična grupa s praštevilskim redom.*

Dokaz. Naj bo G netrivialna grupa brez pravih netrivialnih podgrup. Potem je $\langle a\rangle = G$ za vsak $a \in G \setminus \{1\}$. Torej je G ciklična grupa. Po izreku 3.8 je G izomorfna bodisi grupi $\mathbb{Z}$ bodisi grupi $\mathbb{Z}_n$ za neki $n \in \mathbb{N}$. Grupa $\mathbb{Z}$ seveda ima prave netrivialne podgrupe (npr. $2\mathbb{Z}$), zato v pride v poštev le druga možnost. Če je število n deljivo s številom d in je $1 < d < n$, je $d\mathbb{Z}_n$ prava netrivialna podgrupa grupe $\mathbb{Z}_n$. Torej mora biti n praštevilo.

Obratno, če je G ciklična grupa s praštevilskim redom in je H njena netrivialna podgrupa, potem po posledici 5.6 za vsak $a \neq 1$ iz H velja $H \supseteq \langle a\rangle = G$. Torej je $H = G$. □

Grupe s praštevilskim redom torej poznamo. Edina grupa z dvema elementoma je $\mathbb{Z}_2$, edina s tremi elementi pa $\mathbb{Z}_3$. Seveda z »edina« mislimo na »edina do izomorfizma natančno«. Že v primeru 3.10 smo našli dve neizomorfni grupi s štirimi elementi, namreč

$$\mathbb{Z}_4 \quad \text{in} \quad \mathbb{Z}_2 \oplus \mathbb{Z}_2.$$

Pokažimo, da drugih ni. Naj bo $G = \{1, a, b, c\}$ poljubna grupa s štirimi elementi. Če ima kateri izmed elementov a, b, c red 4, je $G \cong \mathbb{Z}_4$. Če nobeden nima reda 4, imajo po posledici 5.3 vsi red 2. Torej je $a^2 = b^2 = c^2 = 1$. Zaradi pravila krajšanja v grupi element ab ne more biti enak a, b ali 1, zato je $ab = c$. Iz istega razloga je tudi $ba = c$ in podobno $ac = ca = b$ ter $bc = cb = a$. Bralcu sedaj ne bi smelo biti pretežko pokazati, da je $G \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2$. Grupe z največ štirimi elementi tako poznamo. Ker je 5 praštevilo, drugih grup s petimi elementi razen $\mathbb{Z}_5$ ni. Poiskati vse grupe s šestimi elementi je že malce zahtevnejša naloga, a z nekaj truda bi ji bili kos. Izkaže se, da sta le dve, namreč

$$\mathbb{Z}_3 \oplus \mathbb{Z}_2 \quad \text{in} \quad S_3.$$

Simetrična grupa S_3 je torej najmanjša nekomutativna grupa. Seveda ima tudi ciklična grupa $\mathbb{Z}_6$ šest elementov, toda grupa $\mathbb{Z}_3 \oplus \mathbb{Z}_2$ ji je izomorfna (gl. primer 4.60). Po praštevilu 7 je na vrsti število 8. Izkaže se, da so edine grupe z osmimi elementi

$$\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2, \quad \mathbb{Z}_4 \oplus \mathbb{Z}_2, \quad \mathbb{Z}_8, \quad D_8 \quad \text{in} \quad Q.$$

Prve tri so Abelove, diedrska grupa D_8 in kvaternionska grupa Q pa nista.

Lahko bi dodali še nekaj seznamov vseh grup z danim številom elementov, ki je dovolj majhno ali pa zelo posebno. Podati tak seznam za vsako število pa se zdi nerešljiv problem. Omejiti se moramo na grupe posebnih tipov. V razdelku 5.4 bomo opisali vse končne Abelove grupe. To je torej elementaren, nam dostopen problem. Vse kaj drugega pa je problem poiskati vse *končne enostavne grupe*, torej končne grupe brez pravih netrivialnih edink. Med Abelovimi grupami so po posledici 5.7 take le ciklične grupe s praštevilskim redom. Omenili smo že, da so alternirajoče grupe A_n, $n \geq 5$, enostavne. Dokaz ni pretežek, a ga izpustimo. Tako poznamo dve neskončni družini končnih enostavnih grup. Eden največjih dosežkov matematike druge polovice 20. stoletja je opis *vseh* končnih enostavnih grup. Izkaže se, da poleg omenjenih dveh obstaja še 16 družin takih grup ter 26 posameznih primerov (t. i. *sporadičnih grup*). Največja izmed slednjih, imenovana *pošast* (angl. *monster group*), ima približno 8×10^{53} elementov.

Naloge

1. Naj bo G končna grupa in H, K taki podgrupi G, da je $K \subseteq H$. Pokaži, da je $[G : K] = [G : H][H : K]$.
2. Naj bo K prava podgrupa prave podgrupe grupe G. Denimo, da je $|G| = 24$. Koliko je lahko $|K|$?
3. Določi vse končne grupe G, ki vsebujejo kako podgrupo reda $|G| - 2$.

4. Denimo, da grupa G vsebuje taka elementa $a \neq 1$ in $b \neq 1$, da je $a^{91} = 1$ in $b^{15} = 1$. Pokaži, da je $|G| \geq 21$.
5. Naj bo $n \geq 3$. Pokaži, da grupa $(\mathbb{Z}_n^*, \cdot)$ vsebuje element reda 2 in od tod sklepaj, da je njen red sodo število.

   Komentar. Slednje lahko povemo tudi tako, da ima Eulerjeva funkcija φ sode vrednosti v vseh številih $n \geq 3$ (gl. nalogo 2.2/10).
6. Naj bosta n in a tuji si naravni števili. Pokaži, da $n \mid a^{\varphi(n)} - 1$.

   Komentar. Tej posplošitvi Fermatovega malega izreka pravimo **Eulerjev izrek**.
7. S pomočjo Fermatovega malega izreka izračunaj, koliko je 4^{19} v $\mathbb{Z}_7$ in koliko je v $\mathbb{Z}_{17}$.
8. S pomočjo Eulerjevega izreka izračunaj zadnjo števko števila 23^8 in zadnjo števko števila 23^{23}.
9. Naj bo p praštevilo in naj bo q praštevilski delitelj števila $2^p - 1$. Pokaži, da je p red elementa 2 grupe $(\mathbb{Z}_q^*, \cdot)$ in od tod sklepaj, da $p \mid q - 1$; med drugim je zato $q > p$.

   Komentar. Iz rezultata naloge sledi, da ne obstaja največje praštevilo p, da je torej praštevil neskončno mnogo. Seveda to že vemo (izrek 2.9, naloga 2.1/8). Vendarle pa je zanimivo, da lahko to fundamentalno matematično ugotovitev izpeljemo tudi s pomočjo Langrangeovega izreka. Omenimo še, da številu oblike $2^p - 1$, kjer je p praštevilo, pravimo **Mersennovo število**. S takimi števili smo se srečali že v nalogi 2.1/7.
10. Denimo, da je $|G| = 55$. Pokaži:
    (a) Vsaka prava podgrupa G je ciklična.
    (b) G je bodisi Abelova bodisi ima trivialen center.

    Namig. Naloga 4.2/6.
11. Pojasni, zakaj lahko v prejšnji nalogi število 55 zamenjamo s katerimkoli številom, ki je produkt dveh praštevil. Ali ga lahko zamenjamo tudi z 8?
12. Naj bosta H in K končni podgrupi grupe G. Pokaži, da iz vsakega izmed naslednjih dveh pogojev sledi, da je $H \cap K = \{1\}$:
    (a) Števili $|H|$ in $|K|$ sta si tuji.
    (b) $|H| = |K|$ je praštevilo in $H \neq K$.
13. Naj bosta H in K končni podgrupi grupe G. Pokaži, da je

$$|HK| = \frac{|H||K|}{|H \cap K|}.$$

    Navodilo. Naj bo m število vseh različnih odsekov oblike hK, kjer je $h \in H$. Najprej pokaži, da je $|HK| = m|K|$. Zatem pokaži, da za

elementa $h, h' \in H$ velja $hK = h'K$ natanko tedaj, ko je $h(H \cap K) = h'(H \cap K)$. Od tod sklepaj, da je $m = [H : H \cap K]$ in naposled uporabi Lagrangeov izrek.

Komentar. Če je katera izmed podgrup H in K edinka, ta enakost sledi tudi iz drugega izreka o izomorfizmu.

14. Red alternirajoče grupe A_4 je 12. Po Lagrangeovem izreku lahko imajo njene prave netrivialne podgrupe red 2, 3, 4 ali 6. Pokaži, da podgrupe reda 2, 3 in 4 res obstajajo, podgrupa reda 6 pa ne.

Navodilo. Denimo, da je $H \leq A_4$ in $|H| = 6$. Potem je H edinka in $A_4/H \cong \mathbb{Z}_2$ (gl. nalogo 4.2/8), zato za vsak $\sigma \in A_4$ velja $\sigma^2 \in H$. Če je $\pi \in A_4$ 3-cikel, je torej $\pi = (\pi^2)^2 \in H$. Zdaj lahko uporabiš nalogo 2.7/20 ali pa enostavno prešteješ 3-cikle v A_4.

5.2. Razredna formula

Namen tega razdelka je izpeljati formulo, ki povezuje red grupe z redom njenega centra in indeksi nekih njenih posebnih podgrup. Pravimo ji razredna formula. Pogosto se izkaže kot koristno orodje pri študiju končnih grup. Primer njene uporabe bomo spoznali v naslednjem razdelku.

Spomnimo se, da za elementa a in a' iz grupe G pravimo, da sta si *konjugirana*, če obstaja tak $g \in G$, da je

$$a' = gag^{-1}.$$

Pokažimo, da je *konjugiranost ekvivalenčna relacija na* G. Refleksivnost je očitna, saj je $a = 1a1^{-1}$. Iz $a' = gag^{-1}$ sledi $a = g^{-1}a'g$, kar dokazuje simetričnost. Še tranzitivnost: če je $a' = gag^{-1}$ in $a'' = ha'h^{-1}$, potem je $a'' = (hg)a(hg)^{-1}$. Relacija konjugiranosti tako porodi razpad množice G na ekvivalenčne razrede. Imenujemo jih **konjugiranostni razredi**. Če je grupa G končna, torej velja

$$|G| = \sum_i |R_i|, \tag{5.1}$$

kjer so R_i konjugiranostni razredi. V bistvu je to že formula, ki jo imamo v mislih. Le preoblikovati jo moramo, da bo dobila bolj uporabno obliko.

Za poljuben element $a \in G$ naj $R(a)$ označuje konjugiranostni razred, ki mu a pripada. V njem so vsi elementi, ki so si z a konjugirani. Torej je

$$R(a) = \{gag^{-1} \mid g \in G\}.$$

Vpeljimo še množico

$$C(a) := \{x \in G \mid ax = xa\},$$

torej množico vseh elementov, ki z a komutirajo. Imenujemo jo **centralizator elementa** a (gl. nalogo 1.6/8). Poleg elementa a očitno vsebuje tudi vse elemente iz centra $Z(G)$ grupe G.

LEMA 5.8. *Za vsak element a iz grupe G je njegov centralizator $C(a)$ podgrupa G in velja*

$$|R(a)| = [G : C(a)].$$

DOKAZ. Če enakost $ax = xa$ z leve in desne pomnožimo z x^{-1}, dobimo $x^{-1}a = ax^{-1}$. Torej iz $x \in C(a)$ sledi $x^{-1} \in C(a)$. Ker očitno iz $x, y \in C(a)$ sledi $xy \in C(a)$, je $C(a)$ podgrupa.

Za poljubna $g, h \in G$ velja $gC(a) = hC(a)$ natanko tedaj, ko je $g^{-1}h \in C(a)$ (lema 4.6), torej ko je

$$ag^{-1}h = g^{-1}ha.$$

Z množenjem z leve z g in z desne s h^{-1} vidimo, da lahko to enakost zapišemo v obliki

$$gag^{-1} = hah^{-1}.$$

Torej velja

$$gag^{-1} = hah^{-1} \iff gC(a) = hC(a).$$

Od tod sledi, da je

$$gag^{-1} \mapsto gC(a)$$

dobro definirana injektivna preslikave iz množice $R(a)$ v množico vseh odsekov grupe G po podgrupi $C(a)$. Njena surjektivnost je očitna, zato je moč množice $R(a)$ enaka indeksu grupe G po podgrupi $C(a)$. □

Skoraj smo na cilju, le še besedo namenimo elementom iz centra grupe. Če je $a \in Z(G)$, je očitno $R(a) = \{a\}$ in $C(a) = G$. Velja tudi

$$a \in Z(G) \iff |R(a)| = 1.$$

Konjugiranostnih razredov z enim samim elementom je torej toliko, kot ima center grupe elementov. Enakost (5.1) zato lahko zapišemo kot

$$|G| = |Z(G)| + \sum_j |R_j|, \tag{5.2}$$

kjer so R_j konjugiranostni razredi z več kot enim elementom, tj. razredi, katerih elementi ne ležijo v centru. S pomočjo leme 5.8 lahko (5.2) zapišemo nekoliko drugače.

IZREK 5.9. *Naj bo G končna grupa. Potem obstajajo taki $a_j \in G \setminus Z(G)$, da velja*

$$|G| = |Z(G)| + \sum_j [G : C(a_j)].$$

DOKAZ. Konjugiranostni razred R_j lahko zapišemo kot $R(a_j)$ za katerikoli $a_j \in R_j$. Rezultat tako sledi takoj iz leme 5.8 in enakosti (5.2). □

Enakosti iz izreka pravimo **razredna formula**.

Naloge

1. Pokaži, da imata elementa istega konjugiranostnega razreda enak red.
2. Ali elementa z enakim redom vselej ležita v istem konjugiranostnem razredu?
3. Pokaži, da ima simetrična grupa S_3 tri konjugiranostne razrede: v prvem je samo identiteta, v drugem so vse tri transpozicije, v tretjem pa oba 3-cikla.
4. Ali cikla $(1\,2\,3)$ in $(1\,3\,2)$ ležita v istem konjugiranostnem razredu grupe A_3?
5. Pokaži, da ima kvaternionska grupa Q pet konjugiranostnih razredov in jih opiši.
6. Pokaži, da ima diedrska grupa D_8 pet konjugiranostnih razredov in jih opiši.
7. Pokaži, da ima grupa G netrivialen center, če je $|G| = p^m$ za neko praštevilo p in naravno število m.

   Komentar. Takim grupam pravimo p-grupe. Obravnavane bodo v naslednjih razdelkih.
8. Pokaži, da je grupa G Abelova, če je $|G| = p^2$ za neko praštevilo p.
9. Naj končna grupa G deluje na množici X. Pokaži, da za vsak $x \in X$ velja
$$|G \cdot x| = [G : G_x],$$
tj. moč orbite elementa x je enaka indeksu njegovega stabilizatorja (definicije so v nalogi 3.5/5). To je posplošitev leme 5.8. Namreč, prepričaj se, da je s predpisom $g \cdot x = gxg^{-1}$ definirano delovanje grupe G na množici G in da za to posebno delovanje zgornja enakost sovpada z enakostjo iz leme 5.8.

   Razmisli, da tudi izrek 5.9 lahko posplošimo na poljubna delovanja. Vlogo $|G|$ prevzame $|X|$, vlogo centra $Z(G)$ množica
$$X_0 = \{x \in X \mid g \cdot x = x \text{ za vsak } g \in G\},$$
vlogo centralizatorjev pa stabilizatorji.

5.3. Cauchyjev izrek

Naj bo G končna grupa. Posledica 5.3 pove, da je red vsakega elementa iz G število, ki deli $|G|$. Ali velja tudi obrat, torej ali je število n red kakega elementa iz G, če $n \mid |G|$? V splošnem je odgovor negativen. Na primer, če G ni ciklična grupa, potem ne vsebuje elementa reda $|G|$. Naslednji izrek pove, da je odgovor pozitiven, če je n praštevilo. Ime nosi po *Augustin-Louisu*

Cauchyu, enemu najbolj znamenitih matematikov prve polovice devetnajstega stoletja.

IZREK 5.10. ***(Cauchyjev izrek)*** *Naj bo G končna grupa. Če praštevilo p deli $|G|$, potem G vsebuje element reda p.*

DOKAZ. Izrek dokažimo z indukcijo na $n := |G|$. Ker $p \mid n$, je $n \geq p$. Če je $n = p$, je po posledici 5.6 G ciklična grupa in z izjemo enote ima vsak njen element red p. Privzemimo torej, da je $n > p$ in da izrek velja za vse grupe z manj kot n elementi, torej tudi za vse prave podgrupe grupe G.

Najprej obravnavajmo primer, ko G ni Abelova. Potem je njen center $Z(G)$ prava podgrupa, zato smemo privzeti, da $p \nmid |Z(G)|$. Iz razredne formule (izrek 5.9) sledi, da $p \nmid [G : C(a_j)]$ za neki $a_j \in G \setminus Z(G)$. Ker je po Langrangeovem izreku

$$n = [G : C(a_j)] \cdot |C(a_j)|,$$

mora p deliti $|C(a_j)|$. Toda $C(a_j)$ je prava podgrupa G, zato želeni zaključek sledi iz indukcijske predpostavke.

Naj bo torej G Abelova. Ker ima G več kot p elementov, po posledici 5.7 vsebuje kako pravo netrivialno podgrupo N. Kot podgrupa Abelove grupe je N edinka, zato lahko tvorimo kvocientno grupo G/N. Lagrangeov izrek pove, da je

$$n = |G/N| \cdot |N|$$

in zato $p \mid |G/N|$ ali $p \mid |N|$. V drugem primeru lahko uporabimo indukcijsko predpostavko. Naj torej $p \mid |G/N|$. Ker ima grupa G/N manj kot n elementov, po indukcijski predpostavki vsebuje element, torej odsek aN, ki ima red p. Označimo z m red elementa a. Po opombi 5.2 (d) je $m = kp$ za neko naravno število k. Element a^k ima zato red p (gl. opombo 5.2 (b)). □

OPOMBA 5.11. Cauchyjev izrek lahko ekvivalentno povemo takole: če praštevilo p deli red grupe G, potem G vsebuje podgrupo s p elementi. Namreč, če ima $a \in G$ red p, ima tudi ciklična podgrupa $\langle a \rangle$ red p. Obratno, če ima podgrupa p elementov, je ciklična (posledica 5.6) in zato vsebuje element reda p. Nasploh ne velja za vsako naravno število m, da iz $m \mid |G|$ sledi obstoj podgrupe z m elementi (gl. nalogo 5.1/14).Vendarle pa to ni samo posebnost praštevil – velja namreč tudi za vse potence praštevil. To in veliko več povedo **izreki Sylowa** (gl. nalogo 14), ki odprejo vrata v poglobljen študij končnih grup.

Grupe iz naslednje definicije se bodo naravno pojavile v naslednjem razdelku.

DEFINICIJA 5.12. Naj bo p praštevilo. Grupa G se imenuje **p-grupa**, če je red vsakega njenega elementa potenca števila p.

Definicija p-grupe ima smisel tako za končne kot neskončne grupe. S pomočjo Cauchyjevega izreka pa za končne grupe dobimo tale enostavnejši opis.

POSLEDICA 5.13. *Končna grupa G je p-grupa natanko tedaj, ko je $|G| = p^m$ za neki $m \in \mathbb{N}$.*

DOKAZ. Če je G p-grupa, je po Cauchyjevem izreku p edino praštevilo, ki deli $|G|$. Torej je $|G| = p^m$. Obratna trditev sledi iz posledice 5.3. □

Preprosti primeri p-grup so ciklične grupe $\mathbb{Z}_p$, $\mathbb{Z}_{p^2}$, $\mathbb{Z}_{p^3}$ itd. Kvaternionska grupa Q in diedrska grupa D_8 imata 8 elementov in sta torej 2-grupi. Direktni produkt p-grup je spet p-grupa, pa tudi podgrupe p-grup so očitno tudi same p-grupe.

Naloge

1. **Eksponent** končne grupe G definiramo kot najmanjše naravno število m z lastnostjo, da je $x^m = 1$ za vsak $x \in G$. Pokaži, da je eksponent grupe enak najmanjšemu skupnemu večkratniku redov vseh elementov grupe, da deli red grupe in da ima iste praštevilske delitelje kot red grupe.

   Komentar. Eksponent lahko definiramo tudi za neskončne grupe. Če naravno število m iz zgornje definicije ne obstaja, rečemo, da je eksponent grupe enak ∞. Znaš poiskati primer neskončne grupe s končnim eksponentom? Če ne znaš takoj, se najprej loti naloge 6.
2. Določi eksponent končne ciklične grupe.
3. Določi eksponent simetrične grupe S_3.
4. Podaj primer grupe, katere eksponent je manjši od njenega reda.
5. Za katere p-grupe je eksponent enak redu grupe?
6. Pokaži, da je lahko eksponent poljubno majhen v primerjavi z redom grupe.

   Namig. Direktni produkt grup.
7. Grupe reda 8 so navedene v razdelku 5.1. Katera izmed njih ne vsebuje nobenega elementa reda 4? Pokaži, da za vsako praštevilo p in naravno število m obstaja grupa reda p^m, v kateri imajo vsi elementi razen enote red p.
8. Naj bo G končna grupa. Pokaži, da je moč množice $\{x \in G \mid x \neq x^{-1}\}$ sodo število. Od tod izpelji Cauchyjev izrek za $p = 2$.
9. Pokaži, da je poljubna nekomutativna grupa G reda 6 izomorfna simetrični grupi S_3.

Navodilo. Po Cauchyjevem izreku G vsebuje element a reda 3 in element b reda 2. S pomočjo naloge 5.1/13 vidimo, da je $G = \langle a \rangle \langle b \rangle$. Ugotovi, da je element bab lahko enak le a^2 in da je s tem je množenje v G enolično določeno.

10. Denimo, da grupa G vsebuje taka elementa $a \neq 1$ in $b \neq 1$, da je $a^3 = b^2$ in $a^2 b = ba$. Pokaži, da iz $|G| < 12$ sledi, da je $G \cong S_3$.

11. Denimo, da je $|G| = mp$, kjer je p praštevilo in je $m < p$. Pokaži, da G vsebuje natanko eno podgrupo reda p in da je ta podgrupa edinka. Oglej si tudi poseben primer, ko je $|G| = 6$ in $p = 3$ (edini grupi reda 6 sta $\mathbb{Z}_3 \oplus \mathbb{Z}_2$ in S_3).

    Nasvet. Če ne uspeš rešitve najti neposredno, si pomagaj z nalogami 5.1/12, 5.1/13 in 4.2/9.

12. Denimo, da je $|G| = 2p$, kjer je p liho praštevilo. Pokaži, da je $G \cong \mathbb{Z}_{2p}$ ali $G \cong D_{2p}$.

13. S pomočjo delovanj grup na množicah podaj drugačen, zanimiv in eleganten dokaz Cauchyjevega izreka.

    Navodilo. Naj bo p praštevilo, ki deli $|G|$. Vpeljimo

    $$X := \{(a_1, \ldots, a_p) \,|\, a_i \in G \text{ in } a_1 \cdots a_p = 1\}.$$

    Pojasni, zakaj je $|X| = |G|^{p-1}$ (namig: $a_p = (a_1 \cdots a_{p-1})^{-1}$). Ker p deli $|G|$, torej p deli tudi $|X|$. Zatem pokaži, da je s predpisom

    $$k \cdot (a_1, \ldots, a_p) := (a_{k+1}, \ldots, a_p, a_1, \ldots, a_k)$$

    definirano delovanje grupe $\mathbb{Z}_p$ na množici X. Definirajmo X_0 kot v nalogi 5.2/9. S pomočjo te naloge iz $p \,|\, |X|$ izpelji, da $p \,|\, |X_0|$. Zatem pokaži, da $(a_1, \ldots, a_p) \in X$ leži v X_0 natanko tedaj, ko je $a_1 = \cdots = a_p$. Ker $(1, \ldots, 1) \in X_0$, $|X_0| \neq 0$. Iz $p \,|\, |X_0|$ tako sledi, da obstajajo taki $(a, \ldots, a) \in X_0$, da $a \neq 1$. Za vsak tak a je $a^p = 1$ po definiciji X.

    Komentar. Iz tega dokaza je razvidno, da je število elementov $a \in G$ z lastnostjo $a^p = 1$ deljivo s p. To je koristno dopolnilo h Cauchyjevemu izreku.

14. Dokaži **prvi izrek Sylowa**: če je G končna grupa in p tako praštevilo, da p^k deli $|G|$ za neki $k \geq 0$, potem G vsebuje podgrupo reda p^k.

    Navodilo. Primer, ko je $|G| = 1$, je trivialen. Naj bo torej $|G| > 1$ in naj izrek velja za vse grupe z manjšim redom kot G. Tako smemo brez škode za splošnost predpostaviti, da iz $H \leq G$ in $H \neq G$ sledi $p^k \nmid |H|$. S pomočjo te predpostavke in razredne formule izpelji, da $p \mid |Z(G)|$. Po Cauchyjevem izreku $Z(G)$ vsebuje element c reda p. Z uporabo indukcijske predpostavke ugotovi, da kvocientna grupa $G/\langle c \rangle$ vsebuje

podgrupo reda p^{k-1}. Po izreku 4.19 jo lahko zapišemo kot $K/\langle c\rangle$, kjer je $K \leq G$. Iz Lagrangeovega izreka sledi $|K| = p^k$.

Komentar. Naj bo $|G| = p^m r$, kjer $p \nmid r$. Prvi izrek Sylowa pove, da ima G za vsak $k \leq m$ vsaj eno podgrupo reda p^k. Podgrupam reda p^m pravimo **podgrupe Sylowa**. **Drugi izrek Sylowa** pravi, da je vsaka podgrupa reda p^k vsebovana v kaki podgrupi Sylowa, poljubni podgrupi Sylowa H in K pa sta si konjugirani (tj. $K = aHa^{-1}$ za neki $a \in G$). **Tretji izrek Sylowa** pove, da število vseh podgrup Sylowa deli $|G|$ in je oblike $sp + 1$ za neki $s \geq 0$.

5.4. Končne Abelove grupe

Katere končne Abelove grupe poznamo? Najprej nam na misel pridejo končne ciklične grupe. Tudi direktni produkt končnega števila takih grup je končna Abelova grupa. Se lahko domislimo še kakega primera? Odgovor je, presenetljivo, da drugih ni. Pokazali bomo namreč, da je vsaka končna Abelova grupa direktni produkt cikličnih grup. Z dokazom, ki bo nekoliko daljši in zahtevnejši, se bomo prepričali, da kvocientne grupe in homomorfizmi grup niso zanimivi zgolj sami po sebi, ampak jih lahko s pridom uporabljamo.

Dogovorimo se, da bodo naše grupe v tem razdelku aditivne, tj. operacijo bomo označevali s $+$. Prednost tega označevanja je, da na možnost, da elementi med seboj ne komutirajo, niti ne pomislimo. Potrebno pa bo nekaj pozornosti glede oznak in terminologije. Tako na primer namesto $a^n = 1$ pišemo $na = 0$, red elementa a pa je najmanjše naravno število n s to lastnostjo. V skladu z dogovorom iz razdelka 4.5 izraz direktni produkt zamenjamo z direktno vsoto. Ker je vsaka končna ciklična grupa izomorfna grupi $(\mathbb{Z}_n, +)$, bomo torej pokazali, da je vsaka končna Abelova grupa izomorfna grupi oblike

$$\mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2} \oplus \cdots \oplus \mathbb{Z}_{n_r}. \tag{5.3}$$

To je osnovno, ne pa edino sporočilo tega razdelka. Podali bomo namreč popolno klasifikacijo končnih Abelovih grup. To pomeni, da bomo ugotovili, katere grupe oblike (5.3) so si med seboj izomorfne in katere si niso. Tega problema smo se že dotaknili v primeru 4.60. Tako vemo, da je

$$\mathbb{Z}_6 \cong \mathbb{Z}_3 \oplus \mathbb{Z}_2 \quad \text{in} \quad \mathbb{Z}_4 \ncong \mathbb{Z}_2 \oplus \mathbb{Z}_2.$$

Ali bi lahko uganili kako splošno pravilo, ki se skriva za tema opazkama? Delni odgovor daje naslednja lema. Najprej pa dogovor: v tem razdelku bomo z G ves čas označevali končno aditivno (seveda Abelovo) grupo.

LEMA 5.14. *Denimo, da je $|G| = mn$, kjer sta si števili m in n tuji. Potem sta množici*

$$H = \{x \in G \,|\, mx = 0\} \quad \textit{in} \quad K = \{x \in G \,|\, nx = 0\}$$

podgrupi grupe G in $G = H \oplus K$.

Dokaz. Zlahka preverimo, da sta H in K res podgrupi. Iz Lagrangeovega izreka smo izpeljali posledico 5.4, ki, prevedena v jezik aditivnih grup, pove, da je $(mn)x = 0$ za vse $x \in G$. Od tod razberemo, da je

$$nx \in H \text{ in } mx \in K \text{ za vsak } x \in G. \tag{5.4}$$

Ker sta si števili m in n tuji, obstajata taki celi števili u in v, da je $vn+um = 1$ (posledica 2.5). Zato je

$$x = v(nx) + u(mx) \text{ za vsak } x \in G, \tag{5.5}$$

kar v luči (5.4) dokazuje, da je $G = H + K$. Če je $x \in H \cap K$, je $mx = nx = 0$ in tako iz (5.5) sledi $x = 0$. Torej je $H \cap K = \{0\}$ in G je res (notranja) direktna vsota svojih podgrup H in K. □

Primer 5.15. Formulo $\mathbb{Z}_6 \cong \mathbb{Z}_3 \oplus \mathbb{Z}_2$ lahko zdaj posplošimo. Hitro se prepričamo, da je

$$\{x \in \mathbb{Z}_{mn} \mid mx = 0\} = \{0, n, 2n, \ldots, (m-1)n\} \cong \mathbb{Z}_m;$$

izomorfizem je podan s $kn \mapsto k$. Podobno je $\{x \in \mathbb{Z}_{mn} \mid nx = 0\} \cong \mathbb{Z}_n$. Od tod in iz leme 5.14 izpeljemo, da je

$$\mathbb{Z}_{mn} \cong \mathbb{Z}_m \oplus \mathbb{Z}_n,$$

če sta si seveda števili m in n tuji. Lahko pa to dokažemo tudi neposredno, brez uporabe leme 5.14 (glej nalogo 3.1/8).

Naredimo korak naprej v smeri, ki jo nakazuje lema 5.14.

Lema 5.16. *Denimo, da je* $|G| = p_1^{k_1} p_2^{k_2} \cdots p_s^{k_s}$, *kjer so* p_i *različna praštevila in* k_i *naravna števila. Potem je*

$$G = H_1 \oplus H_2 \oplus \cdots \oplus H_s,$$

kjer je H_i p_i*-grupa in* $|H_i| = p_i^{k_i}$.

Dokaz. Lema 5.14 pove, da je $G = H_1 \oplus K$, kjer je

$$H_1 = \{x \in G \mid p_1^{k_1} x = 0\} \text{ in } K = \{x \in G \mid p_2^{k_2} \cdots p_s^{k_s} x = 0\}.$$

Iz definicije H_1 (in opombe 5.2 (a)) je očitno, da je H_1 p_1-grupa. Po posledici 5.13 je $|H_1|$ potenca števila p_1. Trdimo, da $p_1 \nmid |K|$. Če to ne bi bilo res, bi namreč po Cauchyjevem izreku podgrupa K vsebovala element reda p_1 in bi zato (spet po opombi 5.2 (a)) število p_1 delilo število $p_2^{k_2} \cdots p_s^{k_s}$. Ker je

$$|G| = |H_1 \oplus K| = |H_1| \cdot |K|,$$

je edina možnost, da je $|H_1| = p_1^{k_1}$ in $|K| = p_2^{k_2} \cdots p_s^{k_s}$. Na enak način sedaj lahko obravnavamo grupo K. Po končnem številu korakov očitno pridemo do želenega zaključka. □

PRIMER 5.17. Denimo, da je $|G| = 30 = 5 \cdot 3 \cdot 2$. Iz leme 5.16 in posledice 5.6 takoj sledi, da je $G \cong \mathbb{Z}_5 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_2$. Po drugi strani pa zaenkrat ne moremo še nič reči o Abelovi grupi z npr. $8 = 2^3$ elementi.

Preostal nam je študij Abelovih p-grup. Take grupe vsebujejo podgrupe reda p. To namreč sledi iz Cauchyjevega izreka, saj element reda p porodi ciklično podgrupo reda p. Naslednja lema obravnava primer, ko je taka podgrupa ena sama.

LEMA 5.18. *Naj bo G p-grupa. Potem je G ciklična natanko tedaj, ko ima eno samo podgrupo reda p.*

DOKAZ. Če je G ciklična, je izomorfna grupi $\mathbb{Z}_{p^m}$ za neki $m \geq 1$. Njene edine podgrupe so oblike $p^k\mathbb{Z}_{p^m}$, $0 \leq k \leq m$ (gl. primer 4.20). Natanko ena izmed njih, namreč $p^{m-1}\mathbb{Z}_{p^m}$, ima red p.

