Abstraktní algebra

Úvodní kurz

Roman Nedela

Abstraktní algebra

Úvodní kurz

Roman Nedela

Západočeská univerzita v Plzni
Česká republika

Kniha byla napsána použitím typografického systému LaTeX.

Obsah

Kapitola 1

Permutace

Definice 1.1. Permutace množiny M je bijekce $M \to M$. Množinu všech permutací množiny $M = \{1, 2, \ldots, n\}$ označíme S_n. Pro obecnou množinu M ji označíme S_M. Množina S_n je pro velké n velmi velká, počet jejích prvků je $n! = 1 \cdot 2 \cdot 3 \cdot \cdots \cdot (n-1) \cdot n$.

Operace složení. Složení dvou permutací α, β množiny M je permutace množiny M. Složení zapisujeme $\alpha \circ \beta(i) = \alpha(\beta(i))$. Permutaci zapíšeme do tabulky:

$$\alpha = \begin{pmatrix} 1 & 2 & \ldots & n \\ \alpha(1) & \alpha(2) & \ldots & \alpha(n) \end{pmatrix}.$$

Všimněme si, že skládání permutací není pro $n \geq 3$ komutativní. To znamená, že pro každé $n \geq 3$ existují permutace takové, že $\alpha \cdot \beta \neq \beta \cdot \alpha$. Například pokud

$$\alpha = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \beta = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix},$$

potom

$$\beta \circ \alpha = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \neq \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \alpha \circ \beta.$$

Cyklový zápis permutace. Je-li $\alpha(k) = k$, říkáme, že permutace α *fixuje* prvek k. Nechť $M = \{i_0, i_1, \ldots, i_{r-1}\} \subseteq \{1, 2, \ldots, n\}$ je r-prvková podmnožina, $r > 1$. Nechť $\alpha \in S_n$ je permutace taková, že $\alpha(i_j) = i_{j+1}$, $j = 0, 1, \ldots, r-1$ a $\alpha(k) = k$ pro $k \in \{1, 2, \ldots, n\} \setminus M$. Potom permutaci α nazveme *cyklus* délky r a budeme ji zapisovat $\alpha = (i_0, i_1, \ldots, i_{r-1})$. Všimněme si, že zápis $\alpha = (i_1, i_2, \ldots, i_{r-1}, i_0)$ definuje stejnou permutaci. Číslo r nazveme délka cyklu; cyklus délky 2 se nazývá *transpozice*. Dva cykly α, β se nazývají *disjunktní*, pokud množiny prvků, které nejsou fixované těmito permutacemi, jsou disjunktní.

Pro permutaci α označíme α^m permutaci $\underbrace{\alpha \circ \alpha \circ \cdots \circ \alpha}_{m}$.

Věta 1.2. *Každou permutaci různou od identity můžeme rozložit na součin disjunktních cyklů. Navíc, tento rozklad je až na pořadí cyklů jednoznačný.*

Důkaz. Pokud je $j \in \{1, 2, \ldots, n\}$, označme $O(j) = \{k \in M : \exists m, k = \phi^m(j)\}$. Zřejmě množiny $O(j)$ tvoří rozklad M. Dále postupujeme indukcí podle počtu množin $O(j)$. Pokud existuje $i \in M$, které ještě není pokryté, vytvoříme cyklus $(i, \phi(i), \phi^2(i), \ldots, \phi^{m-1}(i))$, přičemž m je nejmenší číslo takové, že $\phi^m(i) = i$. □

Množinu $O(i) = \{i, \alpha(i), \alpha^2(i), \ldots\}$ budeme nazývat orbita prvku i.

Definice 1.3. Úplná faktorizace permutace je rozklad permutace na disjuktní cykly, kde za každý fixovaný bod doplníme cyklus délky 1.

Uvažujme součin transpozic

$$(1,2)\ldots(1,r-1)(1,r) = (1,r,r-1,r-2,\ldots,2).$$

Toto pozorovaní můžeme lehce zobecnit na libovolný cyklus. V kombinaci s větou 1.2 lze dokázat následující větu.

Věta 1.4. *Každou permutaci různou od identity můžeme rozložit na součin transpozic.*

Tento rozklad však už nebude v rozumném smyslu jednoznačný. Porovnáním různých rozkladů té samé permutace však zjistíme, že parita počtu transpozic v rozkladech zůstává nezměněná. Důvod je skrytý v efektu složení transpozic (a, b) s libovolnou permutací.

Definice 1.5. Nechť $\alpha = \beta_1\beta_2\ldots\beta_t$ je úplný rozklad permutace $\alpha \in S_n$. Označme $\operatorname{sgn}(\alpha) = (-1)^{n-t}$.

Lemma 1.6. *Pokud $\beta \in S_n$ a τ je transpozice, platí*

$$\operatorname{sgn}(\tau\beta) = -\operatorname{sgn}(\beta).$$

Důkaz. Uvažujme rozklad $\beta = \gamma_1\gamma_2\ldots\gamma_t$ na disjunktní cykly. Nechť $\tau = (m, k)$, kde $m \in \gamma_i$ a $k \in \gamma_j$. V důkazu rozlišíme dva případy: $i = j$ a $i \neq j$. Pokud $i = j$, počet disjunktních cyklů je v rozkladě $\tau\beta$ rovný $t + 1$; pokud $i \neq j$, příslušný počet cyklů je $t - 1$. (Dokažte podrobně!) □

Věta 1.7. *Pro každé $\alpha, \beta \in S_n$ platí*

$$\operatorname{sgn}(\alpha\beta) = \operatorname{sgn}(\alpha)\operatorname{sgn}(\beta).$$

Důkaz. Nechť $\alpha = \tau_1\tau_2\ldots\tau_m$ je rozklad na součin transpozic, kde m je minimální. Použijeme indukci podle m. Je-li $m = 1$, použijeme Lemma 1.6. Je-li $m > 1$, označíme $\alpha' = \tau_2\ldots\tau_m$. Pak z předchozího lemmatu dostáváme:

$$\operatorname{sgn}(\alpha\beta) = -\operatorname{sgn}(\alpha'\beta) = -\operatorname{sgn}(\alpha')\operatorname{sgn}(\beta) = \operatorname{sgn}(\tau_1\alpha')\operatorname{sgn}(\beta) = \operatorname{sgn}(\alpha)\operatorname{sgn}(\beta).$$

Pokud $\alpha' = \tau_2\ldots\tau_m$ je minimální rozklad, tvrzení platí. Proč α' musí být minimální rozklad? □

Definice 1.8. Permutace se nazývá sudá, pokud se dá rozložit na sudý počet transpozic. Pokud permutace není sudá, je lichá.

Věta 1.9. *Permutace $\alpha \in S_n$ je sudá právě tehdy, když* $\operatorname{sgn}(\alpha) = 1$.

Cvičení

1.1. Nechť $\alpha(i) = 10 - i$ je permutace v S_9. Zapište α jako součin disjunktních cyklů.

1.2. Kolik je permutací α v S_6 takových, že $\alpha^2 = 1$? Zkuste tvrzení zobecnit pro S_n.

1.3. Pro které r je r-cyklus sudá permutace?

1.4. Určete $\operatorname{sgn}(\alpha)$ pro

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 9 & 8 & 7 & 6 & 5 & 4 & 3 & 2 & 1 \end{pmatrix}.$$

1.5. Máme dánu množinu S_n, kde $n \geq 3$. Kolik fixovaných prvků k může existovat v nějaké permutaci v S_n? Jak vypadá inverzní permutace k permutaci α, v níž je fixováno právě $n - 2$ prvků?

1.6. V pytlíku je každá permutace v S_3 napsaná právě na jednom lístečku. Jaká je pravděpodobnost, že vytáhneme najednou dva lístečky s permutacemi α a β, pro něž platí $\alpha \cdot \beta = \beta \cdot \alpha$? Jak se pravděpodobnost změní, vytáhneme-li nejprve první lístek, který následně vrátíme zpět do pytlíku, a teprve poté vytáhneme druhý lístek?

1.7. Nechť jsou dány permutace

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 4 & 7 & 3 & 2 & 10 & 9 & 1 & 5 & 6 & 8 \end{pmatrix},$$

$$\beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 1 & 4 & 3 & 6 & 9 & 8 & 5 & 10 & 7 & 2 \end{pmatrix}.$$

Najděte cykly, znaménka a inverze obou permutací. Zjistěte, zda platí $\alpha \cdot \beta = \beta \cdot \alpha$.

1.8. Nechť je dána permutace $\alpha = (1, 2, 5, 6)(3, 4)(7, 10, 9)(8)$.
Určete nejmenší mocninu $k \geq 1$, pro níž dostaneme $\alpha^k = id$?
Určete α^{-14}, α^9, α^{-12} a α^7.

1.9. Jak vypadá permutace α v S_n, pro níž $\alpha^2 = id$? A jak vypadá permutace β v S_n, pro níž $\beta^{n-1} = id$?

1.10. Nechť $\alpha, \beta, \gamma, \delta$ jsou permutace v S_n a platí $\alpha \cdot \beta = \beta \cdot \alpha$ i $\gamma \cdot \delta = \delta \cdot \gamma$. Platí pak nutně, že $\alpha \cdot \gamma = \gamma \cdot \alpha$ nebo $\alpha \cdot \delta = \delta \cdot \alpha$? Pokud ano, dokažte. Pokud ne, najděte příklad, kdy věta neplatí.

1.11. Identická funkce 1_X na množině X je permutace, kterou obvykle značíme 1 (nebo id). Dokažte, že $1 \cdot \alpha = \alpha = \alpha \cdot 1$ pro každou permutaci $\alpha \in S_X$.

1.12. Pro každou permutaci $\alpha \in S_X$ existuje permutace $\beta \in S_X$ taková, že $\alpha\beta = 1 = \beta\alpha$. Dokažte.

1.13. Pro všechny permutace $\alpha, \beta, \gamma \in S_X$ dokažte, že $\alpha(\beta\gamma) = (\alpha\beta)\gamma$.

1.14. Nechť $1 \leq r \leq n$. Kolik existuje r-cyklů v S_n?

1.15. Nechť α, β, γ jsou permutace. Dokažte, že pokud $\alpha\beta = \alpha\gamma$ nebo $\beta\alpha = \gamma\alpha$, pak $\beta = \gamma$.

1.16. Nechť $\alpha = (i_1 i_2 \cdots i_r)$ a $\beta = (j_1 j_2 \cdots j_s)$. Dokažte, že α a β jsou disjunktní permutace právě tehdy, když $\{i_1, i_2, \ldots, i_r\} \cap \{j_1, j_2, \ldots, j_s\} = \emptyset$.

1.17. Nechť α a β jsou disjunktní permutace. Dokažte, že potom $\alpha\beta = \beta\alpha$.

1.18. Pokud α a β jsou disjunktní permutace a $\alpha\beta = 1$, platí, že $\alpha = 1 = \beta$. Dokažte.

1.19. Najděte permutace $\alpha, \beta, \gamma \in S_5$ takové, že α komutuje s β, β komutuje s γ, ale α nekomutuje s γ.

1.20. Nechť α, β jsou permutace v S_n. Pokud α i β mají stejnou paritu, je $\operatorname{sgn}(\alpha\beta) = 1$, pokud α a β mají rozdílnou paritu, je $\operatorname{sgn}(\alpha\beta) = -1$. Dokažte.

1.21. Zapište následující permutace jako součin disjunktních cyklů:

- $(1,2,3,5)(4,1,3)$,
- $(1,3,2,5,6)(2,3)(4,6,5,1,2)$,
- $(1,2)(1,3)(2,3)(1,4,2)$.

Následně permutace zapište tabulkou.

1.22. Nechť jsou dány dvě permutace $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 3 & 4 & 5 & 1 & 7 & 8 & 6 \end{pmatrix}$ a $\beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 3 & 8 & 7 & 6 & 5 & 2 & 4 \end{pmatrix}$. Zapište $\alpha\beta$ jako součin disjunktních cyklů a poté jako součin dvou cyklů. Totéž proveďte pro $\beta\alpha$.

1.23. Nechť α a β jsou permutace v S_n. Dokažte, že $\alpha^{-1}\beta^{-1}\alpha\beta$ je sudá permutace.

1.24. Najděte tři permutace α z S_9 takové, že $\alpha^3 = (1,5,7)(2,8,3)(4,6,9)$.

1.25. Nechť je dána permutace $\beta = (1,3,5,7,9,8,6)(2,4,10)$. Jaké je nejmenší přirozené číslo n takové, že $\beta^n = \beta^{-5}$?

1.26. Nechť je dána permutace $\gamma = (1,3,5,7,9)(2,4,6)(8,10)$. Pokud γ^m je 5-cyklus, co můžete říci o m?

1.27. Nechť o permutaci β víme následující: $\beta \in S_7$ a $\beta^4 = (2,1,4,3,5,6,7)$. Určete permutaci β.

1.28. Nechť $\beta = (1,2,3)(1,4,5)$. Zapište β^{99} jako součin disjunktních cyklů.

Následující příklady vyřešte po nastudování úvodních čtyř kapitol.

