ALGEBRA 2 - ZAPISKI

Gal Anton Gorše

1 Osnovne algebrske strukture

1.1 Binarne operacije

Definicija 1.1. Binarna operacija na neprazni množici S je preslikava iz $S \times S$ v S.

Zgled 1.1. *Oglejmo si nekaj osnovnih primerov že znanih binarnih operacij.*
- *Seštevanje je binarna operacija $\mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ s predpisom $(m, n) \mapsto m + n$ (namesto $\mathbb{Z}$ lahko vzamemo različne številske množice).*
- *Množenje je binarna operacija $\mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ s predpisom $(m, n) \mapsto m \cdot n$.*
- *Naj bo X poljubna neprazna množica in naj $\mathcal{F}(X)$ označuje množico vseh funkcij $f : X \to X$. Potem je komponiranje funkcij binarna operacija na množici $\mathcal{F}(X)$.*
- *Vektorski produkt $\vec{x} \times \vec{y}$ je binarna operacija na prostoru $\mathbb{R}^3$ (za razliko od na primer skalarnega produkta, ki pa to ni).*

Dogovor. Do nadaljnega bomo uporabljali oznako $*$ za poljubno binarno operacijo na S.

Definicija 1.2. Nevtralni element za operacijo $*$ je tak element $e \in S$, da je $e * x = x * e = x$ za vse $x \in S$.

Zgled 1.2. *Navedimo še nevtralne elemente prejšnjih operacij.*
- *Število 0 je nevtralni element seštevanja na $\mathbb{Z}$ (za razliko od seštevanja na $\mathbb{N}$, ki nima nevtralnega elementa).*
- *Množenje na $\mathbb{Z}$ ima nevtralni element 1.*
- *Kompozicija na $\mathcal{F}(X)$ ima za nevtralni element funkcijo id_X.*

Definicija 1.3. Element $e' \in S$ je levi nevtralni element, če je $e' * x = x$ za vse $x \in S$. Podobno je e'' desni nevtralni element, če je $x * e'' = x$ za vse $x \in S$.

Zgled 1.3. *Naj bo S poljubna množica in $x * y = y$ za vse $x, y \in S$. Potem je vsak element množice S levi nevtralni element.*

Trditev 1.1. *Če je e' levi nevtralni element in e'' desni nevtralni element, je $e' = e''$.*

Dokaz. $e' = e' * e'' = e''$ □

Posledica 1.2. *Če nevtralni element obstaja, je en sam.*

Dokaz. Nevtralni element je hkrati levi in desni nevtralni element. □

Definicija 1.4. Binarna operacija $*$ je asociativna, če je $x * (y * z) = (x * y) * z$ za vse $x, y, z \in S$.

Definicija 1.5. Elementa $x, y \in S$ komutirata, če je $x*y = y*x$. Če komutirata poljubna elementa iz S, rečemo, da je operacija $*$ komutativna.

Zgled 1.4. *Iz prejšnjih zgledov so operacije seštevanja, množenja in komponiranja asociativne, operacija vektorskega produkta na $\mathbb{R}^3$ pa ne. Komutativna pa sta le seštevanje in množenje.*

Opomba. Odštevanje (na $\mathbb{Z}$ in preostalih znanih številskih množicah) ni niti asociativna niti komutativna binarna operacija. Obravnavamo jo kot iz seštevanja izpeljano operacijo. Podobno seveda velja tudi za deljenje.

Naj bo $T \subseteq S$. Pravimo, da je T zaprta za binarno operacijo $*$ na S, če je $t_1 * t_2 \in T$ za vse $t_1, t_2 \in T$. V tem primeru tudi rečemo, da je $*$ notranja operacija na T. Zunanja binarna operacija je preslikava iz $K \times S \to S$, kjer sta K in S (lahko) različni množici.

Zgled 1.5. *Če vzamemo $K = \mathbb{R}$ in $S = \mathbb{R}^3$,je množenje s skalarjem*

$$\lambda \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = \begin{bmatrix} \lambda x_1 \\ \lambda x_2 \\ \lambda x_3 \end{bmatrix}$$

zunanja binarna operacija.

1.2 Polgrupe in monoidi

Algebrske strukture so množice, opremljene z eno ali več binarnimi operacijami, ki izpolnjujejo neke aksiome.

Definicija 1.6. Množici S skupaj z asociativno binarno operacijo $*$ pravimo polgrupa $(S, *)$.

Zgled 1.6. *Najpreprostejši primer polgrupe je $(\mathbb{N}, +)$, seveda pa podobno velja tudi za množice $\mathbb{Z}$, $\mathbb{Q}$ ipd.*

Če je operacija $*$ asociativna (oziroma ekvivalentno če je S polgrupa), lahko vedno odpravimo oklepaje. To je netrivialen, a preprost razmislek, ki sledi z indukcijo in ki smo ga že naredili na predavanjih. V polgrupi lahko zato vpeljemo potence elementa:

$$x^n = \underbrace{x * x * \cdots * x}_{n}.$$

Takoj lahko preverimo, da velja $x^m * x^n = x^{m+n}$ in $(x^m)^n = x^{m \times n}$.

Definicija 1.7. Polgrupa z nevtralnim elementom se imenuje monoid.

Zgled 1.7. *Polgrupa $(\mathbb{N}, +)$ ni monoid, zato pa so to na primer $(\mathbb{N} \cup \{0\}, +)$, $(\mathbb{N}, \cdot)$, $(\mathbb{Z}, \cdot)$ in $(\mathcal{F}(X), \circ)$.*

Definicija 1.8. Naj bo $(S, *)$ monoid z nevtralnim elementom e.
- Element y je levi inverz elementa x, če je $y * x = e$.
- Element z je desni inverz elementa x, če je $x * z = e$.
- Element w je inverz elementa x, če je $w * x = x * w = e$ (tj. w je hkrati levi in desni inverz). Če ima x inverz, pravimo, da je obrnljiv element.

Zgled 1.8. *Oglejmo si nekaj primerov obrnljivih elementov v monoidih.*
- *V monoidu* $(\mathbb{N} \cup \{0\}, +)$ *je edini obrnljivi element* 0.
- *V* $(\mathbb{N}, \cdot)$ *je obrnljivi element* 1.
- *V* $(\mathbb{Z}, \cdot)$ *sta obrnljiva elementa* 1 *in* -1.
- *V* $(\mathbb{R}, \cdot)$ *so obrnljivi vsi razen* 0.

Zgled 1.9. *V* $(\mathcal{F}(X), \circ)$ *velja, da ima* f *levi inverz natanko tedaj, ko je* f *injektivna (če* f *ni surjektivna, pa jih ima celo več). Podobno sledi, da ima* f *desni inverz natanko tedaj, ko je surjektivna. Ta razmislek je nekoliko bolj delikaten in zahteva uporabo aksioma izbire. Iz teh dveh izjav pa sledi, da je* f *bijektivna natanko tedaj, ko ima inverz. Ta inverz označujemo s* f^{-1} *in velja* $f \circ f^{-1} = f^{-1} \circ f = \mathrm{id}_X$.

Trditev 1.3. *Naj bo* $(S, *)$ *monoid. Če je* l *levi in* d *desni inverz elementa* $x \in S$*, je* $l = d$.

Dokaz. $d = (l * x) * d = l * (x * d) = l$ □

Posledica 1.4. *Obrnljiv element ima en sam inverz.*

Posledica 1.5. *Če je* x *obrnljiv element, potem iz* $x * y = e$ *sledi* $y * x = e$ *(in seveda obratno).*

Inverz elementa x označujemo s x^{-1}. Velja torej $x * x^{-1} = x^{-1} * x = e$ in $\left(x^{-1}\right)^{-1} = x$.

Trditev 1.6. *Če sta* x, y *obrnljiva elementa monoida* S*, je tudi* $x * y$ *obrnljiv in je njegov inverz* $(x * y)^{-1} = y^{-1} * x^{-1}$.

Dokaz. $(x * y) * (y^{-1} * x^{-1}) = e$ in $(y^{-1} * x^{-1}) * (x * y) = e$. □

Velja tudi posplošitev te trditve, saj za obrnljive elemente $x_1, \ldots, x_n$ velja $(x_1 * \cdots * x_n)^{-1} = x_n^{-1} * \cdots * x_1^{-1}$. Od tod pa je očitno $\left(x^{-1}\right)^n = (x^n)^{-1}$. Po dogovoru velja $x^0 = e$. Če je x obrnljiv, veljata tudi formuli $x^m * x^n = x^{m+n}$ in $(x^m)^n = x^{m \cdot n}$ za poljubni celi števili m, n.

Trditev 1.7. *Naj bo* x *obrnljiv element monoida* S*. Potem iz* $x * y = x * z$ *sledi* $y = z$*. Podobno tudi iz* $y * x = z * x$ *sledi* $y = z$.

Dokaz.

$$x * y = x * z \Rightarrow x^{-1} * x * y = x^{-1} * x * z \Rightarrow y = z$$

□

1.3 Grupe

Definicija 1.9. Monoid, v katerem je vsak element obrnljiv, se imenuje grupa. Grupa, v kateri je operacija komutativna, pa se imenuje Abelova grupa.

Grupa G je končna, če ima končno mnogo elementov. Red končne grupe je število njenih elementov.

Zgled 1.10. *$(\mathbb{Z},+)$, $(\mathbb{Q},+)$, $(\mathbb{R},+)$ in $(\mathbb{C},+)$ so Abelove grupe.*

Trditev 1.8. *Naj bo $(S,*)$ monoid. Potem je množica $S^* = \{x \in S \mid x \text{ obrnljiv}\}$ grupa za operacijo $*$.*

Dokaz. Če sta $x, y \in S^*$, potem je tudi $x * y \in S^*$. Operacija $*$ je torej notranja (in seveda asociativna) na množici S^*. Hkrati pa velja $e \in S^*$ in $x \in S^* \Rightarrow x^{-1} \in S^*$, torej S^* res ustreza vsem pogojem za grupo. □

Zgled 1.11. *Oglejmo si nekaj primerov grup.*

1. *Iz zgornje trditve sledi, da ker sta $(\mathbb{N} \cup \{0\},+)$ in $(\mathbb{N},\cdot)$ monoida, sta $(\{0\},+)$ in $(\{1\},\cdot)$ grupi. Grupi z enim samim elementom pravimo trivialna grupa.*
2. *Za monoid $(\mathbb{Z},\cdot)$ je $\mathbb{Z}^* = \{-1,1\}$ grupa.*
3. *Množice $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$, $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$ in $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$ so Abelove grupe za množenje.*
4. *Za monoid $(\mathcal{F}(X),\circ)$ je množica $\mathcal{F}^*(X) = \mathrm{Sim}X = \{f : X \to X \mid f \text{ bijektivna}\}$ grupa za kompozitum. Tej grupi pravimo tudi simetrična grupa množice X. Če ima X več kot 2 elementa, ta grupa ni Abelova. Permutacija na X je bijekcija iz X nazaj v X. Za končno množico $X = \{1,2,\ldots,n\}$ označimo $S_n = \mathrm{Sim}X$ kot množico permutacij na X.*

Da si olajšamo delo, bomo uporabili nekoliko ohlapnejše oznake. Namesto $*$ bomo od sedaj naprej na mestu operacije uporabili $\cdot$, torej bomo pisali $x \cdot y$ ali kar xy. Enoto e označimo kot 1, operacijo $\cdot$ pa kot produkt. V teh novih oznakah lahko ponovno navedemo ekvivalentno (a nekoliko bolj konkretno) definicijo grupe.

Definicija 1.10. Neprazna množica G skupaj z binarno operacijo $(x,y) \mapsto x \cdot y$ je grupa, če veljajo naslednje točke.

- Velja $(xy)z = x(yz)$ za vse $x,y,z \in G$.
- Obstaja $1 \in G$, da velja $x \cdot 1 = 1 \cdot x = x$ za vsak $x \in G$. Elementu 1 rečemo enota grupe G.
- Za vsak $x \in G$ obstaja tak $y \in G$, da je $xy = yx = 1$. Imenujemo ga inverz elementa x in ga označimo z x^{-1}.

Če velja tudi $xy = yx$ za vse $x,y \in G$, potem je G Abelova grupa.

Iz drugega podpoglavja že vemo:

- grupa ima eno samo enoto,
- vsak element ima natanko en inverz,
- $(x^{-1})^{-1} = x$, $\forall x \in G$,
- $(xy)^{-1} = y^{-1}x^{-1}$, $\forall x,y \in G$,
- $x^m \cdot x^n = x^{m+n}$ in $(x^m)^n = x^{m \cdot n}$ za $\forall x \in G$ ter $m,n \in \mathbb{Z}$,
- $xy = 1 \Rightarrow yx = 1$, $\forall x,y \in G$,
- $xy = xz \Rightarrow y = z$ in $yx = zx \Rightarrow y = z$ in
- $x^0 = 1$.

Opomba. Kljub dogovoru bomo operacijo včasih v Abelovih grupah označevali s $+$. Takrat bomo namesto z 1 enoto označevali z 0, inverznemu elementu x pa bomo rekli obratni element x in ga označili z $-x$. Lahko bomo definirali operacijo razlike in namesto x^n pisali $n \cdot x$. Tako pa dobimo tudi formulo $0 \cdot x = 0$, kjer na levi ničla označuje celo število, na desni pa enoto v grupi.

1.4 Kolobarji in polja

Do sedaj smo spoznali, da so osnovne številske množice $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ in $\mathbb{C}$ Abelove grupe za seštevanje. Vendar pa imamo na teh množicah tudi operacijo množenja, za katero so te množice monoidi. Operaciji seštevanja in množenja povezujeta zakona distributivnosti.

Definicija 1.11. Neprazna množica skupaj z binarnima operacijama seštevanja $(x, y) \mapsto x + y$ in množenja $(x, y) \mapsto x \cdot y$ se imenuje kolobar, če velja:
- $(K, +)$ je Abelova grupa,
- $(K, \cdot)$ je monoid (torej je $(xy)z = x(yz)$ in $\exists 1 \in K$, da je $1 \cdot x = x \cdot 1 = x$, $\forall x \in K$),
- izpolnjena sta distributivnostna zakona: $x(y + z) = xy + xz$ in $(y + z)x = yx + zx$ za $\forall x, y, z \in K$.

Če velja vse razen obstoja enote 1, je K kolobar brez enote.

Trditev 1.9. *V poljubnem kolobarju K velja:*

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

Dokaz. Dokazi teh točk so preprosti.
- $0x = (0 + 0)x = 0x + 0x \Rightarrow 0x = 0$
- $0 = 0y = (x + (-x))y = xy + (-x)y \Rightarrow -xy = (-x)y$
- sledi iz (b)
- sledi iz (b)
- $(x - y)z = (x + (-y))z = xz + (-y)z = xz - yz$ □

Definicija 1.12. Kolobar je komutativen, če je množenje komutativno, tj. $xy = yx$, $\forall x, y \in K$.

Zgled 1.12. *Oglejmo si nekaj osnovnih primerov kolobarjev.*
- $\{0\}$ *je trivialni (ali ničelni) kolobar. V njem je* $1 = 0$ *(to velja* $\Leftrightarrow$ *K trivialen).*
- $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ *so komutativni kolobarji. Pri tem je* $\mathbb{Z}$ *najbolj osnoven primer kolobarja, ostali pa so že „nekaj več“.*
- $M_n(\mathbb{R})$, *tj. množica* $n \times n$ *matrik nad* $\mathbb{R}$ *(za običajni operaciji* $+$ *in* $\cdot$*) je nekomutativen kolobar. Vendar pa v tem kolobarju veljajo nekatere posebnosti:*

$$\underbrace{\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}}_{E_{12}} \cdot \underbrace{\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}}_{E_{11}} = 0.$$

Definicija 1.13. Element x kolobarja K je delitelj niča, če $x \neq 0$ in če obstaja tak $y \neq 0$, da je $xy = 0$ ali $yx = 0$. Pri tem x ustrezno poimenujemo levi oziroma desni delitelj niča.

V kolobarju brez deliteljev niča velja pravilo krajšanja: $xy = xz$ in $x \neq 0 \Rightarrow y = z$.

Definicija 1.14. Kolobar je obseg, če so vsi njegovi neničelni elementi obrnljivi. Komutativne obsege imenujemo polja.

Zgled 1.13. *Množice $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ so polja. S primeri nekomutativnega obsega za sedaj počakajmo.*

Trditev 1.10. *Obrnljiv element kolobarja ni delitelj niča. Obsegi so torej kolobarji brez deliteljev niča.*

Dokaz. Naj bo na primer $xy = 0$ in x obrnljiv. Potem je $x^{-1}xy = 0$ in posledično $y = 0$. □

Zgled 1.14. *Prejšnja trditev ne velja v obratno smer. Množica $\mathbb{Z}$ na primer nima deliteljev niča, a ni obseg.*

1.5 Vektorski prostori in algebre

Definicija 1.15. Naj bo F polje. Množica V skupaj z notranjo binarno operacijo seštevanja $(u, v) \mapsto u + v$ in zunanjo binarno operacijo $F \times V \to V$ s predpisom $(\lambda, v) \mapsto \lambda v$, imenovano množenje s skalarjem, je vektorski prostor nad F, če velja:

- $(V, +)$ je Abelova grupa,
- $(\lambda + \mu)v = \lambda v + \mu v$ za vse $\lambda, \mu \in F$, $v \in V$,
- $\lambda(u + v) = \lambda u + \lambda v$ za vse $\lambda \in F$, $u, v \in V$,
- $(\lambda\mu)v = \lambda(\mu v)$ za vse $\lambda, \mu \in F$, $v \in V$,
- $1 \cdot v = v$ za vse $v \in V$.

Elementi V so vektorji, elementi F pa so skalarji. Prostorom $\mathbb{R}^n$ pravimo realni vektorski prostori, $\mathbb{C}^n$ pa kompleksni vektorski prostori. Iz aksiomov sledi $\lambda \cdot 0 = 0$, $0 \cdot v = 0$ in $\lambda v \Rightarrow \lambda = 0$ ali $v = 0$. Prav tako lahko vidimo, da velja $(-\lambda)v = \lambda(-v) = -\lambda v$.

Zgled 1.15. *Navedimo nekaj primerov vektorskih prostorov (podrobneje smo si jih že ogledali prejšnje leto pri algebri 1).*

- *$F^n = F \times F \times \cdots \times F$ je vektorski prostor za operaciji $(x_1, \ldots, x_n) + (y_1, \ldots, y_n) = (x_1 + y_1, \ldots, x_n + y_n)$ in $\lambda(x_1, \ldots, x_n) = (\lambda x_1, \ldots, \lambda x_n)$.*
- *$\{0\}$ je trivialni vektorski prostor.*
- *Vektorski prostor realnih polinomov $\mathcal{P}$ je neskončnorazsežni vektorski prostor nad $\mathbb{R}$.*
- *Množica $\mathbb{C}$ je vektorski prostor nad $\mathbb{R}$ z običajnim množenjem (s skalarjem).*

Definicija 1.16. Množica A skupaj z binarnima operacijama seštevanja $(x, y) \mapsto x + y$, množenja $(x, y) \mapsto x \cdot y$ in zunanjo obinarno operacijo $F \times A \to A$, $(\lambda, x) \mapsto \lambda x$ (tu je F polje) je algebra nad F, če velja:

- A je vektorski prostor za operaciji seštevanja in množenja s skalarjem,
- A je kolobar za operaciji seštevanja in množenja,
- $\lambda(xy) = (\lambda x)y = x(\lambda y)$ za vse $\lambda \in F$, $x, y \in V$.

Zgled 1.16. *Oglejmo si nekaj zgledo algeber, ki smo jih tudi že spoznali pri algebri 1.*

- *Množica F^n je algebra za operacijo množenja $(x_1, \ldots, x_n)(y_1, \ldots, y_n) = (x_1y_1, \ldots, x_ny_n)$, kjer je $0 = (0, \ldots, 0)$ in $1 = (1, \ldots, 1)$.*
- *Trivialna (ničelna) algebra je $\{0\}$.*
- *Množica $\mathcal{P}$ realnih polinomov je algebra nad $\mathbb{R}$ (realna algebra).*
- *$M_n(\mathbb{R})$ je realna algebra.*
- *$M_n(\mathbb{C})$ je kompleksna algebra.*

1.6 Podstrukture

Definicija 1.17. Podmnožica H grupe G je podgrupa (grupe G), če je za isto operacijo tudi sama grupa. To označimo $H \leq G$.

Zgled 1.17. *Za vsako grupo G je $G \leq G$ in $\{1\} \leq G$. Slednji podgrupi pravimo trivialna podgrupa. Vsaka podgrupa G, ki ni enaka G, je prava podgrupa.*

Trditev 1.11. *Za neprazno podmnožico H grupe G je ekvivalentno:*

1. $H \leq G$,
2. *za vse $x, y \in H$ je $xy^{-1} \in H$,*
3. *H je zaprta za množenje in $\forall x \in H : \ x^{-1} \in H$.*

Za aditivno grupo se pogoj (2) glasi: za vse $x, y \in H$ je $x - y \in H$, pogoj (3) pa: H je zaprta za seštevanje in $\forall x \in H : \ -x \in H$.

Dokaz. (1) $\Rightarrow$ (2) je očitno. Oglejmo si (2) $\Rightarrow$ (3). Vzemimo $x \in H$. Potem iz točke (2) najprej sledi $1 = xx^{-1} \in H$ in zato $x^{-1} = 1 \cdot x^{-1} \in H$. Torej za vse $x, y \in H$ velja $xy = x(y^{-1})^{-1} \in H$. Za (3) $\Rightarrow$ (1) pa je dokaz ponovno preprost in sledi po točkah. □

Zgled 1.18. *Vzemimo grupo $G = \mathbb{C}^* = \mathbb{C} \setminus \{0\}$. Njene podmnožice so na primer $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$, $\mathbb{R}^+ = \{x \in \mathbb{R} \mid x > 0\}$, $\mathbb{T} = \{z \in \mathbb{C} \mid |z| = 1\}$ in $\{1, -1, i, -i\}$, pri čemer je druge hkrati podgrupa prve, četrta pa podgrupa tretje.*

Zgled 1.19. *Oglejmo si nekaj primerov podgrup.*

- *Naj bo $G = \mathbb{Z}$, potem je $\{0\}, \mathbb{Z} \leq \mathbb{Z}$ in $2\mathbb{Z}, 3\mathbb{Z}, \ldots, k\mathbb{Z} \leq \mathbb{Z}$.*
- *Naj bo G grupa. Potem definiramo center grupe kot*

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

  Očitno ta množica vsebuje enoto in je zaprta za množenje. Če zvezo $cx = xc$ iz obeh strani pomnožimo s c^{-1}, dobimo, da za vsak $x \in G$ velja $c^{-1}x = xc^{-1}$.
- *Za $H \leq G$ in $a \in G$ definiramo $aHa^{-1} = \{axa^{-1} \mid x \in H\}$ in potem je $aHa^{-1} \leq G$.*

Definicija 1.18. Podmnožica L kolobarja K je podkolobar (od K), če je kolobar za isti operaciji in vsebuje enoto 1 kolobarja K.

Trditev 1.12. *Podmnožica L kolobarja K je podkolobar natanko tedaj, ko je $1 \in L$ in za vse $x, y \in L$ velja $xy, x - y \in L$.*

Zgled 1.20. *Navedimo nekaj primerov podkolobarjev.*

- *Množica*

$$L = \left\{ \begin{bmatrix} x & 0 \\ 0 & 0 \end{bmatrix} \middle| x \in \mathbb{R} \right\}$$

  je kolobar za običajni notranji operaciji seštevanja in množenja z enoto $\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$, ki pa ni enota $M_2(\mathbb{R})$. Torej L ni podkolobar $M_2(\mathbb{R})$.
- *Za osnovne številske množice velja $\mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$, kjer $\subseteq$ označuje relacijo podkolobarjev.*

- *Če je K kolobar, je njegov center $Z(K) = \{c \in K \mid cx = xc \text{ za vsak } x \in K\}$ tudi njegov podkolobar.*

Definicija 1.19. Podmnožica U vektorskega prostora V je podprostor, če je za isti operaciji tudi sama vektorski prostor.

Trditev 1.13. *Za podmnožico U vektroskega prostora V so naslednje izjave ekvivalentne.*

1. *U je podprostor V.*
2. *Iz $u, v \in U$ sledi $u + v, \lambda u \in U$ za vse $\lambda \in F$.*
3. *Iz $u, v \in U$ sledi $\lambda u + \mu v \in U$ za vse $\lambda, \mu \in F$.*

Dokaz te trditve in mnoge primere podprostorov smo že spoznali lani pri predmetu algebra 1.

Definicija 1.20. Podmnožica B algebre A je podalgebra, če je algebra za iste operacije operacije in vsebuje enoto 1 algebre A. Algebra je podprostor, ki je hkrati tudi podkolobar.

Trditev 1.14. *Podmnožica B algebre A je podalgebra natanko tedaj, ko velja $1 \in B$, za vse $x, y \in B$ velja $x + y, xy \in B$ in za vse $\lambda \in F$ velja $\lambda x \in B$.*

Zgled 1.21. *Navedimo nekaj primerov podalgeber.*
- *Podalgebra $M_2(\mathbb{R})$ je množica vseh realnih zgornjetrikotnih 2×2 matrik.*
- *Center algebre $Z(A)$ definiramo podobno kot prej in ponovno je to podalgebra.*

Definicija 1.21. Podmnožica F polja E je podpolje, če je za isti operaciji tudi sama polje. Pri tej definiciji je vsebovanje enote samoumevno, saj iz $e^2 = e$ sledi $e(1 - e) = 0$ in ker E nima deliteljev niča, je e lahko le 1.

Trditev 1.15. *Podmnožica F polja E je podpolje natanko tedaj, ko je $1 \in F$ in za vse $x, y \in F$ velja $x - y, xy, x^{-1} \in F$ (za slednjo lastnost mora x biti neničelen).*

Definicija 1.22. Polje E je razširitev polja F, če je F podpolje E.

Presek podgrup je prav tako podgrupa. Enako velja tudi za podkolobarja, podalgebre, podpolja in podprostore. V primeru podgrup pa velja še več: celo presek poljubne družine podgrup je spet podgrupa.

1.7 Generatorji

Naj bo G grupa in $X \subseteq G$ neprazen. Označimo z $\langle X \rangle$ množico elementov oblike $y_1 y_2 \dots y_n$, kjer je $y_i \in X$ ali $y_i^{-1} \in X$.

Zgled 1.22. *Za $X = \{x, y\}$ množica $\langle X \rangle$ vsebuje elemente, kot so $xy, yx, yx^{-1}y^{-11}x^3, \dots$*

Množico $\langle X \rangle$ imenujemo množica, generirana z množico X. To je podgrupa, saj je očitno zaprta za množenje in inverze. Vsaka podgrupa grupe G, ki vsebuje X, vsebuje tudi $\langle X \rangle$. Torej je $\langle X \rangle$ najmanjša podgrupa G, ki vsebuje X. Z „najmanjšo“ mislimo, da je $\langle X \rangle$ vsebovana v vsaki podgrupi G, ki vsebuje X. Ker je presek podgrup podgrupa, je $\langle X \rangle$ enaka preseku vseh podgrup, ki vsebujejo X (s tem smo tudi utemeljili eksistenco $\langle X \rangle$). Elemente X imenujemo generatorji in namesto $\langle X \rangle$ lahko pišemo tudi $\langle x_1, \dots, x_n \rangle$.

Če je $\langle X \rangle = G$, potem rečemo, da je G generirana z X, elemente iz X pa imenujemo kar generatorji G. G je končno generirana, če je enakost $\langle X \rangle = G$ izpolnjena za kakšno končno množico X. Enako definiramo pojme, kot so na primer podkolobar, podprostor, podalgebra ali podpolje, generirani z X. Če je $X = \emptyset$, je $\langle X \rangle = \langle \emptyset \rangle = \{1\}$. Podprostor, generiran z $\emptyset$ je $\{0\}$. Podkolobar generiran z $\emptyset$ je enak podkolobarju, generiranem z $\{0, 1\}$. Enako velja tudi za podalgebre in podpolja.

Kot že vemo, za $X \neq \emptyset$ velja

$$\langle X \rangle = \{x_1^{n_1} \dots x_k^{n_k} \mid x_i \in X,\ n_i \in \mathbb{Z}\}.$$

Grupi $\langle X \rangle = \{x^n \mid n \in \mathbb{Z}\}$, generirani z enim samim elementom, pravimo ciklična grupa. Grupa $\langle x, y \rangle$ vsebuje elemente, kot so 1, x, y, x^{-1}, y^{-1}, $x^2y^3x^{-1}, \dots$ in ta množica je števna. Če je G Abelova, potem je $\langle x, y \rangle = \{x^i y^j \mid i, j \in \mathbb{Z}\}$.

Zgled 1.23. *Naj bo $G = \mathbb{Q}^+$ grupa. Potem je primer generirane podgrupe množica $\langle 2, 3 \rangle = \{2^i 3^j \mid i, j \in \mathbb{Z}\}$. Očitno je, da velja $\langle \mathbb{N} \rangle = \langle \mathbb{P} \rangle = G$, kjer je $\mathbb{P}$ množica praštevil.*

Zgled 1.24. *Vzemimo tokrat $G = \mathbb{Z}$. Sedaj je $\langle X \rangle = \{n_1 x_1 + \dots + n_k x_k \mid n_i \in \mathbb{Z},\ x_i \in X\}$. Potem je na primer $\langle 1 \rangle = \langle -1 \rangle = \mathbb{Z}$ in $\langle 3 \rangle = \langle 6, 9 \rangle = 3\mathbb{Z}$.*

Naj bo $\emptyset \neq X \subseteq K$ in K kolobar. Označimo z $\overline{X}$ podgrupo za seštevanje, generirano z vsemi produkti elementov iz $X \cup \{1\}$. Element iz $\overline{X}$ lahko zapišemo v obliki

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

kjer so $x_{ij} \in X \cup \{1\}$ in $k_i \in \mathbb{Z}$. Hitro vidimo, da je $\overline{X}$ podkolobar 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 in podobno definiramo tako kot analogne pojme v grupah.

