Algebra 2

Ruslan Urazbakhtin

6. avgust 2025

Kazalo

1 Cela števila

1.1 Osnovni izrek o deljenju celih števil

Načela dobre urejenosti

- Vsaka neprazna podmnožica množice $\mathbb{N}$ vsebuje najmanjši element.
- Vsaka neprazna navzdol omejena podmnožica $\mathbb{Z}$ vsebuje najmanjši element.
- Vsaka neprazna navzgor omejena podmnožica $\mathbb{Z}$ vsebuje največji element.

Izrek 1.1 (Osnovni izrek o deljenju celih števil)**.** *Za vsaki števili $m \in Z$ in $n \in \mathbb{N}$ obstajata taki enolično določeni števili $q, r \in Z$, da je*

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

*Število r imenujemo **ostanek** pri deljenju števila m s številom n.*

1.2 Največji skupni delitelj

Definicija 1.2. Pravimo, da celo število $k \neq 0$ **deli** celo število m, če obstaja celo število q, da velja

$$m = qk.$$

Pravimo, da je število d **največji skupni delitelj** števil m in n, če

1. $d \in \mathbb{N}$;
2. d je skupni delitelj m in n, tj. $d \mid m$ in $d \mid n$;
3. če je c skupni delitelj m in n, potem $c \mid d$.

Izrek 1.3. *Vsak par celih števil m in n, od katerih vsaj eno ni enako 0, ima največji skupni delitelj d. Lahko ga zapišemo v obliki*

$$d = mx + ny$$

za neka $x, y \in \mathbb{Z}$.

Definicija 1.4. Za celi števili m in n, ne obe enaki 0, pravimo, da sta **tuji**, če je njun največji skupni delitelj enak 1.

Posledica 1.5. *Celi števili m in n sta tuji natanko tedaj, ko obstajata taki celi števili x in y, da je*

$$mx + ny = 1.$$

1.3 Osnovni izrek aritmetike

Lema 1.6 (Evklidova lema)**.** *Naj bo p praštevilo in m, n celi števili. Če $p \mid mn$, potem $p \mid m$ ali $p \mid n$.*

Izrek 1.7 (Osnovni izrek aritmetike)**.** *Vsako naravno število $n > 1$ lahko zapišemo kot produkt praštevil. Ta zapis je enoličen do vrstnega reda faktorjev natančno.*

2 Uvod v teorijo grup

2.1 Osnovni pojmi teoriji grup

Definicija 2.1. Naj bo S neprazna množica. **Operacija na množice** S je preslikava

$$* : S \times S \to S,\ (a, b) \mapsto a * b.$$

Operacija $*$ je **asociativna**, če $\forall a, b, c \in S \,.\, (a * b) * c = a * (b * c)$.
Operacija $*$ je **komutativna**, če $\forall a, b \in S \,.\, a * b = b * a$.

Definicija 2.2. Neprazna množica S skupaj z operacijo $*$ je **polgrupa**, če je operacija $*$ asociativna.

Definicija 2.3. Naj bo S množica z operacijo $*$. Pravimo, da je $e \in S$ **enota** (oz. **nevtralni element**) za operacijo $*$, če

$$\forall x \in S \,.\, e * x = x * e = x.$$

Trditev 2.4. *Če v množici S obstaja enota za operacijo $*$, potem je ena sama.*

Definicija 2.5. Polgrupa z enoto je **monoid**.

Definicija 2.6. Naj bo S množica z operacijo $*$ in $e \in S$ enota. Naj bo $x \in S$.
- Element $l \in S$ je **levi inverz** elementa x, če $l * x = e$.
- Element $d \in S$ je **desni inverz** elementa x, če $x * d = e$.
- Element $y \in S$ je **inverz** elementa x, če $x * y = y * x = e$.

Definicija 2.7. Pravimo, da je element $x \in S$ **obrnljiv**, če obstaja inverz od x.

Trditev 2.8. *Če je S monoid, $x \in S$, l levi inverz x ter d desni inverz x, potem $l = d$.*

Posledica 2.9. *Če je S monoid, $x \in S$ ter x obrnljiv, potem inverz en sam.*

Posledica 2.10. *Če je S monoid, $x \in S$ ter x obrnljiv, potem iz $xy = 1$ sledi $yx = 1$.*

Trditev 2.11. *Naj bo S monoid ter $a, b \in S$ obrnljiva. Tedaj obrnljiv tudi ab ter velja*

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

Definicija 2.12. Naj bo S z operacijo $*$ monoid. Pravimo, da je S **grupa**, če je vsak element iz S obrnljiv. Če je operacija $*$ komutativna, pravimo, da je S **Abelova grupa**.

