Algebrske strukture - zapiski predavanj prof. Klavžarja

Yon Ploj

2. semester 2021

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 0.1. 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 0.4 (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 0.2. Inverz je enoličen.

Dokaz. Predpostavimo, da obstajata dva inverza 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)**.**

$$f : A \times A \to A$$

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: $\{0, 1, \ldots, n-1\}$

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

Trditev 1.1. $(\mathbb{Z}_n, +_n)$ je grupa

Trditev 1.2. $(\mathbb{Z}_n, \cdot_n)$ 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.

$$\begin{array}{c|cccccc} \cdot & i & r & s & x & y & z \\ \hline i & i & r & s & x & y & z \\ r & r & s & i & y & z & x \\ s & s & i & r & z & x & y \\ x & x & z & y & i & s & r \\ y & y & x & z & r & i & s \\ z & z & y & x & s & r & i \end{array}$$

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 2.1

Izrek 2.1 (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 2.2 (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 2.1. Red elementa je dobro definiran

Dokaz. Poglejmo zaporedje: $a^1, a^2, \cdots, a^{k+1}$, 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 $(H, \cdot)$ podrgupa $(G, \cdot)$. 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. $F := \{f : \mathbb{R} \to \mathbb{R}\}$. $(F, +)$ je grupa.
$C := \{f : \mathbb{R} \to \mathbb{R}; f \text{ je zvezna}\}$. $(C, +)$ je grupa.
$(C, +) < (F, +)$

Izrek 3.1 (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 3.2. 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 3.3 (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 enoto a.

Trditev 3.1. 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 3.4 (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 3.3. 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 $x \in G$:

$$\begin{aligned} a^{-1} \cdot / \quad ax &= xa \quad / \cdot a^{-1} \\ a^{-1}axa^{-1} &= a^{-1}xaa^{-1} \\ (a^{-1}a)xa^{-1} &= a^{-1}ax(a^{-1}) \\ xa^{-1} &= a^{-1}x \end{aligned}$$

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 3.1 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

$$\langle a \rangle = G$$

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 4.1. 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
$$\langle a \rangle = \{e, a, a^2, \ldots, a^{n-1}\}$$
Nadalje, $a^i = a^j$ velja natanko tedaj, ko $n|(i - j)$.

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.

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

Pokažimo $\langle a \rangle = X$. Očitno je $X \subseteq \langle a \rangle$, saj $a^i \in X \overset{\text{def.}}{\implies} a^i \in \langle a \rangle$. 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 $n|(i-j)$.

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

■

Posledica 4.1. Naj bo G grupa in $a \in G$ reda n.

Dokaz.

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

$$0, k \Rightarrow n|(k-0) \Rightarrow n|k$$

■

Izrek 4.2. 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 4.2 (Permutacija množice A)**.** Je bijekcija $A \to A$.

Definicija 4.3 (Permutacijska grupa)**.** Je množica permutacij, ki za komponiranje preslikav tvorijo grupo.

Definicija 4.4 (Simetrična grupa S_n)**.** Če vzamemo vse permutacije množice $[n]$, dobimo simetrično grupo S_n. Ta grupa ni abelova.

Trditev 4.1. $|S_n| = n!$

Trditev 4.2. Vsako permutacijo lahko enolično (do vrstnega reda faktorjev natančno) zapišemo kot produkt disjunktnih ciklov.

Dokaz. Lmao you thought ■

Trditev 4.3. Vsako permutacijo lahko zapišemo kot produkt transpozicij.

Trditev 4.4. Neko permutcijo lahko zapišemo bodisi samo kot produkt sodo ali liho število transpozicij. Pravimo, da je permutacija liha ali soda.

Definicija 4.5 (Alternirajoča grupa A_n)**.** Je grupa vseh sodih permutacij množice $[n]$.

Dokaz da je to grupa lahko naredite sami.

Izrek 4.3. Če je $n > 1$, potem je $|A_n| = \frac{n!}{2}$

Dokaz. Vzemimo poljubno liho permutacijo Π.

$$\underset{\text{liha}}{\Pi} \quad \underset{\text{injektivno}}{\to} \quad \underset{\text{soda}}{(12) \cdot \Pi}$$

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

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

4.2 Izomorfizmi grup

Definicija 4.6 (Homomorfizem)**.** Naj bosta $(G, \cdot)$ in $(H, *)$ grupe. Preslikava $\alpha G \to H$ je homomorfizem, če

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

Definicija 4.7 (Avtomorfizem)**.** Homomorfizem $G \to G$.

Definicija 4.8 (Izomorfizem)**.** Bijektivni homomorfizem.

Definicija 4.9 (Izomorfni grupi)**.** Grupi, med katerima obstaja izomorfizem.

Proposition: Loi image

Soit $X : \Omega \longrightarrow E$ une variable aléatoire et $f : E \longrightarrow F$. La loi de la variable aléatoire $Y = f \circ X$ est donnée par

$$\forall y \in f(X(\Omega)), \quad \mathbb{P}(Y = y) = \sum_{x \in f^{-1}(\{y\})} \mathbb{P}(X = x).$$

Izrek 4.4 (Cayleyev)**.** Vsaka grupa je izomorfna neki permutacijski grupi.

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

$$T_g(x) = gx$$

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

Trditev 4.5. Če je $\alpha : G \to H$ izomorfizem grup, potem (med drugim) veljajo naslednje lastnosti:

- α preslika enoto G v enoto H.
- če je $a \in G, a \in \mathbb{Z} \implies \alpha(a^n) = (\alpha(a))^n$
- 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. $G = S_3$. $H = \{(1), (2)\}$

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

Primer. $G = (\mathbb{Z}_{10}, +)$. $H = (\{0, 2, 4, 6, 9\}, +)$

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

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 5.1 (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. $aH = H \iff a \in H$:

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

   ($\Leftarrow$) 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.