Dokažimo še obratno trditev. Privzemimo torej, da ima G natanko eno podgrupo reda p. Dokazati želimo, da je G ciklična. Če je $|G| = p$, to očitno velja (gl. posledico 5.6). Zato smemo predpostaviti, da je $|G| > p$ in da želeni zaključek velja za vse p-grupe, ki imajo manj elementov kot G. Označimo (edino) podgrupo reda p z N. Seveda imajo vsi od 0 različni elementi iz N red p, in obratno, vsak element reda p iz G leži v N, saj generira podgrupo reda p. Torej je

$$N = \{x \in G \mid px = 0\}.$$

Povedano drugače, N je jedro endomorfizma φ grupe G, podanega s predpisom

$$\varphi(x) = px.$$

Po izreku o izomorfizmu (izrek 4.40) je

$$G/N \cong \operatorname{im} \varphi.$$

Ker $N \neq \{0\}$, ima G/N, in zato tudi $\operatorname{im} \varphi$, manj elementov kot G. Podgrupe grupe $\operatorname{im} \varphi$ so seveda hkrati podgrupe grupe G. Zato $\operatorname{im} \varphi$ ne more imeti več kot ene podgrupe reda p, vsaj eno pa ima po Cauchyjevem izreku. Torej ima natanko eno tako podgrupo in iz indukcijske predpostavke sledi, da je grupa $\operatorname{im} \varphi$ ciklična. Zato je ciklična tudi grupa G/N. Naj bo $a \in G$ tak, da element $a + N$ generira grupo G/N. Vsak element $g + N$, kjer je $g \in G$, je torej oblike

$$k(a + N) = ka + N$$

za neki $k \in \mathbb{Z}$. Torej je $g - ka \in N$, kar dokazuje, da je

$$G = \langle a \rangle + N.$$

Ker je $|G| > p = |N|$, je $\langle a \rangle$ netrivialna podgrupa grupe G. Kot p-grupa ima po Cauchyevem izreku element reda p. Toda potem je $N \subseteq \langle a \rangle$ in zato $G = \langle a \rangle$. S tem smo dokazali, da je G ciklična. □

Iz linearne algebre vemo, da za vsak podprostor U vektorskega prostora V obstaja tak podprostor W, da je $V = U \oplus W$. V grupah kaj podobnega ne velja. Denimo, za podgrupo $H = \{0, 2\}$ grupe $\mathbb{Z}_4$ ne obstaja taka podgrupa K, da bi veljalo $\mathbb{Z}_4 = H \oplus K$. Naslednja lema torej ni očitna.

LEMA 5.19. *Naj bo G p-grupa. Če je C njena ciklična podgrupa, ki ima med vsemi cikličnimi podgrupami največji red, potem G vsebuje tako podgrupo K, da je $G = C \oplus K$.*

DOKAZ. Privzeti smemo, da G ni ciklična (sicer vzamemo $K = \{0\}$). Torej je $|G| > p$. Kot v prejšnjem dokazu lahko privzamemo, da lema velja za vse p-grupe, ki imajo manj elementov kot G. Po lemi 5.18 ima G vsaj dve podgrupi reda p, medtem ko ima C natanko eno. Naj bo N podgrupa reda p, ki ni vsebovana v C. Ker N ne vsebuje pravih netrivialnih podgrup (posledica 5.7), je $C \cap N = \{0\}$. Od tod sledi, da je s predpisom $c \mapsto c + N$ definiran izomorfizem iz C v $(C + N)/N$. Torej je

$$C \cong (C + N)/N.$$

Trdimo, da ima ciklična grupa $(C+N)/N$ izmed vseh cikličnih podgrup grupe G/N največji red. Res, največji red cikličnih podgrup grupe je enak največjemu redu elementov te grupe, red vsakega elementa $x \in G$ pa je kvečjemu večji kot red elementa $x + N \in G/N$ (gl. opombo 5.2 (d)). Po predpostavki zato obstaja taka podgrupa L grupe G/N, da je grupa G/N direktna vsota svojih podgrup $(C + N)/N$ in L. Izrek 4.19 pove, da je L oblike $L = K/N$ za neko podgrupo K grupe G, ki vsebuje N. Iz enakosti

$$G/N = \big((C + N)/N\big) \oplus K/N$$

takoj izpeljemo, da je $G = C + N + K$; ker pa K vsebuje N, je G enaka že vsoti podgrup C in K. Dokazati moramo še, da je $C \cap K = \{0\}$. Denimo, da to ni res. Izberimo neničeln element $x \in C \cap K$. Iz $C \cap N = \{0\}$ sledi $x \notin N$, zato je $x + N$ neničeln element preseka podgrup $(C + N)/N$ in K/N. To je protislovje, saj je vsota teh dveh podgrup direktna. □

Naposled smo prišli do **osnovnega izreka o končnih Abelovih grupah**.

IZREK 5.20. *Vsaka končna Abelova grupa G je direktna vsota cikličnih podgrup. Če je G netrivialna, te podgrupe lahko izberemo tako, da je red vsake izmed njih potenca praštevila.*

DOKAZ. V luči leme 5.16 zadošča obravnavati primer, ko je G p-grupa. Po lemi 5.19 je zato G direktna vsota ciklične podgrupe C in neke podgrupe K, ki ima seveda manjši red kot G. Po isti lemi lahko na enak način razstavimo podgrupo K. Postopek ponavljamo in po končnem številu korakov pridemo do želenega zapisa. □

Izrek seveda govori o notranji direktni vsoti. Ker je ciklična grupa z n elementi izomorfna grupi $\mathbb{Z}_n$, ga lahko povemo tudi takole: vsaka končna Abelova grupa je izomorfna zunanji direktni vsoti (5.3), pri čemer za n_i lahko izberemo potence praštevil. Katere izmed njih so si med seboj izomorfne? Najprej razmislimo, da se tudi pri tem vprašanju lahko omejimo na p-grupe. Naj bosta G in G' izomorfni končni Abelovi grupi. Potem imata isto število elementov, zato ju po lemi 5.16 lahko zapišemo kot

$$G = H_1 \oplus \cdots \oplus H_s \text{ in } G' = H_1' \oplus \cdots \oplus H_s',$$

kjer so H_i, H_i' p_i-grupe za neka (različna) praštevila $p_1, \ldots, p_s$. Velja tudi $|H_i| = |H_i'|$. Če je φ izomorfizem iz G v G' in je $h_i \in H_i$, je $\varphi(h_i) \in H_i'$. Namreč, red elementa h_i je potenca praštevila p_i, zato isto velja za $\varphi(h_i)$, edini elementi iz G' s to lastnostjo pa so tisti iz H_i'. Ker je φ injektivna preslikava, množici H_i in H_i' pa imata isto moč, mora veljati $\varphi(H_i) = H_i'$. Torej je

$$H_i \cong H_i', \quad i = 1, \ldots, s.$$

Zato moramo samo razvozlati, katere p_i-grupe so si med seboj izomorfne. To bomo naredili v naslednjem izreku. Zaradi preglednejšega zapisa bomo grupi v izreku predstavili v obliki

$$\mathbb{Z}_{p^{k_1}} \oplus \cdots \oplus \mathbb{Z}_{p^{k_u}}, \text{ kjer je } k_1 \geq \cdots \geq k_u.$$

Po izreku 5.20 je namreč vsaka p-grupa izomorfna taki grupi. Obenem smo tu upoštevali, da za grupe nasploh velja $G_1 \oplus G_2 \cong G_2 \oplus G_1$. Vrstni red sumandov v direktni vsoti zato lahko poljubno izberemo.

Izrek 5.21. *Naj bo p praštevilo. Če za naravna števila $k_1 \geq \cdots \geq k_u$ in $\ell_1 \geq \cdots \geq \ell_v$ velja*

$$\mathbb{Z}_{p^{k_1}} \oplus \cdots \oplus \mathbb{Z}_{p^{k_u}} \cong \mathbb{Z}_{p^{\ell_1}} \oplus \cdots \oplus \mathbb{Z}_{p^{\ell_v}},$$

potem je $u = v$ in $k_i = \ell_i$ za vsak i.

Dokaz. Označimo prvo grupo z G, drugo pa z G'. Red obeh je p^n, kjer je

$$n = k_1 + \cdots + k_u = \ell_1 + \cdots + \ell_v. \tag{5.6}$$

Izrek bomo dokazali z indukcijo na n. Za $n = 1$ je trditev očitna, zato privzemimo, da je $n > 1$ in da izrek velja za vse grupe reda manj kot p^n. Za poljubno Abelovo p-grupo K bomo pisali $pK := \{px \mid x \in K\}$. Bralec naj razmisli, da je

$$p\mathbb{Z}_{p^m} \cong \mathbb{Z}_{p^{m-1}}$$

(če je $m = 1$, je to trivialna grupa $\{0\}$). Seveda je $pG \cong pG'$ in tako

$$\mathbb{Z}_{p^{k_1-1}} \oplus \cdots \oplus \mathbb{Z}_{p^{k_w-1}} \cong \mathbb{Z}_{p^{\ell_1-1}} \oplus \cdots \oplus \mathbb{Z}_{p^{\ell_z-1}},$$

pri čemer je w največje število, za katerega je $k_w > 1$, z pa največje število, za katerega je $\ell_z > 1$. Iz indukcijske predpostavke sledi, da je $w = z$ in $k_i - 1 = \ell_i - 1$ za $i = 1, \ldots, w$. Torej se k_i in ℓ_i ujemata na prvih w mestih. Preostal nam je le še dokaz, da je $u = v$, tj. dokaz, da G in G' vsebujeta isto število kopij grupe $\mathbb{Z}_p$. To pa sledi takoj iz (5.6), če upoštevamo, da je $k_i = \ell_i$ za $i = 1, \ldots, w = z$. □

Oba izreka skupaj podajata klasifikacijo končnih Abelovih grup.

PRIMER 5.22. Določimo – seveda do izomorfizma natančno – vse Abelove grupe reda 200. Ker je $200 = 5^2 \cdot 2^3$, lahko vsako tako grupo predstavimo kot $H \oplus K$, kjer je H 5-grupa reda 25 in K 2-grupa reda 8. Za H imamo dve možnosti, $\mathbb{Z}_{25}$ in $\mathbb{Z}_5 \oplus \mathbb{Z}_5$, za K pa tri: $\mathbb{Z}_8$, $\mathbb{Z}_4 \oplus \mathbb{Z}_2$ in $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$. Poljubna Abelova grupa reda 200 je torej izomorfna eni izmed grup

$$\mathbb{Z}_{25} \oplus \mathbb{Z}_8, \quad \mathbb{Z}_{25} \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_2, \quad \mathbb{Z}_{25} \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2,$$

$$\mathbb{Z}_5 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_8, \quad \mathbb{Z}_5 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_2, \quad \mathbb{Z}_5 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2.$$

Vse končne Abelove grupe lahko torej opišemo s pomočjo cikličnih grup. Tudi grupa celih števil $\mathbb{Z}$ je ciklična. Grupa $\mathbb{Z} \oplus \mathbb{Z}$ seveda ni ciklična, je pa *končno generirana*. Generirata jo na primer elementa $(1, 0)$ in $(0, 1)$. Prav tako je končno generirana grupa $\mathbb{Z}^m$, ki jo definiramo kot direktno vsoto m kopij grupe $\mathbb{Z}$. **Osnovni izrek o končno generiranih Abelovih grupah** pravi, da je vsaka taka grupa direktna vsota končnega števila cikličnih grup. Z drugimi besedami, izomorfna je grupi oblike

$$\mathbb{Z}^m \oplus \mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2} \oplus \cdots \oplus \mathbb{Z}_{n_r}.$$

Za dokaz bi bilo potrebno malo več truda kot za dokaz izreka 5.20.

Naloge

1. Ali je $\mathbb{Z}_{12} \cong \mathbb{Z}_4 \oplus \mathbb{Z}_3$? Ali je $\mathbb{Z}_{12} \cong \mathbb{Z}_6 \oplus \mathbb{Z}_2$?
2. Pokaži, da je $\mathbb{Z}_{36} \oplus \mathbb{Z}_{24} \cong \mathbb{Z}_{72} \oplus \mathbb{Z}_{12}$.
3. Pokaži, da je $\mathbb{Z}_{78} \oplus \mathbb{Z}_{18} \cong \mathbb{Z}_{26} \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_6$.
4. Pokaži, da je
$$\mathbb{Z}_{11} \oplus \mathbb{Z}_{25} \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_2 \cong \mathbb{Z}_{9900} \oplus \mathbb{Z}_{90} \oplus \mathbb{Z}_3.$$
5. Pokaži, da je vsaka končna Abelova grupa izomorfna grupi oblike
$$\mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2} \oplus \cdots \oplus \mathbb{Z}_{n_r},$$
kjer $n_{i+1} \mid n_i$ za vse $i = 1, \ldots, r - 1$.
Namig. Prejšnja naloga obravnava poseben primer.
6. Določi (do izomorfizma natančno) vse Abelove grupe reda 324.

7. Določi število neizomorfnih Abelovih grup reda:
   (a) $16 = 2^4$.
   (b) $32 = 2^5$.
   (c) $42336 = 7^2 \cdot 3^3 \cdot 2^5$.
   (d) $211680 = 7^2 \cdot 5 \cdot 3^3 \cdot 2^5$.
8. Koliko elementov reda 2, 4 in 8 imajo Abelove grupe reda 8, torej grupe $\mathbb{Z}_8$, $\mathbb{Z}_4 \oplus \mathbb{Z}_2$ in $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$?
9. Za vsak $n \in \mathbb{N}$ je $\mathbb{Z}_n^*$, grupa obrnljivih elementov kolobarja $(\mathbb{Z}_n, +, \cdot)$, končna Abelova grupa. Kateri grupi oblike (5.3) je grupa $\mathbb{Z}_n^*$ izomorfna, če je:
   (a) $n = 5$.
   (b) $n = 8$.
   (c) $n = 10$.
   (d) $n = 16$.

   Komentar. Z osnovnim znanjem o ničlah polinomov lahko z izsledki tega razdelka pokažemo, da je za vsako praštevilo p grupa $\mathbb{Z}_p^*$ ciklična (povedati se da še več, gl. nalogo 7.7/7).
10. Pokaži, da ima ciklična p-grupa $\mathbb{Z}_{p^n}$ za vsak $k \leq n$ natanko eno ciklično podgrupo reda p^k in da so to tudi njene edine podgrupe.

    Komentar. To je poseben primer naloge 3.1/10.
11. Denimo, da je red končne Abelove grupe G deljiv s pq, kjer sta p in q različni praštevili. Pokaži, da G vsebuje ciklično podgrupo reda pq. Ali to velja tudi, kadar je $p = q$?
12. Naj bodo G, H in H' končne Abelove grupe. Pokaži, da iz $G \oplus H \cong G \oplus H'$ sledi $H \cong H'$.

    Komentar. Namen naloge je prikazati uporabnost osnovnega izreka o končnih Abelovih grupah. Z drugačnimi metodami se da sicer pokazati precej več. Na primer, dovolj je privzeti, da je G končna (ne nujno Abelova) grupa, H in H' pa sta lahko poljubni. Brez vseh omejitev pa vseeno ne gre. Na primer, če je G aditivna grupa vseh realnih zaporedij, je $G \cong G \oplus G$, torej $G \oplus \{0\} \cong G \oplus G$. Tu grupe G seveda ne moremo »okrajšati«.
13. Naj bodo p_i, $i = 1, \ldots, s$, različna praštevila in naj bodo H_i, $i = 1, \ldots, s$, Abelove p_i-grupe. Pokaži, da je grupa $H_1 \oplus \cdots \oplus H_s$ ciklična natanko tedaj, ko so ciklične vse grupe H_i, $i = 1, \ldots, s$.
14. Pokaži, da so za končno Abelovo grupo G naslednji pogoji ekvivalentni:
   (i) G je ciklična.
   (ii) Za vsako praštevilo p velja: če p deli $|G|$, potem G vsebuje $p - 1$ elementov reda p.
   (iii) G vsebuje manj kot $p^2 - 1$ elementov reda p za vsako praštevilo p.

(iv) Nobena podgrupa G ni izomorfna grupi $\mathbb{Z}_p \oplus \mathbb{Z}_p$ za kako praštevilo p.

15. Pokaži, da vsaka Abelova grupa reda 200 vsebuje podgrupo reda 20.

16. Naj bo sedaj G poljubna končna Abelova grupa in $m \in \mathbb{N}$ poljubno število, ki deli $|G|$. Pokaži, da G vsebuje podgrupo reda m.

Komentar. V končnih Abelovih grupah torej velja obrat Lagrangeovega izreka, za razliko od splošnih končnih grup (gl. nalogo 5.1/14).

17. Naj bo K kolobar. Pokaži:
(a) Če je $|K| = p$ za neko praštevilo p, je K izomorfen kolobarju $\mathbb{Z}_p$.
(b) Če je aditivna grupa $(K, +)$ ciklična, je K komutativen.
(c) Če je $|K| = p^2$ za neko praštevilo p, je K komutativen.
Iz teh ugotovitev sklepaj, da so vsi kolobarji z manj kot 8 elementi komutativni. Poišči kak nekomutativen kolobar z 8 elementi!

Namig. Centralizator vsakega elementa kolobarja je podgrupa za seštevanje. To lahko pomaga pri dokazu (c). Pri iskanju nekomutativnih kolobarjev najprej pomislimo na matrične kolobarje. Če je K končen kolobar, je $|M_2(K)| = |K|^4$ (zakaj?). Kolobar vseh matrik velikosti 2×2 torej ne more imeti 8 elementov. Išči med njegovimi podkolobarji!

POGLAVJE 6

Deljivost v komutativnih kolobarjih

V razdelku 2.1 smo obravnavali pojem deljivosti v kolobarju celih števil. Glavni namen tega poglavja je pokazati, da rezultati, ki smo jih izpeljali, veljajo tudi v nekaterih splošnejših komutativnih kolobarjih, med drugim v kolobarju polinomov nad poljem. V zadnjem razdelku se bomo seznanili še s klasičnimi rezultati o nerazcepnih polinomih. To so nekonstantni polinomi, ki jih ne moremo zapisati kot produkt polinomov nižje stopnje.

Nekatere rezultate tega poglavja bomu uporabili pri študiju ničel polinomov v naslednjem poglavju.

6.1. Glavni ideali

Naj bo K komutativen kolobar in a njegov element. Množica

$$(a) := \{ax \,|\, x \in K\}$$

je ideal kolobarja K. Res je podgrupa za seštevanje (saj je $ax - ay = a(x-y) \in (a)$) in produkt elementa iz (a) z elementom iz K očitno leži v (a) (ker je K komutativen, lahko množimo z leve ali z desne). Seveda (a) vsebuje element a. Vsak ideal kolobarja K, ki vsebuje a, očitno mora vsebovati tudi ideal (a). Torej je (a) **ideal, generiran z elementom** a, tj. najmanjši ideal, ki vsebuje a. Vsak ideal oblike (a) za neki $a \in K$ imenujemo **glavni ideal**. Povedano drugače, ideal je glavni ideal, če je generiran z enim samim elementom.

Opomba 6.1. Če je K poljuben, ne nujno komutativen kolobar, je množica $\{ax \,|\, x \in K\}$ *desni ideal*, generiran z elementom a. Označujemo ga z aK. *Levi ideal*, generiran z a je seveda množica $Ka := \{xa \,|\, x \in K\}$. *Dvostranski ideal*, generiran z a pa sestoji iz vseh elementov oblike

$$x_1 a y_1 + \cdots + x_n a y_n,$$

kjer so $x_i, y_i \in K$. Označimo ga s KaK ali pa z (a). Tudi zanj uporabljamo izraz glavni ideal. Vendar se bomo v tem poglavju ukvarjali le s komutativnimi kolobarji, kjer vse omenjene množice sovpadajo, torej $aK = Ka = KaK = (a)$.

Povrnimo se k oznakam in terminologiji pred opombo 6.1. Sledi nekaj preprostih zgledov glavnih idealov.

PRIMER 6.2. Ideala $\{0\}$ in K sta glavna. Prvi je generiran z elementom 0, drugi z elementom 1 oziroma s katerimkoli obrnljivim elementom. Pravzaprav velja

$$(a) = K \iff a \text{ je obrnljiv.} \tag{6.1}$$

Namreč, iz $(a) = K$ sledi, da je enačba $ax = 1$ rešljiva in in zato mora biti a obrnljiv.

Če je K polje, sta $\{0\}$ in K tudi edina ideala. Polja torej imajo lastnost, da so vsi njihovi ideali glavni. Vendar nas polja v tem poglavju ne bodo res zanimala. Pozornost usmerimo v cele kolobarje, torej komutativne kolobarje brez deliteljev niča, ki niso polja.

PRIMER 6.3. Za poljuben $n \in \mathbb{N} \cup \{0\}$ je ideal $n\mathbb{Z}$ kolobarja $\mathbb{Z}$ glavni. Generiran je seveda s številom n, torej $n\mathbb{Z} = (n)$. Ker so to edini ideali kolobarja $\mathbb{Z}$ (gl. primer 4.23), je torej vsak ideal v $\mathbb{Z}$ glavni.

Kolobar $\mathbb{Z}$ bomo tudi v nadaljevanju uporabljali kot osnovni zgled, ki nam bo pomagal razjasniti teorijo. Primer, ki je v središču našega zanimanja, pa je kolobar polinomov ene spremenljivke nad poljem. Označevali ga bomo s $F[X]$, kjer je seveda F polje.

PRIMER 6.4. Naj bo I množica vseh polinomov iz $F[X]$, ki imajo konstantni člen enak 0. Očitno je I ideal. Ker je $f(X) \in I$ natanko tedaj, ko ga lahko zapišemo kot $f(X) = Xg(X)$ za neki polinom $g(X)$, je $I = (X)$ in je torej glavni ideal (gl. tudi primer 4.50). Kasneje bomo videli, da so vsi ideali kolobarja $F[X]$ glavni.

Nekoliko splošnejši kot glavni ideali so **končno generirani ideali**, torej ideali, generirani s končno mnogo elementi. Naj bo K poljuben komutativen kolobar in naj bodo $a_1, \ldots, a_n$ njegovi elementi. Ideal, generiran s temi elementi označujemo z $(a_1, \ldots, a_n)$. Seveda vsebuje vse glavne ideale (a_i) in zato tudi njihovo vsoto $(a_1) + \cdots + (a_n)$. Ker je kot vsota idealov ta množica sama ideal in ker vsebuje vse elemente a_i, dejansko velja

$$(a_1, \ldots, a_n) = (a_1) + \cdots + (a_n).$$

Torej $(a_1, \ldots, a_n)$ sestoji iz vseh elementov oblike $a_1x_1 + \cdots + a_nx_n$, kjer so $x_i \in K$. Na kratko: končno generiran ideal je končna vsota glavnih idealov.

PRIMER 6.5. Ideal kolobarja $\mathbb{Z}$, generiran z elementoma 4 in 6 je torej $(4, 6) = 4\mathbb{Z} + 6\mathbb{Z}$. Ker je vsak ideal kolobarja $\mathbb{Z}$ glavni, lahko ta generatorja nadomestimo z enim samim. Res, elementi tega ideala so vsa soda števila, zato je $(4, 6) = (2)$.

PRIMER 6.6. V primeru 6.4 smo omenili, da je vsak ideal kolobarja polinomov nad poljem glavni. Za kolobar polinomov $\mathbb{Z}[X]$ to ne velja. Oglejmo

si na primer ideal $(2, X)$. Njegovi elementi so vsi polinomi iz $\mathbb{Z}[X]$, katerih prosti člen je sodo celo število. Denimo, da obstaja tak polinom $f(X) \in \mathbb{Z}[X]$, da je $(2, X) = (f(X))$. Iz $2 \in (f(X))$ sledi, da je $f(X)$ konstanten polinom a_0. Ker pripada idealu $(2, X)$, je a_0 sodo število. Toda to je v nasprotju z $X \in (f(X))$. Ideal $(2, X)$ torej ni glavni.

PRIMER 6.7. Kot v primeru 6.4 naj bo I množica vseh polinomov s konstantnim členom 0, a tokrat obravnavajmo polinome v dveh spremenljivkah X in Y; torej je $I \subseteq F[X, Y]$. Vsak polinom iz I lahko lahko zapišemo kot

$$X f_1(X, Y) + Y f_2(X, Y),$$

polinomi te oblike pa imajo konstantni člen enak 0. Zato je $I = (X, Y)$. Ali lahko generatorja X in Y nadomestimo z enim samim generatorjem? Denimo, da bi to bilo res. Potem bi obstajal tak polinom $f(X, Y)$, da bi bil I enak $(f(X, Y))$. Tako bi za neka polinoma $g_1(X, Y)$ in $g_2(X, Y)$ veljalo

$$X = g_1(X, Y) f(X, Y) \quad \text{in} \quad Y = g_2(X, Y) f(X, Y).$$

Bralec naj razmisli, da je to možno le tedaj, ko je $f(X, Y)$ konstanten polinom. Toda to je v nasprotju z $I \subsetneq F[X, Y]$. Torej I ni glavni ideal.

Naloge

1. Pokaži, da je $\{m + ni \in \mathbb{Z}[i] \mid m + n \in 2\mathbb{Z}\}$ glavni ideal kolobarja Gaussovih celih števil $\mathbb{Z}[i]$ in poišči njegov generator.
2. Naj bo K poljuben kolobar. Pokaži, da je množica vseh takih polinomov v $K[X]$, da je vsota vseh njihovih koeficientov enaka 0, glavni ideal kolobarja $K[X]$ in poišči njegov generator.
3. Naj bo F polje. Pokaži, da so vsi ideali kolobarja formalnih potenčnih vrst $F[[X]]$ oblike (X^n) za neki $n \geq 0$ (in so torej glavni ideali).

   Namig. Naloga 2.6/15.
4. Naj bo K cel kolobar, ki ni polje. Pokaži, da kolobar $K[X]$ vsebuje ideal, ki ni glavni.

   Komentar. To je posplošitev ugotovitev iz primerov 6.6 in 6.7. V prvem je K kolobar celih števil, v drugem pa je K kolobar polinomov nad poljem (kolobar $F[X, Y]$ smo namreč definirali kot $(F[Y])[X]$).
5. Naj bo I množica vseh realnih zaporedij, ki imajo le končno mnogo od 0 različnih členov. Pokaži, da je I ideal kolobarja vseh realnih zaporedij (primer 1.89), ki ni končno generiran.
6. Glavni ideal I iz primera 6.4 lahko opišemo kot množico vseh polinomov $f(X)$ z lastnostjo, da je $f(0) = 0$. Naj bo sedaj $\mathcal{F}$ kolobar vseh funkcij iz $\mathbb{R}$ v $\mathbb{R}$. Pokaži, da je množica $J = \{f \in \mathcal{F} \mid f(0) = 0\}$ glavni ideal

kolobarja $\mathcal{F}$ in poišči njegov generator. Pokaži tudi, da množica $L = \{f \in C(\mathbb{R}) \mid f(0) = 0\}$ ni glavni ideal kolobarja zveznih funkcij $C(\mathbb{R})$. Še več, L ni niti končno generiran.

Namig. Iz $f_1, \ldots, f_n \in L$ sledi $\sqrt{|f_1| + \cdots + |f_n|} \in L$.

6.2. Deljivost in nerazcepnost

Od idealov preidimo na temo, ki je samo na prvi pogled povsem drugačna. Pričnimo z definicijo, ki jo sicer dobro poznamo – toda morda le v kolobarju celih števil.

Definicija 6.8. Pravimo, da element $b \neq 0$ iz komutativnega kolobarja K **deli** element $a \in K$, kar pišemo kot $b \mid a$, če obstaja tak element $q \in K$, da je $a = qb$. V tem primeru tudi rečemo, da je b **delitelj** a ali da je a **deljiv** z b.

Relacijo deljivosti lahko izrazimo z inkluzijo glavnih idealov:

$$b \mid a \iff (a) \subseteq (b). \tag{6.2}$$

Res, iz $a = qb$ sledi $ax \in (b)$ za vse $x \in K$, in iz $(a) \subseteq (b)$ sledi $a \in (b)$ in zato $a = qb$ za neki $q \in K$. Čeprav je (6.2) samo trivialna opazka, je ključnega pomena za nadaljevanje. Kot poseben primer velja

$$b \mid a \text{ in } a \mid b \iff (a) = (b). \tag{6.3}$$

Za elementa, ki zadoščata pogoju (6.3), bomo rekli, da sta si **asociirana**. V celih kolobarjih, torej neničelnih komutativnih kolobarjih brez deliteljev niča, lahko ta pojem opišemo še jasneje.

Trditev 6.9. *Neničelna elementa a in b celega kolobarja K sta si asociirana natanko tedaj, ko obstaja tak obrnljiv element $u \in K$, da je $a = ub$.*

Dokaz. Če sta si a in b asociirana, je $a = ub$ in $b = va$ za neka $u, v \in K$. Iz obojega sledi $a = uva$ in zato $(1 - uv)a = 0$. Ker je K cel in $a \neq 0$, mora biti $uv = 1$. Torej je u obrnljiv. Obratno, iz $a = ub$, kjer je u obrnljiv, sledi $b = u^{-1}a$, torej sta si a in b asociirana. □

Primer 6.10. Ker sta 1 in -1 edina obrnljiva elementa kolobarja $\mathbb{Z}$, sta si neničelni celi števili asociirani natanko tedaj, ko se razlikujeta kvečjemu za predznak.

Primer 6.11. Ker je stopnja produkta polinomov enaka vsoti stopenj, polinoma $u(X), v(X) \in F[X]$ lahko zadoščata $u(X)v(X) = 1$ le tedaj, ko imata stopnjo 0. Edini obrnljivi elementi kolobarja $F[X]$, kjer je F polje, so torej neničelni konstantni polinomi. Neničelna polinoma $f(X)$ in $g(X)$ sta si torej asociirana natanko tedaj, ko je $f(X) = ug(X)$ za neki $u \in F \setminus \{0\}$.

Kot se hitro prepričamo, imata asociirana elementa iste delitelje in sta delitelja istih elementov. Z vidika teorije deljivosti elementov ju zato lahko identificiramo. Zgornja primera pokažeta, da sta v obeh za nas najbolj zanimivih primerih asociirana elementa res »skoraj« enaka.

Tudi pojem največjega skupnega delitelja lahko iz celih števil prenesemo v komutativne kolobarje.

Definicija 6.12. Naj bo K komutativen kolobar in naj bosta a in b njegova elementa, ne oba enaka 0. Element $d \neq 0$ iz K se imenuje **največji skupni delitelj** a in b, če izpolnjuje naslednja pogoja:

(a) $d \mid a$ in $d \mid b$.
(b) Če je $c \neq 0$ iz K tak, da $c \mid a$ in $c \mid b$, potem $c \mid d$.

Če je največji skupni delitelj elementov a in b enak 1, pravimo, da sta si a in b **tuja**.

Največji skupni delitelj ne obstaja vedno, tudi v celih kolobarjih ne. Če obstaja, pa običajno ni en sam. Res pa, kot sledi iz definicije, različna največja skupna delitelja istega para elementov drug drugega delita in sta si torej asociirana. Pri študiju problemov, povezanih z deljivostjo, pa med asociiranimi elementi dejansko ne ločujemo. Zato v nekem smislu največji skupni delitelj vendarle je enolično določen. V nekaterih konkretnih kolobarjih zgornjo definicijo dopolnimo in dosežemo »pravo« enoličnost. V kolobarju celih števil tako zahtevamo, da je največji skupni delitelj naravno število, v kolobarju polinomov $F[X]$ pa, da ima največji skupni delitelj vodilni koeficient enak 1 (kot je razvidno iz primera 6.11, je s tem enolično določen).

O obstoju največjega skupnega delitelja dveh celih števil govori posledica 2.3. Če dokaz »preoblečemo« v jezik, ki smo ga sedaj vpeljali, dobimo tole trditev.

Trditev 6.13. *Naj bo K komutativen kolobar in naj bosta a in b njegova elementa, ne oba enaka 0. Če je ideal (a, b) glavni, potem največji skupni delitelj elementov a in b obstaja in je oblike $d = ax + by$ za neka $x, y \in K$.*

Dokaz. Po predpostavki obstaja tak element $d \in K$, da je

$$(a, b) = (d).$$

Iz $a, b \in (d)$ sledi $d \mid a$ in $d \mid b$. Ker $d \in (a, b)$, ga lahko zapišemo kot $d = ax + by$ za neka $x, y \in K$. Če $c \mid a$ in $c \mid b$, torej če je $a = cz$ in $b = cw$ za neka $z, w \in K$, potem je

$$d = c(zx + wy)$$

in tako $c \mid d$. To dokazuje, da je d največji skupni delitelj a in b. □

Iz dokaza vidimo, da je največji skupni delitelj elementov a in b katerikoli element d, za katerega velja $(a, b) = (d)$. Omenimo še, da največji skupni

delitelj lahko obstaja tudi tedaj, ko ideal (a, b) ni glavni. Denimo, največji skupni delitelj elementov 2 in X kolobarja $\mathbb{Z}[X]$ je enak 1, vendar ideal $(2, X)$ ni glavni (gl. primer 6.6).

