1. Grupy

Last upgrade: 28.2.2019
Poznámky spracované podľa učebnice Joseph A. Gallian, Contemporary abstract algebra, Brooks/Cole, Boston, 2010.

1 Definícia grupy

Definícia 1 (Binárna operácia) *Nech G je množina. Binárna operácia je funkcia $G \times G \to G$.*

Ak f je binárna operácia, tak namiesto $f(a, b)$ budeme písať ab, $a \circ b$, $a * b$, alebo $a + b$.

Definícia 2 (Grupa) *Nech G je množina s binárnou operáciou. Binárna operácia je funkcia $G \times G \to G$ spĺňujúca nasledovné podmienky:*

- *pre každé $a, b, c \in G$ platí: $a(bc) = (ab)c$, (asociatívnosť)*
- *existuje $e \in G$ také, že pre každý prvok $a \in G$ $ea = ae = 1$.*
- *pre každý prvok a existuje prvok b taký, že $ab = e = ba$.*

Binárna operácia definovaná na G sa nazýva *komutatívna*, ak pre každé dva prvky a, b platí $ab = ba$.
Poznámka.

Príklad 3 (Príklady grúp a negrúp.)

- $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{Q}^+, \cdot)$, $(\mathbb{R} - \{0\}, \cdot)$, $(\mathbb{C}, +)$, $(\mathbb{C} - \{0\}, \cdot)$.
- *Je $(\mathbb{Z}, \cdot)$ grupa?*
- $(U, \cdot)$, *kde* $U = \{x \in \mathbb{C}; |x| = 1\}$.
- *Kladné iracionálne čísla s operáciou násobenia spĺňujú všetky 3 axiomy, ale netvoria grupu.*
- *Matice 2×2 so sčitovaním.*
- $(\mathbb{Z}_n, +)$.
- $GL(2, R)$ *aj* $GL(2, Q)$, $GL(2, C)$.
- *Kedy je $(\mathbb{Z}_n - \{0\}, \cdot)$ grupa?*
- *Grupy $U(n)$.*
- *Vektory nad poľom so sčitovaním.*
- $GL(2, \mathbb{Z}_p)$.
- *Lineárna a afinná grupa.*

Prvok e budeme označovať 1 vo všeobecnej grupe, a 0 v komutatívnej grupe. Prvok $b = a^{-1}$ z axiomy (iii) budeme nazývať inverzný prvok ku prvku a. Zápis $1 = aa^{-1} = a^{-1}a$.

Lema 4 (Základné vlastnosti) *Nech G je grupa. Potom*

- *G má jediný neutrálny prvok,*
- *$ba = ca$ implikuje $b = c$, (pravé krátenie)*
- *$ab = ac$ implikuje $b = c$, (ľavé krátenie)*
- *pre každý prvok existuje jediný inverzný prvok.*
- *$(ab)^{-1} = b^{-1}a^{-1}$.*

Definícia 5 (Mocnina prvku) *Nech G je grupa. Z asociativity operácie vyplýva, že výraz $x_1x_2 \dots x_m$ je v grupe G dobre definovaná pre každé prirodzené m. Nech G je grupa a x je prvok. Pre prirodzené číslo m definujeme $x^m = xx \dots x$, m-krát. Mocninu môžeme rozšíriť na celé čísla nasledovne: $x^0 = 1$ a $x^m = (x^{-m})^{-1} = x^{-1}x^{-1} \dots x^{-1}$ pre $m < 0$.*

Definícia 6 (Cayleyho tabuľka) *Ak G je grupa, potom príslušnú binárnu operáciu možno definovať Cayleyho tabuľkou rozmerov $G \times G$. Tabuľka je definovaná lineárnym usporiadaním prvkov grupy, spravidla dávame na začiatok 1. Riadky a stĺpce odpovedajú prvkom grupy. V poli so súradnicami $[a, b]$ píšeme prvok $c = ab$. Takýto spôsob zadania grupy je vhodný len pre malé konečné grupy. Navyše, tú istú grupu môžeme v závislosti od poradia definovať rôznymi tabuľkami.*

Cvičenie, Základné pojmy

Napríklad,..., nie je dôkaz!

