

Algebra 2

11. december 2024

1 Uvod v teorijo grup

1.1 Osnovni pojmi teoriji grup

Definicija. Naj bo S neprazna množica. **Operacija na množice S** je preslikava $*$: $S \times S \rightarrow S$, $(a, b) \mapsto a * b$. 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. Neprazna množica S skupaj z operacijo $*$ je **polgrupa**, če je operacija $*$ asociativna.

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

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

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

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

Definicija. 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 **multiplikativni 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 $(xy)^n \neq x^n y^n$	$n(x + y) = nx + ny$
$xy = xz \Rightarrow y = z$	$x + y = x + z \Rightarrow y = z$ (pravila krajšanja)
$yx = zx \Rightarrow y = z$	
$xy = 1 \Rightarrow yx = 1$	

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

Zgled (Simetrije kvadrata). Simetrije kvadrata K so izometrije $f: \mathbb{R}^2 \rightarrow \mathbb{R}^2$, da je $f(K) = K$.

Primeri simetriji: r - rotacija za 90° okoli središča kvadrata, z - zrcaljenje čez fiksno os simetrije ter kompozicije r in z . Iz geometrije lahko vidimo, da je $zr = r^3z$. To pomeni, da je vsak kompozitum r in z oblike r^kz .

Kvadrat ima kvečjemu 8 simetriji, ker je vsaka simetrija določena s sliko oglišča 1 in informacijo, ali smo naredili zrcaljenje ali ne. Dobimo množico simetriji $D_{2,4} = \{\text{id}, r, r^2, r^3, z, rz, r^2z, r^3z\}$. $D_{2,4}$ 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 čez neko fiksno os simetrije.

Velja: $zr = r^{n-1}z$.

Množica vseh simetriji je $D_{2n} = \{1, r, r^2, \dots, r^{n-1}, z, rz, r^2z, \dots, r^{n-1}z\}$. D_{2n} je **diedrska grupa moči $2n$** .

Zgled (Monoid \rightarrow Grupa). Naj bo $(S, *)$ monoid. Definiramo $S^* = \{\text{obrnljive elementi iz } S\}$, potem S^* je grupa za $*$.

Primer. Naj bo $S = (\mathbb{R}^{n \times n}, \cdot)$, $S^* = \{A \in \mathbb{R}^{n \times n} \mid \det A \neq 0\} = \text{GL}_n(\mathbb{R})$. $\text{GL}_n(\mathbb{R})$ je **splošna linearna grupa $n \times n$ matrik**.

Zgled (Direktni produkt grup). Naj bodo G_1, G_2, \dots, G_n grupe z operacijami $*_1, *_2, \dots, *_n$. Na množice $G_1 \times G_2 \times \dots \times G_n$ vpeljamo operacijo $(g_1, g_2, \dots, g_n) * (h_1, h_2, \dots, h_n) = (g_1 *_1 h_1, g_2 *_2 h_2, \dots, g_n *_n h_n)$. Potem $(G_1 \times G_2 \times \dots \times G_n, *)$ je grupa.

1.2 Ponovitev o permutacijah

Izrek. Vsaka permutacija je produkt disjunktih ciklov.

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

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

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

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

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

1.3 Podgrupe

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

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

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

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

Dokaz. Karakterizacija podgrupe. □

Definicija. 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 $G = S_3$, $H = \{\text{id}, (1\ 2)\}$, $K = \{\text{id}, (1\ 3)\}$.

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

Dokaz. Karakterizacija podgrupe in definicija produkta podgrup. □

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. 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 **konjugiranje podgrupe H z elementom a** .

Dokaz. Karakterizacija podgrupe. □

Trditev. 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 podgrupe. □

1.4 Odseki podgrup in Lagrangeev izrek

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

Trditev. Relacija \sim je ekvivalenčna relacija na G .

Dokaz. Preverimo refleksivnost, simetričnost in tranzitivnost. □

Definicija. 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. 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. **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. 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 (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 $i = 1, \dots, r$. □

Posledica. 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. G/H je za to operacijo Abelova grupa.

Dokaz. Enostavno preverimo aksiome. □

Primer. Naj bo $G = \mathbb{Z}$ in $H = n\mathbb{Z}$, $n \in \mathbb{N}$. Potem $\mathbb{Z}/n\mathbb{Z} = \{0 + n\mathbb{Z}, 1 + n\mathbb{Z}, \dots, (n-1) + n\mathbb{Z}\}$.