Tudi pojem praštevila lahko razširimo na komutativne kolobarje.

Definicija 6.14. Element p komutativnega kolobarja K je **nerazcepen**, če $p \neq 0$, p ni obrnljiv in če iz $p = ab$ sledi, da je eden izmed elementov a in b obrnljiv. Elementu, ki ni enak 0, ni obrnljiv in ni nerazcepen, pravimo **razcepen** element.

Primer 6.15. Poleg praštevil so v kolobarju $\mathbb{Z}$ nerazcepni elementi tudi nasprotne vrednosti praštevil.

Pojem nerazcepnosti je posebej zanimiv v kolobarju polinomov $F[X]$, a več o tem kasneje. Zaključimo razdelek s karakterizacijo nerazcepnih elementov v celih kolobarjih. Omejitev na take kolobarje je pri obravnavi deljivosti in sorodnih pojmov običajna. Pri samih definicijah ta omejitev ni bila potrebna, pri študiju pa pride zelo prav.

Trditev 6.16. *Naj bo K cel kolobar in naj bo p njegov neničeln element. Naslednji trditvi sta ekvivalentni:*

(i) *p je nerazcepen.*
(ii) *Ideal (p) je maksimalen med glavnimi ideali (to pomeni, da $(p) \neq K$ in za vsak $a \in K$ iz $(p) \subseteq (a) \subsetneq K$ sledi $(a) = (p)$).*

Dokaz. Pogoj $(p) \subseteq (a)$ je ekvivalenten pogoju, da je $p = ab$ za neki $b \in K$ (gl. (6.2)), pogoj $(a) \neq K$ pa je ekvivalenten pogoju, da a ni obrnljiv (gl. (6.1)). V luči trditve 6.9 zato lahko (ii) zapišemo tudi takole: p ni obrnljiv in če je $p = ab$ in a ni obrnljiv, potem obstaja tak obrnljiv element $u \in K$, da je $p = au$. Toda iz $p = ab$ in $p = au$ sledi $b = u$, saj je K cel in $a \neq 0$. Torej je b obrnljiv. Skratka, (ii) pravi tole: p ni obrnljiv in če je $p = ab$ in a ni obrnljiv, potem je b obrnljiv. To pa ni nič drugega kot definicija nerazcepnosti elementa p. □

Naloge

1. Naj bo d celo število, ki ni kvadrat naravnega števila. Označimo

$$\mathbb{Z}[\sqrt{d}] := \{m + n\sqrt{d} \mid m, n \in \mathbb{Z}\}.$$

(Če je $d < 0$, je $\sqrt{d} = i\sqrt{-d}$; tako je $\mathbb{Z}[\sqrt{-1}]$ kolobar Gaussovih celih števil $\mathbb{Z}[i]$). Vpeljimo preslikavo $N : \mathbb{Z}[\sqrt{d}] \to \mathbb{Z}$ s predpisom

$$N(m + n\sqrt{d}) := (m + n\sqrt{d})(m - n\sqrt{d}) = m^2 - dn^2.$$

Imenujemo jo **norma**. Pokaži:

(a) $\mathbb{Z}[\sqrt{d}]$ je podkolobar polja $\mathbb{C}$.
(b) Množica

$$\mathbb{Q}(\sqrt{d}) := \{p + q\sqrt{d} \,|\, p, q \in \mathbb{Q}\}$$

je podpolje $\mathbb{C}$, generirano z $\mathbb{Z}[\sqrt{d}]$.
(c) Za vse $x, y \in \mathbb{Z}[\sqrt{d}]$ je $N(xy) = N(x)N(y)$.
(d) Element $x \in \mathbb{Z}[\sqrt{d}]$ je obrnljiv natanko tedaj, ko je $N(x) = \pm 1$.
(e) Denimo, da je $N(x) = \pm p$, kjer je p praštevilo. Pokaži, da je potem x nerazcepen.

Komentar. Kolobarji $\mathbb{Z}[\sqrt{d}]$ so seveda celi. Pojmi, ki smo jih v tem razdelku vpeljali, v njih lepo zaživijo. To bo razvidno že iz naslednjih nalog. Poglobljeno teh kolobarjev sicer ne bomo obravnavali, čeprav so brez dvoma zanimivi in igrajo pomembno vlogo v *algebraični teoriji števil*. Prednost bomo dali podrobnejšemu študiju kolobarjev polinomov. Naloge v zvezi z deljivostjo polinomov bodo prišle na vrsto kasneje, ko bomo imeli več teoretičnega ozadja.

2. Pokaži, da sta 1 in -1 edina obrnljiva elementa kolobarja $\mathbb{Z}[\sqrt{d}]$, če je $d < -1$.
3. Pokaži, da so 1, -1, i in $-i$ edini obrnljivi elementi kolobarja $\mathbb{Z}[i]$. Katera števila so torej asociirana številu $m + ni \in \mathbb{Z}[i]$?
4. Pokaži, da so $(1 + \sqrt{2})^n$, $n \in \mathbb{Z}$, obrnljivi elementi kolobarja $\mathbb{Z}[\sqrt{2}]$.
5. Pokaži, da je norma števila $x \in \mathbb{Z}[i]$ sodo število natanko tedaj, ko je x deljiv z $1 + i$.
6. Poišči vse delitelje števila 2 v $\mathbb{Z}[i]$.
7. S pomočjo ugotovitve (e) iz naloge 1 zlahka poiščemo primere nerazcepnih elementov kolobarja $\mathbb{Z}[i]$, npr. $1+i$, $4-i$, $-3+2i$, $7+8i$ itd. Pokaži, da je tudi 3 nerazepen element, čeprav njegova norma ni praštevilo.

   Namig. Iz $xy = 3$ sledi $N(x)N(y) = 9$.
8. Pokaži, da 5 in 7 sta, 2 in 3 pa nista nerazcepna elementa kolobarja $\mathbb{Z}[\sqrt{-2}]$.
9. Naj bosta a in b elementa komutativnega kolobarja K, ne oba enaka 0. Denimo, da je $ax + by = 1$ za neka $x, y \in K$. Pokaži, da sta si a in b tuja.
10. Pokaži, da sta si števili $2\sqrt{2}$ in 9 tuji kot elementa kolobarja $\mathbb{Z}[\sqrt{2}]$ na dva načina:
    (a) S pomočjo prejšnje naloge.
    (b) S pomočjo norme.
11. Poišči največji skupni delitelj števil $a = 3 - 4i$ in $b = 1 - 3i$ v kolobarju $\mathbb{Z}[i]$.

12. Pokaži, da števili $a = 6$ in $b = 2 + 2\sqrt{-5}$ v kolobarju $\mathbb{Z}[\sqrt{-5}]$ nimata največjega skupnega delitelja.

    Namig. Če bi d bil največji skupni delitelj a in b, bi bil deljiv s $c = 2$ in $c' = 1 + \sqrt{-5}$. Število $N(d)$ bi bilo zato deljivo z $N(c)$ in $N(c')$ in bi po drugi strani delilo $N(a)$ in $N(b)$.

6.3. Evklidski kolobarji

Ugotovitve o kolobarju celih števil, ki smo jih dokazali v razdelku 2.1, gotovo niso bile povsem nove. S celimi števili se srečujemo že predolgo in prepogosto. Morda je bil nov sistematičen pristop, ki je do teh ugotovitev vodil. V tem razdelku bomo pokazali, da lahko s podobnim pristopom izpeljemo podobne rezultate za razred kolobarjev, ki jim pravimo evklidski kolobarji. Poleg kolobarja $\mathbb{Z}$ mednje sodi tudi kolobar $F[X]$, torej kolobar polinomov (ene spremenljivke) nad poljem F. Tako bomo videli, da sta si kolobarja $\mathbb{Z}$ in $F[X]$ presenetljivo podobna. Očitna skupna lastnost je, da sta oba cela kolobarja, torej komutativna in brez deliteljev niča (gl. trditev 2.19). Toda celih kolobarjev je veliko. Ključna podobnost, iz katere bodo vse ostale sledile, je veljavnost **osnovnega izreka o deljenju**. Za cela števila ga že poznamo (izrek 2.1), za polinome pa ga dokažimo.

Spomnimo se, da s $\mathrm{st}(f(X))$ označujemo stopnjo polinoma $f(X)$.

Izrek 6.17. *Naj bo F polje in naj bosta $f(X), g(X) \in F[X]$ poljubna polinoma. Če $g(X) \neq 0$, potem obstajata taka polinoma $q(X), r(X) \in F[X]$, da je*

$$f(X) = q(X)g(X) + r(X)$$

in je bodisi $r(X) = 0$ bodisi je $\mathrm{st}(r(X)) < \mathrm{st}(g(X))$.

Dokaz. Če je $f(X)$ enak 0 ali pa ima nižjo stopnjo kot $g(X)$, vzamemo kar $q(X) = 0$ in $r(X) = f(X)$. Zato smemo privzeti, da je število $m := \mathrm{st}(f(X))$ kvečjemu večje kot $n := \mathrm{st}(g(X))$.

Izrek bomo dokazali z indukcijo na m. Če je $m = 0$, je tudi $n = 0$ in tako vzamemo $q(X) = f(X)g(X)^{-1}$ in $r(X) = 0$. Naj bo torej $m > 0$. Zapišimo

$$f(X) = aX^m + f_1(X), \quad g(X) = bX^n + g_1(X),$$

kjer sta $a, b \in F \setminus \{0\}$, $f_1(X)$ je 0 ali stopnje manj kot m, in $g_1(X)$ je 0 ali stopnje manj kot n. Polinom

$$f(X) - ab^{-1}X^{m-n}g(X) = f_1(X) - ab^{-1}X^{m-n}g_1(X)$$

je zato bodisi 0 bodisi ima stopnjo manjšo kot m. Po indukcijski predpostavki je tako

$$f(X) - ab^{-1}X^{m-n}g(X) = q_1(X)g(X) + r(X)$$

za neka polinoma $q_1(X)$ in $r(X)$, pri čemer je $r(X)$ bodisi enak 0 bodisi je njegova stopnja manjša od n. Od tod sledi želeni zapis

$$f(X) = q(X)g(X) + r(X),$$

kjer je $q(X) = ab^{-1}X^{m-n} + q_1(X)$. □

Omenimo še, da sta polinoma $q(X)$ in $r(X)$ enolično določena. O tem se hitro prepričamo.

Evklidske kolobarje definiramo kot kolobarje, za katere velja inačica osnovnega izreka o deljenju.

Definicija 6.18. Cel kolobar K se imenuje **evklidski kolobar**, če obstaja preslikava $\delta : K \setminus \{0\} \to \mathbb{N} \cup \{0\}$ z naslednjima lastnostima:

(a) Za poljuben par elementov $a, b \in K$, kjer $b \neq 0$, obstajata taka elementa $q, r \in K$, da je $a = qb + r$ in je $r = 0$ ali pa je $\delta(r) < \delta(b)$.
(b) $\delta(a) \leq \delta(ab)$ za vse $a, b \in K \setminus \{0\}$.

Primer 6.19. Kolobar $\mathbb{Z}$ je evklidski. Ustrezna preslikava je $\delta(n) = |n|$ (za $n < 0$ je $m = q(-n) + r = (-q)n + r$, kjer je $0 \leq r < -n$).

Primer 6.20. Kolobar polinomov $F[X]$, kjer je F polje, je evklidski. Seveda je cel, preslikava $\delta(f(X)) = \mathrm{st}(f(X))$ pa zadošča pogojema iz definicije.

Primer 6.21. Kolobar Gaussovih celih števil $\mathbb{Z}[i]$ je evklidski. Dokaz prepuščamo bralcu kot nalogo, a z dovolj jasnim navodilom (naloga 2). Izmed drugih kolobarjev $\mathbb{Z}[\sqrt{d}]$ iz naloge 6.2/1 nekateri so evklidski (npr. $\mathbb{Z}[\sqrt{-2}]$ in $\mathbb{Z}[\sqrt{2}]$), nikakor pa ne vsi (npr. $\mathbb{Z}[\sqrt{-3}]$ ni). Toda v to se ne bomo spuščali.

Primer 6.22. Tudi vsako polje F je evklidski kolobar; »ostanek« r iz definicije je namreč vselej enak 0 in za δ lahko izberemo katerokoli konstantno preslikavo. Vendar ta primer ni zanimiv, saj so rezultati o splošnih evklidskih kolobarjih za polja praviloma očitni.

Lahko bi navedli še več primerov. Toda poglobljen študij evklidskih kolobarjev ni naš namen. V središču našega zanimanja je kolobar polinomov $F[X]$. Lahko bi obravnavo omejili tudi samo na ta kolobar, vendar si s tem dela ne bi kaj dosti olajšali. V matematiki je pogosto študij splošnejše teme jasnejši in preglednejši, kot če se omejimo na konkreten primer.

Kot vemo, so vsi ideali kolobarja $\mathbb{Z}$ oblike $(n) = n\mathbb{Z}$ in so zato glavni. To sledi iz posledice 2.2. Dokaz naslednjega izreka temelji na isti ideji kot dokaz te posledice.

Izrek 6.23. *Vsak ideal evklidskega kolobarja je glavni.*

Dokaz. Ničelni ideal je generiran z elementom 0. Vzemimo torej neničeln ideal I evklidskega kolobarja K. Izberimo tak $a \in I$, da je $\delta(a) \leq \delta(x)$ za vsak $x \in I$. Trdimo, da je $I = (a)$. Ker je $a \in I$, je seveda $(a) \subseteq I$. Pokažimo,

da je poljuben element $x \in I$ vsebovan v (a). Naj bosta $q, r \in K$ taka, da je $x = qa + r$ in je $r = 0$ ali pa je $\delta(r) < \delta(a)$. Toda druga možnost ne pride v poštev, saj iz $x, a \in I$ sledi, da je $r = x - qa \in I$. Torej je $r = 0$ in $x = qa \in (a)$. □

Izrek ima več zanimivih posledic.

POSLEDICA 6.24. *Naj bo K evklidski kolobar in naj bo $p \neq 0$ njegov element. Naslednje trditve so si ekvivalentne:*

(i) *p je nerazcepen.*
(ii) *(p) je maksimalen ideal.*
(iii) *Kvocientni kolobar $K/(p)$ je polje.*

DOKAZ. Ker je po izreku 6.23 vsak ideal v K oblike (a) za neki $a \in K$, se drugi pogoj iz trditve 6.16 prebere enako kot definicija maksimalnosti ideala (p). Trditvi (i) in (ii) sta torej ekvivalentni. Ekvivalentnost trditev (ii) in (iii) pa sledi iz posledice 4.37. □

V primeru, ko je $K = \mathbb{Z}$, posledico 6.24 že poznamo, gl. primer 4.49. Povzemimo bistvo: vsako praštevilo p porodi polje, namreč $\mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z}$. Zdaj vemo, da vsak nerazcepen element p evklidskega kolobarja K porodi polje $K/(p)$. To dejstvo je posebej zanimivo v primeru, ko je $K = F[X]$. Toda o tem kasneje.

Naslednji posledici sta posplošitvi posledic 2.3 in 2.7.

POSLEDICA 6.25. *Naj bo K evklidski kolobar. Za vsak par elementov a in b iz K, ki nista oba enaka 0, obstaja največji skupni delitelj in je oblike $d = ax + by$ za neka $x, y \in K$.*

DOKAZ. Uporabi izrek 6.23 in trditev 6.13. □

Največji skupni delitelj sicer ni enolično določen, toda poljubna dva sta si asociirana in se tako razlikujeta kvečjemu za produkt z obrnljivim elementom. Zato iz posledice 6.25 sledi, da je *vsak* največji skupni delitelj elementov a in b oblike $ax + by$ (ni pa vsak element oblike $ax + by$ njun največji skupni delitelj).

POSLEDICA 6.26. *Naj bo K evklidski kolobar in naj bodo a, b in p njegovi elementi. Če je p nerazcepen in $p \mid ab$, potem $p \mid a$ ali $p \mid b$.*

DOKAZ. Denimo, da p ne deli a. Ker je p nerazcepen, sta si potem elementa p in a tuja. Po posledici 6.25 je $px + ay = 1$ za neka $x, y \in K$. Če pomnožimo to enakost z b, dobimo $pxb + (ab)y = b$. Ker $p \mid ab$, od tod sledi, da $p \mid b$. □

V kolobarju $\mathbb{Z}$ lahko z izjemo elementov $-1, 0$ in 1 vsak drug element zapišemo kot produkt nerazcepnih elementov in ta zapis je enoličen, če se ne

oziramo na vrstni red in predznak faktorjev. Tako lahko povemo osnovni izrek aritmetike (izrek 2.8). Tudi v evklidskih kolobarjih velja tak izrek. Preden ga zapišemo in dokažemo, pojasnimo pomen besedne zveze, ki jo bomo uporabili. Denimo, da element a lahko zapišemo kot $a = p_1 \cdots p_s$, kjer so p_i (ne nujno različni) nerazcepni elementi. Rekli bomo, da je ta zapis **enoličen do vrstnega reda in asociiranosti faktorjev natančno**, kadar velja naslednje: če lahko a zapišemo tudi kot $a = q_1 \cdots q_t$, kjer so elementi q_i nerazcepni, potem je $s = t$ in obstaja taka permutacija σ množice $\{1, \ldots, s\}$, da sta si elementa p_i in $q_{\sigma(i)}$ asociirana za vsak i. Tovrstna enoličnost je največ, kar lahko pričakujemo (če je na primer $a = p_1p_2p_3$, ga lahko zapišemo tudi kot $a = (up_2)(vp_3)(wp_1)$, kjer je $uvw = 1$). Zato v tem primeru rečemo, da ima element a **enolično faktorizacijo**.

Izrek 6.27. *Naj bo K evklidski kolobar. Vsak element $a \in K$, ki ni enak 0 in ni obrnljiv, lahko zapišemo kot produkt nerazcepnih elementov. Ta zapis je enoličen do vrstnega reda in asociiranosti faktorjev natančno.*

Dokaz. Najprej pokažimo, da za vsaka $b, c \in K \setminus \{0\}$ velja:

$$b \text{ ni obrnljiv} \implies \delta(c) < \delta(bc). \tag{6.4}$$

Zapišimo $c = q(bc) + r$. Element r ne more biti enak 0, saj bi sicer veljalo $(1 - qb)c = 0$ in zato $qb = 1$. Zato je $\delta(r) < \delta(bc)$. Po drugi strani pa zaradi pogoja (b) iz definicije evklidskega kolobarja iz $r = (1 - qb)c$ sledi $\delta(c) \leq \delta(r)$. Torej je $\delta(c) < \delta(bc)$.

Od tod dalje dokaz poteka enako kot dokaz osnovnega izreka aritmetike.

Denimo, da obstajajo elementi, ki niso enaki 0, niso obrnljivi in jih ne moremo zapisati kot produkt nerazcepnih elementov. Izmed vseh takih izberimo element a, za katerega je število $\delta(a)$ najmanjše. Seveda a tudi sam ni nerazcepen, zato ga lahko zapišemo kot $a = bc$, kjer b in c nista obrnljiva. Iz (6.4) sledi, da je $\delta(b) < \delta(a)$ in, podobno, $\delta(c) < \delta(a)$. Toda potem lahko b in c zapišemo kot produkt nerazcepnih elementov. To pa je v očitnem protislovju s predpostavko, da to ne velja za $a = bc$.

Dokazati moramo še enoličnost. Denimo, da je $a = p_1 \cdots p_s = q_1 \cdots q_t$, kjer so p_i, q_i nerazcepni. Ker p_1 deli $q_1 \cdots q_t$, s pomočjo posledice 6.26 ugotovimo, da p_1 deli q_i za neki $i \in \{1, \ldots, t\}$. Ker smemo indekse permutirati, lahko brez škode za splošnost privzamemo, da je $i = 1$. Zaradi nerazcepnosti q_1 in neobrnljivosti p_1 iz $p_1 \mid q_1$ sledi, da sta si p_1 in q_1 asociirana, torej $q_1 = up_1$. Ker je K cel, lahko v enakosti

$$p_1p_2 \cdots p_s = (up_1)q_2 \cdots q_t$$

krajšamo p_1. Tako dobimo

$$p_2p_3 \cdots p_s = (uq_2)q_3 \cdots q_t.$$

Ker je, kot zlahka preverimo, tudi uq_2 nerazcepen, lahko zgornji razmislek ponovimo. Po končnem številu korakov (ali, bolj formalno, z indukcijo na s) pridemo do želenega zaključka. □

V dokazih posledic 6.24, 6.25, 6.26 in v dokazu enoličnosti faktorizacije v izreku 6.27 smo uporabili le celost kolobarja K in dejstvo, da so vsi ideali v K glavni. Z malce več truda bi iz teh dveh predpostavk izpeljali tudi obstoj faktorizacije. Vse tri posledice in izrek 6.27 torej veljajo za poljubne cele kolobarje, v katerih so vsi ideali glavni. Takim kolobarjem pravimo **glavni kolobarji**. Evklidski kolobarji seveda so taki, medtem ko glavni kolobarji niso nujno evklidski. Tudi celi kolobarji, za katere velja izrek 6.27, imajo svoje ime. Pravimo jim **kolobarji z enolično faktorizacijo**. Izkaže se, da je za vsak kolobar z enolično faktorizacijo K tudi kolobar polinomov $K[X]$ kolobar z enolično faktorizacijo. Kolobarja $\mathbb{Z}[X]$ in $F[X,Y] = (F[X])[Y]$ sta torej kolobarja z enolično faktorizacijo, a nista glavna (gl. primera 6.6 in 6.7). Glavni kolobarji so kolobarji z enolično faktorizacijo, obrat pa torej ne velja. Nazadnje omenimo še **noetherske kolobarje**, ki v teoriji komutativnih kolobarjev igrajo izjemno pomembno vlogo. To so komutativni kolobarji, v katerih je vsak ideal končno generiran (poznamo sicer tudi nekomutativne noetherske kolobarje, ki pa so definirani nekoliko drugače). **Hilbertov izrek o bazi** pravi, da je za vsak (komutativen) noetherski kolobar K tudi kolobar polinomov $K[X]$ noetherski. Kolobarja $\mathbb{Z}[X]$ in $F[X,Y] = (F[X])[Y]$ sta torej noetherska, ne pa tudi glavna.

Naloge

1. Za polinoma $f(X) = X^5 - X^4 + X - 1 \in F[X]$ in $g(X) = X^2 - X - 1 \in F[X]$ poišči polinoma $q(X)$ in $r(X)$ iz osnovnega izreka o deljenju za primer, ko je:
   (a) $F = \mathbb{Q}$.
   (b) $F = \mathbb{Z}_2$.
   (c) $F = \mathbb{Z}_3$.
2. Pokaži, da je kolobar Gaussovih celih števil $\mathbb{Z}[i]$ evklidski.

   Navodilo. Ustrezna preslikava je norma (gl. nalogo 6.2/1), torej $\delta(m + ni) = m^2 + n^2$. Pokazati moramo, da za poljubna $a, b \in \mathbb{Z}[i]$, $b \neq 0$, obstajata taka $q, r \in \mathbb{Z}[i]$, da je $a = qb + r$ in $\delta(r) < \delta(b)$. Če kompleksno število a delimo s kompleksnim številom b, dobimo kompleksno število $u + iv$, kjer sta u in v racionalni (ne nujno celi) števili. Naj bosta k in ℓ taki celi števili, da je $|u - k| \leq \frac{1}{2}$ in $|v - \ell| \leq \frac{1}{2}$. Pokaži, da sta $q := k + i\ell$ in $r := a - qb$ iskani števili.

   Komentar. Števili q in r v splošnem nista enolično določeni.

3. Pokaži, da Evklidov algoritem za iskanje največjega skupnega delitelja, kot ga poznamo za števila (gl. opombo 2.4), lahko uporabimo v poljubnem evklidskem kolobarju.
4. Ponovno poišči največji skupni delitelj števil $a = 3 - 4i$ in $b = 1 - 3i$ v kolobarju $\mathbb{Z}[i]$ (naloga 6.2/11), tokrat s pomočjo Evklidovega algoritma.
5. Poišči največji skupni delitelj polinomov $f(X) = X^5 + X^3 + 2X^2 + 2$ in $g(X) = X^6 - X^3 - 6$ v kolobarju $\mathbb{Q}[X]$.
6. Poišči največji skupni delitelj polinomov $f(X) = X^5 + X^4 + X + 1$ in $g(X) = X^4 + X^2$ v kolobarju $\mathbb{Z}_2[X]$.
7. Poišči vse take $a \in F$, da si polinoma $f(X) = X^5 + 1$ in $g(X) = X^3 + a$ nista tuja v kolobarju $F[X]$, kjer je:
   (a) $F = \mathbb{R}$.
   (b) $F = \mathbb{C}$.
8. Naj bo K evklidski kolobar in naj $a \in K \setminus \{0\}$. Pokaži:
   (a) Če je $\delta(a) = 0$, je a obrnljiv.
   (b) Če je $\delta(a) = 1$, je a obrnljiv ali nerazcepen.

   Namig. Dokaz izreka 6.27.
9. Pokaži, da sta si neničelna elementa a in b evklidskega kolobarja asocirana natanko tedaj, ko $a \mid b$ in je $\delta(a) = \delta(b)$.
10. Naj bo K cel kolobar in naj preslikava $\delta : K \setminus \{0\} \to \mathbb{N} \cup \{0\}$ zadošča pogoju (a) iz definicije 6.18. Pokaži, da preslikava $\overline{\delta} : K \setminus \{0\} \to \mathbb{N} \cup \{0\}$,

$$\overline{\delta}(a) = \min\{\delta(ax) \mid x \in K \setminus \{0\}\},$$

    potem zadošča obojema pogojema (a) in (b).

    Komentar. V definiciji evklidskega kolobarja bi torej načeloma lahko pogoj (b) izpustili. Vendar bi potem morali preslikavo δ nadomestiti s preslikavo $\overline{\delta}$ in si s tem nakopali dodatno delo.
11. Naj bodo a, b, c elementi evklidskega kolobarja K. Denimo, da $a \mid c$, $b \mid c$ in da sta si a in b tuja. Pokaži, da potem tudi $ab \mid c$.
12. Naj bo P ideal komutativnega kolobarja K. Če $P \neq K$ in če za vse $a, b \in K$ iz $ab \in P$ sledi $a \in P$ ali $b \in P$, potem P imenujemo **praideal**. Pokaži:
   (a) P je praideal natanko tedaj, ko je kvocientni kolobar K/P cel.
   (b) Če je P maksimalen ideal, je P praideal.
   (c) Če je K cel kolobar, ki ni polje, je $\{0\}$ njegov praideal, ki ni maksimalen.
   (d) Če je $P \neq \{0\}$ praideal evklidskega kolobarja K, je P maksimalen (in je torej $P = (p)$ za neki nerazcepen element p iz K).
13. Ali je kolobar $K[X]$ evklidski, če je K evklidski?

14. Naj bosta p in q nerazcepna elementa evklidskega kolobarja K. Pokaži, da je $K/(pq) \cong K/(p) \times K/(q)$ natanko tedaj, ko si p in q nista asociirana.

6.4. Nerazcepni polinomi

Kot ponavadi naj F označuje polje. Kolobar polinomov $F[X]$ je evklidski in zato zanj veljajo vsi izsledki prejšnjega razdelka. Ponovimo in obenem malce preoblikujmo najpomembnejše.

(a) Vsak **ideal** I kolobarja $F[X]$ je glavni, torej oblike

$$I = (a(X)) = \{a(X)f(X) \mid f(X) \in F[X]\}$$

za neki polinom $a(X) \in F[X]$. Če $I \neq \{0\}$, za $a(X)$ izberemo (katerikoli) polinom najnižje stopnje v I.

(b) Za vsak par polinomov $a(X), b(X) \in F[X]$, ki nista oba enaka 0, obstaja **največji skupni delitelj** in je oblike

$$d(X) = a(X)f(X) + b(X)g(X)$$

za neka $f(X), g(X) \in F[X]$. (Za največji skupni delitelj polinomov zahtevamo, da ima vodilni koeficient 1. S tem je enolično določen.)

(c) V kolobarju $F[X]$ so edini obrnljivi elementi neničelni konstantni polinomi. Zato je polinom $p(X) \in F[X]$ **nerazcepen**, če je nekonstanten in se ga ne da zapisati kot produkt dveh nekonstantnih polinomov iz $F[X]$, torej dveh polinomov, ki imata oba nižjo stopnjo kot $p(X)$. Naslednje trditve so si ekvivalentne:
   (i) $p(X)$ je nerazcepen v $F[X]$.
   (ii) $(p(X))$ je maksimalen ideal kolobarja $F[X]$.
   (iii) Kvocientni kolobar $F[X]/(p(X))$ je polje.

(d) Vsak nekonstanten polinom $f(X) \in F[X]$ lahko zapišemo v obliki

$$f(X) = ap_1(X) \cdots p_s(X),$$

kjer je a vodilni koeficient $f(X)$ in so $p_i(X)$ nerazcepni polinomi z vodilnim koeficientom 1. Ta zapis je enoličen do vrstnega reda faktorjev natančno. Z zahtevo, da so njihovi vodilni koeficienti enaki 1, smo se namreč izognili asociiranosti. Nekateri izmed polinomov $p_i(X)$ so lahko med seboj enaki. Če take združimo, dobimo zapis

$$f(X) = ap_1(X)^{k_1} \cdots p_r(X)^{k_r},$$

kjer so $k_i \in \mathbb{N}$ in so sedaj $p_i(X)$ različni.

Kateri polinomi so nerazcepni? Zanesljivo so taki seveda linearni polinomi. Za polinome višjih stopenj pa lahko rečemo, da zanesljivo *niso* nerazcepni tisti, ki imajo v F ničlo. Velja namreč naslednja trditev.

TRDITEV 6.28. *Polinom $f(X) \in F[X]$ ima ničlo $a \in F$ natanko tedaj, ko polinom $X - a$ deli $f(X)$.*

DOKAZ. Po izreku 6.17 obstajata taka polinoma $q(X), r(X) \in F[X]$, da je

$$f(X) = q(X)(X - a) + r(X)$$

in je $r(X)$ konstanten polinom, torej $r(X) = c$ za neki $c \in F$. Če izračunamo vrednost leve in desne strani v a, dobimo $f(a) = c$. Od tod trditev jasno sledi. □

POSLEDICA 6.29. *Polinom $f(X) \in F[X]$ stopnje 2 ali 3 je nerazcepen natanko tedaj, ko nima ničle v F.*

DOKAZ. Iz predpostavke o stopnji očitno sledi, da je $f(X)$ razcepen natanko tedaj, ko je deljiv z linearnim polinomom. □

Za polinome poljubnih stopenj posledica ne velja.

PRIMER 6.30. Polinom $X^4+2X^2+1 \in \mathbb{R}[X]$ nima ničle v $\mathbb{R}$, a je razcepen, saj ga lahko zapišemo kot $(X^2 + 1)^2$.

Osnovni izrek algebre (izrek B.1) pravi, da ima vsak nekonstanten polinom iz $\mathbb{C}[X]$ vsaj eno ničlo v $\mathbb{C}$. V luči trditve 6.28 to lahko povemo tudi takole.

IZREK 6.31. *V kolobarju $\mathbb{C}[X]$ so nerazcepni le linearni polinomi.*

Z zaporedno uporabo trditve 6.28 vidimo, da lahko izrek 6.31 izrazimo tudi na tale način: vsak nekonstanten polinom iz $\mathbb{C}[X]$ je produkt linearnih polinomov iz $\mathbb{C}[X]$. Tu seveda kompleksnih števil ne moremo zamenjati z realnimi. Če je $b^2 - 4ac < 0$, kvadratni polinom $aX^2 + bX + c \in \mathbb{R}[X]$ nima realnih ničel, zato je nerazcepen v $\mathbb{R}[X]$ in ni enak produktu linearnih polinomov iz $\mathbb{R}[X]$. Naslednji izrek pove, da so v $\mathbb{R}[X]$ taki polinomi poleg linearnih tudi edini nerazcepni.

