

# Algebrske strukture - zapiski predavanj prof. Klavžarja

Yon Ploj

2. semester 2021

## Kazalo

0.1	Lastnosti operacij . . . . .	1
<b>1</b>	<b>Algebrske strukture</b>	<b>2</b>
1.1	Množica $\mathbb{Z}_n$ . . . . .	2
<b>2</b>	<b>Grupe</b>	<b>3</b>
<b>3</b>	<b>Podgrupe</b>	<b>4</b>
<b>4</b>	<b>Ciklične in permutacijske grupe, izomorfizmi</b>	<b>5</b>
4.1	Permutacijske grupe . . . . .	6
4.2	Izomorfizmi grup . . . . .	7
<b>5</b>	<b>Odseki in pogrupe edinke</b>	<b>8</b>
5.1	Podgrupe edinke in faktorske grupe . . . . .	10
<b>6</b>	<b>Kolobarji in polja</b>	<b>11</b>
6.1	Lastnosti kolobarjev . . . . .	12
6.2	Podkolobarji . . . . .	12
6.3	Delitelji ničla in celi kolobarji . . . . .	13
6.4	Polja in obsegi . . . . .	13
6.5	Podpolja . . . . .	14
6.6	Karakteristika kolobarja . . . . .	15
6.7	Ideali . . . . .	15
<b>7</b>	<b>Kolobarji polinomov</b>	<b>16</b>
7.1	Ničle polinomov in nerazcepni polinomi . . . . .	18

## 0.1 Lastnosti operacij

**Definicija 0.1** (Asociativnost).

$$(a \cdot b) \cdot c = a \cdot (b \cdot c)$$

**Definicija 0.2** (Komutativnost).

$$a \cdot b = b \cdot a$$

**Definicija 0.3** (Enota).

$$a \cdot e = e \cdot a = a$$

**Izrek 0.4.** Enota je enolična.

*Dokaz.* Predpostavimo, da obstajata dve enoti  $e_1$  in  $e_2$ . Ker je  $e_1$  enota, je  $e_1 \cdot e_2 = e_2$ . Ker je  $e_2$  enota, je  $e_1 \cdot e_2 = e_1$ . Sledi, da je  $e_1 = e_2$ . ■

**Definicija 0.5** (Inverz / Obratna vrednost  $a$ ).

$$a \cdot a^{-1} = a^{-1} \cdot a = e$$

*Opomba.* Inverz abstraktnega množenja označujemo z  $a^{-1}$ , inverz abstraktnega seštevanja pa z  $-a$ .

**Izrek 0.6.** Inverz je enoličen, če imamo asociativnost.

*Dokaz.* Predpostavimo asociativnost in obstoj dveh inverzov  $b_1$  in  $b_2$ .

$$b_1 = b_1 \cdot e = b_1 \cdot (a \cdot b_2) = (b_1 \cdot a) \cdot b_2 = e \cdot b_2 = b_2$$

## 1 Algebrske strukture

**Definicija 1.1** (Notranja operacija množice  $A$ ).

$$f : A \times A \rightarrow A$$

Z infiksno notacijo označujemo  $f(a, b)$  kot  $a \cdot b$  ali  $ab$

**Definicija 1.2** (Algebrska struktura). Množica z vsaj eno notrajno operacijo

**Definicija 1.3** (Grupoid). Množica z notrajno operacijo.  $(M, \cdot)$

**Definicija 1.4** (Polgrupa). Asociativen grupoid.

**Definicija 1.5** (Monoid). Polgrupa z enoto.

**Definicija 1.6** (Grupa). Monoid, kjer je vsak element obrnljiv.

**Definicija 1.7** (Abelova grupa). Komutativna grupa.

### 1.1 Množica $\mathbb{Z}_n$

**Definicija 1.8** (Kongruenca).  $a$  in  $b$  sta kongruentna po modulu  $m$  ntk. obstajajo  $p, q, r \in \mathbb{Z}_n$ , da velja:

$$a = p * m + r$$

$$b = q * m + r$$

$$r < p \quad \wedge \quad r < q$$

Relacija kongruence je ekvivalenčna, zato razdeli  $\mathbb{Z}_n$  na ekvivalenčne razrede ostankov:  $\{0, 1, \dots, n-1\}$

*Opomba.* V nadaljevanju bomo uporabljali operaciji  $+_n$  in  $\cdot_n$  kot seštevanje/množenje po modulu  $n$ .

**Trditev 1.9.**  $(\mathbb{Z}_n, +_n)$  je grupa

**Trditev 1.10.**  $(\mathbb{Z}_n, \cdot_n)$  je monoid

$x \in \mathbb{Z}_n$  je obrnljiv  $\iff x \perp m$ . Zato velja, da so vsi elementi v  $\mathbb{Z}_p$  (kjer je  $p$  praštevilo) obrnljivi.  $\mathbb{Z}_p$  je torej grupa.

## 2 Grupe

**Definicija 2.1** (Cayleyeva tabela). Tabela, ki prikazuje definicijo operacije v končnem monoidu.

$$\begin{array}{c} \cdot \quad i \quad r \quad s \quad x \quad y \quad z \\ \begin{array}{c} i \\ r \\ s \\ x \\ y \\ z \end{array} \left[ \begin{array}{cccccc} i & r & s & x & y & z \\ r & r & s & i & y & z & x \\ s & s & i & r & z & x & y \\ x & x & z & y & i & s & r \\ y & y & x & z & r & i & s \\ z & z & y & x & s & r & i \end{array} \right] \end{array}$$

*Opomba.* V Cayleyevi tabeli grupe so vsi elementi v vsakem stolpcu in vsaki vrstici med seboj različni (Cayleyeva tabela je latinski kvadrat reda  $n$ ). To sledi iz izreka 2.2

**Izrek 2.2** (Pravilo krajšanja). Če je  $(G, \cdot)$  grupa in  $a, b, c \in G$ , potem velja:

$$ba = ca \implies b = c$$

$$ab = ac \implies b = c$$

*Dokaz.* Naj bo  $ba = ca$ . Na desni pomnožimo z  $a^{-1}$  in zaradi asociativnosti dobimo:

$$(ba)a^{-1} = (ca)a^{-1}$$

$$b(aa^{-1}) = c(aa^{-1})$$

$$be = ce$$

$$b = c$$

■

**Definicija 2.3** (Red elementa). Naj bo  $(G, \cdot)$  končna grupa. Tedaj je red elementa  $a \in G$  najmanjše naravno število  $n$ , za katerega velja

$$a^n = e$$

Če je  $G$  neskončna in za  $a$  ne obstaja noben  $n$  da velja  $a^n = e$ , je red  $a$  neskončno.

**Trditev 2.4.** Red elementa je dobro definiran

*Dokaz.* Poglejmo zaporedje:  $a^1, a^2, \dots, a^{k+1}$ , kjer je  $k = |G|$ . Zaporedje ima  $k+1$  elementov, naša grupa pa jih ima  $k$ . Po dirichletovem načelu

$$\exists p, q : (p \neq q \wedge (\text{BŠS } p < q) \wedge a^p = a^q)$$

Tedaj

$$e = (a^p)(a^p)^{-1} = (a^q)(a^p)^{-1} = a^q a^{-p} = a^{q-p}$$

Sledi  $a^{q-p} = e$ , kar smo želeli pokazati.

