Algebrske strukture, 1.del

Grupoidi in polgrupe

Operacija na množici nam pove, kako iz dveh elementov te množice zgradimo nov element te množice. Formalno jo definiramo takole:

Definicija operacije na množici

Operacija na množici M je funkcija iz $M \times M$ v M.

Opomba: Množica $M \times M$ se sestoji iz vseh urejenih parov (a, b), kjer sta a in b elementa M. Funkcija $\circ\colon M \times M \to M$ preslika urejeni par (a, b) v element $\circ(a, b)$. Namesto $\circ(a, b)$ bomo običajno pisali $a \circ b$.

Opomba: Na isti množici imamo lahko več različnih operacij. Da jih ločimo, uvedemo pojem grupoida. Grupoid je množica skupaj z izbrano operacijo na tej množici. Formalno ga definiramo takole:

Definicija grupoida

Grupoid je urejeni par $(M, \circ)$, kjer je M množica in je $\circ$ operacija na M.

Definicija polgrupe

Operacija $\circ$ na množici M je **asociativna**, če za vse a, b, c iz M velja

$$(a \circ b) \circ c = a \circ (b \circ c).$$

Polgrupa je tak grupoid $(M, \circ)$, kjer je $\circ$ asociativna operacija na M.
Operacija $\circ$ je **komutativna** če velja $a \circ b = b \circ a$ za vse $a, b \in M$.
Polgrupi s komutativno operacijo pravimo **komutativna polgrupa**.

Opomba: Iz asociativnosti operacije $\circ$ sledi, da je vrednost izraza $a_1 \circ a_2 \circ \ldots \circ a_n$ neodvisna od tega, kako postavimo oklepaje. Seveda pri postavljanju oklepajev ne smemo spreminjati vrstnega reda faktorjev.

Opomba: Če želimo, da je vrednost izraza $a_1 \circ a_2 \circ \ldots \circ a_n$ neodvisna tudi od vrstnega reda faktorjev, mora biti operacija $\circ$ tudi **komutativna**.

Primeri komutativnih polgrup

Naj bo $\mathbb{N} = \{1, 2, \ldots\}$ množica vseh naravnih števil. Množenje in seštevanje naravnih števil sta operaciji, ki sta tako komutativni kot asociativni. Torej sta $(\mathbb{N}, \cdot)$ in $(\mathbb{N}, +)$ komutativni polgrupi.

Polgrupa vseh $n \times n$ matrik

Naj bo $M_n(\mathbb{R})$ množica vseh $n \times n$ matrik in naj bo $\cdot$ množenje matrik. Potem je $(M_n(\mathbb{R}), \cdot)$ polgrupa. Če je $n \geq 2$, ta polgrupa ni komutativna.

Polgrupa vseh preslikav iz S v S

2) Naj bo S poljubna množica in naj bo F_S množica vseh funkcij iz S v S. Operacija $\circ$ naj bo kompozitum dveh funkcij. Potem je $(F_S, \circ)$ polgrupa. Za vse funkcije $f, g, h \in F_S$ in vse elemente $s \in S$ namreč velja

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

Če ima S vsaj tri različne elemente potem polgrupa $(F_S, \circ)$ ni komutativna. Recimo, da so $a, b, c \in S$ paroma različni elementi. Naj bo f transpozicija elementov a in b, g pa transpozicija elementov a in c. Potem velja, da $f(g(a)) = f(c) = c$ ni enak $g(f(a)) = g(b) = b$. Torej $f \circ g \neq g \circ f$.

Polgrupa vseh besed s črkami iz A

Naj bo A neprazna množica črk. Naj bo M množica vseh besed, ki jih lahko sestavimo s črkami iz A. Operacija $\circ$ naj bo stikanje besed.

Recimo *aba* in *bab* sta dve besedi s črkami iz $A = \{a, b\}$. Če ju staknemo, dobimo besedo $aba \circ bab = ababab$. To ni isto kot $bab \circ aba = bababa$.

