Algebra

Ivan Prokić

Fakultet tehničkih nauka, Novi Sad

Predavanje 8

Na prethodnom času

- Grupoidi
- Monoidi
- Grupe
- Abelove grupe
- Kejlijeve tablice (za konačne skupove)
- Pogrupoidi i podgrupe
- Red grupe i red podgrupe, Lagranžova teorema

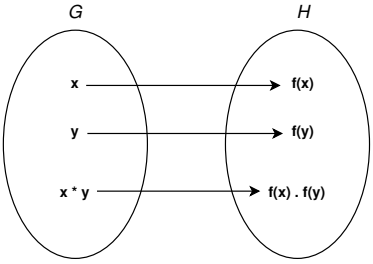
Homomorfizmi i izomorfizmi

Homomorfizmi i izomorfizmi

Definicija (Homomorfizam)

Neka su $(G, \star)$ *i* $(H, \cdot)$ *grupoidi. Za funkciju* $f : G \to H$ *kažemo da je homomorfizam ako za sve* $x, y \in G$ *važi*

$$f(x \star y) = f(x) \cdot f(y)$$



Definicija (Specijalni homomorfizmi)

- *Bijektivni homomorfizam zove se* **izomorfizam**, *i tada se grupoidi zovu* **izomorfni**
- *Izomorfizam grupoida u samog sebe zove se* **automorfizam**
- *Sirjektivni homomorfizam je* **epimorfizam**
- *Injektivni homomorfizam je* **monomorfizam**
- *Homomorfizam grupoida u samog sebe zove se* **endomorfizam**

Primeri

1. Jedan homomorfizam grupe $(\mathbb{R}, +)$ u grupu $(\mathbb{R}^+, \cdot)$ jeste $g(x) = 1$, jer je $g(x + y) = g(x) \cdot g(y) = 1$
2. Jedan izomorfizam grupe $(\mathbb{R}, +)$ u grupu $(\mathbb{R}^+, \cdot)$ jeste $f(x) = e^x$, jer je $e^{x+y} = e^x \cdot e^y$
3. Jedan izomorfizam grupe $(\mathbb{R}^+, \cdot)$ u grupu $(\mathbb{R}, +)$ jeste $f(x) = \ln x$, jer je $\ln(x \cdot y) = \ln x + \ln y$

Osobine izomorfizama 1/2

Teorema (Inverzna funkcija od izomorfizma)

Neka je $f : G \to H$ izomorfizam grupoida $(G, \star)$ u grupoid $(H, \cdot)$. Tada je f^{-1} izomorfizam grupoida $(H, \cdot)$ u grupoid $(G, \star)$.

Dokaz

Ako je $f : G \to H$ bijekcija, tada je i $f^{-1} : H \to G$ bijekcija (rađeno kod funkcija). Ostaje da pokažemo da je f^{-1} homomorfizam, tj. da za sve $x_1, y_1 \in H$ važi $f^{-1}(x_1 \cdot y_1) = f^{-1}(x_1) \star f^{-1}(y_1)$. Pošto je f izomorfizam znamo da za $x_1, y_1 \in H$ postoje $x, y \in G$ takvi da je $f(x) = x_1$ i $f(y) = y_1$ i da, ako je $x \star y = z$ i $f(z) = z_1$, tada je i $x_1 \cdot y_1 = z_1$. Sledi $f^{-1}(x_1 \cdot y_1) = f^{-1}(z_1) = z = x \star y = f^{-1}(x_1) \star f^{-1}(y_1)$.