■

*Opomba.* Red enote je 1 in ker je enota enolična, je enota edini element reda 1.

### 3 Podgrupe

**Definicija 3.1** (Podgrupa). Naj bo  $(G, \cdot)$  grupa. Tedaj je  $H \subseteq G$  podgrupa, če je  $(H, \cdot)$  tudi grupa. Pri tem je operacija obakrat ista. Označimo  $H \leq G$ .

**Definicija 3.2** (Prava podgrupa). Naj bo  $(H, \cdot)$  podgrupa  $(G, \cdot)$ . Če je  $H \subset G$  (torej  $H \neq G$ ), je  $H$  prava podgrupa  $G$ . Označimo  $H < G$ .

*Primer* (Trivialna podgrupa). Za vsako grupo  $G$  velja  $G \leq G$  in  $\{e\} \leq G$ .

*Primer.*  $(\mathbb{Q}^+, \cdot) < (\mathbb{R}^+, \cdot)$

*Primer.*  $F := \{f : \mathbb{R} \rightarrow \mathbb{R}\}$ .  $(F, +)$  je grupa.

$C := \{f : \mathbb{R} \rightarrow \mathbb{R}; f \text{ je zvezna}\}$ .  $(C, +)$  je grupa.

$(C, +) < (F, +)$

**Izrek 3.3** (Glavni izrek o podgrupah). Naj bo  $(G, \cdot)$  grupa in  $\emptyset \neq H \subseteq G$ . Tedaj je  $(H, \cdot)$  podgrupa v  $(G, \cdot)$  natanko tedaj, ko

$$\forall x, y \in H : (x^{-1}y \in H)$$

*Dokaz.*  $(\Rightarrow)$  Naj bosta  $x, y \in H$ . Ker je  $(H, \cdot)$  podgrupa in s tem sama zase grupa, je tudi  $x^{-1} \in H$ . Zato je tudi  $x^{-1}y \in H$ .

$(\Leftarrow)$  Naj  $\forall x, y \in H : (x^{-1}y \in H)$ .

- asociativnost  
če so  $x, y, z \in H$ , potem so tudi  $x, y, z \in G$ . Ker v  $G$  velja asociativnost, velja tudi v  $H$ .
- enota  
Ker je  $H \neq \emptyset$ ,  $\exists x \in H$ . Postavimo  $y = x$ . Potem je tudi  $x^{-1}x = e \in H$ .
- inverz  
Vemo, da je  $e \in H$ . Naj bo  $x \in H$ . Postavimo  $y = e$ :  $x^{-1}y \in H \implies x^{-1}e \in H \implies x^{-1} \in H$ .
- zaprtost  
 $x, y \in H$ . Vemo že, da je  $x^{-1} \in H$ , zato je tudi  $(x^{-1})^{-1} \in H$ . Zato je  $xy = (x^{-1})^{-1}y \in H$ .

■

Za končne grupe je kriterij še enostavnejši:

**Izrek 3.4.** Naj bo  $(G, \cdot)$  končna grupa in  $\emptyset \neq H \subseteq G$ . Tedaj je  $(H, \cdot) \leq (G, \cdot) \iff (x, y \in H \implies xy \in H)$

*Dokaz.* Dokaz je tako zelo enostaven, da ga ne bomo šli dokazovat. Glavna ideja je, da malo gledate ta zaporedja in potem dobite neke zaključke. ■

**Definicija 3.5** (Ciklična podgrupa). Naj bo  $(G, \cdot)$  grupa in  $a \in G$ . Potem naj bo

$$\langle a \rangle := \{a^n : n \in \mathbb{Z}\}$$

Podgrupa  $(\langle a \rangle, \cdot)$  je ciklična podgrupa v  $G$ , generirana z elementom  $a$ .

**Trditev 3.6.** Če je  $(G, \cdot)$  grupa in  $a \in G$ , potem je

$$(\langle a \rangle, \cdot) \leq (G, \cdot)$$

*Dokaz.* Ker je  $a^1 = a$ , je  $a \in \langle a \rangle$ , torej  $\langle a \rangle \neq \emptyset$ . Naj bosta sedaj  $a^n, a^m \in \langle a \rangle$ . Ker je

$$(a^n)^{-1}a^m = (a^{-1})^n a^m = a^{m-n} \in \langle a \rangle$$

je po glavnem izreku potem  $(\langle a \rangle, \cdot)$  podgrupa grupe  $G$ . ■

*Primer.*  $(\mathbb{Z}_{12}, +_{12})$

$$\langle 3 \rangle = \{3, 6, 9, 0\}$$

$$(\{0, 3, 6, 9\}, +_{12}) \leq (\mathbb{Z}_{12}, +_{12})$$

**Definicija 3.7** (Center grupe). Naj bo  $(G, \cdot)$  grupa. Potem je  $Z(G)$  center grupe  $G$  podmnožica z elementi, ki komutirajo z vsemi elementi v  $G$ .

$$Z(G) = \{a \in G : \forall x \in G (ax = xa)\}$$

*Opomba.* Če je  $G$  abelova, je  $Z(G) = G$ .

**Izrek 3.8.** Če je  $(G, \cdot)$  grupa, potem je  $(Z(G), \cdot) \leq (G, \cdot)$ .

*Dokaz.* Pokažimo najprej, da  $a \in Z(G) \implies a^{-1} \in Z(G)$ . Če  $a$  komutira z vsemi  $x \in G$ , potem tudi  $a^{-1}$  komutira z vsemi  $x \in G$ :

$$a^{-1} \cdot / \quad ax = xa \quad / \cdot a^{-1}$$

$$a^{-1}axa^{-1} = a^{-1}xaa^{-1}$$

$$(a^{-1}a)xa^{-1} = a^{-1}ax(a^{-1})$$

$$xa^{-1} = a^{-1}x$$

Sedaj pa še  $a^{-1}b \in Z(G)$ :

$$(a^{-1}b)x = a^{-1}(bx) = a^{-1}(xb) = (a^{-1}x)b = (xa^{-1})b = x(a^{-1}b)$$

Po izreku 3.3 je to zadosti. ■

## 4 Ciklične in permutacijske grupe, izomorfizmi

**Definicija 4.1** (Ciklična grupa). Naj bo  $(G, \cdot)$  grupa in  $a \in G$ . Če velja

$$\langle a \rangle = G$$

kjer je  $\langle a \rangle$  definiran kot v 3.5:

$$\langle a \rangle := \{a^n : n \in \mathbb{Z}\}$$

potem je  $G$  ciklična grupa,  $a$  pa njen generator.

*Primer.*  $(\mathbb{Z}, +)$  je ciklična grupa z generatorjema 1 in  $-1$ .

*Primer.*  $(\mathbb{Z}_9, +)$  je ciklična grupa. 1 je gotovo generator, obstajajo pa tudi drugi (recimo 4). Našteli jih bomo kasneje.

**Izrek 4.2.** Naj bo  $G$  grupa in  $a \in G$ .

1. Če ima  $a$  neskončen red, potem so vse potence  $a^n$  med seboj paroma različne.
2. Če ima  $a$  končen red, potem je

$$\langle a \rangle = \{e, a, a^2, \dots, a^{n-1}\}$$

Nadalje,  $a^i = a^j$  velja natanko tedaj, ko  $n \mid (i - j)$ .

