5. ALGEBARSKE STRUKTURE

5.1 Binarne operacije

Definicija Binarna operacija na skupu G je bilo koja funkcija $\circ : G \times G \to G$. Vrijednost te funkcije na uređenom paru $(a, b) \in G \times G$ označavamo sa $a \circ b$ ili (ab).

Definicija Skup G zajedno s binarnom operacijom $\circ$ nazivamo grupoid. Točnije, grupoid je uređeni par $(G, \circ)$, gdje je G skup a $\circ$ binarna operacija na G.

Definicija Neka je $(G, \circ)$ grupoid i $A \subseteq G$. Kažemo da je skup A grupoid s obzirom na operaciju $\circ$ naslijeđenu iz G ako za svaki $a, b \in A$ vrijedi $a \circ b \in A$. Još kažemo da je A zatvoren s obzirom na operaciju $\circ$.

Napomena: Nadalje ćemo identificirati:

$$a \circ b \equiv a \cdot b \equiv ab$$

Definicija

- Polugrupa je grupoid $(G, \cdot)$ kod kojeg je operacija $\cdot$ asocijativna, tj. za sve $a, b, c \in G$ vrijedi:

$$a\,(bc) = (ab)\,c;$$

- Monoid je polugrupa $(G, \cdot)$ u kojoj postoji element e takav da za sve $a \in G$ vrijedi:

$$ea = ae = a.$$

Element e nazivamo jedinični ili neutralni element.

Propozicija 1 Svaki monoid ima točno jedan jedinični element.

5.2 Grupe

Definicija

- Grupa je monoid $(G, \cdot)$ kod kojeg je svaki element invertibilan, tj. za svaki $a \in G$ postoji element kojeg označavamo sa a^{-1}, takav da vrijedi:

$$aa^{-1} = a^{-1}a = e;$$

Element a^{-1} nazivamo inverzni element od a.

Alternativna (detaljnija) definicija grupė:

Definicija

- Uređeni par $(G,\cdot)$, gdje je G skup a $\circ$ binarna operacija na G, nazivamo grupom ako su ispunjeni sljedeći uvjeti:

  i) za sve $a,b\in G$ vrijedi $ab\in G$; (grupoidnost)

  ii) za sve $a,b,c\in G$ vrijedi $a\,(bc)=(ab)\,c$; (asocijativnost)

  iii) postoji jedinični element e, tj. postoji element za kojeg vrijedi da je za sve $a\in G$, $ea=ae=a$;

  iv) za svaki $a\in G$ postoji inverzni element a^{-1}, tj. element za kojeg vrijedi da je $aa^{-1}=a^{-1}a=e$;

Definicija

Za grupu $(G,\cdot)$ kažemo da je komutativna ili Abelova grupa ako za sve $a,b\in G$ vrijedi $ab=ba$.

Napomena: Apstraktnu grupu $(G,\cdot)$ (neprecizno) nazivamo "multiplikativna" grupa, a binarnu operaciju $\cdot$ "množenje".

U Abelovoj grupi binarnu operaciju zapisujemo aditivno, tj. ako grupu zadamo sa $(G,+)$ onda je nazivamo "aditivna" grupa i podrazumijevamo da je Abelova.
Neutralni element aditivne grupe nazivamo nula (i označavamo sa 0), a inverzni element od a označavamo sa $-a$ (umjesto a^{-1}) i nazivamo suprotni element.

Propozicija 2 Inverzni element a^{-1} od a u grupi G je jedinstven za svaki $a \in G$ i vrijedi $\left(a^{-1}\right)^{-1} = a$.

Propozicija 3 Neka je $(G,\cdot)$ grupa.

- **(invertiranje produkta)** Za sve $a, b \in G$ vrijedi

$$(ab)^{-1} = b^{-1}a^{-1}.$$

- **(pravilo skraćivanja)** Za sve $a, b, c \in G$ vrijedi

$$\begin{aligned} ac &= bc \implies a = b \\ ca &= cb \implies a = b \end{aligned}$$

Definicija Ako je n prirodan broj onda se u grupi $(G,\cdot)$ definira potencija elementa $a \in G$ sa $a^n := a \cdot ... \cdot a$, $a^{-n} := \left(a^{-1}\right)^n$, $a^0 := e$.

Propozicija 4 U svakoj grupi $(G, \cdot)$ vrijede sljedeća pravila potenciranja za sve $a \in G$ i $m, n \in \mathbb{Z}$.

i) $a^m a^n = a^n a^m = a^{m+n}$;

ii) $(a^m)^n = a^{mn}$;

iii) ako je grupa komutativna, onda za sve $a, b \in G$ vrijedi $(ab)^n = a^n b^n$;

Napomena: Za nekomutativne grupe tvrdnja **iii)** ne vrijedi.