Očitno je stikanje besed asociativna operacija, torej je $(M, \circ)$ polgrupa. Če množica A vsebuje vsaj dve črki, potem je ta polgrupa nekomutativna.

Primer grupoida, ki ni polgrupa

Vektorski produkt je očitno operacija na $\mathbb{R}^3$. Pokažimo, da ta operacija ni niti asociativna niti komutativna. Velja namreč

$$\mathbf{e}_1 \times \mathbf{e}_2 = \mathbf{e}_3 \qquad (\mathbf{e}_1 \times \mathbf{e}_1) \times \mathbf{e}_2 = \mathbf{0}$$

$$\mathbf{e}_2 \times \mathbf{e}_1 = -\mathbf{e}_3 \qquad \mathbf{e}_1 \times (\mathbf{e}_1 \times \mathbf{e}_2) = \mathbf{e}_1 \times \mathbf{e}_3 = -\mathbf{e}_2$$

Grupoid $(\mathbb{R}^3, \times)$ torej ni komutativen in ni polgrupa.

Primer komutativnega grupoida, ki ni polgrupa

Označimo z $M_2(\mathbb{R})$ množico vseh 2×2 matrik. Jordanski produkt na $M_2(\mathbb{R})$ je definiran z

$$A \circ B = \frac{1}{2}(AB + BA)$$

Očitno je ta operacija komutativna. Pokažimo, da ni asociativna. Vzemimo

$$A = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}, \qquad B = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}$$

Očitno je $A \circ B = \frac{1}{2}I$ in $A \circ A = 0$. Torej je

$$(A \circ A) \circ B = 0, \qquad A \circ (A \circ B) = A \circ \frac{1}{2}I = \frac{1}{2}A$$

Torej je $(M_2(\mathbb{R}), \circ)$ komutativen grupoid, ki ni polgrupa.

Monoidi

Definicija enote

Naj bo $(M, \circ)$ grupoid. Element $e \in M$ je **enota** tega grupoida če velja $a \circ e = a$ in $e \circ a = a$ za vsak $a \in M$. Polgrupi z enoto pravimo **monoid**.

Opomba: Element $e \in M$ je **desna enota** grupoida $(M, \circ)$, če velja $a \circ e = a$ vsak $a \in M$. Element $e \in M$ je **leva enota** grupoida $(M, \circ)$, če velja $e \circ a = a$ vsak $a \in M$. Enota je torej tak element, ki je tako leva enota kot desna enota.

Trditev o enoličnosti enote

Vsak grupoid ima lahko največ eno enoto.

Dokaz: Naj bosta e in f dve enoti grupoida $(M, \circ)$. Potem za vsak $a \in M$ velja $e \circ a = a$ in za vsak $b \in M$ velja $b \circ f = b$. Če vstavimo $a = f$ in $b = e$, dobimo $e \circ f = f$ in $e \circ f = e$. Torej je $e = f$.

Opomba: Dokazali smo celo več, kot smo obljubili. Dokaz nam pove, da je vsaka leva enota grupoida enaka vsaki desni enoti grupoida. Odtod sledi, da grupoid z enoto nima drugih levih ali desnih enot.

Opomba: Če grupoid nima nobene leve enote, potem se lahko zgodi, da ima več desnih enot. Če grupoid nima nobene desne enote, potem se lahko zgodi, da ima več levih enot.

Primeri enot

- Polgrupa $(\mathbb{N}, \cdot)$ ima enoto 1. Polgrupa $(\mathbb{N}, +)$ nima enote, ker $0 \notin \mathbb{N}$.
- Polgrupa $(M_n(\mathbb{R}), \cdot)$ ima za enoto identično $n \times n$ matriko I_n.
- Polgrupa $(F_S, \circ)$ ima za enoto **identično preslikavo** iz S v S. To je preslikava definirana z $\mathrm{id}_S(x) = x$ za vsak $x \in S$.
- Polgrupa vseh besed s črkami iz A ima za enoto prazno besedo.
- Grupoid $(\mathbb{R}^3, \times)$ nima niti leve niti desne enote.