Zgled 1.25. *Naj bo K kolobar kompleksnih števil $\mathbb{C}$.*

- *Podkolobar, generiran z elementom 1, je kolobar celih števil $\mathbb{Z}$. Tako je $\mathbb{Z}$ najmanjši podkolobar v $\mathbb{C}$.*
- *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 ga imenujemo kolobar Gaussovih celih števil.*

Naj bo $\emptyset \neq X \subseteq F$ in F polje. Kaj je podpolje, generirano z X? To podpolje gotovo vsebuje $\overline{X}$ od prej. Trdimo, da podpolje generirano z X vsebuje natanko elemente oblike uv^{-1}, kjer sta $u, v \in \overline{X}$ in $v \neq 0$. Vsako podpolje F, ki vsebuje X, očitno vsebuje tudi vse take elemente. Preverimo, da je ta množica zaprte za seštevanje. Res, to sledi direktno iz enakosti $uv^{-1} - wz^{-1} = (uz - vw)(vz)^{-1}$

Zgled 1.26. *Naj bo F polje kompleksnih števil $\mathbb{C}$.*

- *Podpolje, generirano z elementom 1, je polje racionalnih števil $\mathbb{Q}$. Tako je $\mathbb{Q}$ najmanjše podpolje v $\mathbb{C}$.*
- *Podpolje, generirano z elementom i, sestoji iz kompleksnih števil oblike $p + qi$, kjer sta $m, n \in \mathbb{Q}$. Označujemo ga z $\mathbb{Q}(i)$ in to je razširitev polje $\mathbb{Q}$ s priključitvijo elementa i.*

Naj bo $\emptyset \neq X \subseteq V$, kjer je V vektorski prostor. Podprostor, generiran z X je linearna ogrinjača (lupina) množice X, torej množica vseh linearnih kombinacij elementov iz X. Oznaka za ta podprostor je $\mathrm{Lin}\,(X)$, kjer množici X pravimo ogrodje. Prostor V je končnorazsežen natanko tedaj, ko ima končno ogrodje (tj. je končno generiran). Podmnožica B prostora V je baza, če je ogrodje in linearno neodvisna. Vsak vektor iz V lahko na enoličen način zapišemo kot linearno kombinacijo vektorjev iz baze. Baze v vektorskih prostorih vedno obstajajo. Če je V končnorazsežen, imajo vse njegova baze enako število

elementov – temu številu pravimo dimenzija prostora V in označimo $\dim_F V = n$. V tem primeru je vsako ogrodje z n elementi baza.

Zgled 1.27. *Navedimo nekaj primerov baz vektorskih prostorov.*

- *Vektorski prostor F^n je n-razsežen. Njegovo standardno bazo sestavljajo vektorji*

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

- *Kot vektorski prostor nad $\mathbb{R}$ je prostor $\mathbb{C}$ 2-razsežen, nad samim sabo pa 1-razsežen.*
- *Realni vektorski prostor matrik $M_2(\mathbb{R})$ je 4-razsežen. Njegova standardna baza sestoji iz matrik*

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

- *Vektorski prostor vseh realnih polinomov $\mathcal{P}$ je neskončnorazsežen. Njegovo standardno bazo sestavljajo polinomi $1,\ x,\ x^2,\ \ldots$*

Naj bo A algebra nad poljem F in naj bo $\emptyset \neq X \subseteq A$. Podobno kot pri obravnavi generatorjev kolobarjev razmislimo, da je podalgebra, generirana z X množica vseh elementov oblike

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

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

Zgled 1.28. *Algebra realnih polinomov $\mathcal{P}$ je generirana z enim samim elementom, in sicer s polinomom x (kot tudi z vsakim njegovim neničelnim skalarnim večkratnikom).*

Za algebro rečemo, da je končnorazsežna, če je končnorazsežna kot vektorski prostor.

Zgled 1.29. *Algebra matrik $M_2(\mathbb{R})$ je končnorazsežna, njena dimenzija je 4. 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 vsako matriko zapišemo kot linearno kombinacijo matrik E_{11}, E_{22}, $E_{12}E_{21}$ in $E_{21}E_{12}$. Za primerjavo pa E_{11} in E_{22} generirata samo podalgebro vseh diagonalnih matrik. Seveda pa lahko $M_2(\mathbb{R})$ obravnavamo tudi samo kot kolobar. Podkolobar, generiran z elementoma E_{12} in E_{21}, je potem kolobar vseh matrik s celoštevilskimi koeficienti.*

1.8 Direktni produkti in grupe

Naj bodo $G_1, \ldots, G_m$ grupe. Množica $G_1 \times \cdots \times G_m$ je grupa, če definiramo operacijo

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

Tedaj je enota $1 = (1, \ldots, 1)$ in inverz $(x_1, \ldots, x_m)^{-1} = (x_1^{-1}, \ldots, x_m^{-1})$. To grupo imenujemo direktni produkt grup $G_1, \ldots, G_m$ in jo označimo z $G_1 \times \cdots \times G_m$. Če so G_i aditivne grupe, namesto direktnega produkta govorimo o direktni vsoti $G_1 \oplus \cdots \oplus G_m$ z operacijo

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

To ponovimo še za kolobarje. Naj bodo $K_1, \ldots, K_m$ kolobarji. Njihov direktni produkt $K_1, \ldots, K_m$ je (kot množica) kartezičen produkt $K_1 \times \cdots \times K_m$, opremljen z operacijama:

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

Opomba. 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.

Naj bodo sedaj $V_1, \ldots, V_m$ vektorski prostori nad F. Njihova direktna vsota $V_1 \oplus \cdots \oplus V_m$ je kot množica kartezični produkt $V_1 \times \cdots \times V_m$, opremljen z operacijama

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

Tedaj je $V_1 \times \cdots \times V_m$ vektorski prostor nad F.

Preostanejo nam še algebre. Naj bodo $A_1, \ldots, A_m$ algebre nad F. Njihov direktni produkt $A_1 \times \cdots \times A_m$ je (kot množica) zopet kar kartezični produkt $A_1 \times \cdots \times A_m$, opremljen z operacijami

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

Opomba. Kaj pa direktni produkti polj? Polja so kolobarji, zato o njihovem direktnem produktu lahko govorimo. Vn endar pa dobljeni kolobar ni polje, saj ima delitelje niča.

V zgornjih definicijah smo se zaradi enostavnosti omejili na direktne produkte in vsote končnega števila algebrajskih objektov. Lahko pa bi vzeli tudi neskončno družino grup, kolobarjev, itd.

Zgled 1.30. *Oglejmo si direktni produkt števno neskončno mnogo kopij algebre $\mathbb{R}$ nad $\mathbb{R}$:*

$$(x_1, x_2, \ldots) + (y_1, y_2, \ldots) = (x_1 + y_1, x_2 + y_2, \ldots)$$
$$(x_1, x_2, \ldots) \cdot (y_1, y_2, \ldots) = (x_1 y_1, x_2 y_2, \ldots)$$
$$\lambda(x_1, x_2, \ldots) = (\lambda x_1, \lambda x_2, \ldots)$$

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

2 Primeri grup in kolobarjev

2.1 Cela števila

Načelo dobre urejenosti: vsaka neprazna podmnožica $\mathbb{N}$ vsebuje najmanjše število. Vemo, da je množica $S \subseteq \mathbb{Z}$ navzdol omejena, če obstaja celo število m, da je $m \leq s$ za $\forall s \in S$. Splošna verzija načela dobre urejenosti pravi, da vsaka neprazna navzdol omejena podmnožica $\mathbb{Z}$ vsebuje najmanjše število in vsaka neprazna navzgor omejena podmnožica $\mathbb{Z}$ vsebuje največje število.

Izrek 2.1 (Osnovni izrek o deljenju)**.**

Naj bo $m \in \mathbb{Z}$ in $n \in \mathbb{N}$. Potem obstajata taki celi števili q in r, da je $m = qn + r$ in $0 \leq r < n$.

Dokaz. Definiramo množico $\{k \in \mathbb{Z} \mid kn \leq m\}$. Ta množica je navzgor omejena, saj obstajajo taka števila $l \in \mathbb{Z}$, da je $kl > m$ in tak l je zgornja meja za S. Podobno lahko sklepamo, da je S neprazna, saj bi sicer veljalo $kn > m$ za vsa cela števila k. Po načelu dobre urejenosti ima S največji element q, za katerega velja $q + 1 \notin S$. Tako velja $qn \leq m < (q + 1)n$ in če definiramo $r = m - qn$, dobimo $0 \leq r < n$. Število r imenujemo ostanek pri deljenju m z n in očitno je, da sta r in q enolično določena. □

Za vsak $n \in \mathbb{N} \cup \{0\}$ naj bo $n\mathbb{Z} = \{nx \mid x \in \mathbb{Z}\}$. Tako je $0\mathbb{Z} = \{0\}$, $1\mathbb{Z} = \mathbb{Z}$, $2\mathbb{Z} = \{2x \mid x \in \mathbb{Z}\}$ in tako dalje.

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

Dokaz. Trivialno je pokazati, da je $n\mathbb{Z}$ res podgrupa. Dokažimo torej trditev v obratno smer. Če je $H = \{0\}$, je $H = 0\mathbb{Z}$, torej predpostavimo, da H ni trivialna. Vemo, da je $H \cap \mathbb{N} \neq \emptyset$, saj je $H \neq \{0\}$ in vsebuje nasprotna števila vseh svojih elementov. Po načelu dobre urejenosti $H \cap \mathbb{N}$ vsebuje najmanjši element n. Dokazujemo, da velja $H = n\mathbb{Z}$. Očitno je $n\mathbb{Z} \subseteq H$. Vzemimo poljuben $m \in H$. Tako je $m = qn + r$, kjer je $0 \leq r < n$. Ker je n najmanjše naravno število v H, je $r = 0$ in $m = qn \in n\mathbb{Z}$. □

Celo število $k \neq 0$ deli celo število m, če je $m = qk$ za nek $q \in \mathbb{Z}$. Rečemo, da je $k \in \mathbb{N}$ skupni delitelj m in n, če $k \mid m$ in $k \mid n$. Od tod sledi, da je d največji skupni delitelj m in n, če je skupni delitelj teh dveh števil in je d deljiv z vsakim drugim skupnim deliteljem m in n.

Posledica 2.3. *Največji skupni delitelj celih števil m in n (ki nista obe 0) obstaja, je en sam in je oblike $d = mx + ny$ za neka $x, y \in \mathbb{Z}$.*

Naj bosta H, K podgrupi aditivne (in zato tudi Abelove) grupe. Potem je tudi $H + K = \{h + k \mid h \in H,\ k \in K\}$ podgrupa G.

Dokaz. Množica $m\mathbb{Z} + n\mathbb{Z}$ je podgrupa $\mathbb{Z}$, torej obstaja tak $d \in \mathbb{N} \cup \{0\}$, da je $m\mathbb{Z} + n\mathbb{Z} = d\mathbb{Z}$. Ker nista oba izmed m, n ničelna, tudi d ni ničeln. Očitno je, da je d skupni delitelj m in n. Dokazati moremo le še, da je največji skupni delitelj. Ker je $d \in d\mathbb{Z} = m\mathbb{Z} + n\mathbb{Z}$, obstajata taka $x, y \in \mathbb{Z}$, da je $d = mx + ny$. Denimo, da je $m = cq_1$ in $n = cq_2$, torej je c nek skupni delitelj m in n. Potem je $d = c(q_1x + q_2y)$, torej $c \mid d$ in smo dokazali. □

Opomba. Največji skupni delitelj lahko izračunamo s pomočjo Evklidovega algoritma. Če je največji skupni delitelj dveh enak 1, pravimo, da sta si ti števili tuji.

Posledica 2.4. *Celi števili m in n (ne obe 0) sta si tuji natanko tedaj, ko je $mx + ny = 1$ za neka $x, y \in \mathbb{Z}$.*

Opomba. Največji skupni delitelj števil $n_1, \ldots, n_k$ definiramo podobno. Kot prej dokažemo, da tako število d obstaja, je eno damo in je oblike $d = n_1x_1 + \cdots + n_kx_k$ za $x_i \in \mathbb{Z}$. Seveda velja, da so si števila $n_1, \ldots, n_k$ tuja (a ne nujno paroma tuja) natanko tedaj, ko je $n_1x_1 + \cdots + n_kx_k = 1$ za neka $x_1, \ldots, x_k \in \mathbb{Z}$.

Lema 2.5 (Evklid)**.** *Naj bo p praštevilo in $m, n \in \mathbb{Z}$. Če velja $p \mid mn$, potem $p \mid m$ ali $p \mid n$.*

Dokaz. Denimo, da p ne deli m, torej je največji skupni delitelj p in m enak 1. Potem je $px+my = 1$ za neka $x, y \in \mathbb{Z}$. Od tod sledi $pnx+mny = n$ in posledično $pnx+pqy = n$. Torej je $p(nx+qy) = n$ in $p \mid n$. □

Izrek 2.6 (Osnovni izrek aritmetike)**.**

Vsako naravno število $n \geq 2$ je produkt praštevil. Zapis števila kot produkt je enoličen do vrstnega reda faktorjev natančno.

Dokaz. Dokaz poteka z indukcijo po n. □

Izrek 2.7 (Evklid)**.**

Praštevil je neskončno mnogo.

2.2 Grupa in kolobar ostankov

Definicija 2.1. Celi števili a in b sta kongruentni po modulu n, če $n \mid a - b$. To zapišemo $a \equiv b \pmod{n}$.

Zgled 2.1. *Primera:* $14 \equiv 2 \pmod{12}$ *in* $24 \equiv 0 \pmod{12}$.

Sedaj kongruentnost obravnavajmo kot relacijo $\mathbb{Z}$. Hitro vidimo, da je to ekvivalenčna relacija na $\mathbb{Z}$, zato porodi ekvivalenčne razrede: $[0] = n\mathbb{Z}, [1] = n\mathbb{Z} + 1, \ldots, [n-1] = n\mathbb{Z} + n - 1$. Torej vidimo, da je ekvivalenčnih razredov za relacijo kongruentnosti pomodulu n natanko n. Vpeljemo oznako $\mathbb{Z}_n = \{[0], [1], \ldots, [n-1]\}$.

Trditev 2.8. *Če v množico $\mathbb{Z}_n$ vpeljemo seštevanje s predpisom $[a] + [b] = [a + b]$, postane $\mathbb{Z}_n$ Abelova grupa. Če v tej aditivni grupi vpeljemo še seštevanje s predpisom $[a] \cdot [b] = [a \cdot b]$, postane $\mathbb{Z}_n$ komutativen kolobar.*

Dokaz. Dokažemo, da je seštevanje dobro definirano: to pomeni, da iz $[a] = [a']$ in $[b] = [b']$ sledi $[a + b] = [a' + b']$. Torej moramo dokazati, da iz $n \mid a - a'$ in $n \mid b - b'$ sledi $n \mid (a + b) - (a' + b')$, kar pa je očitno. Podobno dokažemo tudi za množenje. Ostale lastnosti seštevanja in množenja so rutinske. □

Množici $(\mathbb{Z}_n, +)$ pravimo grupa ostankov po modulu n, kjer je $\mathbb{Z}_1$ aditivna grupa. Od tod sledi, da je $(\mathbb{Z}_n, +, \cdot)$ kolobar ostankov po modulu n. V navadi je, da oglate oklepaje izpuščamo in pišemo kar $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$. Seveda ima $\mathbb{Z}_n$ lahko tudi deliteljе niča. Za primer $\mathbb{Z}_2$ velja, da je to tudi polje.

Definicija 2.2. Komutativen kolobar brez deliteljev niča se imenuje cel kolobar.

Vemo že, da je vsako polje hkrati tudi cel kolobar (med končnimi kolobarji drugih celih ni), a ta trditev ne velja v nasprotno smer (primer je kar kolobar celih števil $\mathbb{Z}$).

Lema 2.9. *Končen cel kolobar je polje.*

Dokaz. Naj bo K končen cel kolobar in a njegov poljuben neničeln element. Definiramo preslikavo $f : K \to K$ s predpisom $f(x) = ax$. Ker K nima deliteljev niča, velja

$$\begin{aligned} f(x) = f(y) &\Rightarrow ax = ay \\ &\Rightarrow a(x - y) = 0 \\ &\Rightarrow x = y \end{aligned}$$

in f je injektivna. Ker je K končna množica, je f tudi surjektivna in zato je $1 \in K$ v njeni zalogi vrednosti, torej obstaja tak $b \in K$, da je $f(b) = 1$. To pa pomeni, da obstaja inverz od a. □

Trditev 2.10. *Kolobar $\mathbb{Z}_p$ je polje natanko tedaj, ko je p praštevilo.*

Dokaz. Če p ni praštevilo, ima $\mathbb{Z}_p$ delitelje niča in torej ni polje. Naj bo p torej praštevilo. Z_p je končen komutativen kolobar, zato je po prejšnji lemi dovolj pokazati, da nima deliteljev niča. Predpostavimo, da je $[a] \cdot [b] = [0]$. Po definiciji operacije množenja je $[ab] = [0]$ oziroma $p|ab$. Iz evklidove leme pa sledi $p \mid a$ ali $p \mid b$, torej je bodisi $[a] = [0]$ bodisi $[b] = [0]$. □

Izkaže se calo, da v prejšnji lemi za predpostavko ni potrebno vzeti komutativnosti kolobarja. Wedderburnov izrek pravi, da so vsi končni obsegi komutativni. S prejšnjo trditvijo pa lahko seznam doslej znanih polj dopolnimo z bistveno drugačnimi primeri, in sicer končnimi polji $\mathbb{Z}_p$.

2.3 Obseg kvaternionov

Ali lahko vektorski prostor $\mathbb{R}^3$ s kakšnim množenjem postane obseg? Denimo, da tako množenje xy obstaja. Naj bo $a \in \mathbb{R}^3$ poljuben neničeln element $\mathbb{R}^3$ in vpeljemo linearno preslikavo $A : \mathbb{R}^3 \to \mathbb{R}^3$ s predpisom $Ax = ax$. Za to preslikavo gotovo obstaja vsaj ena realna lastna vrednost λ. Potem obstaja tudi neničelni vektor $x \in \mathbb{R}^3$, da je $Ax = \lambda x$. Od tod pa sledi $ax = \lambda x$ in posledično $(a - \lambda \cdot 1)x = 0$. Tako smo dobili $a = \lambda \cdot 1$, kar pa je protislovje, saj je bil a poljuben. Torej $\mathbb{R}^3$ ne more postati obseg (in podobno velja tudi za $\mathbb{R}^5$, $\mathbb{R}^7, \dots$)

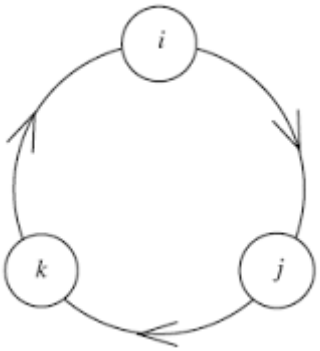
Naj bo $\mathbb{H}$ 4-razsežen realen vektorski prostor z bazo $1, i, j, k$. Elementi v $\mathbb{H}$ so torej oblike $\alpha_0 + \alpha_1 i + \alpha_2 j + \alpha_3 k$, kjer so $\alpha_0, \alpha_1, \alpha_2, \alpha_3$ realna števila. Pri tem je 1 enota za množenje, množenje preostalih elementov pa je enolično določeno z množenjem baznih vektorjev. Torej je dovolj, da definiramo množenje teh s samimi seboj:

$$\begin{aligned} i^1 = j^2 = k^2 &= -1, \\ ij &= -ji = k, \\ jk &= -kj = i, \\ ki &= -ik = j. \end{aligned}$$

Trditev 2.11. *Z vpeljanim množenjem postane $\mathbb{H}$ realna algebra.*

Dokaz. Dokaz te trditve je rutinski. □

Trditev 2.12. *$\mathbb{H}$ je obseg.*



Slika 1: Diagram množenja kvaternionov

Dokaz. Vzemimo poljuben $0 \neq h \in \mathbb{H}$, kjer je $h = \alpha_0 + \alpha_1 i + \alpha_2 j + \alpha_3 k$. Vpeljimo konjugiran element $\overline{h} = \alpha_0 - \alpha_1 i - \alpha_2 j - \alpha_3 k$. Tedaj je $h\overline{h} = \overline{h}h = \alpha_0^2 + \alpha_1^2 + \alpha_2^2 + \alpha_3^2 > 0$. Sedaj pa lahko definiramo inverz kot $h^{-1} = \frac{1}{h\overline{h}}\overline{h}$. □

Elemente $\mathbb{H}$ imenujemo kvaternioni. $\mathbb{H}$ je nekomutativen obseg. Izkaže se, da lahko v prostoru $\mathbb{R} \times \mathbb{R}^3$ vpeljemo definicijo množenja, ki je ekvivalentna množenju v $\mathbb{H}$:

$$(\alpha_0, \vec{u}) \cdot (\beta_0, \vec{v}) = (\alpha_0\beta_0 - \vec{u} \cdot \vec{v}, \alpha_0\vec{v} + \beta_0\vec{u} + \vec{u} \times \vec{u}).$$

Definirajmo grupo za množenje $Q = \{\pm 1, \pm i, \pm j, \pm k\}$. To je kvaternionska grupa, ki je z osmimi elementi druga najmanjša nekomutativna grupa za S_3 (izkazalo pa se bo, da ni edina nekomutativna grupa z 8 elementi).

Čeprav kvaternione ne obravnavamo kot števila, je množica $\mathbb{H}$ v nekem smislu naravni naslednik številskih množic $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$. Na to namiguje dejstvo, da je $\mathbb{H}$ obseg. Izkaže se, da so $\mathbb{R}$, $\mathbb{C}$ in $\mathbb{H}$ edine končnorazsežne realne algebre, ki so obsegi. Njihove dimenzije so 1, 2 in 4. Če bi zaporedje nadaljevali, bi dobili množico oktonionov, ki ima veliko lepih lastnosti, vendar a v njej množenje ni več asociativno.

2.4 Matrični kolobarji in linearne grupe

Naj bo n poljubno naravno število in K poljuben (lahko celo nekomutativen) kolobar. Potem lahko definiramo $M_n(K)$, t.j. množico $n \times n$ matrik z elementi iz K. Potem je $M_n(K)$ kolobar za običajni operaciji z matrikami.

Matrika (a_{ij}) se imenuje diagonalna matrika, če je $a_{ij} = 0$ za vse $i \neq j$. Če je $a_{ij} \neq 0$ za vse $i > j$, potem matriki (a_{ij}) pravimo zgoraj trikotna matrika. Če so hkrati tudi njeni diagonalci ničelni, je to strogo zgornje trikotna matrika. Podobno vpeljemo (strogo) spodnje trikotne matrike.

Element e kolobarja je idempotent, če je $e^2 = e$. V tem primeru je tudi $1 - e$ idempotent. Očitna primera idempotentov v kolobarju sta 0 in 1, ki pa sta tudi edina v kolobarjih brez deliteljev niča. Primer idempotenta v kolobarju $M_n(K)$ je na primer vsaka diagonalna matrika, ki ima na diagonali zgolj ničle in enice.

Element a iz kolobarja je nilpotent, če je $a^n = 0$ za nek $n \in \mathbb{N}$. Očitno je v kolobarjih brez deliteljev niča edini nilpotent kar ničla sama. Primer nilpotentnega elementa v $M_n(K)$ je vsaka strogo zgoraj (ali spodaj) trikotna matrika. Opazimo, da lahko v $M_n(\mathbb{R})$ vsako Jordanovo formo zapišemo kot linearno kombinacijo nilpotenov in idempotentov. Če je K algebra nad poljem F, potem je tudi $M_n(K)$ algebra nad F za množenje s skalarji, definirano kot $\lambda(a_{ij}) = (\lambda a_{ij})$. Take primere smo že spoznali: $M_n(\mathbb{R})$ je realna algebra, $M_n(\mathbb{C})$ pa kompleksna.

Sedaj si oglejmo matrične grupe, katerih elementi so matrike nad poljem, operacija pa je množenje.

Množica vseh $n \times n$ matrik nad poljem F ni grupa, temveč le monoid. Spomnimo se, da je množica vseh obrnljivih elementov monoida S tvori grupo S^*. Torej je množica $\mathrm{GL}_n(F) = M_n(F)^*$ grupa, imenovana splošna linearna grupa. Za $n > 1$ je ta grupa nekomutativna.

Sedaj vpeljimo pojem determinante matrike za poljubno polje F. Determinanto matrike $A = (a_{ij}) \in M_n(F)$ vpeljemo kot

$$\det(A) = \sum_{\sigma \in S_n} \mathrm{sgn}(\sigma) a_{1\sigma(1)} \dots a_{n\sigma(n)},$$

kjer S_n označuje množico vseh permutacij, $\mathrm{sgn}(\sigma)$ pa predznak permutacije σ. Za tsplošno vpeljano determinanto veljajo naslednje lastnosti:

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

Opomba. Prvi dve lastnosti veljata že, če polje F nadomestimo s komutativnim kolobarjem K. Previdni pa moramo biti pri tretji točki: tam velja ekvivalenca takrat, ko je $\det(A)$ obrnljiv element v K.

Sedaj lahko splošno linearno grupo karakteriziramo kot $\mathrm{GL}_n(F) = \{A \in M_n(F) \mid \det(A) \neq 0\}$. Iz zgoraj navedenih lastnosti sledi, da je tudi množica $\mathrm{SL}_n(F) = \{A \in M_n(F) \mid \det(A) = 1\}$ grupa za množenje matrik. Pravimo je posebna linearna grupa. Podobno sledi tudi za naslednje množice:

- $O_n(F) = \{A \in M_n(F) \mid AA^\top = I\}$ – ortogonalna grupa.
- $SO_n(F) = \{A \in O_n(F) \mid \det(A) = 1\}$ – posebna ortogonalna grupa.
- $U_n = \{A \in M_n(\mathbb{C}) \mid AA^* = I\}$ – unitarna grupa.
- $SU_n = \{A \in U_n \mid \det(A) = 1\}$ – posebna unitarna grupa.

Zgled 2.2. *Omenimo še en poseben primer podgrupe* $\mathrm{GL}_n(F)$*. Naj bo*

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

Potem je množica $\mathrm{Sp}_{2n}(F) = \{A \in M_{2n}(F) \mid A^\top JA = J\}$ *simplektična grupa.*

2.5 Kolobarji funkcij

Naj bo X neprazna množica. Potem množica $\{f : X \to \mathbb{R}\}$ postane kolobar za operaciji $(f+g)(x) = f(x) + g(x)$ in $(fg)(x) = f(x) \cdot g(x)$ (hkrati pa tudi algebra za $(\lambda f)(x) = \lambda \cdot f(x)$). Podobno je tudi $C(X) = \{f : X \to \mathbb{R} \mid f \text{ zvezna}\}$ kolobar in algebra (množica X je na primer $\mathbb{R}$ ali nek poljuben interval). Enako velja za $C^1(X), C^2(X), \dots, C^\infty(X)$.

Zgled 2.3. *Algebro realnih polinomov lahko opišemo kot podalgebro algebre vseh funkcij iz* $\mathbb{R}$ *v* $\mathbb{R}$*, generirano z identično funkcijo* $\mathrm{id}_\mathbb{R}$*. Seveda pa tukaj besede algebra ne moremo zamenjati s kolobarjem.*

Sedaj vzemimo $X = \mathbb{N}$. Potem dobimo algebro realnih zaporedij $(a_1, a_2, \dots)$. Definiciji seštevanja in množenja sta običajni definiciji teh operacij na zaporedjih:

$$(a_1, a_2, \dots) + (b_1, b_2, \dots) = (a_1 + b_1, a_2 + b_2, \dots)$$
$$(a_1, a_2, \dots) \cdot (b_1, b_2, \dots) = (a_1 b_1, a_2 b_2, \dots).$$

Tudi množica konvergentnih zaporedij c in množica omejenih zaporedij l^∞ sta algebri. Če pa je množica X končna oziroma velja $|X| = n$, potem lahko funkcijo $f : X \to \mathbb{R}$ predstavimo kar z n-terico vrednosti, ki jih zavzame. Tedaj lahko $K = \{f : X \to \mathbb{R}\}$ identificiramo z $\mathbb{R}$.

2.6 Kolobarji polinomov

Naj bo K poljuben kolobar. Polinom s koeficienti iz K je formalna vsota $f(X) = a_0 + a_1X + \cdots + a_nX^n$, kjer so a_i elementi nekega kolobarja K. Imenujemo jih koeficienti $f(X)$, a_0 in a_n pa posebej prosti člen in vodilni koeficient. Formalna definicija polinoma je zaporedje oblike

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

oziroma vsota $\sum_{k\geq 0} a_kX^k$, kjer je $a_k = 0$ za vsa števila k, večja od nekega števila $m \in \mathbb{N}$. Množica vseh polinomov $K[X]$ s koeficienti iz kolobarja K postane kolobar, če vpeljemo operaciji

$$\sum_{k\geq 0} a_kX^k + \sum_{k\geq 0} b_kX^k = \sum_{k\geq 0}(a_k + b_k)X^k$$
$$\left(\sum_{k\geq 0} a_kX^k\right) \cdot \left(\sum_{k\geq 0} b_kX^k\right) = \sum_{k\geq 0} c_kX^k,$$

kjer je $c_k = a_0b_k + a_1b_{k-1} + \cdots + a_kb_0$.