1. Ktoré z nasledovných binárnych operácií sú uzavreté:

1. rozdiel dvoch kladných celých čísel,
2. delenie nenulových celých čísel,
3. skladanie polynómov nad $\mathbb{R}$,
4. násobenie matíc 2×2 s celočíselnými koeficientami.

2. Ktoré z nasledovných binárnych operácií sú komutatívne:

1. rozdiel dvoch kladných celých čísel,
2. delenie nenulových reálnych čísel,
3. skladanie polynómov nad $\mathbb{R}$,
4. násobenie matíc 2×2 s reálnymi koeficientami.

3. Ktoré z nasledovných množín sú uzavreté na danú operáciu?

1. $\{0, 4, 8, 12\}$ na sčitovanie modulo 16,
2. $\{0, 4, 8, 12\}$ na sčitovanie modulo 15,
3. $\{1, 4, 7, 13\}$ na násobenie modulo 15,
4. $\{1, 4, 5, 7\}$ na násobenie modulo 9.

4. Nájdite inverzný prvok k prvku a grupy G.

1. $a = 13$, $G = \mathbb{Z}_{20}$.
2. $a = 13$, $G = U(14)$,
3. $a = n - 1$, $G = U(n)$ $n > 2$,
4. $a = 3 - 2i$, $G = (\mathbb{C} - \{0\}, \cdot)$.

5. Uvažujme množinu $\mathrm{Sym}(M)$ všetkých permutácií množiny M s operáciou skladania. Dokážte, že $(\mathrm{Sym}(M), \circ)$ je grupa.

6. Nájdite inverzný prvok k matici $\begin{pmatrix} 2 & 6 \\ 3 & 5 \end{pmatrix}$ v grupe $GL(2, \mathbb{Z}_{11})$.

7. Určte všetky prvky x dihedrálnej grupy D_4 spĺňujúce rovnicu $x^2 = 1$.

8. Z grupy $U(91)$ sme odstránili dva prvky, takže ostala množina $\{1, 9, 16, 22, 53, 74, 79, 81\}$. Ktoré dva prvky chýbajú?

9. Skonštrujte Cayleyho tabuľku pre grupu $U(12)$.

10. Čiastočne definovaná binárna operácia je daná tabuľkou:

	1	a	b	c	d
1	1	-	-	-	-
a	-	b	-	-	1
b	-	c	d	1	-
c	-	d	-	a	b
d	-	-	-	-	-

Doplňte chýbajúce polia tabuľky tak, aby definovala grupu.

11. Dokážte, že množina racionálnych čísel tvaru $3^m 6^n$, kde $m, n \in \mathbb{Z}$ tvorí grupu vzhľadom na operáciu násobenia.

12. (Heisenbergerova grupa, projekt) Nech G je množina trojuhoníkových reálnych matíc rozmeru 3×3 s binárnou operáciou definovanou nasledovne:

$$\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \times \begin{pmatrix} 1 & a' & b' \\ 0 & 1 & c' \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & a + a' & b' + ac' + b \\ 0 & 1 & c' + c \\ 0 & 0 & 1 \end{pmatrix}$$

Dokážte, že uvedená množina matíc s danou operáciou tvorí grupu.

12. Koľko prvkov má grupa $GL(2, \mathbb{Z}_2)$? Je to komutatívna grupa?

2 Podgrupy

Nové grupy zo známych.

Definícia 7 (Rád grupy) *Počet prvkov grupy G sa nazýva rád grupy, označenie $|G|$. Ak G je nekonečná, položíme $|G| = \infty$.*

Definícia 8 (Rád prvku) *Nech $g \in G$ je prvok grupy. Rád prvku g, označenie $|g|$, je najmenšie kladné n také, že $a^n = 1$. Ak také n neexistuje, potom g má nekonečný rád.*

Príklad 9 *Grupa $U(15) = \{1, 2, 4, 7, 8, 11, 13, 14\}$ má rád 8. Rády prvkov sú $|7| = 4$, $|11| = 2$, $|13| = 4$. V grupe $(Z, +)$ je rád každého nenulového prvku ∞.*

Definícia 10 (Podgrupa) *Podmnožina $H \subseteq$ grupy $(G, \cdot)$ sa nazýva podgrupa, ak $(H, \cdot)$ je grupa. Zápis, $H \leq G$.*