1.29. Určete řád následujících permutací:

- $(1,2,4)(3,5,7)$,
- $(1,2,4)(3,5,7,8,6,9)$,
- $(3,4,5)(2,4,5)$.

1.30. Ukažte, že v grupě A_8 existuje prvek řádu 15.

1.31. Jaké jsou možné řády prvků grup S_6 a A_6. Jak je to u grupy A_7?

1.32. Uveďte dva důvody, pro množina lichých permutací v S_n není podgrupa grupy S_n.

1.33. Kolik prvků řádu 5 obsahuje grupa S_7? Kolik prvků řádu 4 obsahuje grupa S_6?

1.34. V grupě S_4 najděte jednu cyklickou a jednu necyklickou podgrupu řádu 4.

1.35. Předpokládejme, že permutace δ je 10-cyklus. Pro jaké přirozené číslo $i = \{2, 3, \ldots, 10\}$ je δ^i rovněž 10-cyklus?

1.36. Najděte jednu cyklickou a jednu necyklickou podgrupu grupy A_8, jež má řád 4.

1.37. Nechť H je podgrupa grupy S_n lichého řádu. Dokažte, že H je podgrupa grupy A_n.

1.38. Ukažte, že pro všechna $n \geq 3$ je $Z(S_n) = \{id\}$.

Nápověda k vybraným cvičením

1.4 Zapište permutaci α jako součin cyklů a použijte vzorec $\mathrm{sgn}(\alpha) = (-1)^{n-t}$, kde $n = 9$ a t je počet cyklů.

1.5 Evidentně $0 \leq k \leq n$. Pokud $k = 0$, neexistuje žádný fixovaný prvek, pokud $k = n$, dostáváme identitu. Jak vypadá permutace s právě $n-1$ fixovanými prvky? Protože $\alpha \cdot \alpha^{-1} = id$, musí stejných $n-2$ prvků být fixních i v α^{-1}. Budete platit $\alpha^{-1} = \alpha$, nebo $\alpha^{-1} = id$?

1.6 Celkem existuje $3! = 6$ různých permutací v S_3. Vytahujeme-li z pytlíku dva lístečky s permutacemi, máme celkem $\binom{6}{2} = 15$ možností. Prověřte, pro kolik z 15 variant platí $\alpha \cdot \beta = id$. Vrátíme-li lísteček zpět do pytlíku, zvětší se počet možností, konkrétně o 6 (můžeme vytáhnout stejný lísteček).

1.7 Jeden cyklus permutace α je například $(1, 4, 2, 7)$. Po převedení do součinu cyklů pro zjištění znaménka permutace použijte vzorec $\mathrm{sgn}(\alpha) = -1^{n-t}$, kde $n = 10$ a t je počet cyklů. Pro zjištění inverzních permutací stačí například v obou permutacích v tabulkové podobě prohodit řádky a pak setřídit sloupce od nejmenšího.

1.8 První cyklus má délku 4, každý prvek bude tedy nazpět na svém místě po každých čtyřech iteracích. Například pro α^{-14} spočítejme nejprve $\alpha^{14} = \alpha^8 \cdot \alpha^4 \cdot \alpha^2$ a následně proveďte inverzi.

1.9 Podobně jako v příkladu 1.2. Pokud $n-1$ je nejmenší mocnina taková, že $\beta^{n-1} = id$, musí v permutaci β existovat cyklus délky $n-1$, a tedy právě jeden fixovaný prvek. Diskutujte možnost, že $n-1$ není nejmenší mocnina.

1.10 Nechť α, β, γ a δ jsou permutace v S_3. Dále nechť $\beta = id$ a $\gamma = \delta \neq id$ (tzn., že existuje právě jeden fixní prvek). Nalezněte α a γ a přesvědčete se, že daná věta neplatí.

1.12 Položme $\beta = \alpha^{-1}$.

1.13 Připomeňme, že dvě funkce $f, g : A \to B$ jsou stejné právě tehdy, když pro všechna $a \in A$ platí $f(a) = g(a)$.

Řešení vybraných cvičení

1.1 Permutace α vypadá následovně:

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 9 & 8 & 7 & 6 & 5 & 4 & 3 & 2 & 1 \end{pmatrix}.$$

Vyskytuje se zde 5 cyklů, konkrétně čtyři transpozice $\tau_1 = (1,9), \tau_2 = (2,8), \tau_3 = (3,7)$ a $\tau_4 = (4,6)$ a jeden fixní prvek (5). Proto $\alpha = (1,9)(2,8)(3,7)(4,6)(5)$.

1.2 Aby $\alpha^2 = 1$, nesmí existovat v α žádný trojcyklus, čtyřcyklus, pěticyklus a ani šesticyklus. Permutaci α můžeme tedy vyjádřit jako součin transpozic a fixních prvků. Fixní prvek nemusí existovat nebo jich počet musí být sudý. Tzn. buď je $\alpha = 1$, nebo lze α vyjádřit jako součin jedné transpozice a čtyř fixních prvků, dvou transpozic a dvou fixních prvků, a nebo jako součin tří transpozic.

0 transpozic: To je identita, tedy 1 možnost.

1 transpozice: Máme tedy čtyři fixní prvky, transpozice je tedy po zafixování těchto čtyř prvků dána jednoznačně. Tedy $\binom{6}{4} = \binom{6}{2} = \frac{6\cdot5}{2\cdot1} = 15$ možností.

2 transpozice: Máme tedy dva fixní prvky: $\binom{6}{2} = 15$ možností; čtyři prvky musíme po dvou prohodit, to jsou 3 možnosti. Tedy celkem $15 \cdot 3 = 45$ možností.

3 transpozice: Prvek 1 lze prohodit s pěti prvky. Dále vezmeme dosud neprohozený prvek. Ten může být prohozen s třemi zbývajícími prvky. Poslední prohození je již dáno dvěma zbývajícími dosud neprohozenými prvky. Celkem: $5 \cdot 3 \cdot 1 = 15$ možností.

Celkem tedy v S_6 existuje $1 + 15 + 45 + 15 = 76$ permutací α takových, že $\alpha^2 = 1$.

V S_n existuje $\frac{n(n-1)}{2}$ 2-cyklů, $\frac{n(n-1)(n-2)(n-3)}{2^2\cdot2}$ součinů dvou disjunktních 2-cyklů a obecně $\frac{n(n-1)\ldots(n-2k+1)}{2^k\cdot k!}$ součinů k disjunktních 2-cyklů, kde $2k \leq n$.

1.3 Cyklus délky r je tvořen $r-1$ transpozicemi: $\alpha = (i_0, i_1, \ldots, i_{r-1}) = (i_0, i_1)(i_0, i_2)\ldots(i_0, i_{r-1})$. Tzn., že $\operatorname{sgn}(\alpha) = (-1)^{r-1}$. Pro sudou permutaci β platí, že $\operatorname{sgn}(\beta) = 1$, a proto $r-1$ musí být sudé. A tedy r je nutně liché.

1.4 Permutaci α zapíšeme jako součin disjunktních cyklů, tedy: $\alpha = (1,9)(2,8)(3,7)(4,$ Využijeme vztah $\operatorname{sgn}(\alpha) = (-1)^{n-t}$, kde $n = 9$ a $t = 5$ je počet cyklů. Po dosazení zjistíme, že $\operatorname{sgn}(\alpha) = 1$, jedná se tedy o sudou permutaci.

Kapitola 2

Grupy

Definice 2.1 (Binární operace)**.** Nechť G je množina. Binární operace je funkce $G \times G \to G$.

Pokud f je binární operace, budeme namísto $f(a, b)$ psát ab, $a \circ b$, $a * b$ nebo $a + b$.

Definice 2.2 (Grupa)**.** Nechť G je množina s binární operací. Binární operace je funkce $G \times G \to G$ splňující následující podmínky:

- pro každé $a, b, c \in G$ platí: $a(bc) = (ab)c$ (asociativnost),
- existuje $e \in G$ takové, že pro každý prvek $a \in G$ platí $ea = ae = 1$,
- pro každý prvek a existuje prvek b takový, že platí $ab = e = ba$.

Binární operace definovaná na G se nazývá *komutativní*, pokud pro každé dva prvky a, b platí $ab = ba$.

Poznámka.

Příklad 2.3 (Příklady grup a negrup)**.**

(a) $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{Q}^+, \cdot)$, $(\mathbb{R} - \{0\}, \cdot)$, $(\mathbb{C}, +)$, $(\mathbb{C} - \{0\}, \cdot)$.

(b) Je $(\mathbb{Z}, \cdot)$ grupa?

(c) $(U, \cdot)$, kde $U = \{x \in \mathbb{C}; |x| = 1\}$.

(d) Kladná iracionální čísla s operací násobení splňují všechny 3 axiomy, ale netvoří grupu. Proč?

(e) Matice 2×2 s operací sčítání.

(f) $(\mathbb{Z}_n, +)$.

(g) Grupy lineárních transformací $GL(2, R)$, $GL(2, Q)$, $GL(2, C)$.

(h) Kdy je $(\mathbb{Z}_n - \{0\}, \cdot)$ grupa?

(i) Multiplikativní grupy $U(n)$.

Grupa $U(n)$ je grupou jedniček modulo n, tzn. že množina $U(n)$ obsahuje všechna čísla $1, \ldots, n$ nesoudělná s n. Př.: $U(12) = \{1, 5, 7, 11\}$.

(j) Vektory nad polem $\mathbb{R}^n$ se sčítáním.

(k) $GL(2, \mathbb{Z}_p)$.

(l) Lineární a afinní grupa.

(m) Permutační grupy S_n, dihedrální grupy D_n.

Prvek e budeme v obecné grupě značit 1 a v komutativní grupě 0. Prvek $b = a^{-1}$ z axiomu (*iii*) nazveme inverzním prvkem k prvku a. Zapisujeme $1 = aa^{-1} = a^{-1}a$.

Lemma 2.4 (Základní vlastnosti)**.** *Nechť G je grupa. Potom*

- *G má jediný neutrální prvek,*
- *$ba = ca$ implikuje $b = c$ (pravé krácení),*
- *$ab = ac$ implikuje $b = c$ (levé krácení),*
- *pro každý prvek existuje jediný inverzní prvek,*
- $(ab)^{-1} = b^{-1}a^{-1}$.

Definice 2.5 (Mocnina prvku)**.** Nechť G je grupa. Z asociativity operace vyplývá, že výraz $x_1x_2 \ldots x_m$ je v grupě G dobře definován pro každé přirozené m. Nechť G je grupa a x je prvek. Pro přirozené číslo m definujeme $x^m = xx \ldots x$, m-krát. Mocninu můžeme rozšířit na celá čísla následovně: $x^0 = 1$ a $x^m = (x^{-m})^{-1} = x^{-1}x^{-1} \ldots x^{-1}$ pro $m < 0$.

Definice 2.6 (Cayleyho tabulka)**.** Pokud G je konečná grupa, potom příslušnou binární operaci můžeme definovat pomocí Cayleyho tabulky, jež má rozměry $G \times G$. Tabulka je definovaná lineárním uspořádáním prvků grupy, zpravidla dáváme na začátek 1. Řádky a sloupce odpovídají prvkům grupy. V poli se souřadnicemi $[a, b]$ píšeme prvek $c = ab$. Takovýto způsob zadání grupy je vhodný jen pro malé konečné grupy. Navíc, stejnou grupu můžeme v závislosti na pořadí definovat různými tabulkami.

Cvičení

2.1. Najděte inverzní prvek 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. $a = 3 - 2i$, $G = (\mathbb{C} - \{0\}, \cdot)$.

2.2. Najděte inverzní prvek k matici $\begin{pmatrix} 2 & 6 \\ 3 & 5 \end{pmatrix}$ v grupě $GL(2, \mathbb{Z}_{11})$.

2.3. Určete všechny prvky x dihedrální grupy D_4 splňující rovnici $x^2 = 1$.

2.4. Zkonstruujte Cayleyho tabulku pro grupu $U(12)$.

2.5. Částečně definovaná binární operace je daná tabulkou:

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

Doplňte chybějící políčka tabulky tak, aby definovala grupu.

2.6. Dokažte, že množina racionálních čísel tvaru $3^m 6^n$, kde $m, n \in \mathbb{Z}$, tvoří grupu vzhledem k operaci násobení.

2.7. [Heisenbergova grupa] Nechť G je množina trojúhelníkových reálných matic rozměrů 3×3 s binární operací definovanou následovně:

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

Dokažte, že uvedená množina matic s danou operací tvoří grupu.