IZREK 6.32. *Vsak nekonstanten polinom $f(X) \in \mathbb{R}[X]$ lahko zapišemo kot produkt linearnih in kvadratnih polinomov iz $\mathbb{R}[X]$. Poleg linearnih polinomov so v kolobarju $\mathbb{R}[X]$ torej edini nerazcepni polinomi kvadratni polinomi brez realnih ničel, torej polinomi oblike aX^2+bX+c, kjer $a \neq 0$ in je $b^2-4ac < 0$.*

DOKAZ. Izrek dokažimo z indukcijo na $n := \mathrm{st}(f(X))$. Za $n = 1$ ni kaj dokazovati, zato smemo privzeti, da je $n > 1$ in da izrek velja za vse polinome stopnje manj kot n. Če ima $f(X)$ realno ničlo a, ga lahko po trditvi 6.28 zapišemo kot $f(X) = (X - a)g(X)$ za neki polinom $g(X) \in \mathbb{R}[X]$. Za $g(X)$ uporabimo indukcijsko predpostavko in želena trditev sledi. Naj bo torej polinom $f(X)$ brez realnih ničel. Če ga obravnavamo kot element kolobarja $\mathbb{C}[X]$, dobimo zapis

$$f(X) = a(X - z_1)(X - z_2) \cdots (X - z_n) \tag{6.5}$$

za neke $z_i \in \mathbb{C} \setminus \mathbb{R}$ in $a \in \mathbb{R}$. Ker ima $f(X)$ realne koeficiente, za vse $z \in \mathbb{C}$ velja $f(\overline{z}) = \overline{f(z)}$. Iz $f(z_1) = 0$ tako sledi $f(\overline{z}_1) = 0$. Torej je $\overline{z}_1$ ena izmed preostalih ničel z_i, na primer $\overline{z}_1 = z_2$. Pišimo

$$g(X) := (X - z_1)(X - \overline{z}_1) = X^2 - (z_1 + \overline{z}_1)X + z_1\overline{z}_1.$$

Ker sta števili $z_1 + \overline{z}_1$ in $z_1\overline{z}_1$ realni, je $g(X) \in \mathbb{R}[X]$. Iz (6.5) dobimo $f(X) = g(X)h(X)$, kjer je $h(X) \in \mathbb{C}[X]$ polinom stopnje $n - 2$. Toda ker imata tako $f(X)$ kot $g(X)$ realne koeficiente, jih ima tudi $h(X)$. To preverimo neposredno z računom, lahko pa tudi s pomočjo izreka 6.17. Zato lahko za $h(X)$ uporabimo indukcijsko predpostavko in želeni zaključek sledi. □

V nadaljevanju razdelka se bomo ukvarjali z nerazcepnostjo polinomov iz $\mathbb{Q}[X]$. Tudi ti polinomi imajo kompleksne ničle, vendar si s tem ne moremo pomagati na podoben način kot pri polinomih iz $\mathbb{R}[X]$. Vprašanje nerazcepnosti polinomov iz $\mathbb{Q}[X]$ ni enostavno in popolnega odgovora ne moremo podati.

Če polinom pomnožimo z neničelnim elementom iz polja, to ne vpliva na nerazcepnost. Zato se lahko omejimo na obravnavo polinomov s celoštevilskimi koeficienti. Če namreč polinom iz $\mathbb{Q}[X]$ pomnožimo s skupnim večkratnikom imenovalcev njegovih koeficientov, dobimo polinom iz $\mathbb{Z}[X]$.

Definicija 6.33. Polinom s celoštevilskimi koeficienti je **primitiven**, če je največji skupni delitelj njegovih koeficientov enak 1.

Z drugimi besedami, polinom

$$a_nX^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0 \in \mathbb{Z}[X]$$

je primitiven, če so si števila $a_n, a_{n-1}, \ldots, a_0$ tuja, torej če ne obstaja praštevilo p, ki deli vse a_i. Denimo, polinom $6X^3 - 3X^2 + 2$ je primitiven, polinom $6X^3 - 4X^2 + 2$ pa ni. Če $f(X) \in \mathbb{Z}[X]$ ni primitiven in je d največji skupni delitelj njegovih koeficientov, ga lahko zapišemo kot $f(X) = df_0(X)$, kjer $f_0(X)$ je primitiven. Tako je npr. $6X^3 - 4X^2 + 2 = 2(3X^3 - 2X^2 + 1)$.

Tako naslednja lema kot naslednji izrek se v literaturi pojavljata pod imenom **Gaussova lema**.

Lema 6.34. *Produkt primitivnih polinomov je primitiven polinom.*

Dokaz. Naj bosta $f(X)$ in $g(X)$ primitivna polinoma. Denimo, da njun produkt $f(X)g(X)$ ni primitiven. Naj bo p praštevilo, ki deli vse njegove koeficiente. Torej $f(X)g(X)$ pripada idealu $p\mathbb{Z}[X]$ kolobarja $\mathbb{Z}[X]$ (to je glavni ideal, generiran s konstantnim polinomom p). Ker sta $f(X)$ in $g(X)$ primitivna, sama nista elementa tega ideala. Odseka

$$f(X) + p\mathbb{Z}[X],\ g(X) + p\mathbb{Z}[X] \in \mathbb{Z}[X]/p\mathbb{Z}[x]$$

sta torej neničelna, njun produkt

$$(f(X) + p\mathbb{Z}[X])(g(X) + p\mathbb{Z}[X]) = f(X)g(X) + p\mathbb{Z}[X]$$

pa je enak 0. Kolobar $\mathbb{Z}[X]/p\mathbb{Z}[X]$ ima torej delitelje niča. Toda to ne more biti res, saj je, kot bomo pokazali,

$$\mathbb{Z}[X]/p\mathbb{Z}[X] \cong \mathbb{Z}_p[X], \tag{6.6}$$

kolobar $\mathbb{Z}_p[X]$ pa je kot kolobar polinomov nad poljem cel. Dokažimo torej (6.6). Naj bo $\pi : \mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}\,(= \mathbb{Z}_p)$ kanonični epimorfizem. Zlahka preverimo, da je preslikava $\varphi : \mathbb{Z}[X] \to \mathbb{Z}_p[X]$, podana s predpisom

$$\varphi(a_nX^n + a_{n-1}X^{n-1} + \cdots + a_0) = \pi(a_n)X^n + \pi(a_{n-1})X^{n-1} + \cdots + \pi(a_0)$$

epimorfizem kolobarjev in da je $\ker\varphi = p\mathbb{Z}[X]$. Iz izreka o izomorfizmu (izrek 4.40) zato sledi (6.6). □

Lemo bi lahko dokazali tudi brez uporabe kvocientnih kolobarjev, ki jih navsezadnje tudi *Carl Friedrich Gauss* (1777–1855) še ni poznal. Prednost našega abstraktnejšega dokaza je, da sloni na konceptih in zahteva le malo računanja. Ima pa tudi slabšo plat – bralec bi lahko dobil vtis, da je rezultat globlji, kot je v resnici. Zato naj neposreden dokaz poskusi poiskati sam.

Polinom $f(X) \in \mathbb{Z}[X]$ lahko obravnavamo tudi kot polinom iz kolobarja $\mathbb{Q}[X]$. Če je nerazcepen v $\mathbb{Q}[X]$, ga seveda ne moremo zapisati kot produkt dveh nekonstantnih polinomov iz $\mathbb{Z}[X]$ (celo iz $\mathbb{Q}[X]$ ne). Naslednji izrek pove, da, presenetljivo, za vsak nekonstanten polinom velja tudi obratna trditev. Najprej pa pojasnilo v zvezi s formulacijo izreka. Pogoj, da se nekonstanten polinom $f(X)$ ne more zapisati kot produkt dveh nekonstantnih polinomov, v kolobarju $\mathbb{Z}[X]$ ni ekvivalenten pogoju, da je $f(X)$ nerazcepen element tega kolobarja. Če namreč $f(X)$ ni primitiven, ga lahko zapišemo kot $f(X) = pf_1(X)$, kjer niti konstantni polinom p niti polinom $f_1(X)$ nista obrnljiva elementa kolobarja $\mathbb{Z}[X]$.

Izrek 6.35. *Če nekonstantnega polinoma $f(X) \in \mathbb{Z}[X]$ ne moremo zapisati kot produkt dveh nekonstantnih polinomov iz $\mathbb{Z}[X]$, je $f(X)$ nerazcepen v $\mathbb{Q}[X]$.*

Dokaz. Predpostavimo, da je $f(X) = g(X)h(X)$ za neka polinoma $g(X)$, $h(X) \in \mathbb{Q}[X]$. Dokazati moramo, da ima eden izmed njiju stopnjo 0.

Če polinom z racionalnimi koeficienti pomnožimo z nekim skupnim večkratnikom imenovalcev njegovih koeficientov, dobimo polinom s celoštevilskimi koeficienti. Torej obstajata taki naravni števili k in ℓ, da polinoma $kg(X)$ in $\ell h(X)$ ležita v $\mathbb{Z}[X]$. V enakosti

$$k\ell f(X) = kg(X) \cdot \ell h(X) \tag{6.7}$$

tako nastopajo polinomi iz $\mathbb{Z}[X]$. Naj bo d največji skupni delitelj koeficientov polinoma $f(X)$, d_1 največji skupni delitelj koeficientov polinoma $kg(X)$ in d_2 največji skupni delitelj koeficientov polinoma $\ell h(X)$. Potem lahko zapišemo

$$f(X) = df_0(X),\ kg(X) = d_1g_0(X)\ \text{ in }\ \ell h(X) = d_2h_0(X),$$

kjer so $f_0(X)$, $g_0(X)$ in $h_0(X)$ primitivni polinomi. Če vpeljemo še $a := k\ell d$ in $b := d_1 d_2$, lahko enakost (6.7) prepišemo kot

$$af_0(X) = bg_0(X)h_0(X). \tag{6.8}$$

Po lemi 6.34 je polinom $g_0(X)h_0(X)$ primitiven. Zato je največji skupni delitelj koeficientov polinoma $bg_0(X)h_0(X)$ enak b. Podobno je največji skupni delitelj koeficientov polinoma $af_0(X)$ enak a. Iz (6.8) tako sledi $a = b$, zato

$$f_0(X) = g_0(X)h_0(X)$$

in naposled

$$f(X) = df_0(X) = dg_0(X)h_0(X).$$

Po predpostavki izreka je eden izmed polinomov $g_0(X)$ in $h_0(X)$ konstanten. Potem pa isto velja za enega izmed polinomov $g(X)$ in $h(X)$. □

Iz dokaza je razvidno, da velja malce več, kot pravi sam izrek: če lahko polinom $f(X) \in \mathbb{Z}[X]$ zapišemo kot produkt dveh polinomov iz $\mathbb{Q}[X]$ stopenj n_1 in n_2, potem ga lahko zapišemo tudi kot produkt dveh polinomov iz $\mathbb{Z}[X]$ istih stopenj n_1 in n_2.

Naslednja posledica predstavi koristen način za ugotavljanje nerazcepnosti polinoma. Imenuje se po nemškem matematiku *Gottholdu Eisensteinu*.

Posledica 6.36. ***(Eisensteinov kriterij)*** *Naj bo*

$$f(X) = a_n X^n + a_{n-1}X^{n-1} + \cdots + a_1 X + a_0 \in \mathbb{Z}[X]$$

polinom stopnje $n \geq 1$. Če obstaja tako praštevilo p, da

$$p \mid a_0,\ p \mid a_1, \ldots, p \mid a_{n-1},\ \ p \nmid a_n \ \text{ in } \ p^2 \nmid a_0,$$

potem je $f(X)$ nerazcepen v $\mathbb{Q}[X]$.

Dokaz. Denimo, da to ni res, da torej $f(X)$ ni nerazcepen v $\mathbb{Q}[X]$. Po izreku 6.35 potem obstajata taka polinoma s celoštevilskimi koeficienti

$$g(X) = b_r X^r + b_{r-1}X^{r-1} + \cdots + b_1 X + b_0$$

in

$$h(X) = c_s X^s + c_{s-1}X^{s-1} + \cdots + c_1 X + c_0,$$

da je $b_r \neq 0$, $c_s \neq 0$, $r < n$, $s < n$ in

$$f(X) = g(X)h(X).$$

Prosti členi naših polinomov so v enostavni zvezi: $a_0 = b_0 c_0$. Ker $p \,|\, a_0$ in $p^2 \nmid a_0$, p deli natanko eno izmed števil b_0 in c_0. Predpostaviti smemo, da $p \mid b_0$ in $p \nmid c_0$. Iz $a_n = b_r c_s$ in $p \nmid a_n$ sledi, da $p \nmid b_r$. Zato obstaja tako naravno število $k \leq r$, da $p \mid b_0, \ldots, p \mid b_{k-1}$ in $p \nmid b_k$. Ker je

$$a_k = b_k c_0 + b_{k-1}c_1 + \cdots + b_0 c_k$$

in ker p deli števila $b_0, \ldots, b_{k-1}$ in a_k (saj je $k < n$), p deli tudi $b_k c_0$. To je protislovje, saj $p \nmid b_k$ in $p \nmid c_0$. □

PRIMER 6.37. Polinom $X^n - p$, kjer je p praštevilo in $n \geq 2$, očitno zadošča pogojem izreka in je torej nerazcepen v $\mathbb{Q}[X]$. Med drugim zato nima ničle v $\mathbb{Q}$. Z drugimi besedami, število $\sqrt[n]{p}$ ni racionalno. Bralcu je najbrž to dejstvo poznano. Seveda ga brez težav dokažemo tudi neposredno.

PRIMER 6.38. Za poljubno praštevilo p definirajmo polinom

$$\Phi_p(X) = X^{p-1} + X^{p-2} + \cdots + X + 1.$$

Eisensteinov kriterij zanj sicer očitno ni neposredno uporaben. Do uporabe bomo prišli po ovinku. Najprej opazimo, da je

$$\Phi_p(X)(X-1) = X^p - 1. \tag{6.9}$$

Če v tej enakosti X zamenjamo z $X+1$, dobimo

$$\Phi_p(X+1)X = (X+1)^p - 1 = X^p + pX^{p-1} + \cdots + \binom{p}{p-2} X^2 + pX.$$

S krajšanjem X dobimo zapis $\Phi_p(X+1)$, ki kar kliče po uporabi Eisensteinovega kriterija. Namreč, ker je p praštevilo, so števila $\binom{p}{k}$, $1 \leq k \leq p-1$, vsa deljiva s p (gl. dokaz leme 7.60). Zato je polinom $\Phi_p(X+1)$ nerazcepen v $\mathbb{Q}[X]$. Potem pa je nerazcepen tudi $\Phi_p(X)$, saj iz

$$\Phi_p(X) = g(X)h(X)$$

sledi

$$\Phi_p(X+1) = g(X+1)h(X+1).$$

Iz enakosti (6.9) lahko z zaporedno uporabo trditve 6.28 izpeljemo, da $\Phi_p(X)$ lahko zapišemo kot $\Pi_{\omega \in \Omega_p}(X - \omega)$, kjer je $\Omega_p = \{\omega \in \mathbb{C} \mid \omega^p = 1\} \setminus \{1\}$. Za poljubno naravno število n definiramo

$$\Phi_n(X) := \Pi_{\omega \in \Omega_n}(X - \omega),$$

kjer je Ω_n množica **primitivnih n-tih korenov enote**. To so kompleksna števila oblike $\omega = \cos\frac{2k\pi}{n} + i \sin\frac{2k\pi}{n}$, kjer je $1 \leq k < n$ in sta si števili k in n tuji. Ni težko videti, da jih lahko opišemo tudi kot kompleksna števila z lastnostjo $\omega^n = 1$ in $\omega^j \neq 1$ za vse $1 \leq j < n$. Izkaže se, da je $\Phi_n(X)$ polinom s celoštevilskimi koeficienti in da je nerazcepen v $\mathbb{Q}[X]$. Toda dokaz za poljuben $n \in \mathbb{N}$ ni tako enostaven kot za praštevilo. Polinome $\Phi_n(X)$ imenujemo **ciklotomični polinomi**.

Naloge

1. Polinom $f(X) = X^5 - 81X$ zapiši kot produkt nerazcepnih polinomov iz $\mathbb{R}[X]$.

2. Polinom $f(X) = X^5 + 81X$ zapiši kot produkt nerazcepnih polinomov iz $\mathbb{R}[X]$.
3. Pokaži, da je polinom $p(X) = 7X^6 + 30X^3 - 6X^2 + 60$ nerazcepen v $\mathbb{Q}[X]$.
4. Pokaži, da je polinom $p(X) = \frac{3}{7}X^5 - \frac{7}{2}X^2 - X + 2$ nerazcepen v $\mathbb{Q}[X]$.
5. Pokaži, da je polinom $f(X) = X^n + 1$ nerazcepen v $\mathbb{Q}[X]$ natanko tedaj, ko je n potenca števila 2.

   Namig. Eisensteinov kriterij ni vedno uporaben neposredno (gl. primer 6.38).
6. Polinom $f(X) = X^{16} - 6X^8 + 5$ zapiši kot produkt nerazcepnih polinomov iz $\mathbb{Q}[X]$.
7. Naj bodo $a_0, a_1, \ldots, a_n$ cela števila in naj bo p praštevilo, ki ne deli a_n. Denimo, da je polinom $\sum_{i=0}^{n}(a_i + p\mathbb{Z})X^i$ nerazcepen v $\mathbb{Z}_p[X]$. Pokaži, da je potem polinom $\sum_{i=0}^{n} a_i X^i$ nerazcepen v $\mathbb{Q}[X]$.

   Komentar. S tem prevedemo problem nerazcepnosti polinoma v kolobarju $\mathbb{Q}[X]$ na enak problem v kolobarju $\mathbb{Z}_p[X]$. Včasih je slednji lažje rešljiv. Vsaj za male p lahko neposredno preverimo, če ima polinom ničlo v $\mathbb{Z}_p$. Če je nima in je razcepen, mora biti deljiv s polinomom stopnje vsaj 2 (ki prav tako nima ničel v $\mathbb{Z}_p$). Tako lahko problem poenostavimo. To metodo lahko uporabiš v naslednjih treh nalogah.
8. Naj bodo a, b, c liha cela števila. Pokaži, da je polinom $p(X) = aX^4 + bX + c$ nerazcepen v $\mathbb{Q}[X]$.
9. Pokaži, da je polinom $p(X) = 7X^5 + 3X^2 + 1$ nerazcepen v $\mathbb{Q}[X]$.
10. Pokaži, da je polinom $p(X) = 36X^3 + 7X + 6$ nerazcepen v $\mathbb{Q}[X]$.
11. Pokaži, da je polinom $p(X) = X^2 + X + 1$ nerazcepen v $\mathbb{Z}_2[X]$. Kot vemo, je zato $\mathbb{Z}_2[X]/(p(X))$ polje. Koliko elementov ima?

    Komentar. Z znanjem naslednjega poglavja bi bilo nalogo lažje rešiti. Morda pa uspeš preko tega posebnega primera sam odkriti kako splošno lastnost polj oblike $F[X]/(p(X))$.
12. Za vsak $n = 2, 3, 4, 5, 6$ zapiši polinom $f_n(X) = X^n + 1$ kot produkt nerazcepnih polinomov iz $\mathbb{Z}_2[X]$.
13. Polinom $f(X) = X^4 + 2$ zapiši kot produkt nerazcepnih polinomov iz $\mathbb{Z}_3[X]$.
14. Polinom $f(X) = X^4 - 2X^3 - 2X + 4$ zapiši kot produkt nerazcepnih polinomov iz $\mathbb{Z}_7[X]$.
15. Naj bo F končno polje. Pokaži, da za vsak $n \in \mathbb{N}$ obstaja nerazcepen polinom $p(X) \in F[X]$ stopnje vsaj n.

Komentar. Dejansko obstaja nerazcepen polinom stopnje *natanko* n. Vendar je dokazati to nekoliko težje. Zadano nalogo pa lahko rešiš s posnemanjem Evklidovega dokaza o neskončnosti množice praštevil.

16. Naj bo F poljubno polje. Denimo, da so $a_1, \ldots, a_n \in F$ različne ničle polinoma $f(X) \in F[X]$ stopnje n. Pokaži, da je potem
$$f(X) = c(X - a_1) \cdots (X - a_n),$$
kjer je c vodilni koeficient polinoma $f(X)$.
17. Izrek 6.32 smo izpeljali iz osnovnega izreka algebra. Pokaži, da se da tudi osnovni izrek algebre izpeljati iz izreka 6.32.
18. Denimo, da ima nekonstanten polinom $f(X) \in F[X]$ isto vrednost v n različnih elementih iz F. Pokaži, da je potem $\mathrm{st}(f(X)) \geq n$.
19. Naj bo F neskončno polje. Pokaži, da sta polinoma $f(X), g(X) \in F[X]$ enaka, če imata enaki polinomski funkciji.
20. Naj bodo $a_1, \ldots, a_n$ različna cela števila. Pokaži, da je polinom
$$p(X) = (X - a_1) \cdots (X - a_n) - 1$$
nerazcepen v $\mathbb{Q}[X]$.
21. Naj bodo $a_1, \ldots, a_n$ različna cela števila. Pokaži, da je polinom
$$p(X) = (X - a_1)^2 \cdots (X - a_n)^2 + 1$$
nerazcepen v $\mathbb{Q}[X]$.

POGLAVJE 7

Ničle polinomov in razširitve polj

Osrednja tema tega poglavja so ničle polinomov in s tem povezane razširitve polj. Pričeli bomo s kratkim zgodovinskim pregledom vpeljave številskih množic in reševanja polinomskih (ali, kot jim tudi rečemo, algebraičnih) enačb, torej enačb oblike $f(x) = 0$, kjer je $f(X)$ polinom. Tako bomo bolje razumeli pomen tematike tega poglavja. Zatem bomo izpeljali zaokroženo teorijo, ki podaja odgovore na naravna vprašanja o ničlah polinomov. Le-te včasih ne moremo najti v originalnih poljih, pač pa v kakih njihovih razširitvah. Prikazali bomo tudi uporabnost te teorije, ki sega od geometrijskih problemov iz antike do pomembnih tem modernega časa, kot so končna polja.

7.1. Pogled v zgodovino

Ko pomislimo na matematiko, pomislimo na števila. Pod števili si ponavadi predstavljamo eno izmed številskih množic

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

Najprej seveda spoznamo **naravna števila**, ki se pojavljajo v vsakdanjem življenju. **Cela števila** so skoraj tako »naravna« kot naravna števila; navsezadnje lahko tudi dolgujemo, ne le posedujemo. Kljub temu so se negativna cela števila in število 0 v matematiki pojavili razmeroma pozno, še posebej v primerjavi s pozitivnimi racionalnimi števili, ki so jih Babilonci poznali že pred štirimi tisočletji. Seveda tudi o pomenu **racionalnih števil**, s katerimi lahko izrazimo dele celote, ne kaže izgubljati besed. Zakaj bi potrebovali še kaka druga števila? To vprašanje morda nima povsem enoznačnega odgovora. Pri praktičnih problemih si z iracionalnimi števili težko pomagamo. Njihov decimalni zapis vsebuje neskončno decimalk, ki se ne ponavljajo periodično, zato smo prisiljeni delati z njihovimi racionalnimi približki. S teoretičnega vidika pa ni težko ugotoviti, da so racionalna števila nezadostna. Denimo, iz Pitagorovega izreka sledi, da je dolžina diagonale kvadrata s stranico dolžine 1 enaka $\sqrt{2}$. To število pa ni racionalno. Povedano drugače, za vsako racionalno število q velja $q^2 \neq 2$. To je bilo znano že v antični Grčiji. Spomnimo se dokaza.

Dokaz iracionalnosti števila $\sqrt{2}$. Privzemimo, da $q^2 = 2$ je izpolnjeno za neki $q \in \mathbb{Q}$. Naj bo $q = \frac{m}{n}$ zapis q v obliki okrajšanega ulomka. Obe števili m in

n torej nista sodi. Enakost $q^2 = 2$ lahko zapišemo kot $m^2 = 2n^2$. Torej je m^2 sodo število. To je možno le takrat, ko je tudi m sodo število. Zato je n liho število, m pa lahko zapišemo kot $m = 2k$ za neko celo število k. Iz tega zapisa sledi $2k^2 = n^2$. Toda to je protislovje, saj je kvadrat lihega števila n liho število.

Dolžine diagonale kvadrata s stranico dolžine 1 torej ne moremo zapisati v obliki ulomka. Izkaže se, da to velja tudi za razmerje med obsegom kroga in njegovim premerom, seveda poznanim kot število π. Dokaz uporablja nekaj standardnih orodij matematične analize in je tako precej zahtevnejši kot dokaz za $\sqrt{2}$, ni pa posebej dolg.

Za opis najbolj osnovnih geometrijskih opažanj tako potrebujemo tudi števila, ki niso racionalna. To spoznanje je sčasoma vodilo do vpeljave **realnih števil**. Sprva brez natančne definicije, o tej se je razmišljalo v drugi polovici devetnajstega stoletja. Definicija z aksiomi, ki jo uporabljamo danes, se je dokončno uveljavila šele v dvajsetem stoletju. Morda se bo pogled na realna števila v prihodnosti še spremenil. V vsakem primeru pa sedanji pristop omogoča razvoj čudovitih matematičnih teorij, ki imajo široko uporabo.

Zakaj bi širili tudi polje realnih števil? Tu je morda težje podati kratek odgovor, ki se zdi že na prvi pogled prepričljiv. Največkrat izhajamo iz dejstva, da enačba $x^2 = -1$ nima rešitve v množici realnih števil. **Kompleksna števila** vpeljemo tako, da to enačbo lahko rešimo. Tako najprej definiramo imaginarno enoto i, že po imenu torej nekakšno namišljeno število, za katero velja $i^2 = -1$. Zatem na znani način vpeljemo množico vseh kompleksnih števil in jo na naraven način opremimo s seštevanjem in množenjem. Kot vemo, s tem dobimo polje. Toda čemu bi kompleksna števila lahko koristila? Čeprav so se v taki ali drugačni obliki pojavljala že od 16. stoletja dalje (in mestoma še prej), so bili matematiki do njih dolgo nezaupljivi. Temu se ne smemo čuditi. Študij abstraktnih algebrskih struktur, kot so kolobarji ali polja, je značilnost moderne matematike. Dejstvo, da je neka množica polje, je morda zanimivo za nas, saj je ta aspekt poudarjen v našem izobraževanju. Matematikom iz prejšnjih obdobij to ne bi povedalo ničesar. Kompleksna števila so bila sčasoma sprejeta, ker so se izkazala kot izredno uporabna na različnih področjih. Tudi kadar rešujemo problem, ki se tiče zgolj realnih števil, v reševanju pogosto nastopajo kompleksna števila. Tako se na primer pojavijo le v dokazu izreka, ne pa v njegovi formulaciji (gl. npr. izrek 6.32). Čeprav so se kompleksna števila porodila iz navidez sporne ideje, da bi korenili negativna realna števila, o njihovem smislu danes ni nikakršnega dvoma. Moderne matematike si brez kompleksnih števil ne moremo več predstavljati. Še posebej veliko uporabno vrednost ima **osnovni izrek algebre**, ki pravi, da ima za poljubne $a, b, \ldots, u, v \in \mathbb{C}$ polinomska enačba

$$ax^n + bx^{n-1} + \cdots + ux + v = 0$$

vsaj eno rešitev v $\mathbb{C}$, če je le $n \geq 1$ in $a \neq 0$. Izrek se največkrat pripisuje *Carlu Friedrichu Gaussu*, čeprav njegov originalni dokaz ni izpolnjeval današnjih standardov matematične strogosti. Prvi popoln dokaz naj bi leta 1806 podal ljubiteljski matematik *Jean-Robert Argand*. Res pa je kasneje Gauss našel tudi povsem nesporne dokaze.

Vpeljave racionalnih, realnih in kompleksnih števil imajo skupno značilnost. Pri vseh je bil osnovni vzvod nerešljivost polinomskih enačb, torej neobstoj ničel polinomov, v dotlej znanih množicah števil. Racionalna števila so ničle linearnih polinomov $nX - m$, ki nimajo (nujno) ničel v $\mathbb{Z}$. Polinomi kot na primer $X^2 - 2$ nimajo ničel v $\mathbb{Q}$, kar je vodilo do vpeljave realnih števil. Podobno polinom $X^2 + 1$ nima ničle v $\mathbb{R}$, kar je napeljalo h konstrukciji kompleksnih števil. Reševanje polinomskih enačb je torej odigralo eno ključnih vlog v zgodovini matematike. Klasična algebra se je pravzaprav ukvarjala izključno s polinomskimi enačbami. Šele v 19. stoletju se je z vpeljavo prvih abstraktnih algebrskih struktur odlepila od te teme in začela prehajati v abstraktno (ali moderno) algebro, kot jo poznamo danes in jo obravnava ta knjiga.

Na kratko se sprehodimo skozi zgodovino reševanja polinomskih enačb.

Linearne in kvadratne enačbe so znali rešiti v različnih starih kulturah. Že Babilonci so reševali kvadratne enačbe na način, ki se v svojem bistvu ne razlikuje veliko od današnjega. To seveda ne pomeni, da so poznali koncept enačbe v današnjem smislu. Naloge so bile podane le z besedami, brez matematičnih simbolov, in v njih so nastopala konkretna (in to zgolj pozitivna racionalna) števila. Tudi razvoj simboličnega označevanja polinomskih enačb ima dolgo in zanimivo zgodovino, a o podrobnostih tu ne bomo govorili. Povejmo le, da je bila pot do zapisa splošne kvadratne enačbe v obliki

$$ax^2 + bx + c = 0$$

in njene rešitve kot

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a} \tag{7.1}$$

dolga.

Od rešitve kvadratne do rešitve kubične enačbe (tj. enačbe tretje stopnje) je trajalo kaka tri tisočletja, vse do obdobja renesanse. Slednjo, kot tudi rešitev enačbe četrte stopnje, je v knjigi *Velika umetnost* leta 1545 opisal italijanski matematik *Gerolamo Cardano*. Rešitvi sicer nista bili njegovi; predstavil je izsledke *Scipiona del Ferra*, *Niccola F. Tartaglia* in *Ludovica Ferrarija*.

Iz Cardanovega besedila se da izluščiti, da lahko rešitev enačbe

$$x^3 = px + q$$

izrazimo kot

$$x = \sqrt[3]{\frac{q}{2} + \sqrt{\left(\frac{q}{2}\right)^2 - \left(\frac{p}{3}\right)^3}} + \sqrt[3]{\frac{q}{2} - \sqrt{\left(\frac{q}{2}\right)^2 - \left(\frac{p}{3}\right)^3}}. \tag{7.2}$$

Temu danes pravimo **Cardanova formula**. Lahko jo uporabimo za kompleksne koeficiente p in q in dobimo kompleksne rešitve x, kar v Cardanovem času sicer še ni bilo znano. Morda še bolj zanimivo je, da so lahko vse rešitve x kot tudi oba koeficienta p in q realna števila, v formuli pa se vseeno pojavijo kompleksna števila (če je $\left(\frac{q}{2}\right)^2 - \left(\frac{p}{3}\right)^3 < 0$). Pri seštevanju se imaginarni deli tedaj seveda izničijo. To je lep, klasičen zgled uporabnosti kompleksnih števil (gl. nalogo 5).

Splošno kubično enačbo

$$ax^3 + bx^2 + cx + d = 0,$$

kjer $a \neq 0$, prevedemo na zgornji primer z vpeljavo nove spremenljivke $u := x + \frac{b}{3a}$. Enačbo četrte stopnje pa z nekaj truda prevedemo na kubično enačbo. V Cardanovi formuli je torej skrito bistvo reševanja enačb tretje in četrte stopnje.

Naslednji izziv je bila **enačba pete stopnje**. Po osnovnem izreku algebre taka enačba zanesljivo ima rešitve, toda kako jih izraziti? Rešitve polinomskih enačb nižjih stopenj lahko izrazimo s koeficienti polinoma z uporabo operacij seštevanja, odštevanja, množenja, deljenja in korenjenja (kot v formulah (7.1) in (7.2)). Dejansko poznamo postopke ali kar formule, ki vodijo do rešitev. Po uspehih italijanskih matematikov iz 16. stoletja bi seveda pričakovali odkritje podobnega postopka za enačbe pete stopnje. Najbrž le bolj zapletenega in zato težje izsledljivega. Vsi poskusi njegovega odkrivanja so bili dolgo neuspešni – dokler se ni izkazalo nekaj bistveno bolj zanimivega: tak postopek sploh ne more obstajati. Ta presenetljivi rezultat je leta 1799 objavil italijanski matematik *Paolo Ruffini*, toda njegov dokaz je bil nepopoln. Prvi korekten dokaz je podal *Niels Henrik Abel* leta 1824. O Abelu, kot tudi o *Évaristu Galoisu*, smo spregovorili že v razdelku 1.3. Prav Galoisu se je posrečil naslednji veliki preboj. Izdelal je teorijo, ki, povedano v modernem jeziku, opisuje zvezo med razširitvami polj in (končnimi) grupami. Pojem grupe je tudi vpeljal in sicer kot, spet povedano v našem jeziku, podgrupo simetrične grupe. Po Cayleyevem izreku je ta definicija v bistvu ekvivalentna naši (gl. razdelek 3.5). Galoisova teorija prevede problem rešljivosti enačb s pomočjo osnovnih računskih operacij in korenjenja na problem iz teorije grup. Preko tega se lahko najdejo konkretni polinomi stopnje 5 (ali več), katerih ničle ne moremo izraziti z njihovimi koeficienti z uporabo seštevanja, odštevanja, množenja, deljenja in korenjenja. Preprost primer je polinom $f(X) = X^5 - X - 1$.

Nekateri Galoisovo teorijo štejejo za prelom, ko je klasična algebra prešla v abstraktno algebro. Še zdaj, po skoraj dvesto letih, velja za enega največjih in najlepših dosežkov matematike. Žal pa nekoliko presega okvir te knjige.