Teoréma 11 (Test podgrupy) *Nech G je grupa a $H \subseteq G$, $H \neq \emptyset$. Potom H je podgrupou G práve vtedy, ak pre každé dva prvky $a, b \in H$ platí $ab^{-1} \in H$.*

Príklad 12 (Podgrupy abelovskej grupy)

- *Množina prvkov rádu 2 v abelovskej grupe je podgrupou.*
- *Množina prvkov konečného rádu v abelovskej grupe je podgrupou.*
- *Ak $H \leq G$ a $K \leq G$ sú podgrupy, potom množina $HK = \{hk; h \in H, k \in K\}$ je podgrupa.*

Teoréma 13 (Test podgrupy v konečnej grupe) *Konečná podmnožina $\emptyset \neq H \subseteq (G, \cdot)$ je podgrupa G práve vtedy, ak H je uzavretá na binárnu operáciu $\cdot$.*

Nech $a \in G$. Označme $\langle a \rangle = \{a^n; n \in \mathbb{Z}\}$.

Teoréma 14 *Nech G je grupa a nech $a \in G$. Potom $\langle a \rangle$ je podgrupa.*

Príklad 15 *Nech D_n je dihedrálna grupa. Nech $R \in D_n$ je rotácia o $360/n$ stupňov. Potom $\langle R \rangle$ je podgrupa rádu n.*

Je dobré si uvedomiť, že $\langle a \rangle$ je najmenšia podgrupa obsahujúca prvok a.

Definícia 16 *Nech G je grupa a $S \subseteq G$ je podmnožina. Označme $\langle S \rangle \leq G$ najmenšiu podgrupu G obsahujúcu S.*

Príklad 17 (Gaussove čísla) *Nech $\{1, i\} \subset \mathbb{C}$. Potom $\langle 1, i \rangle = \{a + bi; a, b \in \mathbb{Z}\}$ je podgrupa $(\mathbb{C}, +)$.*

Definícia 18 (Centrum grupy) *Nech G je grupa. Potom $Z(G) = \{a \in G; ax = xa$ pre každý $x \in G\}$ sa nazýva centrum grupy.*

Teoréma 19 *Nech G je grupa. Centrum grupy je abelovská podgrupa grupy G.*

Všimnime si, že $Z(G) = G$, ak G je abelovská.

Teoréma 20 *Centrum grupy je abelovská podgrupa.*

Príklad 21 *Centrum dihedrálnej grupy D_n.*

Definícia 22 *Nech $a \in G$. Centralizátor $C(a)$ prvku a je podmnožina $C(a) = \{x \in G; xa = ax\}$.*

Ak $a \in Z(G)$ potom $C(a) = G$. Platí $Z(G) \leq C(a) \leq G$.

Teoréma 23 *Centralizátor prvku $a \in G$ je podgrupa G.*

Cvičenia, Podgrupy

Cieľom dôkazu je porozumieť, nie len preveriť!

1. Pre nasledovné grupy zistite rády grúp a rády ich prvkov: $\mathbb{Z}_{12}$, $U(10)$, $U(12)$, D_4. Je nejaký vzťah medzi rádom prvku a rádom grupy.

2. Vymenujte 10 prvkov podgrupy $\langle \frac{1}{2} \rangle$ grupy Q^* (nenulové racionálne čísla s násobením).

3. Vysvetlite, prečo rády prvkov $\{2, 28\}$ a $\{8, 22\}$ v $\mathbb{Z}_{30}$ sú rovnaké; rády prvkov $\{2, 8\}$ a $\{7, 13\}$ v U_{15} sú rovnaké.

4. Nech $a, b \in G$, $|a| = 6$, $|b| = 7$. Vyjadrite prvok $(a^4c^{-2}b^4)^{-1}$ bez použitia záporných exponentov.

5. Nech $(G; +)$ je grupa polynómov s koeficiantami v $\mathbb{Z}_{10}$. Aké sú rády prvkov $f(x) = 7x^2 + 5x + 4$, $g(x) = 4x^2 + 8x + 6$, $h(x) = x^2 + 3x$. Pokúste sa vysloviť tvrdenie o ráde prvku v tejto grupe.

3 Cyklické grupy

Grupa G sa nazýva cyklická, ak existuje prvok $a \in G$, taký že platí $G = \langle a \rangle$.