Napomena:

- Potenciji a^n u multiplikativnoj grupi odgovara u aditivnoj $na := a + ... + a$;
- Potenciji a^{-n} u multiplikativnoj grupi odgovara u aditivnoj $-na := -(na)$;
- Potenciji $a^0 = e$ u multiplikativnoj grupi odgovara u aditivnoj $0a := 0$ (oprez!);

Sada Propozicija 3 za aditivnu grupu glasi:

Propozicija 4' U svakoj grupi $(G,+)$ vrijede sljedeća pravila potenciranja za sve $a \in G$ i $m, n \in \mathbb{Z}$.

i) $ma + na = (m+n)\,a;\,;$

ii) $m\,(na) = (mn)\,a;$

iii) $n\,(a+b) = na + nb$. **(**$(G,+)$ $-$komutativna)

Definicija Ako je grupa $(G,\cdot)$ konačna, tj. ako skup G ima konačno elemenata, onda broj elemenata od G nazivamo red grupe i označavamo sa $|G|$.

Definicija Za grupu $(H,\cdot)$ kažemo da je podgrupa grupe $(G,\cdot)$ ako je $H \subseteq G$ i binarna operacija $\cdot$ je naslijeđena iz G. Pišemo $H \leq G$.
Svaka grupa ima dvije trivijalne podgrupe: jediničnu podgrupu $\{e\}$ i podgrupu G.

Propozicija 5 Neka je $(G,\cdot)$ grupa i H neprazan podskup od G.

i) H je podgrupa od G onda i samo onda ako za sve $a, b \in H$ vrijedi $ab^{-1} \in H$;

ii) Presjek dviju ili više podgrupa od G je opet podgrupa.

Napomena: Svojstvo i) iz Propozicije 5 za aditivne grupe glasi:

- Neka je $(G, +)$ grupa. H je podgrupa od G onda i samo onda ako za sve $a, b \in H$ vrijedi $a - b \in H$;

Definicija Neka je grupa $(G, \cdot)$ i $a \in G$. Skup

$$\left\{a^k : k \in \mathbb{Z}\right\}$$

je podgrupa od G. Oznaka

$$\langle a \rangle = \left\{a^k : k \in \mathbb{Z}\right\}.$$

Podgrupa $\langle a \rangle$ je najmanja podgrupa od G koja sadrži a. Podgrupu $\langle a \rangle$ nazivamo podgrupom <u>generiranom</u> elementom a, a element a <u>generator</u>.

Definicija Neka je grupa $(G, \cdot)$ i $a \in G$, $a \neq e$. Ako za neki prirodan broj n vrijedi $a^n = e$, onda najmanji takav n zovemo <u>redom elementa a</u> i označavamo sa $n = |a|$.

Ako je a reda n, onda je inverz elementa a^k jednak a^{n-k}, jer je

$$a^k a^{n-k} = e.$$

Definicija Za grupu $(G, \cdot)$ kažemo da je <u>ciklička grupa</u> ako postoji element $a \in G$ tako da je $G = \langle a \rangle$, tj. svaki $b \in G$ možemo napisati kao

$$b = a^k$$

za neki $k \in \mathbb{Z}$. Tada kažemo da je G <u>ciklička grupa generirana elementom</u> a.

Ako je a konačnog reda n, onda je G reda n :

$$G = \left\{e, a, a^2 ..., a^{n-1}\right\}.$$

Ako je $a^k \neq e$ za sve $k \in \mathbb{N}$, onda je G <u>beskonačna ciklička grupa</u>

$$G = \left\{..., a^{-2}, a^{-1}, e, a, a^2 ...\right\}.$$

Svaka ciklička grupa je komutativna.

Teorem (Lagrange) Neka je $H \leq G$ i grupa G konačna.

i) Red podgrupe $|H|$ je djelitelj od $|G|$;

ii) Za svaki $a \in G$, pripadni red $|a|$ je djelitelj od $|G|$.

Homomorfizmi i izomorfizmi grupa

Definicija Neka su $(G, \cdot)$ i $(H, \cdot)$ dvije grupe. Preslikavanje $f : G \to H$ nazivamo homomorfizam grupa ako za sve $a, b \in G$ vrijedi

$$f(ab) = f(a) \cdot f(b).$$

Propozicija 6 Ako je $f : G \to H$ homomorfizam grupa onda je:

i) Ako je e_1 jedin. u G, onda je $f(e_1) = e_2$ jedinica u H;

ii) $(f(a))^{-1} = f\left(a^{-1}\right)$.

