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

$$a^n = e$$

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. ■