Algebra 2

29. november 2024

1 Uvod v teorijo grup

1.1 Osnovni pojmi teoriji grup

Definicija 1.1. 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 1.2. Neprazna množica S skupaj z operacijo $*$ je **polgrupa**, če je operacija $*$ asociativna.

Definicija 1.3. 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 1.1. *Če v množici S obstaja enota za operacijo $*$, potem je ena sama.*

Definicija 1.4. Polgrupa z enoto je **monoid**.

Definicija 1.5. 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 $x * y = y * x = e$.

Trditev 1.2. *Če je S monoid, $x \in S$, l levi inverz x ter d desni inverz x, potem $l = d$.*

Definicija 1.6. Pravimo, da je element $x \in S$ **obrnljiv**, če obstaja inverz od x.

Definicija 1.7. 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.

Multiplikativni zapis	Aditivni zapis (Abelova grupa)
G ima natanko eno enoto	G ima natanko en ničeln element
Vsak element iz G ima natanko en inverz	Vsak element iz G ima natnako en nasprotni element
$(x^{-1})^{-1} = x$	$-(-x) = x$
$(xy)^{-1} = y^{-1}x^{-1}$	$-(x + y) = -x - y$
$x^{m+n} = x^m x^n$	$(m + n)x = mx + nx$
$(x^m)^n = x^{mn}$	$n(mx) = (nm)x$
V splošnem $(xy)^n \neq x^n y^n$	$n(x + y) = nx + ny$
$xy = xz \Rightarrow y = z$ $yx = zx \Rightarrow y = z$	$x + y = x + z \Rightarrow y = z$ (pravila krajšanja)
$xy = 1 \Rightarrow yx = 1$	

Tabela 1: Lastnosti računanja v grupah

Zgled. 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 $\mathrm{Sim}(X) = \{$vse bijektivne preslikave $f : X \to X\}$. $(\mathrm{Sim}(X), \circ)$ je grupa, imenujemo jo **simetrična grupa** množice X.
   V posebnem primeru, ko je X končna dobimo $\mathrm{Sim}(\{1, 2, \ldots, n\}) = S_n$. Torej običajne permutacije.

Zgled (Simetrije kvadrata). Simetrije kvadrata K so izometrije $f : \mathbb{R}^2 \to \mathbb{R}^2$, da je $f(K) = K$.
Primeri simetrij: r - rotacija za $90°$ okoli središča kvadrata, z - zrcaljenje čez fiksno os simetrije ter 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 (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 (Monoid $\to$ Grupa). Naj bo $(S, *)$ monoid. Definiramo $S^* = \{\text{obrnljive elementi iz } S\}$, potem S^* je grupa za $*$.

Primer. 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 (Direktni produkt grup). Naj bodo $G_1, G_2, \ldots, G_n$ grupe z operacijami $*_1, *_2, \ldots, *_n$. 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 $(G_1 \times G_2 \times \ldots \times G_n, *)$ je grupa.

1.2 Ponovitev o permutacijah

Izrek 1.3. *Vsaka permutacija je produkt disjunktnih ciklov.*

Definicija 1.8. Cikli dolžine 2 so **transpozicije**.

Trditev 1.4. *Vsaka permutacija $\pi \in S_n$ je produkt transpozicij. Teh transpozicij je vedno sodo mnogo ali vedno liho mnogo.*

Definicija 1.9. Permutacija je **soda (oz. liha)**, če je produkt sodo (oz. liho) mnogo transpozicij.

Definicija 1.10. Znak permutacije je $\mathrm{sgn}(\pi) = \begin{cases} 1; & \pi \text{ je soda} \\ -1; & \pi \text{ je liha} \end{cases}$.

Trditev 1.5. $\mathrm{sgn}(\pi\rho) = \mathrm{sgn}(\pi) \cdot \mathrm{sgn}(\rho)$.

1.3 Podgrupe

Definicija 1.11. 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. 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. Pri monoidih se enota ne deduje nujno, npr. $(\mathbb{Z}, \cdot)$ in $(\{0\}, \cdot)$.

Trditev 1.6. *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.*

Dokaz. Definicija podgrupe. □

Posledica 1.6.1. *Naj bo G končna grupa in $H \subseteq G,\ H \neq \emptyset$. Velja:*

$$H \leq G \Leftrightarrow H \textit{ je zaprta za množenje.}$$

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

Opomba. V končnih grupih ni potrebno preverjati zaprtost za invertiranje.

Primer. 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 $\mathrm{O}(n) = \left\{A \in \mathrm{GL}_n(\mathbb{R}) \mid AA^T = A^T A = I\right\}$. 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 1.7. *Naj bosta H in K podgrupi grupe G. Potem $H \cap K \leq G$. Enako velja za preseke poljubnih družin podgrup.*

Dokaz. Karakterizacija podrgupe. $\square$

Definicija 1.12. Naj bosta $H, K \leq G$. Definiramo $HK = \{hk \mid h \in H,\ k \in K\}$. Temu pravimo **produkt podgrup**.

