Grupe

May 15, 2008

Osnovne lastnosti

Algebrska struktura $(A, \cdot)$ je **grupa**, če:

1. velja notranjost, tj. $\forall x, y \in A : x \cdot y \in A$;
2. velja asociativnost, tj. $\forall x, y, z \in A : x \cdot (y \cdot z) = (x \cdot y) \cdot z$;
3. obstaja enota $e \in A$, tj. $\forall x \in A : x \cdot e = e \cdot x = x$;
4. je vsak element iz $x \in A$ obrnljiv, tj. $\exists x^{-1} \in A : x \cdot x^{-1} = x^{-1} \cdot x = e$.

Zgled: Naj bo U_n množica rešitev enačbe $x^n = 1$ v $\mathbb{C}$. Recimo

- $U_1 = \{1\}$
- $U_2 = \{-1, 1\}$
- $U_3 = \{1, -\frac{1}{2} + \frac{\sqrt{3}}{2}i, -\frac{1}{2} + \frac{\sqrt{3}}{2}i\}$
- $U_4 = \{1, i, -1, -i\}$.

Algebrska struktura $(U_n, \cdot)$ je grupa.

Trditev 1 *V grupi* $(G, \cdot)$ *veljata pravili krajšanja:*

$$a \cdot x = b \cdot x \qquad \Rightarrow \qquad a = b$$

in

$$x \cdot a = x \cdot b \qquad \Rightarrow \qquad a = b.$$

Dokaz. Dokažimo le prvo pravilo, dokaz drugega je podoben.

$$a \cdot x = b \cdot x \qquad / x^{-1}$$

$$a \cdot x \cdot x^{-1} = b \cdot x \cdot x^{-1}$$

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

$$a = b$$

□

Trditev 2 *V grupi* $(G, \cdot)$ *sta enačbi* $a \cdot x = b$ *in* $y \cdot a = b$ *enolično rešljivi za vsak par* $a, b \in G$.

Dokaz. Rešitev prve enačbe je $x = a^{-1} \cdot b$. Preverimo,

$$a \cdot x = a \cdot (a^{-1} \cdot b) = (a \cdot a^{-1}) \cdot b = e \cdot b = b$$

Pokažimo, da je to edina rešitev. Če imamo dve rešitvi x_1, x_2, potem

$$a \cdot x_1 = b \quad \text{in} \quad a \cdot x_2 = b$$

iz tega sledi

$$a \cdot x_1 = a \cdot x_2$$

in po pravilu krajšanja dobimo

$$x_1 = x_2$$

Druge enačbe se lotimo podobno. □

Naloga 1 *V grupi* $(\mathbb{Z}_{12}^*, \cdot_{12})$ *reši* $7 \cdot_{12} x = 11$.

Naloga 2 *V grupi* $(\mathbb{Z}_{97}^*, \cdot_{97})$ *poišči* 26^{-1}.

Posledica 3 *Naj bo a element iz grupe $(G, \cdot)$. Funkcijo f_a definiramo takole:*

$$\forall x \in G : f_a(x) = a \cdot x$$

Potem je f_a bijektivna funkcija.

Dokaz. Injektivnost sledi po trditvi 1, surjektivnost pa po trditvi 2.

Naj bo a element iz grupe $(G, \cdot)$ ter H (končna) podmnožica v G. Definiramo

$$\begin{aligned} \mathbf{aH} &= \{a \cdot h : h \in H\}, \\ \mathbf{Ha} &= \{h \cdot a : h \in H\}, \\ \mathbf{a^{-1}Ha} &= \{a^{-1} \cdot h \cdot a : h \in H\}. \end{aligned}$$

Posledica 4 *Množice definirane zgoraj imajo enako moč, tj.*

$$|a\,H| = |H| = |H\,a| = |a^{-1}\,H\,a|.$$

Dokaz.

Naloga 3 *Sestavi Cayleyjeve tabele za grupe* $(\mathbb{Z}_5, +_5)$ *ter* $(\mathbb{Z}_9^*, \cdot_9)$. *Kakšne lastnosti imajo Cayleyjeve tabele grup?*

Odgovor:

Podgrupe

$H \subseteq G$ je **podgrupa** grupe $(G, \cdot)$, če velja:

1. $x, y \in H \Rightarrow x \cdot y \in H$,
2. $e \in H$,
3. $x \in H \Rightarrow x^{-1} \in H$.

V tem primeru pišemo $(H, \cdot) \leq (G, \cdot)$. Notacijo poenostavimo ter pišemo samo $H \leq G$.

Zgledi: $\{0, 3\}$ ter $\{0, 2, 4\}$ sta podgrupi v $\mathbb{Z}_6$. Množici $\{1, 3\}$ ter $\{0, 3, 5\}$ pa nista podgrupi v $\mathbb{Z}_6$.