*Dokaz.*

1. Naj ima  $a$  neskončen red. Opazujmo  $a^i$  in  $a^j$ ,  $i \neq j$ . Če bi veljalo  $a^i = a^j$ , bi  $a^{i-j} = e$ . Ampak  $i \neq j$ : to bi pomenilo, da ima  $a$  končen red.

2. Naj ima  $a$  končen red  $n$ .

$$X := \{e, a, a^2, \dots, a^{n-1}\}$$

Pokažimo  $\langle a \rangle = X$ . Očitno je  $X \subseteq \langle a \rangle$ , saj  $a^i \in X \xrightarrow{\text{def}} a^i \in \langle a \rangle$ . Pokažimo torej, da  $\langle a \rangle \subseteq X$ , oziroma:

$$a^k, k \in \mathbb{Z} \implies a^k \in X$$

Po izreku o deljenju:

$$k = p \cdot n + r \quad 0 \leq r < n$$

$$a^k = a^{p \cdot n + r} = a^{pn} \cdot a^r = (a^n)^p \cdot a^r = e^p \cdot a^r = a^r$$

ampak  $0 \leq r < n$ , torej  $a^k = a^r \in X$

3.  $a^i = a^j \iff n|(i-j)$ :

$$i - j = p \cdot n + r$$

( $\Rightarrow$ ) Naj bo  $a^i = a^j$ . Tedaj

$$e = a^{i-j} = a^{p \cdot n + r} = a^p \cdot a^r = a^r \quad r < n$$

Ker je red  $a$  enak  $n$  in je  $r < n$ , velja  $r = 0$ . Torej  $i - j = p \cdot n$ , oziroma  $n|(i-j)$ .

( $\Leftarrow$ ) Naj  $n|(i-j)$ .

$$i - j = p \cdot n + r \quad (0 \leq r < n) \xrightarrow{n|(i-j)} r = 0 \implies i - j = p \cdot n$$

$$a^i = a^{p \cdot n + j} = (a^n)^p \cdot a^j = a^j$$

■

**Posledica 4.3.** Naj bo  $G$  grupa in  $a \in G$  reda  $n$ . Če  $a^k = e$ , potem  $n|k$ .

*Dokaz.*

$$a^0 = e = a^k$$

Poprej vemo, da  $a^i = a^j \iff n|(i-j)$ . Vstavimo  $i = k, j = 0$ , dobimo  $n|(k-0)$ , torej  $n|k$ . ■

**Izrek 4.4.** Naj bo  $G$  ciklična grupa in  $a \in G$  element reda  $n$ . Potem je  $G = \langle a^k \rangle$  natanko tedaj, ko je  $(n, k) = 1$

*Primer.*

$$(\mathbb{Z}_9, +) = \langle 1 \rangle = \langle 9 \rangle$$

$$\mathbb{Z}_9 = \langle 1^k \rangle \iff \langle k, 9 \rangle = 1$$

Torej generatorji so 1, 2, 4, 5, 7, 8.

## 4.1 Permutacijske grupe

**Definicija 4.5** (Permutacija množice  $A$ ). Je bijekcija  $A \rightarrow A$ .

**Definicija 4.6** (Permutacijska grupa). Je množica permutacij, ki za komponiranje preslikav tvorijo grupo.

**Definicija 4.7** (Simetrična grupa  $S_n$ ). Če vzamemo vse permutacije množice  $[n]$ , dobimo simetrično grupo  $S_n$ . Ta grupa ni abelova.

**Trditev 4.8.**  $|S_n| = n!$

**Trditev 4.9.** Vsako permutacijo lahko enolično (do vrstnega reda faktorjev natančno) zapišemo kot produkt disjunktnih ciklov.

*Dokaz.* Lmao you thought

■

**Trditev 4.10.** Vsako permutacijo lahko zapišemo kot produkt transpozicij.

**Trditev 4.11.** Neko permutacijo lahko zapišemo bodisi samo kot produkt sodo ali liho število transpozicij. Pravimo, da je permutacija liha ali soda.

**Definicija 4.12** (Alternirajoča grupa  $A_n$ ). Je grupa vseh sodih permutacij množice  $[n]$ .

Dokaz da je to grupa lahko naredite sami.

**Izrek 4.13.** Če je  $n > 1$ , potem je  $|A_n| = \frac{n!}{2}$

*Dokaz.* Vzemimo poljubno liho permutacijo  $\Pi$ .

$$\begin{array}{ccc} \Pi & \rightarrow & (12) \cdot \Pi \\ \text{liha} & \text{injektivno} & \text{soda} \end{array}$$

$$\forall \Pi, \Sigma \text{ lihi: } \Pi \neq \Sigma \implies (12) \cdot \Pi \neq (12) \cdot \Sigma$$

Število sodih permutacij  $\geq$  število lihih permutacij. Z obratnim razmislekom ugotovimo, da je število sodih = število lihih permutacij. ■

## 4.2 Izomorfizmi grup

**Definicija 4.14** (Homomorfizem). Naj bosta  $(G, \cdot)$  in  $(H, *)$  grupe. Preslikava  $\alpha: G \rightarrow H$  je homomorfizem, če

$$\forall a, b \in G : \alpha(a \cdot b) = \alpha(a) * \alpha(b)$$

**Definicija 4.15** (Avtomorfizem). Homomorfizem  $G \rightarrow G$ .

**Definicija 4.16** (Izomorfizem). Bijektivni homomorfizem.

**Definicija 4.17** (Izomorfni grupi). Grupi, med katerima obstaja izomorfizem.

**Izrek 4.18** (Cayleyev). Vsaka grupa je izomorfna neki permutacijski grupi.

*Dokaz.* Naj bo  $G$  poljubna grupa in  $g \in G$ . Definirajmo  $T_g : G \rightarrow G$ :

$$T_g(x) = gx$$

$T_g$  je permutacija množice  $G$ .

$H = \{T_g : g \in G\}$  je grupa za komponiranje.

$H \cong G$  ■

**Trditev 4.19.** Če je  $\alpha : G \rightarrow H$  izomorfizem grup, potem (med drugim) veljajo naslednje lastnosti:

- $\alpha$  preslika enoto  $G$  v enoto  $H$ .
- če je  $a \in G, n \in \mathbb{Z} \implies \alpha(a^n) = (\alpha(a))^n$
- če  $a$  in  $b$  komutirata v  $G$ , potem  $\alpha(a)$  in  $\alpha(b)$  komutirata v  $H$ .
- $G$  je abelova  $\iff H$  je abelova.
- $G$  je ciklična  $\iff H$  je ciklična.
- če je  $K \leq G$ , potem je  $\alpha(K) = \{\alpha(k) : k \in K\} \leq H$

## 5 Odseki in pogrupe edinke

Naj bo  $G$  grupa in  $H \subseteq G$ . Za  $a \in G$  definirajmo:

**Definicija 5.1** (Levi odsek  $aH$ ).

$$aH = \{ak : k \in H\}$$

**Definicija 5.2** (Desni odsek  $Ha$ ).

$$Ha = \{ka : k \in H\}$$

*Primer.*  $G = S_3$ .  $H = \{(1), (2)\}$

- $(1)H = H$
- $(12)H = \{(12)(1), (12)(2)\} = \{(12), (1)(2)(3)\} = H$
- $(13)H = \{(13)(1), (13)(2)\} = \{(13), (123)\}$
- $(23)H = \{(23)(1), (23)(2)\} = \{(23), (123)\}$
- $(123)H = \{(123)(1), (123)(2)\} = \{(123), (13)\}$
- $(132)H = \{(132)(1), (132)(2)\} = \{(132), (23)\}$

*Primer.*  $G = (\mathbb{Z}_{10}, +)$ .  $H = (\{0, 2, 4, 6, 8\}, +)$

- $0 + H = 2 + H = 4 + H = 6 + H = 8 + H$
- $1 + H = 3 + H = 5 + H = 7 + H = 9 + H$

Ugotovitve: opazimo, da odseki niso nujno podgrupe  $H$ . Lahko se zgodi, da je  $aH = bH$  za  $a \neq b$  ( $H(13) = (13)H$ ).  $aH \neq Ha$  je povsem možno.