Propozicija 7 Neka je $f : G \to H$ homomorfizam grupa.

i) Skup

$$Ker(f) := \{a \in G : f(a) = e\}$$

je (normalna) podgrupa grupe G i naziva se jezgra homomorfizma f;

ii) Homomorfizam je injektivan onda i samo onda ako je $Ker(f) := \{e\}$.

iii) Slika

$$Im(f) := \{y \in H : (\exists a \in G)\ y = f(a)\}$$

homomorfizma f je podgrupa grupe H.

Definicija Homomorfizam grupa $f : G \to H$ nazivamo <u>izomorfizam grupa</u> ako je f bijekcija. Kažemo da je grupa G <u>izomorfna</u> grupi H i pišemo $G \simeq H$.

Napomena: Da bi pokazali da je $f : G \to H$ izomorfizam grupa treba pokazati:

- f je homomorfizam;
- $Ker\,(f) := \{e\}$;
- f je surjekcija.

Propozicija 8 Neka je $f : G \to H$ homomorfizam grupa.

i) Ako su $f : G \to H$ i $g : H \to K$ homomorfizmi (izomomorfizmi) grupa, onda je i $f \circ g : G \to K$ homomorfizam (izomomorfizam) grupa.

ii) Ako je $f : G \to H$ izomomorfizam grupa, onda je i $f^{-1} : H \to G$ izomomorfizam grupa.

Propozicija 9 Relacija $\simeq$ izomorfnosti među grupama je relacija ekvivalencije.

Napomena: Grupe G i H koje su međusobno izomorfne s motrišta teorije grupa ne razlikujemo, tj. smatramo da su jednake. Poistovjećivanje vrši izomomorfizam f:

- $|G| = |H|$ (f je bijekcija);
- množi se na isti način: množenju ab u G odgovara množenje $f(a) \cdot f(b)$ u H (ako su G i H konačne, tablica množenja je ista);

Definicija Homomorfizam grupa $f : G \to H$ nazivamo epimorfizam grupa ako je f surjekcija.

Injektivni homomorfizam grupa nazivamo monomorfizam.

Monomorfizam $f : G \to H$ nazivamo još i ulaganje G u H, jer je

$$G \simeq Im(f) \leq H$$

Izmomorfizam $f : G \to G$ nazivamo automorfizam grupe G.

5.3 Prsteni i polja

Definicija

Prsten je bilo koji skup $R \neq \emptyset$ zajedno s dvije binarne operacije $+$ i $\cdot$ na R koje nazivamo zbrajanje i množenje, tako da vrijedi:

- $(R, +)$ je Abelova grupa, tj. ako vrijedi:
  - **i)** za sve $a, b, c \in R$ vrijedi $a + (b + c) = (a + b) + c$; (asocijativnost zbrajanja)
  - **ii)** postoji jedinični element 0, tj. postoji element za kojeg vrijedi da je za sve $a \in G$, $0 + a = a + 0 = a$;
  - **iii)** za svaki $a \in G$ postoji suprotni element $-a$, tj. element za kojeg vrijedi da je $a+(-a) = -a+a = 0$;
  - **iv)** za sve $a, b \in R$ vrijedi $a + b = b + a$ (komutativnost zbrajanja).
- $(R, \cdot)$ je polugrupa, tj. množenje na R je asocijativno: za sve $a, b, c \in R$ vrijedi $a \cdot (b \cdot c) = (a \cdot b) \cdot c$;
- za sve $a, b, c \in R$ vrijede zakoni distributivnosti

$$a\cdot(b + c) = (a \cdot b)+(a \cdot c) \quad \text{i} \quad (a + b)\cdot c = (a \cdot c)+(b \cdot c)\,.$$

Kraće, prsten je uređena trojka $(R, +, \cdot)$ tako da vrijede gornja svojstva.

Definicija

- Ako prsten $(R,+,\cdot)$ sadrži jedinični element e s obzirom na množenje onda ga nazivamo prsten s jedinicom.

- Za S kažemo da je potprsten prstena $(R,+,\cdot)$ ako je $S \subseteq R$ i S je prsten s obzirom na operacije naslijeđene iz R.

- Ako je množenje u prstenu $(R,+,\cdot)$ komutativno, tj. za sve $a, b \in R$ vrijedi $a \cdot b = b \cdot a$ onda ga nazivamo komutativan prsten.