Primer polgrupe, ki ima več levih enot in nobene desne enote

Naj bo

$$M = \{ \begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix} \mid a, b \in \mathbb{R} \}$$

in naj bo $\circ$ običajno množenje matrik. Ker velja

$$\begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix} \begin{bmatrix} c & d \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} ac & ad \\ 0 & 0 \end{bmatrix}$$

je produkt dveh matrik iz M spet matrika iz M. Torej je $(M, \circ)$ grupoid. Ker je matrično množenje asociativno, je tudi operacija $\circ$ asociativna. Torej je $(M, \circ)$ polgrupa. Opazimo, da je vsak element oblike

$$\begin{bmatrix} 1 & x \\ 0 & 0 \end{bmatrix}$$

leva enota polgrupe $(M, \circ)$. Imamo torej neskončno levih enot. Odtod in iz prve opombe sledi, da nimamo nobene desne enote.

Grupe

Definicija inverza

Naj bo $(M, \circ)$ monoid z enoto e. Pravimo, da je element $a \in M$ **obrnljiv**, če obstaja tak element $b \in M$, ki zadošča $a \circ b = e$ in $b \circ a = e$. V tem primeru pravimo, da je element b **inverz** elementa a in pišemo $b = a^{-1}$. Monoidu, v katerem je vsak element obrnljiv, pravimo **grupa**.

Opomba: Element $b \in M$ je **desni inverz** elementa $a \in M$, če je $a \circ b = e$. Element $b \in M$ je **levi inverz** elementa $a \in M$, če je $b \circ a = e$. Inverz elementa $a \in M$ je torej tak element M, ki je tako levi kot desni inverz a.

Trditev o enoličnosti inverza

V vsakem monoidu ima vsak element največ en inverz.

Dokaz: Recimo, da sta elementa b in c inverza elementa a. Potem velja $a \circ b = e$, $b \circ a = e$, $a \circ c = e$ in $c \circ a = e$. Ker smo v monoidu, velja

$$b = b \circ e = b \circ (a \circ c) = (b \circ a) \circ c = e \circ c = c.$$

Opomba: V dokazu smo uporabili samo, da je b levi inverz a in da je c desni inverz a. Dokazali smo torej močnejšo trditev, da je vsak levi inverz elementa a enak vsakemu desnemu inverzu elementa a.

Opomba: Če element nima nobenega levega inverza, potem se lahko zgodi, da ima več desnih inverzov. Če element nima nobenega desnega inverza, potem se lahko zgodi, da ima več levih inverzov.

Opomba: Če monoid $(M, \circ)$ ni grupa, označimo z $M^\times$ množico vseh obrnljivih elementov v M. Opazimo, da $(M^\times, \circ)$ grupa, ker velja:

- Če $a, b \in M^\times$, potem tudi $a \circ b \in M^\times$. Velja namreč $(a \circ b)^{-1} = b^{-1} \circ a^{-1}$. Torej je $(M^\times, \circ)$ polgrupa.
- Velja $e \in M^\times$, ker je $e^{-1} = e$. Torej je $(M^\times, \circ)$ monoid.
- Če $a \in M^\times$, potem tudi $a^{-1} \in M^\times$. Velja namreč $(a^{-1})^{-1} = a$. Torej je $(M^\times, \circ)$ grupa.

Primer: Inverzi števil

- Množica vseh celih števil $\mathbb{Z}$ je grupa za operacijo seštevanja $+$. Očitno je namreč $(\mathbb{Z}, +)$ monoid z enoto 0 in vsak $x \in \mathbb{Z}$ ima inverz $-x \in \mathbb{Z}$.
- Tudi $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$ so grupe.
- $(\mathbb{Q}, \cdot)$ je monoid z enoto 1, ampak ni grupa, ker element 0 ni obrnljiv. Vsak neničeln element $x \in \mathbb{Q}$ ima inverz $\frac{1}{x}$. Množica obrnljivih elementov v $\mathbb{Q}$ je torej $\mathbb{Q}^\times = \mathbb{Q} \setminus \{0\}$. Vemo, da je $(\mathbb{Q}^\times, \cdot)$ grupa.
- Tudi $(\mathbb{R}^\times, \cdot)$ in $(\mathbb{C}^\times, \cdot)$ sta grupi.