Naloga 4 *Naj bo $2\mathbb{Z}$ množica vseh sodih celih števil. Potem je $(2\mathbb{Z}, +) \leq (\mathbb{Z}, +)$.*

Odgovor:

Naloga 5 *Naj bosta H_1 in H_2 podgrupi v G. Potem je*

$$H_1 \cap H_2 \leq G.$$

Odgovor:

Izrek 5 *Naj bo H podmnožica v grupi G. H je podgrupa natanko takrat, ko je*

$$H \neq \emptyset \quad in \quad \forall x, y \in H : x^{-1} \cdot y \in H.$$

Dokaz. ($\Rightarrow$). Ker $H \leq G$ sledi $e \in H$ in od tod $H \neq \emptyset$.

Recimo $x, y \in H$, potem tudi $x^{-1}, y \in H$ in od tod $x^{-1} \cdot y \in H$.

($\Leftarrow$). Ker je $H \neq \emptyset$, lahko izberemo element $x \in H$. Dokažimo vse tri pogoje 1.–3. definicije o podgrupah:

Če postavimo $y := x$, potem

$$x^{-1} \cdot y \in H \Rightarrow x^{-1} \cdot x \in H \Rightarrow e \in H,$$

kar je pogoj 2.

Če postavimo $y := \alpha$ ter $x := e$, potem

$$x^{-1} \cdot y \in H \Rightarrow e \cdot \alpha^{-1} \in H \Rightarrow \alpha^{-1} \in H,$$

kar je pogoj 3.

Pogoj 1. pa izpeljemo takole:

$$x, y \in H \Rightarrow x^{-1}, y \in H \Rightarrow (x^{-1})^{-1} \cdot y \in H \Rightarrow x \cdot y \in H.$$

□

Zgledi:

Trditev 6 *Naj bo $H \leq G$ in $a \in G$. Potem je $a^{-1} H a \leq G$.*

Dokaz. Uporabimo kriterij iz izreka 5. Ker $H \neq \emptyset$, sledi da je tudi $a^{-1} H a \neq \emptyset$. Naj bo $x, y \in a^{-1} H a$.

Potem za neka $h_1, h_2 \in H$ velja

$$x = a^{-1} h_1 a \quad \text{ter} \quad y = a^{-1} h_2 a.$$

Od tod pa sledi

$$x^{-1}y = (a^{-1} h_1 a)^{-1}(a^{-1} h_2 a) = a^{-1} h_1^{-1} a a^{-1} h_2 a = a^{-1} (h_1^{-1}h_2) a.$$

Ker je H podgrupa v G, velja $h_1^{-1}h_2 \in H$. In od tod sledi

$$a^{-1} (h_1^{-1}h_2)a \ \in \ a^{-1} H a$$

t.j.

$$x^{-1}y \ \in \ a^{-1} H a.$$

□

Kriterij iz izreka 5 za končne grupe poenostavimo takole:

Izrek 7 *Naj bo G končna grupa. Potem je $H \leq G$ natanko takrat, ko je H trdna podmnožica.*

Dokaz.

Naloga 6 *Poišči vse podgrupe v $(\mathbb{Z}_6, +_6)$.*

Odgovor:

Lagrangev izrek

Naj bo $H \leq G$ in $x \in G$.

Levi odsek elementa x **po podgrupi** H je

$$x\,H = \{x \cdot h : h \in H\}.$$

Trditev 8 *Naj bo* $H \leq G$ *in* R *relacija v* G*, definirana s predpisom:*

$$x\,R\,y \Leftrightarrow x\,H = y\,H.$$

Potem velja:

1. R *ekvivalenčna relacija*
2. $x\,R\,y \Leftrightarrow x^{-1}y \in H$
3. $R[x] = x\,H$.

Dokaz. Prva trditev je očitna. Pokažimo drugo trditev:

$$\begin{array}{rcl} x\,R\,y & \Rightarrow & x\,H = y\,H \quad \Rightarrow \quad x \in y\,H \\ & \Rightarrow & \exists h \in H : x = y \cdot h \\ & \Rightarrow & x^{-1} \cdot y = h^{-1} \in H. \end{array}$$

še v drugo smer

$$\begin{array}{rcl} x^{-1} \cdot y \in H & \Rightarrow & \exists h \in H : x^{-1} \cdot y = h \\ & \Rightarrow & y = x \cdot h \wedge x = y \cdot h^{-1} \\ & \Rightarrow & y\,H \subseteq x\,H \wedge x\,H \subseteq y\,H. \end{array}$$

Za konec pokažimo še tretjo trditev:

$$y \in R[x] \quad \Leftrightarrow \quad x\,R\,y \quad \Leftrightarrow \quad x^{-1} \cdot y \in H \quad \Leftrightarrow \quad y \in xH$$

□

Če je število levih odsekov po podgrupi H končno, ga imenujemo **indeks** podgrupe H v grupi G in ga označimo z $[G : H]$.