Napomena:

- Svaka prsten $(R,+,\cdot)$ ima dva trivijalna podprstena: potprsten $\{0\}$ i potprsten R;

- Dogovorno je $\cdot$ "jače" od $+$ po snazi vezivanja. Npr. imamo

$$ab + ac = (a \cdot b) + (a \cdot c)\,, \quad \text{a ne} \quad a \cdot (b + a) \cdot c.$$

Propozicija 10 U svakom prstenu vrijedi

$$0 \cdot a = a \cdot 0 = 0, \qquad\qquad a\,(-b) = (-a)\,b = -ab.$$

Definicija

- Za element $a \neq 0$ u komutativnom prstenu R kažemo da je djelitelj nule ako postoji $b \neq 0$ takav da je $ab = 0$. Onda je i b djelitelj 0.

- Komutativan prsten s jedinicom e koji nema djelitelja nule nazivamo integralnom domenom.

Propozicija 11 Ako je D integralna domena i $a \neq 0$, onda vrijedi pravilo lijevog i desnog skraćivanja, tj.

$$\begin{aligned} ab &= ac \implies b = c \\ ba &= ca \implies b = c \end{aligned}$$

Definicija

Komutativan prsten F u kojem je skup $F^* = F \setminus \{0\}$ grupa s obzirom na množenje nazivamo polje.

Dakle, polje je integralana domena u kojoj svaki element $\neq 0$ ima multiplikativni inverz.

Napomena:

- Polje $(F, +, \cdot)$ je generalizacija polja realnih brojeva:
  - Definiramo razlomak

$$\frac{a}{b} := ab^{-1}, \;\; a, b \in F \text{ i } b \neq 0;$$

Zbog komutativnosti množenja imamo

$$\frac{a}{b} \cdot \frac{c}{d} = \left(ab^{-1}\right)\left(cd^{-1}\right) \overset{kom}{=} acb^{-1}d^{-1} \overset{kom}{=} ac\,(bd)^{-1} = \frac{ac}{bd};$$

Slično:

  - pravilo skraćivanja

$$\frac{ac}{bc} = \frac{a}{b} \quad b, c \neq 0;$$

  - pravilo svođenja na zajednički nazivnik

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + cb}{bd} \quad b, d \neq 0;$$

Vrijedi:

polja $\subset$ **int.dom**. $\subset$ **kom.prstenovi** $\subset$ **prstenovi**

Propozicija 12 Svaka konačna integralna domena D je polje.

Definicija Za K kažemo da je potpolje pola F ako je $K \subseteq F$ i K je polje s obzirom na operacije naslijeđene iz F. U tom slučaju kažemo da je F proširenje polja K.

Propozicija 13 Neka je F polje i K neprazan podskup od F. K je potpolje od F onda i samo onda ako za sve $a, b \in H$ vrijedi:

i) $e \in K$

ii) za sve $a, b \in K$ vrijedi $a - b \in K$;

ii) za sve $a, b \in K$ vrijedi $ab^{-1} \in K^*$.

Homomorfizmi i izomorfizmi prstenova

Definicija Neka su R i S dva prstena. Preslikavanje $f : R \rightarrow S$ nazivamo homomorfizam prstenova ako za sve $a, b \in R$ vrijedi

$$f(a+b) = f(a) + f(b) \quad \text{i} \quad f(ab) = f(a) \cdot f(b).$$

Napomena:

- Budući je $f : R \rightarrow S$ i homomorfizam Abelovih grupa $(R, +)$ i $(S, +)$ onda je

$$f(0) = 0 \quad \text{i} \quad f(-a) = -f(a).$$

Definicija

- Ako je $f : R \to S$ bijekcija onda f nazivamo izomomorfizam prstenova i pišemo $R \simeq S$;
- Ako je $f : R \to S$ surjekcija onda f nazivamo epimomorfizam prstenova;
- Ako je $f : R \to S$ injekcija onda f nazivamo monomorfizam prstenova;
- Izmomorfizam $f : R \to R$ nazivamo automorfizam prstena R.

Propozicija 14 Relacija $\simeq$ izomorfnosti među prstenovima je relacija ekvivalencije.

Propozicija 15 Neka su prstenovi R i S izomorfni, tj. neka postoji izomorfizam prstenova $f : R \to S$. Tada vrijedi:

i) Ako je e_1 jedinica u R, onda je $f(e_1) = e_2$ jedinica u S;

ii) Ako je R komutativan prsten, onda je i S komutativan prsten;

ii) Ako je R polje, onda je i S polje.