Opomba. Omenimo še kolobar formalnih potenčnih vrst $K[[X]]$, kjer koeficienti a_k niso nujno ničelni od nekod dalje. Operaciji seštevanja in množenja sta definirani enako kot v $K[X]$.

Stopnja polinoma $0 \neq f(X) = a_0 + a_1X + \cdots + a_nX^n$ je enaka 0, če $a_n \neq 0$. Tedaj pišemo $\mathrm{st}(f(X)) = n$.

Trditev 2.13. *Če K nima deliteljev niča, za vsaka neničelna polinoma $f(X), g(X) \in K(X)$ velja* $\mathrm{st}(f(X)g(X)) = \mathrm{st}(f(X)) + \mathrm{st}(g(X))$.

Naj bo sedaj kolobar K komutativen. Vrednost polinoma $f(X) = a_0 + a_1X + \cdots + a_nX^n$ v elementu $x \in K$ definiramo kot $f(x) = a_0 + a_1x + \cdots + a_nx^n$. Vsakemu polinomu $f(X) \in K[X]$ priredimo polinomsko funkcijo $x \mapsto f(x)$. To je preslikava iz K v K, ki jo določa polinom $f(X)$. Vendar pa ne velja obratno, saj polinom ni enolično določen s svojo polinomsko funkcijo.

Zgled 2.4. *Polinoma 0 in $X + X^2$ imata kot elementa $\mathbb{Z}_2[X]$ isto polinomsko funkcijo in sicer ničelno funkcijo $x \mapsto 0$ za vsak $x \in \mathbb{Z}_2$.*

Omenimo še polinome več spremenljivk. Ti so vsota monomov, pomnoženih s koeficienti iz kolobarja K. Stopnja takega polinoma je najvišja stopnja monoma, ki nastopa v njem. Operaciji seštevanja in množenja definiramo tako kot prej.

Povsem formalna definicija polinomov več spremenljivk je naslednja: kolobar polinomov v dveh spremenljivkah nad kolobarjem K definiramo kot $K[X, Y] = (K[Y])[Y]$, njegovi elementi pa so polinomi $\sum_{j\geq 0}\left(\sum_{i\geq 0} a_{ij}X^i\right)Y^j$, kjer je le končno mnogo elementov a_{ij} različnih od 0, spremenljivki X in Y pa komutirata. Induktivno lahko uvedemo splošno definicijo polinoma n spremenljivk:

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

2.7 Simetrične grupe

Grupo vseh permutacij množice $\{1, 2, \ldots, n\}$ označujemo s S_n in ji pravimo simetrična grupa. Operacija v tej grupi je komponiranje, torej je $\sigma\pi$ produkt permutacij σ in π. Enota v S_n je identična preslikava, ki jo bomo označevali kar z 1. Permutacijo $\sigma \in S_n$ označimo kot

$$\sigma = \begin{pmatrix} 1 & 2 & \ldots & n \\ i_1 & i_2 & \ldots & i_n \end{pmatrix}.$$

Vseh permutacij množice n elementov je $n!$, zato velja $|S_n| = n!$. Transpozicija je permutacija, ki med seboj zamenja elementa i in j iz $\mathbb{N}_n$, vse druge elemente pa preslika vase. Transpozicija je očitno sama sebi inverz. Hitro preverimo, da permutacije med seboj ne komutirajo za $n \geq 3$.

Trditev 2.14. *Vsaka permutacija $\sigma \in S_n$ se da zapisati kot produkt transpozicij.*

Iz te trditve sledi, da množica vseh transpozicij generira grupo S_n, vendar pa zapis permutacije kot produkt transpozicij ni enoličen.

Trditev 2.15. *Če permutacijo $\sigma \in S_n$ lahko zapišemo kot produkt sodega (iz. lihega) števila transpozicij, potem ima tudi vsak drug zapis σ v obliki produkta transpozicij sodo oziroma liho število faktorjev.*

Skica dokaza. Naj bo $f(X_1, \ldots, X_n)$ polinom v n spremenljivkah nad nekim kolobarjem. Za neko permutacijo $\sigma \in S_n$ vpeljemo polinom $(\sigma f)(X_1, \ldots, X_n) = f(X_{\sigma(1)}, \ldots, X_{\sigma(n)})$. Za neko drugo permutacijo $\pi \in S_n$ dobimo $(\pi(\sigma f))(X_1, \ldots, X_n) = (\sigma f)(X_{\pi(1)}, \ldots, X_{\pi(n)})$. Hitro dobimo enakost $(\pi(\sigma f))(X_1, \ldots, X_n) = ((\pi\sigma)f)(X_{\pi(1)}, \ldots, X_{\pi(n)})$. Najti moramo tak polinom $f(X_1, \ldots, X_n) \in \mathbb{Z}[X_1, \ldots, X_n]$, da za vsako transpozicijo τ velja $(\tau f)(X_1, \ldots, X_n) = -f(X_1, \ldots, X_n)$ in od tod sledi $((\tau_1 \ldots \tau_k)f)(X_1, \ldots, X_n) = (-1)^k f(X_1, \ldots, X_n)$ za poljubne transpozicije $\sigma_1, \ldots, \sigma_k$. Iskani polinom pa je $f(X_1, \ldots, X_n) = \prod_{i<j}(X_i - X_j)$. □

Soda permutacija je produkt sodega števila transpozicij, liha pa lihega števila transpozicij. Predznak permutacije $\operatorname{sgn}(\sigma)$ je 1, če je σ soda in -1, če je σ liha. Potem velja $\operatorname{sgn}(\sigma\pi) = \operatorname{sgn}(\sigma)\operatorname{sgn}(\sigma)$ in $\operatorname{sgn}(\sigma^{-1}) = \operatorname{sgn}(\tau)^{-1}$ za vse $\sigma, \pi \in S_n$. Opazimo, da je množica sodih permutacij zaprta za množenje in inverze, zato je podgrupa S_n. Imenujemo jo alternirajoča grupa A_n in velja $|A_n| = \frac{n!}{2}$.

Pri predmetu algebra 1 smo omenili drugačne gradnike permutacij, to so cikli. Cikel dolžine k imenujemo $k-$cikel in ga označimo kot $\begin{pmatrix} i_1 & i_2 & \ldots & i_k \end{pmatrix}$. Ciklom, med katerimi nobena dva ne vsebujeta skupnega elementa, imenujemo disjunktni cikli.

Trditev 2.16. *Vsaka permutacija $\sigma \in S_n$ se da zapisati kot produkt disjunktnih ciklov.*

Tak zapis je enoličen do vrstnega reda ciklov natančno (disjunktni cikli med seboj komutirajo).

2.8 Diedrske grupe

Denimo, da imamo kvadrat v ravnini. Njegova oglišča označimo z 1, 2, 3 in 4 kot na sliki. Kvadrat v prostoru poljubno premikamo in vrtimo in ga nato postavimo na prvotno mesto. Zato oglišča morda zamenjajo mesto in taki transformaciji pravimo simetrija. Nanjo lahko gledamo na permutacijo oglišč. Ker je tako produkt dveh simetrij kot tudi inverz simetrije spet simetrija, je množica simetrij podgrupa simetrične grupe S_4. Pravimo ji diedrska grupa reda 8.

Označimo vrtenje za 90° v levo kot r in zrcaljenje preko vodoravne osi kot z. Potem ima ta grupa elemente

$$D_8 = \{1, r, r^2, r^3, z, rz, r^2z, r^3z\}.$$

Elementa r in z očitno generirata grupo D_8. Ker je $rz \neq zr$, grupa ni Abelova. Veljajo pa še zveze $r^4 = 1$, $z^2 = 1$ in $(rz)^2 = 1$.

Na enak način lahko obravnavamo simetrije pravilnega n-kotnika za $n \geq 3$. Tako grupo označimo z D_{2n} in je generirana z rotacijo r (za kot $\frac{360^\circ}{n}$) in zrcaljenjem z. Pri tem ponovno velja $r^n = 1$, $z^2 = 1$ in $(rz)^2 = 1$, od koder sledi $zr^i = r^{-i}z$. Ta grupa ima elemente

$$D_{2n} = \{1, r, \ldots, r^{n-1}, z, rz, \ldots, r^{n-1}z\}.$$

Lahko pa definiramo diedrsko grupo tudi za $n = 2$ in $n = 1$. V prvem primeru definiramo D_4 kot grupo simetrij pravokotnika, ki ni kvadrat. Sestavljajo jo elementi 1, r, z in rz, kjer je $zr = rz$, zato je ta grupa Abelova. Diedrsko grupo D_2 pa sestavljata elementa 1 in r, kjer je $r^2 = 1$.

3 Homomorfizmi

3.1 Izomorfnost grup in ciklične grupe

Zgled 3.1. *Končno grupo lahko predstavimo s Cayleyevo tabelo. Če zapišemo Caylejevi tabeli za* $(\mathbb{Z}_4, +)$ *in grupo* $\{1, -1, i, -i\}$ *za seštevanje, ugotovimo, da sta zgradbi obeh tabel enaki. S stališča teorije grup se ti dve grupi torej sploh ne razlikujeta.*

Definicija 3.1. Naj bosta G in G' grupi. Bijektivna preslikava $\varphi : G \to G'$ je izomorfizem grup, če velja $\varphi(xy) = \varphi(x)\varphi(y)$. Grupi G in G' sta si izomorfni, če obstaja izomorfizem iz G v G'. Takrat pišemo $G \cong G'$.

Trditev 3.1. *Če je* φ *izomorfizem iz* G *v* G'*, je* φ^{-1} *izomorfizem iz* G' *v* G*.*

Zgled 3.2. *Oglejmo si nekaj osnovnih primerov izomorfizmov.*

- *Za vsako grupo* G *velja* $G \cong G$*. Najenostavnejši primer takega izomorfizma je identična preslikava* id_G*.*
- *Vsaka netrivialna podgrupa grupe* $(\mathbb{Z}, +)$ *ji je izomorfna: za* $n \geq 1$ *je* $(n\mathbb{Z}, +)$ *izomorfizem preslikava* $\varphi : \ x \mapsto nx$*.*
- *Ker velja* $e^{xy} = e^x e^y$*, sta grupi* $(\mathbb{R}, +)$ *in* $(\mathbb{R}^+, \cdot)$ *izomorfni.*

Definicija 3.2. Grupa G je ciklična, če je generirana z enim samim elementom: $G = \langle a \rangle = \{a^k \mid k \in \mathbb{Z}\}$.

Zgled 3.3. *Primeri cikličnih grup so* $U_4 = \langle i \rangle$, $\mathbb{Z}_4 = \langle 1 \rangle$, $\mathbb{Z}_n$ *in* $\mathbb{Z}$*.*

Izrek 3.2.

Vsaka ciklična grupa je izomorfna bodisi $\mathbb{Z}$ *bodisi* $\mathbb{Z}_n$ *za nek* $n \geq 1$*.*

Dokaz. Naj bo $G = \langle a \rangle = \{a^k \mid k \in \mathbb{Z}\}$. Če so vsi elementi a^k različni, potem iz $a^k = a^l$ sledi $k = l$. To pomeni, da je preslikava $\varphi : \mathbb{Z} \to G$ s predpisom $\varphi(k) = a^k$ injektivna. Seveda je φ tudi surjektivna in hitro se prepričamo, da je res izomorfizem.
Obravnavajmo drugo možnost, ko obstajata taki celi števili $k < l$, da je $a^k = a^l$. Torej je $a^{l-k} = 1$ in definirajmo n kot najmanjše naravno število, za katerega je $a^n = 1$. Trdimo, da je $|G| = n$ in $G = \{1, a, \ldots, a^{n-1}\}$. Če je $0 \leq p < q < n$, sta elementa a^p in a^q res različna, saj bi sicer za naravno število $q - p < n$ veljalo $a^{q-p} = 1$. Torej je $|G| \geq n$. Vzemimo sedaj poljuben element $a^k \in G$. Po osnovnem izreku o deljenju obstajata taki celi števili q, r, da je $k = qn + r$ in $0 < r \leq n$. Zato je $a^k = a^r$, s čimer smo dokazali našo trditev. Sedaj je očitno, da sta grupi G in $\mathbb{Z}_n$ izomorfni. □

Ker imata izomorfni grupi isti red, je vsaka končna ciklična grupa reda n izomorfna grupi $(\mathbb{Z}_n, +)$, vsaka neskončna ciklična grupa pa grupi $(\mathbb{Z}, +)$.

Definicija 3.3. Element $a \in G$ ima končen red, če je $a^n = 1$ za nek $n \in \mathbb{N}$. Če je n najmanjše naravno število s to lastnostjo, ima a red natanko n. To je ekvivalentno dejstvu $|\langle a \rangle| = n$. Če a nima končen red, ima neskončen red.

Zgled 3.4. *V grupi* $(\mathbb{Z}_4, +)$ *ima element* 0 *red* 1*, element* 2 *red* 2*, elementa* 1 *in* 3 *pa red* 4*. Diedrska grupa* D_4 *ima prav tako* 4 *elemente, vendar imajo razen enote vsi red enak* 2*. Ker izomorfizem ohranja red vsakega elementa, grupi* $\mathbb{Z}_4$ *in* D_4 *nista izomorfni (grupa* D_4 *pa je izomorfna* $(\mathbb{Z}_2 \oplus \mathbb{Z}_2, +)$*).*

3.2 Izomorfnost vektorskih prostorov

Vektorska prostora V in V' sta si izomorfna, če obstaja bijektivna linearna preslikava $\varphi : V \to V'$. Tedaj je φ izomorfizem vektorskih prostorov.

Trditev 3.3. *Če sta* V *in* V' *končnorazsežna, sta si izomorfna natanko tedaj, ko velja* $\dim_F V = \dim_F V'$*.*

Posledica 3.4. *Vsak netrivialen končnorazsežen vektorski prostor nad poljem* F *je izomorfen prostoru* F^n*.*

3.3 Pojem homomorfizma

Definicija 3.4. 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 vektorskih prostorov, če sta A in A' vektorska prostora nad F in je $\varphi(x+y) = \varphi(x) + \varphi(y)$ in $\varphi(\lambda x) = \lambda\varphi(x)$ za vse $x, y \in A$, $\lambda \in F$.
- homomorfizem kolobarjev, če sta A in A' kolobarja in je $\phi(1) = 1$, $\varphi(x + y) = \varphi(x) + \varphi(y)$ in $\varphi(xy) = \varphi(x)\varphi(y)$ za vse $x, y \in A$.
- homomorfizem algeber, če sta A in A' algebri nad F in je $\phi(1) = 1$, $\varphi(x + y) = \varphi(x) + \varphi(y)$, $\varphi(\lambda x) = \lambda\varphi(x)$ in $\varphi(xy) = \varphi(x)\varphi(y)$ za vse $x, y \in A$, $\lambda \in F$.

Bijektivnemu homomorfizmu pravimo izomorfizem, surjektivnemu epimorfizem, injektivnemu pa monomorfizem ali vložitev. Homomorfizmu iz A v A pravimo endomorfizem, bijektivnemu endomorfizmu pa avtomorfizem.

Opomba. Če sta A in A' aditivni grupi, potem je $\varphi : A \to A'$ homomorfizem in $\varphi(x+y) = \varphi(x)+\varphi(y)$. Rečemo tudi, da je ϕ aditivna preslikava.

Opomba. Za homomorfizme kolobarjev in algeber smo zahtevali, da slikajo enoto 1 kolobarja (algebre) A v enoto 1 kolobarja (algebre) A'. Tako na primer preslikava $\varphi : \mathbb{R} \to M_2(\mathbb{R})$ s predpisom

$$\varphi(x) = \begin{bmatrix} x & 0 \\ 0 & 0 \end{bmatrix}$$

ni homomorfizem, čeprav ohranja tako vsoto kot produkt.

Opomba. Izraz vložitev za injektiven homomorfizem $\varphi : A \to A'$ uporabimo takrat, ko A identificiramo z zalogo vrednosti φ znotraj A'. Tako lahko kolobar K vložimo v $K[X]$ s predpisom $a \mapsto a + 0 \cdot X + 0 \cdot X^2 + \ldots$ Podobno lahko polje realnih števil vložimo v polje kompleksnih števil s predpisom $x \mapsto x + i0$.

Trditev 3.5. *Kompozitum homomorfizmov je homomorfizem.*

Trditev 3.6. *Inverzna preslikava izomorfizma je izomorfizem.*

Očitno sledi, da je $\cong$ ekvivalenčna relacija.

Trditev 3.7. *Množica vseh avtomorfizmov grupe (kolobarja, vektorskega prostora, algebre)* A *je grupa za komponiranje.*

Trditev 3.8. *Če je* $\varphi : G \to G'$ *homomorfizem grup, je* $\varphi(1) = 1$ *in* $\varphi(x^{-1}) = \varphi(x)^{-1}$*.*

Dokaz. Po definiciji izomorfizma velja $\varphi(1) = \varphi(1)^2$ in po pravilu krajšanja sledi $1 = \varphi(1)$. Druga točka sledi direktno iz te ugotovitve. □

Opomba. To lahko posplošimo na formulo $\varphi(x^n) = \varphi(x)^n$ za vsa cela števila n (oziroma $\varphi(nx) = n\varphi(x)$ v primeru aditivnih grup).

Trditev 3.9. *Če je $\varphi : K \to K'$ homomorfizem kolobarjev in je x obrnljiv, je tudi $\varphi(x^{-1}) = \varphi(x)^{-1}$.*

Dokaz. Po predpostavki je $\varphi(1) = 1$ in hitro pokažemo, da je $\varphi(x)\varphi(x^{-1}) = \varphi(x^{-1})\varphi(x) = 1$. □

Definicija 3.5. Zalogi vrednosti homomorfizma $\varphi : A \to A'$ pravimo slika homomorfizma in jo označujemo kot $\operatorname{im}\varphi = \{\varphi(x) \mid x \in A\}$.

Trditev 3.10. *Slika homomorfizma grup (oz. kolobarjev, vektorskih prostorov algeber) je podgrupa (oz. podkolobar, podprostor, podalgebra).*

Dokaz. Naj bo $\varphi : G \to G'$ homomorfizem grup. Potem je $\operatorname{im}\varphi$ zaprta za množenje zaradi $\varphi(xy) = \varphi(x)\varphi(y)$ in zaprta za inverze zaradi $\varphi(x)^{-1} = \varphi(x^{-1})$. □

Definicija 3.6. Jedro homomorfizma grup $\varphi : G \to G'$ je $\ker\varphi = \{x \in G \mid \varphi(x) = 1\}$. Če gre za aditivno grupo, pa se ta definicija glasi $\ker\varphi = \{x \in G \mid \varphi(x) = 0\}$. Jedro homomorfizma koloberjev, vektorskih prostorov in algeber definiramo na slednji način.

Trditev 3.11. *Homomorfizem φ je injektiven natanko tedaj, ko je $\ker\varphi$ trivialen.*

Dokaz. Naj bosta G, G' grupi. Ker je $\varphi(1) = 1$, je $1 \in \ker\varphi$. Če je φ injektiven, je $\ker\varphi = \{1\}$. Dokažimo še obrat. Naj bo $\ker\varphi = \{1\}$. Potem je

$$\begin{aligned}\varphi(x) = \varphi(y) &\Rightarrow \varphi(x)\varphi(y)^{-1} = 1\\ &\Rightarrow \varphi(xy^{-1}) = 1\\ &\Rightarrow x = y\end{aligned}$$

□

Izomorfizmi imajo trivialno jedro in največjo možno sliko. Njihovo nasprotje so trivialni homomorfizmi grup, ki vse elemente prve grupe preslika v enoto druge grupe. Na podoben način lahko trivialne homomorfizme definiramo za kolobarje, vektorske prostore in algebre.

3.4 Primeri homomorfizmov

Navedimo nekaj zgledov homomorfizmov grup.

Zgled 3.5. *Naj bo G Abelova grupa in $n \in \mathbb{Z}$. Potem je $\varphi(x) = x^n$ endomorfizem, saj velja*

$$\varphi(xy) = (xy)^n \overset{\text{G Abelova}}{=} x^n y^n = \phi(x)\phi(y).$$

Za $n = 1$ je to seveda avtomorfizem. V Abelovi grupi imamo predpis $\varphi(x) = nx$.

Zgled 3.6. *Preslikava $z \mapsto |z|$ je epimorfizem iz grupe $\mathbb{C}^*$ v $\mathbb{R}^+$. Operacija v obeh grupah je seveda množenje. Jedro tega epimorfizma je enotska krožnica $\mathbb{T} = \{z \in \mathbb{C} \mid |z| = 1\}$.*

Zgled 3.7. *Preslikava $\varphi(x) = e^{ix}$ je homomorfizem iz $\mathbb{R}$ v $\mathbb{T}$.*

Zgled 3.8. *Iz formule $\operatorname{sgn}(\pi\sigma) = \operatorname{sgn}(\pi)\operatorname{sgn}(\sigma)$ direktno sledi, da je preslikava $\sigma \mapsto \operatorname{sgn}(\sigma)$ epimorfizem iz simetrične grupe S_n v grupo $\{1, -1\}$ z množenjem. Jedro φ je alternirajoča grupa A_n.*

Zgled 3.9. *Preslikava $A \mapsto \det A$ je epimorfizem iz splošne linearne grupe $\mathrm{GL}_n(F)$ v grupo $(F^*, \cdot)$, saj je determinanta matrike multiplikativna. Jedro tege homomorfizma je SL_n.*

Zgled 3.10. *Naj bo G poljubna grupa in $a \in G$. Potem je $\varphi_a : G \to G$ s predpisom $\varphi_a(x) = axa^{-1}$ bijektivni endomorfizem oziroma avtomorfizem. Rečemo mu notranji avtomorfizem. Ker je $\varphi_a\varphi_b = \varphi_{ab}$ in $\varphi_{a^{-1}} = \varphi_a^{-1}$, je množica vseh notranjih avtomorfizmov $\mathrm{Inn}(G)$ podgrupa grupe vseh avtomorfizmov $\mathrm{Aut}(G)$.*

Sedaj si oglejmo še primere homomorfizmov kolobarjev in algeber.

Zgled 3.11. *Naj bo K kolobar. Vsak $a \in K$, ki je obrnljiv, porodi notranji avtomorfizem $\varphi_a(x) = axa^{-1}$. Enako velja tudi za algebre.*

Zgled 3.12. *Za naravno število n je preslikava $\varphi : \mathbb{Z} \to \mathbb{Z}_n$ s predpisom $\phi(a) = [a]$ epimorfizem kolobarjev.*

Zgled 3.13. *Preslikava $\varphi : K[X] \to K$, ki polinomu $f(X)$ priredi njegov konstantni člen, je epimorfizem. To preslikavo lahko opišemo tudi kot preslikavo, ki vsakemu polinomu $f(X)$ priredi element $f(0)$. Element 0 lahko tu zamenjamo s poljubnim elementom $x \in K$ in dobimo epimorfizem $f(X) \mapsto f(x)$ iz kolobarja $K[X]$ v K.*

Zgled 3.14. *Podoben primer kot v prejšnjem zgledu lahko ponovimo na kolobarju $C[0, 1]$. Za poljubno število $x \in [0, 1]$ je $f \mapsto f(x)$ epimorfizem iz kolobarja $C[0, 1]$ v $\mathbb{R}$. Izkaže se, da je tovrstna preslikava celo homomorfizem algeber.*

Zgled 3.15. *Naj bo V vektorski prostor nad F. Z $\mathrm{End}_F(V)$ označimo množico vseh endomorfizmov prostora V. Pri algebri 1 smo dokazali, da je tovrstna množica algebra nad F in je izomorfna $M_2(F)$.*

Zgled 3.16. *Oglejmo si štiri primere podkolobarjev kolobarja realnih oz. kompleksnih matrik*

velikosti 2×2.

$$K_1 = \left\{ \begin{bmatrix} x & 0 \\ 0 & x \end{bmatrix} \mid x \in \mathbb{R} \right\} \cong \mathbb{R},$$
$$K_2 = \left\{ \begin{bmatrix} x & 0 \\ 0 & y \end{bmatrix} \mid x, y \in \mathbb{R} \right\} \cong \mathbb{R}^2,$$
$$K_3 = \left\{ \begin{bmatrix} x & y \\ -y & x \end{bmatrix} \mid x, y \in \mathbb{R} \right\} \cong \mathbb{C},$$
$$K_4 = \left\{ \begin{bmatrix} z & w \\ -\overline{w} & \overline{z} \end{bmatrix} \mid z, w \in \mathbb{C} \right\} \cong \mathbb{H}.$$

3.5 Cayleyev izrek in druge vložitve

Izrek 3.12 (Cayley)**.**

Vsako grupo lahko vložimo v neko simetrično grupo.

Dokaz. Za vsak element $a \in G$ definirajmo $l_a : G \to G$, kjer je $l_a(x) = ax$. Hitro lahko preverimo, da je ta funkcija bijektivna, torej $l_a \in \mathrm{Sim}(G)$. Sedaj definiramo preslikavo $\varphi : G \to \mathrm{Sim}(G)$ s predpisom $\varphi(a) = l_a$. Potem velja $\varphi(ab) = l_{ab} = l_a \cdot l_b = \varphi(a)\varphi(b)$. Preslikava φ je injektivna, saj je $\ker \varphi = \{\mathrm{id}_G\}$. Torej je φ injektiven homomorfizem oziroma vložitev. □

Izrek nam pove, da bi brez škode za splošnost grupo lahko definirali kot množico permutacij, ki je zaprta za množenje in inverze. Kot je razvidno iz dokaza, pa nam izrek pove še več: grupo G lahko vložimo v simetrično grupo $\mathrm{Sim}(G)$.

Posledica 3.13. *Vsako končno grupo G lahko vložimo v simetrično grupo S_n za neki $n \in \mathbb{N}$.*

Definicija 3.7. Grupa G deluje na množici X, če obstaja preslikava iz $G \times X$ v X, ki vskemu paru (a, x) priredi element $a \cdot x$, tako da velja:
- $(ab) \cdot x = a \cdot (b \cdot x)$ za vse $a, b \in G$ in vse $x \in X$.
- $1 \cdot x = x$ 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 $\varphi : G \to \mathrm{Sim}(X)$ kot $\varphi(a)(x) = a \cdot x$. Grupa G deluje na sama sebi z običajnim množenjem; prav to je delovanje, ki smo ga uporabili v dokazu Cayleyevega izreka.

Naj bo sedaj M aditivna grupa in označimo z $\mathrm{End}\,(M)$ množico vseh njenih endomorfizmov, torej vseh aditivnih preslikav iz M vase. Potem za $f, g \in \mathrm{End}\,(M)$ definiramo $f + g$ kot vsoto funkcij po točkah, fg pa kot kompozitum $f \circ g$. Za tako definirani operaciji je $\mathrm{End}\,(M)$ kolobar.

Izrek 3.14.

Vsak kolobar K lahko vložimo v kolobar endomorfizmov neke aditivne grupe.

Dokaz. Dokaz je podoben Cayleyevemu izreku, le da ima tokrat vlogo aditivne grupe kar kolobar K. Kot prej za $a \in K$ definiramo $l_a : K \to K$ kot $l_a(x) = ax$. Hitro preverimo, da je preslikava

$\varphi : K \to \mathrm{End}\,(K)$ s predpisom $\varphi(a) = l_a$ homomorfizem kolobarjev s trivialnim jedrom. □

Kot smo prej vpeljali pojem delovanja grupe na množici, lahko sedaj definiramo pojem modula M nad kolobarjem K.

Definicija 3.8. 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:

- $(a + b)m = am + bm$ za vse $a, b \in K$ in vse $m \in M$.
- $a(m + n) = am + an$ za vse $a \in K$ in vse $m, n \in M$.
- $(ab)m = a(bm)$ za vse $a, b \in K$ in vse $m \in M$.
- $1m = m$ za vse $m \in M$.

Podobno kot prej je pojem modula ekvivalenten pojmu homomorfizma iz kolobarja K v kolobar endomorfizmov aditivne grupe M. Natančneje se modulu, ki smo ga vpeljali, reče levi modul. Desnega definiramo analogno.

Izrek 3.15.

Vsako algebro A lahko vložimo v algebro endomorfizmov nekega vektorskega prostora.

Levi modul nad algebro A definiramo kot vektorski prostor M, v katerem se poleg zahtev (i)-(iv) 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 prejšnjem izreku za vektorski prostor seveda lahko izberemo kar A. Če je A končno-razsežna, lahko torej A vložimo v algebro endomorfizmov končno-razsežnega vektorskega prostora, ta pa je izomorfna matrični algebri $M_n(F)$.

Posledica 3.16. *Vsako končno-razsežno algebro lahko vložimo v matrično algebro $M_n(F)$ za neki $n \in \mathbb{N}$.*

Zgled 3.17. *Ali lahko končno-razsežna algebra A nad (denimo) $\mathbb{R}$ vsebuje taka elementa s in t, da je $st - ts = 1$? S prejšnjo posledico lahko ta problem pretvorimo v naslednje vprašanje: ali obstajata takšni matriki $S, T \in M_n(\mathbb{R})$, da je $ST - TS = I$? Odgovor je ne, saj je sled matrike komutativna.*

3.6 Vložitev celega kolobarja

Naj bo K poljuben cel kolobar.