Izrek 9 (Lagrangev izrek) *Naj bo G končna grupa in $H \leq G$. Potem je moč grupe G deljiva z močjo podgrupe H in velja formula*

$$|G| = [G : H] \cdot |H|.$$

Dokaz. Naj bo $a \in G$ poljuben element. Pokažimo, da je preslikava $f : H \to a\,H$ bijekcija:

- injektivost: $f(x) = f(y) \quad \Rightarrow \quad a \cdot x = a \cdot y \quad \Rightarrow \quad x = y$

- surjektivnost: $y \in a\,H \quad \Rightarrow \quad \exists x \in H : y = a \cdot x$
  $\Rightarrow \quad \exists x \in H : y = f(x)$

Ker je f bijekcija, sledi

$$|a\,H| = |H|$$

Vsi levi odseki po H imajo enako moč kot podgrupa H. Torej, vsi odseki po H imajo enako moč.

Ker levi odseki sestavljajo razbitje grupe G, dobimo:

$$\begin{aligned} |G| &= \text{vsota moči levih odsekov po } H \\ &= (\text{število levih odsekov}) \cdot (\text{moč odseka}) \\ &= [G : H] \cdot |H| \end{aligned}$$

□

Red elementa in končne grupe

Naj bo G končna grupa in $a \in G$.

Red elementa a je definiran kot najmanjše naravno število n tako, da velja $a^n = e$, tj.

$$\mathrm{red}(a) = \min\{r \in \mathbb{N} : a^r = e\}.$$

Če tak n ne obstaja, pravimo, da ima a red ∞, tj. $\mathrm{red}(a) = \infty$.

Naloga 7 *Poišči red elementov grupe* $(\mathbb{Z}_{12}^*, \cdot_{12})$.

Odgovor:

Problem 1 *Naj bo a element v G reda r. Potem je*

$$H = \{e, a, a^2, \ldots, a^{r-1}\}$$

podgrupa v G.

Dokaz.

Trditev 10 *Naj bo G končna grupa reda n in $a \in G$. Potem velja*

1. $a^{\mathrm{red}(a)} = e$
2. $\mathrm{red}(a) = 1 \Leftrightarrow a = e$
3. $\mathrm{red}(a) \mid n$
4. $a^n = e$.

Dokaz. Pokažimo vsako trditev posebej:

1. Sledi iz definicije.
2. V eno smer: $\mathrm{red}(a) = 1 \quad \Rightarrow \quad a^1 = e \quad \Rightarrow \quad a = e$
   ter v drugo smer: $e^1 = e \quad \Rightarrow \quad \mathrm{red}(e) = 1$.
3. Iz prejšnjega problema sledi, da je $\{e, a, a^2, \ldots, a^{\mathrm{red}(a)-1}\}$ podgrupa v G reda $\mathrm{red}(a)$. Zato po Langrangevem izreku sledi, da $\mathrm{red}(a) \mid n$.
4. Iz prejšnje trditve sledi, da je $n = \mathrm{red}(a)\, k$, za neko naravno število k. Torej,
$$a^n = a^{\mathrm{red}(a)k} = (a^{\mathrm{red}(a)})^k = e^k = e.$$

□

Problem 2 *Poišči vse grupe reda* 4.

Rešitev:

Izrek 11 (Euler) *Če* $\gcd(a, m) = 1$, *potem je* $a^{\varphi(m)} \equiv 1 \pmod{m}$.

Dokaz. Grupa $(\mathbb{Z}_m^*, \cdot_m)$ ima $\varphi(m)$ elementov. Ker je $\gcd(a, m) = 1$, lahko vzamemo, da je $a \in \mathbb{Z}_m^*$. Po zgornji trditvi velja $a^{\varphi(m)} \equiv 1 \pmod{m}$ v $\mathbb{Z}_m^*$. Za $a \in \mathbb{Z}$ pa to pomeni $a^{\varphi(m)} \equiv 1 \pmod{m}$. □

Posledica 12 (Mali Fermatov izrek) *Naj bo* $a \in \mathbb{Z}$ *in* p *praštevilo, ki ne deli* a. *Potem je*

$$a^{p-1} \equiv 1 \pmod{p}.$$

Dokaz. Ker $p \nmid a$ sledi, da $\gcd(p, a) = 1$. In ker je p praštevilo vemo, da $\varphi(p) = p - 1$. Zdaj iz prejšnjega izreka sledi dokaz. □

Izrek 13 (Cauchy) *Naj bo* G *končna grupa moči* n *ter naj bo* p *praštevilo, ki deli* n. *Potem* G *vsebuje element reda* p.