**Trditev 5.3** (Najpomembnejše lastnosti odsekov). Naj bo  $H$  poljubna podgrupa grupe  $G$ ,  $a, b \in G$ . Tedaj veljajo naslednje lastnosti:

1.  $a \in aH \wedge a \in Ha$
2.  $aH = H \iff a \in H \iff Ha = H$
3. bodisi  $aH = Ha$  bodisi  $aH \cap Ha = \emptyset$
4.  $aH = bH \iff a^{-1}b \in H \iff Ha = Hb$
5.  $|aH| = |bH| \wedge |Ha| = |Hb|$
6.  $aH = Ha \iff H = aHa^{-1}$
7.  $aH \leq G \iff a \in H \iff Ha \leq G$

*Dokaz.* Dokazali bomo prve tri trditve, ostale si boste pa sami.

1.  $a \in aH$ :  $e \in H \implies a \cdot e \in aH$
2.  $aH = H \iff a \in H$ :

( $\implies$ ) Naj velja  $aH = H$ . Ker je  $a \in aH$  (po 1.) in ker je  $aH = H$ , je  $a \in H$ .

( $\impliedby$ ) Naj bo  $a \in H$ . Dokažimo  $aH = H$ .

Najprej  $aH \subseteq H$ : Naj bo  $x \in aH$ . Torej je  $x = ak$  za nek  $k \in H$ .

$$a \in H, k \in H \implies ak \in H$$

Sedaj še  $H \subseteq aH$ : naj bo  $k \in H$ . Ker je  $a \in H$ , je

$$a^{-1} \in H \implies a^{-1}k \in H$$



$$a(a^{-1}k) = k \in aH$$

3. Če sta odseka disjunktna, ni kaj dokazovati. Recimo, da obstaja  $x \in aH \cup bH$ .  $x \in aH \implies x = ak$  za nek  $k \in H$ .  $x \in bH \implies x = bk'$  za nek  $k' \in H$ . Torej  $ak = bk'$ .

$$a = bk'k^{-1}$$

$$aH = (bk'k^{-1})H = (bk')(k^{-1}H)$$

Točka 2 pravi, da  $k^{-1}H = H$  (ker je  $k^{-1} \in H$ ).

$$aH = (bk')H = b(k'H) = bH$$

■

Če združimo lastnosti 1, 2 in 5, ugotovimo, da levi odseki po podgrupi  $H$  razdelijo grupo  $G$  v (paroma disjunktne) bloke iste moči.

*Primer.*  $G = (\mathbb{R}^2, +)$ .  $H$  = premica skozi izhodišče.

$$(a, b) \in \mathbb{R}^2 : (a, b)H = (a, b) + H = \{(a + x, b + y) : (x, y) \in H\}$$

Desni odseki po podgrupi  $H$  (premica  $p$ ) nam razdelijo ravnino v premice, ki so vzporedne s  $p$ .

**Izrek 5.4** (Lagrange). Moč podgrupe deli moč grupe. Število različnih levih (in desnih) odsekov po  $H$  je  $\frac{|G|}{|H|}$ .

*Dokaz.* Naj bodo  $a_1H, \dots, a_kH$  paroma različni levi odseki podgrupe  $H$ . Tedaj velja:

$$|G| = |a_1H \cup \dots \cup a_kH|$$

To nam zagotavlja prva lastnost trditve 5.3 ( $a \in aH$ ).

$$= |a_1H| + \dots + |a_kH|$$

(po lastnosti 3)

$$= k \cdot |H|$$

(po lastnosti 5)

$$\implies k = \frac{|G|}{|H|}$$

■

**Posledica 5.5.** Red elementa končne grupe deli moč grupe.

*Dokaz.* Vzemimo poljuben element  $a \in G$  reda  $n$ .

$$\langle a \rangle = \{e, a, \dots, a^{n-1}\} \leq G \xrightarrow{\text{lagrange}} n = |\langle a \rangle| \text{ deli } |G|$$

■

**Posledica 5.6.** Grupa praštevilske moči je ciklična.

*Dokaz.*

$$|\langle a \rangle| \text{ deli } p \quad |\langle a \rangle| \geq 2$$

Od tod sledi, da  $|\langle a \rangle| = p$ , torej  $\langle a \rangle = G$ .

■

**Posledica 5.7.** Če je  $a$  element končne grupe  $G$ , velja  $a^{|G|} = e$ .

*Dokaz.* Po posledici 5.5  $n$  deli  $|G|$ , torej  $|G| = k \cdot n$ .

$$a^{|G|} = a^{k \cdot n} = (a^n)^k = e$$

■

**Posledica 5.8** (Mali Fermatov izrek). Če je  $p$  praštevilo in  $a \in \mathbb{Z}$ , potem je

$$a^p \bmod p = a \bmod p$$

*Dokaz.*  $a = k \cdot p + r$ , kjer  $0 \leq r < p$ . Naj bo  $r = 0$ :  $a \bmod p = 0$ ,  $a^p \bmod p = 0$ . Naj bo  $1 \leq r < p$ : pogledjmo grupo

$$G := (\mathbb{Z}_p - \{0\}, \cdot) \quad |G| = p - 1$$

Po posledici 5.7 velja  $r^{p-1} = 1$ , torej  $r^p = r$ .

■

## 5.1 Podgrupe edinke in faktorske grupe

**Definicija 5.9** (Podgrupa edinka). Podgrupa  $H$  je edinka, če velja

$$\forall a \in G : (aH = Ha)$$

Označimo  $H \triangleleft G$ .

Po točki 6 iz lastnosti odsekov (5.3) je torej

$$H \triangleleft G \iff H = aHa^{-1} \quad \forall a \in G$$

**Trditev 5.10.**  $aHa^{-1} \leq G$

*Dokaz.*

$$x, y \in aHa^{-1} \implies x^{-1}y \in aHa^{-1}$$

$$x = aka^{-1} \quad \text{za nek } k \in H$$

$$y = ak'a^{-1} \quad \text{za nek } k' \in H$$

$$x^{-1}y = (aka^{-1})^{-1}(ak'a^{-1}) = (ak^{-1}a^{-1})(ak'a^{-1}) = a(k^{-1}k')a^{-1} \implies x^{-1}y \in aHa^{-1}$$

■

*Primer.*

$$a = e \quad eHe^{-1} = \{eke^{-1} : k \in H\} = \{k : k \in H\} = H$$

**Definicija 5.11** (Konjugirana grupa).  $aHa^{-1}$  je konjugirana grupa v  $G$

**Trditev 5.12.**  $H \triangleleft G$ , če je to edina možna konjugirana grupa v  $G$ .

**Definicija 5.13** (Enostavna grupa). Je grupa, katere edini edinki sta  $G$  in  $\{e\}$ .

Osrednji razlog za pomembnost edink je to, da lahko iz odsekov edink tvorimo grupo.