Lema 3.17. *S predpisom $(a, b) \sim (a', b') \Leftrightarrow ab' = a'b$ je definirana ekvivalenčna relacija na množici $K \times (K \setminus \{0\})$.*

Vpeljimo oznako $\frac{a}{b}$ za ekvivalenčni razred elementa (a, b). Tu je a poljuben element iz K in b poljuben element $K \setminus \{0\}$. Takoj sledi, da je $\frac{a}{b} = \frac{a'}{b'} \Leftrightarrow ab' = a'b$.

Lema 3.18. *Za poljubne $a, a', c, c' \in K$ in $b, b', d, d' \in K \setminus \{0\}$ iz $\frac{a}{b} = \frac{a'}{b'}$ in $\frac{c}{d} = \frac{c'}{d'}$ sledi $\frac{ad+bc}{bd} = \frac{a'd'+b'c'}{b'd'}$ in $\frac{ac}{bd} = \frac{a'c'}{b'd'}$.*

Izrek 3.19.

Naj bo K cel kolobar. Če v množico vseh ekvivalenčnih razredov $F = \left\{ \frac{a}{b} \,\middle|\, a, b \in K,\ b \neq 0 \right\}$ vpeljemo seštevanje in množenje s predpisoma $\frac{a}{b} + \frac{b}{d} = \frac{ad+bc}{bd}$ in $\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$ postane F polje. Preslikava $\varphi : K \to F$, definirana z $\varphi(a) = \frac{a}{1}$

Dokaz. Po prejšnji lema sta operaciji seštevanja in množenja dobro definirani. To, da je F polje, dokazujemo po definiciji. Da je φ homomorfizem, sledi iz enakosti $\frac{a+b}{1} = \frac{a}{1} + \frac{b}{1}$ in $\frac{ab}{1} = \frac{a}{1} \cdot \frac{b}{1}$. Če je $\varphi(a) = 0$, je očitno $a = 0$, torej je φ res tudi vložitev. □

Definicija 3.9. Polje F iz prejšnjega izreka se imenuje polje ulomkov nekega kolobarja K.

Kolobar K obravnavamo kot podkolobar polja ulomkov F, pri čemer namesto $\frac{a}{1}$ pišemo kar a. Polje ulomkov celega kolobarja K je generirano z množico K.

Zgled 3.18. *Navedimo nekaj zgledov.*

1. *Če je K že samo polje, je $F = K$.*
2. *Polje racionalnih števil $\mathbb{Q}$ je polje ulomkov kolobarja $\mathbb{Z}$.*
3. *Kolobar polinomov več spremenljivk $F[X_1, \ldots, X_n]$ je cel kolobar in njegovemu polju ulomkov $F(X_1, \ldots, X_n)$ pravimo polje racionalnih funkcij več spremenljivk.*

Posledica 3.20. *Vsak cel kolobar lahko vložimo v polje.*

Pri konstrukciji polja ulomkov smo večkrat uporabili komutativnost kolobarja K. Izkaže se, da ne moremo vsakega nekomutativnega kolobarja brez deliteljev niča vložiti v (nekomutativen) obseg.

3.7 Karakteristika kolobarja in prapolja

Definicija 3.10. 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, pravimo, da ima kolobar K karakteristiko 0.

Kolobar je aditivna grupa za seštevanje in njegova karakteristika je enaka redu enote, če je ta seveda končen, sicer pa je enaka 0. Ker je $n \cdot x = x + \cdots + x = (1 + \cdots + 1)x = (n \cdot 1)x$, v kolobarju s karakteristiko n velja $n \cdot x = 0$ za vse $x \in K$.

Zgled 3.19. *Večina kolobarjev, na katere najprej pomislimo, ima karakteristiko 0. Taki so na primer kolobarji $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ in $\mathbb{C}$. Kolobar ostankov $\mathbb{Z}_n$ pa 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.*

Zgled 3.20. *Kolobar $\mathbb{Z}_3 \times \mathbb{Z}_2$ ima karakteristiko 6.*

Trditev 3.21. *Karakteristika neničelnega kolobarja K brez deliteljev niča je bodisi 0 bodisi praštevilo.*

Dokaz. Privzemimo, da je karakteristika K naravno število n. Naj bo torej $n = rs$ 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 praštevilsko ali ničelno karakteristiko.

Izrek 3.22.

Naj bo F polje.

1. *Če je karakteristika F enaka 0, lahko polje $\mathbb{Q}$ vložimo v F.*
2. *Če je karakteristika F praštevilo p, lahko polje $\mathbb{Z}_p$ vložimo v F.*

Dokaz. Naredimo doaz za prvo točko. Definiramo 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 še dobro definiranost. Imamo:

$$\begin{aligned} \frac{m}{n} = \frac{m'}{n'} &\Rightarrow mn' = m'n \\ &\Rightarrow (m \cdot 1)(n' \cdot 1) = (m' \cdot 1)(n \cdot 1) \\ &\Rightarrow (m \cdot 1)(n \cdot 1)^{-1} = (m' \cdot 1)(n' \cdot 1)^{-1}, \end{aligned}$$

kjer smo v zadnji vrstici uporabili predpostavko, da ima F karakteritiko 0. Tako smo pokazali, da je φ dobro definirana preslikava. Z neposrednim računom pa preverimo tudi, da je homomorfizem s trivialnim jedrom. V drugi točki naredimo podoben dokaz, tako da definiramo $\varphi : \mathbb{Z}_p \to F$ s predpisom $\varphi([k]) = k \cdot 1$. □

Vsako podpolje vsebuje enoto 1, zato je podpolje, generirano z 1, najmanjše izmed vseh podpolj F. Imenujemo ga prapolje. V dokazu izreka smo videli, da je v obeh primerih $\operatorname{im}\varphi$ enak prapolju polja F. Torej lahko zaključimo, da če ima polje F karakteristiko 0, je njegovo prapolje izomorfno $\mathbb{Q}$, če pa ima karakteristiko p, pa je njegovo prapolje izomorfno $\mathbb{Z}_p$.

4 Kvocientne strukture

4.1 Odseki in Lagrangev izrek

Definicija 4.1. Naj bo H podgrupa grupe G in naj bo $a \in G$. Množici $aH = \{ah \mid h \in H\}$ pravimo odsek grupe G po podgrupi H.

Če je G aditivna grupa, pišemo odsek kot $a + H$. Odseki v splošnem niso podgrupe, saj če $a \neq H$, potem aH ne vsebuje enote. Hkrati pa velja $aH = H \Leftrightarrow a \in H$, kar je enostavno dokazati. Odsek aH natančneje imenujemo levi odsek. Desni odsek vpeljemo kot množico $Ha = \{ha \mid h \in H\}$.

Zgled 4.1. *Vpeljimo nekaj primerov odsekov.*

- *Naj bo $G = \mathbb{Z}$ in $H = n\mathbb{Z}$ za $n \in \mathbb{N}$. Odseki, ki jih porodijo $0, 1, \ldots, n-1$, so $n\mathbb{Z}$, $1 + n\mathbb{Z}$, $\ldots$, $(n-1) + n\mathbb{Z}$.*
- *Naj bo G aditivna grupa $\mathbb{R}^2$ in naj bo H abscisna os, torej premica $y = 0$. Odseki $a + H$ so korizontalne premice, torej premice vzporedne premici H.*
- *Naj bo $G = C^*$, tj. grupa neničelnih kompleksnih števil z operacijo množenja. Za H vzemimo krožno grupo $\mathbb{T}$. Odsek zH je množica vseh kompleksnih števil. ki imajo isto absolutno vrednost kot število $z \in C^*$, torej so ti odseki koncentrične krožnice.*
- *Naj bo G simetrična grupa S_n in H alternirajoča grupa A_n. Če je $\sigma \in H$, potem je $\sigma H = H$, sicer pa je σH množica vseh lihih permutacij.*

Lema 4.1. *Za poljubna $a, b \in G$ velja $aH = bH \Leftrightarrow a^{-1}b \in H$.*

Dokaz. Če je $aH = bH$, potem je $b = b \cdot 1 \in bH = aH$. Torej je $b = ah_0$ za neki $h_0 \in H$. To pa je ekvivalentno $a^{-1}b = h_0 \in H$. Obratno; naj bo $h_0 = a^{-1}b \in H$. Potem je $b = ah_0$ in zato $bh = a(h_0h) \in aH$ za vsak $h \in H$, torej $bH \subseteq aH$. Ker je $b^{-1}a = (a^{-1}b)^{-1} = h_0^{-1} \in H$, podobno vidimo, da je $aH \subseteq bH$. □

Če sta $a, b \in G$, potem je pogoj $ab^{-1} \in H$ ekvivalenten enakosti desnih odsekov Ha in Hb. V aditivni grupi ugotovitev iz leme zapišemo kot $a + H = b + H \Leftrightarrow b - a \in H \Leftrightarrow a - b \in H$.

Lema 4.2. *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 $ah_1 = bh_2$. Potem je $a^{-1}b = h_1h_2^{-1} \in H$ in po lemi velja $aH = bH$. □

Grupa G je torej disjunktna unija odsekov aH. Tako lahko uvedemo ekvivalenčno relacijo s predpisom $a \sim b \Leftrightarrow a^{-1}b \in H$.

Definicija 4.2. 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, kot na primer $[\mathbb{Z} : n\mathbb{Z}] = n$.

Izrek 4.3 (Lagrange)**.**

Naj bo H podgrupa končne grupe G. Potem je $|G| = [G : H] \cdot |H|$.

Dokaz. Naj bo $[G : H] = r$, potem lahko zapišemo množico vseh odsekov kot $\{a_1H, \ldots, a_rH\}$ za neke $a_1, \ldots, a_r \in G$. Hkrati pa vemo, da velja $|a_1H| + \cdots + |a_rH| = |G|$. Vsako izmed števil $|a_iH|$ pa je kar enako $|H|$, saj je preslikava $h \mapsto a_ih$ namreč bijekcija iz H v a_iH. Torej je $|G| = r|H|$. □

Ta izrek nam pove, da je red končne grupe deljiv z redom vsake njene podgrupe.

4.2 Podgrupe edinke in kvocientne grupe

Naj bo G poljubna grupa in N njena podgrupa. Označimo množico vseh odsekov kot $G/N = \{aN \mid a \in G\}$. Intuitivno se zdi, da se s predpisom $aN \cdot bN = (ab)N$ ponuja operacija množenja v tej množici. Vendar pa moraveljati določen pogoj, da je ta operacija dobro definirana.

Lema 4.4. *Naj bo N podgrupa grupe G. Naslednja pogoja sta ekvivalentna.*

- *Za vse $a, a', b, b' \in G$ iz $aN = a'N$ in $bN = b'N$ sledi $(ab)N = (a'b')N$.*
- *Za vse $a \in G$ in $n \in N$ je $ana^{-1} \in N$.*

Dokaz. Prvi pogoj lahko zapišemo kot

$$a^{-1}a' \in N \ \wedge \ b^{-1}b' \in N \ \Rightarrow b^{-1}a^{-1}a'b' \in N.$$

Dokažimo $(i) \Rightarrow (ii)$. Za poljubna elementa $n \in N$ in $a \in G$ je $1^{-1}n = n \in N$ in $aa^{-1} = 1 \in N$, zato je $ana^{-1} = (a^{-1})^{-1}1^{-1}na^{-1} \in N$. Sedaj pa še $(ii) \Rightarrow (i)$. Naj bodo $a, a', b, b' \in G$ taki, da je $n_1 = a^{-1}a' \in N$ in $n_2 = b^{-1}b' \in N$. Ker je $b^{-1}a^{-1}a'b' = (b^{-1}n_1b)n_2$ in je N podgrupa, sledi $b^{-1}a^{-1}a'b' \in N$. □

Definicija 4.3. Če podgrupa N grupe G ustreza pogoju (ii) iz leme 4.4, se imenuje podgrupa edinka in pišemo $N \lhd G$.

Hitro sledi, da je N podgrupa edinka grupe G natanko tedaj, ko je $N \leq G$ in $aNa^{-1} \subseteq N$ za vsak $a \in G$. Od tod pa takoj sledi naslednja trditev.

Trditev 4.5. *Za podgrupo N grupe G so naslednji pogoji ekvivalentni.*

1. *N je edinka (tj. $aNa^{-1} \subseteq N$ za vsak $a \in G$)*
2. *$aN \subseteq Na$ za vsak $a \in G$.*
3. *$aN = Na$ za vsak $a \in G$.*
4. *$aNa^{-1} = N$ za vsak $a \in G$.*

Pogoj (iv) je ekvivalenten temu, da je edina konjugirana podgrupa podgrupe N podgrupa N sama.

Izrek 4.6.

Naj bo $N \lhd G$. Če v množico G/N vpeljemo množenje s predpisom $aN \cdot bN = (a \cdot b)N$, 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 4.4, asociativnost pa je posledica asociativnosti množenja v G. Enota je odsek $N = 1N$, inverz odseka aN pa je $a^{-1}N$, zato je G/N res grupa. Očitno je π surjektiven homomorfizem. Vemo pa tudi, da velja $aN = N$ natanko tedaj, ko je $a \in N$, zato je $\ker \pi = N$. □

Definicija 4.4. Grupi G/N pravimo kvocientna ali faktorska grupa, preslikavi π pa kanonični epimorfizem.

Vsaka edinka je torej jedro nekega homomorfizma. Pokazali bomo, da velja tudi obratno.

Trditev 4.7. *Podmnožica N grupe G je podgrupa edinka natanko tedaj, ko je N jedro homomorfizma iz grupe G v neko grupo G'.*

Dokaz. Dokažimo trditev v levo. Naj bo $N = \ker \varphi$ za neki homomorfizem $\varphi : G \to G'$. Potem je N tudi podgrupa. Za vsak $a \in G$ in vsak $n \in N$ je $\varphi(ana^{-1}) = \varphi(a)\varphi(n)\varphi(a)^{-1} = \varphi(a)1\varphi(a)^{-1} = 1$, torej $aNa^{-1} \subseteq N$ in N je edinka. □

Vsaka netrivialna grupa G ima vsaj dve podgrupi edinki, to sta $\{1\}$ in G. Če sta to tudi edini grupi edinki, je G enostavna grupa. Primer take grupe je na primer ciklična grupa praštevilskega reda in alternirajoča grupa A_n za $n \geq 5$.

Če je G končna grupa in $N \lhd G$, je po Lagrangevem izreku $|G/N| = \frac{|G|}{|N|}$. Od tod med drugim sledi, da red kvocientne grupe deli red grupe. V Abelovi grupi je očitno vsaka podgrupa edinka. Primer je kvocientna grupa $\mathbb{Z}/n\mathbb{Z}$, ki je kar grupa ostankov $\mathbb{Z}_n$.

Definicija 4.5. Če sta H in K podgrupi G, njun produkt definiramo kot množico $HK = \{hk \mid h \in H,\ k \in K\}$.

V splošnem ta množica ni podgrupa.

Trditev 4.8. *Naj bo G grupa.*

- *Če sta $H, K \leq G$ in je $HK = KH$, je $HK \leq G$.*
- *Če je $H \leq G$ in $N \lhd G$, je $HN = NH \leq G$.*
- *Če sta $M, N \lhd G$, je $MN = NM \lhd G$.*

Dokaz. Dokažimo prvo točko. Vzemimo $h_1, h_2 \in H$ in $k_1, k_2 \in K$. Najprej moramo pokazati, da $(h_1k_1)(h_2k_2)^{-1} = h_1k_1k_2^{-1}h_2^{-1} \in HK$. Ker je $k_1k_2^{-1} \in K$, $h_2^{-1} \in H$ in $KH = HK$, je $k_1k_2^{-1}h_2^{-1} = h_3k_3$ za neka $h_3 \in H,\ k_3 \in K$. Torej je $h_1k_1k_2^{-1}h_2^{-1} = h_1h_3k_3 \in HK$. Druga točka sledi po trditvi 4.5, saj je $hN = Nh$ za vsak $h \in H$ in zato je $HN = NH$. Tretjo točko pa dobimo, saj iz enakosti $a(mn)a^{-1} = (ama^{-1})(ana^{-1})$ sledi $aMNa^{-1} \subseteq MN$ za vsak $a \in G$. □

Produkt podgrup Abelove grupe torej je podgrupa. V aditivnih grupah namesto o produktu seveda govorimo o vsoti podgrup $H + K = \{h + k \mid h \in H,\ k \in K\}$. Ne glede na to, ali je G Abelova, pa je torej produkt edink spet edinka. Kot lahko zlahka preverimo, enako velja za presek edink:

$$M \cap N \subseteq N, M \subseteq MN = NM$$

Naj bo sedaj komutator elementov a in b definiran kot $aba^{-1}b^{-1}$ in ga označimo z $[a, b]$. Če a in b komutirata, je njun komutator enak 1.

Trditev 4.9. *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 $mn = nm$ 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, je $[m, n] \in M$. Podobno za $[m, n] \in N$. □

Nazadnje omenimo, da lahko govorimo tudi o produktu več podgrup.

Definicija 4.6. Produkt podgrup $H_1, \ldots, H_m$ grupe G definiramo kot množico $H_1 H_2 \ldots H_m = \{h_1 h_2 \ldots h_m \mid h_i \in H_i,\ i = 1, \ldots, m\}$.

Če so $N_1, \ldots, N_m$ edinke, je edinka tudi $N_1 \ldots N_m$.

Lema 4.10. *Naj bo $\varphi : G \to G'$ homomorfizem grup.*
- *Če je $H' \leq G'$, je $\varphi^{-1}(H') \leq G$.*
- *Če je $N' \lhd G'$, je $\varphi^{-1}(N') \lhd G$.*
- *Če je $H \leq G$, je $\varphi(H) \leq G'$.*
- *Če je $N \lhd G$ in je φ epimorfizem, je $\varphi(N) \lhd G'$.*

Dokaz. Dokažimo prvo točko. Če sta $h, k \in \varphi^{-1}(H')$, potem sta $\varphi(h), \varphi(k) \in H'$. Od tod pa velja, da $\varphi(hk^{-1}) = \varphi(h)\varphi(k)^{-1} \in H'$ in zato je $hk^{-1} \in \varphi^{-1}(H')$. Dokažimo še drugo točko. Po prvi točke vemo, da je $\varphi^{-1}(N')$ podgrupa, moramo pokazati le, da iz $a \in G$ in $n \in \varphi^{-1}(N')$ sledi $ana^{-1} \in \varphi^{-1}(N')$. To pa je res, saj je $\varphi(ana^{-1}) = \varphi(a)\varphi(n)\varphi(a)^{-1}$ in N' je edinka. Preostali dve točki dokažemo podobno. □

Naj bo $N \lhd G$. Če je H podgrupa G, ki vsebuje N, potem je N očitno tudi podgrupa edinka grupe H. Zato lahko tvorimo kvocientno grupo H/N, ki pa je podgrupa G/N (to sledi iz trditve (c), če vzamemo kanonični epimorfizem $\pi : G \to G/N$). Podobno razmislimo, da je za vsako podgrupo edinko M grupe G, ki vsebuje N, grupa M/N podrgupa edinka grupe G/N.

Izrek 4.11.

Naj bo $N \lhd G$.

- *Vsaka podgrupa G/N je oblike H/N za neko podgrupo H grupe G, ki vsebuje N.*
- *Vsaka podgrupa edinka grupe G/N je oblike M/N za neko podgrupo edinko M grupe G, ki vsebuje N.*

Dokaz. Označimo z π kanonični epimorfizem iz G v G/N. Dokažimo najprej prvo točko. Naj bo H' podgrupa G/N. Po prejšnji lemi je $H = \pi^{-1}(H')$ podgrupa grupe G. V H so taki elementi h, za katere je $hN \in H'$. Zato je $N \subseteq H$, saj je $nN = N$ za vsak $n \in N$. Ker je preslikava π surjektivna, je $\pi(\pi^{-1}(H')) = H'$ in zato $H' = \pi(H) = H/N$. Dokaz drug točke poteka enako, le da vzamemo podgrupo edinko N' grupe G/N in uporabimo drugo točko prejšnje leme. □

Zgled 4.2. *Prejšnji izrek lahko uporabimo na podgrupah grupe $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$. Ker je vsaka podgrupa grupe $\mathbb{Z}$ oblike $k\mathbb{Z}$ za nek $k \in \mathbb{Z}$, je vsaka podgrupa grupe $\mathbb{Z}_n$ oblike $k\mathbb{Z}/n\mathbb{Z}$, kjer je $n\mathbb{Z} \subseteq k\mathbb{Z}$. To pa je izpolnjeno natanko tedaj, ko k deli n, torej lahko grupo $k\mathbb{Z}/n\mathbb{Z}$ zapišemo kot $k\mathbb{Z}$.*

4.3 Ideali in kvocientni kolobarji

Lema 4.12. *Naj bo I podgrupa za seštevanje K. Naslednja pogoja sta ekvivalentna.*
1. *Za vse $a, a', b, b' \in K$ iz $a + I = a' + I$ in $b + I = b' + I$ sledi $(ab) + I = (a'b') + I$.*
2. *Za vse $a \in K$ in $u \in I$ je $au \in I$ in $ua \in I$.*

Dokaz. Prvi pogoj lahko zapišemo tako, da iz $a' - a \in I$ in $b' - b \in I$ sledi $a'b' - ab \in I$. Začnimo s trditvijo v smeri $(i) \Rightarrow (ii)$. Za vsak $a \in K$ in $u \in I$ velja $au = au - a0 \in I$ in $ua = ua - 0a \in I$. Sedaj pa še $(ii) \Rightarrow (i)$. Denimo, da za $a, a', b, b' \in K$ velja $u_1 = a' - a \in I$ in $u_2 = b' - b \in I$. Iz $a'b' - ab = (a + u_1)(b + u_2) - ab = u_1 b + a u_2 + u_1 u_2$ sledi $a'b' - ab \in I$. □

Definicija 4.7. Naj bo I podgrupa kolobarja K za seštevanje. Če I zadošča drugemu pogoju, se imenuje ideal kolobarja K. Tedaj pišemo $I \lhd K$.

Velja torej, da je $I \lhd K$ natanko tedaj, ko je I podgrupa za seštevanje, $KI \subseteq I$ in $IK \subseteq I$. Ideal je torej med drugim zaprt za množenje, vendar pa praviloma ni podkolobar, saj ne vsebuje nujno enote 1. Če jo vsebuje, je pravzaprav enak celemu K.

Zgled 4.3. *Podmnožica kolobarja $\mathbb{Z}$ je ideal natanko tedaj, ko je $n\mathbb{Z}$ za $n \in \mathbb{Z} \cap \{0\}$.*

Izrek 4.13.

Naj bo $I \lhd K$. 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 pa je dobro definirano po prejšnji lemi. Asociativnost in distributivnostna zakona sledita direktno iz lastnosti K, enota za množenje pa je $1 + I$. Iz definicij seštevanja in množenja vidimo, da je preslikava π epimorfizem, hitro pa tudi sledi, da so v njegovem jedru natanko elementi iz I. □

Definicija 4.8. Kolobarju K/I pravimo kvocientni ali faktorski kolobar, preslikavi π pa kanonični epimorfizem.

Zgled 4.4. *Za primer vzemimo kolobar $\mathbb{Z}/n\mathbb{Z}$, ki pa je kot v primeru z grupami enak $\mathbb{Z}_n$. Omenimo še očitna primera idealov poljubnega kolobarja K, ki sta kar $\{0\}$ in K.*

Trditev 4.14. *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 $u - v \in I$ in I je podgrupa. 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 $ua \in I$ in je zato I ideal. □

Če sta I in J ideala kolobarja K, sta ideala tudi njun presek $I \cap J$ in vsota $I + J$. Prav tako je ideal njun produkt IJ, ki smo ga definirali kot podgrupo K za seštevanje, generirano z vsemi elementi oblike uv za $u \in I$ in $v \in J$. Če je kolobar K 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 $IJ \subseteq I \cap J \subseteq I \subseteq I + J$.

Definicija 4.9. Podmnožico L kolobarja K imenujemo levi ideal, če je podgrupa za seštevanje in če velja $KL \subseteq L$, torej $al \in L$ za vse $a \in K$ in $l \in L$. Podobno definiramo desni ideal, pri čemer zahtevamo $LK \subseteq L$.

Ideali so seveda hkrati levi in desni ideali, zato jim pravimo dvostranski ideali. V komutativnih idealih vsi ti pojmi sovpadajo, v nekomutativnih pa v mnogih pomembnih ne.

Zgled 4.5. *Množica vseh matrik oblike* $\begin{bmatrix} a & 0 \\ b & 0 \end{bmatrix}$ *za* $a, b \in \mathbb{R}$ *je levi ideal kolobarja* $M_2(\mathbb{R})$*, ki ni desni ideal. Obratno: množica matrik oblike* $\begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix}$.

Trditev 4.15. *Če levi ideal* L *kolobarja* K *vsebuje kak obrnljiv element, je* $L = K$.

Dokaz. Označimo obrnljiv element $l \in L$. Potem je $1 = ll^{-1} \in KL \subseteq L$ in od tod $a = a1 \in KL \subseteq L$ za vsak $a \in K$. □

Trditev 4.16. *Neničeln kolobar* K *je obseg natanko tedaj, ko sta* $\{0\}$ *in* K *njegova edina leva ideala.*

Dokaz. Trditev v desno sledi direktno iz prejšnje trditve. Dokažimo trditev v nasprotno smer. Naj bosta $\{0\}$ in K edina leva ideala kolobarja K. Vzemimo poljuben $a \neq 0$ iz K, potem je množica Ka očitno levi ideal. Ker vsebuje $a = 1a$, ni enak $\{0\}$ in je zato po predpostavki enak K. Torej obstaja $b \in K$, da je $ba = 1$. Potem očitno $b \neq 0$ zato lahko vzamemo levi ideal Kb in podobno zaključimo, da obstaja $c \in K$, da je $cb = 1$. Ker je levi inverz enak desnemu, je $ab = ba = 1$ in zato je poljuben neničeln element K obrnljiv. □

Definicija 4.10. Neničeln kolobar K se imenuje enostaven kolobar, če sta K in $\{0\}$ njegova edina ideala.

Iz prejšnje trditve sledi, da so vsi obsegi enostavni kolobarji, vendar pa ta trditev ne velja v nasprotno smer; protiprimer je recimo kolobar $n \times n$ matrik nad obsegom. V komutativnih kolobarjih pa ta dva pojma očitno sovpadata.

Posledica 4.17. *Komutativen kolobar* K *je enostaven natanko tedaj, ko je polje.*

Lema 4.18. *Naj bo* $\varphi : K \to K'$ *homomorfizem kolobarjev.*
- *Če je* $I' \lhd K'$*, je* $\varphi^{-1}(I') \lhd K$.
- *Če je* $I \lhd K$ *in je* φ *epimorfizem, je* $\varphi(I) \lhd K'$.

Izrek 4.19.

Naj bo $I \lhd K$. *Vsak ideal kolobarja* K/I *je oblike* J/I *za neki ideal* J *kolobarja* K*, ki vsebuje* I.

Seveda pa velja tudi obrat tega izreka, torej je J/I ideal K/I za vsak ideal J, ki vsebuje I.

Definicija 4.11. Idealu I kolobarja K pravimo maksimalen ideal, če $I \neq K$ in če ne obstaja tak ideal J, da bi veljalo $I \subseteq J \subseteq K$.

Zgled 4.6. *Trdimo, da je* $2\mathbb{Z}$ *maksimalen ideal kolobarja* $\mathbb{Z}$*. Če namreč neki ideal kolobarja* $\mathbb{Z}$ *vsebuje vsa soda števila in še kakšno liho število povrhu, potem je enak celemu kolobarju* $\mathbb{Z}$.

Posledica 4.20. *Ideal* I *kolobarja* K *je maksimalen natanko tedaj, ko je kvocientni prostor* K/I *enostaven.*

Dokaz. Če je I maksimalen, potem K/I ni ničelni kolobar in po prejšnjem izreku nima drugih idealov kot $I/I = \{0\}$ in K/I, zato je K/I enostaven. Obratno; če I ni maksimalen, potem obstaja tak ideal J, da je $I \subseteq J \subseteq K$ in tedaj je J/I tak ideal K/I, ki ni enak niti $\{0\}$ niti K/I, zato K/I ni enostaven. □

Posledica 4.21. *Ideal I komutativnega kolobarja K je maksimalen natanko tedaj, ko je kvocientni kolobar K/I polje.*

Omenimo še, da je vsak pravi ideal kolobarja vsebovan v nekem maksimalnem idealu.

Definicija 4.12. 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 ideala, je ideal podprostor.

Izrek 4.22.

Naj bo U podprostor vektorskega prostora V. Če v množico vseh odsekov V/U vpeljemo seštevanje in množenje s skalarji s predpisom $(v+U)+(w+U) = (v+w)+U$ in $\lambda(v+U) = \lambda v + U$, postane V/U vektorski prostor. Preslikava $\pi : V \to V/U$, definirana s $\pi(v) = v + U$ je epimorfizem in $\ker \pi = U$.

Vektorskemu prostoru V/U pravimo kvocientni ali faktorski vektorski prostor, preslikavi π pa kanonični epimorfizem.

Izrek 4.23.