Generatorji ter ciklične grupe

Grupa G je **ciklična**, če obstaja $a \in G$ tako, da je vsak element grupe G enak neki potenci elementa a.

Element a imenujemo **generator** grupe G.

Naloga 8 *Ali je* $(\mathbb{Z}_n, +_n)$ *ciklična? Pošči vse generatorje za grupo* $(\mathbb{Z}_{12}, +_{12})$.

Trditev 14 *Naj bo* G *končna grupa reda* n. *Potem velja:*

$$G \text{ je ciklična grupa} \iff G \text{ vsebuje element reda } n.$$

Posledica 15 *Če je red grupe* G *praštevilo, potem je* G *ciklična grupa.*

Trditev 16 *Naj bo $\mathcal{D}$ neka družina podgrup grupe G. Potem je presek teh podgrup podgrupa v G, tj.*

$$\bigcap_{F \in \mathcal{D}} F \leq G.$$

Dokaz. Dokaz poteka podobno kot pri nalogi 5.

□

Naj bo $S \subseteq G$ neka podmnožica v grupi G. **Najmanjša podgrupa** v G, ki vsebuje S, je

$$\langle S \rangle = \bigcap \{H \leq G : S \subseteq H\}.$$

Množica S **generira** grupo G, če velja $\langle S \rangle = G$.

Opomba: Če je G ciklična grupa, potem obstaja S moči 1, ki generira G.

Če $S = \{a\}$ potem namesto $\langle \{a\} \rangle$ pišemo $\langle a \rangle$.

Naloga 9 *Za grupo* $(\mathbb{Z}_{12}^*, \cdot_{12})$ *izračunaj* $\langle 5 \rangle$, $\langle \{5, 7\} \rangle$, $\langle \{7, 11\} \rangle$, $\langle \{11, 5\} \rangle$.

Naloga 10 *Za grupo* $(\mathbb{Z}_{12}, +_{12})$ *izračunaj* $\langle 3 \rangle$, $\langle 4 \rangle$, $\langle 6 \rangle$, $\langle 5 \rangle$, $\langle 7 \rangle$, $\langle \{3, 4\} \rangle$.

Cayleyjevi digrafi

Naj bo H grupa ter $S \subseteq H$. **Cayleyjev digraf** $G = \mathrm{Cay}(H; S)$ je definiran takole:

- $V(G) = H$
- $E(G) = \{uv \mid u^{-1}v \in S\}$.

Zgledi: Cayleyjevi digrafi $(\mathbb{Z}_6, \{1\})$, $(\mathbb{Z}_6, \{2, 3\})$

Problem 3 *Nariši hiperkocko Q_3 kot Cayleyjev graf.*

Podgrupe edinke

Naj bo G grupa in $H \leq G$.

H je **edinka**, če velja: $\forall a \in G : a^{-1} H a \subseteq H$.

Pišemo $H \lhd G$.

$\{e\}$ in G sta **trivialni** edinki v G.

Trditev 17 *Naj bo G grupa in H podgrupa v G. Naslednje trditve so enakovredne:*

(i) $H \lhd G$

(ii) $\forall a \in G : a^{-1} H a = H$

(iii) $\forall a \in G : a H = H a$.

Dokaz.

Trditev 18 *V Abelovi grupi je vsaka podgrupa edinka.*

Dokaz.

Izrek 19 *Naj bo R kongruenčna relacija v grupi G. Tedaj je $R[e] \lhd G$.*

Izrek 20 *Naj bo $H \lhd G$. Potem je relacija R definirana kot*

$$a\,R\,b \quad \equiv \quad a\,H = b\,H$$

kongruenčna relacija.

Izrek 21 *Naj bo H podgrupa v G tako, da je $[G : H] = 2$. Potem $H \lhd G$.*

Dokaz. Naj bo $a \in G \setminus H$. Potem sta H in aH leva odseka in zato velja

$$aH \cup H = G \quad \text{ter} \quad aH \cap H = \emptyset.$$

Podobno sta H in Ha desna odseka in zato velja

$$Ha \cup H = G \quad \text{ter} \quad Ha \cap H = \emptyset.$$

Tako sklepamo, da je $aH = Ha$ in od tod, da je H edinka.

Homomorfizmi

Naj bosta $(G, \circ)$ in $(H, *)$ grupi. Preslikava $f : G \to H$ je **homomorfizem**, če velja

$$\forall a, b \in G : f(a \circ b) = f(a) * f(b)$$

Bijektivni homomorfizem je **izomorfizem**. Če je $G = H$, potem izomorfizem imenujemo **avtomorfizem**.

Zgled: Preslikava $h(x) = e^x$ je izomorfizem iz $(\mathbb{R}, +)$ v $(\mathbb{R}^+, \cdot)$.