Zgled. HK ni nujno podgrupa v G. Vzemimo $G = S_3,\ H = \{\mathrm{id}, (1\ 2)\},\ K = \{\mathrm{id}, (1\ 3)\}$.

Trditev 1.8. *Naj bosta $H, K \leq G$. Če velja $HK = KH$, potem je $HK \leq G$.*

Dokaz. Karakterizacija podrgupe in definicija produkta podgrup. $\square$

Opomba. 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 1.13. Naj bo $H \leq G,\ a \in G$. Definiramo množico $aHa^{-1} = \{aha^{-1} \mid h \in H\}$. Potem $aHa^{-1} \leq G$. Temu se reče **konjungiranje podgrupe H z elementom a**.

Dokaz. Karakterizacija podrgupe. $\square$

Trditev 1.9. *Naj bo G grupa.*

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

Dokaz. Karakterizacija podrgupe. $\square$

1.4 Odseki podgrup in Lagrangeev izrek

Naj bo G grupa in $H \leq G$. Definiramo relacijo na G s predpsiom $\forall a, b \in G \,.\, a \sim b :\Leftrightarrow a^{-1}b \in H$.

Trditev 1.10. *Relacija $\sim$ je ekvivalenčna relacija na G.*

Dokaz. Preverimo refleksivnost, simetričnost in tranzitivnost. $\square$

Definicija 1.14. Naj bo G grupa, $H \leq H,\ a \in G$. **Ekvivalenčni razred elementa** $a \in G$ je množica $[a] = \{b \in G \mid a \sim b\}$.

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

Definicija 1.15. Množico aH imenujemo **levi odsek grupe G po podgrupi H**.

Opomba. V grupo G lahko vpeljamo tudi relacijo $\approx$ s predpisom $\forall a, b \in G \,.\, a \approx b :\Leftrightarrow ab^{-1} \in H$.
To je ekvivalenčna relacija. Ekvivalentni razredi so $[a] = \{ha \mid h \in H\} =: Ha$, ki jih imenujemo **desni odseki**.

Definicija 1.16. Faktorska (oz. kvocientna) množica glede na relacijo $\sim$ je množica $G/_\sim = \{aH \mid a \in G\} =: G/H$.

Opomba. G/H ni nujno grupa.

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

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

Definicija 1.17. Naj bo G končna grupa. Moč množce G/H označimo z $G : H$ (oz $[G : H]$) in jo imenujemo **indeks podgrupe H v grupi G**.

Izrek 1.11 (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 $i = 1, \ldots, r$. $\square$

Posledica 1.11.1. *Moč vsake podgrupe končne grupe deli moč grupe.*

Opomba. 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 1.12. *G/H je za to operacijo Abelova grupa.*

Dokaz. Enostavno preverimo aksiome. $\square$

Primer. 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 1.12.1. *Za vsako število $n \in \mathbb{N}$ obstaja vsaj ena grupa moči n.*

1.5 Generatorji grup. Ciklične grupe

Definicija 1.18. 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. $\langle X \rangle$ je presek vseh podgrup grupe G, ki vsebujejo množico X.

Definicija 1.19. 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 $X = \{x_1, \dots, x_n\}$, pišemo $\langle \{x_1, \dots, x_n\} \rangle = \langle x_1, \dots, x_n \rangle$.
- Če je $G = \langle x_1, \dots, x_n \rangle$, 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 1.13. *Naj bo G grupa in $X \subseteq G$.* $\langle X \rangle = \left\{ x_{i_1}^{\pm 1} x_{i_2}^{\pm 1} \dots x_{i_r}^{\pm 1} \mid x_{i_j} \in X;\ r \in \mathbb{N}_0 \right\} =: S.$

Dokaz. Dovolj dokazati, da je S podgrupa grupe G. $\square$

Posledica 1.13.1. *Naj bo G grupa, $a \in G$. Potem* $\langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}$.

Primer. Primeri generatorjev grup:

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

Definicija 1.20. 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. 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 1.14. *Naj bo G grupa, $a \in G$. Potem je red elementa a enak n natanko tedaj, ko* $|\langle a \rangle| = n$.

Dokaz. Uporabimo ustrezne definicije in izreki o celih številih. $\square$

Posledica 1.14.1. *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.*

Dokaz. Uporabimo ustrezne definicije in izreki. $\square$

2 Uvod v teorijo kolobarjev

Definicija 2.1. 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. 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 2.2. 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. Primeri deliteljev niča, idempotentov in nilpotentov.

- V $\mathbb{R}^2$ 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 2.3. Cel kolobar je komutativen kolobar brez deliteljev niča.

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

Definicija 2.4. 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. $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ so polja.

Trditev 2.1. *Obrnljiv element kolobarja K ne more biti delitelj niča.*

Dokaz. Enostavno. □

Definicija 2.5. Naj bo A kolobar in F polje. A je **algebra** nad F, če

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

Zgled. Kolobarji in algebri.

- Naj bo K kolobar, $K^{n\times n} = M_n(K) = \{n \times n$ 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).
- Naj bo X neprazna množica. 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 $\mathbb{R}$.

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

Dokaz. Enostavno. □