Opomba: Vse grupe v zgornjem primeru so komutativne. Komutativnim grupam pravimo tudi Abelove grupe.

Primer: Aditivna grupa matrik

Naj bo $M_{m,n}(\mathbb{R})$ množica vseh $m \times n$ matrik in naj bo operacija $+$ seštevanje matrik. Potem je $(M_{m,n}(\mathbb{R}), +)$ Abelova grupa z enoto $0_{m,n}$. Inverz matrike A v tej Abelovi grupi je matrika $-A$.

Primer: Inverzi matrik

Naj bo $M_n(\mathbb{R})$ množica vseh $n \times n$ matrik in naj bo $\cdot$ operacija množenja matrik. Pokazali smo, da je $(M_n(\mathbb{R}), \cdot)$ polgrupa z enoto I_n, torej monoid.

Vemo, da je matrika $A \in M_n(\mathbb{R})$ obrnljiva natanko tedaj, ko je $\det A \neq 0$. V tem primeru je $A^{-1} = \frac{1}{\det A}\tilde{A}^T$. Vemo tudi, da iz $AB = I$ sledi $BA = I$, torej pojmi levega inverza, desnega inverza in inverza sovpadejo.

Grupo vseh obrnljivih $n \times n$ matrik označimo z $\mathrm{GL}_n(\mathbb{R})$. Pravimo ji n-ta **glavna linearna grupa**.

Primer: Inverzi besed

Naj bo M množica vseh besed nad neko abecedo in naj bo $\circ$ stikanje besed. Potem je $(M, \circ)$ monoid, katerega enota je prazna beseda. Če staknemo neprazno besedo s poljubno besedo, dobimo neprazno besedo. Neprazne besede torej niso obrnljive, saj nimajo niti levega niti desnega inverza. Prazna beseda je seveda obrnljiva in njen inverz je spet prazna beseda.

Primer: Inverzi funkcij

Naj bo S neprazna množica in naj bo F_S množica vseh funkcij iz S v S. Vemo, da je F_S monoid za operacijo kompozitum funkcij. Pokazali bomo, da je funkcija $f : S \to S$ obrnljiva natanko tedaj, ko je bijektivna. Bijektivni funkciji iz S v S pravimo tudi **permutacija** množice S. Grupo vseh permutacij množice S bomo označili z $\mathcal{P}(S)$. Primer je $S_n := \mathcal{P}(\mathbb{N}_n)$.

Ekvivalentnost obrnljivosti in bijektivnosti sledi iz naslednjih dveh trditev:

- Funkcija $f : S \to S$ ima levi inverz natanko tedaj, ko je injektivna.
- Funkcija $f : S \to S$ ima desni inverz natanko tedaj, ko je surjektivna.

Dokaz: Če ima funkcija f levi inverz g, potem iz $f(x) = f(y)$ sledi $x = g(f(x)) = g(f(y)) = y$. Torej je f injektivna.

Če je funkcija f injektivna, potem definirajmo funkcijo $g : S \to S$ takole: Elemente, ki so v zalogi vrednosti funkcije f, preslikamo v njihove originale (ti so zaradi injektivnosti f enolično določeni). Elemente, ki niso v zalogi vrednosti funkcije f, preslikajmo v poljubne elemente. Po definiciji g velja $g(f(x)) = x$ za vsak $x \in S$, torej je g levi inverz f.

Če ima funkcija f desni inverz g, potem iz $y = f(g(y))$ sledi, da je f surjektivna, saj je vsak element $y \in S$ slika nekega elementa $g(y) \in S$.