2.8. Kolik prvků má grupa $GL(2, \mathbb{Z}_2)$? Je to komutativní grupa?

2.9. Dokažte, že pokud pro každý prvek grupy G platí $x^2 = 1$, je G abelovská.

2.10. Uvažujme zobrazení $f : Z_{11} \to Z_{11}$ dané polynomem $f(x) = 4x^2 - 3x^7$. Zjistěte, zda f je permutace. Jestliže ano, vypočítejte řád f.

2.11. Nechť G je grupa a nechť $a_1, \ldots, a_n \in G$. Dokažte, $(a_1 \cdot a_2 \cdots a_n)^{-1} = a_n^{-1} \cdot a_{n-1}^{-1} \cdots a_1^{-1}$.

2.12. Nechť G je grupa, $a \in G$ a nechť m, n jsou nesoudělná čísla. Jestliže $a^m = 1$, ukažte, že existuje $b \in G$, pro nějž je $a = b^n$.

2.13. Zkonstruujte Cayleyho tabulku pro grupu D_4 (což je dihedrální grupa řádu 8).

2.14. Je grupa D_3 abelovská?

2.15. Geometricky vysvětlete, proč složíme-li v D_n za sebou dvě reflexe, dostaneme rotaci.

2.16. Geometricky vysvětlete, proč složíme-li v D_n za sebou dvě rotace, dostaneme rotaci.

2.17. Geometricky vysvětlete, proč složíme-li v D_n za sebou rotaci a reflexi, dostaneme reflexi.

2.18. Nechť r_1, r_2, r_3 reprezentují tři rotace v D_n a nechť f_1, f_2, f_3 reprezentují v D_n tři reflexe. Je $r_1 r_2 f_1 r_3 f_2 f_3 r_3$ rotace, nebo reflexe?

2.19. Najděte prvky (symetrie) $A, B, C \in D_4$ takové, že $AB = BC$, ale $A \neq C$. Co tím ukážeme?

2.20. Proč množina lichých čísel není grupa? Uveďte dva důvody.

2.21. Ukažte, že množina $\{1, 2, 3\}$ s násobením modulo 4 není grupa, ale množina $\{1, 2, 3, 4\}$ s násobením modulo 5 grupa je.

2.22. Ukažte, že množina $\{5, 15, 25, 35\}$ je grupa s násobením modulo 40. Jaký prvek představuje identitu? Vidíte nějaký vztah s touto grupou a grupou $U(8)$?

2.23. Profesor abstraktní algebry měl v úmyslu dát studentům seznam devíti čísel, jež tvoří grupu při násobení modulo 91. Omylem však vynechal jedno číslo, takže seznam vypadal následovně: $\{1, 9, 16, 22, 53, 74, 79, 81\}$. Na jaké číslo profesor zapomněl?

2.24. Dokažte, že grupa G je abelovská právě tehdy, když $(ab)^{-1} = a^{-1}b^{-1}$ pro všechna $a, b \in G$.

2.25. Nechť a, b jsou prvky abelovské grupy a n nějaké celé číslo. Ukažte, že $(ab)^n = a^n b^n$. Platí tento vztah i pro neabelovské grupy?

2.26. Čísla 5 a 15 patří do seznamu dvanácti přirozených čísel, která tvoří grupu při násobení modulo 56. Nalezněte všech dvanáct čísel patřící do této grupy.

2.27. Najděte grupu se 105 prvky. Najděte dvě grupy se 44 prvky.

2.28. Dokažte, že pokud $(ab)^2 = a^2 b^2$ v grupě G, je $ab = ba$.

Nápověda k vybraným cvičením

2.1

1. $\mathbb{Z}_{20} = \{0, 1, \ldots, 19\}$. Najděte mocninu m čísla 13 takovou, že $a^m = 1$. Prvek a^{m-1} je pak inverzním prvkem k prvku a.

2. $U(14) = \{1, 3, 5, 9, 11, 13\}$. Platí $13^2 \pmod{14} = 1$, a tedy inverzním prvkem k prvku $a = 13$ je prvek $a^{-1} = 13$. Určete inverzní prvky ke zbývajícím prvkům grupy $U(14)$.

2.2 Pro inverzní matici $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ musí platit, že $\begin{pmatrix} 2 & 6 \\ 3 & 5 \end{pmatrix} \cdot \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. Hledáme tedy řešení soustavy čtyř rovnic o čtyřech neznámých.

2.3 Dihedrální grupa D_n je grupa shodností pravidelného n-úhelníku, ten má tak $2n$ shodností (n otočení a n osových souměrností). V případě čtverce tak existuje 8 shodností. Zapište D_4 Caleyho tabulkou (8×8).

2.5 Mohou se prvky v řádku či sloupci opakovat?

2.6 Ukážeme, že jsou splněny vlastnosti grupy. Jednotkový prvek je $1 = 3^0 \cdot 6^0$, platí, že $3^0 \cdot 6^0 \cdot 3^m \cdot 6^n = 3^m \cdot 6^n \cdot 3^0 \cdot 6^0 = 3^m \cdot 6^n = 1$. Asociativnost je splněna triviálně. Inverzní prvek k prvku $3^m \cdot 6^n$ je $3^{-m} \cdot 6^{-n}$. Operace je uzavřená. Důsledně ověřte a obhajte jednotlivé dílčí kroky (například, že skutečně $a \cdot a^{-1} = a^{-1} \cdot a = 1$, kde $a = 3^m 6^n$).

2.7 Prověřte vlastnosti grupy (uzavřenost operace, asociativnost, existenci inverzního a jednotkového prvku).

2.8 Matice $GL(2, \mathbb{Z}_2)$ je řádu 2 a na každé ze čtyř pozic může být 0 nebo jednička.

2.12 Existují celá čísla s a t taková, že $1 = sm + tn$.

2.13 Grupa D_n je grupa symetrií pravidelného n-úhelníku, jež má $2n$ symetrií, konkrétně grupa D_4 je grupa symetrií čtverce. Grupa D_4 má 4 rotace (o $0°$ – to je identita – o $90°, 180°$ a $270°$) a 4 symetrie (dle vertikální a horizontální osy a obou diagonálních os). Tabulka je tak 8×8.

Řešení vybraných cvičení

2.4 Grupa $U(12) = \{1, 5, 7, 11\} = \{1, -1, 5, -5\}$.

	1	-1	5	-5
1	1	-1	5	-5
-1	-1	1	-5	5
5	5	-5	1	-1
-5	-5	5	-1	1

2.10 Prostým dosazením čísel $0, \ldots, 11$ za x zjistíme, že $f(0) = 0$, $f(1) = 1$, $f(2) = 6$, $f(3) = 9$, $f(4) = 5$, $f(5) = 3$, $f(6) = 10$, $f(7) = 2$, $f(8) = 8$, $f(9) = 4$ a $f(10) = 7$. Jelikož každé z čísel $0, \ldots, 11$ je právě jednou vzorem a právě jednou obrazem, je $f = \alpha$ permutací.

Permutace α vypadá následovně:

$$\alpha = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 0 & 1 & 6 & 9 & 5 & 3 & 10 & 2 & 8 & 4 & 7 \end{pmatrix}.$$

Zapíšeme α jsou součin cyklů: $\alpha = (0)(1)(2, 6, 10, 7)(3, 9, 4, 5)(8)$. Řád permutace určíme dle nejmenšího společného násobku délek všech cyklů. To znamená, že řád permutace α je 4.

Kapitola 3

Podgrupy

Z již známých grup vytvoříme grupy nové.

Definice 3.1 (Řád grupy)**.** Počet prvků grupy G se nazývá řád grupy, značíme $|G|$. Pokud G je nekonečná, položíme $|G| = \infty$.

Definice 3.2 (Řád prvku)**.** Nechť $g \in G$ je prvek grupy. Řád prvku g, značíme $|g|$, je nejmenší kladné n takové, že $a^n = 1$. Pokud takové n neexistuje, potom g má nekonečný řád.

Příklad 3.3. Grupa $U(15) = \{1, 2, 4, 7, 8, 11, 13, 14\}$ má řád 8. Řády prvků jsou $|7| = 4$, $|11| = 2$, $|13| = 4$. V grupě $(Z, +)$ je řád každého nenulového prvku ∞.

Definice 3.4 (Podgrupa)**.** Podmnožina $H \subseteq$ grupy $(G, \cdot)$ se nazývá podgrupa, pokud $(H, \cdot)$ je grupa. Zapisujeme $H \leq G$.

Věta 3.5 (Test podgrupy)**.** *Nechť G je grupa a $H \subseteq G$, $H \neq \emptyset$. Potom H je podgrupou G právě tehdy, když pro každé dva prvky $a, b \in H$ platí $ab^{-1} \in H$.*

Příklad 3.6 (Podgrupy abelovské grupy)**.** Nechť G je abelovská grupa. Potom platí:

- Množina prvků řádu 2 v abelovské grupě je podgrupou.
- Množina prvků konečného řádu v abelovské grupě je podgrupou.
- Jsou-li $H \leq G$ a $K \leq G$ podgrupy, množina $HK = \{hk; h \in H, k \in K\}$ je podgrupa.

Věta 3.7 (Test podgrupy v konečné grupě)**.** *Konečná podmnožina $\emptyset \neq H \subseteq (G, \cdot)$ je podgrupa G právě tehdy, když H je uzavřená na binární operaci $\cdot$.*

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

Věta 3.8. *Nechť G je grupa a nechť $a \in G$. Potom $\langle a \rangle$ je podgrupa.*

Příklad 3.9. Nechť D_n je dihedrální grupa. Nech $R \in D_n$ je rotace o $360/n$ stupňů. Potom $\langle R \rangle$ je podgrupa řádu n.

Je dobré si uvědomit, že $\langle a \rangle$ je nejmenší podgrupa obsahující prvek a.

Věta 3.10. *Nechť G je grupa a nechť G_i, $i \in I$, je systém podgrup grupy G. Potom $\cap_{i \in I} G_i$ je podgrupa G.*

Definice 3.11. Nechť G je grupa a $S \subseteq G$ je podmnožina. Označme $\langle S \rangle \leq G$ nejmenší podgrupu G obsahující S.

Díky větě 3.10 je podgrupa $\langle S \rangle$ jednoznačně definovaná.

Příklad 3.12 (Gaussova čísla)**.** Nechť $\{1, i\} \subset \mathbb{C}$. Potom $\langle 1, i \rangle = \{a + bi; a, b \in \mathbb{Z}\}$ je podgrupa $(\mathbb{C}, +)$. Pokud použijeme standardní reprezentaci komplexních čísel v Euklidovské rovine, tak Gaussova čísla odpovídají bodům s celočíselnými souřadnicemi.

Definice 3.13 (Centrum grupy)**.** Nechť G je grupa. Potom $Z(G) = \{a \in G; ax = xa$ pro každý $x \in G\}$ se nazývá centrum grupy.

Věta 3.14. *Nechť G je grupa. Centrum grupy je abelovská podgrupa grupy G.*

Všimneme si, že $Z(G) = G$, pokud G je abelovská.

Definice 3.15. Nechť $a \in G$. Centralizátor $C(a)$ prvku a je podmnožina $C(a) = \{x \in G; xa = ax\}$.

Pokud $a \in Z(G)$, je $C(a) = G$. Platí $Z(G) \leq C(a) \leq G$.

Věta 3.16. *Centralizátor prvku $a \in G$ je podgrupa G.*

Cvičení

3.1. Najděte všechny podgrupy Z_{12}.

3.2. Najděte centrum dihedrální grupy D_n.

3.3. Najděte všechny podgrupy S_4.

3.4. Určete centralizátor permutací $(1, 2)$, $(1, 2)(3, 4)$ a $(1, 2, 3)$ v S_4.

3.5. Nechť je dána grupa $G = \mathbb{Z}_{20}$. Najděte nejmenší podgrupu grupy G obsahující

- prvek 1,
- prvek 8,
- prvek 7,
- prvky $2, 3, 5$.

3.6. Dokažte, že alternující grupa A_n, množina sudých permutací v S_n, je podgrupa s $\frac{n!}{2}$ prvky.

3.7. Nechť k je pole. Ukažte, že $SL(n, k)$, množina všech $n \times n$ matic přes k mající determinant 1, je podgrupa grupy $GL(n, k)$.

3.8. Nechť $n > 2$. Dokažte, že grupa A_n je generovaná všemi trojcykly.

3.9. Pro každou z následujících grup určete řád grupy a řád každého prvku příslušné grupy. Jaký vztah vidíte mezi těmito řády?

$\mathbb{Z}_{12}$, $U(10)$, $U(12)$, $U(20)$, D_4

3.10. Máme dány dvě grupy $\mathbb{Q} = (\mathbb{Q}, +)$ a $\mathbb{Q}^* = (\mathbb{Q} \setminus 0, \cdot)$. V obou dvou grupách určete $\langle \frac{1}{2} \rangle$ a určete řády všech prvků.