Naloge

1. Naj bo n naravno število, ki ni kvadrat nobenega naravnega števila. Pokaži, da $\sqrt{n} \notin \mathbb{Q}$.
2. Pokaži, da $\sqrt{2} + \sqrt{3} \notin \mathbb{Q}$.
3. Pokaži, da $\log_2 3 \notin \mathbb{Q}$.
4. Pokaži, da za vsako naravno število s velja
$$\frac{1}{s+1} + \frac{1}{(s+1)(s+2)} + \frac{1}{(s+1)(s+2)(s+3)} + \cdots < 1.$$
Od tod izpelji, da število $e = \sum_{n=0}^{\infty} \frac{1}{n!}$ ni oblike $\frac{r}{s}$, $r, s \in \mathbb{N}$, da torej $e \notin \mathbb{Q}$.
Komentar. Obe znameniti matematični konstanti π in e sta torej iracionalni števili. To lahko dokažemo še za marsikatero drugo znano število. Še vedno pa se denimo ne ve, če sta iracionalni tudi števili $\pi + e$ in πe. Nasploh dokazovanje iracionalnosti števila ni vedno lahka naloga.
5. S pomočjo Cardanove formule poišči celoštevilsko rešitev enačbe $x^3 = 15x + 4$. Lahko si pomagaš tudi z enakostima $(2 + i)^3 = 2 + 11i$ in $(2 - i)^3 = 2 - 11i$.
Komentar. Ta enačba skupaj z nakazanim načinom reševanja je zgodovinsko pomembna, povezuje se celo z rojstvom kompleksnih števil. Obravnavana je bila v knjigi *Algebra* italijanskega matematika *Rafaela Bombellija* iz leta 1572. Razvoj kompleksnih števil zatem je bil sicer počasen. Med matematiki so bila zares sprejeta šele v 19. stoletju.

7.2. Algebraični in transcendentni elementi

V tem razdelku pričenjamo s sistematično obravnavo polj in njihovih razširitev. Pri tem se bomo naslanjali na teorijo iz prejšnjega poglavja. Kot je razvidno iz prejšnjega razdelka, je namreč študij razširitev polj tesno povezan s študijem polinomov, še zlasti s študijem njihovih ničel.

V abstraktno teorijo se težko vživimo brez konkretnih zgledov. Zato se za uvod spomnimo primerov polj, ki smo jih že srečali:

- Osnovni primeri polj so stari znanci $\mathbb{Q}$, $\mathbb{R}$ in $\mathbb{C}$. V primeru 1.88 smo omenili polje $\mathbb{Q}(i) = \{p + qi \mid p, q \in \mathbb{Q}\}$, v nalogah pa smo srečali še nekaj podobnih primerov podpolj polja realnih ali kompleksnih števil.
- Za vsako praštevilo p je kolobar $\mathbb{Z}_p$ polje (trditev 2.15).

- V razdelku 3.6 smo se seznanili s poljem ulomkov celega kolobarja. Zanimiv poseben primer je polje racionalnih funkcij $F(X)$.

Kako priti do novih primerov? V tem razdelku se bomo seznanili s pojmom algebraičnega elementa, v naslednjem pa pokazali, da vsak tak element porodi polje, ki ima enostaven, takoj razumljiv opis.

Še nekaj besed pred definicijo. Realna števila delimo na racionalna in iracionalna. Šolska primera iracionalnih števil sta $\sqrt{2}$ in π. Vendar pa je v nekem smislu π dlje od racionalnih števil kot $\sqrt{2}$. Izkaže se namreč, da za poljubna racionalna števila $q_0, \ldots, q_n$, ki niso vsa enaka 0, velja

$$q_0 + q_1\pi + \cdots + q_{n-1}\pi^{n-1} + q_n\pi^n \neq 0.$$

Z drugimi besedami, π ni ničla neničelnega polinoma iz $\mathbb{Q}[X]$. Kot iracionalno število $\sqrt{2}$ sicer ni ničla nobenega linearnega polinoma iz $\mathbb{Q}[X]$, seveda pa je ničla polinoma $X^2 - 2$. Zato rečemo, da je število $\sqrt{2}$ algebraično, medtem ko števila, kot je π, imenujemo transcendentna. Definiciji obeh pojmov podajmo v večji splošnosti.

Definicija 7.1. Naj bo a element iz neke razširitve E polja F. Pravimo, da je a **algebraičen nad** F, če obstaja tak neničeln polinom $f(X) \in F[X]$, da je $f(a) = 0$. Če a ni algebraičen nad F, rečemo, da je a **transcendenten nad** F.

Neničelnih polinomov, katerih ničla je algebraičen element, je več; en pa je posebej odlikovan.

Definicija 7.2. Polinomu $p(X) \in F[X]$ pravimo **minimalni polinom** algebraičnega elementa $a \in E$, če je $p(a) = 0$, $p(X)$ ima vodilni koefiecient enak 1 in izmed vseh neničelnih polinomov iz $F[X]$, katerih ničla je a, ima $p(X)$ najnižjo stopnjo. Če je $\mathrm{st}(p(X)) = n$, rečemo, da je a **algebraičen stopnje** n (nad F).

Obstoj minimalnega polinoma algebraičnega elementa a je očiten. Res, izberimo katerikoli polinom $f(X)$ najnižje stopnje, katerega ničla je a. Če je λ njegov vodilni koeficient, potem je $p(X) := \lambda^{-1} f(X)$ minimalni polinom. Njegova stopnja je namreč enaka stopnji $f(X)$, vodilni koeficient pa je enak 1. Zahteva, da je vodilni koeficient minimalnega polinoma enak 1, sama po sebi nima globljega pomena, ima pa za posledico *enoličnost*. Namreč, če bi bil $p_1(X)$ neki drugi minimalni polinom, bi bil element a ničla neničelnega polinoma $p(X) - p_1(X)$, ki ima nižjo stopnjo kot $p(X)$.

Naslednji izrek nam da celovitejši pogled na pojem minimalnega polinoma.

Izrek 7.3. *Naj bo element $a \in E$ algebraičen nad F in naj bo $p(X) \in F[X]$ tak polinom z vodilnim koeficientom* 1*, da je $p(a) = 0$. Naslednje trditve so si ekvivalentne:*

(i) $p(X)$ *je minimalni polinom elementa* a.
(ii) $p(X)$ *je nerazcepen v* $F[X]$.
(iii) $p(X)$ *deli vsak polinom* $f(X) \in F[X]$, *za katerega je* $f(a) = 0$.

Dokaz. (i)⇒(ii). Če minimalni polinom $p(X)$ zapišemo kot $g(X)h(X)$ za neka polinoma $g(X), h(X) \in F[X]$, potem je $g(a)h(a) = p(a) = 0$ in zato $g(a) = 0$ ali $h(a) = 0$. Privzemimo prvo možnost. Zaradi minimalnosti $p(X)$ je potem $\mathrm{st}(g(X)) \geq \mathrm{st}(p(X))$, iz $p(X) = g(X)h(X)$ pa sledi obratna neenakost. Torej imata $g(X)$ in $p(X)$ isto stopnjo, kar dokazuje nerazcepnost polinoma $p(X)$.

(ii)⇒(iii). Kot se takoj prepričamo, je množica

$$\mathcal{I} := \{f(X) \in F[X] \mid f(a) = 0\}$$

ideal kolobarja $F[X]$. Po izreku 6.23 obstaja tak polinom $p_1(X) \in F[X]$, da je $\mathcal{I} = (p_1(X))$. Torej je $p(X) = q(X)p_1(X)$ za neki polinom $q(X) \in F[X]$. Ker je $p(X)$ nerazcepen in ker $p_1(X)$ ni konstanten polinom (saj je $p_1(a) = 0$), je konstanten polinom $q(X)$. Zato je

$$(p(X)) = (p_1(X)) = \mathcal{I}.$$

To pa je le drugačen zapis trditve (iii).

(iii)⇒(i). To je očitno, saj je neničeln polinom lahko deljiv samo s polinomom kvečjemu nižje stopnje. □

Pojma »nerazcepen polinom« in »minimalni polinom« sta torej tesno povezana. Kandidata za minimalni polinom danega elementa včasih hitro najdemo, pri preverjanju, ali je res pravi, pa si včasih težko pomagamo z definicijo. Lažje je obravnavati nerazcepnost.

Zdaj lahko preidemo na primere.

Primer 7.4. Elementi iz F so algebraični stopnje 1 nad F. Res, vsak $a \in F$ je ničla polinoma $X - a \in F[X]$. Tudi obratno, če je a algebraičen stopnje 1 nad F, je $a \in F$ (zakaj?).

Primer 7.5. Vsak $z \in \mathbb{C}$ je algebraičen nad $\mathbb{R}$. Namreč, z je ničla polinoma

$$(X - z)(X - \overline{z}) = X^2 - (z + \overline{z})X + z\overline{z} \in \mathbb{R}[X].$$

Števili $z + \overline{z}$ in $z\overline{z}$ sta namreč realni. Stopnja algebraičnosti z nad $\mathbb{R}$ je torej enaka 2 (če $z \notin \mathbb{R}$) ali 1 (če $z \in \mathbb{R}$).

Primer 7.6. Naj bo F poljubno polje. Polje racionalnih funkcij $F(X)$ (primer 3.53) je njegova razširitev in element X iz $F(X)$ je transcendenten nad F (to je očitno, le definicije moramo dobro razumeti!).

V klasičnem in tudi za nas najzanimivejšem primeru je $F = \mathbb{Q}$ in $E = \mathbb{C}$. Algebraičnim elementom tedaj pravimo **algebraična števila**, transcendentnim pa **transcendentna števila**. Kompleksno število a je torej algebraično

število, če obstaja tak neničeln polinom $f(X) \in \mathbb{Q}[X]$, da je $f(a) = 0$. Mimogrede, če $f(X)$ pomnožimo s skupnim večkratnikom imenovalcev njegovih koeficientov, dobimo polinom s celoštevilskimi koeficienti, katerega ničla je a. Zato lahko v definiciji algebraičnega števila $\mathbb{Q}[X]$ nadomestimo z $\mathbb{Z}[X]$.

PRIMER 7.7. Število i je ničla polinoma $X^2 + 1 \in \mathbb{Q}[X]$ in je zato algebraično stopnje 2.

PRIMER 7.8. Naj bo p praštevilo. Število $\sqrt[n]{p}$ je algebraično stopnje n. Polinom $X^n - p$ je namreč nerazcepen v $\mathbb{Q}[X]$ po Eisensteinovem kriteriju (gl. primer 6.37) in je zato po izreku 7.3 minimalni polinom števila $\sqrt[n]{p}$.

PRIMER 7.9. Z nekaj znanja o kardinalnih številih lahko dokažemo, da je množica vseh algebraičnih števil števna (množica vseh polinomov z racionalnimi koeficienti je števna, vsak izmed njih ima končno mnogo ničel). Zato transcendentna števila obstajajo. Še več, množica vseh transcendentnih števil je neštevna. Kljub temu za nobeno konkretno število ni lahko pokazati, da je transcendentno. Morda še najlažje za **Liouvillovo konstanto** $\sum_{n=1}^{\infty} 10^{-n!}$, pa tudi to vzame kar nekaj prostora in se zato temu raje izognimo. Omenili smo že, da je število π transcendentno. Prav tako je transcendentno število e. Dokaza pa sta zahtevna. Vsaj za število π že dokaz iracionalnosti ni povsem enostaven. Lahko si mislimo, da je dokazati transcendentnost precej težje kot iracionalnost (ki pomeni le, da število ni algebraično stopnje 1).

V primerih 7.7 in 7.8 smo podali primere algebraičnih števil, ki se ponujajo sami od sebe. Kako priti do nadaljnjih primerov? Na primer, tudi število $\sqrt{2} + \sqrt{3}$ je algebraično. Če ga kvadriramo in se malo poigramo z dobljenim izrazom, hitro ugotovimo, da je ničla polinoma $X^4 - 10X^2 + 1$ (to je tudi minimalni polinom tega števila, gl. primer 7.25). Kaj pa, denimo, število $\sqrt{2} + \sqrt[3]{3}$? Tudi to število je algebraično, toda iskanje ustreznega polinoma terja malce več truda. To nalogo prepuščamo bralcu. V naslednjem razdelku bomo izpeljali bistveno splošnejše dejstvo: tako vsota, razlika, produkt kot inverz poljubnih algebraičnih elementov so spet algebraični elementi. Z drugimi besedami, algebraični elementi tvorijo polje. Do tega pa ne bomo prišli z iskanjem polinomov. Problema se bomo lotili bolj premišljeno.

Naloge

1. Naj bo a element razširitve E polja F. Denimo, da obstaja tak nekonstanten polinom $f(X) \in F[X]$, da je element $f(a)$ algebraičen nad F. Pokaži, da je potem tudi a algebraičen nad F.
2. Naj bo element $a \in E \setminus \{0\}$ algebraičen stopnje n nad F. Pokaži, da obstaja tak polinom $g(X) \in F[X]$ stopnje $n - 1$, da je $a^{-1} = g(a)$.

3. Naj bo element $a \in E$ algebraičen stopnje n nad F. Pokaži, da je za poljubna $\alpha, \beta \in F$, $\beta \neq 0$, tudi element $\alpha + \beta a$ algebraičen stopnje n.
4. Pojasni, zakaj element katerekoli razširitve polja $\mathbb{C}$ ne more biti algebraičen stopnje 2 ali več nad $\mathbb{C}$.
5. Pojasni, zakaj element katerekoli razširitve polja $\mathbb{R}$ ne more biti algebraičen stopnje 3 ali več nad $\mathbb{R}$.
6. Naj bo z algebraično število. Pokaži, da je tudi $\overline{z}$ algebraično število in da ima isti minimalni polinom kot z.
7. Pokaži, da je število $\sqrt{2+\sqrt{3+\sqrt{5}}}$ algebraično.
8. Pokaži, da je število $\sqrt{2} + i\sqrt{3}$ algebraično.
9. Pokaži, da je število $\sqrt{10} + \sqrt[4]{6}$ algebraično.
10. Naj bo p praštevilo. Pojasni, zakaj je ciklotomični polinom $\Phi_p(X)$ (gl. primer 6.38) minimalni polinom algebraičnega števila $\cos\frac{2\pi}{p} + i\sin\frac{2\pi}{p}$.
11. Poišči minimalni polinom algebraičnega števila $\cos\frac{2\pi}{6} + i\sin\frac{2\pi}{6}$.
12. Poišči minimalni polinom algebraičnega števila $\cos\frac{2\pi}{8} + i\sin\frac{2\pi}{8}$.

7.3. Končne razširitve

Pogosto se izkaže za koristno, če v matematičnem objektu prepoznamo kako algebrsko strukturo. Pri študiju razširitev polj je pomemben tale vidik: vsako razširitev E polja F lahko obravnavamo kot *vektorski prostor* nad F. Seveda je E kot polje aditivna grupa, za množenje s skalarji pa vzamemo kar dano množenje v E, le da je prvi faktor element iz F. Elemente iz F imamo tako za skalarje, elemente iz E pa za vektorje. Aksiomi za vektorski prostor so res izpolnjeni: enakosti $\lambda(x+y) = \lambda x + \lambda y$ in $(\lambda+\mu)x = \lambda x + \mu x$ sta posledici distributivnosti v E, $\lambda(\mu x) = (\lambda\mu)x$ je posledica asociativnosti v E, $1x = x$ pa sledi iz dejstva, da imata F in E isto enoto 1. Dejansko je E celo algebra nad F, toda to nam ne bo v posebno pomoč. Ključnega pomena je, da lahko govorimo o dimenziji E nad F.

Definicija 7.10. Naj bo polje E razširitev polja F. Pravimo, da je E **končna razširitev** F, če je E končno-razsežen vektorski prostor nad F. Dimenziji E nad F v tem primeru pravimo **stopnja razširitve** in jo označujemo z $[E : F]$.

V linearni algebri bi namesto $[E : F]$ pisali $\dim_F E$. Na različnih področjih so pač v navadi različne oznake.

Primer 7.11. Polje $\mathbb{C}$ je končna razširitev polja $\mathbb{R}$. Očiten primer baze vektorskega prostora $\mathbb{C}$ nad poljem $\mathbb{R}$ je množica $\{1, i\}$. Torej je $\mathbb{C}$ končna razširitev $\mathbb{R}$ in $[\mathbb{C} : \mathbb{R}] = 2$.

PRIMER 7.12. Bralec z osnovnim znanjem o kardinalnih številih bo hitro preveril, da je vsaka končna razširitev polja $\mathbb{Q}$ števna množica. Zato, denimo, polje $\mathbb{R}$ ni končna razširitev polja $\mathbb{Q}$. V primeru 7.27 bomo to (in več kot to) dokazali z algebraičnimi metodami.

Do nadaljnjih primerov in jasnejše predstave o končnih razširitvah bomo prišli proti koncu razdelka. Nadaljujemo z izrekom, ki pove, da je končna razširitev končne razširitve tudi sama končna razširitev.

IZREK 7.13. *Naj bo polje L končna razširitev polja F in naj bo polje E končna razširitev polja L. Potem je E končna razširitev F in velja*

$$[E : F] = [E : L] \cdot [L : F]. \tag{7.3}$$

DOKAZ. Naj bo $\{a_1, \ldots, a_m\}$ baza L nad F in $\{b_1, \ldots, b_n\}$ baza E nad L. Torej je $m = [L : F]$ in $n = [E : L]$. Pokažimo, da je množica

$$B := \{a_i b_j \mid i = 1, \ldots, m, j = 1, \ldots, n\}$$

baza E nad F. S tem bo izrek dokazan.

Vzemimo $x \in E$. Potem obstajajo taki $\ell_j \in L$, da je $x = \sum_{j=1}^{n} \ell_j b_j$. Vsak ℓ_j pa lahko zapišemo kot $\sum_{i=1}^{m} \lambda_{ij} a_i$ za neke $\lambda_{ij} \in F$. Zato je

$$x = \sum_{j=1}^{n} \Big(\sum_{i=1}^{m} \lambda_{ij} a_i \Big) b_j = \sum_{j=1}^{n} \sum_{i=1}^{m} \lambda_{ij} a_i b_j.$$

Torej je B ogrodje E nad F.

Pokažimo še, da je B linearno neodvisna množica. Privzemimo, da so $\lambda_{ij} \in F$ taki, da je

$$\sum_{j=1}^{n} \sum_{i=1}^{m} \lambda_{ij} a_i b_j = 0.$$

Če zapišemo to enakost v obliki

$$\sum_{j=1}^{n} \Big(\sum_{i=1}^{m} \lambda_{ij} a_i \Big) b_j = 0$$

in upoštevamo, da so $b_1, \ldots, b_n$ linearno neodvisni nad L, sledi

$$\sum_{i=1}^{m} \lambda_{ij} a_i = 0$$

za vsak j. Ker so $a_1, \ldots, a_m$ linearno neodvisni nad F, morajo biti vsi λ_{ij} enaki 0. □

Ta izrek ima v teoriji končnih razširitev podobno vlogo kot Lagrangeov izrek v teoriji končnih grup. Posebej uporabna je tale posledica izreka.

POSLEDICA 7.14. *Naj bo polje E končna razširitev polja F. Če je L podpolje E, ki vsebuje F, potem $[L : F]$ deli $[E : F]$.*

Dokaz. Ker je E končna razširitev F, je tudi končna razširitev L. Namreč, če je $\{c_1, \ldots, c_r\}$ ogrodje vektorskega prostora E nad poljem F, je tudi ogrodje vektorskega prostora E nad poljem L. Seveda je tudi L končna razširitev F (podprostor končno-razsežnega prostora je končno-razsežen). Zato velja enakost (7.3). □

Z naslednjo definicijo se vračamo na tematiko prejšnjega razdelka. Razlika je, da zdaj ne bomo obravnavali le posameznih, pač pa vse elemente razširitve danega polja. Tak pristop je za algebro značilen – tudi informacije o enem samem elementu pogosto laže dobimo tako, da si ogledamo algebrsko strukturo, ki ji ta element pripada.

Definicija 7.15. Razširitev E polja F je **algebraična**, če je vsak element iz E algebraičen nad F. Razširitev, ki ni algebraična, se imenuje **transcendentna**.

Pogoj, da je element $a \in E$ algebraičen nad F, torej da je

$$\lambda_0 + \lambda_1 a + \cdots + \lambda_n a^n = 0$$

za neki $n \in \mathbb{N}$ in neke $\lambda_i \in F$, ki niso vsi enaki 0, lahko ekvivalentno opišemo kot linearno odvisnost elementov $1, a, \ldots, a^n \in E$ nad F. Ta interpretacija algebraičnosti je lahko zelo koristna.

Trditev 7.16. *Vsaka končna razširitev je algebraična.*

Dokaz. Naj bo $[E : F] = n$. Za vsak $a \in E$ so potem elementi $1, a, \ldots, a^n$ linearno odvisni nad F, saj jih je več od dimenzije prostora. Torej je a algebraičen nad F. □

Opomba 7.17. Iz dokaza je razvidno, da je vsak element iz E algebraičen stopnje največ n nad F, če je $n = [E : F]$. Iz $[\mathbb{C} : \mathbb{R}] = 2$ tako sledi, da je vsak $z \in \mathbb{C} \setminus \mathbb{R}$ algebraičen stopnje 2 nad $\mathbb{R}$, kar pa že vemo (gl. primer 7.5).

Obrat trditve 7.16 ne velja, algebraična razširitev ni nujno končna (gl. primer 7.27). Kot bomo kmalu videli, pa so končne razširitve tesno povezane z algebraičnimi elementi.

Vpeljimo nekaj oznak. Vnaprej opozorimo bralca, da so usklajene z oznakami za kolobar polinomov $F[X]$ (oglati oklepaj) in polje racionalnih funkcij $F(X)$ (navadni oklepaj). Naj bo polje E razširitev polja F in naj bo A podmnožica E. S $F[A]$ označujemo *podkolobar* E, generiran s F in A, s $F(A)$ pa *podpolje* E, generirano s F in A. Če je $A = \{a_1, \ldots, a_n\}$, namesto $F[A]$ oziroma $F(A)$ pišemo $F[a_1, \ldots, a_n]$ oziroma $F(a_1, \ldots, a_n)$. Največkrat bomo imeli opravka s primerom, ko ima A en sam element, torej s kolobarjem $F[a]$ in poljem $F(a)$. S sklicem na razdelek 1.7 ali pa kar neposredno ugotovimo, da $F[a]$ sestoji iz elementov oblike

$$\lambda_0 + \lambda_1 a + \cdots + \lambda_r a^r, \quad \lambda_i \in F,$$

$F(a)$ pa iz elementov oblike xy^{-1}, kjer $x, y \in F[a]$ in $y \neq 0$. Povedano drugače,

$$F[a] = \{f(a) \mid f(X) \in F[X]\} \tag{7.4}$$

in

$$F(a) = \{f(a)g(a)^{-1} \mid f(X), g(X) \in F[X], g(a) \neq 0\}. \tag{7.5}$$

Podobno opišemo $F[A]$ in $F(A)$, le da nastopajo polinomi več spremenljivk. Tako na primer $F[a_1, \ldots, a_n]$ sestavljajo elementi oblike

$$f(a_1, \ldots, a_n),$$

kjer je $f(X_1, \ldots, X_n) \in F[X_1, \ldots, X_n]$.

Polje $F(a)$ imenujemo **razširitev polja** F **s priključitvijo elementa** a. Pravimo, da je E **enostavna razširitev** polja F, če obstaja tak $a \in E$, da je $E = F(a)$. Elementu a tedaj pravimo **primitivni element** razširitve E.

V naslednjem izreku bomo videli, da se opis polja $F(a)$ iz (7.5) precej poenostavi, če je element a algebraičen. Najprej pa preprost zgled.

PRIMER 7.18. Imaginarna enota i je primer algebraičnega števila stopnje 2. Ker je $i^n \in \{1, -1, i, -i\}$ za vse $n \in \mathbb{N}$, za poljuben polinom $f(X) \in \mathbb{Q}[X]$ velja $f(i) = \lambda_0 + \lambda_1 i$ za neka $\lambda_0, \lambda_1 \in \mathbb{Q}$. Tako nič ne izgubimo, če se v (7.4) omejimo le na linearne polinome $f(X)$. Ker je kolobar $\mathbb{Q}[i] = \{\lambda_0 + \lambda_1 i \mid \lambda_i \in \mathbb{Q}\}$ že sam polje (primer 1.88), je $\mathbb{Q}[i] = \mathbb{Q}(i)$. Podobno je $\mathbb{R}[i] = \mathbb{R}(i) = \mathbb{C}$. Polje kompleksnih števil je torej enostavna razširitev polja realnih števil, primer primitivnega elementa pa je imaginarna enota i.

IZREK 7.19. *Naj bo polje E razširitev polja F. Če je element $a \in E$ algebraičen stopnje n nad F, potem je*

$$F(a) = F[a] = \{\lambda_0 + \lambda_1 a + \cdots + \lambda_{n-1} a^{n-1} \mid \lambda_i \in F\} \tag{7.6}$$

končna razširitev F in $[F(a) : F] = n$.

DOKAZ. Vsak element iz $F[a]$ lahko zapišemo kot $f(a)$ za neki polinom $f(X) \in F[X]$. Denimo, da je $f(a) \neq 0$. Označimo s $p(X)$ minimalni polinom elementa a. Ker je $p(X)$ nerazcepen (izrek 7.3) in ne deli $f(X)$ (saj $f(a) \neq 0$), sta si $p(X)$ in $f(X)$ tuja. Zato obstajata taka polinoma $h(X), k(X) \in F[X]$, da je

$$p(X)h(X) + f(X)k(X) = 1$$

(posledica 6.25). Ker je $p(a) = 0$, od tod sledi $f(a)k(a) = 1$. Torej je $f(a)^{-1} = k(a) \in F[a]$. S tem smo dokazali, da je $F[a]$ polje. Tako je $F[a] = F(a)$. Dokazati moramo še, da lahko $f(a)$ zapišemo kot vrednost polinoma stopnje manj kot n v a. Za to uporabimo osnovni izrek o deljenju. Naj bosta $q(X), r(X) \in F[X]$ taka polinoma, da je $f(X) = q(X)p(X) + r(X)$ in je $r(X) = 0$ ali pa je $\mathrm{st}(r(X)) < n$. Od tod sledi $f(a) = r(a)$. S tem je enakost (7.6) dokazana.

Iz (7.6) vidimo, da je množica $\{1, a, \ldots, a^{n-1}\}$ ogrodje vektorskega prostora $F(a)$ nad poljem F. Ker je stopnja minimalnega polinoma elementa a enaka n, je ta množica linearno neodvisna. Torej je baza prostora; ker ima n elementov, je $[F(a) : F] = n$. □

Izrek med drugim pove, da je kolobar $F[a]$ polje. Za algebraičen element a je zato vseeno, katero izmed oznak $F[a]$ in $F(a)$ uporabimo. Ponavadi bomo dali prednost drugi.

PRIMER 7.20. Če je p praštevilo in n poljubno naravno število, je $\sqrt[n]{p}$ algebraično število stopnje n (primer 7.8). Zato je $[\mathbb{Q}(\sqrt[n]{p}) : \mathbb{Q}] = n$, množica $\{1, \sqrt[n]{p}, \sqrt[n]{p^2}, \ldots, \sqrt[n]{p^{n-1}}\}$ pa je baza vektorskega prostora $\mathbb{Q}(\sqrt[n]{p})$ nad poljem $\mathbb{Q}$. Tako je denimo

$$\mathbb{Q}(\sqrt{2}) = \{\lambda_0 + \lambda_1\sqrt{2} \mid \lambda_i \in \mathbb{Q}\},$$
$$\mathbb{Q}(\sqrt[3]{2}) = \{\lambda_0 + \lambda_1\sqrt[3]{2} + \lambda_2\sqrt[3]{4} \mid \lambda_i \in \mathbb{Q}\} \text{ ipd.}$$

OPOMBA 7.21. Za vsak element $a \in E$, algebraičen ali transcendenten, je preslikava $\varphi : F[X] \to F[a]$, $\varphi(f(X)) = f(a)$, očitno epimorfizem kolobarjev.

(a) Naj bo element a algebraičen nad F. Potem je $\ker\varphi = (p(X))$, kjer je $p(X)$ minimalni polinom elementa a (izrek 7.3). Po izreku o izomorfizmu je zato

$$F[a] \cong F[X]/(p(X)).$$

Iz posledice 6.24 tako tudi od tod sledi, da je $F[a]$ polje in zato $F[a] = F(a)$.

(b) Naj bo sedaj element a transcendenten nad F. Potem je

$$F[a] \cong F[X] \text{ in } F(a) \cong F(X).$$

Res, epimorfizem φ je injektiven, torej izomorfizem, in s prav tako naravnim predpisom $f(X)g(X)^{-1} \mapsto f(a)g(a)^{-1}$ ga razširimo na izomorfizem iz $F(X)$ v $F(a)$. V tem primeru kolobar $F[a]$ ni polje in zato je $F[a] \subsetneq F(a)$.

OPOMBA 7.22. Eno izmed sporočil izreka 7.19 je, da za algebraičen element $a \in E$ nad poljem F velja

$$[F(a) : F] = \text{stopnja algebraičnosti } a,$$

torej stopnja minimalnega polinoma tega elementa. Če je L polje, ki leži med F in E, je a seveda algebraičen tudi nad L, stopnja algebraičnosti nad L pa je kvečjemu manjša kot stopnja algebraičnosti nad F. Slednje lahko zapišemo tudi s formulo:

$$[L(a) : L] \leq [F(a) : F].$$

Nadaljujmo z obravnavo splošnejše situacije, ko polju priključimo ne le enega samega, pač pa končen nabor algebraičnih elementov.

IZREK 7.23. *Naj bo polje E razširitev polja F. Če so elementi $a_1, \ldots, a_n \in E$ algebraični nad F, potem je $F(a_1, \ldots, a_n)$ končna razširitev F. Ob tem velja*

$$F(a_1, \ldots, a_n) = F[a_1, \ldots, a_n]. \tag{7.7}$$

DOKAZ. Za $n = 1$ nam to pove izrek 7.19. Zato smemo predpostaviti, da izrek velja za $n - 1$ elementov, torej da je

$$L := F(a_1, \ldots, a_{n-1})$$

končna razširitev F in da je

$$L = F[a_1, \ldots, a_{n-1}].$$

Ker je a_n algebraičen nad poljem F, je algebraičen tudi nad L. Izrek 7.19 tako pove, da je $L(a_n)$ končna razširitev polja L. Potem pa je po izreku 7.13 to polje tudi končna razširitev polja F. Njegove elemente lahko, spet po izreku 7.19, zapišemo kot vsote izrazov oblike

$$f(a_1, \ldots, a_{n-1})a_n^k,$$

kjer je $f(X_1, \ldots, X_{n-1}) \in F[X_1, \ldots, X_{n-1}]$ in $k \geq 0$. To pa so natanko elementi oblike

$$g(a_1, \ldots, a_{n-1}, a_n),$$

kjer je $g(X_1, \ldots, X_{n-1}, X_n) \in F[X_1, \ldots, X_{n-1}, X_n]$. Torej je

$$L(a_n) = F[a_1, \ldots, a_{n-1}, a_n]. \tag{7.8}$$

Kolobar $F[a_1, \ldots, a_n]$ je torej polje, kar je le z besedami izražena enakost (7.7). □

Skupaj z enakostjo (7.8) izrek pove, da za vse algebraične elemente a_i velja

$$F(a_1, \ldots, a_n) = \big(F(a_1, \ldots, a_{n-1})\big)(a_n) = F[a_1, \ldots, a_n].$$

Od tod hitro izpeljemo, da je

$$F(a_1, \ldots, a_n) = \big(F(a_1, \ldots, a_k)\big)(a_{k+1}, \ldots, a_n)$$

za vse $1 \leq k \leq n$.

PRIMER 7.24. Polje $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ lahko predstavimo kot $(\mathbb{Q}(\sqrt{2}))(\sqrt{3})$. Njegove elemente tako lahko zapišemo kot $a + b\sqrt{3}$, kjer sta $a, b \in \mathbb{Q}(\sqrt{2})$. Zato je

$$\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \{\lambda_0 + \lambda_1\sqrt{2} + \lambda_2\sqrt{3} + \lambda_3\sqrt{6} \mid \lambda_i \in \mathbb{Q}\}.$$

Pokažimo, da je

$$[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 4. \tag{7.9}$$

Vsak element iz $\mathbb{Q}(\sqrt{2},\sqrt{3})$ je linearna kombinacija štirih elementov, namreč 1, $\sqrt{2}$, $\sqrt{3}$ in $\sqrt{6}$, zato je $[\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}]\leq 4$. Ker je $\mathbb{Q}(\sqrt{2})\subseteq\mathbb{Q}(\sqrt{2},\sqrt{3})$ in je $[\mathbb{Q}(\sqrt{2}):\mathbb{Q}]=2$, je glede na posledico 7.14 število $[\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}]$ lahko enako le 2 ali 4. Prvo možnost bomo izločili, če pokažemo, da $\sqrt{3}$ ne moremo zapisati kot $\lambda+\mu\sqrt{2}$ za neka $\lambda,\mu\in\mathbb{Q}$ (zakaj?). To pa ni težka naloga in jo prepuščamo bralcu. Izraza kvadriramo, potem pa se vse odvije samo od sebe.