V grupah ponavadi uporabljamo **miltiplikativni zapis**:
- operacija: $\cdot$;
- enota: 1;
- inverz od x: x^{-1};
- potenca: x^n.

V Abelovih grupah uporabljamo **aditivni zapis**:
- operacija: $+$;
- enota: 0;
- inverz od x: $-x$;
- potenca: nx.

Trditev 2.13. *Naj bo $(G, \cdot)$ grupa. Tedaj velja*
- $x^{m+n} = x^m x^n$;
- $(x^m)^n = x^{mn}$;
- *če je G Abelova, tedaj $n(x+y) = nx + ny$;*
- *pravilo krajšanja: $xy = xz \implies y = z$ ter $yz = zx \implies y = z$.*

Zgled 2.14. Nekaj primerov grup.
1. $(\mathbb{Z}, +),\ (\mathbb{Q}, +),\ (\mathbb{R}, +),\ (\mathbb{C}, +), (\mathbb{Q} \setminus \{0\}, \cdot)$ so Abelove grupe.
2. Naj bo X neprazna množica. Definiramo

$$\mathrm{Sym}(X) = \{\text{vse bijektivne preslikave } f : X \to X\}.$$

   $(\mathrm{Sym}(X), \circ)$ je grupa, imenujemo jo **simetrična grupa** množice X.
   V posebnem primeru, ko je X končna dobimo $\mathrm{Sym}(\{1, 2, \ldots, n\}) = S_n$. Torej običajne permutacije.

Zgled 2.15 (Simetrije kvadrata)**.** Simetrije kvadrata K so izometrije $f : \mathbb{R}^2 \to \mathbb{R}^2$, za kateri velja $f(K) = K$.
Primeri simetrij:
- r - rotacija za $90°$ okoli središča kvadrata;
- z - zrcaljenje čez fiksno os simetrije;
- kompozicije r in z.

Iz geometrije lahko vidimo, da je $zr = r^3 z$. To pomeni, da je vsak kompozitum r in z oblike $r^k z$.
Kvadrat ima kvečjemu 8 simetrij, ker je vsaka simetrija določena s sliko oglišča 1 in informacijo, ali smo naredili zrcaljenje ali ne. Dobimo množico simetrij

$$D_{2\cdot 4} = \{\mathrm{id}, r, r^2, r^3, z, rz, r^2 z, r^3 z\}.$$

$D_{2\cdot 4}$ je **diedrska grupa** moči 8.

Zgled 2.16 (Diedrska grupa moči $2n$)**.** Imamo naslednje simetrije pravilnega n-kotnika:
- r - rotacija za $\frac{2\pi}{n}$ okoli središča.
- z - zrcaljenje čes neko fiksno os simetrije.

Velja: $zr = r^{n-1} z$.
Množica vseh simetrij je

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

D_{2n} je **diedrska grupa** moči $2n$.

Zgled 2.17 (Monoid $\to$ Grupa)**.** Naj bo $(S, *)$ monoid. Definiramo

$$S^* = \{\text{obrnljive elementi iz } S\},$$

potem S^* je grupa za $*$.

Primer 2.18. Naj bo $S = (\mathbb{R}^{n \times n}, \cdot)$,

$$S^* = \{A \in \mathbb{R}^{n \times n} \mid \det A \neq 0\} = \mathrm{GL}_n(\mathbb{R}).$$

$\mathrm{GL}_n(\mathbb{R})$ je **splošna linearna grupa** $n \times n$ matrik.

Zgled 2.19 (Direktni produkt grup)**.** Naj bodo $G_1, G_2, \ldots, G_n$ grupe, ki imajo operacije $*_1, \ldots, *_n$. Na množice $G_1 \times G_2 \times \ldots \times G_n$ vpeljamo operacijo

$$(g_1, g_2, \ldots, g_n) * (h_1, h_2, \ldots, h_n) = (g_1 *_1 h_1, g_2 *_2 h_2, \ldots, g_n *_n h_n).$$

Potem je $(G_1 \times G_2 \times \ldots \times G_n, *)$ grupa.

2.2 Grupa permutacij

Izrek 2.20. *Vsaka permutacija je produkt disjunktnih ciklov.*

Definicija 2.21. Cikli dolžine 2 so **transpozicije**.