3.11. Dokažte, že v každé grupě G má prvek α stejný řád jako prvek α^{-1}.

3.12. Bez počítání jednotlivých řádů, vysvětlete, proč dva prvky 8 a 22 mají v grupě $\mathbb{Z}_{30}$ stejný řád. Totéž proveďte pro dvojici 2 a 28 a v grupě $U(15)$ pro dvojice prvků $2, 8$ a $7, 13$.

3.13. Pro prvek a v grupě G platí $a^6 = id$. Jaký může být řád prvku a?

3.14. Nechť a je prvek grupy G nekonečného řádu. Dokažte, že $a^m \neq a^n$, když $m \neq n$.

3.15. Ukažte, že pro jakýkoliv prvek a v grupě G platí $|a| \leq |G|$.

3.16. Ukažte, že grupa $U(14) = \langle 3 \rangle = \langle 5 \rangle$. Je $U(14) = \langle 11 \rangle$?

3.17. Ukažte, že $U(20) \neq \langle k \rangle$ pro všechna $k \in U(20)$. Co z toho plyne?

3.18. Dokažte, že abelovská grupa s dvěma prvky řádu 2 musí obsahovat podgrupu řádu 4.

3.19. Najděte grupu G obsahující prvky a, b takové, že $|a| = |b| = 2$, pro něž

- $|ab| = 3$,
- $|ab| = 4$,
- $|ab| = 5$.

Vidíte nějaký vztah mezi a, b a ab?

3.20. Nechť H, K jsou podgrupy grupy G. Ukažte, že $H \cap K$ je rovněž podgrupa grupy G.

3.21. Nechť grupa H je vlastní podgrupa grupy $(\mathbb{Z}, +)$. Grupa H obsahuje prvky

- 18, 30, 40,
- 12, 30, 54.

Určete grupu H. Existuje vždy právě jedna možnost?

3.22. Ukažte, že dihedrální grupa řádu 6 neobsahuje podgrupu řádu 4.

3.23. Nechť G je grupa a $a \in G$. Ukažte, že $C(a) = C(a^{-1})$.

3.24. Nechť a, b jsou dva různé prvky grupy G. Dokažte, že buď $a^2 \neq b^2$ nebo $a^3 \neq b^3$.

3.25. Nechť je dána grupa G a její podgrupa H. Dokažte, že $C(H)$ je podrgupa grupy G.

3.26. Dokažte, že grupa sudého řádu musí obsahovat prvek řádu 2.

3.27. Předpokládejme, že grupa G obsahuje právě osm prvků řádu 3. Kolik podgrup řádu 3 obsahuje grupa G?

3.28. Spočtěte řády následujících grup. Na základě Vašich odpovědí vytvořte hypotézu o vztahu mezi $|U(r)|, |U(s)|$ a $|U(rs)|$.

- $U(3), U(4), U(12)$,

- $U(5), U(7), U(35)$,
- $U(4), U(5), U(20)$,
- $U(3), U(5), U(15)$.

3.29. Spočtěte $|U(4)|, |U(10)|$ a $|U(40)|$. Odporuje tento příklad Vaší hypotéze z předchozího cvičení? Pokud ano, revidujte tuto hypotézu.

3.30. Nechť $H = \{a + bi | a, b \in \mathbb{R}, ab \geq 0\}$. Je H podgrupou $(\mathbb{C}, +)$?

3.31. Nechť $G = GL(2, \mathbb{R})$. Najděte $C(\mathbb{J} \setminus \mathbb{I})$, kde $\mathbb{J}$ je matice samých jedniček řádu 2 a $\mathbb{I}$ je jednotková matice řádu 2.

Nápověda k vybraným cvičením

3.1 Generujte podgrupu pomocí každého prvku $a \in G$ kromě 0. Po nastudování následující kapitoly se k tomuto příkladu vraťte, určete počet generátorů grupy G a vylaďte postup řešení.

3.3 Grupa S_4 má 30 podgrup: samotnou grupu S_4, jednu řádu 12 (to je A_4), tři řádu 8, čtyři řádu 6, sedm řádu 4, čtyři řádu 3, devět řádu 2 a identitu. Najděte konkrétně tyto podgrupy.

3.4 Hledáme všechny permutace $x_i \in S_4$ takové, že $x_i\alpha = \alpha x_i$ pro všechna i a příslušnou permutaci α. Identita je vždy v centralizátoru příslušné permutace. V prvním případě je $\alpha_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix}$. Triviálně: v x_i musejí být fixovány prvky 3 a 4, protože jsou fixovány v permutaci α_1. Máme tedy dvě možnosti: $x_1 = 1$ a $x_2 = \alpha_1$, které jsou obě splněny triviálně. Proto $C((1,2)) = \{(1), (1,2)\}$. Proveďte pro $\alpha_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$ a $\alpha_3 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}$.

3.6 Ukažte, že grupa S_n má stejný počet sudých a lichých permutací.

3.8 Platí: $(ij)(jk) = (ijk)$ a $(ij)(kl) = (ijk)(jkl)$.

3.19 Ukažme řešení pro třetí případ. V symetrické grupě S_5 platí $(1,2,3,4,5) = (1,2)(3,5) \cdot (2,5)(3,4)$. Tak tedy $a = (1,2)(3,5)$ a $b = (2,5)(3,4)$.

Řešení vybraných cvičení

3.2 Pro $n \leq 2$ je $|D_n| \leq 4$ a grupa D_n je pro $n \leq 2$ abelovská (proč?). A tedy $Z(D_n) = D_n$ pro $n \leq 2$.

Nechť nyní $n \geq 3$. Grupu D_n můžeme zapsat následovně: $D_n = \langle a, b : a^n = b^2 = id, bab = a^{-1} \rangle$. A dále pro všechna celá čísla $k \geq 0$ v D_n platí: $ba^k = a^{n-k}b$ (proč?). Grupa D_n je tedy generována prvky a, b a prvek x náleží $Z(D_n)$ právě tehdy, když platí $xa = ax$ a $xb = bx$. Prvek $x \in Z(D_n)$ tedy můžeme zapsat jako $x = a^i b^j$. Dosazením za x v $xa = ax$ dostane $b^j a = ab^j$. Což pro $j = 1$ udává $a^2 = id$ (využíváme faktu, že $bab = a^{-1}$ a $b^2 = id$). Jelikož ale řád a je $n > 2$, nutně $a^2 \neq id$. Obdobně pro $j > 1$. Z toho tedy vyplývá, že $j = 0$ a $x = a^i$.

Pro prvek $x \in Z(D_n)$ platí $xb = bx$ a dosazením a^i za x dostaneme $a^i b = ba^i = a^{n-1}b$. To je ekvivalentní se vztahem $a^{2i} = id$. Z toho vyplývá, že n dělí $2i$. A tedy $i = 0$ nebo $n = 2i$ $(0 \leq i \leq n)$. Dostáváme tedy následující výsledek: Centrum grupy $Z(D_n) = id$, pokud n je liché, nebo $Z(D_n) = \{id, a^{\frac{n}{2}}\}$, pokud n je sudé.

Řádně z důkazu zodpovězte doplňující otázky *proč?*.

3.17 Pokud grupa G řádu n není cyklická, každý její prvek může generovat podgrupu grupy G řádu nejvýše $n - 1$ (jak to bude pro grupy nekonečného řádu?). Grupa $U(20) = \{1, 3, 7, 9, 11, 13, 17, 19\}$ má osm generátorů (vzpomeňme na Eulerovu funkci), je tedy třeba pro všechny prvky $x \in U(20)$ ukázat, že $x^m = 1$, kde $m \leq 4$. Grupa $\langle 3 \rangle = \{1, 3, 7, 9\}$ je řádu 4. Pro každý prvek $y \in \langle 3 \rangle$ je množina $\langle y \rangle$ podgrupa grupy $\langle 3 \rangle$, a tedy $|y| \leq 4$. Dále $\langle 13 \rangle = \{1, 9, 13, 17\}$ a zbývají tedy jen prvky 11 a 19. Pro ně dostáváme: $\langle 11 \rangle = \{1, 11\}$ a $\langle 19 \rangle = \{1, 19\}$. Z toho tedy plyne, že $U(20) \neq \langle k \rangle$ pro všechna $k \in U(20)$. Grupa $U(20)$ není cyklická grupa.

3.23 Pokud $x \in C(A)$, je $ax = xa$. Pak $x = a^{-1}ax = a^{-1}xa$ a $xa^{-1} = a^{-1}xaa^{-1} = a^{-1}x$. A tedy $x \in C(a^{-1})$. Dostáváme tedy $C(a) \subset C(a^{-1})$. Nyní po provedení stejné myšlenky pro a^{-1} dostaneme $C(a^{-1}) \subset C((a^{-1})^{-1}) = C(a)$. A z toho již triviálně plyne, že $C(a) = C(a^{-1})$.

3.26 Pokud pro prvek $a \in G$ platí $a = a^{-1}$, je $|a| = 2$. Protože každý prvek grupy G má stejný řád jako jeho inverzní prvek, můžeme zpárovat všechny prvky G s řádem větším než 2 s jejich inverzními prvky. A tedy musí existovat sudý počet prvků s řádem větším než dva. Jelikož ale je ale řád grupy sudý, grupa G obsahuje lichý počet prvků různých od identity. Z toho tedy již plyne, že G musí obsahovat prvek řádu 2.

Kapitola 4

Cyklické grupy

Grupa G se nazývá cyklická, existuje-li prvek $a \in G$ takový, že platí $G = \langle a \rangle$.

Věta 4.1 (Kritérium rovnosti mocnin)**.** *Nechť $a \in G$, kde G je grupa. Potom*

- *pokud $|a| = \infty$, $a^i = a^j$ právě tehdy, když $i = j$,*
- *pokud $|a| = n$, $a^i = a^j$ právě tehdy, když $n \mid (i - j)$.*

Důsledek 4.2. *Pro každý prvek a grupy platí $|a| = |\langle a \rangle|$.*

Důsledek 4.3. *Nechť a je prvek řádu n. Nechť $a^k = 1$, potom $n \mid k$.*

Věta 4.4. *Nechť a je prvek řádu n. Potom $\langle a^k \rangle = \langle a^{\gcd(n,k)} \rangle$ a $|a^k| = n/\gcd(n,k)$.*

Náčrt důkazu: Chceme dokázat, že $\langle a^d \rangle = \langle a^k \rangle$. Protože $d \mid k$, je $\langle a^d \rangle \geq \langle a^k \rangle$. Jelikož $d = \gcd(n,k) = ns + kt$, je $a^d = a^{ns+kt} = (a^k)^t \in \langle a^k \rangle$. Tedy i $\langle a^d \rangle \leq \langle a^k \rangle$.

Řády: $(a^d)^{n/d}$, proto $|a^d| \mid \frac{n}{d}$.

Na druhé straně, $a^{di} = 1$, potom $a^{ki} = 1$. Tedy $i \mid n/k$ a rovněž $i \mid n/d$.

Důsledek 4.5. *Je-li G konečná cyklická grupa, potom řád prvku dělí řád G.*

Důsledek 4.6. *Nechť $|a| = n$. Potom $\langle a^i \rangle = \langle a^j \rangle$ právě tehdy, když $\gcd(n,i) = \gcd(n,j)$, a $|a^i| = |a^j|$ právě tehdy, když $\gcd(n,i) = \gcd(n,j)$.*

Důsledek 4.7. *Nechť G je cyklická grupa řádu n, nechť $|a| = k$. Potom $\langle a \rangle = G$ právě tehdy, když $\gcd(k,n) = 1$.*

Věta 4.8. *Každá podgrupa cyklické grupy G je cyklická. Navíc, pokud $|G| = n$, pro každé k, $k \mid n$, má G právě jednu podgrupu řádu k.*

Důkaz. Pokud $H \leq G = \langle a \rangle$, $H = \{1\}$ a je cyklická. Pokud H je netriviální, obsahuje nějakou mocninu a^t. Nechť t je minimální kladný exponent, $a^t \in H$. Potom $H = \langle a^t \rangle$. Triviálně platí $H \geq \langle a^t \rangle$. Pokud $a^m \in H$, pro $m > t$, je

$m = qt + r$, kde $0 \leq r < t$. Potom $a^m = (a^t)^q \cdot a^r$. Pokud $r > 0$, je $a^r \in H$, a dostáváme tak spor s minimalitou t. Proto $r = 0$ a $a^m = a^{qt} \in \langle a^t \rangle$.