Naj bo  $G$  grupa in  $H \leq G$ . Definirajmo množico odsekov

$$G/H := \{aH : a \in G\}$$

in vpeljimo operacijo

$$(aH) * (bH) := (ab)H$$

**Izrek 5.14.** Če je  $H \triangleleft G$ , potem je  $(G/H, *)$  grupa.

*Dokaz.* Vse lastnosti grupe zelo lahko sledijo iz definicije odseka in operacije med njimi.

- enota:  $eH$
- inverz:  $a^{-1}H$
- ...

Bistvo je, da pokažemo, da je  $*$  dobro definirana, t.j. da je rezultat neodvisen od izbire elementa iz odseka.

Naj bosta  $a$  in  $a'$  iz istega odseka ( $aH = a'H$ ) ter  $b$  in  $b'$  iz istega odseka ( $bH = b'H$ ). Pokazati moramo, da je  $(aH) * (bH) = (a'H) * (b'H)$ .

$$\begin{aligned}
 a' \in aH &\implies a' = ak' \quad k' \in H \\
 b' \in bH &\implies b' = bk'' \quad k'' \in H \\
 (a'H) * (b'H) &\stackrel{\text{def.}}{=} (a'b')H = ak'bk''H = ak'b(k''H) \\
 ak'(bH) &\stackrel{\text{edinka}}{=} ak'(Hb) = a(k'H)b \stackrel{k' \in H}{=} aHb \\
 a(Hb) &\stackrel{\text{edinka}}{=} a(bH) \stackrel{\text{def.}}{=} (aH) * (bH)
 \end{aligned}$$

■

**Definicija 5.15** (Faktorska grupa grupe  $G$  po edinki  $H$ ). Grupa  $(G/H, *)$  po zgoraj definiranih operacijah  $*$  in  $/$ .

**Izrek 5.16.** Če je  $G$  grupa in  $G/Z(G)$  ciklična grupa, potem je  $G$  abelova.

*Dokaz.* QED.

■

## 6 Kolobarji in polja

*Opomba.* Hi, author here. V naslednjem razdelku spuščam nekatere dokaze in primere, ker so bodisi zelo trivialni, ali pa smo jih že videli pri Linearni algebri. Spuščeni dokazi so označeni z “Redacted”. Author out.

**Definicija 6.1** (Kolobar). Množica z 2 operacijama  $(R, +, \cdot)$  kjer je  $(R, +)$  abelova grupa in  $(R, \cdot)$  polgrupa.

Velja distributivnost množenja prek seštevanja:

$$a(b + c) = ab + ac \quad \wedge \quad (a + b)c = ac + bc$$

**Definicija 6.2** (Komutativen kolobar). Kolobar, v katerem je množenje komutativno.

*Primer.*  $2\mathbb{Z}$  soda cela števila.

**Definicija 6.3** (Kolobar z enoto). Kolobar, v katerem obstaja enota za množenje.

*Primer.*  $M_2(\mathbb{Z})$  2x2 matrike z elementi iz  $\mathbb{Z}$ .

**Definicija 6.4** (Kokoid). Komutativen kolobar z identiteto (enoto).

**Definicija 6.5** (Direktna vsota).

$$\begin{aligned}
 (R, +_R, \cdot_R) \oplus (S, +_S, \cdot_S) &:= (R \times S, +_{R \times S}, \cdot_{R \times S}) \\
 (r, s) +_{R \times S} (r', s') &:= (r +_R r', s +_S s') \\
 (r, s) \cdot_{R \times S} (r', s') &:= (r \cdot_R r', s \cdot_S s')
 \end{aligned}$$

**Izrek 6.6.** Če sta  $R$  in  $S$  kolobarja, je  $R \oplus S$  kolobar. Če imata enoto, jo ima tudi produkt. Če sta komutativna, je tak tudi produkt.

*Dokaz.* Z enostavnim izračunom. ■

*Opomba.* Konstrukcijo lahko razširimo na direktne vsote končnega števila kolobarjev:  $R_1 \oplus R_2 \oplus \dots \oplus R_n$ . To je v bistvu posplošitev  $\mathbb{R}^n$ .

## 6.1 Lastnosti kolobarjev

- Nevtralni element za  $+$ , torej  $0$ , je enoličen.
- Če je  $R$  kolobar z enoto  $1$ , je tudi ta enolična.

**Izrek 6.7.** Naj bo  $R$  kolobar in  $a, b \in R$ . Potem velja:

1.  $0 \cdot a = a \cdot 0 = 0$
2.  $(-a) \cdot b = a \cdot (-b) = -(a \cdot b)$
3.  $(-a) \cdot (-b) = a \cdot b$

*Dokaz.* Redacted. ■

**Posledica 6.8.** Če ima kolobar enoto  $1$ , velja  $(-1) \cdot a = -(1 \cdot a) = -a$

## 6.2 Podkolobarji

**Definicija 6.9.** Naj bo  $R$  kolobar in  $S \subseteq R$ . Če je  $S$  kolobar za isti operaciji kot jih ima  $R$ , je  $S$  podkolobar kolobarja  $R$ .

*Primer.*  $\mathbb{Z} \subseteq \mathbb{Q}$

*Primer.*  $\mathbb{Q} \subseteq \mathbb{R}$

*Primer.*  $n \geq 2 \quad n\mathbb{Z} \subseteq \mathbb{Z}$

**Izrek 6.10.**  $S$  je podkolobar  $R$  natanko tedaj, ko velja vse izmed:

- $S \subseteq R$
- $0 \in S$
- $\forall a, b \in S : a - b \in S$
- $\forall a, b \in S : a \cdot b \in S$

*Dokaz.* Redacted. ■

**Definicija 6.11** (Center kolobarja). Je množica tistih elementov, ki komutirajo z vsemi elementi.

$$\{x \in R : ax = xa \quad \forall x \in R\}$$

**Trditev 6.12.** Center kolobarja je njegov podkolobar.

*Dokaz.* Redacted. ■

### 6.3 Delitelji ničā in celi kolobarji

*Primer.* Kolobar  $(\mathbb{Z}_6, +, *)$ . Vemo, da je  $1 * 3 = 5 * 3$ , iz tega pa ne sledi, da  $1 = 5$ .

**Definicija 6.13** (Delitelj ničā).  $a \in R$  je delitelj ničā, če obstaja  $b \in R, b \neq 0$ , tako da je  $ab = 0$ .

**Definicija 6.14** (Cel kolobar). Komutativen kolobar z enoto (kokoid) brez deliteljev ničā.

*Primer.*  $\mathbb{Z}_n$ , kjer  $n$  ni praštevilo, ni cel kolobar.