Trditev 2.22. *Vsaka permutacija $\pi \in S_n$ je produkt transpozicij. Teh transpozicij je vedno sodo mnogo ali vedno liho mnogo.*

Definicija 2.23. Permutacija je **soda (oz. liha)**, če je produkt sodo (oz. liho) mnogo transpozicij.

Definicija 2.24. Znak permutacije je $\operatorname{sgn}(\pi) = \begin{cases} 1; & \pi \text{ je soda} \\ -1; & \pi \text{ je liha} \end{cases}$.

Trditev 2.25. $\operatorname{sgn}(\pi\rho) = \operatorname{sgn}(\pi) \cdot \operatorname{sgn}(\rho)$.

2.3 Podgrupe

Definicija 2.26. Naj bo G grupa in $H \subseteq G$, $H \neq \emptyset$. H je **podgrupa grupe** G, če je H za isto operacijo tudi grupa. Oznaka $H \leq G$.

Opomba 2.27. Očitno o podgrupah:
1. Naj bo G grupa. Vedno velja: $\{1\} \leq G$ in $G \leq G$.
2. Če je $H \leq G$, potem (nujno!) $1 \in H$, kjer 1 je enota v G.

Opomba 2.28. Pri monoidih se enota ne deduje nujno, npr. $(\mathbb{Z}, \cdot)$ in $(\{0\}, \cdot)$.

Trditev 2.29. *Naj bo G grupa, $H \subseteq G$, $H \neq \emptyset$. Naslednje trditve so ekvivalentne:*
1. *$H \leq G$.*
2. *$\forall x, y \in H \,.\, xy^{-1} \in H$.*
3. *H je zaprta za množenje in invertiranje.*

Posledica 2.30. *Naj bo G končna grupa in $H \subseteq G$, $H \neq \emptyset$. Velja:*

$$H \leq G \iff H \text{ je zaprta za množenje.}$$

Dokaz. Ker je G končna, ko potenciramo $x \in H$, ena izmed potenc zagotovo ponovi. □

Primer 2.31. Primeri podrgup.
1. Vse prave podrgupe v grupi $(\mathbb{Z}, +)$ so oblike $n\mathbb{Z}$, $n \in \mathbb{N}$.
2. Definiramo $\mathrm{SL}_n(\mathbb{R}) = \{A \in \mathrm{GL}_n(\mathbb{R}) \mid \det A = 1\}$. Potem $\mathrm{SL}_n(\mathbb{R}) \leq \mathrm{GL}_n(\mathbb{R})$. $\mathrm{SL}_n(\mathbb{R})$ imenujemo **specialna linearna grupa**.
3. Definiramo $\mathrm{O}(n) = \{A \in \mathrm{GL}_n(\mathbb{R}) \mid AA^T = A^T A = I\}$. Potem $\mathrm{O}(n) \leq \mathrm{GL}_n(\mathbb{R})$.
4. Definiramo $\mathrm{SO}(n) = \{A \in \mathrm{O}(n) \mid \det A = 1\}$. Potem $\mathrm{SO}(n) \leq \mathrm{O}(n)$. Grupo $\mathrm{SO}(n)$ imenujemo **specialne ortogonalne matrike**.

Trditev 2.32. *Naj bosta H in K podgrupi grupe G. Potem $H \cap K \leq G$. Enako velja za preseke poljubnih družin podgrup.*

Definicija 2.33. Naj bosta $H, K \leq G$. Definiramo $HK = \{hk \,|\, h \in H,\ k \in K\}$. Temu pravimo **produkt podgrup**.

Zgled 2.34. Izkaže se, da HK ni nujno podgrupa v G. Vzemimo grupo $G = S_3$ ter podgrupi $H = \{\mathrm{id}, (1\ 2)\}$ in $K = \{\mathrm{id}, (1\ 3)\}$.

Trditev 2.35. *Naj bosta $H, K \leq G$. Če velja $HK = KH$, potem je $HK \leq G$.*

Opomba 2.36. Ni nujno, da produkt podgrup HK komutativen. Torej ni nujno vsak element $hk \in HK$ se da zapisati kot $k'h' \in KH$ za neki $k' \in K$ in $h' \in H$.

Definicija 2.37. Naj bo $H \leq G$, $a \in G$. Definiramo množico $aHa^{-1} = \{aha^{-1} \,|\, h \in H\}$. Potem $aHa^{-1} \leq G$. Temu se reče **konjungiranje podgrupe H z elementom a**.