Jednoznačnost. Víme, že ke každému děliteli k existuje cyklická podgrupa řádu k generovaná $a^{n/k}$. Mějme nějakou podgrupu H řádu k. Podle předešlé části existuje m takové, že $H = \langle a^m \rangle$. Podle věty 4.4 H můžeme vygenerovat prvkem $a^{\gcd(m,n)}$. Potom pro zvolený dělitel k platí: $k = |H| = |\langle a^m \rangle| = |\langle a^{\gcd(m,n)} \rangle| = n/\gcd(n,m) = n/m$. Proto $m = n/k$, a tedy podgrupa je jednoznačně určena. □

Poznámka. Všimněme si, že existuje jednoznačná korespondence mezi podgrupami cyklické grupy G a děliteli $n = |G|$. Tato bijekce definuje izomorfismus mezi svazem dělitelů n a svazem podgrup G. Pro dané podgrupy $H_1, H_2 \leq G$ tvoří infimum a supremum podgrupy $H_1 \cap H_2$ a $\langle H_1, H_2 \rangle$.

Další věc hodná povšimnutí je úloha elementární aritmetiky v tvrzeních o cyklických grupách (dělení se zbytkem a Euklidův algoritmus).

Eulerova funce. Označme $\varphi(n)$ počet přirozených čísel $\leq n$, která jsou nesoudělná s n. Z předešlého textu vyplývá, že $\langle a \rangle = G$, kde G je cyklická grupa, $a \in G$ právě tehdy, když $\gcd(a, n) = 1$. Proto $\varphi(n)$ je počet generátorů G. Eulerova funkce hraje důležitou úlohu v teorii čísel a kombinatorice. Jde o takzvanou multiplikativní funkci. Splňuje následující vlastnosti.

Lemma 4.9. *Nechť n, k, m jsou přirozená čísla a p je prvočíslo. Potom*

- $\varphi(p) = p - 1$ *a* $\varphi(p^k) = (p-1)p^{k-1}$,
- $\varphi(mk) = \varphi(m)\varphi(k)$,
- *Pokud* $n = \prod_{i=1}^{k} p_i^{e_i}$ *je rozklad přirozeného čísla na mocniny prvočísel, platí*

$$\varphi(n) = \prod_{i=1}^{k} (p-1)p^{e_i - 1},$$

- $n = \sum_{d|n} \varphi(d)$.

Důkaz. Dokážeme jen poslední rovnost. Nechť C_n je cyklická grupa řádu n. Z věty 4.8 víme, že pro každý dělitel $d \mid n$ existuje jediná cyklická podgrupa C_d řádu d. Označme $gen(C_d)$ množinu jednoprvkových generátorů C_d. Potom $|gen(C_d)| = \varphi(d)$. Potom $C_n = \cup_{d|n} gen(C_d)$ a platí

$$n = \sum_{d|n} |gen(C_d)| = \sum_{d|n} \varphi(d).$$

□

Cvičení

Dejte si pozor, abyste v argumentaci nepoužili to, co se snažíte zdůvodnit!

4.1. Vyjmenujte generátory $\mathbb{Z}_6$, $\mathbb{Z}_8$, $\mathbb{Z}_{20}$.

4.2. Vyjmenujte prvky $\langle 3\rangle$, $\langle 7\rangle$ v $U(20)$.

4.3. Vypočítejte $\langle 21\rangle \cap \langle 10\rangle$ v grupě $\mathbb{Z}_{24}$.

4.4. Nechť $G = \langle a\rangle$ je řádu n. Najděte generátor $H = \langle a^{21}\rangle \cap \langle a^{10}\rangle$. Jaký je řád H?

4.5. Nechť G je cyklická grupa řádu n s právě jednou vlastní podgrupou H. Co můžete říci o řádech G a H?

4.6. Nechť G je abelovská grupa. Označme $H = \{g \in G |\ |g| \text{ dělí } 12\}$. Dokažte, že H je grupa. Číslo 12 můžete nahradit i jiným číslem. Pokuste se zformulovat obecné tvrzení.

4.7. Najděte maximální řetězec podgrup $H_1 < H_2 < \cdots < H_m$ v cyklické grupě $\mathbb{Z}_{240}$. Pokuste se zformulovat všeobecné tvrzení pro cyklickou grupu řádu n.

4.8. Vypište podgrupy $(Z, +)$.

4.9. Kolik prvků řádu d pro $d \mid n$ má dihedrální grupa D_n? Spočítejte prvky dihedrální grupy D_n.

4.10. Jaké jsou možnosti pro řád prvku ab v dihedrální grupě D_{21}, víme-li, že $|a| = |b| = 2$.

4.11. Najděte všechny podgrupy grupy $\mathbb{Z}_{30}$ a určete jejich řád.

4.12. Najděte příklad necyklické grupy, jejíž všechny vlastní podgrupy jsou cyklické.

4.13. Nechť a je prvek grupy G a nechť $|a| = 15$. Spočtěte řády následujících prvků grupy G:

- a^3, a^6, a^9, a^{12},
- a^5, a^{10},
- a^2, a^4, a^8, a^{14}.

4.14. Nechť G je grupa a nechť $a \in G$. Dokažte, že $\langle a\rangle = \langle a^{-1}\rangle$.

4.15. Kolik podgrup má grupa $\mathbb{Z}_{20}$? Pro každou podgrupu nalezněte generátor. Předpokládejme, že $G = \langle a\rangle$ a $|a| = 20$. Kolik podgrup grupa G obsahuje? Pro každou podgrupu nalezněte generátor.

4.16. Nechť G je cyklická grupa, jež má právě tři podgrupy, z nichž jedna je řádu 7. Kolik je $|G|$? Co můžeme říci, nahradíme-li číslo 7 libovolným prvočíslem?

4.17. Doplňte následující tvrzení, aby bylo pravdivé: $|a| = |a^2|$ *právě tehdy, když* $|a| \ldots$.

4.18. Nechť cyklická grupa obsahuje prvek nekonečného řádu. Kolik tato grupa obsahuje prvků konečného řádu?

4.19. Vypište cyklické podgrupy grupy $U(30)$.

4.20. Nechť je dána abelovská grupa G řádu 35 a každý její prvek splňuje rovnici $x^{35} = id$. Dokažte, že grupa G je cyklická. Bude tvrzení platit, když řád 35 nahradíme řádem 33?

4.21. Dokažte, že grupa řádu 3 musí být cyklická.

4.22. Nechť d je přirozené číslo různé od dvou a nechť d dělí n. Ukažte, že počet prvků řádu d v D_n je $\varphi(d)$. Kolik prvků řádu 2 má grupa D_n?

4.23. Dokažte, že konečná grupa G je sjednocením vlastních podgrup právě tehdy, když grupa G není cyklická.

4.24. Najděte příklad grupy G, jež obsahuje právě šest podgrup. Zobecněte pro přirozené číslo n.

4.25. Nechť p je prvočíslo. Pokud grupa G obsahuje více než $p-1$ prvků řádu p, nemůže být grupa G cyklická. Dokažte.

4.26. Nechť G je abelovská grupa a obsahuje cyklické podgrupy řádu 4 a 5. Podgrupy jakého řádu musí grupa G obsahovat? Zobecněte.

4.27. Dokažte, že žádná grupa nemůže obsahovat právě dva prvky řádu 2.

4.28. Nechť a, b jsou prvky grupy G. Pokud $|a| = 10$ a $|b| = 21$, ukažte, že $\langle a\rangle \cap \langle b\rangle = id$. Pro jaká dvě čísla toto platí obecně?

4.29. Dokažte, že grupa $U(2^n)$, kde $n \geq 3$, není cyklická.

4.30. Nechť $|a^5| = 12$. Jaké možnosti připadají v úvahu pro $|a|$? A jak to bude pro $|a^4| = 12$?

4.31. Nechť a je prvek grupy G takový, že $|a^{28}| = 10$ a $|a^{22}| = 20$. Určete $|a|$.

4.32. Dokažte, že grupa $H = \{\begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} | n \in \mathbb{Z}\}$ je cyklická podgrupa grupy $GL(2, \mathbb{R})$.

4.33. Nechť a, b jsou prvky grupy G a nechť $|a| = 12$, $|b| = 22$ a $\langle a\rangle \cap \langle b\rangle \neq id$. Dokažte, že $a^6 = b^{11}$.

4.34. Předpokládejme, že konečná grupa G, v níž každý prvek různý od identity je prvočíselného řádu. Uveďte příklad takovéto grupy. Pokud $Z(G)$ není triviální, dokažte, že všechny prvky grupy G mají stejný řád.

4.35. Pro jaké přirozené číslo n není grupa $U(n^2-1)$ cyklická? Dokažte.

4.36. Uveďte příklad nekonečné grupy G, jež má právě dva prvky řádu 4.

Nápověda k vybraným cvičením

4.1 Může být číslo k, jež je dělitelem čísla n, generátorem grupy $\mathbb{Z}_n$? A je každé číslo l, jež je s n nesoudělné, generátorem této grupy?

4.3 Podobně jako v minulém příkladě najděte $\langle 21\rangle$ a $\langle 10\rangle$. Pak nalezněte průnik obou množin.

4.7 Postupujte *odzadu*. Jaký je největší dělitel čísla 240 menší než 240? Atd.

4.9 Použijte Eulerovu funkci $\varphi(d)$.

4.12 Jedná se o grupu G, jež má následující reprezentaci: $G = \langle -1, i, j, k; (-1)^2 = 1, i^2 = j^2 = k^2 = ijk = -1\rangle$, kde 1 je neutrální prvek a -1 komutuje se všemi ostatními prvky. Jak grupě říkáme?

4.14 Platí $a^{n-1} = a^{-1}$.

4.24 Pokud G je cyklická grupa řádu n, pro každé přirozené číslo m, jež je dělitelem čísla n, existuje právě jedna podgrupa grupy G řádu m. Kolik dělitelů existuje pro 2^{n-1}?

Řešení vybraných cvičení

4.2 Počítejme modulo 20, tedy: $3^0 = 1, 3^1 = 3, 3^2 = 9, 3^3 = 9 \cdot 3 = 7$ a $3^4 = 3 \cdot 7 = 1$, tzn. $3^0 = 3^4$, a tedy $\langle 3 \rangle = \{1, 3, 7, 9\}$. A $\langle 7 \rangle = \{1, 3, 7, 9\}$.

4.8 Nejprve ukážeme, že neexistuje žádná konečná podgrupa grupy $(\mathbb{Z}, +)$. Pro spor předpokládejme, že konečná podgrupa existuje a označme ji K. Tato podgrupa musí mít nějaký největší prvek, nazvěme jej m. Pokud $m \neq 0$, uzavřeností sčítání a existencí inverzního prvku, musejí prvky $2n$ a $-n$ být rovněž v K. Jeden z nich (v závislosti na tom, zda je m kladné či záporné), je však určitě větší než n a dostáváme spor. Pokud $m = 0$, musejí existovat prvky $l, -l \in K$ a opět dostáváme spor s maximalitou m. Podgrupa tedy nemůže být konečná.

Dále předpokládejme, že existuje nekonečná podgrupa H grupy $(\mathbb{Z}, +)$ s nejmenším kladným prvkem n. Libovolný prvek k grupy H pak lze zapsat jako $k = nq + r$, kde $q, r \in \mathbb{Z}$ a $0 \leq r < n$. Jelikož $k, n \in H$, rovněž $r = k - nq \in H$. Protože $0 \leq r < n$ a n je nejmenší přirozené číslo, je $r = 0$, a tedy $k = nq$. Ukázali jsme tedy, že libovolný prvek grupy H je ve tvaru nq, kde $q \in \mathbb{Z}$. Tedy $H = n\mathbb{Z}$.

4.11

- $\langle 1 \rangle = \{0, 1, 2, \ldots, 29\}$ – řádu 30,
- $\langle 2 \rangle = \{0, 2, 4, \ldots, 28\}$ – řádu 15,
- $\langle 3 \rangle = \{0, 3, 6, \ldots, 27\}$ – řádu 10,
- $\langle 5 \rangle = \{0, 5, 10, 15, 20, 25\}$ – řádu 6,
- $\langle 6 \rangle = \{0, 6, 12, 18, 24\}$ – řádu 5,
- $\langle 10 \rangle = \{0, 10, 20\}$ – řádu 3,
- $\langle 15 \rangle = \{0, 15\}$ – řádu 2,
- $\langle 30 \rangle = \{0\}$ – řádu 1.

4.18 Grupa G je cyklická, a proto $G = \{g^n : n \in \mathbb{Z}\}$ pro nějaký prvek $g \in G$ nekonečného řádu. Pokud $x \in G$, je $x = g^m$ pro nějaké $m \in \mathbb{N} \cup \{0\}$. Pokud $m \neq 0$ (tedy x není identita), pro každé $k \in \mathbb{Z}$ dostáváme $x^k = g^{m^k} = g^{km}$ a $g^{km} = g^0$ právě tehdy, když $km = 0$, což nastává jen tehdy, když $k = 0$. To tedy znamená, že jediný prvek konečného řádu je identita. Existuje jen jeden prvek konečného řádu.