Če je funkcija f surjektivna, potem definirajmo funkcijo $g\colon S \to S$ takole: $g(x) =$ poljuben tak $y \in S$, da velja $f(y) = x$. Obstoj y sledi iz definicije surjektivnosti. Iz definicije g sledi, da velja $f(g(x)) = x$ za vsak $x \in S$, torej je g desni inverz f. □

Za konec si oglejmo še konkreten primer. Naj bo $S = \mathbb{N}$ in naj bo funkcija $f : \mathbb{N} \to \mathbb{N}$ definirana z $f(x) = x + 1$. Očitno je f injektivna, ni pa surjektivna. Torej ima f levi inverz, nima pa desnega. Za vsak $a \in \mathbb{N}$ je

$$g(x) = \begin{cases} x - 1 & \text{če } x \geq 2 \\ a & \text{če } x = 1 \end{cases}$$

levi inverz funkcije f. Torej ima f neskončno levih inverzov.

Lahko poiščemo tudi funkcijo iz $\mathbb{N}$ v $\mathbb{N}$, ki ima neskončno desnih inverzov in nobenega levega. Primer je funkcija $f(2x) = x$ in $f(2x - 1) = 1$.

Podgrupoidi, podpolgrupe in podmonoidi

Naj bo $\circ$ operacija na množici M in naj bo N podmnožica v M. Pravimo, da je podmnožica N **zaprta** za operacijo $\circ$, če za vsaka elementa a in b iz N tudi element $a \circ b$ pripada N. V tem primeru lahko definiramo operacijo $\circ_N$ na N s predpisom $a \circ_N b := a \circ b$ za vsaka a in b iz N.

Operaciji $\circ_N$ pravimo **skrčitev** operacije $\circ$ na podmnožico N. Skrčitev $\circ_N$ podeduje številne lastnosti operacije $\circ$. Če je recimo $\circ$ asociativna, potem je tudi $\circ_N$ asociativna. Podobno velja tudi za komutativnost. Po drugi strani se obstoj enote ne podeduje vedno. Prav tako se ne obstoj inverza.

Definicije podstruktur

- Naj bo $(M, \circ)$ grupoid. Podmnožica $N \subseteq M$ je **podgrupoid** v $(M, \circ)$, če je zaprta za $\circ$. (Potem je $(N, \circ_N)$ grupoid.)
- Naj bo $(M, \circ)$ polgrupa. Podmnožica $N \subseteq M$ je **podpolgrupa** v $(M, \circ)$, če je podgrupoid v $(M, \circ)$. (Potem je $(N, \circ_N)$ polgrupa.)
- Naj bo $(M, \circ)$ monoid. Podmnožica $N \subseteq M$ je **podmonoid** v $(M, \circ)$, če je podpolgrupa in če vsebuje enoto. (Potem je $(N, \circ_N)$ monoid.)

Opomba: Če je $(M, \circ)$ polgrupa z enoto e in če je N podpolgrupa v $(M, \circ)$, potem je $N \cup \{e\}$ podmonoid v $(M, \circ)$.

Primeri

- Množica sodih naravnih števil je podpolgrupa v $(\mathbb{N}, +)$ in v $(\mathbb{N}, \cdot)$.
- Množica lihih naravnih števil je podmonoid v $(\mathbb{N}, \cdot)$.
- Množica vseh matrik oblike $\begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix}$ je podpolgrupa v $(M_2(\mathbb{R}), \cdot)$.
- Množica 2×2 matrik s elementi ≥ 0 je podmonoid v $(M_2(\mathbb{R}), +)$.
- Množica vseh besed, ki se začnejo z črko a je podpolgrupa v monoidu vseh besed. (Operacija je stikanje besed.)
- Množica vseh funkcij oblike $kx + n$ je podmonoid v monoidu vseh funkcij iz $\mathbb{R}$ v $\mathbb{R}$. (Operacija je kompozitum funkcij.)
- Množica vseh polinomov s pozitivnim vodilnim koeficientom je podpolgrupa v $(\mathbb{R}[x], +)$ ter podmonoid v $(\mathbb{R}[x], \cdot)$ in v $(\mathbb{R}[x], \circ)$.

Opomba: Če je $(M, \circ)$ polgrupa z enoto e in če je N podpolgrupa v $(M, \circ)$, potem se lahko zgodi, da ima $(N, \circ_N)$ enoto različno od e.