Trditev 2.38. *Naj bo G grupa.*
1. *Definiramo $Z(G) = \{y \in G \,|\, \forall x \in G \,.\, yx = xy\}$. Potem $Z(G) \leq G$. Tej grupi pravimo* ***center grupe G****.*
2. *Naj bo $a \in G$. Definiramo $C_G(a) = \{y \in G \,|\, ya = ay\}$. Potem $C_G(a) \leq G$. Tej podgrupi pravimo* ***centralizator elementa a v G****.*

2.4 Odseki podgrup in Lagrangeev izrek

Naj bo G grupa in $H \leq G$. Definiramo relacijo na G s predpisom

$$\forall a, b \in G \,.\, a \sim b :\iff a^{-1}b \in H.$$

Trditev 2.39. *Relacija $\sim$ je ekvivalenčna relacija na G.*

Definicija 2.40. Naj bo G grupa, $H \leq H$, $a \in G$. **Ekvivalenčni razred elementa** $a \in G$ je množica $[a] = \{b \in G \,|\, a \sim b\}$.

Opomba 2.41. $[a] = \{ah \,|\, h \in H\} =: aH$.

Definicija 2.42. Množico aH imenujemo **levi odsek grupe G po podgrupi H**.

Opomba 2.43. V grupo G lahko vpeljamo tudi relacijo $\approx$ s predpisom

$$\forall a, b \in G \,.\, a \approx b :\iff ab^{-1} \in H.$$

To je ekvivalenčna relacija. Ekvivalentni razredi so $[a] = \{ha \,|\, h \in H\} =: Ha$, ki jih imenujemo **desni odseki**.

Definicija 2.44. Faktorska (oz. kvocientna) množica glede na relacijo $\sim$ je množica

$$G/_{\sim} = \{aH \,|\, a \in G\} =: G/H.$$

Opomba 2.45. G/H ni nujno grupa.

Opomba 2.46. Kadar sta dva odseka enaka? $aH = bH \iff a \sim b \iff a^{-1}b \in H$.

Opomba 2.47. Naj bo G končna grupa. Potem je G/H tudi končna množica.

Definicija 2.48. Naj bo G končna grupa. Moč množice G/H označimo z $[G : H]$ in jo imenujemo **indeks podgrupe** H v grupi G.

Izrek 2.49 (Lagrangeev izrek)**.** *Če je G končna grupa in $H \leq G$, potem je*

$$|G| = |H| \cdot |G : H|.$$

Dokaz. Recimo, da $|G : H| = r$. Pokažemo, da $|a_i H| = |H|$ za vse $i = 1, \ldots, r$. □

Posledica 2.50. *Moč vsake podgrupe končne grupe deli moč grupe.*

Opomba 2.51. Če je grupa G Abelova in $H \leq G$, potem odseki pišemo kot $a + H$. Velja:

$$G/H = \{a + H \mid a \in G\}.$$

Vpeljamo operacijo na G/H: $(a + H) + (b + H) = (a + b) + H$. Ta operacija je dobro definirana, ker je G Abelova.

Trditev 2.52. *G/H je za to operacijo Abelova grupa.*

Primer 2.53. Naj bo $G = \mathbb{Z}$ in $H = n\mathbb{Z}$, $n \in \mathbb{N}$. Potem

$$\mathbb{Z}/n\mathbb{Z} = \{0 + n\mathbb{Z}, 1 + n\mathbb{Z}, \ldots, (n-1) + n\mathbb{Z}\}.$$

Operacija $+$ na $\mathbb{Z}/n\mathbb{Z}$ je seštevanje po modulu n. Grupa $\mathbb{Z}_n := \mathbb{Z}/n\mathbb{Z}$ je **grupa ostankov po modulu** n, $|\mathbb{Z}_n| = n$.

Posledica 2.54. *Za vsako število $n \in \mathbb{N}$ obstaja vsaj ena grupa moči n.*

2.5 Generatorji grup. Ciklične grupe

Definicija 2.55. Naj bo G grupa in X podmnožica v G. Potem označimo z $\langle X \rangle$ najmanjšo podgrupo v G, ki vsebuje množico X. To podgrupo imenujemo **podgrupa, generirana z množico** X.

Opomba 2.56. $\langle X \rangle$ je presek vseh podgrup grupe G, ki vsebujejo množico X.

Definicija 2.57. Naj bo G grupa.