Velja tudi obrat izreka 7.23: vsaka končna razširitev E polja F je oblike $F(a_1,\ldots,a_n)$ za neke algebraične elemente $a_1,\ldots,a_n$. Ti elementi niso enolično določeni, lahko vzamemo na primer kar elemente kake baze E nad F (da so algebraični, sledi iz trditve 7.16). V poljih s karakteristiko 0 lahko, na prvi pogled presenetljivo, elemente $a_1,\ldots,a_n$ nadomestimo z enim samim elementom. Natančneje, vsaka končna razširitev polja F s karakteristiko 0 je enostavna, torej oblike $F(a)$ za neki algebraičen element a. To je **izrek o primitivnem elementu**. Dokaz bomo izpustili, ker izreka v nadaljevanju ne bomo potrebovali. Oglejmo si samo preprost zgled.

Primer 7.25. Pokažimo, da je

$$\mathbb{Q}(\sqrt{2},\sqrt{3})=\mathbb{Q}(\sqrt{2}+\sqrt{3}). \tag{7.10}$$

Označimo $\sqrt{2}+\sqrt{3}$ z a. Zadošča dokazati, da $\sqrt{2},\sqrt{3}\in\mathbb{Q}(a)$ in da $a\in\mathbb{Q}(\sqrt{2},\sqrt{3})$. Slednje je očitno. Dokažimo torej prvo. Dovolj je, če pokažemo, da je $\sqrt{2}\in\mathbb{Q}(a)$, saj potem iz $\sqrt{3}=a-\sqrt{2}$ sledi, da je tudi $\sqrt{3}\in\mathbb{Q}(a)$. Kvadrirajmo enakost $a-\sqrt{2}=\sqrt{3}$. Dobimo $a^2-2a\sqrt{2}+2=3$ in od tod $\sqrt{2}=\frac{1}{2}(a-a^{-1})$. To pa že pove, da je $\sqrt{2}\in\mathbb{Q}(a)$, saj je $\mathbb{Q}(a)$ polje in zato vsebuje a^{-1} (lahko izpeljemo tudi $\sqrt{2}=\frac{1}{2}(-9a+a^3)$ in s tem izrazimo $\sqrt{2}$ kot element $\mathbb{Q}(a)$ na standarden način, kot v izreku 7.19). Omenimo še, da iz (7.9) in (7.10) sledi, da je stopnja algebraičnosti števila $\sqrt{2}+\sqrt{3}$ enaka 4.

Naslednjo posledico izreka 7.23 smo napovedali na koncu prejšnjega razdelka.

Posledica 7.26. *Naj bo polje E razširitev polja F. Množica vseh elementov iz E, ki so algebraični nad F, je podpolje polja E.*

Dokaz. Označimo to množico z A. Seveda A vsebuje F, zato $A\neq\{0\}$. Vzemimo poljubna elementa $a,b\in A$. Po izreku 7.23 je $F(a,b)$ končna razširitev F. Trditev 7.16 tako pove, da je $F(a,b)\subseteq A$. Med drugim zato A vsebuje elemente $a-b$, ab in, če $a\neq 0$, tudi a^{-1}. Zato je A podpolje. □

Primer 7.27. Množica vseh algebraičnih števil je torej polje. To je primer algebraične razširitve polja $\mathbb{Q}$, ki ni končna. Namreč, nobena razširitev $\mathbb{Q}$, ki vsebuje $\sqrt[n]{2}$ za poljuben $n\in\mathbb{N}$, ne more biti končna. Res, če bi tako polje, imenujmo ga L, bilo končna razširitev $\mathbb{Q}$, bi bilo po posledici 7.14 število $[L:\mathbb{Q}]$ deljivo z $n=[\mathbb{Q}(\sqrt[n]{2}):\mathbb{Q}]$ (gl. primer 7.20). Ker je n poljuben, je to seveda nemogoče.

V naslednjem razdelku si bomo ogledali presenetljivo uporabo teorije, ki smo jo v tem izpeljali.

Naloge

1. Pokaži, da je $\mathbb{R}(a) = \mathbb{C}$ za vsak $a \in \mathbb{C} \setminus \mathbb{R}$.

   Komentar. Eden izmed namenov te naloge je opozoriti, da primitivni element razširitve ni en sam.
2. Naj bo $[E : F] = 12$. Pojasni, zakaj element iz E ne more biti algebraičen stopnje 8 nad F. Ali je lahko algebraičen stopnje 4?
3. Ugotovi, za katera naravna števila k v polju $\mathbb{Q}(\sqrt[12]{2})$ obstajajo elementi, ki so algebraični stopnje k nad $\mathbb{Q}$. Za vsak tak k poišči primer takega elementa.
4. Naj bo n liho število. Pokaži, da za vsak $a \in \mathbb{Q}(\sqrt[n]{2}) \setminus \mathbb{Q}$ velja $a^2 \notin \mathbb{Q}$.

   Namig. Izogni se računanju in uporabi teorijo. Nasploh se pri nalogah tega razdelka ne loti računanja prehitro!
5. Denimo, da je stopnja razširitve polja E nad poljem F praštevilo p. Pokaži, da je vsak element iz $E \setminus F$ algebraičen stopnje p nad F.
6. Koliko je $[\mathbb{Q}(3 - \sqrt{7}) : \mathbb{Q}]$? Koliko je $[\mathbb{Q}(3 - 5\sqrt[3]{7} + 4\sqrt[3]{49}) : \mathbb{Q}]$?
7. Koliko je $[\mathbb{Q}(\sqrt[3]{3 + \sqrt{3}}) : \mathbb{Q}]$?

   Nasvet. Poišči nerazcepen polinom, katerega ničla je $\sqrt[3]{3 + \sqrt{3}}$.
8. Naj bosta a in b algebraična elementa nad poljem F. Pokaži, da je
   $$[F(a, b) : F] = [F(a) : F] \cdot [F(b) : F],$$
   če sta si stopnji algebraičnosti obeh elementov, torej števili $[F(a) : F]$ in $[F(b) : F]$, tuji.
9. Koliko je $[\mathbb{Q}(\sqrt{3}, \sqrt[3]{5}) : \mathbb{Q}]$?
10. Koliko je $[\mathbb{Q}(\sqrt{3} + \sqrt[3]{5}) : \mathbb{Q}]$?

    Namig. Primer 7.25.
11. Pokaži, da je $[\mathbb{Q}(\sqrt{3}, i) : \mathbb{Q}] = 4$. Poišči tudi kako tako število a, da je $\mathbb{Q}(a) = \mathbb{Q}(\sqrt{3}, i)$.
12. Pokaži, da je $F(a) = F(a^2)$, če je stopnja algebraičnosti a nad F liho število.
13. Pokaži, da je $F(a^k, a^\ell) = F(a^d)$, če je d največji skupni delitelj števil k in ℓ.
14. S pomočjo prejšnje naloge določi $[\mathbb{Q}(\sqrt{2}, \sqrt[3]{2}) : \mathbb{Q}]$ in $\mathbb{Q}(\sqrt[4]{2}, \sqrt[6]{2}) : \mathbb{Q}]$.

    Namig. $(\sqrt[6]{2})^2 = \sqrt[3]{2}$ in $(\sqrt[6]{2})^3 = \sqrt{2}$.

15. Koliko je $[\mathbb{Q}(\sqrt{2}+\sqrt[3]{2}):\mathbb{Q}]$?
16. Koliko je $[\mathbb{Q}(\sqrt{2}+\sqrt[4]{2}):\mathbb{Q}]$?
17. Koliko je $[\mathbb{Q}(\sqrt[6]{2}):\mathbb{Q}(\sqrt{2})]$?

    Namig. Izrek 7.13.
18. Koliko je $[\mathbb{Q}(\sqrt[6]{3},i):\mathbb{Q}(\sqrt{3}+i)]$?
19. Pokaži, da $\mathbb{Q}(\sqrt{2}) \ncong \mathbb{Q}(\sqrt{3})$.
20. Pokaži, da za poljubne elemente $a_1,\ldots,a_n$, ki so algebraični nad poljem F, velja
$$[F(a_1,\ldots,a_n):F] \leq [F(a_1):F]\cdots[F(a_n):F].$$
21. Naj bodo elementi $a_1,\ldots,a_n$ algebraični stopnje 2 nad F. Pokaži, da je $[F(a_1,\ldots,a_n):F]=2^k$ za neki $k\leq n$.
22. Pokaži, za različna praštevila $p_1,\ldots,p_n$ velja $[\mathbb{Q}(\sqrt{p_1},\ldots,\sqrt{p_n}):\mathbb{Q}] = 2^n$.

7.4. Konstrukcije z ravnilom in šestilom

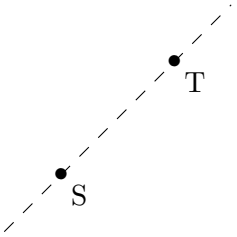
Stari Grki so zaslužni za eno najsijajnejših obdobij v zgodovini matematike. Med drugim jim lahko pripišemo idejo matematičnega dokaza, kar ima samo po sebi neprecenljivo vrednost. Bili so predvsem odlični geometri. Tudi rezultate iz teorije števil so izrazili v geometrijskem jeziku. Algebraični način razmišljanja jim ni bil blizu.

Med značilnimi problemi, s katerimi so se Grki ukvarjali, so konstrukcije z ravnilom in šestilom. Izkazali so se s številnimi domiselnimi konstrukcijami. Nekaterih problemov pa vendarle niso znali rešiti. Posebej znameniti so tile trije.

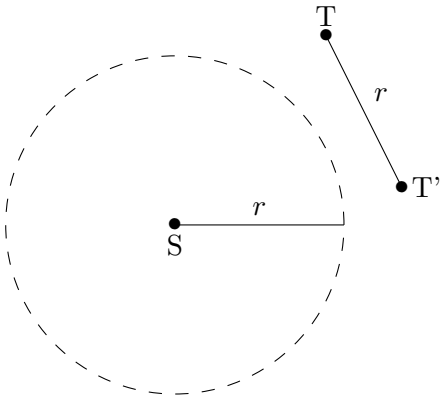
1. **Podvojitev kocke:** z ravnilom in šestilom konstruiraj kocko z dvakratno prostornino dane kocke.
2. **Trisekcija kota:** z ravnilom in šestilom dani kot razdeli na tri enake dele.
3. **Kvadratura kroga:** z ravnilom in šestilom konstruiraj kvadrat z enako ploščino kot dani krog.

Na odgovore se je čakalo več kot dve tisočletji. Vsi pa so enaki: taka konstrukcija ni možna. Za podvojitev kocke in trisekcijo kota je to leta 1837 dokazal *Pierre Wantzel*, za kvadraturo kroga pa leta 1882 *Ferdinand von Lindemann* (izraz »kvadratura kroga« se je zatem uveljavil kot prispodoba za reševanje nerešljivih problemov, ne le v matematiki). Osnovna ideja rešitev je, da te geometrijske probleme prevedemo v algebraični jezik. Kot bomo videli, si potem lahko pomagamo z rezultati prejšnjega razdelka.

Najprej precizirajmo, kaj pomeni uporaba ravnila in šestila. Ravnilo ni označeno. Skozi dani točki S in T lahko z ravnilom potegnemo premico, in to je vse:



Če so dane točke S, T in T', lahko s šestilom narišemo krožnico s središčem v S in polmerom enakim dolžini daljice s krajiščema T in T':



To sta torej naši »pravili igre«. Povsem na začetku imamo podani vsaj dve točki. S presečišči premic in krožnic, ki jih dobimo iz začetnih točk, pridemo do novih točk. Te smemo uporabiti za nadaljnje konstrukcije. Običajni cilj je priti do določene točke. Poglejmo si izhodišče in cilj pri zgornjih problemih.

1. Podano imamo kocko. Zaradi enostavnosti privzemimo, da ima njen rob dolžino 1. Potem je tudi njena prostornina enaka 1. Konstruirati želimo kocko s prostornino 2. Le-ta ima rob dolžine $\sqrt[3]{2}$. Kocka je seveda natanko določena s svojim robom. Naš problem je tako iz daljice z dolžino 1 konstruirati daljico z dolžino $\sqrt[3]{2}$. Da bo delo bolj udobno, opremimo ravnino s koordinatnim sistemom. Potem lahko problem predstavimo takole: iz danih točk
$$T_1 = (0, 0), \;\; T_2 = (1, 0)$$
z ravnilom in šestilom konstruiraj točko
$$Z = (\sqrt[3]{2}, 0).$$

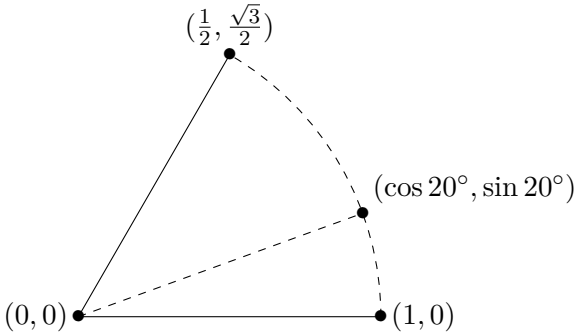
2. Nekatere kote, na primer pravega, pravzaprav lahko razdelimo na tri enake dele. Zato ni vseeno, kateri kot obravnavamo. Izberimo kot $60°$. Problem se potem glasi: iz danih točk

$$T_1 = (0,0),\ \ T_2 = (1,0),\ \ T_3 = (\cos 60°, \sin 60°) = \Big(\frac{1}{2}, \frac{\sqrt{3}}{2}\Big)$$

z ravnilom in šestilom konstruiraj točko

$$Z = (\cos 20°, \sin 20°)$$

(gl. sliko).



3. Krog s polmerom 1 ima ploščino π. Enako ploščino ima kvadrat s stranico $\sqrt{\pi}$. Problem kvadrature kroga torej lahko opišemo takole: iz danih točk

$$T_1 = (0,0),\ \ T_2 = (1,0)$$

z ravnilom in šestilom konstruiraj točko

$$Z = (\sqrt{\pi}, 0).$$

Preidimo na splošni primer. V ravnini naj bo podana množica točk $\mathcal{T} = \{T_1, T_2, \dots\}$ z vsaj dvema elementoma. Zanimajo nas lastnosti točk, ki jih s konstrukcijami z ravnilom in šestilom dobimo iz točk množice $\mathcal{T}$. Vsako tako točko dobimo po končnem številu korakov. V prvem dobimo točko, imenujmo jo A, za katero velja ena izmed možnosti:

(pp) A je presečišče dveh (med seboj različnih) premic, dobljenih iz $\mathcal{T}$;
(pk) A je presečišče premice in krožnice, dobljenih iz $\mathcal{T}$;
(kk) A je presečišče dveh (med seboj različnih) krožnic, dobljenih iz $\mathcal{T}$.

V drugem koraku dobimo točko B, ki je dobljena na enak način, le da vlogo množice $\mathcal{T}$ prevzame množica $\mathcal{T} \cup \{A\}$. V tretjem koraku imamo opravka z množico $\mathcal{T} \cup \{A, B\}$ itd. Točkam, ki jih na ta način dobimo po končnem številu korakov, torej točkam A, B itd., bomo rekli **točke, konstruirane iz množice $\mathcal{T}$.**

Kako te geometrijske pojme povezati s teorijo polj? Bistvo našega pristopa je, da ne bomo obravnavali posameznih točk T_i iz $\mathcal{T}$, pač pa tako podpolje F polja $\mathbb{R}$, da je $\mathcal{T} \subseteq F \times F$, torej podpolje, ki vsebuje komponente vseh točk iz $\mathcal{T}$. Tako podpolje seveda ni enolično določeno. Čeprav v naslednjem izreku tega ne bomo predpostavili, si zaradi boljše nazornosti lahko predstavljamo, da izberemo najmanjše možno podpolje. Če $\mathcal{T}$ sestoji iz točk $T_i = (\lambda_i, \mu_i)$, potem je to podpolje, generirano z vsemi števili λ_i in μ_i.

Primer 7.28. Pri prvem in tretjem klasičnem problemu je $\mathcal{T} = \{T_1, T_2\}$, zato je $F = \mathbb{Q}$. Namreč, $\mathbb{Q}$ je najmanjše podpolje (prapolje) polja $\mathbb{R}$. Pri drugem problemu pa je $F = \mathbb{Q}(\sqrt{3})$.

Naslednji izrek nam bo dal ključ za rešitev vseh treh problemov.

Izrek 7.29. *Naj bo $\mathcal{T}$ množica točk v ravnini in naj bo F tako podpolje $\mathbb{R}$, da je $\mathcal{T} \subseteq F \times F$. Če je točka $Z = (a, b)$ konstruirana iz množice $\mathcal{T}$, potem sta števili a in b algebraični nad F. Stopnja algebraičnosti vsakega izmed njiju je potenca števila 2.*

Dokaz. Naj bo A točka kot zgoraj, torej točka, konstruirana iz $\mathcal{T}$ v prvem koraku. Dokazali bomo, da obstaja tako polje L, da je

$$A \in L \times L \text{ in } [L : F] \in \{1, 2, 4\}.$$

S tem se bomo dokazu izreka že zelo približali, le to ugotovitev moramo zaporedoma uporabiti za primerno množico točk in primerno polje. Za točko B (kot zgoraj) izberemo množico $\mathcal{T} \cup \{A\}$ (namesto $\mathcal{T}$) in polje L (namesto F). Tako najdemo tako polje M, da je $B \in M \times M$ in $[M : L] \in \{1, 2, 4\}$. S pomočjo izreka 7.13 od tod dobimo

$$[M : F] = [M : L] \cdot [L : F] = 2^u \cdot 2^v = 2^{u+v}$$

za neka $u, v \in \{0, 1, 2\}$. Ta argument ponavljamo. Po končnem številu korakov pridemo do točke $Z = (a, b)$ in take razširitve E polja F, da je $Z \in E \times E$ in $[E : F] = 2^r$ za neki $r \geq 0$. Od tod do konca dokaza pa je le še korak. Namreč, števili a in b sta po trditvi 7.16 kot elementa končne razširitve E polja F algebraični nad F. Ker je $F(a)$ podpolje E, po posledici 7.14 število $[F(a) : F]$ deli $[E : F] = 2^r$. Potem pa je tudi to število, ki je po izreku 7.19 enako stopnji algebraičnosti a nad F, lahko samo potenca števila 2. Isto seveda velja za stopnjo algebraičnosti b nad F.

Osredotočimo se torej na točko A in iskanje polja L. Ločeno bomo obravnavali zgoraj opisane tri primere, torej **(pp)**, **(pk)** in **(kk)**. Najprej pa dve splošni opazki. Premica, ki poteka skozi točki iz $\mathcal{T}$, ima enačbo

$$y = \alpha x + \beta \text{ ali } x = \gamma, \text{ kjer so } \alpha, \beta, \gamma \in F. \tag{7.11}$$

Res, spomnimo se enačbe premice skozi dani točki. Če premica ni vertikalna, ima obliko $y = \alpha x + \beta$, pri čemer se števili α in β z osnovnimi aritmetičnimi

operacijami (vsoto, razliko, produktom in kvocientom) izražata s komponentami obeh danih točk iz $\mathcal{T}$. Ker te komponente ležijo v polju F, isto velja za α in β. Če premica je vertikalna, pa ima očitno enačbo $x = \gamma$ za neki $\gamma \in F$. Podobno razmislimo, da ima krožnica s središčem v točki iz $\mathcal{T}$ in polmerom enakim dolžini daljice s krajiščema iz $\mathcal{T}$ enačbo

$$x^2 + y^2 = \delta x + \epsilon y + \zeta, \text{ kjer so } \delta, \epsilon, \zeta \in F. \tag{7.12}$$

In zdaj k posameznim primerom.

(pp) Naj bo točka A presečišče dveh (različnih) premic, ki potekata skozi točki iz $\mathcal{T}$. Enačba prve naj bo podana s (7.11), enačba druge pa z

$$y = \alpha' x + \beta' \text{ ali } x = \gamma', \text{ kjer so } \alpha', \beta', \gamma' \in F.$$

Komponenti točke A sta rešitvi sistema teh dveh linearnih enačb. Očitno sta obe vsebovani v F. Zato lahko za polje L izberemo kar F (in je tako $[L : F] = 1$).

(pk) Točka A naj bo zdaj presečišče premice, podane z enačbo (7.11), in krožnice, podane z enačbo (7.12). Če označimo $A = (x, y)$, sta števili x in y rešitvi obeh enačb (7.11) in (7.12). Pokažimo, da od tod sledi, da sta x in y algebraična nad F in da je

$$[F(x) : F] \leq 2 \text{ in } [F(y) : F] \leq 2. \tag{7.13}$$

Dokažimo le prvo neenakost; dokaz druge je seveda podoben. Če je $x \in F$, je $F(x) = F$ in je tako $[F(x) : F] = 1$. Privzemimo torej, da $x \notin F$. Potem je $y = \alpha x + \beta$ za neka $\alpha, \beta \in F$. Če ta izraz vstavimo v enačbo (7.12), ugotovimo, da je x ničla kvadratnega polinoma s koeficienti iz F. Torej je x algebraičen nad F in sicer stopnje 2, saj po predpostavki $x \notin F$. Po izreku 7.19 je zato $[F(x) : F] = 2$, s čimer je dokaz (7.13) končan.

Za L seveda izberimo polje $F(x, y)$. Če zapišemo L kot $(F(x))(y)$ in uporabimo opombo 7.22, dobimo

$$[L : F(x)] \leq [F(y) : F] \leq 2.$$

Iz izreka 7.13 tako naposled sledi

$$[L : F] = [L : F(x)] \cdot [F(x) : F] \in \{1, 2, 4\}.$$

(kk) Nazadnje naj bo točka A presečišče krožnice, podane z enačbo (7.12), in krožnice, podane z enačbo

$$x^2 + y^2 = \delta' x + \epsilon' y + \zeta', \text{ kjer so } \delta', \epsilon', \zeta' \in F.$$

Ker seveda predpostavljamo, da sta krožnici različni in da presečišče obstaja, ne more hkrati veljati $\delta = \delta'$ in $\epsilon = \epsilon'$. Če odštejemo drugo enačbo od prve, dobimo

$$(\delta - \delta')x + (\epsilon - \epsilon')y + (\zeta - \zeta') = 0. \tag{7.14}$$

Ker vsa števila $\delta - \delta'$, $\epsilon - \epsilon'$ in $\zeta - \zeta'$ ležijo v F in ker je vsaj eno izmed prvih dveh različno od 0, lahko enačbo (7.14) predstavimo na enak način kot enačbo (7.11). S tem smo primer **(kk)** prevedli na primer **(pk)**. □

Antični geometrijski problemi so zdaj na dosegu roke.

Posledica 7.30. *Iz dane kocke z ravnilom in šestilom ne moremo konstruirati kocke z dvakratno prostornino.*

Dokaz. Kot smo zgoraj pojasnili, lahko problem podvojitve kocke izrazimo takole: ali lahko točko $Z = (\sqrt[3]{2}, 0)$ konstruiramo iz množice $\mathcal{T} = \{(0,0),(1,0)\}$? Če bi bil odgovor pozitiven, bi po izreku 7.29 morala biti stopnja algebraičnosti števila $\sqrt[3]{2}$ nad $\mathbb{Q}$ potenca števila 2. Toda enaka je 3. Namreč, polinom $X^3 - 2$ je nerazcepen v $\mathbb{Q}[X]$ (gl. primer 7.8) in je zato minimalni polinom števila $\sqrt[3]{2}$ (gl. izrek 7.3). □

Saj ni bilo tako težko. Zakaj je bilo na rešitev treba čakati več kot 2000 let? To vprašanje seveda nima jasnega odgovora. Lahko pa rečemo, da so bili za rešitev potrebni veliki miselni preskoki. Ideja o možnosti obstoja dokaza, da *nobena* konstrukcija ne more obroditi sadov, je pravzaprav drzna. Pa tudi ideja, da bi problem, ki ga v mislih rešujemo s šestilom in ravnilom v roki, predstavili z enačbami, se ne ponuja sama od sebe. Predvsem pa moramo za rešitev imeti razjasnjen koncept števila. Ker je to del naše osnovne izobrazbe, si morda težko predstavljamo, da ni bilo zmeraj tako.

Problem trisekcije kota bomo rešili podobno, le nekaj več prostora bo vzelo. Omenimo, da sta bili Wantzelovi rešitvi obeh problemov v svojem bistvu podobni našima, čeprav ni uporabljal jezika teorije polj.

Posledica 7.31. *Kota* 60° *z ravnilom in šestilom ne moremo razdeliti na tri enake dele.*

Dokaz. Pokazati moramo, da točke $Z = (\cos 20^\circ, \sin 20^\circ)$ ne moremo konstruirati iz množice $\mathcal{T} = \left\{(0,0),(1,0),\left(\frac{1}{2},\frac{\sqrt{3}}{2}\right)\right\}$. Če bi jo lahko, bi bila po izreku 7.29 stopnja algebraičnosti števila $u := \cos 20^\circ$ nad poljem $\mathbb{Q}(\sqrt{3})$ potenca števila 2. Pokažimo, da je dejansko enaka 3.

Z izračunom realnega dela enakosti

$$\cos 3\varphi + i \sin 3\varphi = (\cos\varphi + i \sin\varphi)^3$$

dobimo formulo

$$\cos 3\varphi = 4\cos^3\varphi - 3\cos\varphi,$$

ki nam za $\varphi = 20^\circ$ da $\frac{1}{2} = 4u^3 - 3u$. Torej je u ničla polinoma

$$p(X) := 8X^3 - 6X - 1 \in \mathbb{Q}[X] \subseteq (\mathbb{Q}(\sqrt{3}))[X].$$

Naš cilj je pokazati, da je $p(X)$ nerazcepen v $(\mathbb{Q}(\sqrt{3}))[X]$. Denimo, da to ni res. Potem ima $p(X)$ ničlo $a \in \mathbb{Q}(\sqrt{3})$. Za število $b := 2a$, ki prav tako leži

v $\mathbb{Q}(\sqrt{3})$, tako velja $b^3 - 3b - 1 = 0$. Če pišemo $b = q + r\sqrt{3}$, $q, r \in \mathbb{Q}$, in upoštevamo, da sta števili $1, \sqrt{3}$ linearno neodvisni nad $\mathbb{Q}$, dobimo

$$q^3 + 9qr^2 - 3q - 1 = 0 \text{ in } r(q^2 + r^2 - 1) = 0. \tag{7.15}$$

Eden izmed faktorjev v drugi enakosti mora biti enak 0. Denimo, da je $r = 0$. Potem se prva enakost glasi $q^3 - 3q - 1 = 0$. Če zapišimo q kot okrajšani ulomek $\frac{m}{n}$ in pomnožimo enakost z n^3, dobimo

$$m^3 - 3mn^2 - n^3 = 0. \tag{7.16}$$

Od tod sledi, da $m|n^3$ in $n|m^3$. Ker sta si števili m in n tuji, je edina možnost, da sta enaki 1 ali -1. Toda to je v nasprotju s (7.16). Možnost, da je $r = 0$, nas je torej vodila v protislovje. Obravnavati moramo še možnost, ko je drugi faktor v drugi enakosti iz (7.15) enak 0. Z računom izpeljemo, da v tem primeru število $s := 2q \in \mathbb{Q}$ zadošča $s^3 - 3s + 1 = 0$. Toda podobno kot v prejšnjem primeru razmislimo, da tudi ta enakost ne more biti izpolnjena za nobeno racionalno število s. □

K našemu dokazu moramo dodati komentar. Z elementarnimi geometrijskimi sredstvi lahko pokažemo, da točko $\left(\frac{1}{2}, \frac{\sqrt{3}}{2}\right)$ lahko konstruiramo iz točk $(0,0)$ in $(1,0)$. Če bi to naredili, bi lahko to točko iz množice $\mathcal{T}$ izvzeli. S tem bi se računski del našega dokaza malce skrajšal (namesto s $\mathbb{Q}(\sqrt{3})$ bi imeli opravka s $\mathbb{Q}$). Praviloma v matematiki dajemo prednost elegantnejšim, neračunskim dokazom. V tem primeru smo se odločili za drugačno pot z željo pokazati, da lahko težek geometrijski problem rešimo z izključno algebraičnimi sredstvi.

Omenimo še, da točkam, ki jih lahko konstruiramo iz točk $(0,0)$ in $(1,0)$, pravimo **konstruktibilne točke**. Ni težko pokazati, da je vsaka točka iz $\mathbb{Q}\times\mathbb{Q}$ konstruktibilna, in še laže, da je točka (k, ℓ) konstruktibilna natanko tedaj, ko sta konstruktibilni točki $(k, 0)$ in $(0, \ell)$. Komponentam konstruktibilnih točk, torej takim številom k in ℓ, pravimo **konstruktibilna števila**. Izkaže se, da je množica konstruktibilnih števil K polje, ki vsebuje kvadratne korene vseh svojih pozitivnih elementov (točka $\left(\frac{1}{2}, \frac{\sqrt{3}}{2}\right)$ je torej konstruktibilna). Dokazi vseh omenjenih dejstev so zanimivi in lepi, kot nasploh dokazi v elementarni geometriji. Vendar vse to za našo razpravo ni ključno, zato se podrobnostim izognimo.

Nazadnje še o problemu kvadrature kroga.

Posledica 7.32. *Iz danega kroga z ravnilom in šestilom ne moremo konstruirati kvadrata z enako ploščino.*

Dokaz. Zdaj je $Z = (\sqrt{\pi}, 0)$ in $\mathcal{T} = \{(0,0), (1,0)\}$. V luči izreka 7.29 zadošča dokazati, da število $\sqrt{\pi}$ ni algebraično. Če bi bilo, bi bil (po posledici 7.26) algebraičen tudi njegov kvadrat, torej število π. To pa ni res. □

Resnici na ljubo temu zapisu ne bi smeli reči dokaz. Uporabili smo sicer že omenjano, a v tej knjigi nedokazano dejstvo, da je število π transcendentno. Problem kvadrature kroga smo v resnici samo prevedli na problem transcendentnosti števila π. Za rešitev slednjega se uporabljajo orodja, ki niso tema te knjige.

Naloge

1. S šestilom in ravnilom razdeli kot 90° na tri enake dele.
2. Pokaži, da so racionalna števila konstruktibilna.

7.5. Kratnost ničle polinoma

Po izletu v geometrijo se vrnimo na stare tire. Naša glavna tema bodo zdaj ničle polinomov. Tema ni nova, saj pojem ničle polinoma v nekem smislu sovpada s pojmom algebraičnega elementa. Toda k njej bomo pristopili z drugega zornega kota. V središču zanimanja ne bo algebraični element sam, pač pa polinom, katerega ničla je ta element. Pričnimo s preprosto ugotovitvijo, ki je le z drugimi besedami izražena trditev 6.28.

TRDITEV 7.33. *Naj bo polje E razširitev polja F. Polinom $f(X) \in F[X]$ ima ničlo $a \in E$ natanko tedaj, ko obstaja tak polinom $g(X) \in E[X]$, da je $f(X) = (X - a)g(X)$.*

DOKAZ. Ker je E razširitev F, je kolobar $F[X]$ podkolobar kolobarja $E[X]$. Zato je $f(X) \in E[X]$ in če je $a \in E$ njegova ničla, po trditvi 6.28 obstaja tak $g(X) \in E[X]$, da je $f(X) = (X - a)g(X)$. Obratna trditev je očitna, tj. iz $f(X) = (X - a)g(X)$ sledi $f(a) = 0$. □

Privzemimo, da je polinom $f(X)$ iz te trditve neničeln. Če element a ni ničla polinoma $g(X)$, rečemo, da je a **enostavna ničla** polinoma $f(X)$. Denimo, da je $g(a) = 0$. Po trditvi 6.28 (ali 7.33) je potem $g(X) = (X - a)g_1(X)$ za neki polinom $g_1(X) \in E[X]$, in zato je $f(X) = (X-a)^2 g_1(X)$. Če je a ničla $g_1(X)$, pridemo do zapisa $f(X) = (X - a)^3 g_2(X)$ itd. Seveda tega ne moremo ponavljati v nedogled, število možnih korakov je očitno omejeno s stopnjo polinoma $f(X)$. Torej obstajata tak $k \in \mathbb{N}$, $k \leq \mathrm{st}(f(X))$, in tak polinom $h(X) \in E[X]$, da je

$$f(X) = (X - a)^k h(X) \text{ in } h(a) \neq 0. \tag{7.17}$$

V tem primeru rečemo, da je a **k-kratna ničla** polinoma $f(X)$.

PRIMER 7.34. Polinom $X^4 - 2X^3 + 2X - 1 \in \mathbb{Q}[X]$ lahko zapišemo kot $(X + 1)(X - 1)^3$. Zato ima dve ničli: -1 in 1. Prva je enostavna, druga pa 3-kratna.