Naj bo I ideal algebre A. Če v množico A/I vpeljemo seštevanje, množenje in množenje s skalarji s predpisi $(a+I)+(b+I) = (a+b)+I$, $(a+I)(b+I) = ab+I$ in $\lambda(a+I) = \lambda a + I$, postane A/I algebra. Preslikava $\pi : A \to A/I$, definirana s $\pi(a) = a + I$ je epimorfizem in $\ker \pi = I$.

4.4 Izrek o izomorfizmu in primeri kvocientnih prostorih

Izrek 4.24.

Naj bo $\varphi : A \to A'$ homomorfizem (grup, kolobarjev, vektorskih prostorov ali algeber). Potem je $A/\ker\varphi \cong \operatorname{im}\varphi$.

Dokaz. Obravnavajmo φ kot homomorfizem grup. Kot vemo, je $\ker\varphi$ podgrupa edinka, zato lahko vpeljemo kvocientno grupo $A/\ker\varphi$. Za poljubna $a, a' \in A$ velja

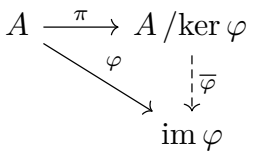
$$\begin{aligned} a\ker\varphi = a'\ker\varphi &\Leftrightarrow a^{-1}a' \in \ker\varphi \\ &\Leftrightarrow \varphi(a^{-1}a') = 0 \\ &\Leftrightarrow \varphi(a) = \varphi(a'). \end{aligned}$$

Od tod sledi, da je preslikava $\overline{\varphi} : A/\ker\varphi \to \operatorname{im}\varphi$, definirana s predpisom $\overline{\varphi}(a\ker\varphi) = \varphi(a)$ dobro definirana in injektivna. 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 in je očitno tudi surjektiven. □

Pri dokazu smo implicitno uporabili naslednji komutativni diagram.



Zgled 4.7. *Oglejmo si preprost dokaz osnovnega izreka o cikličnih grupah. Naj bo G ciklična grupa in $a \in G$ tak element, da je $G = \langle a \rangle$. Preslikava $\varphi : \mathbb{Z} \to G$ s predpisom $\varphi(n) = a^n$ je očitno epimorfizem grup. Če ima trivialno jedro, je izomorfizem, v nasprotnem primeru pa je $\ker \varphi = n\mathbb{Z}$ za neki $n \in \mathbb{N}$. Po prejšnjem izreku je tedaj $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z} \cong \operatorname{im} \varphi = G$.*

Zgled 4.8. *Naj bo G poljubna grupa. Potem sta podgrupi $\{1\}$ in G edinki. Za ustrezni kvocientni grupi velja $G/\{1\} \cong G$ in $G/G \cong \{1\}$.*

Zgled 4.9. *Naj bo G aditivna grupa $\mathbb{R}^2$, H pa premica $y = 0$, torej $H = \{(x_1, 0) \mid x_1 \in \mathbb{R}\}$. Potem je H edinka in odseki so vodoravne premice. Vidimo, da je preslikava $(x_1, x_2) + H \mapsto x_2$ izomorfizem iz grupe G/H v $\mathbb{R}$. Lahko pa do tega pridemo po drugi poti. Opazimo, da je preslikava $\varphi : G \to \mathbb{R}$ s predpisom $\varphi(x_1, x_2) = x_2$ epimorfizem aditivnih grup in $\ker \varphi = H$. Zato po izreku velja $G/H \cong \mathbb{R}$.*

Zgled 4.10. *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 kot $|a||b|\mathbb{T}$. Sklepamo, da je $\mathbb{C}^*/\mathbb{T} \cong \mathbb{R}^+$. Res, to sledi izizreka o izomorfizmu, saj je $z \mapsto |z|$ epimorfizem iz $\mathbb{C}^*$ v $\mathbb{R}^+$ in njegovo jedro je $\mathbb{T}$.*

Zgled 4.11. *Alternirajoča grupa A_n je podgrupa edinka simetrične grupe S_n. To zelo hitro sledi iz dejstva, da je A_n jedro epimorfizma $\sigma \mapsto \operatorname{sgn} \sigma$ iz S_n v grupo $(\{1, -1\}, \cdot)$. Od tod pa sledi, da je $S_n/A_n \cong \mathbb{Z}_2$ in zato $[S_n : A_n] = 2$.*

Zgled 4.12. *Posebna linearna grupa $\mathrm{SL}_n(F)$ je jedro epimorfizma $A \mapsto \det(A)$ iz splošne linearne grupe $\mathrm{GL}_n(F)$ v grupo $(F^*, \cdot)$. Zato je $\mathrm{GL}_n(F)/\mathrm{SL}_n(F) \cong F^*$.*

Zgled 4.13. *Center $Z(G)$ grupe G je očitno podgrupa edinka. Torej lahko govorimo o kvocientni grupi $G/Z(G)$. V prejšnjem sklopu smo omenili, da je $a \mapsto \varphi_a$ epimorfizem iz grupe G v grupo notranjih avtomorfizmov $\mathrm{Inn}(G)$. V jedru te preslikave so elementi $c \in G$ z lastnostjo, da je $cxc^{-1} = x$ za vse $x \in G$, torej je jedro kar center $Z(G)$ in je torej $G/Z(G) \cong \mathrm{Inn}(G)$.*

Opomba. Center $Z(G)$ grupe G je edinka, center $Z(K)$ nekomutativnega kolobarja K pa ni ideal, saj vsebuje enoto.

Za naravno število $n \in \mathbb{N}$ so ekvivalentne naslednje izjave:

- p je praštevilo,
- kolobar $\mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z}$ je polje in
- $p\mathbb{Z}$ je maksimalen ideal kolobarja $\mathbb{Z}$.

Zgled 4.14. *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, potem je ideal $XK[X]$ maksimalen.*

Zgled 4.15. *Izberimo točko $x \in [0,1]$. Množica $I_x = \{f \in C[0,1] \mid f(x) = 0\}$ je ideal kolobarja (oziroma algebre) $C[0,1]$ in $C[0,1]/I_x \cong \mathbb{R}$, torej je I_x maksimalen ideal.*

Zgled 4.16. *Naj bo A končno generirana komutativna algebra nad poljem F. Če je $\{a_1, \ldots, a_n\}$ množica njenih generatorjev, je torej vsak element A linearna kombinacija izrazov oblike $a_1^{k_1} \ldots a_n^{k_n}$ za $k_i \geq 0$. Torej je vsak element A oblike $f(a_1, \ldots, a_n)$, kjer je $f(X_1, \ldots, X_n) \in F[X_1, \ldots, X_n]$. Preslikava $\varphi : F[X_1, \ldots, X_N] \to A$ s predpisom $\varphi(f(X_1, \ldots, X_n)) = f(a_1, \ldots, a_n)$ je torej surjektivni homomorfizem algeber in njegovo jedro I je ideal. Po izreku o izomorfizmu je $F[X_1, \ldots, X_n]/I \cong A$. Torej je vsaka komutativna algebra izomorfna kvocientni grupi algebre polinomov v n spremenljivkah z nekim njenim idealom. Lahko bi vzeli tudi algebro polinomov neskončno mnogo spremenljivk (le da so polinomi odvisni od končno mnogo spremenljivk). Torej lahko ta primer posplošimo, da je vsaka komutativna algebra izomorfna kvocientni grupi algebre polinomov z nekim njenim idealom.*

4.5 Zunanji in notranji direktni produkti grup

Definicija 4.13. Grupa G je notranji direktni produkt svojih podgrup edink $N_1, \ldots, N_k$, če je $G = N_1 \ldots N_m$ in če je

$$N_i \cap (N_1 \ldots N_{i-1} N_{i+1} \ldots N_m) = \{1\}$$

za vse $i = 1, \ldots, m$.

Če je grupa G zunanji direktni produkt grup $G_1, \ldots, G_m$, potem je G notranji direktni produkt edink $\tilde{G}_i$, kjer je $\tilde{G}_i = \{(1, \ldots, 1, g_i, 1, \ldots, 1) \mid g_i \in G_i\}$. Dokazali bomo, da velja tudi obratno.

Iz definicije sledi, da je $N_i \cap N_j = \{1\}$ za vse $i \neq j$, zato je po trditvi 4.9 $n_i n_j = n_j n_i$ za vse $n_i \in N_i$, $n_j \in N_j$ ter $i \neq j$. Prvi pogoj pove, da lahko vsak element iz G zapišemo kot produkt elementov iz $N_1, \ldots, N_m$ na vsaj en način, drugi pa nam zagotavlja, da je tak način le eden.

Trditev 4.25. *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 $n_1 \ldots n_m$, kjer je $n_i \in N_i$.*

Dokaz. Naj bo G notranji direktni produkt podgrup edink $N_1, \ldots, N_m$ in naj bo $n_1 \ldots n_m = r_1 \ldots r_m$ za $n_i, r_i \in N_i$. To je ekvivalentno enakosti

$$r_1^{-1} n_1 = (r_2 \ldots r_m)(n_2 \ldots n_m)^{-1}.$$

Ker je $N_2 \ldots N_m$ po trditvi 4.8 podgrupa, vsebuje element $r_1^{-1} n_1$. Seveda je ta element vsebovan tudi v N_1, torej je $n_1 = r_1$. Po indukciji sledi, da velja $n_i = r_i$ za vsak $i = 1, \ldots, m$. Dokažimo še obrat; naj se da vsak element iz G samo na en način zapisati v obliki $n_1 \ldots n_m$, kjer je $n_i \in N_i$. Očitno velja prvi pogoj, zato se osredotočimo na drugega. Naj bo $a \in N_i \cap (N_1 \ldots N_{i-1} N_{i+1} \ldots N_m)$. Potem lahko a zapišemo na dva načina kot $a = 1 \ldots 1 \cdot n_i \cdot 1 \ldots 1$ in $a = n_1 \ldots n_{i-1} \cdot 1 \cdot n_{i+1} \ldots n_m$ za neke $n_j \in N_j$. Od tod pa takoj sledi, da je $a = 1$. □

Izrek 4.26.

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 $\varphi((n_1, \ldots, n_m)) = n_1 \ldots n_m$. Iz prejšnje trditve sledi, da je φ bijektivna, hitro pa se da pokazati tudi, da je homomorfizem. □

Notranji direktni produkt označujemo enako kot zunanjega in med njima v praksi sploh ne ločimo. Naj bo $m = 2$. Potem se pogoja iz definicije glasita $G = N_1N_2$ in $N_1 \cap N_2 = \{1\}$. Po prejšnji trditvi je to ekvivalentno temu, da lahko vsak element iz G na en sam način zapišemo v obliki n_1n_2, kjer je $n_1 \in N_1$ in $n_2 \in N_2$. Torej je preslikava $\varphi : G \to N_2$ s predpisom $\varphi(n_1n_2)$ dobro definirana, zlahko pa se prepričamo tudi, da je epimorfizem. Ker je $\ker \varphi = N_1$, po izreku o izomorfizmu sledi $G/N_1 \cong N_2$ (in analogno $G/N_2 \cong N_1$).

Zgled 4.17. *Vsaka grupa G je notranji direktni produkt svojih edink G in $\{1\}$.*

Zgled 4.18. *Diedrska grupa D_4 je notranji direktni produkt svojih (cikličnih) podgrup $N_1 = \{1, r\}$ in $N_2 = \{1, z\}$ (ker je D_4 Abelova, so vse njene podgrupe edinke).*

Zgled 4.19. *Grupa $\mathbb{C}^*$ je notranji direktni produkt svojih podgrup $\mathbb{R}^+$ in $\mathbb{T}$. To je zato, ker lahko vsak $z \in \mathbb{C}^*$ zapišemo kot $z = |z|\frac{z}{|z|}$, kjer je $|z| \in \mathbb{R}^+$ in $\frac{z}{|z|} \in \mathbb{T}$, hkrati pa je tudi $\mathbb{R}^+ \cap \mathbb{T} = \{1\}$. Potem sledi $\mathbb{C}^*/\mathbb{T} \cong \mathbb{R}^+$ oziroma $\mathbb{C}^*/\mathbb{R}^+ = \mathbb{T}$, kar pa smo že pokazali.*

Zgled 4.20. *Grupa $\mathrm{SL}_n(F)$ je podgrupa edinka grupe $\mathrm{GL}_n(F)$. Enako velja za grupo Z vseh skalarnih matrik λI, saj je le-ta center $\mathrm{GL}_n(F)$. Dokažimo, da če je $x \mapsto x^n$ bijektivna preslikava iz F v F, potem je grupa $\mathrm{GL}_n(F)$ njun notranji direktni produkt. Res, naj bo $A \in \mathrm{GL}_n(F)$. Potem po predpostavki obstaja tak $\lambda \in F^*$, da je $\lambda^n = \det(A)$. Tedaj je $\det(\lambda^{-1}A) = 1$ in posledično $\lambda^{-1}A \in \mathrm{SL}_n(F)$. Opazimo, da lahko A zapišemo kot $A = \lambda I \cdot \lambda^{-1}$. Skalarna matrika λI leži v $\mathrm{SL}_n(F)$ natanko tedaj, ko je $\lambda^n = 1$. Ker je $x \mapsto x^n$ injektivna, je to natanko tedaj, ko je $\lambda = 1$. Torej je $Z \cap \mathrm{SL}_n(F) = \{I\}$.*

V aditivnih grupah izraz direktni produkt zamenjamo z direktno vsoto. 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 $N_i \cap (N_1 + \cdots + N_{i-1} + N_{i+1} + \ldots N_m) = \{0\}$ za vse $i = 1, \ldots, m$.

Zgled 4.21. *Grupa $\mathbb{Z}_6$ je notranja direktna vsota svojih podgrup $\{0, 2, 4\} \cong \mathbb{Z}_3$ in $\{0, 3\} \cong \mathbb{Z}_2$, zato je $\mathbb{Z}_6 \cong \mathbb{Z}_3 \oplus \mathbb{Z}_2$. Grup $\mathbb{Z}_2$, $\mathbb{Z}_3$, $\mathbb{Z}_4$ in $\mathbb{Z}_5$ pa ne moremo razstaviti na direktne vsote praavih netrivialnih podgrup. Nekatere izmed naštetih grup jih pravzaprav sploh nimajo.*

4.6 Direktni produkti in vsote v kolobarjih

Definicija 4.14. Element kolobarja K se imenuje idempotent, če je $e^2 = e$. Idempotent, ki komutira z vsakim elementom iz kolobarja (oziroma idempotent iz centra kolobarja) se imenuje centralen idempotent.

Če je e centralen idempotent, je $eK = \{ex \mid x \in K\}$ očitno ideal K. Idempotenta e in f sta ortogonalna, če je $ef = fe = 0$. Na primer, za vsak idempotent e sta idempotenta e in $1-e$ ortogonalna. Ortogonalni idempotenti imajo to lastnost, da je njihova vsota prav tako idempotent.

Izrek 4.27.

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 idempotenti $e_1, \ldots, e_m \in K$, da je $e_1 + \cdots + e_m = 1$ in $I_i = e_iK$ za vse

$i = 1, \ldots, m$.

Dokaz. Dokažimo najprej implikacijo ($\Rightarrow$). Naj bo $K = I_1 \oplus \cdots \oplus I_m$. Potem je enota 1 kolobarja enaka $e_i + \cdots + e_m$, kjer je $e_i \in I_i$ za vsak $i = 1, \ldots, m$. 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 (oziroma z desne) z $u_i \in I_i$, dobimo $u_i = u_i e_i = e_i u_i$ za vse $u_i \in I_i$. Ta enakost nam pove, da je $I_i \subseteq e_i K$. Ker pa je I_i ideal in $e_i \in I_i$, mora veljati tudi $e_i K \subseteq I_i$, torej je $I_i = e_i K$. Če v prejšnjo enakost sedaj vstavimo $u_i = e_i$, vidimo, da je e_i (centralen) idempotent. Ker je $I_i I_j = I_j I_i = \{0\}$ za $i \neq j$, velja $e_i u_j = u_j e_i = 0$ za vse $u_j \in I_j$. Torej so $e_1, \ldots, e_m$ paroma ortogonalni in smo dokazali. Dokaz v obratno smer ($\Leftarrow$) je preprost. □

Zgled 4.22. *V prejšnjem zgledu smo omenili, da je grupa $(\mathbb{Z}_6, +)$ direktna vsota svojih podgrup $\{0, 2, 4\}$ in $\{0, 3\}$. Ti podgrupi sta ideala kolobarja $\mathbb{Z}_6$, ustrezna idempotenta pa sta $e_1 = 4$ in $e_2 = 1 - e_1 = 3$.*

V prejšnjem dokazu v levo nismo potrebovali uporabiti dejstva, da so idempotenti e_i centralni. Torej smo pokazali, da je kolobar K direktna vsota svojih desnih idealov $e_1 K, \ldots, e_m K$, 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 s svojo enoto e_i, v nasprotju s splošnimi ideali kolobarjev, ki pa nimajo nujno svojih enot. Zato lahko govorimo o direktnem produktu kolobarjev $I_1 \times \cdots \times I_m$.

Izrek 4.28.

Če je kolobar K enak direktni vsoti svojih idelov $I_1, \ldots, I_m$, potem je K izomorfen njihovemu produktu $I_1 \times \cdots \times I_m$.

Dokaz. Dokažimo, da je preslikava $\varphi : I_1 \times \cdots \times I_m \to K$ s predpisom $\varphi((u_1, \ldots, u_m)) = u_1 + \cdots + u_m$ homomorfizem kolobarjev. Ker lahko vsak element iz K na natanko en način zapišemo kot $u_1 + \cdots + u_m$ za $u_i \in I_i$, je φ bijektivna. Dokažimo še, da je multiplikativna. Hočemo, da je za poljubne $u_i, v_i \in I_i$ element

$$\varphi((u_1, \ldots, u_m) \cdot (v_1, \ldots, v_m)) = \varphi(u_1 v_1, \ldots, u_m v_m) = u_1 v_1 + \cdots + u_m v_m$$

enak elementu

$$\varphi(u_1, \ldots, u_m) \cdot \varphi(v_1, \ldots, v_m) = (u_1 + \cdots + u_m)(v_1 + \cdots + v_m).$$

To pa je takojšnja posledica dejstva, da je $u_i v_j = (u_i e_i)(e_j v_j) = 0$ za $i \neq j$. □

Vse, kar smo povedali za produkte in vsote v kolobarjih, velja tudi za algebre.

5 Končne grupe

5.1 Posledice Lagrangevega izreka

Izrek 5.1 (Lagrange)**.**

Če je G končna grupa in H njena podgrupa, potem je $|G| = [G : H] \cdot |H|$.

Pri tem je $[G : H]$ indeks grupe G po podgrupi H, torej število vseh odsekov aH za $a \in G$. Največkrat uporabljamo naslednjo posledico izreka.

Posledica 5.2. *Red vsake končne podgrupe deli red grupe.*

Posledica 5.3. *Naj bo a element grupe G.*

- *Če ima a red n, potem za vsak $m \in \mathbb{Z}$ velja $a^m = 1 \Leftrightarrow n \mid m$.*
- *Če je $a \neq 1$ in za neko praštevilo p velja $a^p = 1$, potem je p red elementa a.*
- *Če ima a red n in je $\varphi : G \to G'$ homomorfizem grup, potem red elementa $\varphi(a)$ deli n.*
- *Če je N edinka v G in ima a red n, potem red $aN \in G/N$ deli n.*

Posledica 5.4. *Red vsakega elementa končne grupe deli red grupe.*

Dokaz. Red elementa a je enak redu ciklične podgrupe $\langle a \rangle$, ki pa po Lagrangevem izreku deli red grupe. □

Posledica 5.5. *Če je G končna grupa z n elementi, je $a^n = 1$ za vsak $a \in G$.*

Posledica 5.6. *Za vsako praštevilo p in naravno število a je $a^p \equiv a \pmod{p}$.*

Dokaz. Privzemimo, da p ne deli a. Elementi polja $\mathbb{Z}_p$ so odseki $x + p\mathbb{Z}$, kjer je $x \in \mathbb{Z}$. Potem je element $a + p\mathbb{Z}$ neničeln in zato element grupe $\mathbb{Z}_p^*$. Po prejšnji posledici je $(a + p\mathbb{Z})^{p-1} = 1 + p\mathbb{Z}$, kar pa je ekvivalentno $a^{p-1} + p\mathbb{Z} = 1 + p\mathbb{Z}$ oziroma $a^{p-1} - 1 \in p\mathbb{Z}$. Trditev je dokazana. □

Posledica 5.7. *Vsaka grupa G s praštevilskim redom je ciklična. Še več, za vsak element $a \in G \setminus \{1\}$ je $\langle a \rangle = G$.*

Vsaka grupa G s p elementi je torej izomorfna grupi $(\mathbb{Z}_p, +)$.

Posledica 5.8. *Netrivialna grupa nima pravih netrivialnih podgrup natanko tedaj, ko je ciklična grupa s praštevilskim redom.*

Dokaz. ($\Rightarrow$) 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 in zato izomorfna bodisi $\mathbb{Z}$ bodisi $\mathbb{Z}_n$ za nek $n \in \mathbb{N}$. Ker ima $\mathbb{Z}$ prave netrivialne podgrupe, pride v poštev le druga možnost: $G \cong \mathbb{Z}_n$. Če n ni praštevilo oziroma je deljiva s številom d, kjer je $1 < d < n$, potem je $d\mathbb{Z}_n$ njena prava netrivialna množica in smo prišli v protislovje. Obrat ($\Leftarrow$) je očiten. □

5.2 Razredna formula

Definicija 5.1. Elementa a in a' iz grupe G sta si konjugirana, če obstaja tak $g \in G$, da je $a' = gag^{-1}$.

Očitno je konjugiranost ekvivalenčna relacija na G. Ta relacija na G porodi razpad množice G na ekvivalenčne razrede. Imenujemo jih konjugiranostni razredi. Če je grupa G končna, velja $|G| = \sum_i |R_i|$, kjer so R_i konjugiranostni razredi. To formulo bomo preoblikovali, da bo dobila želeno obliko. Za poljuben element $a \in G$ naj $R(a)$ označuje konjugiranostni razred, ki mu a pripada, torej $R(a) = \{gag^{-1} \mid g \in G\}$. Vpeljimo še množico $C(a) = \{g \in G \mid ag = ga\}$ vseh elementov G, ki komutirajo z a. Imenujemo jo centralizator elementa a. Poleg elementa a očitno vsebuje tudi vse elemente iz centra $Z(G)$ grupe G.

Lema 5.9. *Za vsak element a iz grupe G je njegov centralizator $C(a)$ podgrupa G in velja $|R(a)| = [G : C(a)]$.*

Dokaz. Očitno je, da je $C(a)$ podgrupa. Za poljubna $g, h \in G$ velja $gC(a) = hC(a)$ natanko tedaj, ko je $g^{-1}h \in C(a)$, torej ko je $g^{-1}ha = ag^{-1}h$. To pa lahko preoblikujemo v $gag^{-1} = hah^{-1}$. Torej velja $gag^{-1} = hah^{-1} \Leftrightarrow gC(a) = hC(a)$. To pa pomeni, da je $gag^{-1} \mapsto gC(a)$ dobro definirana injektivna preslikava iz $R(a)$ v množico vseh odsekov G po podgrupi $C(a)$. Ker je ta preslikava očitno surjektivna, smo na koncu dokaza. □

Omenimo še, da če je $a \in Z(G)$, je očitno $R(a) = \{a\}$ in $C(a) = G$. Velja tudi $a \in Z(G) \Leftrightarrow |R(a)| = 1$. Sedaj lahko prejšnjo enakost zapišemo kot $|G| = |Z(G)| + \sum_j |R_j|$, kjer so R_j konjugiranostni razredi z več kot enim elementom, torej razredi, katerih elementi ne ležijo v centru. Sedaj uporabimo še prejšnjo lemo.

Izrek 5.10.

Naj bo G končna grupa. Potem obstajajo taki $a_j \in G/Z(G)$, da velja $|G| = |Z(G)| + \sum_j [G : C(a_j)]$.

Tej enakosti pravimo razredna formula.

5.3 Cauchyjev izrek

Naj bo G končna grupa. Po Lagrangevem izreku je red vsakega elementa iz G število, ki deli red G. Ali velja tudi obratno? V splošnem ne, saj če G ni ciklična grupa, potem ne vsebuje elementa reda $|G|$. Vendar pa se izkaže, da je odgovor pritrdilen, če je n praštevilo.

Izrek 5.11 (Cauchy)**.**

Naj bo G končna grupa. Če praštevilo p deli $|G|$, potem G vsebuje element reda p.

Dokaz. Izrek dokažimo z indukcijo na $n = |G|$. Če je $p = n$, potem je G ciklična grupa in 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 in če je $p \mid |Z(G)|$, potem smo že končali. Predpostavimo torej, da p ne deli $|Z(G)|$. Iz razredne formule sledi, da p ne deli $[G : C(a_j)]$ za neki $a_j \in G/Z(G)$. Po Lagrangu je $n = [G : C(a_j)] \cdot |C(a_j)|$, zato mora p deliti $|C(a_j)|$. Ker pa je $C(a_j)$ prava podgrupa G, dokaz sledi iz indukcijske predpostavke.
Oglejmo si še primer, ko G je Abelova. Ker $|G|$ ni praštevilo, mora G po eni izmed posledic vsebovati kako pravo netrivialno podgrupo N. Zaradi komutativnosti G velja $N \lhd G$ in zato po Lagrangu

$|G| = |G/N| \cdot |N|$. Če je $p \mid N$, potem smo po indukcijski predpostavki že končali. Naj bo torej $p \mid |G/N|$. Ker ima G/N manj kot n elementov, po indukcijski predpostavki vsebuje element aN, ki ima red p. Po posledici 5.3 (d) je $a \in G$ element reda $m = kp$ in je zato a^k element reda p. □

Definicija 5.2. Naj bo p praštevilo. Grupa G se imenuje p-grupa, če je red vsakega njenega elementa potenca števila p.

Posledica 5.12. *Končna grupa G je p-grupa natanko tedaj, ko je $|G| = p^m$ za neki $m \in \mathbb{N}$.*

Zgled 5.1. *Primeri p-grup so ciklične grupe $\mathbb{Z}_p$, $\mathbb{Z}_{p^2}$ in tako naprej. Prav tako sta kvaternionska grupa Q in diedrska grupa D_8 2-grupi. Direktni produkt p-grup je spet p-grupa, enako velja tudi za podgrupe p-grup.*

5.4 Delovanja grup

Definicija 5.3. Grupa G deluje na množici X, če obstaja taka preslikava iz $G \times X$ v X, ki vsakemu paru (a, x) priredi element $a \cdot x$, da velja:
- $a \cdot (b \cdot x) = (ab)x$ za vse $a, b \in G$ in $x \in X$.
- $1 \cdot x = x$ za vsak $x \in X$.

Tej preslikavi rečemo delovanje G na X.

Zgled 5.2. *Navedimo nekaj zgledov delovanja.*
1. *G deluje na G z običajnim množenjem.*
2. *G deluje na G s konjugiranjem: $a \cdot x = axa^{-1}$.*
3. *Naj bo $H \leq G$ in X množica vseh odsekov xH za $x \in G$. Potem G deluje na X kot $a \cdot xH = (ax)H$.*
4. *G deluje na množici vseh njenih podgrup kot $a \cdot K = aKa^{-1}$.*
5. *Grupa S_n deluje na $\{1, \ldots, n\}$ kot $\sigma \cdot i = \sigma(i)$.*
6. *Grupa $\mathrm{GL}_n(\mathbb{R})$ deluje na $\mathbb{R}^n$ kot $A \cdot v = Av$.*
7. *Trivalno delovanje: $a \cdot x = x$.*

Definicija 5.4. Naj G deluje na X. Orbita elementa $x \in X$ je množica $G \cdot x = \{a \cdot x \mid a \in G\}$, stabilizator elementa $x \in X$ pa množica $G_x = \{a \in G \mid a \cdot x = x\}$.

Zgled 5.3. *Naj G deluje nase s konjugiranjem. Potem je orbita $G \cdot x = R(x)$ in stabilizator $G_x = C(x)$.*

Hitro se da pokazati, da je stabilizator vselej podgrupa: $G_x \leq G$. S predpisom $x \sim y \Leftrightarrow x = a \cdot y$ za nek $a \in G$ je definirana ekvivalenčna relacija na X. Ekvivalenčni razred, v katerem leži x, je orbita $G \cdot x$. V podpoglavju o razredni formuli smo izpeljali rezultat (lemo), ki nam je dala enakost $|R(x)| = [G : C(x)]$. Sedaj lahko izpeljemo njeno posplošitev.

Lema 5.13. *Naj G deluje na X. Potem je $|G \cdot x| = [G : G_x]$ za vse $x \in X$.*

Dokaz. Za vse $a, b \in G$ je

$$\begin{aligned} a \cdot x = b \cdot x &\Leftrightarrow b^{-1}a \cdot x = x \\ &\Leftrightarrow b^{-1}a \in G_x \\ &\Leftrightarrow aG_x = bG_x. \end{aligned}$$

Sedaj ponovno definiramo preslikavo $a \cdot x \mapsto a \cdot G_x$ iz množice $G \cdot x$ v množico vseh odsekov po G_x in po prejšnjem razmisleku je ta preslikava injektivna in dobro definirana. Seveda pa je tudi surjektivna. To je lema o orbiti in stabilizatorju. □

Izrek 5.14.

Naj grupa G deluje na končni množici X. Označimo z Z množico vseh $x \in X$, za katere velja $a \cdot x = x$ za vse $a \in G$. Potem obstajajo taki $x_1, \ldots, x_m \in X \setminus Z$, da je $|X| = |Z| + \sum_{j=1}^{m} [G : G_{x_j}]$. Če je G končna p-grupa, je $|X| \equiv |Z| \pmod{p}$.