*Primer.*  $\{a + b\sqrt{2}; a, b \in \mathbb{Z}\}$  je cel kolobar.

**Izrek 6.15** (Pravilo krajšanja). Če je  $(R, +, *)$  cel kolobar, potem v njem velja pravilo krajšanja (2.2) za  $*$ .

*Dokaz.*

$$ab - ac = 0 \implies a(b - c) = 0 \xrightarrow{R \text{ je cel}} b - c = 0 \implies b = c$$

■

**Trditev 6.16.** Pravilo krajšanja implicira poln kolobar.

*Dokaz.*

$$\begin{aligned} ab = 0, a \neq 0 \\ a0 = 0 \\ ab = a0 \implies b = 0 \end{aligned}$$

■

### 6.4 Polja in obsegi

**Definicija 6.17** (Obseg). Kolobar, kjer so neničelni elementi grupa za množenje. Torej, vsak element  $a \neq 0$  mora imeti inverz za množenje.

**Definicija 6.18** (Polje). Komutativni obseg.

**Trditev 6.19.** Polje je cel kolobar.

*Dokaz.* Naj bosta  $a, b \in R$ , kjer je  $R$  polje in recimo, da je  $ab = 0$  in  $a \neq 0$ . Ker je  $a \neq 0$ ,  $\exists a^{-1} \in R$ .

$$\begin{aligned} \cdot a^{-1} / \quad ab = 0 \\ (a^{-1}a)b = a^{-1}0 \\ b = 0 \end{aligned}$$

■

*Opomba.* Obstajajo celi kolobarji, ki niso polja. Primer bi bil  $(\mathbb{Z}, +, *)$ .

**Izrek 6.20.** Če je  $R$  končen cel kolobar, potem je  $R$  polje.

*Dokaz.* Naj bo  $a \in R, a \neq 0$ . Radi bi pričarali njegov inverz.

Poglejmo  $\{a^k; k \in \mathbb{N}\}$ .  $\forall k \in \mathbb{N} : a^k \in R$ . Ker je  $R$  končen, velja

$$\begin{aligned} \exists i, j : i > j \geq 1 : a^i &= a^j \\ a^j a^{i-j} &= a^i = a^j = a^j 1 \\ \xrightarrow{\text{pravilo krajšanja}} a^{i-1} &= 1 \end{aligned}$$

Ločimo dva primera:

1.  $i - j = 1$ :  $a^1 = 1 \implies a = 1$ , tedaj je  $a$  očitno obrnljiv (inverz enote je enota).
2.  $i - j > 1$ :  $a^{i-j} = aa^{i-j-1} = 1$ , kjer  $i - j - 1 > 0$ . Ta enačba pravi, da je  $a^{i-j-1}$  inverz za  $a$ .

■

Poglejmo končen kolobar  $\mathbb{Z}_n$ .

**Izrek 6.21.** Če je  $n \geq 2$ , potem so naslednje trditve ekvivalentne:

- $\mathbb{Z}_n$  je cel kolobar
- $\mathbb{Z}_n$  je polje
- $n$  je praštevilo

*Dokaz.* Prvi dve točki smo dokazali v prejšnjem izreku (6.20). Pokažimo, da je tretja točka ekvivalentna prvi.

Naj bo  $n = pq$  (sestavljeno število),  $2 \leq p, q \leq n$ . Tedaj v  $\mathbb{Z}_n$  velja  $pq = n = 0$ , torej sta  $p$  in  $q$  delitelja nič.

Naj bo  $n$  praštevilo. Vzemimo delitelj nič  $ij = 0$ ,  $i \neq 0$ ,  $j \neq 0$ . Tedaj

$$n|ij \implies n|i \quad \vee \quad n|j$$

torej  $n$  ni praštevilo.

■

## 6.5 Podpolja

**Definicija 6.22** (Podpolje). Podmnožica polja, ki je tudi sama polje.

**Izrek 6.23.** Če je  $F$  polje, potem je  $K \subseteq F$  njegovo podpolje natano tedaj, ko veljajo naslednje trditve:

1.  $1 \in K$
2.  $a, b \in K \implies a - b \in K$
3.  $a, b \in K \quad (b \neq 0) \implies ab^{-1} \in K$

*Dokaz.* Tega ne bomo šli dokazovat, ker je preprosto in zelo podobno izreku 6.10.

■

*Opomba.* V prvi točki ne moremo zahtevati samo  $0 \in K$ , ker  $\{0\}$  zadošča 2. in 3. točki, a ni polje, saj nima  $1 \neq 0$ .

Lahko pa bi ekvivalentno zahtevali, da  $\exists a \in K, a \neq 0$ :

$$\implies \exists a^{-1} \in K \implies aa^{-1} \in K \implies 1 \in K$$

*Primer.*  $F = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$ ,  $F$  je podpolje v  $\mathbb{R}$ .

$$1 + 0\sqrt{2} \in F \implies 1 \in F$$

$$(a + b\sqrt{2}) - (a' + b'\sqrt{2}) = (a - a') + (b - b')\sqrt{2} \in F$$

$$(a + b\sqrt{2}) * (a' + b'\sqrt{2}) = (aa' + 2bb') + (ab' + ba')\sqrt{2} \in F$$

$$(a + b\sqrt{2})^{-1} \in F:$$

$$b = 0 : a + b\sqrt{2} = a \neq 0 \implies \exists a^{-1} \in \mathbb{Q}$$

$$b \neq 0 : (a + b\sqrt{2})(a - b\sqrt{2}) = (a^2 - 2b^2) \in \mathbb{Q}$$

$$(a^2 - 2b^2) \neq 0 \text{ (sicer bi } \sqrt{2} = \frac{a}{b}) \implies \exists c := (a^2 - 2b^2)^{-1} \in \mathbb{Q}$$

$$(a + b\sqrt{2})^{-1} = (ac - bc\sqrt{2})$$

## 6.6 Karakteristika kolobarja

Naj bo  $R$  kolobar in  $a \in R$ . Naj zapis  $n \cdot a$  pomeni  $a + a + \dots + a$ .

**Definicija 6.24** (Karakteristika kolobarja). Najmanjši  $n \in \mathbb{N}$ , da je  $n \cdot a = 0$  za vse  $a \in R$ . Če tak  $n$  ne obstaja, potem je karakteristika  $R$  enaka 0. Oznaka:  $\text{char } R$

*Primer.*  $\text{char } \mathbb{Z}_n = n$

Če imamo kolobar z enoto (kot primer zgoraj), potem je za določitev njegove karakteritike dovolj opazovati enoto.

**Izrek 6.25.** Če je red 1 v grupi  $(R, +)$  enak  $n < \infty$ , potem je  $\text{char } R = n$ . Če ima 1 neskončen red, potem je  $\text{char } R = 0$ .