Osobine izomorfizama 2/2

Teorema

Neka je $f : G \to H$ izomorfizam grupoida $(G, \star)$ u grupoid $(H, \cdot)$. Tada

1. *Ako u G postoji neutralni element e_G, tada i u H postoji neutralni element e_H i važi $f(e_G) = e_H$;*
2. *Ako je $(G, \star)$ asocijativan (komutativan), tada je to i $(H, \cdot)$;*
3. *Ako G ima neutralni element e_G i ako za neko $x \in G$ postoji inverzni element x', tada je $f(x')$ inverzni element od $f(x)$ u H.*

Dokaz

1. *Ako za sve $x \in G$ važi $x \star e_G = e_G \star x = x$, tada je $f(x \star e_G) = f(e_G \star x) = f(x)$, a pošto je f homomorfizam i $f(x) \cdot f(e_G) = f(e_G) \cdot f(x) = f(x)$. Pošto je f bijekcija, za sve $y \in H$ imamo jedno $x \in G$ takvo da je $f(x) = y$, pa imamo da za sve $y \in H$ važi $y \cdot f(e_G) = f(e_G) \cdot y = y$, tj. $f(e_G)$ jeste neutralni element u $(H, \cdot)$, a zbog njegove jedinstvenosti sledi $f(e_G) = e_H$.*

Osobine izomorfizama 2/2

Teorema

Neka je $f : G \to H$ izomorfizam grupoida $(G, \star)$ u grupoid $(H, \cdot)$. Tada

1. *Ako u G postoji neutralni element e_G, tada i u H postoji neutralni element e_H i važi $f(e_G) = e_H$;*
2. *Ako je $(G, \star)$ asocijativan (komutativan), tada je to i $(H, \cdot)$;*
3. *Ako G ima neutralni element e_G i ako za neko $x \in G$ postoji inverzni element x', tada je $f(x')$ inverzni element od $f(x)$ u H.*

Dokaz

2. *Kako je f izomorfizam, važi: $(x \star y) \star z = x \star (y \star z)$ akko $f\big((x \star y) \star z\big) = f\big(x \star (y \star z)\big)$ akko $\big(f(x) \cdot f(y)\big) \cdot f(z) = f(x) \cdot \big(f(y) \cdot f(z)\big)$. Slično se dokazuje komutativnost.*

Osobine izomorfizama 2/2

Teorema

Neka je $f : G \to H$ izomorfizam grupoida $(G, \star)$ u grupoid $(H, \cdot)$. Tada

1. *Ako u G postoji neutralni element e_G, tada i u H postoji neutralni element e_H i važi $f(e_G) = e_H$;*
2. *Ako je $(G, \star)$ asocijativan (komutativan), tada je to i $(H, \cdot)$;*
3. *Ako G ima neutralni element e_G i ako za neko $x \in G$ postoji inverzni element x', tada je $f(x')$ inverzni element od $f(x)$ u H.*

Dokaz

3. *Neka je $x \star x' = x' \star x = e_G$. Tada je $f(x \star x') = f(x' \star x) = f(e_G)$, odnosno $f(x) \cdot f(x') = f(x') \cdot f(x) = e_H$, odakle zaključujemo da je $f(x')$ inverzni element za $f(x)$.*

Primer

Na skupu $\{1, a, b, c\}$ definišemo operaciju $\cdot$ na sledeći način: 1 je neutralni element, $a^2 = b^2 = c^2 = 1$, $ab = ba = c$, $ac = ca = b$ i $bc = cb = a$. Dokazati da je $(\{1, a, b, c\}, \cdot)$ Abelova grupa.

Primer

Na skupu $\{1, a, b, c\}$ definišemo operaciju $\cdot$ na sledeći način: 1 je neutralni element, $a^2 = b^2 = c^2 = 1$, $ab = ba = c$, $ac = ca = b$ i $bc = cb = a$. Dokazati da je $(\{1, a, b, c\}, \cdot)$ Abelova grupa.