- Če je $X \subseteq G$, za katero velja $G = \langle X \rangle$, pravimo, da je G **generirana z množico** X. Elementam množice X pravimo **generatorji grupe** G.
  Oznaka: Če je $X = \{x_1, \ldots, x_n\}$, pišemo $\langle \{x_1, \ldots, x_n\} \rangle = \langle x_1, \ldots, x_n \rangle$.
- Če je $G = \langle x_1, \ldots, x_n \rangle$, pravimo, da je G **končno generirana grupa**.
- Če obstaja $x \in G$, da je $G = \langle x \rangle$, pravimo, da je G **ciklična grupa**.

Trditev 2.58. *Naj bo G grupa in $X \subseteq G$. Tedaj*

$$\langle X \rangle = \{x_{i_1}^{\pm 1} x_{i_2}^{\pm 1} \ldots x_{i_r}^{\pm 1} \mid x_{i_j} \in X;\ r \in \mathbb{N}_0\}.$$

Dokaz. Dovolj dokazati, da je $\langle X \rangle$ podgrupa grupe G. □

Posledica 2.59. *Naj bo G grupa, $a \in G$. Potem $\langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}$.*

Zgled 2.60. Primeri generatorjev grup:
- $\mathbb{Z} = \langle 1 \rangle$. Velja tudi: $\mathbb{Z} = \langle p, q \rangle$, kjer sta p in q tuji.
- $\mathbb{Z}_n = \langle 1 + n\mathbb{Z} \rangle$.

Zgled 2.61. Grupa $\mathbb{Q}^*$ ni končno generirana. Recimo, da $\langle x_1, \dots, x_n \rangle = \mathbb{Q}^*$. Pokažemo, da če praštevilo $p \notin \{x_1, \dots, x_n\}$, potem $p \notin \langle x_1, \dots, x_n \rangle$.

Definicija 2.62. Naj bo G grupa in $a \in G$. Najmanjšemu naravnemu številu n, za katerega velja $a^n = 1$, pravimo **red** elementa a. Če tak n ne obstaja, pravimo, da ima a neskončen red.

Primer 2.63. Primeri elementov končnega in neskončnega reda.
- Element $1 \in \mathbb{Z}$ ima neskončen red.
- Element $1 + n\mathbb{Z} \in \mathbb{Z}_n$ ima red n.

Trditev 2.64. *Naj bo G grupa, $a \in G$. Tedaj je*

$$|a| = n \iff |\langle a \rangle| = n.$$

Dokaz. Uporabimo posledico 2.59 ter izrek o deljenju celih števil 1.1. □

Posledica 2.65. *Naj bo G končna grupa. Velja:*
1. *Za vsak $a \in G$ red a deli $|G|$.*
2. *Za vsak $a \in G$ velja, da $a^{|G|} = 1$.*
3. *Če je $|G|$ praštevilo, potem je G ciklična grupa.*

3 Uvod v teorijo kolobarjev

Definicija 3.1. Naj bo K neprazna množica z operacijama $+$ in $\cdot$. Pravimo, da je $(K, +, \cdot)$ **kolobar**, če

1. $(K, +)$ je Abelova grupa (enota: 0, inverz od a: $-a$).
2. $(K, \cdot)$ je monoid, tj. kolobar vedno ima enoto za $\cdot$, označimo jo z 1, in rečemo, da je 1 **enica** kolobarja K.
3. Za vse $a, b, c \in K$ velja, da $a(b + c) = ab + ac$ in $(a + b)c = ac + bc$.

Če je množenje komutativno, pravimo, da je K **komutativen kolobar**.

Zgled 3.2. Primeri kolobarjev.

- $(\mathbb{Z}, +, \cdot)$ je komutativen kolobar.
- $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ so komutativni kolobarji.
- $(\mathbb{R}^{n\times n}, +, \cdot)$ je kolobar.
- Naj bo $X \subseteq \mathbb{R}$, $\mathbb{R}^X = \{f : X \to \mathbb{R}\}$. Definiramo $(f + g)(x) = f(x) + g(x)$, $(fg)(x) = f(x)g(x)$. $\mathbb{R}^X$ je komutativen kolobar.

Definicija 3.3. Naj bo K kolobar.

- $l \in K \setminus \{0\}$ je **levi delitelj niča**, če $\exists y \in K \setminus \{0\} \,.\, ly = 0$.
- $d \in K \setminus \{0\}$ je **desni delitelj niča**, če $\exists y \in K \setminus \{0\} \,.\, yd = 0$.
- $x \in K \setminus \{0\}$ je **delitelj niča**, če je levi ali desni delitelj niča.
- $x \in K$ je **idempotent**, če $x^2 = x$.
- $x \in K$ je **nilpotent**, če $\exists n \in \mathbb{N} \,.\, x^n = 0$.