Dokaz. Dokaz poteka skoraj enako kot v razdelku o razredni formuli. Opazimo, da je $x \in Z \Leftrightarrow |G \cdot x| = 1$. Orbite so ekvivalenčni razredi, zato je $|X| = |Z| + \sum_{j=1}^{m} |G \cdot x_j|$, kjer smo uporabili prejšnjo lemo. Če je G končna p-grupa, potem je $|G \cdot x| = [G : G_{x_j}] = \frac{|G|}{|G_{x_j}|} = p^l$ za $l \in \mathbb{N}$, zato je $p \mid |X| - |R|$. □

5.5 Izreki Sylowa

Po Lagrangevem izreku vemo, da če je H podgrupa G, potem velja $|H| \mid |G|$. Kljub temu, da v splošnem obrat te trditve ne velja, pa iz Cauchyjevega izreka vemo, da če je p praštevilo in p deli $|G|$, potem G vsebuje grupo reda p. Ali lahko gremo še dlje?

Zgled 5.4. *Vzemimo alternirajočo grupo A_4 z redom $|A_4| = 12$. Pokažemo lahko, da A_4 ne vsebuje grupe, ki bi imela red 6.*

Naj bo $H \leq G$. Množici $N_G(H) = \{a \in G \mid aHa^{-1} = H\}$ pravimo normalizator H. Očitno velja $H \lhd G \Leftrightarrow N_G(H) = G$, izkaže pa se tudi, da je normalizator H podgrupa v G in velja $H \lhd N_G(H) \leq G$.

Definicija 5.5. Naj bo G končna grupa. Njena podgrupa $H \leq G$ je p-podgrupa, če je $|H| = p^l$ za neki $l \geq 0$. Naprej; H je p-podgrupa Sylowa, če je $|H| = p^k$ in p^{k+1} ne deli $|G|$.

Izrek 5.15 (Izreki Sylowa**).**

Naj bo G končna grupa in p praštevilo, ki deli $|G|$.

1. *Če p^l deli $|G|$, potem G vsebuje vsaj eno p-podgrupo reda p^l.*
2. *Vsaka p-podgrupa je vsebovana v kakšni p-podgrupi Sylowa.*
3. *Poljubni p-podgrupi Sylowa sta si konjugirani.*
4. *Število vseh p-podgrup Sylowa deli red $|G|$.*
5. *Število vseh p-podgrup Sylowa je oblike $mp + 1$ za $m \geq 0$.*

Dokaz. Dokaz točke (1): ponovno naredimo dokaz po indukciji na $|G| = n$, torej naj trditev velja za vse grupe z manj kot n elementi. Najprej obravnavamo primer, ko p ne deli $|Z(G)|$. Potem po razredni formuli obstaja tak $x_j \in G$, da p ne deli $[G : C(x_j)]$. Po Lagrangu je $n = |G| = |G : C(x_j)||C(x_j)|$ in ker je $p^l \mid n$, sledi $p^l \mid |C(x_j)|$. Ker je $C(x_j)$ prava podgrupa, moramo le še uporabiti indukcijsko predpostavko in smo končali. Obravnavajmo še primer $p \mid |Z(G)|$. Potem po Cauchyjevem izreku obstaja tak $c \in Z(G)$, da je $c \neq 1$ in $c^p = 1$. Potem je $\langle c \rangle \lhd G$ in velja $|G/\langle c \rangle| = \frac{|G|}{p} < m$ ter $p^{l-1} \mid |G/\langle c \rangle|$, zato lahko uporabimo indukcijsko predpostavko ima $G/\langle c \rangle$ podgrupo reda p^{l-1} oblike $H/\langle c \rangle$ za $\langle c \rangle \leq H \leq G$. Potem je $|H| = |H/\langle c \rangle| \cdot |\langle c \rangle| = p^{l-1} \cdot p = p^l$ in H je iskana podgrupa.
Dokaz točk (2) in (3): naj bo S p-podgrupa Sylowa in $X = \{xS \mid x \in G\}$. Definirajmo delovanje neke p-podgrupe H na X kot $a \cdot xS = (ax)S$ za $a \in H$ in $x \in G$. Definirajmo Z kot množico vseh takih odsekov xS, da je $a \cdot xS = xS$ za vsak $a \in H$. Ker je H p-grupa, velja $|X| \equiv |Z| \pmod{p}$. Ker je po Lagrangu $|X| = |G|/|S|$ in p ne deli X, potem p tudi ne deli Z. Torej Z ni prazna in obstaja $xS \in Z$. Torej za vsak $a \in H$ velja $axS = xS$, od tod pa sledi $x^{-1}ax \in S$ za vsak $a \in H$. Takoj dobimo $H \subseteq xSx^{-1}$ in očitno je $|xSx^{-1}| = |S|$. Torej je xSx^{-1} taka p-podgrupa, ki vsebuje H. Od tod takoj sledi tudi točka (3), torej če vzamemo, da je H p-podgrupa Sylowa.
Dokaz točke (4): naj bo Y množica vseh p-podgrup Sylowa, torej $Y = \{xSx^{-1} \mid x \in G\}$. Definirajmo delovanje G na Y s konjugiranjem: $a \cdot T = aTa^{-1}$ za vsak $a \in G$. Potem je orbita S kar cela množica Y, njen stabilizator pa je normalizator $N_G(S) = \{a \in G \mid aSa^{-1} = S\}$. Po lemi o stabilizatorju in orbiti je $|G| = |Y||N_G(S)|$, torej $|Y| \mid |G|$ in smo dokazali.
Dokaz točke (5): naj S deluje na Y kot prej, torej $a \cdot T = aTa^{-1}$ za $a \in S$. Naj bo W množica vseh elementov $T \in Y$, da je $a \cdot T = T$ za vsak $a \in S$. To je ekvivalentno temu, da je $S \subseteq N_G(T)$ in zato je $S \in W$. Vzemimo sedaj nek $T \in W$. S in T sta p-podgrupi Sylowa grupe $N_G(T)$. Torej sta si S in T konjugirani in zato je $S = aTa^{-1}$ za neki $a \in N_G(T)$. Ker pa je $aTa^{-1} = T$, je $S = T$ in zato je $W = \{S\}$. Sedaj pa dobimo $|Y| \equiv |W| = 1 \pmod{p}$. □

Zgled 5.5. *Denimo, da je $|G| = pq$, kjer sta p in q praštevili in $p < q$. Predpostavimo še, da p ne deli $q - 1$. Potem obstaja natanko ena p-podgrupa Sylowa in natanko ena q-podgrupa Sylowa. Poimenujmo ti grupi M in N. Očitno sta M in N podgrupi edinki. Ker je $|M| = p$, $|N| = q$ in $|M \cap N|$ deli $|M|$ in $|N|$, mora biti $|M \cap N| = \{1\}$. Hkrati lahko uporabimo dejstvo, da imata M in N praštevilsko moč in sta zato ciklični grupi; $M = \langle a \rangle$ in $N = \langle b \rangle$. Ker je presek edink M in N trivialen, vsak element iz M komutira z vsakim elementom iz N. Potem sledi $(ab)^{pq} = 1$ in takoj lahko pokažemo, da je red tega elementa kar $pq = |G|$. Torej je grupa G ciklična.*

Zanima nas problem klasifikacije končnih grup. Edina grupa (do izomorfizma natančno) z dvema elementoma je na primer $\mathbb{Z}_2$, edina s tremi elementi pa $\mathbb{Z}_3$. Hitro lahko pokažemo, da je poljubna grupa $G = \{1, a, b, c\}$ s štirimi elementi izomorfna bodisi $\mathbb{Z}_4$ bodisi $\mathbb{Z}_2 \oplus \mathbb{Z}_2$. Res, če ima vsaj eden od a, b, c red 4, potem je $G \cong \mathbb{Z}_4$, sicer pa imajo a, b, c vse red 2 in hitro sledi, da je v tem primeru $G \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2$. Vsaka grupa s 5 elementi je izomorfna $\mathbb{Z}_5$, saj je 5 preštevilo. Omenimo še, da je vsaka grupa s 6 elementi izomorfna $\mathbb{Z}_3 \oplus \mathbb{Z}_2$ ali S_3, vsaka grupa s 7 elementi je izomorfna $\mathbb{Z}_7$, vsaka grupa z 8 elementi pa $\mathbb{Z}_8$, $\mathbb{Z}_4 \oplus \mathbb{Z}_2$, $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$, D_8 ali Q.

Z naraščanjem števila elementov ta problem postaja čedalje bolj zahteven. Omejimo se na končne enostavne grupe. Vemo že, da so te lahko oblike $\mathbb{Z}_p$, kjer je p praštevilo, ali pa na primer alternirajoče grupe A_n za $n \geq 5$. Grupa A_5 je pravzaprav najmanjša nekomutativna enostavna grupa. Izkaže se, da lahko končne enostavne grupe klasificiramo v 18 neskončnih družin in 26 izjem, ki jim pravimo sporadične grupe. Največja izmed teh se imenuje monster group in ima približno $8 \cdot 10^{55}$ elementov. To pa so tudi vse. Te grupe imajo mnoge zanimive lastnosti - ena izmed njih je recimo ta, da imajo vse sodi red.

5.6 Končne Abelove grupe

Poznamo že ciklične grupe $\mathbb{Z}_n$ in njihove direktne vsote. Izkaže se, da so take oblike prav vse končne Abelove grupe. V tem razdelku obravnavamo aditivne grupe $(G, +)$, v katerih velja $m \cdot a = 0$ natanko tedaj, ko red elementa a deli m.

Lema 5.16. *Naj bo $|G| = mn$, kjer sta si m in n tuji števili. Naj bo $H = \{x \in G \mid mx = 0\}$ in $K = \{x \in G \mid nx = 0\}$. Potem sta H in K podgrupi in $G = H \oplus K$.*

Dokaz. Očitno sta H in K res podgrupi. Če sta m in n tuji, potem obstajata $u, v \in \mathbb{Z}$, da je $um + vn = 1$. Torej je

$$x = 1 \cdot x = u(mx) + v(nx)$$

in je $G = H + K$. Dokazati moramo še $H \cap K = \{0\}$. Če je $x \in H \cap K$, potem je $mx = nx = 0$ in iz zgornje enačbe takoj sledi $x = 0$. □

Opomba. Iz te leme takoj sledi, da imamo razcep $\mathbb{Z}_6 = \mathbb{Z}_3 \oplus \mathbb{Z}_2$, saj sta si števili 3 in 2 tuji.

Lema 5.17. *Denimo, da je $|G| = p_1^{k_1} \dots p_r^{k_r}$, kjer so p_i paroma različna praštevila. Potem je $G = H_1 \oplus H_2 \oplus \cdots \oplus H_r$, kjer je $|H_i| = p_i^{k_i}$ za vsak $i = 1, \dots, r$.*

Z zgornjima lemama lahko podamo razcep končnih Abelovih grup, ki imajo na primer red $42 = 2 \cdot 3 \cdot 7$. Res, če je $|G| = 42$, potem je $G = \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_7$. Kaj pa na primer $|G| = 16$? Odslej se osredotočimo na p-grupe.

Lema 5.18. *Naj bo G p-grupa. Potem je G ciklična natanko tedaj, ko vsebuje samo eno podgrupo reda p.*

Dokaz. ($\Rightarrow$) Naj bo G izomorfna $\mathbb{Z}_{p^n}$. Iz izreka 4.11 sledi, da so vse podgrupe $\mathbb{Z}_{p^n}$ oblike $p^k\mathbb{Z}_{p^n}$, kjer je $k = 0, 1, \dots, n$, torej je trditev v to smer že dokazana. Dokažimo še obrat ($\Leftarrow$). Denimo, da G vsebuje eno samo podgrupo reda p in jo poimenujmo N. Sedaj naredimo indukcijo po $|G| = n$: če je $n = p$, je to očitno. Predpostavimo torej, da rezultat velja za vse grupe z manj elementi. Takoj lahko vidimo, da je $N = \{x \in G \mid px = 0\}$ in zato je N jedro endomorfizma $\varphi : G \to G$, podanega s predpisom $\varphi(x) = px$. Po izreku o izomorfizmu je $G/N \cong \operatorname{im}\varphi$. Ker je $N \neq \{0\}$, imata G/N in $\operatorname{im}\varphi$ manj elementov kot G. Torej ima φ po Cauchyjevem izreku vsaj eno, a ne več kot eno podgrupo reda p. Zato je po indukcijski predpostavki ciklična in je ciklična tudi grupa G/N. Naj bo $a \in G$ tak, da je G generirana z elementom $a + N$. Za vsak $g + N$, kjer je $g \in G$, obstaja tak $k \in \mathbb{Z}$, da je $g + N = k(a + N) = ka + N$. Zato je $g - ka \in N$ in $G = \langle a \rangle + N$. Ker je $|G| > p = |N|$, je $\langle a \rangle$ netrivialna podgrupa grupe G. Kot p-grupa ima po Cauchyjevem izreku element reda p. Toda potem je $N \subseteq \langle a \rangle$ in zato $G = \langle a \rangle$. □

Lema 5.19. *Naj bo G p-grupa. Če je C njena ciklična podgrupa, ki ima med vsemi cikličnimi grupami največji red, potem G vsebuje tako podgrupo K, da je $G = C \oplus K$.*

Dokaz. Predpostavimo, da G ni ciklična in da lema velja za vse p-grupe z nižjim redom kot G. Po lemi ima G vsaj dve podgrupi reda p, C pa natanko eno. Naj bo N podgrupa reda p, ki ni vsebovana v C. Potem je $C \cap N \geq N$ in zato $C \cap N = \{0\}$. Definiramo preslikavo $\varphi : C \to C + N/N$ s predpisom $\varphi(c) = c + N$. Ta preslikava je očitno homomorfizem in surjekcija in ker je $C \cap N = \{0\}$, tudi injekcija. Torej je $C \cong C + N/N$ in $C + N/N$ je ciklična podgrupa G/N enakega reda kot C. Trdimo, da ima ciklična grupa $C + N/N$ izmed vseh cikličnih podgrup grupa G/N največji red.

To je res, saj je največji red cikličnih podgrup grupe enak največjemu redu elementov te grupe, red vsakega elementa $x \in G$ pa je kvečjemu večji kot red elementa $x+N \in G/N$. Po predpostavki zato obstaja taka podgrupa L grupe G/N, da je grupa G/N direktna vsota svojih podgrup $C+N/N$ in L. Nato pa je po izreku 4.11 $L = K/N$ za neko podgrupo $K \leq G$, ki vsebuje N. Iz enakosti $G/N = (C+N)/N \oplus K/N$ takoj izpeljemo, da je $G = C+N+K = C+K$. Dokazati moramo še, da je $C \cap K = \{0\}$. Denimo nasprotno; izberimo neničeln element $x \in C \cap K$. Iz $C \cap N = \{0\}$ sledi $x \notin N$, zato je $x+N \in (C+N)/N \cap K/N$. Protislovje. □

Naj bo G p-grupa, torej $G = C \oplus K$. Nadaljujmo s tem postopkom in dobimo $K = C' \oplus K'$ in tako naprej. Ta postopek se mora nekje končati, saj je $|K| > |K'| > |K''| > \dots$ S tem pa smo že pravzaprav dokazali naslednji izrek.

Izrek 5.20.

Vsaka končna Abelova grupa je direktna vsota cikličnih podgrup. Če ni trivialna, potem te ciklične podgrupe lahko izberemo tako, da je red vsake potenca nekega praštevila.

Opomba. Podobne argumente uporabimo za dokaz trditve, da lahko vsako matriko nad algebraično ž zaprtim poljem predstavimo v Jordanski formi[1].

Naj bo G končna Abelova grupa, torej $G = H_1 \oplus \dots \oplus H_r$, kjer so H_i p_i-grupe. Naj bo $G \cong G'$, $G' = H_1' \oplus \dots \oplus H_s'$. Vzemimo izomorfizem $\varphi : G \to G'$ in vidimo, da je $r = s$ ter $\varphi(H_1) = H_1'$, $\varphi(H_2)H_2'$ in tako dalje. Poleg tega lahko p-grupo G zapišemo kot direktno vsoto cikličnih p-grup in zato je

$$G \cong \mathbb{Z}_{p^{k_1}} \oplus \mathbb{Z}_{p^{k_2}} \oplus \dots \oplus \mathbb{Z}_{p^{k_r}},$$

kjer je $k_1 \geq k_2 \geq \dots \geq k_r$. Kdaj pa je

$$\mathbb{Z}_{p^{k_1}} \oplus \mathbb{Z}_{p^{k_2}} \oplus \dots \oplus \mathbb{Z}_{p^{k_r}} \cong \mathbb{Z}_{p^{l_1}} \oplus \mathbb{Z}_{p^{l_2}} \oplus \dots \oplus \mathbb{Z}_{p^{l_s}}?$$

Izrek 5.21.

Naj bo p praštevilo. Če so $k_1 \geq k_2 \geq \dots \geq k_r$ in $l_1 \geq l_2 \geq \dots \geq l_s$ taka, da je

$$\mathbb{Z}_{p^{k_1}} \oplus \mathbb{Z}_{p^{k_2}} \oplus \dots \oplus \mathbb{Z}_{p^{k_r}} \cong \mathbb{Z}_{p^{l_1}} \oplus \mathbb{Z}_{p^{l_2}} \oplus \dots \oplus \mathbb{Z}_{p^{l_s}},$$

potem je $k_1 = l_1,\ k_2 = l_2,\ \dots,\ k_r = l_r$ in $r = s$.

Dokaz. Obe grupi imata red $p^{k_1}p^{k_2}\dots p^{k_r} = p^{l_1}p^{l_2}\dots p^{l_s}$, zato je

$$k_1 + k_2 + \dots + k_r = l_1 + l_2 + \dots + l_s = n.$$

Če je $n = 1$, je izrek očiten, zato nadaljujmo z indukcijo po n. Iz $p\mathbb{Z}_{p^m} \cong \mathbb{Z}_{p^{m-1}}$ sledi

$$\mathbb{Z}_{p^{k_1-1}} \oplus \mathbb{Z}_{p^{k_2-1}} \oplus \dots \oplus \mathbb{Z}_{p^{k_u-1}} \cong \mathbb{Z}_{p^{l_1-1}} \oplus \mathbb{Z}_{p^{l_2-1}} \oplus \dots \oplus \mathbb{Z}_{p^{l_v-1}},$$

kjer je u največje število, da je $k_u > 1$ (podobno za v). Po indukcijski predpostavki je $k_1 = l_1,\ k_2 = l_2,\ \dots,\ k_u = l_u$ in $u = v$. Dokazati moramo še, da je $r = s$, kar pa sledi iz začetne vsote

$$k_1 + k_2 + \dots + k_u + \dots + k_r = l_1 + l_2 + \dots + l_v + \dots + l_s = n$$

in $k_{u+1} = \dots = k_r = l_{v+1} = \dots = l_s = 1$. □

[1] glej: angleška knjiga

Zgled 5.6. *Naj bo G Abelova grupa in $|G| = 200 = 2^3 \cdot 5^2$. Za G imamo omejeno izbiro grup, saj so edine 5-grupe reda 25 enake $\mathbb{Z}_5 \oplus \mathbb{Z}_5$ ali $\mathbb{Z}_{25}$, grupe reda 8 pa $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus Z_2$, $\mathbb{Z}_4 \oplus \mathbb{Z}_2$ ali pa $\mathbb{Z}_8$. Grupa G je torej poljubna kombinacija navedenih možnosti.*

Opomba. Ta izrek na končnih grupah lahko do neke mere posplošimo na končno generirane Abelove grupe: $\mathbb{Z} \oplus \mathbb{Z} \oplus \cdots \oplus \mathbb{Z}$.

6 Komutativni kolobarji

6.1 Deljivost v kolobarju polinomov

V tem podpoglavju bomo obravnavali deljivost v kolobarju $F[X]$ polinomov nad poljem F.

Izrek 6.1.

Naj bosta $f(X), g(X) \in F[X]$. Potem obstajata taka (enolično določena) polinoma $q(X), r(X) \in F[X]$, da je $f(X) = g(X)q(X) + r(X)$, kjer je $r = 0$ ali pa $\mathrm{st}(r(X)) < \mathrm{st}(q(X))$.

Dokaz. Z indukcijo. □

Pravimo, da $g(X)$ deli $f(X)$, če obstaja nek polinom $q(X) \in F[X]$, da je $f(X) = g(X)q(X)$.

Posledica 6.2. *Element $a \in F$ je ničla polinoma $f(X) \in F[X]$ natanko tedaj, ko linearni polinom $(X - a)$ deli $f(X)$.*

Dokaz. Uporabimo izrek o deljenju in zapišemo $f(X) = (X - a)q(X) + r(X)$, kjer je $r(X) = c$ konstanten polinom. Potem je $f(a) = c = 0$ natanko tedaj, ko $(X - a)$ deli $f(X)$. □

Definicija 6.1. Polinom $f(X) \in F[X]$ je razcepen, če ga lahko zapišemo kot produkt dveh nekonstantnih polinomov nižje stopnje. Nasprotno pa je $f(X)$ nerazcepen, če ni razcepen in je stopnje vsaj 1.

Ta definicija nerazcepnosti polinoma $f(X)$ je ekvivalentna naslednji:

1. f ni konstanten.
2. Iz $f(X) = g(X)h(X)$ sledi, da je eden od polinomov $g(X)$ in $h(X)$ konstanten.

Lema 6.3. *Naj bo $f(X) \in F[X]$.*
- *Če je $f(X)$ linearen, je nerazcepen.*
- *Če je $f(X)$ nerazcepen in stopnje vsaj 2, potem nima ničle.*
- *Če je $f(X)$ stopnje 2 ali 3 in nima ničel, je nerazcepen.*

Dokaz. Polinom $f(X) = X^4 + 2X^2 + 1 \in \mathbb{R}[X]$ nima ničel v $\mathbb{R}$, a je kljub temu razcepen kot $f(X) = (X^2 + 1)^2$. □

Izrek 6.4 (Osnovni izrek algebre**).**

Edini nerazcepni polinomi v $\mathbb{C}[X]$ so linearni polinomi.

Opomba. Za dokaz glej analizo 2b ali uvod v geometrijsko topologijo.

Izrek 6.5.

Edini nerazcepni polinomi v $\mathbb{R}[X]$ so linearni in kvadratni polinomi oblike $aX^2 + bX + c$, kjer je $b^2 - 4ac < 0$.

Dokaz. Naj bo $p(X) \in \mathbb{R}[X]$ nerazcepen stopnje več od 2. Potem nima realne ničle, a po osnovnem izreku algebre ima kompleksno ničlo z. Potem pa je tudi $\overline{z}$ ničla, saj je $p(\overline{z}) = \overline{p(z)} = 0$. To pa pomeni, da lahko naš polinom zapišemo kot

$$p(X) = (X - z)(X - \overline{z})g(X) = (X^2 - (z + \overline{z})X + z\overline{z})g(X),$$

kjer je $g(X) \in \mathbb{C}[X]$. Ker pa je $(X^2 - (z + \overline{z})X + z\overline{z}) \in \mathbb{R}[X]$, mora biti tudi $g(X) \in \mathbb{R}[X]$, torej je $g(X)$ konstanten. Preostanek trditve je očiten. □

Definicija 6.2. Polinom $f_0(X) = a_0 + a_1X + \cdots + a_nX^n \in \mathbb{Z}[X]$ je primitiven, če je največji skupni delitelj $a_0, a_1, \ldots, a_n$ enak 1.

Drugače povedano: če obstaja praštevilo p, ki deli vse koeficiente a_i polinoma $f(X) \in \mathbb{Z}[X]$, potem je $f(X) = df_0(X)$, kjer je d največji skupni večkratnik koeficientov a_i.

Lema 6.6 (Gaussova lema)**.** *Produkt dveh primitivnih polinomov je primitiven polinom.*

Dokaz. Naj bosta $f_0(X), g_0(X) \in \mathbb{Z}[X]$ primitivna polinoma in denimo, da $f_0(X)g_0(X)$ ni primitiven. Tedaj obstaja praštevilo p, ki deli vse koeficiente tega polinoma, torej velja $f_0(X)g_0(X) \in p\mathbb{Z}[X] =: Y$. Na tem mestu uporabimo dejstvo $p\mathbb{Z}[X] \lhd \mathbb{Z}[X]$, ki ga je lahko dokazati. Potem v kvocientnem kolobarju $\mathbb{Z}[X]/Y$ velja $f_0(X)+Y \neq 0$, $g_0(X)+Y \neq 0$ in $(f_0(X)+Y)(g_0(X)+Y) = 0$. To pomeni, da ima ta kolobar delitelje niča. Po drugi strani pa velja $\mathbb{Z}[X]/p\mathbb{Z}[X] \cong \mathbb{Z}_p[X]$. Res, definiramo preslikavo $\varphi : \mathbb{Z}[X] \to \mathbb{Z}_p[X]$ s predpisom

$$\varphi(a_0 + a_1X + \cdots + a_nX^n) = [a_0] + [a_1]X + \cdots + [a_n]X^n$$

in to je očitno surjektiven homomorfizem z jedrom $\ker \varphi = p\mathbb{Z}$. Po prvem izreku o izomorfizmu je $\mathbb{Z}[X]/p\mathbb{Z}[X]$ homomorfen $\mathbb{Z}_p[X]$ in ker je $\mathbb{Z}_p$ polje, je $\mathbb{Z}[X]/p\mathbb{Z}[X]$ cel kolobar. To pa je v nasprotju s predpostavko, da ima ta kvocientni kolobar delitelje niča. □

Izrek 6.7.

Če nekonstantnega polinoma $f(X) \in \mathbb{Z}[X]$ ne moremo zapisati kot produkt dveh polinomov iz $\mathbb{Z}[X]$ nižje stopnje, potem je $f(X)$ nerazcepen nad $\mathbb{Q}$.

Dokaz. Naj bo $f(X) = g(X)h(X)$, kjer sta $g(X), h(X) \in \mathbb{Q}[X]$ in $kg(X), lh(X) \in \mathbb{Z}[X]$ za primerni konstanti $k, l \in \mathbb{N}$. Naj bo $f(X) = d_0f_0(X)$ za nek $d_0 \in \mathbb{N}$, kjer je $f_0(X) \in \mathbb{Z}[X]$ primitiven polinom. Podobno zapišemo tudi $kg(X) = d_1g_0(X)$ in $lh(X) = d_2h_0(X)$ za primitivna polinoma $g_0(X), h_0(X) \in \mathbb{Z}[X]$. Če to vstavimo v prvotno enačbo, dobimo $(kld_0)f_0(X) = (d_1d_2)g_0(X)h_0(X)$. Po Gaussovi lemi je zmnožek polinomov $g_0(X)h_0(X)$ primitiven, zato je $kld_0 = d_1d_2$. Posledično imamo $f_0(X) = g_0(X)h_0(X)$ in od tod $f(X) = (d_0g_0(X))h_0(X)$, torej imamo razcep $f(X)$ na faktorje iz $\mathbb{Z}[X]$ in je zato po predpostavki vsaj eden od faktorjev $g_0(X)$ in $h_0(X)$ konstanten. Od tod pa seledi, da je vsaj eden od $g(X)$ in $h(X)$ konstanten. S tem pa smo dokazali izrek. □

Izrek 6.8 (Eisensteinov kriterij)**.**

Naj bo $f(X) = a_nX^n + \cdots + a_1X + a_0 \in \mathbb{Z}[X]$, kjer $a_n \neq 0$ in $n \geq 1$. Če obstaja tako praštevilo p, tako da $p \mid a_i$ za $0 \leq i \leq n-1$, p ne deli a_n in p^2 ne deli a_0, potem je $f(X)$ nerazcepen nad $\mathbb{Q}$.

Dokaz. Denimo, da to ni res. Potem obstajata taka celoštevilska polinoma $g(X) = b_r X^r + \cdots + b_1 X + b_0$ in $h(X) = c_s X^s + \cdots + c_1 X + c_0$, tako da je $f(X) = g(X)h(X)$, torej $r + s = n$. Ker p deli $a_0 = b_0 c_0$, p^2 pa ne, lahko predpostavimo, da p deli b_0, ne pa c_0. Ker je $a_n = b_r c_s$, pa p ne deli b_r. Zato obstaja tak $k \in \mathbb{N}$, da p deli vse koeficiente b_i do b_k. Potem pa si oglejmo $a_k = b_0 c_k + b_1 c_{k-1} + \cdots + b_k c_0$. Vemo, da p deli a_k in koeficiente $b_0, \ldots, b_{n-1}$, ne deli pa b_k in c_0, s čimer pridemo v protislovje. □

Zgled 6.1. *Naj bo $n \in \mathbb{N}$ in p praštevilo. Potem je po Eisensteinu $f(X) = X^n - p$ nerazcepen polinom v $\mathbb{Q}$.*

Zgled 6.2. *Naj bo p praštevilo in $\Phi_p(X) = X^{p-1} + \cdots + X + 1$. Potem je $\Phi_p(X)(X-1) = X^p - 1$. Če X zamenjamo z $X+1$, dobimo $\Phi_p(X+1) = X^{p-1} + \binom{p}{1} X^{p-2} + \cdots + \binom{p}{p-1}$. Ponovno uporabimo Eisensteinov kriterij in ugotovimo, da je polinom $\Phi_p(X+1)$ nerazcepen nad $\mathbb{Q}$, torej mora biti tudi $\Phi_p(X)$ nerazcepen nad $\mathbb{Q}$.*

Definicija 6.3. Kompleksno število $\omega = e^{2\pi i \frac{k}{n}}$ je primitivni n-ti koren enote, če je $0 \leq k < n - 1$ in sta n in k tuji. Potem definiramo n-ti ciklotomični polinom definiran kot $\Phi_n(X) = \prod(X - \omega)$, kjer produkt teče po vseh n-tih primitivnih korenih enote.