Kapitola 5

Homomorfismy a izomorfismy

Definice 5.1. Nechť $(G, \cdot)$ a $(H, *)$ jsou grupy. Zobrazení $\varphi : G \to H$ je homomorfismem, pokud pro každé dva prvky $a, b \in G$ platí $\varphi(a \cdot b) = \varphi(a) * \varphi(b)$. Izomorfismus $G \to H$ je homomorfismus, který je bijekcí. Surjektivní homomorfismus se nazývá epimorfismus. Injektivní homomorfismus se nazývá monomorfismus (nebo vnoření).

Věta 5.2. *Nechť $(G, \cdot)$ a $(H, *)$ jsou grupy. Nechť $\varphi : G \to H$ je homomorfismus. Potom platí*

- $\varphi(1_G) = 1_H$,
- *pokud $a \in G$, $\varphi(a^{-1}) = (\varphi(a))^{-1}$,*
- *pro každé $a \in G$ a $n \in \mathbb{Z}$ platí $\varphi(a^n) = (\varphi(a))^n$.*

Příklad 5.3. Funkce $\operatorname{sgn} : S_n \to U(3) \cong (\{1, -1\}, \cdot)$ je homomorfismem.

Funkce determinant $A \mapsto \det(A)$ z $\mathrm{GL}(n, F) \to F$ je homomorfismem. Vzpomeňte si na vztah z lineární algebry $\det(AB) = \det(A)\det(B)$.

Definice 5.4. Nechť $\varphi : G \to H$ je homomorfismus grup. Označme $\ker(\varphi) = \{g \in G |\ \varphi(g) = 1_H\}$ jádro homomorfismu φ a $\operatorname{Im}(\varphi) = \{h \in H |$ existuje $g \in G,\ \varphi(g) = h\}$ obraz homomorfismu φ.

Tvrzení 5.5. *Nechť $\varphi : G \to H$ je homomorfismus grup. Platí $\ker(\varphi) \leq G$ a $\operatorname{Im}(\varphi) \leq H$ jsou podgrupami.*

Cvičení

Cílem důkazu je mu porozumět, ne jen prověřit!

5.1. Dokažte, že na čtyřprvkové množině můžeme definovat dvě neizomorfní grupy.

5.2. Permutační matice $P(\alpha) \in \mathrm{GL}(n, F)$ vzniká z jednotkové diagonální matice $I \in \mathrm{GL}(n, F)$, kde $I = (\epsilon_1, \ldots, \epsilon_n)$, ϵ_i je i-tý sloupec vzniklý permutováním sloupců podle α. Tedy $P(\alpha) = (\epsilon_{\alpha 1}, \ldots, \epsilon_{\alpha n})$. Dokažte, že permutační matice tvoří grupu. Navíc, zobrazení $\alpha \mapsto P(\alpha)$ je homomorfismus $S_n \to \mathrm{GL}(n, F)$.

5.3. Označme T multiplikativní grupu komplexních čísel s absolutní hodnotou 1. Dokažte, že pro každé $y \in \mathbb{R}$ je zobrazení $\varphi_y(x) = e^{iyx}$ homomorfismem $(\mathbb{R}, +) \to (T, \cdot)$.

5.4. Určete jádro a obraz homomorfismů v příkladech 5.2 a 5.3.

5.5. Najděte izomorfismus z grupy celých čísel se sčítáním do grupy sudých čísel se sčítáním.

5.6. Najděte $Aut(\mathbb{Z})$.

5.7. Ukažte, že $U(8)$ není izomorfní s $U(10)$.

5.8. Ukažte, že $U(8)$ je izomorfní s $U(12)$.

5.9. Dokažte, že grupa S_4 není izomorfní s grupou D_{12}.

5.10. Najděte dvě grupy G, H takové, že $G \not\approx H$, ale $Aut(G) \approx Aut(H)$.

5.11. Najděte $Aut(\mathbb{Z}_6)$.

5.12. Jestliže Ψ a Φ jsou jsou izomorfismy z cyklické grupy $G = \langle a \rangle$ do nějaké grupy H a $\Psi(a) = \Phi(a)$, dokažte, že $\Psi = \Phi$.

5.13. Předpokládejme, že $\Phi : \mathbb{Z}_{50} \to \mathbb{Z}_{50}$ je automorfismus s $\Phi(11) = 13$. Najděte předpis pro $\Phi(x)$.

5.14. Jsou grupy $U(20)$ a $U(24)$ izomorfní?

5.15. Dokažte, že grupa $(\mathbb{Z}, +)$ není izomorfní s grupou $(\mathbb{Q}, +)$.

5.16. Nechť $f : X \to Y$ je bijekce mezi množinami X a Y. Ukažte, že $\alpha \mapsto f \circ \alpha \circ f^{-1}$ je izomorfismus $S_X \to S_Y$.

Nápověda k vybraným cvičením

5.3 Ověřte následující: zobrazení $\varphi : G \to H$ je homomorfismem, pokud pro každé dva prvky $a, b \in G$ platí $\varphi(a \cdot b) = \varphi(a) * \varphi(b)$.

5.5 Definujte zobrazení $\phi : \mathbb{Z} \to 2\mathbb{Z}$ jako $\phi(n) = 2n$. Ověřte, že jde o izomorfismus.

5.8 Vezměme bijektivní zobrazení $\Phi : U(8) \to U(12)$ definované následovně: $\Phi(1) = 1$, $\Phi(3) = 11$, $\Phi(5) = 5$ a $\Phi(7) = 7$. S vědomím, že grupa $U(8)$ je abelovská, stačí ověřit jen šest vztahů (jakých?). Existuje ještě nějaké další bijektivní zobrazení, nebo jsme představili jediné možné?

Řešení vybraných cvičení

5.6 Nejprve si uvědomme, že $\mathbb{Z}$ je cyklická grupa generovaná 1, tedy $\mathbb{Z} = \langle 1 \rangle$. Kromě 1 je generátorem grupy ještě -1. Jelikož automorfismus Φ cyklické grupy zobrazuje generátor na generátor, je $\Phi(1) = 1$ nebo $\Phi(1) = -1$. Protože $\Phi(m \cdot 1) = m\Phi(1)$, dostáváme v prvním případě identické zobrazení a ve druhém případě dostáváme $\Phi(x) = -x$. A tedy $Aut(\mathbb{Z}) = \{id, \Phi\}$, kde $\Phi(x) = -x$.

5.7 Grupa $U(10) = \{1, 3, 7, 9\}$ je cyklická grupa generovaná prvkem 3, jež je řádu 4 ($3^4 = 1$, bráno modulo 10). Ale každý neidentický prvek grupy $U(8) = 1, 3, 5, 7$ má řád 2, tedy zde není žádný prvek řádu 4. Proto grupy $U(8)$ a $U(10)$ nejsou izomorfní.

5.1 Lagrangeova věta

Definice 5.6. Nechť G je grupa a $H \leq G$ je podgrupa. Množinu $Hg = \{hg |\ h \in H\}$ nazýváme pravou třídou rozkladu podle podgrupy $H \leq G$. Podobně $gH = \{gh |\ h \in H\}$ nazýváme levou třídou rozkladu podle podgrupy $H \leq G$. Libovolný prvek třídy Hg (gH) se nazývá reprezentant třídy rozkladu.

Příklad 5.7. Nechť $H = \{m \cdot n |\ n \in \mathbb{Z}\} \leq \mathbb{Z}\}$ je podgrupa celých čísel, které jsou násobky čísla $m > 0$. Potom $H, H + 1, H + 2, \ldots, H + m - 1$ jsou pravé třídy rozkladu. Navíc, $\mathbb{Z} = \cup_{i=0}^{m-1} H + i$.

Příklad 5.8. Nechť $\tau = (1, 2) \in S_3$ a $H = \langle \tau \rangle$. Určete množinu pravých a levých tříd rozkladu S_3 podle H. Jak je to s rovností $gH = Hg$?

Věta 5.9 (Vlastnosti tříd rozkladu)**.** *Nechť $H \leq G$ jsou grupy. Potom*

- *$Ha = Hb$ právě tehdy, když $ab^{-1} \in H$,*
- *buď $Ha \cap Hb = \emptyset$, nebo $Ha = Hb$,*
- *$G = \cup_{g \in G} Hg$ je rozkladem grupy G,*
- *počet pravých tříd rozkladu podle H se rovná počtu levých tříd rozkladu.*

Bijekce mezi pravými a levými třídami má tvar $Ha \mapsto a^{-1}H$. Přirozenější by bylo $Ha \mapsto aH$, ale to nefunguje. Proč?

Definice 5.10. Počet tříd rozkladu G podle podgrupy $H \leq G$ nazýváme index podgrupy a označujeme jej $[G : H]$.

Věta 5.11 (Lagrange)**.** *Nechť G je konečná grupa a $H \leq G$ je podgrupa. Potom $|H|$ dělí $|G|$.*

Důkaz. Ukážeme, že všechny třídy rozkladu jsou stejně velké. Nechť $f : Hg \to H$ je funkce daná $hg \mapsto h$. Toto zobrazení je prosté (injektivní), neboť $f(h_1 g) = f(h_2 g)$ implikuje $h_1 = h_2$, a rovněž surjektivní, neboť každé $h \in H$ má vzor $hg \in Hg$.

Nechť $[G : H] = m$. Potom existují reprezentanti $g_i \in G$, $i = 1, \ldots, m$ takoví, že platí $G = Hg_1 \cup \cdots \cup Hg_m$ a $Hg_i \cap Hg_j = \emptyset$ pro $i \neq j$. Proto $|G| = \sum_{i=1}^{m} |Hg_i| = \sum_{i=1}^{m} |H| = m|H|$. □

Důsledek 5.12. *Řád libovolného prvku grupy G dělí řád grupy G.*

Důsledek 5.13. *Nechť G je grupa řádu p, kde p je prvočíslo. Potom G je cyklická.*

Důkaz. Protože $p > 1$, existuje $a \in G$, $a \neq 1$. Podle Lagrangeovy věty $|a| = p$. Proto $\{a^n |\ n \in \mathbb{Z}\} = G$. □

Věta 5.14 (Fermat)**.** *Nechť p je prvočíslo a $x \in \mathbb{Z}$ je celé číslo. Potom $x^p \equiv x \pmod{p}$.*

Důkaz. Uvažujme unitární grupu $U(p) = \{1, 2, \ldots, p-1\}$ řádu $p-1$. Podle důsledku 5.12 platí, že $|x|$ dělí $p-1$. Proto $x^{p-1} = 1$. Přenásobením obou dvou stran rovnice prvkem x dostaneme $x^p = x$ v $U(p)$. Grupa $U(p)$ je však izomorfní grupě zbytkových tříd $\{[1], [2], \ldots, [p-1]\}$ s násobením definovaným následovně: $[a] \cdot [b] = [ab]$. Proto rovnice $x^p = x$ v $U(p)$ implikuje $[x]^p = [x^p] = [x]$. Poslední rovnost je ekvivalentní s $x^p \equiv x \pmod{p}$. □

Cvičení

5.17. Nechť G je konečná grupa, $K \leq H \leq G$. Dokažte $[G : K] = [G : H][H : K]$.

5.18. Nechť $|a| = mk$. Dokažte, že $|a^k| = m$.

5.19. Dokažte, že grupa sudého řádu má lichý počet prvků řádu 2.

5.20. Nechť $a, b \in G$ komutují a nechť $a^n = 1 = b^m$. Potom $(ab)^d = 1$, kde $d = \operatorname{lcm}(n, m)$.

5.21. Nechť $A, B \in GL(2, \mathbb{Q})$ jsou matice

$$A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad B = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}.$$

Dokažte, že řády A a B jsou konečné, ale řád AB je nekonečný.

5.22. Dokažte, že dvě cyklické grupy jsou izomorfní právě tehdy, když mají stejný řád.

5.23. Nechť φ je Eulerova funkce. Dokažte, že pokud $\gcd(r, s) = 1$, je $s^{\varphi(r)} = 1 \pmod{r}$.

5.24. Dokázali jsme, že každá cyklická grupa G má pro každého dělitele d řádu G právě jednu cyklickou podgrupu řádu d. Dá se tato implikace obrátit?

Zkuste dokázat: Pokud G má pro každého dělitele $d \mid |G|$ nejvíce jednu podgrupu řádu d, je grupa G cyklická.

5.25. Kolik řešení má rovnice $x^d = 1$ v cyklické grupě řádu dk?

5.26. Nechť $H \subset G$ má index 2. Dokažte, že $a^2 \in H$ pro všechny prvky $a \in G$.

5.27. Nechť $H = \{(1), (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\}$. Nalezněte levou třídu rozkladu H v A_4. Kolik těchto tříd existuje?

5.28. Nechť $H = \{\pm 0, \pm n, \pm 2n, \pm 3n, \dots\}$, kde n je přirozené číslo. Nalezněte všechny levé rozkladové třídy H.