Teoréma 24 (Kritérium rovnosti mocnín) *Nech $a \in G$, kde G je grupa. Potom*

- *Ak $|a| = \infty$, tak $a^i = a^j$ práve vtedy, ak $i = j$.*
- *Ak $|a| = n$, tak $a^i = a^j$ práve vtedy, ak $n|(i - j)$.*

Dôsledok 25 *Pre každý prvok a grupy $|a| = |\langle a \rangle|$.*

Dôsledok 26 *Nech a je prvok rádu n. Nech $a^k = 1$, potom $n|k$.*

Teoréma 27 *Nech a je prvok rádu n. Potom $\langle a^k \rangle = \langle a^{\gcd(n,k)} \rangle$ a $|a^k| = n/\gcd(n, k)$.*

Náčrt dôkazu: Chceme dokázať, $\langle a^d \rangle = \langle a^k \rangle$. Pretože $d|k$, $\langle a^d \rangle \geq \langle a^k \rangle$. $d = \gcd(n, k) = ns + kt$. $a^d = a^{ns+kt} = (a^k)^t \in \langle a^k \rangle$ Teda aj $\langle a^d \rangle \leq \langle a^k \rangle$.
Rády. $(a^d)^{n/d}$, preto $|a^d||\frac{n}{d}$.
Na druhej strane, $a^{di} = 1$, potom $a^k i = 1$. Teda $i|n/k$ a aj $i|n/d$.

Dôsledok 28 *Ak G je konečná cyklická grupa, potom rád prvku delí rád G.*

Dôsledok 29 *Nech $|a| = n$. Potom $\langle a^i \rangle = \langle a^j \rangle$ práve vtedy, keď $\gcd(n, i) = \gcd(n, j)$ a $|a^i| = |a^j|$ práve vtedy, ak $\gcd(n, i) = \gcd(n, j)$.*

Dôsledok 30 *Nech G je cyklická grupa rádu n, nech $|a| = k$. Potom $\langle a \rangle = G$ práve vtedy, keď $\gcd(k, n) = 1$.*

Teoréma 31 *Každá podgrupa cyklickej grupy G je cyklická. Navyše, ak $|G| = n$, potom pre každé k, $k|n$, G má práve jednu podgrupu rádu k.*

Dôkaz. Ak $H \leq G = \langle a \rangle$, potom $H = \{1\}$ a je cyklická. Ak H je netriviálna, tak obsahuje nejakú mocninu a^t. Nech t je minimálny kladný exponent, $a^t \in H$. Potom $H = \langle a^t \rangle$. Triviálne $H \geq \langle a^t \rangle$. Ak $a^m \in H$, pre $m > t$, potom $m = qt + r$, kde $r < t$. Preto $r = 0$ a $a^m = a^{qt} \in \langle a^t \rangle$.

Jednoznačnosť. Nech $k|n$ a nech podľa predošlej časti existuje m také, že $H = \langle a^m \rangle$. Podľa Teorémy 27 H možno vygenerovať prvkom $a^{\gcd(m,n)}$. Potom pre zvolený deliteľ k platí, $k = |H| = |\langle a^m \rangle| = |\langle a^{\gcd(m,n)} \rangle| = n/\gcd(n,m) = n/m$. Preto $m = n/k$ a teda podgrupa je jednoznačne určená.

Poznámka. Všimnime si, že existuje jednoznačná korešpondencia medzi podgrupami cyklickej grupy G a deliteľmi $n = |G|$. Táto bijekcia definuje izomorfizmus medzi zväzom deliteľov n a zväzom podgrúp G. Pre dané podgrupy $H_1, H_2 \leq G$ sú tvoria infimum a supremum podgrupy $H_1 \cap H_2$ a $\langle H_1, H_2 \rangle$.

Ďalšia vec hodná povšimnutia je úloha elementárnej aritmetiky v tvrdeniach o cyklických grupách (Delenie so zvyškom a Euklidov algoritmus).

Cvičenia, Cyklické grupy

Dávajte si pozor, aby ste v argumentácii nepoužili to, čo sa snažíte zdôvodniť!