Zgled 3.4. Primeri deliteljev niča, idempotentov in nilpotentov.

- V $\mathbb{R}^{2\times 2}$ velja $\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} = 0$.
- Če je K poljuben kolobar, potem 1 in 0 sta idempotenta.
- V $\mathbb{R}^5$ matrika $\begin{bmatrix} 0 & 1 & & & \\ & 0 & 1 & & \\ & & 0 & 1 & \\ & & & 0 & 1 \\ & & & & 0 \end{bmatrix}$ je nilpotenta.

Definicija 3.5. **Cel kolobar** je komutativen kolobar brez deliteljev niča.

Primer 3.6. $(\mathbb{Z}, +, \cdot)$ je cel kolobar.

Definicija 3.7. Naj bo K kolobar.

- Kolobar K je **obseg**, če je vsak neničeln element kolobarja K obrnljiv, tj.

$$K^* = K \setminus \{0\}.$$

- **Polje** je komutativen obseg.

Primer 3.8. $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ so polja.

Trditev 3.9. *Obrnljiv element kolobarja K ne more biti delitelj niča.*

Definicija 3.10. Naj bo A kolobar in F polje. A je **algebra** nad F, če

1. A je vektorski prostor nad F.
2. $\alpha(xy) = (\alpha x)y = x(\alpha y)$.

3.1 Primeri kolobarjev in algeber

Kolobar (algebra) kvadratnih matrik

Naj bo K kolobar. Definiramo

$$K^{n\times n} = M_n(K) = \{n \times n \text{ matrike z elementi iz } K\}.$$

$K^{n\times n}$ z običajnima $+$ in $\cdot$ je kolobar. Če je F polje, potem $F^{n\times n}$ je vektorski prostor in hitro vidimo, da je $F^{n\times n}$ algebra nad F.
Bolj splošno: Naj bo V vektorski prostor nad F. Vzemimo množico $\operatorname{End} V$. Potem $\operatorname{End} V$ je algebra nad F (rečemo tudi F-algebra).

Algebra realnih funkcij

Naj bo $X \subseteq \mathbb{R}^n,\ X \neq \emptyset$. Gledamo funkcije $\mathbb{R}^X$. Na $\mathbb{R}^X$ lahko definiramo $+$, $\cdot$ in množenje s skalarjem iz $\mathbb{R}$ po točkah. $\mathbb{R}^X$ je algebra nad $\mathbb{R}$.

Polinomi

Naj bo K kolobar. **Polinom** s koeficienti iz K je formalna vrsta oblike

$$p(x) = \sum_{i\geq 0} a_i X^i = a_0 + a_1 X + a_2 X^2 + \ldots + a_k X^k,\ a_i \in K,\ k \geq 0.$$

Manj baročno:

$$(a_0, a_1, \ldots, a_k, 0, 0, \ldots).$$

Torej polinom je končno zaporedje elementov iz K.
Naj bo $K[X]$ je množica vseh polinomov s koeficienti iz K. V $K[X]$ definiramo seštevanje in množenje:

- $\sum_{i\geq 0} a_i X^i + \sum_{i\geq 0} b_i X^i := \sum_{i\geq 0} (a_i + b_i) X^i$.
- $\sum_{i\geq 0} a_i X^i \cdot \sum_{i\geq 0} b_i X^i := \sum_{i\geq 0} c_i X^i$, kjer $c_i = \sum_{j\geq 0}^{i} a_{i-j} b_j$.

S temi operacijami $K[X]$ postane kolobar.

Opomba 3.11. Če je K polje, v $K[X]$ lahko vpeljamo množenje s skalarjem:

- $\alpha(\sum_{i\geq 0} a_i X^i) = \sum_{i\geq 0} (\alpha a_i) X^i$

Potem $K[X]$ postane algebra nad K.

Možni pospološitvi $K[X]$:

- Polinomi več spremenljivk: $K[X_1, \ldots, X_n] = K[X_1, \ldots, X_n][X_n]$.
- Če se ne omejimo na končne formalne vsote, dobimo **kolobar formalnih potenčnih vrst** $K[[X]]$.