5.29. Nalezněte všechny levé rozkladové třídy množiny $\{1, 11\}$ v $U(30)$.

5.30. Nechť $a, b \neq id$ jsou prvky různého řádu v grupě G řádu 155. Dokažte, že jediná podgrupa grupy G, která obsahuje oba prvky a, b, je samotná grupa G.

5.31. Nechť G je grupa řádu 60. Podgrupy jakého řádu mohou existovat?

5.32. Předpokládejme, že K je vlastní podgrupa grupy H a grupa H je vlastní podgrupa grupy G. Jestliže $|K| = 42$ a $|G| = 420$, určete $|H|$. Nalezněte všechny možnosti.

5.33. Nechť G je grupa řádu pq, kde p a q jsou prvočísla. Dokažte, že každá vlastní podgrupa grupy G je cyklická.

5.34. Předpokládejme, že H a K jsou podgrupy grupy G. Jestliže $|H| = 12$ a $|K| = 35$, určete $|H \cap K|$. Zobecněte.

5.35. Nechť G je konečná grupa řádu n a m je nesoudělné s n. Pokud $g \in G$ a $g^m = id$, dokažte, že $g = id$.

5.36. Nechť H je podgrupa grupy S_4 a H obsahuje prvky $(1, 2)$ a $(2, 3, 4)$. Dokažte, že $H = S_4$.

5.37. Nechť G je abelovská grupa s lichým počtem prvků. Ukažte, že součinem všech prvků grupy G dostaneme identitu.

5.38. Předpokládejme, že G je grupa s více než jedním prvkem a G nemá žádnou vlastní netriviální podgrupu. Dokažte, že $|G|$ je prvočíslo.

5.39. Nechť $|G| = 15$. Jestliže má grupa G právě jednu podgrupu řádu 3 a právě jednu podgrupu řádu 5, dokažte, že grupa G je cyklická. Pokuste se zobecnit pro $|G| = pq$, kde p, q jsou prvočísla.

5.40. Nechť $|G| = 8$. Ukažte, že grupa G musí obsahovat prvek řádu 2.

5.41. Může grupa řádu 55 obsahovat právě dvacet prvků řádu 11? Své rozhodnutí zdůvodněte.

5.42. Nechť G je grupa řádu p^n, kde p je prvočíslo. Dokažte, že centrum grupy G nemůže být řádu p^{n-1}.

5.43. Nechť $G = GL(2, \mathbb{R})$ a $H = SL(2, \mathbb{R})$. Nechť $\mathbb{A} \in G$ a předpokládejme, že $\det \mathbb{A} = 2$. Ukažte, že $\mathbb{A}H$ je množina matic 2×2 v G mající determinant 2.

5.44. Nechť G je grupa s méně než sto prvky obsahující podgrupy řádu 10 a 25. Určete řád grupy G.

Nápověda k vybraným cvičením

5.22 Ukažte, že řád matice $\mathbb{A}$ je 4, řád matice $\mathbb{B}$ je 3 a dále dokažte (matematickou indukcí), že $(\mathbb{AB})^j = \begin{pmatrix} 1 & j \\ 0 & 1 \end{pmatrix}$.

5.23 Použijte $|U(n)| = \varphi(n)$.

5.27 Protože $|A_4| = 12$ a $|H| = 4$, existují právě tři levé třídy rozkladu. Ukažte, že se jedná o H, $(1,2,3)H$ a $(1,2,4)H$.

5.28 Všimněme si, že $H = \langle n \rangle$. V prvním kroku ukažte, že $H, 1 + H, 2 + H, \ldots, (n-1) + H$ jsou navzájem různé levé rozkladové třídy grupy G. Ve druhém kroku určete, že jsou opravdu všechny.

5.37 Z Lagrangeovy věty víme, že žádný prvek grupy G nemůže mít řád 2 (řád grupy je liché číslo, které dvojka nedělí). Jaké prvky jsou rovny svému inverznímu prvku?

5.38 Grupa G může být jak konečná, tak nekonečná, nezapomeňte!

Řešení vybraných cvičení

5.29 Grupa $U(30) = \{1, 7, 11, 13, 17, 19, 23, 29\}$ má osm prvků, a tedy existují čtyři levé rozkladové třídy množiny $\{1, 11\}$, a to konkrétně: $H = \{1, 11\}, 7H = \{7 \cdot 1, 7 \cdot 11\} = \{7, 11\}, 13H = \{13 \cdot 1, 13 \cdot 11\} = \{13, 23\}$ a $19H = \{19 \cdot 1, 19 \cdot 11\} = \{19, 29\}$.

5.30 Z Lagrangeovy věty musí pro podgrupu H grupy G platit, že $|H| = 5, 31$ nebo 155. Pokud $|H| = 5$, je grupa G cyklická a všechny prvky kromě identity jsou stejného řádu 5. Taktéž pro případ $|H| = 31$. A proto $|H| = 155$, a tedy $H = G$.

5.35 Protože $g^m = id$, $|g|$ dělí m a také $|g|$ dělí $|G| = n$. Tedy g je společný dělitel čísel m a n, což je 1. Proto $|g| = 1$ a $g = id$.

5.36 To, že $(2,3,4) \in H$ a $(1,2) \in H$ znamená, že i $(2,3,4)(1,2) \in H$. A protože $(2,3,4)(1,2) = (1,3,4,2)$, je v H trojcyklus, jehož řád je 3, i čtyřcyklus, jehož řád je 4, a proto řád grupy H musí být dělitelný 3 i 4 (protože H je podgrupa grupy S_4). Z toho vyplývá, že $|H| = 12$ nebo 24. Jediná podgrupa grupy S_4 mající řád 12, je grupa A_4. Protože ale $(1,2) \notin A_4$, musí mít grupa H řád 24. A tedy $H = S_4$.

5.39 Uvědomme si, že řád každého prvku $a \neq id$ z grupy G je 3, 5 nebo 15. Nechť $A = \{x \in G; |x| = 3\}$ a $B = \{y \in G; |y| = 5\}$. Pro $b \in A$ je $\langle b \rangle = \{id, b, b^2\}$ podgrupa řádu 3. Protože existuje právě jedna podgrupa řádu 3, je $A = \{b, b^2\}$ a $|A| = 2$. Podobně pro $c \in B$: $\langle c \rangle = \{id, c, c^2, c^3, c^4\}$ je jediná podgrupa řádu 5, a tedy $|B| = 4$. Z toho vyplývá, že v G je $15 - 2 - 4 - 1 = 8$ prvků řádu 15 (jednička je identita). A protože v G existuje prvek řádu 15, je grupa G cyklická. Obdobně pro obecné tvrzení.

5.2 Normální podgrupy

Definice 5.15. Nechť $S, T \subseteq G$ jsou neprázdné podmnožiny grupy G. Označme $ST = \{st; s \in S, t \in T\} \leq G$.

Věta 5.16 (Součinová věta)**.** *Jsou-li S a T podmnožiny konečné grupy, platí $|ST||S \cap T| = |S||T|$.*

Důkaz. Pravá strana rovnice, kterou máme dokázat, je počet prvků kartézského součinu $S \times T$. Rovnost dokážeme tak, že zkonstruujeme surjekci $\varphi\colon S \times T \to ST$ s vlastností $|\varphi^{-1}(x)| = |S \cap T|$. Pro $x = (s,t) \in S \times T$ položíme $\varphi(s,t) = st$. Tvrdíme, že pro $y_0 = st$ platí

$$\varphi(y_0)^{-1} = \{(sd, d^{-1}t); d \in S \cap T\} = M.$$

Pokud $x = (sd, d^{-1}t) \in M$, $\varphi(x) = st = y_0 \in ST$. Proto $M \subseteq \varphi(y_0)^{-1}$. Nechť $x = (\sigma, \tau) \in \varphi^{-1}(y_0)$. Potom $\sigma\tau = st$. Označme $d = s^{-1}\sigma = t\tau^{-1} \in S \cap T$. Máme $(\sigma, \tau) = (sd, d^{-1}t) \in M$, a odtud $\varphi(y_0)^{-1} \subseteq M$. □

Definice 5.17. Podgrupa $K \leq G$ se nazývá normální, značíme $K \lhd G$, platí-li $gKg^{-1} = K$.

Lemma 5.18. *Jádro homomorfismu $\varphi\colon G \to H$ je normální podgrupa.*

Lemma 5.19. *Je-li $K \lhd G$ normální, pro každé $x \in G$ platí $xK = Kx$. Odtud dostaneme, že množiny levých a pravých tříd rozkladu podle normální podgrupy se rovnají.*

Definice 5.20. Nechť $a \in G$. Zobrazení $\gamma_a\colon x \mapsto axa^{-1}$ nazýváme konjugace prvkem x.

Lemma 5.21. *Konjugace prvkem a je automorfismus grupy G.*

S konjugací jsme se již střetli v lineární algebře, kde konjugace odpovídá relaci podobnosti regulárních matic dimenze n nad daným polem F.

Věta 5.22 (Faktorová grupa)**.** *Pokud $N \lhd G$ je normální, množina pravých tříd podle N s operací $Nx \cdot Ny = Nxy$ tvoří grupu G/N. Řád grupy G/N je $[G : N]$.*

Důkaz. Potřebujeme ověřit, že operace je dobře definovaná. Máme $NxNy = Nxx^{-1}Nxy = NNxy = Nxy$. Tedy součin tříd rozkladu je třída. Zřejmě neutrální prvek je třída $N = N1$ a $(Nx)^{-1} = Nx^{-1}$. □

Lemma 5.23. *Nechť $N \lhd G$. Přirozená projekce $\nu\colon x \mapsto Nx$ je homomorfismus $G \to G/N$ s jádrem N.*

Příklad. V komutativní grupě jsou všechny podgrupy normální. Proto každá podgrupa definuje faktorovou grupu. Podgrupy grupy $(Z,+)$ mají tvar $n \cdot Z$. Faktorová grupa $Z/nZ \cong (Z_n,+)$.

Definice 5.24. Pokud $a,b \in G$ jsou prvky, prvek $[a,b] = aba^{-1}b^{-1}$ nazveme komutátor a,b. Komutátorová podgrupa grupy G, značíme G', je grupa generovaná všemi komutátory.

Věta 5.25. *Platí $G' \lhd G$. Navíc, je-li $N \lhd G$, je G/N abelovská právě tehdy, když $G' \leq N$.*

Důkaz. Nechť $f : G \to G$ je homomorfismus. Potom $f[a,b] = f(aba^{-1}b^{-1}) = f(a)f(b)f(a)^{-1}f(b)^{-1} = [f(a),f(b)]$. Odtud vyplývá, že každá konjugace permutuje množinu komutátorů. Proto $G' \lhd G$.

Nechť $N \lhd G$. Pokud $G' \leq N$, platí $[xN,yN] = [x,y]N = N$. Proto G/N je abelovská. A naopak, pokud G/N, platí $[x,y]N = [xN,yN] = N$, a proto každý komutátor se nachází v N. Odtud $G' \leq N$. □

Cvičení

5.45. Mějme množinu podgrup $\{S_i; i \in I\}$ grupy G a označme $D = \cap_{i\in I} S_i$. Nechť $\{S_it_i; i \in I\}$ je množina pravých tříd. Potom $\cap_{i\in I} S_it_i = \emptyset$ nebo existuje $g \in G$ takové, že $\cap_{i\in I} S_it_i = Dg$. Dokažte!

5.46. Dokažte, že pokud $S \leq G$ a $[G:S] = 2$, je $S \lhd G$.

5.47. Grupa kvaternionů. Nechť $G = \langle A,B\rangle \leq GL(2,\mathbb{C})$, kde

$$A = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}, B = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix},$$

je neabelovská grupa řádu 8 s jedinou podgrupou řádu 2.

Dokažte, že v grupě kvaternionů je každá podgrupa normální.

5.48. Dokažte, že $A_n \lhd S_n$.

5.49. Nechť $K \leq H \leq G$ a nechť $K \lhd G$. Potom $K \lhd H$.

5.50. Najděte příklad $K \lhd H \lhd G$, kde ale K není normální v G.

5.51. Dokažte, že pokud $N \lhd G$ je normální podgrupa indexu n, pro každé $g \in G$ platí $g^n \in H$. Najděte příklad, že pro podgrupu indexu n, která není normální, takovéto tvrzení neplatí.

5.52. Nechť $H = \{(1),(1,2)\}$. Je grupa H normální podgrupa grupy S_3?

5.53. Nechť $H = \{\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}; a,b,d \in \mathbb{R}, ad \neq 0\}$. Je H normální podgrupou grupy $GL(2,\mathbb{R})$?

5.54. Grupy $\langle 3\rangle$ a $\langle 12\rangle$ jsou podgrupy grupy $\mathbb{Z}$. Dokažte, že $\langle 3\rangle/\langle 12\rangle$ je izomorfní s $\mathbb{Z}_4$. Pokuste se zobecnit.