*Dokaz.* Naj ima 1 red  $n$ . To že pomeni, da je  $\text{char } R \geq n$ . Naj bo sedaj  $a \in R$ . Tedaj je

$$n \cdot a = a + \dots + a = 1 \cdot a + 1 \cdot a + \dots + 1 \cdot a = (1 + 1 + \dots + 1) \cdot a = 0 \cdot a = 0$$

■

**Izrek 6.26.** Če je  $R$  cel kolobar, potem je  $\text{char } R$  bodisi 0, bodisi praštevilo.

*Dokaz.* Naj bo  $\text{char } R > 0$ , torej je  $n \geq 2$ . Recimo, da  $n$  ni praštevilo:  $n = pq$ .

$$0 = n1 = (pq)1 = \underbrace{1 + \dots + 1}_{pq\text{-krat}} = \underbrace{(1 + \dots + 1)}_{p\text{-krat}} \underbrace{(1 + \dots + 1)}_{q\text{-krat}} = (p1)(q1)$$
$$p1 = 0 \quad \vee \quad q1 = 0$$

■

## 6.7 Ideali

**Definicija 6.27** (Ideal). Podkolobar  $I$  kolobarja  $R$  je ideal, če velja:

$$a \in I, x \in R \implies ax, xa \in I$$

Če združimo kriterij za “biti podkolobar” takoj dobimo:

**Izrek 6.28.** Če je  $R$  kolobar in  $I$  njegova podmnožica, je  $I$  ideal natanko tedaj, ko veljajo naslednje trditve:

1.  $0 \in I$
2.  $a, b \in I \implies a - b \in I$
3.  $a \in I, x \in R \implies ax, xa \in I$

*Primer.*  $n\mathbb{Z} = \{0, \pm n, \pm 2n, \dots\}$  je ideal v  $\mathbb{Z}$ .

*Primer.*  $\mathbb{Z}$  je podkolobar v  $\mathbb{Q}$ , ni pa ideal.

**Trditev 6.29.** Če je  $R$  kolobar z enoto in ideal  $I$  vsebuje obrnljiv element, potem je  $I = R$ .

*Dokaz.* Naj bo  $a$  obrnljiv element ideala  $I$ .

$$a \in I, a^{-1} \in R \implies aa^{-1} = 1 \in I$$
$$1 \in I, x \in R \implies 1x \in I \implies x \in I \implies I = R$$

■

**Posledica 6.30.** Če je  $F$  polje, sta edina ideala  $F$  in  $\{0\}$ .

Naj bosta  $I$  in  $J$  ideala v kolobarju  $R$  in definirajmo

$$I + J = \{i + j : i \in I, j \in J\}$$

$$I \cdot J = \{i_1 \cdot j_1 + i_2 \cdot j_2 + \dots + i_n \cdot j_n : i_1, \dots, i_n \in I, j_1, \dots, j_n \in J, n \in \mathbb{N}\}$$

**Izrek 6.31.** Če sta  $I$  in  $J$  ideala v  $R$ , potem je sta tudi  $I + J$  in  $I \cdot J$  ideala v  $R$ .

Naj bo  $I$  ideal v kolobarju  $R$ . Definirajmo:

$$R/I = \{a + I : a \in R\}$$

in vpeljimo operacijo

$$(a + I) + (b + I) = (a + b) + I$$

$$(a + I) \cdot (b + I) = (ab) + I$$

**Definicija 6.32** (Faktorski kolobar (po idealu  $I$ )). Če je  $I$  ideal kolobarja  $R$ , potem  $R/I$  za zgornji dve operaciji imenujemo faktorski kolobar.

*Primer.*  $R = M_2(\mathbb{Z})$ ,  $I = \{A \in M_2(\mathbb{Z}) : \text{elementi v } A \text{ so sodi}\}$ .  $I$  je ideal v  $R$ .

## 7 Kolobarji polinomov

**Definicija 7.1** (Kolobar polinomov). Komutativen kolobar  $R[x] := \{a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x^1 + a_0 x^0 : a_i \in R, n \in \mathbb{N}\}$

*Opomba.*  $x$ -i tu niso neznanke oz. spremenljivke, temveč nam povedo samo mesto za koeficient  $a_i$ . Zanimajo nas v resnici samo zaporedja  $(a_n, \dots, a_0)$ .

**Definicija 7.2** (Ekvivalenčna relacija polinomov).

$$a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x^1 + a_0 x^0 = b_n x^n + b_{n-1} x^{n-1} + \dots + b_1 x^1 + b_0 x^0$$

$$\Updownarrow$$

$$a_n = b_n \quad \wedge \quad a_{n-1} = b_{n-1} \quad \wedge \quad \dots \quad \wedge \quad a_0 = b_0$$

**Definicija 7.3** (Stopnja polinoma). Je največji  $n$ , da je  $a_n \neq 0$ . Označimo  $\deg(f(x)) = n$ .

*Primer* (Konstantni polinom).  $f(x) = a_0$  je bodisi ničeln, bodisi ima stopnjo 0.

*Opomba.* Ničelni polinom nima definirane stopnje.

*Primer.* Poglejmo si polinoma v  $\mathbb{Z}_3[x]$ .

$$f(x) = 2x^3 + x^2 + x + 2$$

$$g(x) = x^2 + 2x + 2$$

$$f(x) + g(x) = 2x^3 + 2x^2 + 3x + 4 = 2x^3 + 2x^2 + 1$$

$$\begin{aligned} f(x) \cdot g(x) &= (2x^3 + x^2 + x + 2) \cdot (x^2 + 2x + 2) = \\ &= 2x^5 + x^4 + x^3 + x^4 + 2x^3 + 2x^2 + x^3 + 2x^2 + 2x + 2x^2 + x + 1 \\ &= 2x^5 + 2x^4 + x^3 + 1 \end{aligned}$$

**Izrek 7.4.** Če je  $R$  komutativen kolobar, potem je tudi  $R[x]$  komutativen kolobar.

*Dokaz.* Rutinsko računanje. Enota za seštevanje je ničelni polinom. Nasprotni element je  $-f(x)$ . Več si lahko preverite sami. ■



**Izrek 7.5.** Če je  $R$  cel kolobar, potem je tudi  $R[x]$  cel kolobar.

*Dokaz.*  $R[x]$  je komutativen. To vemo iz prejšnjega dokaza. Nismo dokazal, ampak vemo.

Naj bo  $1 \in R$  enota za kolobar  $R$ . Enota za  $R[x]$  je tedaj  $f(x) = 1$ .  $R[x]$  je torej komutativen z enoto. Pokažimo še, da nima deliteljev nič.

$$p(x), q(x) \neq 0 \implies p(x)q(x) \neq 0$$

Naj bo  $\deg(p(x)) = n$ ,  $\deg(q(x)) = m$ :

$$p(x) = a_n x^n + \dots$$

$$q(x) = b_m x^m + \dots$$

Ker je  $a_n \neq 0$  in  $b_m \neq 0$  in  $R$  brez deliteljev nič, potem  $a_n b_m \neq 0$ .

$$\implies p(x)q(x) \neq 0$$

■

**Izrek 7.6.** Naj bo  $R$  cel kolobar. Če je  $\deg(p(x)) = n$  in  $\deg(q(x)) = m$ , potem je:

- $\deg(p(x) + q(x)) \leq \max\{n, m\}$  (ali pa je  $p(x) + q(x) = 0$ )
- $\deg(p(x) \cdot q(x)) = n + m$

*Opomba.* Za drugo točko zadnjega izreka potrebujemo predpostavko, da je  $R$  cel kolobar.