Trditev 3.12. *Velja:*

- *K je komutativen kolobar natanko tedaj, ko $K[X]$ komutativen.*
- *K je brez deliteljev nična natanko tedaj, ko $K[X]$ brez deliteljev niča.*
- *K je cel kolobar natanko tedaj, ko $K[X]$ cel.*

Polje ulomkov celega kolobarja

Naj bo K cel kolobar. Gledamo množico $P = \{(a, b) \mid a \in K; b \in K \setminus \{0\}\}$. Na P vpeljamo relacijo:

$$(a, b) \sim (a', b') \iff ab' = a'b.$$

Trditev 3.13. *Relacija $\sim$ je ekvivalenčna.*

Dokaz. Kot v $\mathbb{Q}$. $\square$

Definiramo $F = P/_{\sim}$. Ekvivalenčni razred para (a, b) označimo z $\frac{a}{b}$. Definiramo seštevanje in množenje na F:
- $\frac{a}{b} + \frac{a'}{b'} := \frac{ab'+a'b}{bb'}$.
- $\frac{a}{b} \cdot \frac{a'}{b'} = \frac{aa'}{b'b}$.

Preveriti moramo, da sta seštevanje in množenje na F res dobro definirani.

Trditev 3.14. *Množica F s tema operacijama je polje. Pravimo mu* ***polje ulomkov kolobarja*** *K.*

Primer 3.15. $K = \mathbb{Z}$, potem $F = \mathbb{Q}$.

Opomba 3.16. Za ulomki oblike $\frac{a}{1}$, $a \in K$ velja:
- $\frac{a}{1} + \frac{b}{1} = \frac{a+b}{1}$.
- $\frac{a}{1} \cdot \frac{b}{1} = \frac{ab}{1}$

Zato lahko $\frac{a}{1}$ identificiramo z a. Torej kolobar K je **vložen** v F.

Algebre, ki so obsege

Gledamo algebre nad $\mathbb{R}$:
- $\mathbb{R}$ je algebra nad $\mathbb{R}$, $\mathbb{R}$ polje.
- $\mathbb{C}$ je dvorazsežna algebra nad $\mathbb{R}$, $\mathbb{C}$ polje.

Trditev 3.17. *Naj bo A algebra nad $\mathbb{R}$. Če je $\dim A$ liho število večje od 1, potem A ni obseg.*

Dokaz. Izberimo $a \in A \setminus \mathrm{Lin}\{1\}$ in definiramo endomorfizem $\mathcal{A} : A \to A$, $\mathcal{A}x = ax$. Poiščemo s pomočjo karakterisitčnega polinoma delitelji niča. $\square$

Algebra kvaternionov

Primer 3.18. Vzemimo realni vektorski prostor dimenzije 4. Naj bo njegova baza $\{1, i, j, k\}$. Označimo ta prostor s $\mathbb{H}$.
Elementi $\mathbb{H}$ so oblike $\lambda_1 \cdot 1 + \lambda_2 \cdot i + \lambda_3 \cdot j + \lambda_4 \cdot k$. Zaradi zveze med množenjem in množenjem s skalarji v algebri, dovolj, da definiramo množenje le na baznih vektorjih:
- 1 je enota za množenje.
- Elementi i, j, k med sabo množimo po naslednji shemi:

$$\begin{tikzcd}
 & i \arrow[dr] & \\
k \arrow[ur] & & j \arrow[ll]
\end{tikzcd}$$

Torej ko gremo v smeri urinega kazalca, dobimo naslednji element ($ij = k$), ki gremo v nasprotni smeri dobimo nasprotni element naslednjega elementa ($kj = -i$).

- $i^2 = j^2 = k^2 = -1$

Elementi množice $\mathbb{H}$ imenujemo **kvaternione**.
Naj bo $z = \lambda_1 \cdot 1 + \lambda_2 \cdot i + \lambda_3 \cdot j + \lambda_4 \cdot k$. Element $\overline{z} = \lambda_1 \cdot 1 - \lambda_2 \cdot i - \lambda_3 \cdot j - \lambda_4 \cdot k$ je **konjugirani kvaternion**.

Trditev 3.19. $\mathbb{H}$ *je obseg.*

Dokaz. Dovolj dokazati, da je vsak neničelni element obrnljiv. □

Trditev 3.20. $\mathbb{H}$ *je algebra.*

Dokaz. Preverimo usklajenost množenja in množenja s skalarjem. □

Pravimo, da je $\mathbb{H}$ **kvaternionska algebra**.
Grupa za množenje $(\{\pm 1, \pm i, \pm j, \pm k\}, \cdot)$ je **kvaternionska grupa**. Označimo jo z Q.