Trditev 22 *Naj bosta G_1, G_2 ciklični grupi. Velja:*

$$|G_1| = |G_2| \quad \Rightarrow \quad G_1 \cong G_2.$$

Trditev 23 *Veljajo naslednje lastnosti:*

(1) $f(e_G) = e_H$

(2) $f(x^{-1}) = f(x)^{-1}$.

Dokaz. Pokažimo prvo trditev. Velja:

$$f(e_G) = f(e_G \circ e_G) = f(e_G) * f(e_G).$$

Pokrajšamo z $f(e_G)$ ter tako dobimo $f(e_G) = e_H$.

Druga trditev pa takoj sledi iz:

$$f(x) * f(x^{-1}) = f(x \circ x^{-1}) = f(e_G) = e_H$$

ter

$$f(x^{-1}) * f(x) = f(x^{-1} \circ x) = f(e_G) = e_H.$$

□

Naloga 11 *Ali sta grupi* $(\mathbb{Z}_4, +_4)$ *ter* $(\mathbb{Z}_{12}^*, \cdot_{12})$ *izomorfni?*

Jedro in slika homomorfizma

Naj bo $f : (G, \circ) \to (H, *)$ homomorfizem. **Jedro** homomorfizma f je

$$\ker(f) = \{x \in G : f(x) = e_H\},$$

slika homomorfizma f pa je

$$\mathrm{im}(f) = \{f(x) : x \in G\}.$$

Velja: $\ker(f) \subseteq G$ ter $\mathrm{im}(f) \subseteq H$

Naloga 12 *Pokaži, da je* $h(x) = 3x \pmod{12}$ *homomorfizem iz* $(\mathbb{Z}_{12}, +_{12})$ *v* $(\mathbb{Z}_{12}, +_{12})$. *Izračunaj* $\ker(h)$ *ter* $\mathrm{im}(h)$.

Rešitev:

Trditev 24 *Naj bo $f : G \to H$ homomorfizem. Potem, velja*

- *f je injektiven* $\Leftrightarrow \ker(f) = \{e_G\}$;
- *f je surjektiven* $\Leftrightarrow \mathrm{im}(f) = H$.

Dokaz. Druga trditev je očitna, zato pokažimo le prvo.

($\Rightarrow$). Naj bo f injektivna funkcija. Vemo, da $f(e_G) = e_H$. Za $x \in \ker(f)$ velja $f(x) = e_G$. Zdaj pa iz injektivnosti sledi, da je $x = e_G$. In od tod $\ker(f) = \{e_G\}$.

($\Leftarrow$). Naj bo $\ker(f) = \{e_G\}$. Recimo $f(x) = f(y)$. Potem pa izpeljemo takole

$$\begin{aligned} f(x) &= f(y) \qquad / * f(y)^{-1} \\ f(x) * f(y)^{-1} &= f(y \circ y^{-1}) \\ f(x \circ y^{-1}) &= f(e_G) \\ f(x \circ y^{-1}) &= e_H. \end{aligned}$$

Ker je $\ker(f) = \{e_G\}$, dobimo $x \circ y^{-1} = e_G$ in od tod $x = y$. $\square$

Naloga 13 *Poišči injektiven homomorfizem iz $(\mathbb{Z}_6, +_6)$ v $(\mathbb{Z}_{12}, +_{12})$. Potem pa poišči surjektiven homomorfizem iz $(\mathbb{Z}_{12}, +_{12})$ v $(\mathbb{Z}_6, +_6)$.*

Rešitev:

Trditev 25 *Naj bo $f : G \to H$ homomorfizem. Potem, velja*

- $\ker(f) \lhd G$
- $\mathrm{im}(f) \leq H$.

Dokaz. Z uporabo izreka 5 pokažimo, da je $\ker(f)$ podgrupa. Ker $f(e_G) = e_H$, sledi $e_G \in \ker(f)$ in zato $\ker(f) \neq \emptyset$.

Za poljubni $x, y \in \ker(f)$ velja:

$$f(x^{-1} \circ y) = f(x^{-1}) * f(y) = f(x)^{-1} * f(y) = e_H * e_H = e_H.$$

Torej $x^{-1} \circ y \in \ker(f)$ in od tod sledi, da je $\ker(f)$ podgrupa.

Pokažimo, da je $\ker(f)$ edinka. Naj bosta $h \in \ker(f)$ ter $a \in G$ poljubna. Dovolj bo, da pokažemo, da je $a^{-1} \circ h \circ a \in \ker(f)$. Velja

$$f(a^{-1} \circ h \circ a) = f(a^{-1}) * f(h) * f(a) = f(a)^{-1} * e_G * f(a) = e_G.$$

Iz tega sledi, da je $a^{-1} \circ h \circ a$ v jedru preslikave f. Od tod pa sklepamo, da je $a^{-1} \ker(f)\, a \subseteq \ker(f)$, kar implicira, da je $\ker(f)$ edinka.