1. Vymenujte generátory $\mathbb{Z}_6$, $\mathbb{Z}_8$, $\mathbb{Z}_{20}$.

2. Vymenujte prvky $\langle 3 \rangle$, $\langle 7 \rangle$ v $U(20)$.

3. Vypočítajte $\langle 21 \rangle \cap \langle 10 \rangle$ v grupe $\mathbb{Z}_{24}$.

4. Nech $G = \langle a \rangle$ je rádu n. Nájdite generátor $H = \langle a^{21} \rangle \cap \langle a^{10} \rangle$. Aký je rád H.

5. Nech G je cyklická grupa rádu n s práve jednou vlastnou podgrupou H. Čo viete povedať o rádeoch G a H?

6. Nech G je abelovská grupa. Označme $H = \{g \in G |\ |g| \text{ delí } 12\}$. Dokážte, že H je grupa. Možno 12 nahradiť iným číslom. Pokúste sa sformulovať všeobecné tvrdenie.

7. Nájdite maximálny reťazec podgrúp $H_1 < H_2 < \ldots H_m$ v cyklickej grupe $\mathbb{Z}_{240}$. Pokúste sa sformulovať všeobecné tvrdenie pre cyklickú grupu rádu n.

8. Opíšte podgrupy $(Z, +)$.

9. Koľko prvkov rádu d pre $d|n$ má dihedrálna grupa D_n? Spočítajte prvky dihedrálnej grupy D_n. Použite Eulerovu funkciu $\varphi(d)$.

10. Aké sú možnosti pre rád prvku $\alpha\beta$ v dihedrálnej grupe D_{21}, ak vieme, že $|\alpha| = |\beta| = 2$.

4 Permutačné grupy

Definícia 32 *Permutácia množiny A je bijekcia $A \to A$. Množina všetkých permutácií A s operáciou skladania tvorí symetrickú grupu* $\mathrm{Sym}(A)$. *Podgrupa $G \leq \mathrm{Sym}(A)$ sa nazýva permutačná grupa. Ak $A = \{1, 2, \ldots, n\}$, potom* $\mathrm{Sym}(A)$ *označujeme S_n.*

Permutáciu $\alpha \in S_n$ môžeme zapoisovať do tabuľky $2 \times n$, kde prvý riadok obsahuje postupnosť $1, 2, 3, \ldots, n$ a druhý postupnosť hodnôt $\alpha(1), \alpha(2), \alpha(3), \ldots, \alpha(n)$.

V skutočnosti prvý riadok nepotrebujeme, úplnú informáciu obsahuje druhý riadok. Prvý riadok sa však hodí pri určovaní inverznej permutácie ku α, vysvetlite!.

Permutácie môžeme skladať zľava do prava, alebo z prava do ľava. Myslíme tým interpretáciu zápisu $\gamma = \alpha \cdot \beta$. Môžeme pre $x \in A$ môžeme položiť $\gamma(x) = \alpha(\beta(x))$, alebo $\gamma(x) = \beta(\alpha(x))$, oba spôsoby sa v literatúre vyskytujú. Dôležité je v tom istom výpočte ich nemiešať!

Matematici častejšie používajú na zápis permutácie takzvaný cyklový tvar.

Definícia 33 *Orbita $[x]_\alpha$ prvku x v permutácii $\alpha \in \mathrm{Sym}(A)$ je množina $\{\alpha^n(x) \mid n \in Z\}$. Permutácia α množiny A sa nazýva cyklická, ak všetky prvky množiny A patria do jedinej orbity.*

Cyklickú permutáciu α z S_n zapisujeme v cyklickej notácii:

$$\alpha = (x, \alpha(x), \alpha^2(x), \ldots, \alpha^{n-1}(x)),$$

pre $x \in A$.

Napríklad, ak $n = 4$, tak zápis $\alpha = (1, 3, 2, 4)$ znamená: $\alpha(1) = 3$, $\alpha(2) = 4$, $\alpha(3) = 2$ a $\alpha(4) = 1$. Cyklický zápis nie je jednoznačný, napríklad $\alpha = (3, 2, 4, 1)$ definuje tú istú permutáciu. Ak chceme jednoznačnosť, musíme definovať nejaké lineárne usporiadanie na A a potom v cyklovom zápise zapísať na prvom mieste minimálneho reprezentanta orbity.