Povrnimo se na primer, ko velja (7.17). Element a ni ničla polinoma $h(X)$. Seveda pa ima lahko ta polinom kako drugo ničlo v polju E. V tem primeru ga lahko razstavimo na enak način kot $f(X)$ v (7.17). (Koeficienti $h(X)$ sicer ležijo v E in ne v F, toda to v ničemer ne vpliva na argument.) Ta postopek ponavljamo. Vsak novi polinom v razcepu ima nižjo stopnjo kot prejšnji. Zato slej ko prej naletimo na polinom, lahko tudi konstanten, ki v E nima ničel. Tako pridemo do zapisa

$$f(X) = (X - a_1)^{k_1} \cdots (X - a_r)^{k_r} f_0(X), \tag{7.18}$$

kjer so a_i različne ničle kratnosti k_i in je $f_0(X) \in E[X]$ polinom brez ničel v E. Drugih ničel razen a_i v polju E polinom $f(X)$ potem ne more imeti. Namreč, iz $f(b) = 0$, kjer je $b \in E$, sledi

$$(b - a_1)^{k_1} \cdots (b - a_r)^{k_r} f_0(b) = 0.$$

Ker $f_0(b) \neq 0$, eden izmed faktorjev pa mora biti enak 0, je $b = a_i$ za neki i. Vseh ničel v E ima $f(X)$ torej r, če jih štejemo z njihovo kratnostjo, pa $k_1 + \cdots + k_r$. Ker je stopnja produkta polinomov enaka vsoti stopenj, velja

$$\mathrm{st}(f(X)) = k_1 + \cdots + k_r + \mathrm{st}(f_0(X)).$$

Zato je

$$k_1 + \cdots + k_r \leq \mathrm{st}(f(X)).$$

Torej velja tale trditev.

Trditev 7.35. *Neničeln polinom $f(X) \in F[X]$ ima v katerikoli razširitvi E polja F največ toliko ničel, štetih z njihovo kratnostjo, kot je njegova stopnja.*

Primer 7.36. Oglejmo si polinom

$$f(X) = X^6 - 3X^4 + 4 \in \mathbb{Q}[X].$$

Z nekaj spretnosti bi ugotovili, da ga lahko zapišemo kot

$$f(X) = (X^2 - 2)^2(X^2 + 1).$$

Kako ga zapisati v obliki (7.18)? Odgovor je odvisen od izbire polja E.

(a) Če za E izberemo $\mathbb{Q}$, $f(X)$ v E nima ničel in $f_0(X)$ je kar enak $f(X)$.
(b) Če za E izberemo $\mathbb{R}$, je $a_1 = \sqrt{2}$, $a_2 = -\sqrt{2}$, $k_1 = k_2 = 2$ in $f_0(X) = X^2 + 1$. Število ničel, štetih z njihovo kratnostjo, je v tem primeru enako 4.
(c) Če za E izberemo $\mathbb{C}$, je $a_1 = \sqrt{2}$, $a_2 = -\sqrt{2}$, $a_3 = i$, $a_4 = -i$, $k_1 = k_2 = 2$, $k_3 = k_4 = 1$ in $f_0(X) = 1$. Število ničel, štetih z njihovo kratnostjo, je enako stopnji polinoma, torej 6.

Najbolj nas zanimajo razširitve, v katerih lahko polinom razstavimo na linearne faktorje (kot v primeru (c)). Te bomo obravnavali v naslednjem razdelku. Zadnji cilj tega razdelka pa je pokazati, da so ničle nerazcepnih

polinomov vedno enostavne, če je le karakteristika polja enaka 0. V ta namen vpeljimo naslednji pojem, ki sicer bralcu ni ravno neznan.

Definicija 7.37. **Odvod** polinoma

$$f(X) = \lambda_0 + \lambda_1 X + \lambda_2 X^2 + \cdots + \lambda_n X^n \in F[X]$$

je polinom

$$f'(X) = \lambda_1 + 2\lambda_2 X + \cdots + n\lambda_n X^{n-1} \in F[X].$$

V matematični analizi pojem odvoda funkcije vpeljemo s pomočjo limite in zatem za realne in morda še kompleksne polinome izpeljemo formulo, ki smo jo tu preprosto vzeli za definicijo. Morda se zdi presenetljivo, da je pojem odvoda pomemben tudi za polinome nad abstraktnimi polji. Tu se namreč ne moremo nasloniti na geometrijsko ozadje, ki v analizi raztolmači pomen odvoda. Kot bomo videli, pa je uporabno že samo pravilo za odvajanje produkta. Le-to je enako temu, ki ga poznamo iz analize, torej

$$\big(f(X)g(X)\big)' = f'(X)g(X) + f(X)g'(X).$$

Za primer, ko sta $f(X)$ in $g(X)$ monoma, formulo preverimo s kratkim računom. Splošni primer pa prevedemo na tega s pomočjo enakosti

$$\big(f(X) + g(X)\big)' = f'(X) + g'(X),$$

ki iz definicije odvoda sledi takoj.

Tudi formula

$$\mathrm{st}(f'(X)) = \mathrm{st}(f(X)) - 1, \text{ če je } \mathrm{st}(f(X)) \geq 1$$

se nam na prvi pogled najbrž zdi nesporna. Toda zanesljivo velja le ob predpostavki, da je karakteristika polja F enaka 0 (saj tedaj iz $\lambda_n \neq 0$ sledi $n\lambda_n \neq 0$). V poljih s karakteristiko p je denimo $(X^p)' = 0$. Prav to, da je odvod nekonstantnega polinoma lahko enak 0, je razlog, da dokaz naslednjega izreka ne deluje za polja s praštevilsko karakteristiko.

Izrek 7.38. *Naj bo F polje s karakteristiko 0 in naj bo $p(X) \in F[X]$ nerazcepen polinom. Potem je vsaka ničla $p(X)$ v katerikoli razširitvi E polja F enostavna.*

Dokaz. Naj bo $a \in E$ ničla $p(X)$. Ker je $p(X)$ nerazcepen, je po izreku 7.3 enak minimalnemu polinomu elementa a, morda pomnoženemu še z elementom iz F. Zato ima $p(X)$ izmed vseh neničelnih polinomov iz $F[X]$, katerih ničla je a, najnižjo stopnjo. Ker ima F karakteristiko 0, je $p'(X)$ neničeln polinom iz $F[X]$ z nižjo stopnjo kot $p(X)$. Torej je $p'(a) \neq 0$. Od tod hitro sledi, da je a enostavna ničla $p(X)$. Če to ne bi bilo res, bi namreč obstajal tak polinom $k(X) \in E[X]$, da bi veljalo $p(X) = (X-a)^2 k(X)$. Iz formule za odvod produkta bi tako sledilo

$$p'(X) = 2(X-a)k(X) + (X-a)^2 k'(X)$$

in zato $p'(a) = 0$. □

Zaključimo razdelek z omembo nekaterih splošnejših, sicer pomembnih pojmov, ki pa jih v tej knjigi ne bomo obravnavali. Polinomu, ki ima v katerikoli razširitvi samo enostavne ničle, pravimo **separabilen polinom**. Razširitvi polja z lastnostjo, da je minimalni polinom vsakega njenega algebraičnega elementa separabilen, pa pravimo **separabilna razširitev**. Nazadnje, polju F z lastnostjo, da je vsaka njegova končna razširitev separabilna, pravimo **perfektno polje**. Iz izreka 7.38 sledi, da je vsako polje s karakteristiko 0 perfektno. Izkaže se, da so taka tudi vsa končna polja. Nekatera neskončna polja s praštevilsko karakteristiko pa niso perfektna. Tako je npr. polje racionalnih funkcij $\mathbb{Z}_p(X)$. Omenimo še, da izrek o primitivnem elementu, ki smo ga omenili v razdelku 7.3, velja za vsako končno separabilno razširitev (in ne le za polja s karakteristiko 0).

Naloge

1. Določi kratnost ničle $a = 1$ polinoma $f(X) = X^5 - 5X^3 + 5X^2 - 1 \in \mathbb{Q}[X]$.
2. Določi kratnost ničle $a = 1$ polinoma $f(X) = X^4 + X^3 + X + 1 \in \mathbb{Z}_2[X]$.
3. Določi kratnost ničle $a = -1$ polinoma $f(X) = X^{10} - 1 \in \mathbb{Z}_5[X]$.
4. Določi kratnost ničle $a = 1$ polinoma $f(X) = X^{2^n} + 1 \in \mathbb{Z}_2[X]$.
5. Naj bo p praštevilo. S pomočjo Fermatovega malega izreka pokaži, da v $\mathbb{Z}_p[X]$ velja enakost
$$X^{p-1} - 1 = (X - 1)(X - 2) \cdots (X - (p - 1)).$$
Od tod ponovno izpelji Wilsonov izrek (gl. nalogo 3.1/15).
6. Naj bo F poljubno polje. Pokaži, da je vsaka ničla nekonstantnega polinoma $f(X) \in F[X]$ v katerikoli razširitvi E polja F enostavna, če sta si polinoma $f(X)$ in $f'(X)$ tuja.
7. Naj bo F polje s karakteristiko 0 in naj bo E njegova razširitev. Pokaži, da je $a \in E$ k-kratna ničla polinoma $f(X) \in F[X]$ natanko tedaj, ko je $f(a) = f'(a) = \cdots = f^{(k-1)}(a) = 0$ in $f^{(k)}(a) \neq 0$. (Tu je $f^{(i)}(X)$ i-ti odvod polinoma $f(X)$.)

7.6. Razpadna polja in algebraično zaprta polja

Vzemimo polinom s koeficienti iz polja F. Kot vemo, v osnovnem polju F nima nujno ničle, lahko pa jo ima v kaki njegovi razširitvi. *Ali taka razširitev vselej obstaja?* Z drugimi besedami, ali ima vsaka polinomska enačba rešitev v kakem večjem polju? Smisel in pomen tega vprašanja je razviden iz orisa zgodovine klasične algebre iz začetka poglavja. Zato o tem ne bomo več

govorili. Glavni namen razdelka je podati pozitiven odgovor na zastavljeno vprašanje. Na koncu si bomo ogledali še polja, kakršno je polje kompleksnih števil: vsi polinomi s koeficienti iz tega polja imajo ničle že v tem polju.

7.6.1. Razpadna polja. Poudarimo, da smo zgornje vprašanje zastavili za poljubno polje F. Za podpolja polja $\mathbb{C}$ odgovor seveda takoj sledi iz osnovnega izreka algebre. Toda kako konstruirati razširitve abstraktnih polj? Naslednji primer bo nakazal možen pristop. Novih polj v njem sicer ne bomo spoznali, le polje kompleksnih števil bomo »ponovno odkrili«.

Primer 7.39. Označimo z $\mathcal{I}$ ideal kolobarja $\mathbb{R}[X]$, generiran s polinomom X^2+1 (torej $\mathcal{I} = (X^2+1)$). Ker je kot kvadratni polinom brez realnih ničel ta polinom nerazcepen v $\mathbb{R}[X]$, je kolobar $\mathbb{R}[X]/\mathcal{I}$ polje (posledica 6.24). Pokažimo, da je izomorfen polju kompleksnih števil. Definirajmo preslikavo $\varphi : \mathbb{C} \to \mathbb{R}[X]/\mathcal{I}$ s predpisom

$$\varphi(\lambda + \mu i) = \lambda + \mu X + \mathcal{I}$$

za vse $\lambda, \mu \in \mathbb{R}$. Zlahka preverimo, da φ ohranja vsoto. Dokažimo, da ohranja tudi produkt. Za vse $\lambda, \lambda', \mu, \mu' \in \mathbb{R}$ je

$$\varphi((\lambda + \mu i)(\lambda' + \mu' i)) = (\lambda\lambda' - \mu\mu') + (\lambda\mu' + \mu\lambda')X + \mathcal{I}$$

in

$$\begin{aligned}\varphi(\lambda + \mu i)\varphi(\lambda' + \mu' i) &= (\lambda + \mu X + \mathcal{I})(\lambda' + \mu' X + \mathcal{I}) \\ &= \lambda\lambda' + (\lambda\mu' + \mu\lambda')X + \mu\mu' X^2 + \mathcal{I}.\end{aligned}$$

Ker je

$$\mu\mu' X^2 + \mathcal{I} = -\mu\mu' + \mu\mu'(X^2+1) + \mathcal{I} = -\mu\mu' + \mathcal{I},$$

sta oba izraza enaka in φ je homomorfizem. Ideal $\mathcal{I}$ očitno ne vsebuje polinomov stopenj 0 in 1, zato ima φ trivialno jedro. Vzemimo poljuben polinom $f(X) \in \mathbb{R}[X]$. Po izreku 6.17 je

$$f(X) = q(X)(X^2+1) + \lambda + \mu X$$

za neki polinom $q(X) \in \mathbb{R}[X]$ in števili $\lambda, \mu \in \mathbb{R}$. Zato je

$$f(X) + \mathcal{I} = \lambda + \mu X + \mathcal{I}.$$

To dokazuje, da je φ surjektiven in tako izomorfizem. Torej res lahko kolobar $\mathbb{R}[X]/\mathcal{I}$ identificiramo s poljem kompleksnih števil. V tem smislu realnim številom ustrezajo odseki $\varphi(\lambda) = \lambda + \mathcal{I}$, kjer je $\lambda \in \mathbb{R}$. Vlogo števila i ima odsek $\varphi(i) = X + \mathcal{I}$, ki je ničla našega polinoma X^2+1. To sledi iz dejstva, da je φ izomorfizem, a kljub temu potrdimo še z računom:

$$(X + \mathcal{I})^2 = X^2 + \mathcal{I} = -1 + \mathcal{I}.$$

Tu smo upoštevali, da $X^2 + 1 \in \mathcal{I}$. Ker je $-1 + \mathcal{I}$ nasprotni element enote kolobarja $\mathbb{R}[X]/\mathcal{I}$, to dokazuje želeno.

Kako smo v tem primeru prišli do polja, v katerem je imel dani polinom ničlo? Vzeli smo ideal, generiran s tem polinomom in ustrezno polje vpeljali kot kvocientni kolobar kolobarja polinomov po tem idealu. V dokazu naslednjega izreka bomo videli, da lahko to konstrukcijo uporabimo za vsak nerazcepen polinom nad poljubnim poljem.

Izrek 7.40. *Naj bo F polje in naj bo $f(X) \in F[X]$ nekonstanten polinom. Potem obstaja razširitev E polja F, v kateri ima $f(X)$ ničlo.*

Dokaz. Naj bo $p(X) \in F[X]$ nerazcepen polinom, ki deli $f(X)$ (po izreku 6.27 tak res obstaja). Torej $f(X)$ pripada idealu $\mathcal{I} := (p(X))$. Naj bo $E := F[X]/\mathcal{I}$. Po posledici 6.24 je E polje.

Preslikava $\varphi : F \to E$, definirana s predpisom $\varphi(\lambda) = \lambda + \mathcal{I}$, je očitno homomorfizem kolobarjev. Kot nerazcepen polinom $p(X)$ ni konstanten in zato isto velja za vse neničelne polinome iz $\mathcal{I}$. Od tod sledi, da je φ vložitev. Tako lahko E obravnavamo kot razširitev F (element $\lambda \in F$ identificiramo z elementom $\lambda + \mathcal{I} \in E$).

Vzemimo poljuben polinom $g(X) \in F[X]$ in pokažimo, da je njegova vrednost v elementu $X + \mathcal{I} \in E$ enaka $g(X) + \mathcal{I}$, torej da je

$$g(X + \mathcal{I}) = g(X) + \mathcal{I}. \tag{7.19}$$

Naj bo $g(X) = \sum_i \lambda_i X^i$. Tu je λ_i element iz F, ki pa ga je v luči našega cilja bolj priročno pisati kot $\lambda_i + \mathcal{I} \in E$. Tako je

$$g(X + \mathcal{I}) = \sum_i (\lambda_i + \mathcal{I})(X + \mathcal{I})^i = \sum_i (\lambda_i + \mathcal{I})(X^i + \mathcal{I}) = \sum_i \lambda_i X^i + \mathcal{I},$$

kar dokazuje (7.19). Če za $g(X)$ izberemo $f(X)$, dobimo

$$f(X + \mathcal{I}) = f(X) + \mathcal{I} = 0,$$

saj je $f(X) \in \mathcal{I} = (p(X))$. Torej je $X + \mathcal{I}$ ničla polinoma $f(X)$. □

Vsak polinom torej ima ničlo – če ne »doma«, v originalnem polju, pa v neki njegovi razširitvi. To je eden najosnovnejših izrekov teorije polj. Njegov dokaz je lepa ilustracija učinkovitosti abstraktnega pristopa. Čeprav izrek govori o enem samem polinomu, dokaz sloni na obravnavi kolobarja vseh polinomov. Poleg tega vpleta pojme kot so kvocientni kolobarji, nerazcepnost in (vsaj posredno) maksimalni ideali, za katere ob njihovi vpeljavi morda ni bilo jasno, da so lahko koristni.

V nadaljevanju bomo izpeljali izostreni inačici izreka 7.40, ki na prvi pogled povesta veliko več. Toda iz njunih dokazov je razvidno, da sta razmeroma enostavni posledici osnovnega izreka.

Izrek 7.41. *Naj bo F polje in naj bo $f(X) \in F[X]$ nekonstanten polinom z vodilnim koeficientom c. Potem obstaja taka razširitev E polja F in taki (ne nujno različni) elementi $a_i \in E$, da je $f(X) = c(X - a_1) \cdots (X - a_n)$.*

Dokaz. Dokaz je z indukcijo na $n := \mathrm{st}(f(X))$. Za $n = 1$ je trditev očitna, zato naj bo $n > 1$. Privzeti smemo, da želeni rezultat velja za vse polinome stopnje manj kot n s koeficienti iz *poljubnega* polja (ne nujno iz polja F). Izrek 7.40 pove, da obstaja razširitev E_0 polja F, v kateri ima $f(X)$ ničlo a_1. Po trditvi 7.33 obstaja tak polinom $g(X) \in E_0[X]$, da je $f(X) = (X - a_1)g(X)$. Ker je $\mathrm{st}(g(X)) = n-1$, po predpostavki obstaja taka razširitev E polja E_0 (in s tem tudi razširitev polja F), da je $g(X)$ enak produktu linearnih polinomov s koeficienti iz E. Potem pa isto velja za $f(X) = (X - a_1)g(X)$. □

Če smo v prejšnjem razdelku z elementarnim razmislekom ugotovili, da ima neničeln polinom $f(X) \in F[X]$ v *katerikoli* razširitvi polja F *največ* toliko ničel, štetih z njihovo kratnostjo, kot je njegova stopnja (trditev 7.35), potem sedaj vemo, da *obstaja* taka razširitev E, da je število ničel v E, štetih z njihovo kratnostjo, *enako* stopnji polinoma.

Izrek 7.41 lahko izrazimo tudi takole: vsak nekonstanten polinom lahko v neki razširitvi originalnega polja zapišemo kot produkt linearnih polinomov. Takih razširitev je več. Posebej zanimive so »najmanjše« izmed njih. Dajmo jim ime.

Definicija 7.42. Naj bo polje E razširitev polja F. Pravimo, da polinom $f(X) \in F[X]$ **razpade** v E, če je $f(X)$ enak produktu linearnih polinomov iz $E[X]$. Če $f(X)$ razpade v E in ne razpade v nobenem pravem podpolju polja E, ki vsebuje F, potem E imenujemo **razpadno polje** polinoma $f(X)$ nad poljem F.

Izrek 7.41 pove, da vsak nekonstanten polinom $f(X) \in F[X]$ razpade v neki razširitvi polja F. Obstoj razpadnega polja od tod zlahka sledi.

Izrek 7.43. *Naj bo F polje. Za vsak nekonstanten polinom $f(X) \in F[X]$ obstaja razpadno polje nad F.*

Dokaz. Naj bo E razširitev F in $a_1, \ldots, a_n \in E$ elementi iz izreka 7.41. Trdimo, da je potem

$$F(a_1, \ldots, a_n)$$

razpadno polje polinoma $f(X)$. Očitno $f(X)$ v tem polju razpade. Če je E_0 podpolje E, ki vsebuje F in v katerem $f(X)$ razpade, potem E_0 vsebuje vse ničle polinoma $f(X)$ v E (zakaj?). Zato E_0 vsebuje vse elemente a_i in tako je $E_0 \supseteq F(a_1, \ldots, a_n)$. Torej je $F(a_1, \ldots, a_n)$ razpadno polje polinoma $f(X)$. □

Opomba 7.44. Po izreku 7.23 je razpadno polje $F(a_1, \ldots, a_n)$ *končna* razširitev polja F.

Primer 7.45. Kaj je razpadno polje polinoma $X^2 + 1$? To vprašanje nima odgovora, ker ni dobro zastavljeno. Povedati moramo, nad katerim poljem polinom obravnavamo.

(a) Polinom $X^2+1 \in \mathbb{Q}[X]$ seveda razpade v polju $\mathbb{C}$, pa tudi v vsakem podpolju $\mathbb{C}$, ki vsebuje vsa racionalna števila in števili i in $-i$. Če vsebuje eno izmed njiju, seveda vsebuje obe. Torej je razpadno polje tega polinoma enako $\mathbb{Q}(i) = \{\lambda_0 + \lambda_1 i \mid \lambda_i \in \mathbb{Q}\}$.

(b) Razpadno polje polinoma $X^2+1 \in \mathbb{R}[X]$ je $\mathbb{R}(i) = \mathbb{C}$.

(c) Razpadno polje polinoma $X^2+1 \in \mathbb{C}[X]$ je polje $\mathbb{C}$ samo.

(d) Tudi razpadno polje polinoma $X^2+1 \in \mathbb{Z}_2[X]$ je kar polje $\mathbb{Z}_2$ samo. Namreč, ta polinom lahko zapišemo kot $(X+1)^2$. Njegova edina ničla je $1 \in \mathbb{Z}_2$.

Razpadno polje nekonstantnega polinoma torej *obstaja*. Kako pa je z njegovo *enoličnostjo*? Ne moremo pričakovati, da bi bilo razpadno polje dobesedno eno samo. V vseh naših definicijah nastopajo abstraktne razširitve danega polja, ki kot množice morda nimajo veliko skupnega. V bistvu pa razpadno polje polinoma vendarle je eno samo. Poljubni dve sta si namreč izomorfni. Dokazati to dejstvo je naš naslednji cilj. Pravzaprav bomo najprej dokazali malce več, a ne zaradi želje po večji splošnosti. Včasih je lažje izpeljati splošnejšo trditev od tiste, ki nas v resnici zanima.

Kot pripravo za naslednji izrek zabeležimo dve splošni opombi o izomorfizmih. Prva je malce izostrena različica opombe 7.21 (a).

Opomba 7.46. Naj bo polje E razširitev polja F in naj bo element $a \in E$ ničla nerazcepnega polinoma $p(X) \in F[X]$. Preslikava $f(X) \mapsto f(a)$ je epimorfizem iz kolobarja $F[X]$ v kolobar $F[a] = F(a)$, njegovo jedro pa je ideal $(p(X))$. Izrek o izomorfizmu pove, da obstaja izomorfizem

$$\psi : F[X]/(p(X)) \to F(a).$$

Definicija ψ je seveda naravna, tj.

$$\psi(f(X) + (p(X))) = f(a).$$

Tako med drugim velja

$$\psi(X + (p(X))) = a \quad \text{in} \quad \psi(\lambda + (p(X))) = \lambda \text{ za vse } \lambda \in F. \tag{7.20}$$

Opomba 7.47. Izomorfizem polj $\varphi : F \to F'$ lahko enostavno razširimo na izomorfizem kolobarjev $F[X]$ in $F'[X]$. Res, za vsak polinom

$$f(X) = \lambda_0 + \lambda_1 X + \cdots + \lambda_n X^n \in F[X]$$

vpeljimo polinom

$$f_\varphi(X) = \varphi(\lambda_0) + \varphi(\lambda_1)X + \cdots + \varphi(\lambda_n)X^n \in F'[X].$$

Takoj preverimo, da je s predpisom $f(X) \mapsto f_\varphi(X)$ definiran izomorfizem (s podobnim homomorfizmom smo se srečali v dokazu Gaussove leme).

IZREK 7.48. *Naj bo $\varphi : F \to F'$ izomorfizem polj. Če je E razpadno polje polinoma $f(X) \in F[X]$ in E' razpadno polje polinoma $f_\varphi(X) \in F'[X]$, potem obstaja izomorfizem iz E v E', ki se na F ujema s φ.*

DOKAZ. Dokaz je z indukcijo na $n := \mathrm{st}(f(X))$. Če je $n = 1$, je $E = F$ in $E' = F'$, zato je iskani izomorfizem kar φ sam. Naj bo torej $n > 1$. Izberimo nerazcepen polinom $p(X)$, ki deli $f(X)$. Ker je E razpadno polje polinoma $f(X)$, vsebuje kako ničlo polinoma $p(X)$. Označimo jo z a. Naj bo

$$\psi : F[X]/(p(X)) \to F(a)$$

izomorfizem polj, ki zadošča (7.20). Podobno naj bo $a' \in E'$ ničla (prav tako nerazcepnega!) polinoma $p_\varphi(X)$ in

$$\psi' : F'[X]/(p_\varphi(X)) \to F'(a')$$

izomorfizem, ki zadošča

$$\psi'\big(X + (p_\varphi(X))\big) = a' \quad \text{in} \quad \psi'\big(\mu + (p_\varphi(X))\big) = \mu \ \text{ za vse } \mu \in F'. \tag{7.21}$$

Naš namen je poiskati izomorfizem iz $F(a)$ v $F'(a')$. Za to potrebujemo še izomorfizem

$$\overline{\varphi} : F[X]/(p(X)) \to F'[X]/(p_\varphi(X)),$$

ki ga definiramo s predpisom

$$\overline{\varphi}\big(f(X) + (p(X))\big) = f_\varphi(X) + (p_\varphi(X)).$$

Brez težav preverimo, da $\overline{\varphi}$ je dobro definirana preslikava in izomorfizem. Zdaj lahko vpeljemo

$$\Phi := \psi' \circ \overline{\varphi} \circ \psi^{-1} : F(a) \to F'(a').$$

Kot kompozitum izomorfizmov je Φ tudi sam izomorfizem. Iz (7.20) in (7.21) sledi, da je

$$\Phi(a) = a' \quad \text{in} \quad \Phi(\lambda) = \varphi(\lambda) \ \text{ za vse } \lambda \in F. \tag{7.22}$$

Ker je $a \in F(a)$ ničla polinoma $f(X)$, lahko (po trditvi 7.33) zapišemo

$$f(X) = (X - a)g(X), \quad \text{kjer je } g(X) \in F(a)[X]. \tag{7.23}$$

Polinom $g(X)$ seveda razpade v polju E in ne razpade v nobenem pravem podpolju E, ki vsebuje $F(a)$ (saj bi sicer v takem podpolju razpadel tudi $f(X)$). Torej je E razpadno polje polinoma $g(X)$ nad poljem $F(a)$. Ker je, kot sledi iz (7.22) in (7.23),

$$f_\varphi(X) = f_\Phi(X) = (X - a')g_\Phi(X),$$

podobno sklepamo, da je E' razpadno polje polinoma $g_\Phi(X)$ nad poljem $F'(a')$. Polinom $g(X)$ ima stopnjo $n - 1$, kar omogoča uporabo indukcijske predpostavke (vlogo polj F in F' zdaj prevzameta polji $F(a)$ in $F'(a')$, vlogo izomorfizma φ pa izomorfizem Φ). Tako sledi, da obstaja izomorfizem iz E v E', ki se na $F(a)$ ujema s Φ. Le-ta pa se na F ujema s φ. □

Dokaz izreka je morda eden tistih, ki se zaradi obilice oznak na prvi pogled zdijo težki. Ko pa uspemo izluščiti njegovo bistvo, se nam zdi naraven.

Posledica 7.49. *Poljubni razpadni polji istega polinoma $f(X) \in F[X]$ sta si izomorfni.*

Dokaz. Uporabimo izrek 7.48 za $F = F'$ in $\varphi = \mathrm{id}_F$. □

Bralec naj poskusi razmisliti, kje se dokaz izreka 7.48 ustavi, če obravnavamo le primer, ko je $\varphi = \mathrm{id}_F$.

7.6.2. Algebraično zaprta polja. Naredimo korak naprej in si oglejmo polja, v katerih ne razpade le en polinom, pač pa vsi polinomi s koeficienti iz tega polja.

Definicija 7.50. Polje Z je **algebraično zaprto**, če ima vsak nekonstanten polinom $f(X) \in Z[X]$ vsaj eno ničlo v Z.

Z zaporedno uporabo trditve 7.33 zlahka ugotovimo, da so za polje Z naslednje trditve ekvivalentne:

(i) Z je algebraično zaprto.
(ii) Vsak neskonstanten polinom $f(X) \in Z[X]$ razpade v Z, tj. lahko ga zapišemo kot
$$f(X) = c(X - a_1) \cdots (X - a_n)$$
za neke (ne nujno različne) $a_i \in Z$; tu je c njegov vodilni koeficient.
(iii) Vsak nekonstanten polinom $f(X) \in Z[X]$ ima toliko ničel v Z, štetih z njihovo kratnostjo, kot je njegova stopnja.

Primer 7.51. Polje kompleksnih števil $\mathbb{C}$ je algebraično zaprto. To seveda pove osnovni izrek algebre.

Najbrž je polje $\mathbb{C}$ tudi edini primer algebraično zaprtega polja, ki nam takoj pride na misel. Do novih primerov nas bo vodila naslednja trditev.

Trditev 7.52. *Naj bo polje L algebraična razširitev polja F. Če je polje E razširitev polja L in je $x \in E$ algebraičen nad L, potem je x algebraičen tudi nad F.*

Dokaz. Po predpostavki obstajajo taki $a_i \in L$, ne vsi enaki 0, da je
$$a_0 + a_1 x + \cdots + a_n x^n = 0.$$
Zato je x algebraičen tudi nad podpoljem $F(a_0, \ldots, a_n)$ polja L. Po izreku 7.19 je $F(a_0, \ldots, a_n)(x)$ končna razširitev polja $F(a_0, \ldots, a_n)$. Slednje polje pa je končna razširitev polja F. To namreč sledi iz izreka 7.23, saj so vsi a_i kot elementi iz L algebraični nad F. Po izreku 7.13 je zato $F(a_0, \ldots, a_n)(x)$ končna razširitev F. Iz trditve 7.16 pa sledi, da je vsak element iz $F(a_0, \ldots, a_n)(x)$, torej tudi x, algebraičen nad F. □

Kot vemo, je končna razširitev končne razširitve tudi sama končna (izrek 7.13). Iz trditve sledi analogna ugotovitev za algebraične razširitve.

Posledica 7.53. *Če je polje L algebraična razširitev polja F in je polje E algebraična razširitev polja L, potem je E algebraična razširitev F.*

Algebraična zaprtost polja je precej izjemna lastnost. Če dano polje F te lastnosti nima, jo morda ima kaka njegova razširitev Z. Na primer, če je $F = \mathbb{Q}$, lahko izberemo $Z = \mathbb{C}$. Toda kompleksna števila so nam morda zazdijo »preobsežna« razširitev racionalnih števil. Ali obstaja kaka algebraično zaprta razširitev $\mathbb{Q}$, ki je s $\mathbb{Q}$ tesneje povezana? Povejmo natančneje, kaj imamo s tem v mislih.

Definicija 7.54. Polje A se imenuje **algebraično zaprtje** polja F, če je algebraično zaprto in je algebraična razširitev F.

Primer 7.55. Polje $\mathbb{C}$ je algebraično zaprtje polja $\mathbb{R}$. Seveda je algebraično zaprto, pa tudi algebraična razširitev je (gl. primer 7.5 ali opombo 7.17). Ni pa $\mathbb{C}$ algebraično zaprtje polja $\mathbb{Q}$, saj poleg algebraičnih obstajajo tudi transcendentna števila.

Za podpolja algebraično zaprtih polj, na primer za podpolja polja $\mathbb{C}$, je algebraična zaprtja lahko opisati.

Izrek 7.56. *Naj bo F podpolje algebraično zaprtega polja Z. Potem je množica vseh elementov iz Z, ki so algebraični nad F, algebraično zaprtje polja F.*

Dokaz. Označimo to množico z A. Kot vemo, je A polje (posledica 7.26). Seveda je algebraična razširitev F. Dokazati moramo, da je A algebraično zaprto polje. Vzemimo torej nekonstanten polinom $f(X) \in A[X]$. Ker je polje Z algebraično zaprto in je $A \subseteq Z$, obstaja tak $x \in Z$, da je $f(x) = 0$. Element x je torej algebraičen nad A. Po trditvi 7.52 je x algebraičen tudi nad F. Po definiciji A to pomeni, da $x \in A$. Polinom $f(X)$ ima tako ničlo v A. □

Posledica 7.57. *Polje algebraičnih števil je algebraično zaprtje polja $\mathbb{Q}$.*

V naših primerih smo imeli največkrat opravka s številskimi polji, torej podpolji $\mathbb{C}$. Seveda obstajajo tudi drugačna polja. *Ali ima vsako polje F algebraično zaprto razširitev?* V luči izreka 7.56 lahko vprašanje ekvivalentno zastavimo tudi takole: *ali ima vsako polje F algebraično zaprtje?* V takem polju potem razpadejo vsi polinomi iz $F[X]$, ne le en sam kot v razpadnem polju. Vprašanje je torej precej zahtevnejše od vprašanj, ki smo jih obravnavali v prejšnjem razdelku. Vendarle se izkaže, da je *odgovor pozitiven.* Ker pa dokaz razen algebraičnih sredstev, ki so nam zdaj že na voljo, uporablja tudi nekatera orodja teorije množic, ga bomo izpustili. Omenimo še, da je algebraično zaprtje poljubnega polja do izomorfizma natančno eno samo.