Rešenje. Levo dajemo Kejlijevu tablicu za $(\{1, a, b, c\}, \cdot)$, a desno za Klajnovu grupu $(\{i, r, h, v\}, \circ)$

$\cdot$	1	a	b	c
1	1	a	b	c
a	a	1	c	b
b	b	c	1	a
c	c	b	a	1

$\circ$	i	r	h	v
i	i	r	h	v
r	r	i	v	h
h	h	v	i	r
v	v	h	r	i

Možemo proveriti da je $f = \begin{pmatrix} i & r & v & h \\ 1 & a & b & c \end{pmatrix}$ izomorfizam iz $(\{i, r, h, v\}, \circ)$ u grupoid $(\{1, a, b, c\}, \cdot)$, a to znači da obe strukture imaju iste osobine. Pošto je $(\{i, r, h, v\}, \circ)$ Abelova grupa, to je i $(\{1, a, b, c\}, \cdot)$. (Zapravo, to su samo dve interpretacije Klajnove grupe.)

Reprezentacije grupa: Kejlijeva teorema

Teorema (Kejlijeva)

Svaka grupa $(G, \cdot)$ *izomorfna je sa nekom podgrupom grupe permutacija skupa* G*, tj. podgrupom grupe* $Sym\, G = (\{f \mid f : G \xrightarrow[na]{1-1} G\}, \circ)$.

Dokaz

Tražena funkcija je $\Psi : G \to Sym\, G$*, koja svakom elementu iz* G *dodeljuje po jednu permutaciju iz* $Sym\, G$*, a definisana je sa* $\Psi(a) = \sigma_a$*, za sve* $a \in G$*. Funkcije* $\sigma_a : G \to G$ *definisane su sa* $\sigma_a(x) = a \cdot x$*, za sve* $x \in G$. **Prvo bi trebalo pokazati da je** σ_a **bijekcija**.

Ako uzmamo skup svih ovakvih σ_a *funkcija dobijamo*

$H = \{\sigma_a \mid a \in G \wedge \sigma_a : G \xrightarrow[na]{1-1} G \wedge (\forall x \in G)\sigma_a(x) = a \cdot x\}$

Sada treba pokazati da je $(H, \circ)$ **grupa** *i* **da je** $\Psi : G \to H$ **definisana sa** $\Psi(a) = \sigma_a$ **izomorfizam**.

Prvi deo dokaza koji nedostaje

Prvo bi trebalo pokazati da je $\sigma_a : G \to G$ definisana sa $\sigma_a(x) = a \cdot x$, za sve $x \in G$, bijekcija:

1. Iz zatvorenosti operacije $\cdot$ na G sledi da σ_a jeste funkcija iz G u G;
2. Injektivnost: $\sigma_a(x) = \sigma_a(y) \Rightarrow ax = ay \Rightarrow x = y$ jer u grupi G važi zakon kancelacije;
3. Sirjektivnost: treba dokazati da za svako $b \in G$ postoji neko $x \in G$ takvo da je $\sigma_a(x) = b$. Kako je $\sigma_a(x) = ax = b$, dobijamo da je traženo $x = a^{-1}b$. Ovo je definisano jer je G grupa.

Drugi deo dokaza koji nedostaje

$H = \{\sigma_a \mid a \in G \wedge \sigma_a : G \xrightarrow[na]{1-1} G \wedge (\forall x \in G)\sigma_a(x) = a \cdot x\}$

Treba pokazati da je $(H, \circ)$ grupa:

1. Zatvorenost: $(\sigma_a \circ \sigma_b)(x) = \sigma_a(\sigma_b(x)) = a \cdot b \cdot x = \sigma_{a \cdot b}(x)$, kako je za $a, b \in G$ važi $a \cdot b \in G$, sledi $\sigma_{a \cdot b}(x) \in H$;
2. Asocijativnost: $\circ$ je asocijativna operacija (videti kod funkcija);
3. Neutralni element: ako je e neutralni element grupe G, onda je $\sigma_e(x) = e \cdot x = x$ identička funkcija na G, a ona je neutralni element za kompoziciju i važi $\sigma_e \in H$;
4. Inverzni elementi: ako je a^{-1} inverzni element za a u grupi $(G, \cdot)$ tada je $\sigma_a \circ \sigma_{a^{-1}} = \sigma_{a^{-1}} \circ \sigma_a = \sigma_e$, tj. za $\sigma_a \in H$ inverzni je $\sigma_{a^{-1}} \in H$.