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

1.5 Generatorji grup. Ciklične grupe

Definicija. 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. 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. 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 . □

Posledica. 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. 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. 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. □

Posledica. 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. □

2 Uvod v teorijo kolobarjev

Definicija. 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 $X \subseteq \mathbb{R}$, $\mathbb{R}^X = \{f : X \rightarrow \mathbb{R}\}$. Definiramo $(f + g)(x) = f(x) + g(x)$, $(fg)(x) = f(x)g(x)$. \mathbb{R}^X je komutativen kolobar.

Definicija. Naj bo K kolobar.

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

Zgled. Primeri deliteljev ničā, 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. **Cel kolobar** je komutativen kolobar brez deliteljev ničā.

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

Definicija. 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. Obrnljiv element kolobarja K ne more biti delitelj ničā.

Dokaz. Enostavno. □

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

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

2.1 Primeri kolobarjev in algeber

Kolobar (algebra) kvadratnih matrik

Naj bo K kolobar, $K^{n \times n} = M_n(K) = \{n \times n \text{ matrike z elementi iz } K\}$. $K^{n \times n}$ 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 $\text{End } V$. Potem $\text{End } V$ 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

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

Manj baročno:

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

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 $c_i = \sum_{j \geq 0} a_{i-j} b_j$.

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 pospoložitvi $K[X]$:

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

Trditev. Velja:

- Če je K komutativen kolobar, je tudi $K[X]$ komutativen.
- K je brez deliteljev nična natanko tedaj, ko $K[X]$ brez deliteljev nič.
- K je cel kolobar natanko tedaj, ko $K[X]$ cel.

Dokaz. Enostavno. □

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:

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

Trditev. Relacija \sim je ekvivalenčna.

Dokaz. Kot v \mathbb{Q} . □

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

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

Opomba. 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.

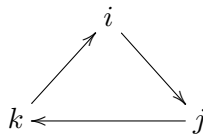
Trditev. Naj bo A algebra nad \mathbb{R} . Če je $\dim A$ liho število večje od 1, potem A ni obseg.

Dokaz. Izberimo $a \in A \setminus \text{Lin}\{1\}$ in definiramo endomorfizem $\mathcal{A}: A \rightarrow A$, $\mathcal{A}x = ax$. Poiščemo s pomočjo karakterisitčnega polinoma delitelji nič. □

Algebra kvaternionov

Primer. 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:



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

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 $\bar{z} = \lambda_1 \cdot 1 - \lambda_2 \cdot i - \lambda_3 \cdot j - \lambda_4 \cdot k$ je **konjugirani kvaternion**.

Trditev. \mathbb{H} je obseg.

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

Trditev. \mathbb{H} je algebra.

Dokaz. Preverimo usklajenost množenja in množenja s skalarjem. □

Pravimo, da je \mathbb{H} **kvaternioniska algebra**.

Grupa za množenje $(\{\pm 1, \pm i, \pm j, \pm k\}, \cdot)$ je **kvaternioniska grupa**. Označimo jo z Q .

2.2 Podkolobarji, podalgebre, podpolja

Definicija. 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. Podobno definiramo tudi **podalgebro** in **podpolje**.

Trditev. Naj bo K kolobar in $L \subseteq K$, $L \neq \emptyset$. Velja:

L je podkolobar kolobarja $K \Leftrightarrow$

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

Opomba. Distributivnost se podeduje.

Opomba. 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. $\mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$.

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

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

2.3 Kolobar ostankov in karakterizacija 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. Množenje je dobro definirano.

Dokaz. **TODO** □

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

Dokaz. **TODO** □

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

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

Primer. Določi

- $\text{char } \mathbb{Z}_n$.
- $\text{char } \mathbb{Z}$.

Trditev. Naj bo K kolobar z karakteristiko $n > 0$. Velja:

1. $n \cdot x = 0$ za vsak $x \in K$.
2. Naj bo $m \in \mathbb{N}$. $m \cdot 1 = 0 \Leftrightarrow n \mid m$.
3. Če je K neničeln kolobar in nima deljiteljev nič, potem je n praštevilo.