Pokažimo drugo trditev. Ker $f(e_G) = e_H$, sledi $\mathrm{im}(f) \neq \emptyset$. Za poljubna $x, y \in \mathrm{im}(f)$ hočemo pokazati, da $x^{-1} * y \in \mathrm{im}(f)$. Potem obstajata a, b za katera velja $f(a) = x$ in $f(b) = y$. Ker

$$f(a^{-1} \circ b) = f(a)^{-1} * f(b) = x^{-1}y,$$

sledi, da $x^{-1} * y \in \mathrm{im}(f)$.

Izrek 26 (Osnovni izrek o izomorfizmu) *Naj bo* $f : G \to H$ *surjektivni homomorfizem grupe* G *v grupo* H *z jedrom* $J = \ker(f)$. *Potem je* $G/J \cong H$.

Zgled: Preslikava $f(x) = x \pmod{n}$ je homomorfizem iz $(\mathbb{Z}, +)$ v $(\mathbb{Z}_n, +_n)$. Jedro je $\ker(f) = \{n \cdot a : a \in \mathbb{Z}\} = n\,\mathbb{Z}_n$. Velja:

$$\mathbb{Z}/n\,\mathbb{Z} \cong \mathbb{Z}_n.$$

Kartezični produkt grup

Trditev 27 *Naj bosta* $(G, *)$ *in* $(H, \cdot)$ *grupi. Definirajmo algebrsko strukturo* $(G \times H, \circ)$ *takole:*

$$(g_1, h_1) \circ (g_2, h_2) = (g_1 * g_2, h_1 \cdot h_2).$$

Pokaži, da je $(G \times H, \circ)$ *grupa.*

Dokaz.

Grupo iz zgornje trditve ponavadi označimo z $(G, *) \times (H, \cdot)$

Naloga 14 *Sestavi Cayleyevo tabelo grupe* $(\mathbb{Z}_2, +_2) \times (\mathbb{Z}_3, +_3)$. *Ali je ta grupa izomorfna grupi* $(\mathbb{Z}_6, +_6)$*?*

Odgovor:

Naloga 15 *Ali je* $(\mathbb{Z}_2, +_2) \times (\mathbb{Z}_4, +_4)$ *izomorfna grupi* $(\mathbb{Z}_8, +_8)$*?*

Odgovor:

Trditev 28 $\mathbb{Z}_m \times \mathbb{Z}_n \cong \mathbb{Z}_{mn} \quad \Leftrightarrow \quad \gcd(m,n) = 1.$

Dokaz.

Naloga 16 *Ali je* $\mathbb{Z}_2^2$ *izomorfna grupi* $(\mathbb{Z}_{12}^*, \cdot_{12})$*?*

Odgovor:

Izrek 29 (Opis končnih Abelovih grup) *Naj bo G končna Abelova grupa, $n = |G|$. Potem obstaja zapis števila n v obliki $n = \prod_{i=1}^{k} p_i^{\alpha_i}$, kjer so p_i praštevila, $p_1 \leq p_2 \leq ... \leq p_k$, $\alpha_i > 0$ tako, da je*

$$G \cong \prod_{i=1}^{k} \mathbb{Z}_{p_i^{\alpha_i}}$$

Opomba: Za različne zapise dobimo neizomorfne grupe.

Naloga 17 *Poišči vse neizomorfne Abelove grupe moči 72.*

Odgovor:

Naloga 18 *Poišči red elementa $(8, 4, 10)$ v grupi $\mathbb{Z}_{12} \times \mathbb{Z}_{60} \times \mathbb{Z}_{24}$.*

Permutacije

Ponovimo iz DS I:

A - končna množica;

$S(A)$ - množica vseh permutacij na A;

$\circ$ - kompozitum oz. produkt funkcij;

$S_n := S(A)$ za $A = \{1, 2, \ldots, n\}$, velja $|S_n| = n!$

Trditev 30 *Velja:*

- *Vsaka permutacija se da (enolično) razcepiti na produkt disjunktnih ciklov.*
- *Vsaka permutacija je bodisi soda ali liha (odvisno od števila transpozicij)*

Zgledi: $(123)(45)$ je liha permutacija, $(125)(34)(6789)$ pa je soda permutacija.

Vemo:

- id je soda permutacija,
- π ter π^{-1} sta enake parnosti,
- Če sta C_1 ter C_2 disjunktna cikla, potem $C_1 \circ C_2 = C_2 \circ C_1$,
- Če je $C = (a_1\, a_2\, \cdots\, a_n)$, potem je $C^{-1} = (a_n\, a_{n-1}\, \cdots\, a_1)$

Naj ima permutacija $\pi \in S_n$ v zapisu k_i ciklov dolžine i, za $i = 1, \ldots, n$.