Treći deo dokaza koji nedostaje

$\Psi : G \to H$ **definisana sa** $\Psi(a) = \sigma_a$ **jeste izomorfizam iz grupe** $(G, \cdot)$ **u grupu** $(H, \circ)$:

1. Injektivnost: Ako je $\Psi(a) = \Psi(b)$, tj. $\sigma_a = \sigma_b$ imamo $a \cdot x = b \cdot x$ (za sve $x \in G$), pa iz zakona kancelacije u G sledi $a = b$;
2. Sirjektivnost: sledi iz konstrukcije skupa H - za svako $\sigma_a \in H$ postoji $a \in G$ takvo da je $\Psi(a) = \sigma_a$;
3. Homomorfizam: Treba pokazati da su $\Psi(a \cdot b) = \sigma_{a \cdot b}$ i $\Psi(a) \circ \Psi(b) = \sigma_a \circ \sigma_b$ jednaki. Ovo sledi jer za svako $x \in G$ važi

$$\sigma_{a \cdot b}(x) = (a \cdot b) \cdot x = a \cdot (b \cdot x) = \sigma_a(b \cdot x) = \sigma_a(\sigma_b(x)) = (\sigma_a \circ \sigma_b)(x)$$

Kongruencije

Kongruencije

Napomena

Kongruencije smo spominjali kod deljenja celih brojeva: $x \equiv_3 y$ (kongruentno po modulu 3) akko x i y daju isti ostatak pri deljenju sa 3. Ali smo imali i kod primera sa analognim satom, samo je tamo relacija bila $\equiv_{12}$.

Definicija (Kongruencije na proizvoljnim grupoidima)

Neka je $(G, \star)$ grupoid i ρ relacija ekvivalencije na G. Kažemo da je ρ kongruencija ako za sve $x, y, u, v \in G$ važi $(x \,\rho\, u \;\wedge\; y \,\rho\, v) \;\Rightarrow\; (x \star y) \,\rho\, (u \star v)$.

Definicija kaže da se relacija "slaže" sa operacijom, tj. ako

$$(x, u) \in \rho$$
$$(y, v) \in \rho$$
—tada važi—
$$(x \star y, u \star v) \in \rho$$

Važan primer

Neka je relacija $\equiv_3$ data sa za sve $a, b \in \mathbb{Z}$ važi $a \equiv_3 b$ akko $3 \mid a - b$. Tada, $\equiv_3$ jeste kongruencija grupe $(\mathbb{Z}, +)$ i polugrupe $(\mathbb{Z}, \cdot)$.

Rešenje. Kod relacija samo pokazali da je $\equiv_3$ relacija ekvivalencije (RST) na $\mathbb{Z}$. Još treba da pokažemo da se slaže sa operacijama:

- U $(\mathbb{Z}, +)$ imamo $(x \equiv_3 u \ \wedge \ y \equiv_3 v) \ \Rightarrow \ (3 \mid x - u \ \wedge \ 3 \mid y - v)$
  $\Rightarrow \ 3 \mid (x - u) + (y - v) \ \Rightarrow \ 3 \mid (x + y) - (u + v) \ \Rightarrow \ (x + y) \equiv_3 (u + v)$

- U $(\mathbb{Z}, \cdot)$ imamo $(x \equiv_3 u \ \wedge \ y \equiv_3 v) \ \Rightarrow \ (3 \mid x - u \ \wedge \ 3 \mid y - v)$
  $\Rightarrow \ (3 \mid xy - uy \ \wedge \ 3 \mid uy - uv)$ (pomnožimo redom sa y i u)
  $\Rightarrow \ 3 \mid (xy - uy) + (uy - uv) \ \Rightarrow \ 3 \mid xy - uv \ \Rightarrow \ xy \equiv_3 uv$

Napomena

Isto bismo dokazali i da je $\equiv_n$ kongruencija grupe $(\mathbb{Z}, +)$ i polugrupe $(\mathbb{Z}, \cdot)$, za sve $n \geq 2$.