Izkaže se, da je $\Phi_n(X) \in \mathbb{Z}[X]$ in je nerazcepen nad $\mathbb{Q}$.

6.2 Deljivost in glavni ideali

Definicija 6.4. Naj bo K komutativen kolobar.

- Element $b \neq 0$ deli element a, če je $a = qb$ za nek $q \in K$. To relacijo označujemo $b \mid a$.
- Elementa $a, b \neq 0$sta asociirana, če velja $a \mid b$ in $b \mid a$.
- Element $p \in K$ je nerazcepen, če je $p \neq 0$, p ni obrnljiv in iz $p = ab$ sledi, da je a ali b obrnljiv.
- Naj bosta $a, b \in K$ in naj ne bosta oba ničelna. Element $d \neq 0$ je največji skupni delitelj a in b, če velja $d \mid a$, $d \mid b$ in iz $c \mid a$, $c \mid b$ sledi $d \mid c$.

Od sedaj naprej se bomo posvetili celim kolobarjem, torej komutativnim kolobarjem brez deliteljev niča. Primeri teh so recimo $\mathbb{Z}$, $F[X]$, $\mathbb{Z}[i]$ ali pa $F[X, Y]$.

Definicija 6.5. Ideal, generiran z enim samim elementom, se imenuje glavni ideal.

V komutativnem kolobarju K je glavni ideal, generiran z $a \in K$, enak $(a) = Ka = \{ax \mid x \in K\}$. Omenimo, da velja:

- $b \mid a$ natanko tedaj, ko je $(a) \subseteq (b)$,
- $(a) = 0$ natanko tedaj, ko je $a = 0$,
- $(a) = K$ natanko tedaj, ko je K obrnljiv,
- a in b sta asociirana natanko tedaj, ko je $(a) = (b)$.

Lema 6.9. *Naj bo K cel kolobar. Elementa $a, b \in K$ sta asociirana natanko tedaj, ko obstaja tak obrnljiv element $u \in K$, da je $b = ua$.*

Dokaz. Dokažimo v desno ($\Rightarrow$). Naj bo $a \mid b$ in $b \mid a$, torej $b = au$ in $a = bv$. Od tod pa sledi $b = buv$ in posledično $b(1 - uv) = 0$. Ker smo v celem kolobarju, velja $uv = 1$ in zaradi komutativnosti je $u \in K$ obrnljiv. □

Zgled 6.3. *V kolobarju $\mathbb{Z}$ sta si elementa a, b asociirana natanko tedaj, ko velja $a = \pm b$, v $F[X]$ pa sta $f(X)$ in $g(X)$ asociirana natanko tedaj, ko je $f(X) = ug(X)$ za $u \in F^*$.*

Zgled 6.4. *V $\mathbb{Z}$ so vsi nerazcepni elementi oblike $\pm p$, kjer je p praštevilo. V kolobarju $F[X]$ pa nova definicija nerazcepnosti sovpada s staro.*

Zgled 6.5. *v $\mathbb{Z}[i]$ so $\pm 1, \pm i$ edini obrnljivi elementi. Izkaže se, da je element $2 = (1 - i)(1 + i)$ v tem kolobarju razcepen, element 3 pa ne. Res, če bi imeli $3 = zw$, potem bi sledilo $|z|^2|w|^2 = 9$. Denimo, da je $|z|^2 = 3$. Potem obstajata $u, v \in \mathbb{Z}$, tako da je $u^2 + v^2 = 3$, kar pa je protislovje.*

Ponovimo definicijo maksimalnega ideala, torej $I \subseteq K$, če je $I \lhd K$, $I \neq K$ in iz $I \subseteq J \subseteq K$, $J \lhd K$ sledi $I = J$ ali $J = K$. če je K komutativen, je K/I seveda polje.

Lema 6.10. *Naj bo K cel kolobar in neobrnljiv element $p \in K$, $p \neq 0$. Potem sta naslednji trditvi ekvivalentni.*

- *p je nerazcepen.*
- *(p) je maksimalen med glavnimi ideali.*

Dokaz. Druga trditev je ekvivalentna temu, da je $(p) \neq K$ in iz $(p) \subseteq (k)$ sledi bodisi $(a) = (p)$ bodisi $(a) = K$. To pomeni, da če p ni obrnljiv in je a tak, da je $p = ab$ za neki $b \in K$, potem je a obrnljiv ali pa velja $p = au$, kjer je u obrnljiv. Iz druge možnosti pa sledi, da je $b = u$ obrljiv, torej je ta trditev ekvivalentna temu, da če je $p = ab$, je bodisi a obrnljiv bodisi b obrnljiv. □

Naj večji skupni delitelj dveh elementov ne obstaja v vsakem kolobarju in tudi če obstaja, ni vedno enolično določen. Če sta d in d' največja skupna delitelja istega para elementov, potem sta si asociirana. Torej lahko največji skupni delitelj določimo do asociiranosti natančno. Po dogovoru v $\mathbb{Z}$ izberemo za največji skupni delitelj naravno število, v $F[X]$ pa monični polinom.

Končno generiran ideal, torej ideal, generiran z $a_1, \ldots, a_n \in K$, označujemo z $(a_1, \ldots, a_n)$. Trdimo, da velja $(a_1, \ldots, a_n) = (a_1) + (a_2) + \cdots + (a_n)$. Ker so $a_1, \ldots, a_n \in (a_1, \ldots, a_n)$, so $(a_1), \ldots, (a_n) \subseteq (a_1, \ldots, a_n)$ in zato $(a_1) + \cdots + (a_n) \subseteq (a_1, \ldots, a_n)$. Po drugi strani pa je tudi $(a_1) + \cdots + (a_n)$ ideal, ki vsebuje $a_1, \ldots, a_n$, zato je $(a_1, \ldots, a_n) \subseteq (a_1) + \cdots + (a_n)$. Torej je $(a_1, \ldots, a_n) = \{a_1x_1 + \cdots + a_nx_n \mid x_i \in K\}$

Zgled 6.6. *Oglejmo si ideal $(X, Y) = \{Xf(X, Y) + Yf(X, Y)\}$ v kolobarju $F[X, Y]$. To je kolobar vseh polinomov dveh spremenljivk v $F[X, Y]$ s konstantnim členom 0. Dokažimo, da ta ideal ni glavni. Če bi to bilo res, bi imeli $(X, Y) = (f(X, Y))$ za nek $f(X, Y) \in F[X, Y]$, torej bi obstajal nek $F[X, Y] \ni g(X, Y) = \sum g_i(X)Y^i$, tako da bi veljalo $X = f(X, Y)g(X, Y)$. To pa bi pomenilo, da je $f(X, Y) = f_0(X)$ odvisen samo od X-a. Analogno pridemo do zaključka, da je $f(X, Y) = \overline{f_0}(Y)$. To pa bi pomenilo, da imamo konstanten polinom $f(X, Y) = a \in F$, kar pa bi impliciralo $(f(X, Y)) = (a) = F[X, Y]$. Protislovje.*

Lema 6.11. *Naj bosta a, b elementa (ne oba ničelna) komutativnega kolobarja K. Če je (a, b) glavni ideal, potem največji skupni delitelj obstaja in je oblike $d = ax + by$ za neka $x, y \in K$.*

Dokaz. Naj bo $(a,b) = (d)$ za neki $d \in K$. Takoj dobimo, da d deli a in b. Iz $(a,b) = (d)$ sledi $d = ax + by$. Naj bo $c \mid a$ in $c \mid b$, torej $a = cz$ in $b = cw$. Potem je $d = c(zx + wy)$ in $c \mid d$. □

6.3 Glavni kolobarji

Definicija 6.6. Cel kolobar je glavni kolobar, če so vsi njegovi ideali glavni.

Dokaz. Kolobar $\mathbb{Z}$ je glavni, kolobar $F[X,Y]$ pa ne. □

Definicija 6.7. Cel kolobar K se imenuje evklidski kolobar, če obstaja taka funkcija $\delta : K \setminus \{0\} \to \mathbb{N} \setminus \{0\}$, da velja naslednje:

- Za vsaka a in b, kjer je $b \neq 0$, obstajata taka $q, r \in K$, da je $a = qb + r$ in je $r = 0$ ali $\delta(a) < \delta(b)$.
- $\delta(a) < \delta(ab)$ za vse $a, b \in K \setminus 0$.

Lema 6.12. *Vsak evklidski kolobar je glavni.*

Dokaz. Naj bo I ideal evklidskega kolobarja K. Predpostaviti smemo, da $I \neq \{0\}$. Izberemo $b \in I$ tako, da je $\delta(b) \leq \delta(x)$ za vse $x \in I$. Po konstrukciji je $(b) \subseteq I$. Vzemimo $a \in I$ in zapišemo $a = bq + r$, kjer je bodisi $r = 0$ bodisi $\delta(r) < \delta(b)$. Od tod sledi, da je $r = 0$ in $a = bq$, torej $a \in (b)$. □

Izrek 6.13.

Kolobarji $\mathbb{Z}$, $F[X]$ in $\mathbb{Z}[i]$ so evklidski (in posledično glavni).

Dokaz. Za prvega vzamemo funkcijo $\delta(a) = |a|$, za drugega $\delta(p(X)) = \mathrm{st}(p(X))$ in za tretjega $\delta(z) = |z|^2$. Nato dokazujemo po definiciji. □

Zgled 6.7. *Kolobar* $\left\{ m + n\frac{1+\sqrt{19}i}{2} \mid m, n \in \mathbb{Z} \right\}$ *je glavni, a ni evklidski.*

Izrek 6.14.

Naj bo $p \neq 0$ element glavnega kolobarja K. Naslednji pogoji so ekvivalentni:

1. *p je nerazcepen.*
2. *(p) je maksimalen.*
3. *$K/(p)$ je polje.*

Dokaz. Trditev sledi direktno iz prejšnje leme. □

Posledica 6.15. *Polinom $p(X) \in F[X]$ je nerazcepen natanko tedaj, ko je $F[X]/(p(X))$ polje.*

Izrek 6.16.

Naj bo K glavni kolobar in $a, b \in K$, ne oba 0. Potem največji skupni delitelj a in b obstaja in je oblike $d = ax + by$ za neka $x, y \in K$.

Spomnimo se Evklidove leme, ki nam pravi, da če praštevilo p deli ab, potem velja $p \mid a$ ali pa $p \mid b$. S to intuicijo vpeljimo naslednji pojem.

Definicija 6.8. Element p komutativnega kolobarja K se imenuje praelement, če velja naslednje:
- $p \neq 0$ in p ni obrnljiv.
- iz $p \mid ab$ sledi $p \mid a$ ali $p \mid b$ za poljubna $a, b \in K$.

Lema 6.17. *Vsak praelement je nerazcepen. V glavnem kolobarju pa velja tudi obratno.*

Dokaz. Najprej se lotimo prve trditve; naj bo p praelement in $p = xy$. Iz definicije praelementa sledi, da velja $p \mid x$ ali $p \mid y$. Brez škode za splošnost predpostavimo prvo in od tod $x = pu$, kjer je $u \in K$. Torej je $x = xyu$ in je torej $uy = 1$, od tod pa sledi, da je y obrnljv in p nerazcepen. Sedaj dokažimo še drugo trditev; naj bo K glavni kolobar in p nerazcepen. Denimo, da je $p \mid xy$. Če p ne deli x, sta si p in x tuja in je zato $pz + xw = 1$ za neka $z, w \in K$. Od tod pa sledi $pzy + xyw = y$ in zato $p \mid y$. □

Lema 6.18. *Naj bo K cel kolobar in $a \in K$ naj bo neničelen in neobrnljiv. Če a ni enak produktu nerazcepnih elementov, potem obstaja tako zaporedje elementov $a_1, a_2, a_3, \dots \in K$, da je $(a_1) \subsetneq (a_2) \subsetneq (a_3) \subsetneq \dots$*

Dokaz. Po predpostavki a ni nerazcepen, zato je enak $a = a_1 b_1$, kjer a_1 in b_1 nista obrnljiva. Naj bo a_1 tak, da ni enak produktu nerazcepnih elementov in imamo $(a) \subsetneq (a_1)$. Sedaj imamo podobno $a_1 = a_2 b_2$, kjer a_2 in b_2 nista obrnljivi, a_2 ni produkt razcepnih elementov in $(a_1) \subsetneq (a_2)$. Postopek ponavljamo v neskončnost. □

Definicija 6.9. Komutativni kolobar K je noetherski, če ne obstaja tako zaporedje idealov v K, da bi veljalo $I_1 \subsetneq I_2 \subsetneq I_3 \subsetneq \dots$

Lema 6.19. *Vsak glavni kolobar je noetherski.*

Dokaz. Naj bo $I_1 \subsetneq I_2 \subsetneq I_3 \subsetneq \dots$ zaporedje idealov v glavnem kolobarju K. Po predpostavki je $I_i = (a_i)$ za nek $a_i \in K$. Definiramo $I := \bigcup_{i=1}^{\infty} I_i$ in preprosto je pokazati, da je to ideal kolobarja I, torej je po predpostavki $I = (a)$ za nek element $a \in I$. Ker je $a \in \bigcup_{i=1}^{\infty} I_i$, obstaja $n \in \mathbb{N}$, da je $a \in I_n = (a_n)$. To pa pomeni, da je $I = (a) \subseteq I_n$ in od tod $I_n = I_{n+1} = \dots$, kar pa vodi v protislovje. □

Zadnji dve lemi nam torej povesta, da je v glavnem idealu vsak element, ki ni 0 in ni obrnljiv, produkt nerazcepnih elementov.

Opomba. Izkaže se, da je K noetherski natanko tedaj, ko so vsi njegovi ideali končno generirani. Primer noetherskega kolobarja, ki ni glavni, je recimo $F[X_1, \dots, X_n]$ za $n > 1$. Lahko pa gremo še naprej; kolobar $F[X_1, X_2, \dots]$ je cel, a ni noetherski.

Definicija 6.10. Cel kolobar K je kolobar z enolično faktorizacijo ali UFD, če za vsak $a \in K$, ki ni ničelen ali obrnljiv, velja naslednje:

- obstajajo taki nerazcepni elementi, da je $a = p_1 p_2 \dots p_n$.
- zapis v prvi točki je do asociiranost in vrstnega reda faktorjev enoličen.

To pomani, da če imamo v kolobarju z enolično faktorizacijo enačbo $a = p_1 \dots p_n = q_1 \dots q_m$, kjer so p_i in q_i nerazcepni, potem je $m = n$ in obstaja taka permutacija $\sigma \in S_n$, da sta si za vsak i elementa p_i in $q_{\sigma(i)}$ asociirana.

Izrek 6.20.

Vsak glavni kolobar je kolobar z enolično faktorizacijo.

Dokaz. Naj bo K glavni kolobar in neobnljiv element $a \in K$, za katerega velja $a \neq 0$. Vemo že, da lahko zapišemo $a = p_1 \dots p_n$, kjer so $p_1, \dots, p_n$ nerazcepni. Naj bo sedaj $a = p_1 \dots p_n = q_1 \dots q_m$, kjer so $q_1, \dots, q_m$ nerazcepni. Potem p_1 deli desno stran enačbe in ker je praelement (sledi iz nerazcepnosti), deli bodisi q_1 bodisi $q_2 \dots q_m$. Ta proces nadaljujemo in dobimo, da p_1 deli enega izmed q_i, naj bo brez škode za splošnost to kar q_1. To pomeni, da je $q_1 = p_1 u$ za neki $u \in K$. Ker je tudi q_1 nerazcepen, je u obrnljiv in sta p_1 in q_1 asociirana. Od tod pa iz začetne enačbe dobimo $p_2 \dots p_n = (uq_2) \dots q_m$ in ker je uq_2 prav tako nerazcepen, lahko z indukcijo po n pridemo do želenega zaključka. □

V tem razdelku smo dokazali, da so kolobarji $\mathbb{Z}$, $F[X]$ in $\mathbb{Z}[X]$ evklidski, zato glavni in posledično tudi z enolično faktorizacijo.

7 Ničle polinomov in razširitve polj

7.1 Algebraični in transcendentni elementi

Definicija 7.1. Naj bo a element razširitve E polja F. Če obstaja tak neničelen polinom $f(X) \in F[X]$, da je $f(a) = 0$, potem rečemo, da je a algebraičen nad F. Če pa a ni algebraičen nad F, pravimo, da je transcendenten.

Zgled 7.1. *Število $\sqrt{2}$ je algebraično nad $\mathbb{Q}$, števili e in π pa sta transcendentni.*

Definicija 7.2. Naj bo $a \in E$ algebraičen nad F. Moničnemu polinomu $p(X) \in F[X]$ pravimo minimalni polinom elementa a, če je $p(a) = 0$ in če ima $p(X)$ izmed vseh polinomov z ničlo a najmanjšo stopnjo.

Minimalni polinom algebraičnega elementa a res obstaja in je en sam. Izmed vseh polinomov, ki imajo a za ničlo, vzamemo enega z najnižjo stopnjo in ga nato pomnožimo z inverzom njegveda vodilnega koeficienta. Sedaj denimo, da sta $p(X)$ in $q(X)$ minimalna polinoma elementa a. Potem je a ničla polinoma $p(X) - q(X)$, ki pa je nižje stopnje kot $p(X)$ in $q(X)$. To pa pomeni, da je $q(X) - p(X) = 0$ in ima a res en sam minimalni polinom.

Definicija 7.3. Če je stopnja minimalnega polinoma elementa a enaka n, rečemo, da je a algebraičen stopnje n.

Izrek 7.1.

Naj bo $a \in E$ algebraičen nad F in naj bo $p(X) \in F[X]$ tak moničen polinom, da je $p(a) = 0$. potem so naslednji pogoji ekvivalentni:

1. *$p(X)$ je minimalni polinom elementa a.*
2. *$p(X)$ je nerazcepen.*
3. *$p(X)$ deli vsak polinom $f(X) \in F[X]$ z lastnostjo $f(a) = 0$.*

Dokaz. (1) $\Rightarrow$ (2) Naj bo $p(X) = g(X)h(X)$, kjer je $p(X)$ minimalni polinom elementa a. Ker je $f(a) = g(a)h(a) = 0$, mora veljati $g(a) = 0$ ali pa $h(a) = 0$. Denimo, da je $g(a) = 0$; potem zaradi minimalnosti velja $\mathrm{st}(g(X)) \geq \mathrm{st}(p(X))$. Očitno pa velja tudi $\mathrm{st}(g(X)) \leq \mathrm{st}(p(X))$, torej je $\mathrm{st}(g(X)) = \mathrm{st}(p(X))$ in p je nerazcepen.
(2) $\Rightarrow$ (3) Naj bo $p(X)$ nerazcepen in $p(a) = 0$. Definirajmo $I = \{f(X) \in F[X] \mid f(a) = 0\}$ in $I \lhd F[X]$, torej je I glavni ideal in velja $I = (p_1(X))$. Vemo, da je $p(X) \in I$ in je nerazcepen, torej je $p(X) = h(X)p_1(X)$ in $h(X)$ mora biti konstanten, torej je $I = (p(X))$.
Implikacija (3) $\Rightarrow$ (1) je očitna. □

Zgled 7.2. *Oglejmo si nekaj zgledov minimalnih polinomov elementov.*

- *Če je $a \in F$, potem je a algebraičen stopnje 1 nad F in je $X - a$ njegov minimalni polinom.*
- *Naj bo sedaj $F = \mathbb{R}$ in $E = \mathbb{C}$. Iz prejšnje točke vemo, da je $z \in \mathbb{R}$ algebraično število stopnje 1 nad F. Če pa je $z \in \mathbb{C} \setminus \mathbb{R}$, potem pa je z algebraičen stopnje 2 nad F z minimalnim polinomom $(X - z)(X - \overline{z})$.*
- *Naj bo F dano polje; oglejmo si njegovo razširitev $F(X)$. Element $X \in F(X)$ ni algebraičen nad F, zato je transcendenten.*

Če govorimo o algebraičnih oziroma transcendentnih številih, se to nanaša na primer, ko je $F = \mathbb{Q}$ in $E = \mathbb{C}$.

Opomba. Če je a algebraično število, potem je ničla nekega polinoma $p(X) \in \mathbb{Z}[X]$.

Zgled 7.3. *Imaginarno število i je algebraično stopnje 2, saj je njen minimalni polinom $X^2 + 1$.*

Zgled 7.4. *Za $n \in \mathbb{N}$ praštevilo p je $\sqrt[n]{p}$ algebraično stopnje n. Res, njegov minimalni polinom je $X^n - p$, ki je po Eisensteinovem kriteriju nerazcepen.*

Zgled 7.5. *Polinomov iz $\mathbb{Q}[X]$ je števno mnogo in vsak ima v $\mathbb{C}$ končno mnogo ničel, zato je algebraičnih števil v $\mathbb{C}$ le končno mnogo. Kljub temu, da so torej skoraj vsa kompleksna števila transcendentna, pa ni lahko podati konkretnih primerov. Eno izmed najbolj znamenitih takih števil je Liouvillova konstanta:*

$$\sum_{n=1}^{\infty} 10^{n!} = 0.11000100\ldots$$

Zgled 7.6. *Dokažimo, da je število $a = \sqrt{2}+\sqrt{3}$ algebraično. Iz $a-\sqrt{2} = \sqrt{3}$ sledi $a^2-2\sqrt{2}a+2 = 3$ in nato $2\sqrt{2}a = a^2 - 1$. Če obe strani kvadriramo, dobimo, da je $a^4 - 10a^2 + 1 = 0$. Izkaže se, da je $X^4 - 10X^2 + 1$ tudi minimalni polinom a.*

7.2 Končne razširitve

Naj bo E razširitev F. Potem lahko E obravnavamo kot vektorski prostor nad F z navadnim seštevanjem in navadnim množenjem s skalarji λx, kjer je $\lambda \in F$ in $x \in E$. Takoj lahko vidimo, da to ustreza vsem aksiomom vektorskega prostora.

Definicija 7.4. Polje E je končna razširitev polja F, če je E kot vektorsko polje nad F končnorazsežno. Tedaj dimenziji E nad F pravimo stopnja razširitve in je označena kot $[E : F] := \dim_F E$.

Zgled 7.7. *Očitno je $[\mathbb{C} : \mathbb{R}] = 2$ (primer baze je na primer $\{1, i\}$). Po drugi strani pa $\mathbb{R}$ ni končna razširitev $\mathbb{Q}$; če bi imeli bazo $\{b_1, \ldots, b_n\}$ prostora $\mathbb{R}$ nad $\mathbb{Q}$, potem bi $\mathbb{R}$ bila števna množica.*

Izrek 7.2.

Naj bo L končna razširitev F in E končna razširitev L. Potem je tudi E končna razširitev F in velja

$$[E : F] = [E : L][L : F].$$

Dokaz. Naj bo $\{a_1, \ldots, a_m\}$ baza L nad F (torej $[L : F] = m$) in $\{b_1, \ldots, b_n\}$ baza E nad L (torej $[E : L] = n$). Dokazujemo, da je $\{a_i b_j \mid 1 \leq i \leq m,\ 1 \leq j \leq n\}$ baza E nad F. Moč je množice je mn, saj bi recimo $a_1 b_1 = a_2 b_3$ pomenilo, da sta b_1 in b_3 linearno odvisna, kar pa ni res po predpostavki.
Dokažimo najprej, da je ta množica ogrodje. Naj bo $x \in E$, kjer je $x = \sum_{j=1}^{n} l_j b_j$ za neke koeficiente $l_j \in L$. Potem za vsak j velja $l_j = \sum_{i=1}^{m} \lambda_{ij} a_i$ za neke $\lambda_{ij} \in F$. Od tod pa sledi $x = \sum_{i=1}^{m} \sum_{j=1}^{n} \lambda_{ij} a_i b_j$, kar smo želeli pokazati.

Dokažimo še, da je ta množica linearno neodvisna. Torej imamo

$$\begin{aligned}\sum_{i=1}^{m}\sum_{j=1}^{n}\lambda_{ij}a_ib_j = 0 &\Rightarrow \sum_{i=1}^{m}\left(\sum_{j=1}^{n}\lambda_{ij}a_i\right)b_j = 0\\ &\Rightarrow \sum_{i=1}^{n}\lambda_{ij}a_i = 0,\ \forall j\\ &\Rightarrow \lambda_{ij} = 0,\ \forall i,j.\end{aligned}$$

□

Posledica 7.3. *Naj bo polje E končna razširitev polja F. Če je L razširitev F, ki je vsebovana v E (tj. L je „vmesno polje“), potem $[L : F]$ deli $[E : F]$.*

Dokaz. Dovolj je dokazati, da je L res končna razširitev F. To pa sledi iz tega, da je podprostor končnorazsežnega prostora E nad F. Ker sta torej E in L končnorazsežna nad F, obstaja tako končno ogrodje E nad F, ki je tudi ogrodje E nad L. Od tod pa res sledi $[E : L] < \infty$. □

Definicija 7.5. Polje E je algebraična razširitev polja F, če je vsak element iz E algebraičen nad F.

Trditev 7.4. *Vsaka končna razširitev je algebraična.*

Dokaz. Naj bo $[E : F] = n < \infty$ in vzemimo $a \in E$. Potem so $1, a, \ldots, a^n \in E$ in ker je teh elementov $n + 1$, so linearno odvisni. Torej obstajajo koeficienti $\lambda_0, \lambda_1, \ldots, \lambda_n \in F$, tako da je $\lambda_0+\lambda_1 a+\cdots+\lambda_n a^n = 0$. To pomeni, da je a ničla polinoma $f(X) = \lambda_0+\lambda_1 X+\cdots+\lambda_n X^n \neq 0$. □

Kot bomo videli, pa obrat te trditve ne velja.

Opomba. Iz dokaza vidimo, dqa iz $[E : F] = n$ sledi, da je stopnja algebraičnosti poljubnega elementa $a \in E$ manjša ali enaka n.

Zgled 7.8. *Ker je $[\mathbb{C} : \mathbb{R}] = 2$, je vsak $z \in \mathbb{C}$ algebraičen stopnje manj ali enako 2 (vemo že, da je minimalni polinom za $z \in \mathbb{C} \setminus \mathbb{R}$ kar $X^2 - (z + \overline{z})X + z\overline{z}$).*

Naj bo $F[X]$ kolobar polinomov in $F(X)$ polje racionalnih funkcij. Vzemimo $F \subseteq E$ in $a \in E$. Nato s $F[a]$ označimo podkolobar E, generiran s F in a, s $F(a)$ pa podpolje E, generirano s F in a. Očitno je $F[a] \subseteq F(a)$. Hitro vidimo, da velja $F[a] = \{f(a) \mid f(x) \in F[X]\}$ in $F(a) = \{xy^{-1} \mid x, y \in F[a],\ y \neq 0\}$. Polje $F(a)$ imenujemo polje s priključitvijo elementa a polju F. Na enak način definiramo tudi $F[a_1, a_2, \ldots, a_n]$ in $F(a_1, a_2, \ldots, a_n)$, kjer so $a_1, a_2, \ldots, a_n \in E$.

Definicija 7.6. Element a polja $F(a)$ imenujemo primitivni element. Ta ni enolično določen.

Zgled 7.9.

$$\mathbb{Q}(i) = \left\{\frac{f(i)}{g(i)} \;\middle|\; f(X), g(X) \in \mathbb{Q}[X],\ q(i) \neq 0\right\} = \{a + bi \mid a, b \in \mathbb{Q}\}$$

Izrek 7.5.

Naj bo E razširitev F. Če je $a \in E$ algebraičen stopnje n nad F, potem je

$$F(a) = F[a] = \{\lambda_0 + \lambda_1 a + \cdots + \lambda_n a^{n-1} \mid \lambda_i \in F\}.$$

Ta razširitev je končna in velja $[F(a) : F] = n$.