Ak $|A| = n$, tak $|\mathrm{Sym}(A)| = n!$. Počet všetkých cyklických permutácií A je $(n-1)!$, prečo?. Cyklické permutácie netvoria grupu, skúste si napríklad zložiť $(123) \cdot (132)$. Všetky orbity permutácie α tvoria rozklad množiny A. Pre každú orbitu $O \subseteq A$ môžeme napísať cyklickú permutáciu definovanú permutáciou α. Dokázali sme tak nasledovné tvrdenie.

Teoréma 34 *Každú permutáciu konečnej množiny možno zapísať ako súčin disjunktných cyklických permutácií. Toto vyjadrenie je jednoznačné až na poradie.*

Poznámka. Predošlá veta platí aj pre permutácie nekonečných množín, ale jej dôkaz vyžaduje použitie axiomy výberu.

Cyklový zápis permutácie je výhodný pre určenie rádu permutácie. Platí totiž nasledovné tvrdenie. V cyklovom zápise často vynechávame cykly dĺžky 1.

Teoréma 35 (Ruffiny 1799) *Ak α vyjadrená v cyklovom tvare je súčinom k cyklov s dĺžkami m_i, $i = 1, \ldots, k$, potom $|\alpha| = \mathrm{lcm}(m_1, \ldots, m_k)$.*

Transpozícia je permutácia, v ktorej cyklovom zápise sú všetky cykly dĺžky najviac dva, pričom obsahuje jediný cyklus dĺžky 2.

Teoréma 36 *Každú permutáciu konečnej konečnej množiny možno vyjadriť ako súčin transpozícií.*

Dôkaz. Každú cyklickú permutáciu v rozklade na disjuktné cykly vieme rozložiť na súčin traspozícií. Napríklad

$$(1, 2, 3, \ldots, n) = (n-1, n)(n-2, n) \ldots (1, n).$$

Rozklad permutácie na súčin transpozícií nie je jednoznačný. Vymyslite príklad! Po vyskúšaní niekoľkých príkladov si všimneme, parita počtu transpozícií v

rozklade permutácie je vždy rovnaká (v každom rozklade α je počet vždy párny (sudý), alebo vždy nepárny (lichý). Navyše, parita je rovná $n-k \pmod 2$, kde k je počet cyklov v rozklade α.

Definícia 37 *Nech $\alpha = \beta_1 \dots \beta_k$, je rozklad permutácie n prvkovej množiny na k disjunktných cyklov. Označme* $\mathrm{sgn}(\alpha) = (-1)^{\mathrm{n-k}}$ *funkciu* $S_n \to \{\pm 1\}$.

Všimnime si, že ak τ je transpozícia, tak $\mathrm{sgn}(\tau) = -1$.

Lema 38 *Nech $\tau\beta \in S_n$ a nech τ je transpozícia. Potom* $\mathrm{sgn}(\tau \cdot \beta) = -\mathrm{sgn}(\beta)$.

Návod na dôkaz. Nech $\tau = (i, j)$. Uvažujte dva prípady: i, j je v tej istej orbite α, i a j sa nachádzajú v rôznych orbitách.

Teoréma 39 *Pre ľubovoľné dve permutácie $\alpha, \beta \in S_n$ platí* $\mathrm{sgn}(\alpha\beta) = \mathrm{sgn}(\alpha)\mathrm{sgn}(\beta)$.

Indukciou podľa počtu transpozícií v minimálnom rozklade α na súčin transpozícií. Použite predošlú lemu.

Teoréma 40 *Nech α je permutácia. Potom nasledovné výroky sú ekvivalentné:*

- $\mathrm{sgn}(\alpha) = 1$,
- *α možno vyjadriť ako súčin párneho počtu transpozícií,*
- *v každom rozklade α na súčin transpozícií je počet transpozícií párny.*

Definícia 41 *Permutácia α konečnej množiny je párna, ak* $\mathrm{sgn}(\alpha) = 1$. *Permutácia je nepárna, ak nie je párna.*

Propozícia 42 *Párne permutácie v S_n tvoria podgrupu $A_n \leq S_n$. Grupa A_n má rád $n!/2$.*

Definícia 43 *Grupa A_n párnych permutácií sa nazýva alternujúca grupa.*

Príklad 44 *Rotačná grupa tetraedra s vrcholmi $\{1, 2, 3, 4\}$ je A_4.*

Príklad 45 *Príklad 2. Grupa Rubikovej kocky. (projekt)*

Cvičenia

1. Dané sú permutácie

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 3 & 4 & 5 & 1 & 7 & 8 & 6 \end{pmatrix}$$

$$\beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 3 & 8 & 7 & 6 & 5 & 2 & 4 \end{pmatrix}$$

Vypočítajte α^{-1}, β^{-1}, $\alpha\beta$, $\beta\alpha$.