Faktor grupoid

Znamo da relacija ekvivalencije vrši particiju skupa na kom je definisana i šta je faktor skup. Npr. na $\mathbb{Z}$ smo relacijom $\equiv_3$ dobili faktor skup $\mathbb{Z}_3 = \{C_0, C_1, C_2\}$. Kongruencijom na faktor skupu grupoida dobijamo nov grupoid.

Teorema

Neka je ρ kongruencija na grupoidu $(G, \cdot)$ i neka je G/ρ faktor skup. Tada je $(G/\rho, \star)$ grupoid, gde je operacija $\star$ definisana sa $C_x \star C_y = C_{x \cdot y}$ za sve $C_x, C_y \in G/\rho$.

Dokaz

Ako su $x, y \in G$, jasno da je $x \cdot y \in G$, jer je $(G, \cdot)$ grupoid. Pitanje koje se ovde postavlja je sledeće: ako uzmemo $u \in C_x$ i $v \in C_y$, znamo da je $C_x = C_u$ i $C_y = C_v$, tj. $(C_x, C_y) = (C_u, C_v)$, ali da li je i $C_x \star C_y = C_u \star C_v$? Ovo će slediti jer je ρ kongruencija:
$(C_x, C_y) = (C_u, C_v) \Rightarrow (C_x = C_u \wedge C_y = C_v) \Rightarrow (x \,\rho\, u \wedge y \,\rho\, v) \Rightarrow$
$(x \cdot y) \,\rho\, (u \cdot v) \Rightarrow C_{x \cdot y} = C_{u \cdot v}$

Ponovo onaj važan primer

Kod relacija smo rekli da, pošto je svaka klasa ekvivalencije određena bilo kojim svojim elementom, pisaćemo $\mathbb{Z}_3 = \{C_0, C_1, C_2\} = \{0, 1, 2\}$.
Pošto je $\equiv_3$ kongruencija grupe $(\mathbb{Z}, +)$ i polugrupe $(\mathbb{Z}, \cdot)$, dobijamo nove faktor grupoide $(\mathbb{Z}_3, +_3)$ i $(\mathbb{Z}_3, \cdot_3)$, gde su operacije definisane sa $C_x +_3 C_y = C_{x+y}$ i $C_x \cdot_3 C_y = C_{x \cdot y}$. Npr. $2 +_3 2 = 1$ i $2 \cdot_3 2 = 1$.

Ponovo onaj važan primer

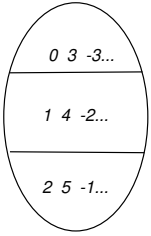
Kod relacija smo rekli da, pošto je svaka klasa ekvivalencije određena bilo kojim svojim elementom, pisaćemo $\mathbb{Z}_3 = \{C_0, C_1, C_2\} = \{0, 1, 2\}$.
Pošto je $\equiv_3$ kongruencija grupe $(\mathbb{Z}, +)$ i polugrupe $(\mathbb{Z}, \cdot)$, dobijamo nove faktor grupoide $(\mathbb{Z}_3, +_3)$ i $(\mathbb{Z}_3, \cdot_3)$, gde su operacije definisane sa $C_x +_3 C_y = C_{x+y}$ i $C_x \cdot_3 C_y = C_{x \cdot y}$. Npr. $2 +_3 2 = 1$ i $2 \cdot_3 2 = 1$.
Sada možemo da crtamo Kejijeve tablice grupoida $(\mathbb{Z}_3, +_3)$ i $(\mathbb{Z}_3, \cdot_3)$

$+_3$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$\cdot_3$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

Proverom osobina dobijamo da je $(\mathbb{Z}_3, +_3)$ Abelova grupa, a $(\mathbb{Z}_3, \cdot_3)$ komutativan monoid. Npr. asocijativnost operacije $+_3$ sledi iz
$(C_x +_3 C_y) +_3 C_z = C_{x+y} +_3 C_z = C_{(x+y)+z} = C_{x+(y+z)} = C_x +_3 C_{y+z} = C_x +_3 (C_y +_3 C_z)$