Primer podpolgrupe z različno enoto

Množica $M = \mathbb{N} \times \mathbb{N}$ je monoid za operacijo $(a, b) \circ (c, d) = (ac, bd)$. Monoid $(M, \circ)$ ima enoto $e = (1, 1)$. Podmnožica $N = \mathbb{N} \times \{0\}$ je zaprta za $\circ$ in ne vsebuje e. Torej je N podpolgrupa, ki ni podmonoid. Polgrupa $(N, \circ_N)$ ima enoto $f = (1, 0)$. Očitno f ni enaka enoti monoida $(M, \circ)$.

Oglejmo si še primer podgrupoida, ki ni podpolgrupa.

Primer podgrupoida

Vemo, da je $(\mathbb{R}^3, \times)$ grupoid, ki ni polgrupa. Naj bo $N \subseteq \mathbb{R}^3$ premica skozi izhodišče, se pravi linearna ogrinjača nekega vektorja. Za vsaka elementa $\mathbf{a}, \mathbf{b} \in N$ velja $\mathbf{a} \times \mathbf{b} = \mathbf{0}$, kar je element N.

Podgrupe

Spomnimo se, da je grupa tak monoid v katerem je vsak element obrnljiv.

Definicije podgrupe

Naj bo $(G, \circ)$ grupa. Podmnožica $H \subseteq G$ je **podgrupa** v $(G, \circ)$, če je podmonoid in če vsebuje inverz vsakega svojega elementa.

Opomba: Na dolgo povedano je podmnožica $H \subseteq G$ podgrupa, če:

- Za vsaka $a, b \in H$ velja $a \circ b \in H$.
- Velja $e \in H$.
- Za vsak $a \in H$ velja $a^{-1} \in H$.

Pokažimo, da lahko te tri lastnosti strnemo v eno samo.

Trditev

Naj bo množica G grupa za operacijo $\circ$. Podmnožica $H \subseteq G$ je **podgrupa** natanko tedaj, ko za vsaka $a, b \in H$ velja $a \circ b^{-1} \in H$.

Dokaz: Naj bo H taka podmnožica v G, ki zadošča lastnosti iz trditve. Preverimo, da H zadošča vsem trem lastnostim iz definicije podgrupe:

- Dokažimo, da $e \in H$. Če v lastnost iz trditve vstavimo $b = a$, dobimo $a \circ a^{-1} \in H$ za vsak $a \in H$. Torej je res $e \in H$.
- Dokažimo, da $a^{-1} \in H$ za vsak $a \in H$. Če v lastnost iz trditve vstavimo $a = e$ in $b = a$, dobimo $e \circ a^{-1} \in H$ za vsak $a \in H$.
- Dokažimo, da $a \circ b \in H$ za vsaka $a, b \in H$. Če $a, b \in H$, potem $a, b^{-1} \in H$ po prejšnji točki. Po lastnosti iz trditve je potem $a \circ (b^{-1})^{-1} \in H$. To pa je ravno $a \circ b \in H$.

Dokažimo še, da vsaka podgrupa H zadošča lastnosti iz trditve. Vzemimo poljubna $a, b \in H$. Po tretji lastnosti iz definicije podgrupe odtod sledi $a, b^{-1} \in H$. Po prvi lastnosti iz definicije podgrupe sledi $a \circ b^{-1} \in H$.

Primer: Ciklične podgrupe

Če je $(G, \circ)$ grupa, potem je za vsak element $a \in G$ množica $\langle a \rangle := \{a^m \mid m \in \mathbb{Z}\}$ podgrupa v $(G, \circ)$. Izraz a^m definiramo z $a^0 = e$, $a^n = \underbrace{a \circ \ldots \circ a}_{\text{n-krat}}$ in $a^{-n} = \underbrace{a^{-1} \circ \ldots \circ a^{-1}}_{\text{n-krat}}$ za vsak $n \in \mathbb{N}$.