2. Permutácie z úlohy č.1 α, β, α^{-1}, β^{-1}, $\alpha\beta$, $\beta\alpha$ vyjadrite v cyklovom tvare.

3. Permutácie z úlohy č.1 α, β, α^{-1}, β^{-1}, $\alpha\beta$, $\beta\alpha$ vyjadrite ako súčin transpozícií. Určte, ktoré z nich sú párne a ktoré nepárne.

4. Aký je rád cyklickej permutácie $(a_1, a_2, \ldots, a_k)$. Určte rády permutácií $(124)(3567)$, $(124)(357869)$.

5. Určte rády permutácií α, β a $\alpha\beta$ z úlohy č.1. Viete určiť rády α^{-1}, β^{-1} a $(\alpha\beta)^{-1}$ bez prevodu na cyklový tvar?

6. Nájdite všetky prvky S_6, ktoré komutujú s permutáciou $(12)(34)(56)$. Tvoria tieto prvky grupu?

7. (projekt) Nech H je podgrupa S_n. Potom buď $H \leq A_n$, alebo presne polovica prvkov H je párnych.

8. (projekt) Dokážte, že ak H je podgrupa S_n nepárneho rádu symetrickej grupy S_n, potom H je podgrupa A_n.

9. Nájdite najmenšie n také, že S_n obsdahuje prvok rádu $> 2n$.

10. Nájdite najmenšie n také, že A_n obsdahuje prvok rádu $> n$.

5 Homomorfizmy, izomorfizmy a automorfizmy grúp

Definícia 46 *Nech $(G, \cdot)$ a $(H, *)$ sú grupy. Zobrazenie $\psi : G \to H$ je homomorfizmus, ak pre každé $a, b \in G$ platí $\psi(x \cdot y) = \psi(x) * \psi(y)$. Ak f je bijekciou, potom f sa nazýva izomorfizmus. Grupy G a H nazývame izomorfné, značíme $G \cong H$, ak existuje izomorfizmus $G \to H$. Izomorfizmus $G \to G$ je automorfizmus.*

Automorfizmy grupy G s operáciou skladania tvoria podgrupu $\mathrm{Sym}(G)$, ktorú označujeme $\mathrm{Aut}(G)$.

Homomorfizmy definované na cyklickej grupe $G = \langle a \rangle$ sú jednoznačne určené obrazom $f(a)$ generátora a. Ak G je nekonečná, potom je izomorfná $(Z, +)$. Každá konečná cyklická grupa rádu n je izomorfná $(Z_n, +)$. Podobne ako pri lineárnych zobrazeniach vektorových priestorov, homomorfizmy grúp sú definované obrazmi generátorov. Vzťahy medzi generátormi však môžu byť zložité, preto náhodne zvolené obrazy generátorov zvyčajne nedefinujú homomorfizmus.

Ak G je grupa, potom každý prvok $g \in G$ definuje (vnútorný) automorfizmus φ_g grupy g daný predpisom $\varphi_g(x) = g^{-1}xg$. Priradenie $\Phi : g \mapsto \varphi_g$ je homomorfizmus $G \to \mathrm{Aut}(G)$. Zloženie vnútorných automorfizmov je znovu vnútorný automorfizmus (overte!), tiež $(\varphi_g)^{-1} = \varphi_{g^{-1}}$, preto vnútorné automorfizmy tvoria podgrupu $\mathrm{Inn}(G) \leq \mathrm{Aut}(G)$. Ľahko vidieť, že ak G je abelovská, tak $Inn(G)$ je triviálna. Otázka kedy platí $\mathrm{Aut}(G) = \mathrm{Inn}(G)$ je veľmi zaujímavá. Rovnosť platí napríklad pre symetrické grupy S_n, pre $n \geq 7$. S vnútornými automorfizmami ste sa mohli stretnúť v lineárnej algebre, kde hrá dôležitú úlohu relácia podobnosti. Dve regulárne matice $A, B \in GL(n, F)$ sú podobné, ak existuje matica $T \in GL(n, F)$ taká, že platí $B = T^{-1}AT$. Inými slovami, existuje vnútorný automorfizmus v $\mathrm{Inn}(GL(n, F))$ daný T, ktorý zobrazuje A na B.