3.2 Podkolobarji, podalgebre, podpolja

Definicija 3.21. Naj bo K kolobar in naj bo $L \subseteq K,\ L \neq \emptyset$. Pravimo, da je L **podkolobar** kolobarja K, če je L na istih operacijah kolobar.

Opomba 3.22. Podobno definiramo tudi **podalgebro** in **podpolje**.

Trditev 3.23. *Naj bo K kolobar in $L \subseteq K,\ L \neq \emptyset$. Velja:*
L je podkolobar kolobarja K $\iff$

- $1 \in L$.
- *L je podgrupa za seštevanje v $(K, +)$.*
- *L je zaprta za množenje.*

Opomba 3.24. Distributivnost se podeduje.

Opomba 3.25. Podobne trditve velja za podalgebre in podpolja:

- Podalgebra je vektorski podprostor in podkolobar. Torej treba še preveriti zaprtost za množenje s skalarji.
- Podpolje je podkolobar v katerem je vsak neničeln element obrnljiv in množenje komutativno. Komutativnost se podeduje. Torej treba preveriti še zaprtost za invertiranje.

Primer 3.26. $\mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$.

Definicija 3.27. Polje E je **razšeritev** polja F, če je F podpolje E.

Primer 3.28. $\mathbb{R}^{n\times n}$ je kolobar in tudi algebra mad $\mathbb{R}$. Definiramo

$$U := \{A \in \mathbb{R}^{n\times n} \mid A \text{ je zgornje trikotna}\}.$$

Pokaži, da je U podkolobar in tudi podalgebra nad $\mathbb{R}$.

Primer 3.29. Naj bo $X \subseteq \mathbb{R}$. Definiramo $\mathbb{R}^X := \{f : X \to \mathbb{R}\}$ in operacije $+$, $\cdot$, množenje s skalarji po točkah. Potem je $\mathbb{R}^X$ algebra nad $\mathbb{R}$. Naj bo $C(X) = \{\text{vse zvezne } f : X \to \mathbb{R}\}$. Pokaži, da je $C(X)$ podalgebra.

3.3 Kolobar ostankov in karakteristika kolobarja

Vemo, da je $(\mathbb{Z}_n, +)$ Abelova grupa. Definiramo še množenje v $\mathbb{Z}_n$. Naj bo $a, b \in \mathbb{Z}_n$. Definiramo

$$(a + n\mathbb{Z}) \cdot (b + n\mathbb{Z}) = ab + n\mathbb{Z}.$$

Lema 3.30. *Množenje je dobro definirano.*

Trditev 3.31. $(\mathbb{Z}_n, +, \cdot)$ *je komutativen kolobar.*

Definicija 3.32. Kolobarju $(\mathbb{Z}_n, +, \cdot)$ pravimo **kolobar ostankov po modulu** n.

Definicija 3.33. Naj bo K kolobar. Najmanjšemu naravnemu številu n, za katerega je $n \cdot 1 = \underbrace{1 + 1 + \ldots + 1}_{n} = 0$, pravimo **karakteristika** kolobarja K. Oznaka: $\operatorname{char} K$. Če tak n ne obstaja, pravimo, da ima kolobar K karakteristiko 0.

Primer 3.34. Določi
- $\operatorname{char} \mathbb{Z}_n$.
- $\operatorname{char} \mathbb{Z}$.

Trditev 3.35. *Naj bo K kolobar z karakteristiko $n > 0$. Velja:*
1. $n \cdot x = 0$ *za vsak* $x \in K$.
2. *Naj bo* $m \in \mathbb{N}$. $m \cdot 1 = 0 \iff n \mid m$.
3. *Če je K neničeln kolobar in nima deljiteljev niča, potem je n praštevilo.*

Lema 3.36. *Končen cel kolobar je vedno polje.*

Dokaz. Dokazujemo, da je vsak element kolobarja K obrnljiv. Naj bo $a \in K$. Definiramo preslikavo $\varphi : K \to K$ s predpisom $\varphi(x) = ax$. Pokažemo, da je bijektivna. □

Trditev 3.37. *Naj bo $n \neq 1$. Velja:*

$$\mathbb{Z}_n \textit{ je polje} \iff n \textit{ je praštevilo.}$$

Dokaz. (⇒) Sledi iz trditve 3.35.
(⇐) Uporabimo lemo 3.36. □

Izrek 3.38 (Mali Fermatov izrek)**.** *Naj bo p praštevilo in $a \in \mathbb{N}$. Tedaj je*

$$a^p \equiv a \mod p.$$