Primeri podgrup v $\mathrm{GL}_n(\mathbb{R})$

Spomnimo se, da je $\mathrm{GL}_n(\mathbb{R}) = \{A \in M_n(\mathbb{R}) \mid \det A \neq 0\}$. Definirajmo:

- $\mathrm{SL}_n(\mathbb{R}) = \{A \in M_n(\mathbb{R}) \mid \det A = 1\}$.
- $\mathrm{UT}_n(\mathbb{R}) =$ vse zgornje trikotne $n \times n$ matrike z enkami po diagonali.
- $\mathrm{O}_n(\mathbb{R}) = \{A \in M_n(\mathbb{R}) \mid A^T A = I\}$.

Te množice so podgrupe v $\mathrm{GL}_n(\mathbb{R})$.

Primeri podgrup v S_n

Spomnimo se, da je S_n grupa vseh permutacij množice $\mathbb{N}_n = \{1, \ldots, n\}$.

- Podmnožica $A_n = \{\sigma \in S_n \mid \mathrm{sgn}(\sigma) = 1\}$ je podgrupa v S_n.
- Naj bo $\sigma = \begin{pmatrix} 1 & 2 & \ldots & n-1 & n \\ 2 & 3 & \ldots & n & 1 \end{pmatrix}$. Potem je $Z_n := \langle \sigma \rangle$ podgrupa v S_n.
- Naj bo R neka relacija na množici $\mathbb{N}_n$. Permutacija $\sigma \in S_n$ je **avtomorfizem** relacije R, če iz iRj vedno sledi $\sigma(i)R\sigma(j)$. Množica vseh avtomorfizmov relacije R je podgrupa v S_n.
- Označimo z R relacijo sosednosti oglišč v n-kotniku. Podgrupi vseh avtomorfizmov R pravimo n-ta **diedrska** grupa in jo označimo z D_n.

Lastnosti končnih grup

Zanimajo nas grupe s končno močjo (moč = število elementov).

Lagrangeov izrek

Moč podgrupe deli moč grupe.

Dokaz: Naj bo H podgrupa končne grupe $(G, \circ)$. Za vsak $g \in G$ naj bo

$$g \circ H := \{g \circ h \mid h \in H\}$$

Izrek sledi iz $G = \bigcup_{g \in G} g \circ H$ in iz naslednjih dveh pomožnih trditev:

- Za vsak g je moč množice $g \circ H$ enaka moči množice H.
- Če imata množici $g_1 \circ H$ in $g_2 \circ H$ neprazen presek, potem sta enaki.

Pokažimo najprej, da je $h \mapsto g \circ h$ bijektivna preslikava iz H v $g \circ H$. Surjektivnost sledi iz definicije $g \circ H$. Dokažimo še injektivnost. Če je $g \circ h_1 = g \circ h_2$, potem je $h_1 = g^{-1} \circ (g \circ h_1) = g^{-1} \circ (g \circ h_2) = h_2$. To nam da prvo pomožno trditev.

Če imata množici $g_1 \circ H$ in $g_2 \circ H$ neprazen presek, potem obstajata taka elementa $h_1, h_2 \in H$, da velja $g_1 \circ h_1 = g_2 \circ h_2$. Sledi $g_2^{-1} \circ g_1 = h_2 \circ h_1^{-1}$. Vzemimo sedaj poljuben element $x \in g_1 \circ H$. Potem obstaja tak element $h \in H$, da velja $x = g_1 \circ h$. Odtod sledi

$$x = e \circ g_1 \circ h = g_2 \circ g_2^{-1} \circ g_1 \circ h = g_2 \circ h_2 \circ h_1^{-1} \circ h \in g_2 \circ H.$$

Dokazali smo torej $g_1 \circ H \subseteq g_2 \circ H$. Če v dokazu zamenjamo g_1 in g_2, dobimo še obratno inkluzijo. To nam da drugo pomožno trditev. □

Primer

Grupa S_n ima $n!$ elementov. Oglejmo si njene podgrupe:

- A_n ima $\frac{n!}{2}$ elementov.
- D_n ima $2n$ elementov.
- Z_n ima n elementov.

V vseh primerih moč podgrupe deli moč grupe.