*Primer.* Vzemimo  $\mathbb{Z}_8[x]$ .

$$p(x) = 2x^4 + 3x + 1$$

$$q(x) = 4x^4 + 2x^2 + 3$$

$$p(x) \cdot q(x) = \underbrace{2 \cdot 4}_{=0} x^2 + \dots$$

Produkt je stopnje  $6 < 7 = 3 + 4$ , ker  $\mathbb{Z}_8$  ni cel kolobar.

**Izrek 7.7** (O deljenju polinomov). Naj bo  $F$  polje in  $f(x), g(x) \in F[x], g(x) \neq 0$ . Potem obstajata enolična  $q(x)$  in  $r(x)$ , da velja:

$$f(x) = p(x) \cdot q(x) + r(x)$$

kjer je bodisi  $r(x) = 0$ , bodisi  $\deg(r(x)) < \deg(q(x))$ .

*Dokaz.* Najprej dokažimo obstoj  $q(x)$  in  $r(x)$ . To bomo naredili z indukcijo po  $\deg(f(x))$ . Še prej preverimo primer  $f(x) = 0$ :  $q(x) = r(x) = 0 \rightarrow \text{OK}$ .

$\deg(f(x)) = 0$ :  $f(x) = a_0 \in F, a_0 \neq 0$ .

- $\deg(g(x)) > 0$ :  $a_0 = g(x) \cdot q(x) + r(x)$
- $\deg(g(x)) = 0$ : sedaj je  $g(x) = b_0 \in F, b_0 \neq 0$ .  
Ker je  $F$  polje,  $b_0 \neq 0 \implies \exists b_0^{-1}$   
postavimo  $q(x) = b_0^{-1} f(x)$  in  $r(x) = 0$ .
- $\deg(f(x)) = n > 0$

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_0$$

$$g(x) = b_n x^n + b_{n-1} x^{n-1} + \dots + b_0$$

- $n < m$ :

$$f(x) = g(x) \cdot q(x) + r(x)$$

$$r(x) = f(x) \implies \deg(r) \leq n < m = \deg(g)$$

- $n \geq m$ : pogledjmo polinom:

$$k(x) = f(x) - \underbrace{a_n b_m^{-1} g(x) x^{n-m}}_{a_n x^n}$$

kar je polinom stopnje  $< n$ . Po IP obstajata polinoma  $q(x)$  in  $r(x)$ , tako da se

$$k(x) = g(x) \cdot q(x) + r(x)$$

$$f(x) - a_n b_m^{-1} g(x) x^{n-m} = g(x) \cdot q(x) + r(x)$$

$$f(x) = g(x) [q(x) + a_n b_m^{-1} x^{n-m}] + r(x)$$

Kar je to, kar smo želeli. ■

*Dokaz.* (Enoličnost)

$$f(x) = g(x) \cdot q_1(x) + r_1(x)$$

$$f(x) = g(x) \cdot q_2(x) + r_2(x)$$

$$g(x)q_1(x) + r_1(x) = g(x)q_2(x) + r_2(x)$$

$$g(x)[q_1(x) - q_2(x)] = [r_2(x) - r_1(x)]$$

če  $q_1 \neq q_2$ , potem  $q_1 - q_2 \neq 0$ .

$$\implies \deg(q_1(x) - q_2(x)) \geq \deg(g(x)) \quad \deg(r_2(x) - r_1(x)) < \deg(g(x))$$

kar je protislovje. Torej velja  $q_1 = q_2$ , torej tudi  $r_1 = r_2$ . ■

## 7.1 Ničle polinomov in nerazcepni polinomi

**Definicija 7.8** (Nerazcepni polinom).  $f(x) \in F[x]$  je nerazcepen polinom, če iz  $f(x) = g(x) \cdot k(x)$  sledi, da je  $g(x) \in F$  ali  $k(x) \in F$ . Sicer je polinom razcepen.

*Primer.*  $p(x) = x^2 - 2 \in \mathbb{Q}[x]$  je nerazcepen polinom. V  $\mathbb{R}[x]$  je razcepen.

*Primer* (Pozor!). V  $\mathbb{R}[x]$  funkcije identificiramo s samim polinomom. V splošnem to ni res! Na primer v  $\mathbb{Z}_5$  sta polinoma  $f(x) = x^3 + x + 1$  in  $g(x) = x^5 + x^3 + 1$  očitno različna, vendar velja  $\forall x \in \mathbb{Z}_5 : (f(x) = g(x))$ , torej določata isto funkcijo.

**Izrek 7.9.** Obstaja  $q(x) \in F[x]$ , tako da velja:

$$f(x) = (x - a) \cdot q(x) + f(a)$$

*Dokaz.* Izrek o deljenju pravi:  $f(x) = (x - a)q(x) + r(x)$  kjer velja bodisi  $r(x) = 0$ , ali pa  $\deg(r(x)) < \deg(x - a) = 1$ , torej  $r(x) \in F$ .

$$f(a) = (a - a)q(a) + r(a) = r(a) = b \implies r(x) = f(a)$$
■

**Definicija 7.10** (Ničla polinoma). Je tisti  $a \in F$  za katerega velja  $f(a) = 0$ .

**Izrek 7.11.**  $a$  je ničla za  $f(x)$  natanko tedaj, ko  $x - a$  deli  $f(x)$ .

*Dokaz.* Po prejšnjem izreku  $f(x) = (x - a)q(x) + f(a)$ . Ker je  $f(a) = 0$ , lahko zapišemo  $f(x) = (x - a)q(x)$ , torej  $(x - a) | q(x)$ .

Naj  $(x - a) | q(x)$ , torej  $f(x) = (x - a)q(x)$ . Tedaj je  $f(a) = (a - a)q(a) = 0$ . ■

**Posledica 7.12.** Če je polinom stopnje  $> 1$  in ima ničlo, potem je razcepen.

*Primer* (Obrat zadnje posledice ne velja).  $x^4 + 2x^2 + 1 = (x^2 + 1)(x^2 + 1)$  je razcepen v  $\mathbb{R}[x]$ , nima pa ničle.

**Posledica 7.13.** Če je  $\deg(f(x))$  stopnje 2 ali 3, potem je nerazcepen natanko tedaj, ko nima ničle.

*Dokaz.* Edini razcep polinoma stopnje 2 ali 3 bi vseboval vsaj en polinom stopnje 1, od koder dobimo ničlo. ■

**Izrek 7.14.** Če je  $\deg(f(x)) = n$ , potem ima  $f(x)$  kvečjemu  $n$  ničel.

*Dokaz.* (indukcija po  $n$ )

$n = 0$ :  $f(x) = a, a \in F, a \neq 0$ . Ta očitno nima ničel.

Naj bo  $f(x)$  polinom z  $\deg(f(x)) > 0$ . Če nima ničel, ni kaj dokazovati. Če jih ima, naj bo  $a$  poljubna ničla polinoma. Tedaj obstaja razcep

$$f(x) = (x - a)q(x)$$

kjer je  $\deg(q(x)) = \deg(f(x)) - 1$  (po zadnjem izreku). Po IP ima tedaj  $q(x)$  največ  $\deg(f(x)) - 1$  ničel.

Naj bo  $b \neq a$  poljubna druga ničla  $f$ . Tedaj  $f(b) = (b - a)q(b) = 0$ , torej je  $b$  ničla od  $q(x)$ . Zato v  $f$  ne more biti več ničel kot v  $q$ . ■