Potem pravimo, da ima π **ciklično strukturo**

$$(k_1, k_2, \ldots, k_n).$$

Velja

$$1 \cdot k_1 + 2 \cdot k_2 + 3 \cdot k_3 + \cdots + n \cdot k_n = n.$$

Zgled: Permutacija $(123)(45)(56)(7)(89)$ ima ciklično strukturo $(1, 3, 2, 0, 0, 0, 0, 0, 0)$.

Trditev 31 *Naj bo C cikel dolžine m. Potem je* $\mathrm{red}(C) = m$.

Dokaz.

Trditev 32 *Naj bo permutacija π kompozitum tujih ciklov dolžine $m_1, m_2, \ldots, m_k$. Potem je* $\mathrm{red}(\pi) = \mathrm{lcm}(m_1, m_2, \ldots, m_k)$.

Dokaz.

Vaja:

Definiramo relacijo **konjugiranost** $\approx$ na $S(A)$ takole:

$$\pi_1 \approx \pi_2, \qquad \text{če} \quad \exists \tau \in G : \pi_2 = \tau \circ \pi_1 \circ \tau^{-1}$$

Izrek 33 *Permutaciji π in σ sta konjugirani natanko takrat, ko imata enako ciklično strukturo.*

Dokaz. ($\Rightarrow$). Če je $C = (i_1\, i_2\, \cdots\, i_k)$ cikel, potem je

$$\tau \circ C \circ \tau^{-1} = (\tau(i_1)\, \tau(i_2)\, \cdots\, \tau(i_k)).$$

Pri produktu disjunktnih ciklov pa tako učinkuje posebej na vsakem ciklu. Naj bo

$$\pi = (a_1\, a_2\, \cdots\, a_k) \circ (b_1\, b_2\, \cdots\, b_l) \circ \cdots \circ (c_1\, c_2\, \cdots\, c_m).$$

Potem je

$$\begin{aligned}
\tau \circ \pi \circ \tau^{-1} &= \tau \circ (a_1\, a_2\, \cdots\, a_k) \circ (b_1\, b_2\, \cdots\, b_l) \circ \cdots (c_1\, c_2\, \cdots\, c_m) \circ \tau^{-1} \\
&= \tau \circ (a_1\, a_2\, \cdots\, a_k) \circ [\tau^{-1} \circ \tau] \circ (b_1\, b_2\, \cdots\, b_l) \circ [\tau^{-1} \circ \tau] \circ \cdots (c_1\, c_2\, \cdots\, c_m) \circ \tau^{-1} \\
&= [\tau \circ (a_1\, a_2\, \cdots\, a_k) \circ \tau^{-1}] \circ [\tau \circ (b_1\, b_2\, \cdots\, b_l) \circ \tau^{-1}] \circ \cdots [\tau \circ (c_1\, c_2\, \cdots\, c_m) \circ \tau^{-1}] \\
&= \big(\tau(a_1)\, \tau(a_2)\, \cdots\, \tau(a_k)\big) \circ \big(\tau(b_1)\, \tau(b_2)\, \cdots\, \tau(b_l)\big) \circ \cdots \big(\tau(c_1)\, \tau(c_2)\, \cdots\, \tau(c_m)\big)
\end{aligned}$$

($\Leftarrow$) Recimo:

$$\pi = (a_1\, a_2\, \cdots\, a_k) \circ (b_1\, b_2\, \cdots\, b_l) \circ \cdots \circ (c_1\, c_2\, \cdots\, c_m)$$

in

$$\sigma = (a'_1\, a'_2\, \cdots\, a'_k) \circ (b'_1\, b'_2\, \cdots\, b'_l) \circ \cdots \circ (c'_1\, c'_2\, \cdots\, c'_m).$$

Definiramo funkcijo $\tau : x \mapsto x'$. Očitno, da je τ permutacija iz $S(A)$. Velja pa $\tau \circ \pi \circ \tau^{-1} = \sigma$. To pa vidimo takole:

$$\tau \circ \pi \circ \tau^{-1}(x'_i) = \tau \circ \pi(x_i) = \tau(x_{i+1}) = x'_{i+1} = \sigma(x'_i)$$

□

Naslednja trditev je hitra posledica prejšnjega izreka.

Posledica 34 *Konjugiranost $\approx$ je ekvivalenčna relacija.*

Simetrična grupa

Pokazali bomo, da je $(S(A), \circ)$ grupa. To grupo imenujemo **simetrična grupa** množice A.