Definicija: Red elementa

Naj bo $(G, \circ)$ grupa. **Red elementa** $a \in G$ je najmanjše naravno število n, ki zadošča $a^n = e$. Če tak n ne obstaja, je red elementa a neskončen.

Trditev

Vsak element vsake končne grupe ima končen red, ki deli moč grupe.

Dokaz. Naj bo m moč grupe in a element grupe. Potem $e, a, a^2, \ldots, a^m$ ne morejo biti paroma različni, ker jih je več kot elementov grupe. Torej obstajata taki števili $k, l = 0, \ldots, m$, da je $k \neq l$ in $a^k = a^l$. Če je $k > l$, sledi $a^{k-l} = e$, sicer pa $a^{l-k} = e$. Torej ima a končen red. Če je red a enak n, potem je $\{e, a, a^2, \ldots, a^{n-1}\}$ podgrupa, torej n deli m. □

Posledica

Podmnožica končne grupe je podgrupa natanko tedaj, ko je zaprta za $\circ$.

Dokaz: Če je a element podmnožice in če je njegov red enak n, potem je $a^{-1} = a^{n-1}$ tudi element podmnožice, ker je ta zaprta za operacijo. Sledi, da podmnožica vsebuje enoto, torej izpolnjuje vse tri lastnosti podgrupe.

Primer: Red cikla

Oglejmo si najprej poseben primer permutacije, ki mu pravimo **cikel**. Naj bodo $a_1, \ldots, a_k$ paroma različni elementi množice $\mathbb{N}_n$. Označimo z

$$(a_1 \ a_2 \ \ldots \ a_k)$$

permutacijo, ki preslika $a_1 \mapsto a_2$, $a_2 \mapsto a_3$, $\ldots$, $a_{k-1} \mapsto a_k$, $a_k \mapsto a_1$, elemente iz $\mathbb{N}_n \setminus \{a_1, \ldots, a_k\}$ pa preslika same vase.

Pokažimo, da je red elementa $\sigma := (a_1 \ a_2 \ \ldots \ a_k)$ enak k. Velja

$$\sigma^l(a_i) = \begin{cases} a_{i+l} & \text{če } i + l \leq k \\ a_{i+l-k} & \text{če } i + l > k \end{cases}$$

za vsak $i, l = 1, \ldots, k$. Torej je $\sigma^k = \mathrm{id}$ in $\sigma \neq \mathrm{id}, \ldots, \sigma^{k-1} \neq \mathrm{id}$.

Primer: Red permutacije

Če cikla σ in τ nimata skupnih elementov, potem velja $\sigma \circ \tau = \tau \circ \sigma$. Potem za vsako naravno število k velja $(\sigma \circ \tau)^k = \sigma^k \circ \tau^k$. Ker σ^k in τ^k nimata skupnih elementov, je $\sigma^k \circ \tau^k = \mathrm{id}$ natanko tedaj, ko je $\sigma^k = \mathrm{id}$ in $\tau^k = \mathrm{id}$. Torej je $(\sigma \circ \tau)^k = \mathrm{id}$ natanko tedaj, ko red σ deli k in red τ deli k. Dokazali smo, da je red $\sigma \circ \tau$ enak najmanjšemu skupnemu večkratniku redov σ in τ. To trditev lahko posplošimo tudi na več ciklov.

Kratek premislek pokaže, da lahko vsako permutacijo zapišemo kot kompozitum disjunktnih ciklov. Torej je njen red enak najmanjšemu skupnemu večkratniku redov teh disjunktnih ciklov.

Izračunajmo red permutacije

$$\rho = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 1 & 3 & 2 \end{pmatrix}$$

Najprej izrazimo permutacijo kot kompozitum disjunktnih ciklov. Dobimo $\rho = (1\ 4\ 3) \circ (2\ 5)$. Red cikla $(1\ 4\ 3)$ je enak 3, red cikla $(2\ 5)$ pa je 2. Najmanjši skupni večkratnik 3 in 2 je 6. Torej je red permutacije ρ enak 6.