V základnej škole ste sa naučili používať distributívny zákon: $c(a+b) = ca + cb$. Distributívny zákon znamená, že pre číselné aditívne grupy $(Z, +)$, $(Q, +)$, $(R, +)$, $(C, +)$, $(Z_n, +)$ je funkcia $f(x) = cx$, pre každé c homomorfizmom. Kedy je tento homomorfizmom automorfizmom? Nie je ťažké zistiť, že $f(x) = cx$ je automorfizmom $(Z_n, +)$, vtedy a len vtedy, ak n a c sú nesúdeliteľné. Zloženie

$f(x)$ a $g(x) = dx$ je automorfizmus $x \mapsto cdx$. Odtiaľ sme už blízko poznaniu, že $\mathrm{Aut}(Z_n) \cong U(n)$.

Teóriu grúp možno vybudovať bez práce s konkrétnymi príkladmi. Takáto teória by však bola ťažko pochopiteľná. Nasledujúca veta ukazuje, že každú grupu možno reprezentovať ako permutačnú grupu.

Teoréma 47 (Cayleho veta.) *Každá grupa je izomorfná nejakej permutačnej grupe.*

Návod na dôkaz. Pre každý prvok $g \in G$ grupy G, definujme permutáciu $T_g(x)$ prvkov grupy G predpisom $T_g(x) = gx$. Treba overiť nasledovné fakty:

- $T_g \in \mathrm{Sym}(G)$
- permutácie T_g, $g \in G$, s operáciou skladania tvoria grupu,
- zobrazenie $\Phi : g \mapsto T_g$ je monomorfizmus $G \to Sym(G)$.

Nasledovná teoréma sumarizuje vybrané vlastnosti (invarianty) izomorfizmov.

Teoréma 48 *Nech $\Phi : G \to H$ je izomorfizmus. Potom*

- $\Phi(1_G) = 1_H$,
- $\Phi(a^n) = (\Phi(a))^n$, *pre každé* $n \in Z$,
- $a, b \in G$ *komutujú práve vtedy, ak* $\Phi(a)$, $\Phi(b)$ *komutujú,*
- G *je cyklická (abelovská), práve vtedy ak* H *je cyklická (abelovská),*
- *ak* G *je konečná, potom počty prvkov daného rádu sú rovnaké v* G *aj v* H.

Cvičenia

1. Označme $kZ = \{kx \in Z \mid x \in Z\}$, množinu násobkov celého čísla k. Dokážte, že $kZ \leq (Z, +)$ je grupa izomorfná $(Z, +)$.

2. Dokážte, že $U(8) \cong U(12)$, ale $U(8)$ nie je izomorfná $U(10)$.

3 Dokážte, že $a \mapsto \ln(a)$ je izomorfizmus $(R^+, \cdot) \to (R, +)$.

4 Nájdite najmenší príklad cyklickej grupy obsahujúcej podgrupy izomorfné Z_{12}, Z_{20}.

5 Dokážte, že zobrazenie $x \mapsto x^3$ je automorfizmus $U(16)$. Ako je to so zobrazeniami $x \mapsto x^5$, $x \mapsto x^7$?

6 Nech G je konečná abelovská grupa bez prvkov rádu 2. Dokážte, že $\psi : x \mapsto x^2$ je automorfizmus. Nájdite príklad nekonečnej abelovskej grupy, kde ψ je bijektívne a nie je automorfizmom.

7 Grupy $(Q, +)$ a $(R^+, \cdot)$ nie sú izomorfné, lebo R^+ ne nespočítateľná a Q je spočítateľná. Nájdite grupovo teoretický argument dokazujúci neizomorfnosť.

8 Určte podgrupu S_8, ktorá je izomorfná D_4.