Izrek 35 *$(S(A), \circ)$ je grupa.*

Dokaz. Pokažemo po vrsti vse lastnosti grupe.

zaprtost: $f, g \in S(A)$ potem je $f \circ g : A \to A$. Pokazati še moramo, da je $f \circ g$ permutacija, tj. bijekcija.

- *Injektivnost funkcije $f \circ g$:*

$$\begin{aligned} (f \circ g)(x) &= (f \circ g)(y) \\ f(g(x)) &= f(g(y)) \\ g(x) &= g(y) \qquad \text{(ker je } f \text{ injektivna)} \\ x &= y \qquad \text{(ker je } g \text{ injektivna)} \end{aligned}$$

- *Surjektivnost funkcije $f \circ g$:* Naj bo $y \in A$ poljuben. Ker je f surjektivna, obstaja $z \in A$ tako, da je $y = f(z)$. In, ker je g surjektivna, obstaja $x \in A$ tako, da je $g(x) = z$. Torej, obstaja tak x, da je $(f \circ g)(x) = f(g(x)) = y$.

asociativnost: Sledi iz

$$((f \circ g) \circ h)(x)) = (f \circ g)(h((x)) = f(g(h(x)))$$

in

$$(f \circ (g \circ h))(x)) = f((g \circ h)(x)) = f(g(h(x)))$$

enota: Enota je permutacija $\mathrm{id} : x \mapsto x$.

inverz: Če je $f : A \to A$ bijekcija, potem vemo, da obstaja bijektivna funkcija $f^{-1} : A \to A$ tako, da velja:

$$f^{-1}(f(x)) = x \quad \text{in} \quad f(f^{-1}(x)) = x.$$

To pa je enakovredno pogoju za obstoj inverza v grupi:

$$f^{-1} \circ f = \mathrm{id} \quad \text{in} \quad f \circ f^{-1} = \mathrm{id}.$$

□

Permutacijska grupa je vsaka podgrupa grupe $S(A)$.

Opomba 1 *S_n ni Abelova (tj. komutativna) za $n \geq 3$. Velja:*

$$(12)(23) = (123) \neq (132) = (23)(12).$$

S_3 je najmanjša nekomutativna grupa.

Zgled: $S_3 = \{id, (123), (132), (1)(23), (2)(13), (12)(3)\}$

$A_3 = \{\mathrm{id}, (123), (132)\}$ je podgrupa v S_3. Velja še več, A_3 je edinka v S_3.

Alternirajoča grupa

Alternirajoča grupa A_n je definirana takole

$$A_n = \{f \in S_n \mid f \text{ soda permutacija}\}$$

V naslednjem izreku pa pokažemo, da je A_n grupa.

Izrek 36 *Za A_n ter S_n verja naslednje:*

(1) *A_n je podgrupa v S_n;*

(2) *Indeks grupe S_n po podgrupi A_n je 2, t.j. $[S_n : A_n] = 2$;*

(3) $|A_n| = n!/2$.

Dokaz. (1) Če π, σ sodi, potem $\pi \circ \sigma$ soda permutacija. Torej je A_n grupa.

Definirajmo $F : A_n \to S_n \setminus A_n$ takole

$$F(f) = (12) \circ f.$$

Očitno, F je bijekcija. Zato

$$|A_n| = |S_n \setminus A_n| \text{ ter } |S_n| = |A_n| + |S_n \setminus A_n| = 2|A_n|.$$

Od tod sledita (2) in (3). □

Posledica 37 *Alternirajoča grupa A_n je podgrupa edinka v simetrični grupi S_n.*

Dokaz. Po prejšnjem izreku, je A_n podgupa v S_n z $[S_n : A_n] = 2$. Potem dokaz sledi takoj iz izreka 21.

Cayleyjev izrek

Izrek 38 *Vsaka grupa je izomorfna neki permutacijski grupi.*

Dokaz. Naj bo $(G, *)$ grupa. Za vsak element $a \in G$ definiramo $f_a : G \to G$ z predpisom

$$f_a(x) = a * x.$$

Opazimo, da je f_a permutacija iz $S(G)$

Naj bo $h : G \to S(G)$ tako, da je $h(a) = f_a$

Trdimo, da je h homomorfizem:

$$h(ab)(x) = (a * b) * x = a * (b * x) = f_a(f_b(x)) = (h(a) \circ h(b))(x)$$

Trdimo, da je h injektivna preslikava:

$$h(a) = h(b) \Rightarrow f_a = f_b \Rightarrow \forall x \in G : a * x = b * x \Rightarrow a = b$$

Torej sledi, da je grupa G izomorfna svoji sliki $\mathrm{im}(h)$ v $S(G)$. Ker pa je $\mathrm{im}(h)$ podgrupa iz $S(G)$, je dokaz končan. □

Automorfizmi grafov

Naj bo G graf, $Aut(G)$, ...