Zgled 7.10. *Naj bo p praštevilo in $n \in \mathbb{N}$. Potem je $\sqrt[n]{p}$ je algebraično število stopnje n in*

$$\mathbb{Q}(\sqrt[n]{p}) = \left\{\lambda_0 + \lambda_1 \sqrt[n]{p} + \lambda_2 \sqrt[n]{p^2} + \cdots + \lambda_{n-1} \sqrt[n]{p^{n-1}} \mid \lambda_i \in \mathbb{Q}\right\}.$$

Dokaz. Vzemimo neničeln element $f(a) \in F[a]$, kjer je $f(X) \in F[X]$. Dokažimo, da je $f(a)^{-1} \in F[a]$. Naj bo $p(X)$ minimalni polinom a. Iz $f(a) \neq 0$ sledi, da p ne deli f. Ker pa je $p(X)$ nerazcepen, sta ta dva polinoma tuja. Torej obstajata polinoma $g(X), h(X) \in F[X]$, tako da je $p(X)g(X) + f(X)h(X) = 1$. Od tod pa sledi $f(a)h(a) = 1$ in zato $f(a)^{-1} = h(a) \in F[a]$, s čimer smo dokazali $F[a] = F(a)$.
Naj bo $f(a)$ kot prej in $f(X) = q(X)p(X) + r(X)$, kjer je $r(X) = 0$ ali pa $\mathrm{st}(r(X)) < n = \mathrm{st}(p(X))$. Potem je $f(a) = q(a)p(a) + r(a) = r(a)$, torej je res

$$F(a) = F[a] = \{\lambda_0 + \lambda_1 a + \cdots + \lambda_n a^{n-1} \mid \lambda_i \in F\}.$$

To pomeni, da je množica $\{1, a, \ldots, a^{n-1}\}$ ogrodje $F(a)$ nad F. Ker je stopnja algebraičnosti elementa a enaka n, je ta množica tud linearno neodvisna in zato baza. □

Naj bo $F \subseteq E$ in $a \in E$. Potem je preslikava $\varphi : F[X] \to F[a]$, dana s predpisom $\varphi(f(X)) = f(a)$, homomorfizem kolobarjev (pravimo ji evalvacijski homomorfizem). Očitno je to epimorizem, zato po izreku o izomorfizmu velja $F[X]/Ker\varphi \cong F[a]$. Če je a algebraičen, je $\ker\varphi = (p(X))$, kjer je $p(X)$ minimalni polinom. Ker pa je $p(X)$ nerazcepen, je $(p(X))$ maksimalen ideal, zato je $F[X]/(p(X))$ polje. Torej imamo $F[X]/(p(X)) \cong F[a] = F(a)$. V primeru, ko pa je a transcendenten, pa je $\ker\varphi = \emptyset$ in zato $F[X] \cong F[a]$, pri čemer je izomorfizem kar $f(X) \mapsto f(a)$. Ta predpis pa lahko razširimo do izomorfizma $F(X) \cong F(a)$ z očitnim predpisom $\frac{f(X)}{g(X)} \mapsto f(a)g(a)^{-1}$.

Posledica 7.6. *Če je $a \in E$ algebraičen nad E, potem je njegovo število algebraičnosti enako $[F(a) : F]$.*

Posledica 7.7. *Naj bo a kot v prejšnji posledici in L vmesno polje, tako da je $F \subseteq L \subseteq E$. Potem je $[L(a) : L] \leq [F(a) : F]$.*

Dokaz. Če je a algebraičen nad F, potem je tudi algebraičen nad L in njegova stopnja algebraičnosti nad L je kvečjemu manjša od stopnje algebraičnosti nad F. Nato uporabimo prvo posledico. □

Opomba. Naj bosta $a, b \in E$. Potem je $F(a, b) = (F(a))(b)$, in, nekoliko splošneje, $F(a_1, \ldots, a_n) = (F(a_1, \ldots, a_k))(a_{k+1}, \ldots, a_n)$.

Izrek 7.8.

Naj bodo $a_1, \ldots, a_n \in E$ algebraični nad F. Potem je $F(a_1, \ldots, a_n)$ končna razširitev polja F in $F(a_1, \ldots, a_n) = F[a_1, \ldots, a_n]$.

Dokaz. Dokaz poteka z indukcijo na n. Bazni korak smo že pokazali, zato predpostavimo, da je $L = F(a_1, \ldots, a_{n-1})$ končna razširitev F in $F(a_1, \ldots, a_{n-1}) = F[a_1, \ldots, a_{n-1}] = L$. Potem je $L(a_n) = F(a_1, \ldots, a_n)$ končna razširitev L po prejšnjem izreku in zato je tudi končna razširitev

F (po indukcijski predpostavki). Prav tako pa iz prejšnjega izreka vemo, da so elementi v $L(a_n)$ oblike

$$\sum_{i=0}^{m} l_i a_m^i = \sum_{i=0}^{m} f_i(a_1, \ldots, a_{n-1}) a_n^i = f(a_1, \ldots, a_n) \qquad \square$$

Zgled 7.11. *Oglejmo si polje $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = (\mathbb{Q}(\sqrt{2}))(\sqrt{3})$. Takoj lahko vidimo, da je množica $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$ ogrodje, zato je $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] \leq 4$. Dokažimo še, da je to tudi baza. Ker je $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$, je dovolj dokazati, da je $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})] > 1$, torej da $\sqrt{3}$ ni oblike $a + b\sqrt{2}$, kjer sta $a, b \in \mathbb{Q}$. To pa je očitno. Sedaj vemo, da je $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] \leq 4$, dokazali pa bomo še, da je $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$. Označimo $a = \sqrt{2} + \sqrt{3}$ in pokažimo, da je $\sqrt{2} \in \mathbb{Q}(a)$. Res, vemo da je $a - \sqrt{2} = \sqrt{3}$ in s kvadriranjem dobimo $a^2 - 2a\sqrt{2} + 2 = 3$, od koder pa sledi $\sqrt{2} = \frac{a - a^{-1}}{2} \in \mathbb{Q}(a)$.*

Izkaže se, da je vsaka končna razširitev polja F s katakteristiko 0 oblike $F(a)$ za nek algebraičen element a. To nam zagotavlja izrek o primitivnem elementu, ki pa ga ne bomo dokazali.

Posledica 7.9. *Naj bo $E \supseteq F$. Množica vseh elementov E, ki so algebraični nad F, je podpolje E.*

Dokaz. Naj bo to množica A. Očitno je $A \supset F$, zato je $A \neq \{0\}$. Če sta $a, b \in A$, potem je $F(a, b) \subseteq A$ končna razširitev polja F, zato velja $a - b, ab, a^{-1} \in A$. S tem smo trditev dokazali. $\square$

Zgled 7.12. *Množica vseh algebraičnih števil je algebraična razširitev polja $\mathbb{Q}$, vendar pa ni končna razširitev. Če bi bila, bi bila stopnja razširitve deljiva z $n = [\mathbb{Q}(\sqrt[n]{2}) : \mathbb{Q}]$ za vsak $n \in \mathbb{N}$, kar pa je seveda nemogoče.*

7.3 Konstrukcije z ravnilom in šestilom

V tem razdelku si bomo ogledali uporabo teorije, ki smo izpeljali. Dokazali bomo, da z ravnilom in šestilom ne moremo:

1. konstruirati kocke z dvakratno prostornino dane kocke.
2. razdeliti kota na tri enake dele.
3. konstruirati kvadrata z enako ploščino kot dani krog.

Najprej pojasnimo, kaj mislimo pod „konstrukcijo z ravnilom in šestilom.“ Z ravnilom lahko potegnemo premico skozi dani točki S in T, s šestilom pa lahko narišemo krožnico s središčem v dani točki S in polmerom enakim dolžini daljice z danima krajiščema T in T'. Na začetku imamo dve točki, iz katerih nato s presečišči premic in kržnic konstruiramo nove. Sedaj lahko zgornje primere prevedemo na naslednje:

1. iz točk $T_1 = (0, 0)$ in $T_2 = (1, 0)$ konstruiraj točko $Z = (\sqrt[3]{2}, 0)$.
2. iz točk $T_1 = (0, 0), T_2 = (1, 0)$ in $T_3 = (\cos 60°, \sin 60°)$ konstruiraj točko $Z = (\cos 20°, \sin 20°)$.
3. iz točk $T_1 = (0, 0)$ in $T_2 = (1, 0)$ konstruiraj $Z = (\sqrt{\pi}, 0)$.

Sedaj preidimo na splošen primer. Naj bo $\mathcal{T} = \{T_1, T_2, \ldots\}$ množica točk v ravnini z vsaj dvema elementoma. Zanimajo nas lastnosti točk, ki jih v končnem številu korakov dobimo s konstrukcijami z ravnilom in šestilom iz $\mathcal{T}$. V prvem koraku dobimo točko A, za katero velja ena izmed lastnosti:

(**pp**) A je presečišče dveh premic dobljenih iz $\mathcal{T}$.

(**pk**) A je presečišče premice in krožnice, dobljenih iz $\mathcal{T}$.

(**kk**) A je presečišče dveh krožnic, dobljenih iz $\mathcal{T}$.

V drugem koraku dobimo točko B na enak način iz $\mathcal{T} \cup \{A\}$. Točkam, ki jih dobimo na ta način po končnem številu korakov, rečemo konstruirane točke iz $\mathcal{T}$. Sedaj vzemimo podpolje $F \subseteq \mathbb{R}$, tako da je $\mathcal{T} \subseteq F \times F$. Ker ja takih polj lahko več, naj bo F polje, generirano z vsemi koordinatami točk iz $\mathcal{T}$. Pri prvem in tretjem problemu bi tako bilo polje $F = \mathbb{Q}$, pri tretjem pa $F = \mathbb{Q}(\sqrt{3})$.

Izrek 7.10.

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 in njuna stopnja algebraičnosti je potenca števila 2.

Dokaz. Naj bo A točka kot prej. Dokazali bomo, da obstaja tako polje $L \supset F$, da je $A \in L \times L$ $[L : F] \in \{1, 2, 4\}$. Sedaj trditev ponovimo za točko B, kjer množico $\mathcal{T}$ zamenjamo z $\mathcal{T} \cup \mathcal{A}$, polje F pa z L. Ponovno dobimo polje M, tako da je $B \in M \times M$ in $[M : L] \in \{1, 2, 4\}$. S tem dobimo $[M : F] = [M : L][L : F] = 2^u \times 2^v = 2^{u+v}$. Ta argument ponavljamo, dokler v končnem številu korakov ne pridemo do točke $Z = (a, b)$ in take razširitve $E \supset F$, da je $Z \in E \times E$. Seveda velja $[E : F] = 2^r$ za neki $r \geq 0$ in ker $[F(a) : F]$ deli $[E : F]$, je tudi stopnja algebraičnosti elementa a potenca 2. Enako seveda velja tudi za b. Osredotočimo se lahko torej na točko A in iskanje polja L. Pri tem moramo obravnavati vse primere (**pp**), (**pk**) in (**kk**). Vemo, da ima premica skozi točki iz $\mathcal{T}$ enačbo $y = \alpha x + \beta$ ali $x = \gamma$, kjer so $\alpha, \beta, \gamma \in F$. Podobno ima krožnica iz točk $\mathcal{T}$ enačbo $x^2 + y^2 = \delta x + \epsilon y + \zeta$, kjer so $\delta, \epsilon, \zeta \in F$. Za polje L vzamemo kar $F(x, y)$, kjer sta x in y koordinati presečišča dveh izmed teh enačb, in nato lahko za vsakega od treh primerov hitro preverimo, da naša trditev drži. □

Posledica 7.11. *Iz dane kocke z ravnilom in šestilom ne moremo konstruirati kocke z dvakratno prostornino.*

Dokaz. Problem je ekvivalenten temu, da točko $(\sqrt[3]{2}, 0)$ konstruiramo iz množice $\mathcal{T} = \{(0, 0), (1, 0)\}$. To pa je nemogoče, saj je stopnja algebraičnosti števila $\sqrt[3]{2}$ nad $\mathbb{Q}$ enaka 3. □

Posledica 7.12. *Kota $60°$ z ravnilom in šestilom ne moremo razdeliti na tri enake dele.*

Dokaz. Pokažimo, da točke $Z = (\cos 20°, \sin 20°)$ 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 stopnja algebraičnosti števila $u = \cos 20°$ nad poljem $\mathbb{Q}(\sqrt{3})$ potenca števila 2, mi pa bomo dokazali, da je v resnici 3. Iz realnega dela enakosti $\cos 3\varphi + i \sin 3\varphi = (\cos \varphi + i \sin \varphi)^3$ dobimo formulo $\cos 3\varphi = 4 \cos^3 \varphi - 3 \cos \varphi$ in če vanjo vstavimo $\varphi = 20°$, dobimo $\frac{1}{2} = 4u^3 - 3u$. Sedaj moramo dokazati le še, da je polinom $p(X) = 8X^3 - 6X - 1$ nerazcepen nad $\mathbb{Q}(\sqrt{3})$. Denimo nasprotno; potem ima p ničlo $a \in \mathbb{Q}(\sqrt{3})$ in lahko zapišemo $a = 2q + 2r\sqrt{3}$, kjer sta $q, r \in \mathbb{Q}$. Ker sta 1 in $\sqrt{3}$ linearno neodvisni nad $\mathbb{Q}$, dobimo enačbi

$$q^3 + 9qr^2 - 3q - 1 \quad \text{in} \quad r(q^2 + r^2 - 1) = 0.$$

Ne glede na to, kateri faktor v drugi je ničeln, lahko prvo enačbo prevedemo na obliko $s^3 - 3s + 1$, kjer je $s \in \mathbb{Q}$. Če zapišemo $s = \frac{m}{n}$, kjer sta si m in n tuji celi števili. Od tod pa sledi $m \mid n^3$ in $n \mid m^3$ in ker sta to tuji števili, sta lahko enaki le 1 ali pa -1. To pa ni rešitev enačbe, zato smo prišli v protislovje. □

Posledica 7.13. *Iz danega kroga z ravnilom in šestilom ne moremo konstruirati kvadrata z enako ploščino.*

Dokaz. Tokrat je $Z = (\sqrt{\pi}, 0)$ in $\mathcal{T} = \{(0,0),(1,0)\}$. Dovolj je dokazati, da število $\sqrt{\pi}$ ni algebraično. Če bi bilo, bi bilo algebraično tudi število π, kar pa ni res. □

7.4 Kratnosti ničel polinomov

Lema 7.14. *Naj bo $a \in E$ ničla polinoma $f(X) \in F[X]$. Potem obstaja tak polinom $g(X) \in E[X]$, da je $f(X) = (X-a)g(X)$.*

Če je $f(X) = (X-a)g(X)$ in $g(a) \neq 0$, potem je a enostavna ničla polinoma $f(X)$. Z večkratno uporabo zgornje leme pridemo do naslednje trditve.

Trditev 7.15. *Neničelni polinom $f(X) \in F[X]$ ima v vsaki razširitvi F največ toliko ničel, štetih z večkratnostjo, kot je stopnja f.*

Definicija 7.7. Odvod polinoma $f(X) = a_0 + a_1X + \cdots + a_nX^n \in F[X]$ je polinom $f'(X) = a_1 + 2a_2X + \cdots + na_nX^{n-1} \in F[X]$.

Odvod polinoma upošteva pričakovani lastnosti, torej $(f(X)+g(X))' = f'(X)+g'(X)$ in $(f(X)g(X))' = f'(X)g(X) + f(X)g'(X)$. V poljih s ničelno karakteristiko velja tudi $\mathrm{st}(f'(X)) = \mathrm{st}(f(X)) - 1$, če je $f(X)$ nekonstanten. V splošnem pa to ne velja nujno; v $\mathbb{Z}_p$ je na primer $(X^p)' = 0$.

Izrek 7.16.

Naj bo F polje s ničelno karakteristiko in $p(X) \in F[X]$ nerazcepen polinom. Potem je vsaka ničla $p(X)$ (v katerikoli razširitvi) enostavna.

Dokaz. Naj bo $a \in E$ ničla $p(X)$. Potem je zaradi nerazcepnosti p minimalni polinom elementa a. Sedaj denimo, da a ni enostavna ničla $p(X)$. Potem je a tudi ničla polinoma $p'(X)$, ki je eno stopnjo nižji od p. To pa je protislovje s tem, da je $p(X)$ minimalni polinom a. □

7.5 Razpadna polja

V tem razdelku odgovoirmo na vprašanje, ali ima vsak nekonstanten polinom ničle (če že ne v originalnem polju, pa v kakšni razširitvi).

Izrek 7.17.

Naj bo F polje in $f(X) \in F[X]$ nekonstanten polinom. Potem obstaja razširitev F, v kateri ima $f(X)$ ničlo.

Dokaz. Naj bo $p(X)$ nerazcepen polinom, ki deli $f(X)$ (ta obstaja, saj je vsak nekonstanten polinom produkt nerazcepnih faktorjev). Definiramo $I = (p(X))$, $E = F[X]/I$ in ker je $p(X)$ nerazcepen, je E polje. Sedaj definiramo vložitev $\varphi : F \to E$ s predpisom $\varphi(t) = t + I$. Tako lahko E obravnavamo kot razširitev F. Za poljuben polinom $g(X) \in F[X]$, kjer je $g(X) = t_0 + t_1X + \cdots + t_nX^n$, imamo

$$\begin{aligned} g(X+I) &= (t_0+I) + (t_1+I)(X+I) + \cdots + (t_n+I)(X+I)^n \\ &= t_0 + t_1X + \cdots + t_nX^n + I \\ &= g(X) + I. \end{aligned}$$

Če sedaj v to vstavimo polinom $f(X)$ namesto $g(X)$, dobimo $f(X+I) = f(X) + I = 0$, torej je $X + I \in E$ ničla f. □

Izrek 7.18.

Naj bo $f(X) \in F[X]$ nekonstanten polinom. Potem obstaja razširitev E polja F in taki elementi $a_1, a_2, \ldots, a_n \in E$, da je $f(X) = c(X - a_1) \ldots (X - a_n)$, kjer je $c \in F$.

Definicija 7.8. Naj bo $f(X) \in F[X]$. Pravimo, da ta polinom razpade v razširitvi E polja F, če obstajajo taki $a_1, \ldots, a_n \in E$, da je $f(X) = c(X - a_1) \ldots (X - a_n)$. Če $f(X)$ razpade v E in ne razpade v nobenem pravem podpolju E, potem E imenujemo razpadno polje polinoma $f(X)$ nad F.

Izrek 7.19.

Za vsak polinom $f(X) \in F[X]$ stopnje najmanj 1 obstaja razpadno polje nad F.

Dokaz. Naj bo polje E in $a_1, \ldots, a_n$ kot v prejšnjem izreku. Potem je razpadno polje $f(X)$ nad E kar $F(a_1, \ldots, a_n)$. Dokaz je očiten. □

Zgled 7.13. *Naj bo $f(X) = X^2 + 1$. Kaj je njegovo razpadno polje?*

- *Razpadno polje nad $\mathbb{Z}_2$ je kar $\mathbb{Z}_2$ sam, saj je $f(X) = X^2 + 1 = (X + 1)^2$.*
- *Razpadno polje nad $\mathbb{C}$ je $\mathbb{C}$.*
- *Razpadno polje nad $\mathbb{R}$ je prav tako $\mathbb{C}$.*
- *Razpadno polje nad $\mathbb{Q}$ je $\mathbb{Q}(i)$.*

Opomba. Razpadno polje nad F je končna razširitev $F(a_1, \ldots, a_n)$, saj so $a_1, \ldots, a_n$ ničle polinoma $f(X)$ in so zato algebraični.

Naj bo E razširitev F in $p(X) \in F[X]$ nerazcepen polinom z ničlo $a \in E$. Definiramo evalvacijski homomorfizem $\varepsilon : F[X] \to F(a)$ s predpisom $\varepsilon(f(X)) = f(a)$. Seveda je ε surjektiven in njegovo jedro je ideal $(p(X))$, saj je p nerazcepen. Po izreku o izomorfizmu je $F[X]/(p(X)) \cong F(a)$ in ta izomorfizem je $\overline{\varepsilon} : F[X]/(p(X)) \to F(a)$, ki slika $\lambda + (p(X))$ v λ, kjer je $\lambda \in F$, in $X + (p(X))$ v a.

$$\begin{array}{ccc} F[X] & \xrightarrow{\pi} & F[X]/(p(X)) \\ & \searrow^{\varepsilon} & \downarrow{\scriptstyle \overline{\varepsilon}} \\ & & F(a) \end{array}$$

Naj bo sedaj $\varphi : F \to F'$ izomorfizem. Trdimo, da lahko φ razširimo na izomorfizem $F[X] \to F'[X]$, ki slika

$$\lambda_0 + \lambda_1 X + \cdots + \lambda_n X^n \mapsto \underbrace{\varphi(\lambda_0) + \varphi(\lambda_1) X + \cdots + \varphi(\lambda_n) X^n}_{f_\varphi(X)}.$$

Dokaz je popolnoma rutinski.

Lema 7.20. *Naj bo $p(X) \in F[X]$ nerazcepen in a njegova ničla v neki razširitvi polja F. Če je kot prej $\varphi : F \to F'$ izomorfizem polj in a' ničla polinoma $p_\varphi(X)$ v neki razširitvi, potem obstaja tak izomorfizem $\Phi : F(a) \to F'(a)$, da je Φ razširitev φ in $\Phi(a) = a'$.*

$$\begin{array}{ccc} F[X]/(p(X)) & \xrightarrow{\overline{\varepsilon}} & F(a) \\ \downarrow \tilde{\varphi} & & \vdots \Phi \\ F[X]/(p_\varphi(X)) & \xrightarrow{\overline{\varepsilon'}} & F(a') \end{array}$$

Dokaz. Naj bosta $\overline{\varepsilon}$ in $\overline{\varepsilon'}$ kot prej (tudi polinom $p_\varphi(X)$ je namreč nerazcepen). Sedaj pa definiramo preslikavo $\tilde{\varphi}$ s predpisom

$$\tilde{\varphi}(f(X) + (p(X))) = f_\varphi(X) + (p_\varphi(X))$$

in takoj lahko preverimo, da je ta preslikava dobro definirana in izomorfizem. Nato pa definiramo še $\Phi := \overline{\varepsilon'} \circ \tilde{\varphi} \circ \overline{\varepsilon}^{-1}$ in očitno je, da zadošča vsem želenim lastnostim. □

Izrek 7.21.

Naj bo $f(X) \in F[X]$ nekonstanten polinom in E njegovo razpadno polje. Če je $\varphi : F \to F'$ izomorfizem polj in je E' razpadno polje polinoma $f_\varphi(X) \in F'[X]$, potem lahko φ razširimo do izomorfizma iz E v E'.

Dokaz. Naredimo indukcijo na $n = [E : F]$ (vemo že, da je to končno število). V baznem koraku $n = 1$ je $E = F$, torej $f(X)$ razpade v F in potem tudi $f_\varphi(X)$ razpade v $F[X]$, zato je $\Phi = \varphi$. Sedaj dokažimo še induktivni korak $n > 1$; ker $f(X)$ ne razpade v F, ima vsaj en nerazcepen faktor stopnje več od 1 (recimo mu $p(X)$). Potem obstaja ničla $a \in E$ polinoma $p(X)$ in podobno ničla $a' \in E'$ polinoma $p_\varphi(X)$. Potem po lemi obstaja izomorfizem $\Phi : F(a) \to F'(a')$, kjer je $\Phi\big|_F = \varphi$ in $\Phi(a) = a'$. Ker je po konstrukciji $\mathrm{st}(p(X)) > 1$ in velja $[E : F] = [E : F(a)][F(a) : F]$, je $[E : F(a)] < n$. Ker je E razpadno polje $f(X)$ nad F, je tudi razpadno polje nad $F(a)$. Podobno je E' razpadno polje $f_\varphi(X)$ nad $F'(a)$. Sedaj pa lahko po indukcijski predpostavki Φ razširimo do izomorfizma iz E v E' in ker je že Φ razširitev φ, je s tem izrek dokazan. □

Posledica 7.22. *Poljubni razpadni polji istega polinoma $f(X) \in F[X]$ sta izomorfni.*

Definicija 7.9. Polje A je algebraično zaprto, če ima vsak neskončni polinom iz $A[X]$ ničlo v A.

Ta definicija je ekvivalentna temu, da lahko vsak nekonstanten polinom $f(X) \in A[X]$ zapišemo kot $f(X) = c(X - a_1) \dots (X - a_n)$, kjer so $c, a_1, \dots, a_n \in A$.

Zgled 7.14. *Primer algebraično zaprtega polja je $\mathbb{C}$ (to nam zagotavlja osnovni izrek algebre).*

Lema 7.23. *Naj bo F polje, L algebraična razširitev F, E razširitev L in $x \in E$ algebraičen nad L. Potem je x algebraičen tudi nad F.*

Dokaz. Po predpostavki je $a_0 + a_1 x + \dots + a_n x^n = 0$ za neke $a_i \in L$, ki niso vsi 0. Seveda je x algebraičen tudi nad $F(a_0, a_1, \dots, a_n)$, to polje pa je končna razširitev F (saj so $a_i \in L$ in zato algebraični). Nato pa je še $(F(a_0, \dots, a_n))(x)$ končna razširitev $F(a_0, \dots, a_n)$. Končna razširitev končne razširitve je sama končna in zato algebraična nad F, torej je x res algebraičen nad F. □

Posledica 7.24. *Algebraična razširitev algebraične razširitve je tudi sama algebraična.*

Definicija 7.10. Naj bo F polje. Polje $\overline{F}$ je njegovo algebraično zaprtje, če je:
- $\overline{F}$ je algebraično zaprto
- $\overline{F}$ e algebraična razširitev polja F.

Zgled 7.15. *Algebraično zaprtje $\mathbb{R}$ je $\mathbb{C}$. Kaj pa algebraično zaprtje polja $\mathbb{Q}$?*

Izrek 7.25.

Naj bo F podpolje algebraično zaprtega polja A. Potem je množica vseh elementov iz A, ki so algebraični nad F, algebraično zaprtje F.

Dokaz. Ta množica (naj bo $\overline{F}$) je res polje. Naj bo $f(X) \in \overline{F}[X]$ nekonstanten polinom. Ker je A algebraično zaprto, ima ničlo $x \in A$. Ker je x algebraičen nad $\overline{F}$, je tudi algebraičen nad Fm, torej je $x \in \overline{F}$. □

Posledica 7.26. *Polje algebraičnih števil je algebraično zaprtje $\mathbb{Q}$.*

Izkaže se, da ima vsako polje algebraično zaprtje in je algebraično zaprtje eno samo do izomorfizma natančno.

7.6 Končna polja

Od končnih polj poznamo le polja $\mathbb{Z}_p$. Vsako končno polje ima očitno končno karakteristiko, torej karakteristiko p, kjer je p neko praštevilo. Vemo, da lahko $\mathbb{Z}_p$ vložimo v polje s karakteristiko p. Če je E torej končno polje, obstaja vložitev $\mathbb{Z}_p$ v E in je E torej razširitev $\mathbb{Z}_p$; med drugim je E končnorazsežen vektorski prostor nad $\mathbb{Z}_p$.

Lema 7.27. *Če je E končno polje s karakteristiko p, je $|E| = p^n$ za nek $n \in \mathbb{N}$.*

Dokaz. Naj bo $\{b_1, \ldots, b_n\}$ baza E nad $\mathbb{Z}_p$. Potem lahko vsak element iz E na enoličen način zapišemo kot

$$\lambda_1 b_1 + \lambda_2 b_2 + \cdots + \lambda_n b_n, \quad \lambda_i \in \mathbb{Z}_p.$$

Vsah takih zapisov pa je $|\mathbb{Z}_p|^n = p^n$. □

Opomba. Iz dokaza leme vidimo, da je $[E : \mathbb{Z}_p] = n$ natanko tedaj, ko je $|E| = p^n$.

Razpadna polja polinomov so končne razširitve in preko teh bomo morda lahko skonstruirali polja s $p^2, p^3, \ldots$ elementi.

Lema 7.28. *Če je E polje s p^n elementi, je E razpadno polje polinoma $X^{p^n} - X \in \mathbb{Z}_p[X]$.*

Dokaz. Vemo, da je $|E| = p^n$ in $E^* = E \setminus \{0\}$ grupa za množenje. Ker je $|E| = p^n - 1$, je po Lagrangevem izreku $x^{p^n - 1} = 1$ za vsak $x \in E^*$. Torej je $x^{p^n} = x$ za vsak $x \in E$. To pomeni, da je vsak element E ničla polinoma $X^{p^n} - X \in \mathbb{Z}_p[X]$. To pa je polinom stopnje p^n, kar pa je ravno število elementov v E, torej je E res razpadno polje tega polinoma. □

Če je K komutativen kolobar s karakteristiko p, potem preslikavo $\varphi : K \to K$ s predpisom $\varphi(x) = x^p$ imenujemo Frobeniusov endomorfizem. Da je res endomorfizem, se zlahka prepričamo, pri tem pa tudi dokažemo formulo $x^p + y^p = (x + y)^p$ („Freshman's dream“), ki velja v takih kolobarjih.

Lema 7.29. *Razpadno polje polinoma $f(X) = X^{p^n} - X$ nad $\mathbb{Z}_p$ ima p^n elementov.*

Dokaz. Naj bo E to polje in označimo

$$E_* = \{x \in E \mid x^{p^n} = x\} = \{x \in E \mid \varphi^n(x) = x\},$$

torej je to množica fiksnih točk endomorfizma E. Lahko je pokazati, da je to podpolje E. Množica vseh ničel je torej že sama polje, zato je razpadno polje in velja $E = E_*$. Dokazati moramo le še, da so vse ničle $f(X)$ različne. Ker je $f(X) = X(X^{p^n-1} - 1)$, je 0 očitno enostavna ničla. Naj bo sedaj $a \neq 0$ poljubna ničla $f(X)$, torej je ničla $X^{p^n-1} - 1$ in zato velja $a^{p^n-1} - 1$. Od tod sledi

$$\begin{aligned} f(X) &= X^{p^n} - X = X(X^{p^n-1} - a^{p^n-1}) \\ &= (X - a)\underbrace{(X^{p^n-1} + X^{p^n-2}a + \cdots + Xa^{p^n-2})}_{g(X)} \end{aligned}$$

in imamo

$$g(a) = (p^n - 1)a^{p^n-1} = p^n - 1 = -1 \neq 0. \qquad \square$$

Iz zadnjih treh lem, obstoja razpadnega polja in njegove enoličnosti pa direktno sledi naslednji izrek.

Izrek 7.30.

Za vsako praštevilo p in naravno število $n \in \mathbb{N}$ obstaja polje $\mathrm{GF}(p^n)$ s p^n elementi. Vsako končno polje je izomorfno enemu izmed teh polj.