I dalje u vezi važnog primera



Faktor skup $\mathbb{Z}_3$

Isto kao što smo dobili grupoide $(\mathbb{Z}_3, +_3)$ i $(\mathbb{Z}_3, \cdot_3)$, možemo dobiti grupoide $(\mathbb{Z}_n, +_n)$ i $(\mathbb{Z}_n, \cdot_n)$ (na vežbama ćemo o njihovim osobinama).

Da bi olakšali notaciju, često ćemo umesto $(\mathbb{Z}_n, +_n)$ i $(\mathbb{Z}_n, \cdot_n)$ pisati samo $(\mathbb{Z}_n, +)$ i $(\mathbb{Z}_n, \cdot)$, jer je iz konteksta jasno da su operacije "sabiranje po modulu n" i "množenje po modulu n".

Ciklične grupe

Red elemenata grupe

Setimo se da smo red grupe definisali kao broj elemenata grupe. Takođe smo za mulitplikativnu notaciju definisali $x^k = x \cdot x^{k-1}$.

Definicija (Red elementa)

Neka je $(G, \cdot)$ grupa, e neutralni element i $x \in G$. Red elementa x je najmanji $k \in \mathbb{N}$ takav da je $x^k = e$.

Primer

1. *U Klajnovoj grupi $\{1, a, b, c\}$, smo imali $a^2 = b^2 = c^2 = 1$, pa su a, b, c svi reda 2 (neutralni je u svakoj grupi reda 1);*
2. *U grupi $(\mathbb{Z}_3 \setminus \{0\}, \cdot)$ imamo $2^2 = 1$, pa je element 2 reda 2;*
3. *U grupi $(\mathbb{Z}_3, +)$ reda 3 (primeti aditivnu notaciju) imamo $1 + 1 + 1 = 3 \cdot 1 = 0$, $2 + 2 + 2 = 3 \cdot 2 = 0$, pa su 1 i 2 reda 3.*

Ciklične grupe

Teorema

Neka je $(G, \cdot)$ konačna grupa sa neutralnim elementom e i neka je element $x \in G$ reda k. Tada je $H = \{x^n \mid n \in \mathbb{N}\} = \{e, x, x^2, \ldots, x^{k-1}\}$ nosač podgrupe.

Dokaz

Pošto je G konačan skup i $\{x^n \mid n \in \mathbb{N}\}$ mora biti konačan. Odatle znamo da postoje $n, m \in \mathbb{N}$ takvi da je $x^n = x^m$. Ako je $n > m$, tada je $n = s + m$, pa iz kancelacije dobijamo $x^s = e$. Neka je k najmanji prirodan broj za koje je $x^k = e$. Tada je $H = \{e, x, x^2, \ldots, x^{k-1}\}$. Zatvorenost operacije $\cdot$ u H sledi iz konstrukcije H $(x^l \cdot x^r = x^{l+r})$, a za $x^i \in H$ inverzni je $x^{k-i} \in H$, pa je $(H, \cdot)$ podgrupa.

Posledica

Neka je $(G, \cdot)$ grupa reda m. Tada red svakog elementa $x \in G$ deli red grupe i $x^m = e$.

Definicija (Ciklične grupe)

Grupa $(G, \cdot)$ reda n je ciklična ako postoji element $x \in G$ reda n.

Primeri cikličnih grupa: Sve grupe prostog reda, $(\mathbb{Z}_n, +)$, ...

Šta smo danas radili

- Homomorfizmi i izomorfizmi
- Kejlijeva teorema o reprezentaciji grupa
- Kongruencije
- Grupa $(\mathbb{Z}_n, +)$ i komutativan monoid $(\mathbb{Z}_n, \cdot)$
- Ciklične grupe