Naloge

1. Pojasni, zakaj je $\mathbb{Q}(\sqrt{2})$ razpadno polje vsakega izmed polinomov $X^2 - 2, 3X^3 - 6X, X^4 - 3X^2 + 2 \in \mathbb{Q}[X]$.
2. Pojasni, zakaj je $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ razpadno polje polinoma $X^4 - 5X^2 + 6 \in \mathbb{Q}[X]$.
3. Označimo z ω primitivni tretji koren enote $-\frac{1}{2} + i\frac{\sqrt{3}}{2}$. Pokaži, da je $\mathbb{Q}(\sqrt[3]{2}, \omega)$ razpadno polje polinoma $X^3 - 2 \in \mathbb{Q}[X]$.
4. Pokaži, da je $\mathbb{Q}(i)$ razpadno polje polinoma $X^4 + 4 \in \mathbb{Q}[X]$.
5. Pokaži, da je $\mathbb{Q}(\sqrt[4]{2}, i)$ razpadno polje polinoma $X^4 + 2 \in \mathbb{Q}[X]$.
6. Pokaži, da je $\mathbb{Q}(\sqrt{2}, i)$ razpadno polje polinoma $X^4 + 1 \in \mathbb{Q}[X]$.
7. Naj bo E razpadno polje polinoma $f(X) \in F[X]$ stopnje n. Pokaži, da je $[E : F] \leq n!$ in da $n \mid [E : F]$, če je $f(X)$ nerazcepen. Koliko je $[E : F]$ v primerih iz zgornjih nalog?
8. V primeru 7.39 smo pokazali, da je $\mathbb{R}[X]/(X^2 + 1) \cong \mathbb{C}$. S pomočjo homomorfizma $f(X) \mapsto f(i)$ iz $\mathbb{R}[X]$ v $\mathbb{C}$ izpelji to na drugačen (in krajši) način.
9. Pokaži, da velja tudi obrat trditve iz naloge 7.5/6, torej da sta si polinoma $f(X)$ in $f'(X)$ tuja, če je vsaka ničla polinoma $f(X) \in F[X]$ v katerikoli razširitvi E polja F enostavna.
10. Dokaz izreka 7.48 ilustriraj s komutativnim diagramom.
11. Naj bodo $a_1, \ldots, a_n$ elementi polja F. Pokaži, da obstaja tak polinom $f(X) \in F[X]$, da je $f(a_1) = \cdots = f(a_n) = 1$. Od tod sklepaj, da končno polje ne more biti algebraično zaprto.
12. Pokaži, da ima algebra nad algebraično zaprtim poljem delitelje niča, če je končno-razsežna in je njena dimenzija vsaj 2.
13. Pokaži, da je polje Z algebraično zaprto natanko tedaj, ko ne obstaja končna razširitev $E \supsetneq Z$.

    Namig. Če je $p(X) \in Z[X]$ nerazcepen polinom, lahko $Z[X]/(p(X))$ obravnavamo kot razširitev Z (kot v dokazu izreka 7.40).
14. Naj bo $E \supsetneq \mathbb{R}$ končna razširitev polja $\mathbb{R}$. Pokaži, da je $E \cong \mathbb{C}$.

7.7. Končna polja

Ta, zadnji razdelek je namenjen klasifikaciji vseh končnih polj, torej polj s končnim številom elementov. Poiskali bomo neke primere končnih polj in hkrati pokazali, da drugih ni (če seveda med izomorfnimi ne ločimo). Tovrsten popoln opis nekega algebraičnega pojma smo doslej uspeli dobiti za ciklične grupe (izrek 3.8) in končne Abelove grupe (izrek 5.20). Rezultat, ki

ga bomo dobili, ni očiten, dokaz pa vseeno ne bo dolg – a le zato, ker se bomo naslonili na že izpeljano teorijo. Posebej zanimivo je, da nam bodo tudi pri iskanju konkretnih primerov teoretični rezultati v ključno pomoč. Tako bomo »nagrajeni« za trud v predhodnih razdelkih.

Kaj že vemo? Za vsako praštevilo p poznamo polje s p elementi $\mathbb{Z}_p$, ki ga lahko vložimo v vsako drugo polje s karakteristiko p (izrek 3.60). V polja s karakteristiko 0 pa lahko, po drugi strani, vložimo (neskončno) polje $\mathbb{Q}$. Vsako končno polje E ima torej praštevilsko karakteristiko p in tako vsebuje podpolje, ki je izomorfno $\mathbb{Z}_p$. Zaradi enostavnosti bomo to podpolje označevali kar z $\mathbb{Z}_p$. Tako je $\mathbb{Z}_p \subseteq E$ in E lahko obravnavamo kot vektorski prostor nad $\mathbb{Z}_p$. To nam omogoča narediti prvi korak pri iskanju vseh končnih polj.

LEMA 7.58. *Če je E končno polje s karakteristiko p, je $|E| = p^n$ za neki $n \in \mathbb{N}$.*

DOKAZ. Kot vektorski prostor nad $\mathbb{Z}_p$ je E seveda končno-razsežen. Če je $\{b_1, \ldots, b_n\}$ njegova baza, lahko vsak element iz E na *en sam* način zapišemo kot

$$\lambda_1 b_1 + \lambda_2 b_2 + \cdots + \lambda_n b_n, \quad \text{kjer } \lambda_i \in \mathbb{Z}_p.$$

Torej ima E toliko elementov, kolikor je različnih n-teric $(\lambda_1, \lambda_2, \ldots, \lambda_n)$. Število teh pa je enako $|\mathbb{Z}_p|^n = p^n$. □

Iz dokaza leme vidimo, da je

$$|E| = p^n \iff [E : \mathbb{Z}_p] = n.$$

To si velja zapomniti.

Število elementov končnega polja je torej lahko le potenca njegove karakteristike, ki je seveda nujno praštevilo. Poznamo polja s p elementi, toda ali obstajajo tudi polja z močjo p^2, p^3 itd.? Kolobarje $\mathbb{Z}_{p^2}$, $\mathbb{Z}_{p^3}$ itd. lahko takoj odmislimo, saj imajo delitelje niča. Vprašanje lahko zastavimo drugače. Ali obstajajo končne razširitve polja $\mathbb{Z}_p$ stopenj $2, 3$ itd.? Razpadna polja polinomov so vedno končne razširitve (gl. opombo 7.44). Načeloma torej lahko vzamemo katerikoli nekonstanten polinom iz $\mathbb{Z}_p[X]$ in preko izreka o obstoju razpadnega polja pridemo do primera polja s p^n elementi za kak $n \in \mathbb{N}$. Toda ne zaletimo se. Zadošča obravnavati samo zelo posebne polinome.

LEMA 7.59. *Če je E polje s p^n elementi, potem je E razpadno polje polinoma $f(X) = X^{p^n} - X$ nad poljem $\mathbb{Z}_p$.*

DOKAZ. Množica E^* neničelnih in zato obrnljivih elementov polja E je za množenje grupa reda $p^n - 1$. Posledica 5.4 pove, da za vsak $x \in E^*$ velja $x^{p^n-1} = 1$. Če to enakost pomnožimo z x, dobimo $x^{p^n} = x$. Ker temu očitno zadošča tudi element $x = 0$, je torej vsak element iz E ničla polinoma $f(X)$. Tako ima $f(X)$ v E toliko različnih ničel, kot je njegova stopnja. Zato $f(X)$

v E razpade. Ker je E kar množica vseh njegovih ničel, v pravem podpolju E seveda ne more razpasti. □

Lema pove tole: *če* obstaja polje s p^n elementi, potem je to polje razpadno polje polinoma $X^{p^n} - X$ nad $\mathbb{Z}_p$. Toda razen za $n = 1$ zaenkrat še ne vemo, ali tako polje sploh obstaja. Lema nam samo predlaga edinega možnega kandidata in hkrati pove, da ne moreta obstajati neizomorfni polji z istim številom elementov. Razpadno polje polinoma je namreč do izomorfizma natančno eno samo.

Naš cilj sedaj je pokazati, da razpadno polje polinoma $X^{p^n} - X$ nad $\mathbb{Z}_p$ dejansko ima p^n elementov. Najprej pa se seznanimo s posebnim endomorfizmom, povezanim s praštevilsko karakteristiko.

LEMA 7.60. *Če je karakteristika komutativnega kolobarja K praštevilo p, je preslikava $\varphi : K \to K$, $\varphi(x) = x^p$, endomorfizem tega kolobarja.*

DOKAZ. Očitno je

$$\varphi(xy) = (xy)^p = x^p y^p = \varphi(x)\varphi(y).$$

Dokazati moramo, da φ ohranja vsoto, torej da v K velja enakost, kot bi si jo od nekdaj želeli:

$$(x + y)^p = x^p + y^p.$$

V komutativnih kolobarjih nasploh velja binomska formula. Izpeljemo jo enako kot za števila. Tako je

$$(x + y)^p = x^p + \binom{p}{1} x^{p-1}y + \binom{p}{2} x^{p-2}y^2 + \cdots + \binom{p}{p-1} xy^{p-1} + y^p.$$

Kot vemo, je binomski koeficient $\binom{p}{k} = \frac{p!}{k!(p-k)!}$ naravno število. Ker je p praštevilo in ker za $k = 1, \ldots, p-1$ v zapisu števila $k!(p-k)!$ nastopajo le od p manjša števila, je $\binom{p}{k}$ deljiv s p. Zato so v zgornji vsoti vsi členi razen prvega in zadnjega enaki 0. □

Preslikavi φ pravimo **Frobeniusov endomorfizem**. Označimo $\varphi \circ \varphi$ s φ^2. Torej je

$$\varphi^2(x) = (x^p)^p = x^{p^2}.$$

Kot kompozitum endomorfizmov je tudi φ^2 endomorfizem vsakega komutativnega kolobarja K s karakteristiko p. Splošneje, $\varphi^n := \varphi \circ \cdots \circ \varphi$, kjer φ nastopa n-krat, je endomorfizem K. Deluje s predpisom

$$\varphi^n(x) = x^{p^n}. \tag{7.24}$$

Zdaj lahko dokažemo napovedano trditev. Kot v dokazu leme 7.59 bomo tudi tu prišli do zaključka, da je razpadno polje našega polinoma kar enako množici vseh njegovih ničel.

LEMA 7.61. *Razpadno polje polinoma $f(X) = X^{p^n} - X$ nad poljem $\mathbb{Z}_p$ ima p^n elementov.*

DOKAZ. Označimo to razpadno polje z E. Po definiciji je E najmanjše polje, ki vsebuje vse ničle tega polinoma. Naj bo E_0 množica vseh ničel, torej

$$E_0 = \{x \in E \mid x^{p^n} = x\}.$$

V luči (7.24) lahko to množico opišemo s pomočjo Frobeniusovega endomorfizma φ:

$$E_0 = \{x \in E \mid \varphi^n(x) = x\}.$$

Iz tega zapisa pa sledi, da je množica E_0 že sama polje. Namreč, ker je φ^n endomorfizem, iz $x, y \in E_0$ sledi $x - y, xy \in E_0$, $1 \in E_0$ in $x^{-1} \in E_0$ za vsak $x \neq 0$ iz E_0. Zato je $E_0 = E$.

Kot polinom stopnje p^n ima $f(X)$ največ p^n različnih ničel. Torej je $|E| \leq p^n$. Če ničle štejemo z njihovo kratnostjo, pa ima $f(X)$ natanko p^n ničel. Pokažimo, da so vse ničle enostavne. S tem bo želena enakost $|E| = p^n$ dokazana. Iz zapisa $f(X) = (X^{p^n-1} - 1)X$ jasno sledi, da 0 je enostavna ničla. Vzemimo ničlo $a \neq 0$. Potem je $a^{p^n-1} = 1$ in zato

$$f(X) = (X^{p^n-1} - a^{p^n-1})X = (X - a)g(X),$$

kjer je

$$g(X) = X^{p^n-1} + aX^{p^n-2} + a^2X^{p^n-3} + \cdots + a^{p^n-3}X^2 + a^{p^n-2}X.$$

Očitno je $g(a) = (p^n - 1)a^{p^n-1} = (p^n - 1) \cdot 1$. Ker pa ima polje E kot razširitev polja $\mathbb{Z}_p$ karakteristiko enako p, sledi $g(a) = -1 \neq 0$. Torej je a enostavna ničla $f(X)$. □

Polju iz zadnje leme pravimo **Galoisovo polje** s p^n elementi in ga označujemo z $GF(p^n)$ (ali s $\mathbb{F}_{p^n}$). Seveda je $GF(p) = \mathbb{Z}_p$. Kot je razvidno iz dokaza leme 7.58, je $[GF(p^n) : \mathbb{Z}_p] = n$.

Pozornemu bralcu se je definicija polja $GF(p^n)$ morda zazdela dvoumna. Razpadno polje polinoma namreč ni dobesedno eno samo. Katero imamo v mislih? Odgovor je, da katerokoli. Ker so si vsa izomorfna, med njimi ne ločujemo. Oznako $GF(p^n)$ dejansko uporabljamo za katerokoli polje s p^n elementi. Zdaj, na koncu knjige, ko smo si že nabrali nekaj izkušenj z algebraičnim načinom premišljevanja, si lahko privoščimo tovrstno poenostavitev, ki na prvi pogled ni v sozvočju z matematično doslednostjo.

Združimo ugotovitve iz lem 7.58, 7.59 in 7.61. S hkratnim sklicem na izrek 7.43 (obstoj razpadnega polja) in posledico 7.49 (enoličnost razpadnega polja) dobimo tale izrek.

IZREK 7.62. *Za vsako praštevilo p in vsako naravno število n obstaja polje $GF(p^n)$ s p^n elementi. Vsako končno polje je izomorfno enemu izmed teh polj.*

Končna polja torej zdaj poznamo – vsaj teoretično. Iz naše definicije polj $GF(p^n)$ namreč ni enostavno razvidno, kako v njih računati. K razumevanju tega bodo nekaj pripomogle naloge.

Na koncu povejmo, da se končna polja uporabljajo v teoriji števil in še nekaterih klasičnih področjih matematike. V modernem času pa so se izkazala kot uporabna tudi v kriptografiji in teoriji kodiranja. Ti področji ležita na meji med matematiko in drugimi znanostmi.

Naloge

1. Naj bo F končno polje in E njegova razširitev. Pokaži, da je $[E : F] = n$ natanko tedaj, ko je $|E| = |F|^n$.
2. Pokaži, da je produkt vseh neničelnih elementov končnega polja enak -1.

   Namig. $X^{p^n-1} - 1 = \prod_{a \in GF(p^n)^*}(X - a)$ (zakaj?).
3. Pokaži, da za vsak $f(X) \in \mathbb{Z}_p[X]$ velja $f(X^{p^n}) = f(X)^{p^n}$ za vse $n \geq 0$.
4. Pokaži, da je Frobeniusov endomorfizem končnega polja avtomorfizem.
5. Pokaži, da Frobeniusov endomorfizem polja racionalnih funkcij $\mathbb{Z}_p(X)$ ni surjektiven.

   Namig. Koliko je lahko stopnja polinoma, ki je v zalogi vrednosti φ?
6. Ali obstaja homomorfizem iz $GF(4)$ v $\mathbb{Z}_4$? Ali obstaja homomorfizem iz $\mathbb{Z}_4$ v $GF(4)$?
7. Naj bo E končno polje. Pokaži, da je grupa $(E^*, \cdot)$ ciklična.

   Navodilo. Denimo, da ni ciklična. Iz ugotovitve naloge 5.4/14 potem sledi, da obstaja tako praštevilo p, da za več kot p elementov $x \in E^*$ velja $x^p = 1$. Toda to ne more biti res, saj bi potem polinom $X^p - 1$ imel v E več ničel, kot je njegova stopnja.
8. Pokaži, da za vsako naravno število n obstaja nerazcepen polinom stopnje n nad $\mathbb{Z}_p$.

   Namig. Naj bo a generator ciklične grupe $GF(p^n)^*$ (gl. prejšnjo nalogo). Potem je $GF(p^n) = \mathbb{Z}_p(a)$. Koliko je torej stopnja algebraičnosti elementa a?
9. Naj bo $q(X) \in \mathbb{Z}_p[X]$ nerazcepen polinom stopnje n. Pokaži, da je $GF(p^n) = \mathbb{Z}_p[X]/(q(X))$ in da $q(X)$ deli polinom $X^{p^n} - X$.

   Namig. Odseki $X^i + (q(X))$, $i = 0, 1, \ldots, n-1$, so linearno neodvisni nad $\mathbb{Z}_p$, vsak odsek $f(X) + (q(X))$ pa je njihova linearna kombinacija.

10. Preveri, da je polinom X^2+X+1 nerazcepen v $\mathbb{Z}_2[X]$. Iz prejšnje naloge sledi, da je $GF(4) = \mathbb{Z}_2[X]/(X^2+X+1)$. S pomočjo te enakosti zapiši tabeli za seštevanje in množenje elementov polja $GF(4)$.
11. S pomočjo naloge 9 pokaži, da je:
    (a) $GF(8) = \mathbb{Z}_2[X]/(X^3+X+1)$.
    (b) $GF(9) = \mathbb{Z}_3[X]/(X^2+1)$.
    (c) $GF(16) = \mathbb{Z}_2[X]/(X^4+X+1)$.
    (d) $GF(25) = \mathbb{Z}_5[X]/(X^2+3)$.
    (e) $GF(27) = \mathbb{Z}_3[X]/(X^3-X-1)$.
12. S pomočjo prejšnjih nalog zapiši polinoma $X^4 - X$ in $X^8 - X$ kot produkt nerazcepnih polinomov iz $\mathbb{Z}_2[X]$.
13. Naj $d \,|\, n$. Pokaži, da je $L := \{x \in GF(p^n) \,|\, x^{p^d} = x\}$ podpolje $GF(p^n)$ in da je $|L| = p^d$.

    Navodilo. Pri dokazu, da je L podpolje, se zgleduj po dokazu leme 7.61. Zatem pokaži, da $p^d - 1$ deli $p^n - 1$, zato $X^{p^d-1} - 1$ deli $X^{p^n-1} - 1$ v $\mathbb{Z}_p[X]$, potem pa tudi $X^{p^d} - X$ deli $X^{p^n} - X$ v $\mathbb{Z}_p[X]$. Kot vemo, ima $X^{p^n} - X$ toliko ničel v $GF(p^n)$, kot je njegova stopnja. Od tod sklepaj, da isto velja za njegov delitelj $X^{p^d} - X$. To pomeni, da je $|L| = p^d$.
14. Naj bo L podpolje polja $GF(p^n)$. Pokaži, da obstaja tak $d \in \mathbb{N}$, da je $|L| = p^d$, $d \,|\, n$ in $L = \{x \in GF(p^n) \,|\, x^{p^d} = x\}$.

    Komentar. Iz te in iz prejšnje naloge sledi, da ima $GF(p^n)$ za vsak delitelj d števila n natanko eno podpolje s p^d elementi in da so to tudi edina podpolja $GF(p^n)$. Polje $GF(p^d)$ tako lahko obravnavamo kot podpolje $GF(p^n)$. Na primer, podpolja $GF(p^{16})$ so

    $$GF(p),\ GF(p^2),\ GF(p^4),\ GF(p^8),\ GF(p^{16}).$$

    Vsako iz seznama je podpolje naslednjega. Bolj prepletena so podpolja $GF(p^{12})$, torej

    $$GF(p),\ GF(p^2),\ GF(p^3),\ GF(p^4),\ GF(p^6),\ GF(p^{12}).$$

    Denimo, nobeno izmed podpolj $GF(p^2)$ in $GF(p^3)$ ni vsebovano v drugem, obe pa sta sta vsebovani v $GF(p^6)$. Podpolje $GF(p^2)$ je vsebovano tudi v $GF(p^4)$, $GF(p^3)$ pa ne.

    Za poljubni naravni števili m in n lahko $GF(p^m)$ in $GF(p^n)$ obravnavamo kot podpolji $GF(p^{mn})$. To nam omogoči vpeljavo seštevanja in množenja v množici

    $$\overline{\mathbb{Z}}_p := \bigcup_{n\in\mathbb{N}} GF(p^n),$$

    ki s tem postane polje. Ni težko razmisliti, da je $\overline{\mathbb{Z}}_p$ algebraično zaprtje polja $\mathbb{Z}_p$.

DODATEK A

Zornova lema in njena uporaba

Na različnih področjih matematike, tudi v algebri, nam pogosto pride prav *Zornova lema* iz teorije množic. V tem dodatku jo bomo predstavili in iz nje izpeljali dve posledici, povezani s tematiko knjige.

Množica $\mathcal{S}$ skupaj z relacijo $\leq$, ki je refleksivna ($s \leq s$), antisimetrična (iz $s \leq t$ in $t \leq s$ sledi $s = t$) in tranzitivna (iz $s \leq t$ in $t \leq u$ sledi $s \leq u$), se imenuje **delno urejena množica**. Npr. vsaka podmnožica potenčne množice, torej množice vseh podmnožic neke množice, je delno urejena za relacijo inkluzije $\subseteq$. Neprazna podmnožica $\mathcal{V}$ delno urejene množice $\mathcal{S}$ se imenuje **veriga**, če za vsaka $u, v \in \mathcal{V}$ velja $u \leq v$ ali $v \leq u$. Elementu $z \in \mathcal{S}$ pravimo **zgornja meja** množice $\mathcal{V}$, če je $v \leq z$ za vsak $v \in \mathcal{V}$. Nazadnje, element $m \in \mathcal{S}$ se imenuje **maksimalen element**, če za vsak $s \in \mathcal{S}$ iz $m \leq s$ sledi $s = m$. Opozorimo, da maksimalen element ni nujno največji, torej tak, da je $s \leq m$ za vse $s \in \mathcal{S}$. Če največji element obstaja, je en sam, maksimalnih elementov pa je lahko več.

Zornova lema. *Če je $\mathcal{S}$ neprazna delno urejena množica, v kateri ima vsaka veriga zgornjo mejo, potem $\mathcal{S}$ vsebuje vsaj en maksimalen element.*

Dokaza ne bomo podali. Omenimo le, da je Zornova lema ekvivalentna aksiomu izbire.

Prva posledica govori o obstoju baz vektorskih prostorov, ki niso nujno končno-razsežni. Spomnimo se, da je baza vektorskega prostora V vsaka podmnožica V, ki je ogrodje in je linearno neodvisna. Slednje pomeni, da je vsaka njena končna podmnožica linearno neodvisna. Enostaven primer baze vektorskega prostora polinomov $F[X]$ nad poljem F je množica $\{1, X, X^2, \dots\}$. Ta baza je sicer neskončna, toda števna. Baze mnogih vektorskih prostorov niso števne in konkretne primere baz je pogosto težko najti. S pomočjo Zornove leme pa je razmeroma enostavno dokazati njihov obstoj.

Izrek A.1. *Vsak vektorski prostor ima bazo.*

Dokaz. Naj bo $\mathcal{S}$ množica vseh linearno neodvisnih podmnožic vektorskega prostora V nad poljem F. Ker je prazna množica linearno neodvisna, je $\mathcal{S}$ neprazna množica. Za $A, B \in \mathcal{S}$ naj $A \leq B$ pomeni $A \subseteq B$. S tem $\mathcal{S}$ postane delno urejena množica. Naj bo $\mathcal{V}$ veriga v $\mathcal{S}$. Označimo z Z unijo vseh množic, ki so v $\mathcal{V}$. Trdimo, da je Z linearno neodvisna množica. Res,

vzemimo $z_1, \ldots, z_n \in Z$. Potem obstajajo take množice $A_1, \ldots, A_n \in \mathcal{V}$, da je $z_i \in A_i$ za vsak i. Ker pa je $\mathcal{V}$ veriga, ena izmed teh množic, denimo A_1, vsebuje vse ostale. Torej so vsi vektorji z_i elementi linearno neodvisne množice A_1 in so zato linearno neodvisni. S tem smo pokazali, da je $Z \in \mathcal{S}$ in je zato zgornja meja verige $\mathcal{V}$. Zornova lema pove, da $\mathcal{S}$ vsebuje maksimalen element. Označimo ga z B.

Pokažimo, da je B baza prostora V. Kot element $\mathcal{S}$ je B linearno neodvisna množica. Zato moramo dokazati le, da je ogrodje. Če je $V = \{0\}$, je $B = \emptyset$ in to trivialno velja. Naj bo torej $V \neq \{0\}$. Izberimo neničeln $v \in V$. Dokazati želimo, da je v linearna kombinacija elementov iz B. Seveda smemo predpostaviti, da $v \notin B$. Potem $B \cup \{v\}$ vsebuje B kot pravo podmnožico in je zato linearno odvisna množica. Torej $B \cup \{v\}$ vsebuje končno linearno odvisno podmnožico. Ker so podmnožice B linearno neodvisne, mora ta množica vsebovati v. Torej obstajajo taki vektorji $b_1, \ldots, b_n \in B$ in skalarji $\lambda_0, \lambda_1, \ldots, \lambda_n \in F$, ne vsi enaki 0, da je

$$\lambda_0 v + \lambda_1 b_1 + \cdots + \lambda_n b_n = 0.$$

Ker so $b_1, \ldots, b_n$ kot vektorji iz B linearno neodvisni, je $\lambda_0 \neq 0$. Zato je

$$v = (-\lambda_0^{-1}\lambda_1)b_1 + \cdots + (-\lambda_0^{-1}\lambda_n)b_n$$

in tako v leži v linearni lupini B. □

Druga posledica govori o obstoju maksimalnih idealov. Spomnimo se, da ideal I kolobarja K imenujemo pravi ideal, če $I \neq K$.

Izrek A.2. *Vsak pravi ideal I kolobarja K je vsebovan v kakem maksimalnem idealu.*

Dokaz. Označimo s $\mathcal{S}$ množico vseh pravih idealov kolobarja K, ki vsebujejo I. Ker je $I \in \mathcal{S}$, je $\mathcal{S}$ neprazna. Kot v prejšnjem dokazu $\mathcal{S}$ delno uredimo z inkluzijo. Vzemimo verigo $\mathcal{V}$ v $\mathcal{S}$. Označimo z J unijo vseh idealov iz $\mathcal{V}$. Če uspemo pokazati, da je J element $\mathcal{S}$ in s tem zgornja meja $\mathcal{V}$, bo iz Zornove leme sledil obstoj maksimalnega elementa v $\mathcal{S}$. Prav to pa želimo dokazati, saj je ta maksimalen element ravno maksimalen ideal, ki vsebuje I.

Pokažimo torej, da je $J \in \mathcal{S}$. Seveda je $J \supseteq I$. Dokazati moramo, da je J pravi ideal kolobarja K. Očitno za vsak $x \in K$ in vsak $u \in J$ velja $xu, ux \in J$. Manj očitno je, da je J podgrupa za seštevanje. Toda če vzamemo $u_1, u_2 \in J$, je u_1 element ideala $I_1 \in \mathcal{V}$, u_2 pa element ideala $I_2 \in \mathcal{V}$. Ker je $\mathcal{V}$ veriga, je $I_1 \subseteq I_2$ ali $I_2 \subseteq I_1$ in zato $u_1 - u_2 \in I_1 \cup I_2 \subseteq J$. Razmisliti moramo le še, da $J \neq K$. To pa je res, ker $1 \notin J$. Namreč, če bi enota 1 bila vsebovana v J, bi bila vsebovana tudi v nekem idealu iz $\mathcal{V}$. Toda trditev 4.29 pove, da to ne more biti res. □

Omenimo še, da tudi dokaz obstoja algebraičnega zaprtja danega polja temelji na Zornovi lemi.

DODATEK B

Osnovni izrek algebre

Če se ozremo na zgodovino algebre, kot smo jo orisali v razdelku 7.1, lahko razumemo, zakaj ugotovitvi o obstoju ničel kompleksnih polinomov pravimo *osnovni izrek algebre*. Nekoliko paradoksalno pa nobeden izmed dokazov izreka ni povsem algebraičen. Vsi vključujejo vsaj pojem zveznosti. Zato je dokaz težko naravno vključiti v učbenik iz algebre. Naj mu bo mesto v dodatku.

V literaturi najdemo veliko dokazov tega znamenitega izreka. Predstavili bomo enega izmed najbolj elementarnih. Razen najbolj standardnih orodij matematične analize bomo potrebovali še tale znani izrek: če je $D \subseteq \mathbb{R}^n$ zaprta in omejena (torej kompaktna) množica in je $g : D \to \mathbb{R}$ zvezna funkcija, potem je g na D omejena in doseže minimalno in maksimalno vrednost.

IZREK B.1. ***(osnovni izrek algebre)*** *Vsak nekonstanten polinom $f(X)$ iz $\mathbb{C}[X]$ ima v $\mathbb{C}$ ničlo.*

DOKAZ. Zapišimo

$$f(X) = a_n X^n + \cdots + a_1 X + a_0,$$

kjer so $a_i \in \mathbb{C}$, $a_n \neq 0$ in $n \geq 1$. Iz zapisa

$$|f(z)| = |a_n| \cdot |z|^n \cdot \left|1 + \frac{a_{n-1}}{a_n z} + \cdots + \frac{a_0}{a_n z^n}\right|$$

razberemo, da je

$$\lim_{|z|\to\infty} |f(z)| = \infty.$$

Tako najdemo tak $r > 0$, da iz $|z| > r$ sledi $|f(z)| > |f(0)|$. Po zgoraj omenjenem izreku obstaja tak $z_0 \in D := \{z \in \mathbb{C} \,|\, |z| \leq r\}$, da je

$$|f(z_0)| \leq |f(z)| \quad \text{za vse } z \in D.$$

Med drugim je $|f(z_0)| \leq |f(0)|$, zato velja

$$|f(z_0)| \leq |f(z)| \quad \text{za vse } z \in \mathbb{C}. \tag{B.1}$$

Pokažimo, da iz (B.1) sledi $f(z_0) = 0$. Problem najprej malce poenostavimo; ker polinom $f_1(X) := f(X + z_0)$ zadošča $|f_1(0)| \leq |f_1(z)|$ za vse $z \in \mathbb{C}$ in je $f_1(0) = f(z_0)$, smemo brez škode za splošnost privzeti, da je $z_0 = 0$.

Denimo, da $f(0) \neq 0$. S pomočjo polinoma $f_2(X) := \frac{1}{f(0)} f(X)$ vidimo, da smemo privzeti, da je $f(0) = 1$. Tako lahko $f(X)$ zapišemo kot

$$f(X) = 1 + aX^m + X^{m+1}h(X),$$

kjer je $m \geq 1$, $0 \neq a \in \mathbb{C}$ in $h(X) \in \mathbb{C}[X]$. Kot bralec gotovo ve, je enačba $z^m = c$ rešljiva v $\mathbb{C}$ za vsak $c \in \mathbb{C}$. Naj bo $b \in \mathbb{C}$ tak, da je $b^m = -a$. Polinom $f_3(X) := f(b^{-1}X)$ prav tako zadošča pogoju (B.1) za $z_0 = 0$. Zato smemo privzeti, da je $a = -1$, torej

$$f(X) = 1 - X^m + X^{m+1}h(X).$$

Opazujmo vrednosti našega polinoma samo za realna števila x iz intervala $[0, 1]$. Ker je $0 \leq x^m \leq 1$, velja

$$|f(x)| \leq 1 - x^m + x^{m+1}|h(x)| \quad \text{za vse } x \in [0, 1]. \tag{B.2}$$

S ponovno uporabo omenjenega izreka dobimo obstoj takega števila $M > 0$, da je $|h(x)| \leq M$ za vse $x \in [0, 1]$. Če je $0 < x < \min\{1, \frac{1}{M}\}$, iz (B.2) sledi

$$|f(x)| \leq 1 - x^m(1 - xM) < 1,$$

kar je v nasprotju s $|f(z)| \geq 1$ za vse $z \in \mathbb{C}$. □

Stvarno kazalo

MATEMATIČNI ROKOPISI

Izdajata: Društvo matematikov, fizikov in astronomov Slovenije
DMFA – založništvo

Založilo: DMFA – založništvo, Jadranska ulica 19, 1000 Ljubljana
www.dmfa-zaloznistvo.si

Odgovorni urednik Miran Černe

26.

Matej Brešar

UVOD V ALGEBRO

Računalniško stavil avtor
Tehnični urednik Matjaž Zaveršnik

Natisnila tiskarna ITAGRAF v nakladi 300 izvodov
Ljubljana 2018

Cena: 12,50 EUR