5.55. Dokažte, že faktorová grupa cyklické grupy je cyklická.

5.56. Nechť H je normální podgrupa G. Pokud H a G/H jsou abelovské, musí i grupa G být abelovská?

5.57. Dokažte, že faktorová grupa abelovské grupy je abelovská.

5.58. Určete řád prvku $14 + \langle 8 \rangle$ ve faktorové grupě $\mathbb{Z}_{24}/\langle 8 \rangle$. Zobecněte.

5.59. Určete řád faktorgrupy $\mathbb{Z}_{60}/\langle 15 \rangle$.

5.60. Zkonstruujte Cayleyho tabulku pro $U(20)/U_5(20)$.

5.61. Dokažte, že abelovská grupa řádu 33 je cyklická.

5.62. Určete řády dvou grup: $(\mathbb{Z} \oplus \mathbb{Z})/\langle (2,2) \rangle$ a $(\mathbb{Z} \oplus \mathbb{Z})/\langle (4,2) \rangle$. Jsou grupy cyklické?

5.63. Nechť $G = U(16), H = \{1, 15\}$ a $K = \{1, 9\}$. Jsou grupy H a K izomorfní? A jsou izomorfní faktorgrupy G/H a G/K?

5.64. Dokažte, že centralizátor normální podgrupy je v této grupě rovněž normální.

5.65. Na příkladu, v němž $a, b \neq id$, ukažte, že se ve faktorové grupě G/H může stát, že $aH = bH$, ale $|a| \neq |b|$.

5.66. Nechť N a M jsou normální podgrupy grupy G. Dokažte, že NM je v grupě G rovněž normální.

5.67. Nechť $|G| = 30$ a $|Z(G)| = 5$. Jaká bude struktura faktorové grupy $G/Z(G)$?

5.68. Ukažte, že grupa A_5 nemůže obsahovat normální podgrupu řádu 2.

Nápověda k vybraným cvičením

5.47 Grupa kvaternionů je grupa $Q_8 = \langle -1, i, j, k; (-1)^2 = 1, i^2 = j^2 = k^2 = ijk = -1 \rangle$. Dále $\langle -1 \rangle = \{1, -1\}$, $\langle i \rangle = \{1, i, -1, -i\}$, $\langle j \rangle = \{1, j, -1, -j\}$ a $\langle k \rangle = \{1, k, -1, -k\}$. Nyní pro každou z těchto podgrup ukažte, že je normální, tj. (například pro podgrupu $\langle i \rangle$) ověřte, že $xix^{-1} \in \langle i \rangle$ pro všechny prvky $x \in Q_8$.

5.50 Pracujte s $G = S_4$ a $H = \langle (1,2)(3,4) \rangle$. Podgrupu K nalezněte.

5.52 Porovnejte $(1,3)H$ a $H(1,3)$.

5.62 Pro $(1,0) \in (\mathbb{Z} \oplus \mathbb{Z})$ pro všechna $m > 0$ platí: $m(1,0) = (m,0) \notin \langle (2,2) \rangle$. Z toho vyplývá, že $m((1,0) + \langle (2,2) \rangle) \neq \langle (2,2) \rangle$ pro všechna $m > 0$. Takže $|(1,0) + \langle (2,2) \rangle| = \infty$, a tedy $|(\mathbb{Z} \oplus \mathbb{Z})/\langle (2,2) \rangle| = \infty$. Dále

$$2((1,1) + \langle (2,2) \rangle) = (2,2) + \langle (2,2) \rangle = \langle (2,2) \rangle.$$

Tedy $|(1,1) + \langle (2,2) \rangle| = 2$. Co plyne z toho, že jsme v nekonečné grupě nalezli prvek konečného řádu? Obdobně pro druhý případ.

Řešení vybraných cvičení

5.46 Máme tedy dvě levé rozkladové třídy: $1S = S$ a aS a máme rovněž dvě pravé rozkladové třídy: $S1 = S$ a Sb. Sjednocením S a aS (resp. S a Sb) dostaneme celou grupu G. Tedy $aS = G \setminus S = Sb$.

Pokud $x \in S$, je $xS = S = Sx$. Pokud $x \notin S$, je $xS = G \setminus S = Sx$. V obou dvou případech se levé rozkladové třídy rovnají pravým rozkladovým třídám, a tedy podgrupa S je normální.

5.55 Nechť $G = \langle a \rangle$ a $N \lhd G$. Potom jakýkoliv prvek v grupě G/N je ve tvaru $a^k N$, což je $(aN)^k$ pro nějaké $k \in \mathbb{Z}$. Tedy $G/N = \langle aN \rangle$, a tedy G/N je cyklická grupa.

5.58

$$\begin{aligned} 14 + \langle 8 \rangle &= 6 + \langle 8 \rangle \\ 2 \cdot (6 + \langle 8 \rangle) &= 12 + \langle 8 \rangle = 4 + \langle 8 \rangle \\ 3 \cdot (6 + \langle 8 \rangle) &= 18 + \langle 8 \rangle = 2 + \langle 8 \rangle \\ 4 \cdot (6 + \langle 8 \rangle) &= 24 + \langle 8 \rangle = \langle 8 \rangle \end{aligned}$$

A tedy $|14 + \langle 8 \rangle| = 4$.

5.67 Z velikosti grupy G a jejího centra plyne, že $|G/Z(G)| = 6$. Všechny grupy řádu 6 jsou izomorfní s grupou S_3 nebo grupou $\mathbb{Z}/6\mathbb{Z}$. Rovněž víme, že pokud $G/Z(G)$ je cyklická, je G abelovská. Pokud $G/Z(G) \cong \mathbb{Z}/6\mathbb{Z}$, je G abelovská. To je ale spor s velikostí centra ($|Z(G)| = 5$). A proto $G/Z(G)$ je izomorfní s grupou S_3.

5.3 Věty o izomorfismu

Věta 5.26 (1. věta o izomorfismu: každý homomorfismus odpovídá přirozené projekci)**.** *Pokud $f\colon G \to H$ je homomorfismus, $Im(f) \cong G/\ker(\varphi)$.*

Důkaz. Označme $K = \ker(\varphi)$ a nechť $\phi\colon G/K \to H$ je zobrazení $\varphi\colon Ka \mapsto \varphi(a)$.

Nejprve dokážeme, že φ je dobře definované: pokud $Ka = Kb$, platí $f(a) = \varphi(Ka) = \varphi(Kb) = f(b)$. Rovnost $Ka = Kb$ implikuje $Kab^{-1} = K$. Odtud $1 = \varphi(K) = \varphi(Kab^{-1}) = f(ab^{-1}) = f(a)f^{-1}(b)$. A proto $f(a) = f(b)$.

Dále potřebujeme dokázat, že φ je homomorfismus. Máme

$$\varphi(KaKb) = \varphi(Kab) = f(ab) = f(a)f(b) = \varphi(Ka)\varphi(Kb).$$

Abychom dokázali, že tento homomorfismus je injektivní, stačí dokázat, že $\ker(\varphi) = K$. Nechť $\varphi(Ka) = f(a) = 1$. Odtud $a \in K$, a proto $Ka = K$. □

Lemma 5.27. *Nechť S, T jsou podgrupy G. Pokud je jedna z nich normální, platí $ST = TS$. Speciálně, ST je podgrupa G. Pokud obě dvě jsou normální podgrupy, je $ST \lhd G$ normální.*

Důkaz.

$$s_1t_1(s_2t_2)^{-1} = s_1(t_1t_2^{-1})s_2^{-1} = s_1s_2^{-1}(s_2(t_1t_2^{-1})s_2^{-1}) = s_1s_2^{-1}t' \in ST.$$

Proto $ST \leq G$. A podobně

$$(t_1s_1)^{-1}t_2s_2 = s_1^{-1}t_1^{-1}t_2s_2 = s_1^{-1}(t_1^{-1}t_2)s_1s_1^{-1}s_2 = t's_1s_1^{-1}s_2 \in TS.$$

Proto $TS \leq G$. Vzhledem k tomu, že $S \leq ST$, $T \leq ST$ a ST, TS jsou grupy, platí $TS \leq ST$ i $ST \leq TS$. A proto $ST = TS$. □

Věta 5.28 (2. věta o izomorfismu)**.** *Nechť $N \lhd G$ a $T \leq G$. Potom $N \cap T \lhd T$ a $T/(N \cap T) \cong NT/N$.*

Důkaz. Uvažujme přirozenou projekci $\nu\colon G \to G/N$ s jádrem N. Potom restrikce $\nu' = \nu|_T$ je homomorfismus s jádrem $\ker(\nu') = N \cap T$. Podle první věty o izomorfismu je $T/(N \cap T) \cong \mathrm{Im}(\nu')$. Jenže $\mathrm{Im}(\nu') = \{Nt;\ t \in T\} = NT/N$. □

Věta 5.29 (3. věta o izomorfismu)**.** *Nechť $K \leq H \leq G$, kde $K \lhd G$ i $H \lhd G$. Potom $H/K \lhd G/K$ a platí $(G/K)/(H/K) \cong G/H$.*

Důkaz. Definujme $\varphi\colon G/K \to G/H$ předpisem $Ka \mapsto Ha$. Je to epimorfismus s jádrem H/K. Z 1. věty o izomorfismu dostáváme $G/H = \mathrm{Im}(\varphi) \cong (G/K)/(H/K)$. □

Věta 5.30 (Věta o korespondenci)**.** *Nechť $K \lhd G$ a nechť ν je přirozená projekce. Potom přiřazení $S \mapsto \nu(S) = S/K = S^*$ je bijekce mezi množinou $\{S \leq G;\ K \leq S\}$ a množinou všech podgrup G/K. Navíc platí*

- *$K \leq T \leq S$ právě tehdy, když $T^* \leq S^*$ a $[S : T] = [S^* : T^*]$,*
- *$K \leq T \lhd S$ právě tehdy, když $T^* \lhd S^*$ a $S/T \cong S^*/T^*$.*

Poznámka: Tuto větu můžeme interpretovat tak, že funkce $S \to S^*$ je izomorfismem mezi svazem podgrup grupy G, které obsahují K, a svazem všech podgrup faktorové grupy G/K. Podobně pro svazy normálních podgrup.

Důkaz. Nejprve dokážeme, že $\nu^*\colon S \mapsto S/K = S^*$ je injektivní. Předpokládejme, že $S/K = T/K$. Potom ke každému $s \in S$ existuje $t \in T$ takové, že $sK = tK$. Odtud $s = tk \in T$. Proto $S \leq T$. Z principu symetrie i $T \leq S$, a tedy $S = T$.

Dále dokážeme, že ν^* je surjekce. Nechť $A \leq G/K$ je podgrupa. Uvažujme $S = \nu^{-1}(A)$. Vezměme $x, y \in S$. Potom $xK, yK \in A$ a $xKyK = xyK \in A$. Proto $xy \in \nu^{-1}(A) = S$. Podobně pro $x \in S$, $xK \in A$. Ale A je grupa, takže $(xK)^{-1} = x^{-1}K \in A$, proto $x^{-1} \in S$.

Nakonec ověříme, že $\nu(S) = S/K = \nu^*(\nu^*)^{-1}(A) \subseteq A$, ale ν^* je surjekce, a proto $\nu^*(S) = A$.

DOKONČIT! □

Cvičení

5.69. Vzpomeňme na znaménko permutace α označované jako $\mathrm{sgn}(\alpha)$. Dokažte, že zobrazení sgn je homomorfismus z G do multiplikativní grupy $\{+1, -1\}$ a určete jádro homomorfismu.

5.70. Najděte homomorfismus z dihedrální grupy D_n do grupy $\{+1, -1\}$ a určete jádro tohoto homomorfismu.

5.71. Dokažte, že homomorfismus $f : G \to H$ je injektivní (prosté) zobrazení právě tehdy, když $ker(f) = 1$.

5.72. Nechť A, B, C jsou podgrupy grupy G a nechť $A \leq B$. Pokud $A \cap C = B \cap C$ a $AC = BC$, je $A = B$.

(Nepředpokládejme, že buď AB, nebo BC je podgrupa.)

5.73. Nechť H, K, L jsou podgrupy grupy G a nechť $H \leq L$. Pak $HK \cap L = H(K \cap L)$.

(Nepředpokládejme, že buď HK, nebo $H(K \cap L)$ je podgrupa.)

Nápověda k vybraným cvičením

5.70 Nechť máme prvek $x \in D_n$. Dokažte, že zobrazení $\Phi(x)$ definované

$$\Phi(x) = \begin{cases} +1, & \text{pokud } x \text{ je rotace;} \\ -1, & \text{pokud } x \text{ je reflexe} \end{cases}$$

je oním homomorfismem.

Řešení vybraných cvičení

5.71 Nejprve předpokládejme, že homomorfismus $f : G \to H$ je injektivní. Dále víme, že identita $id \in G$ se zobrazí na identitu $id' \in H$, tzn. $f(id) = id'$. Pokud $g \in ker(f)$, dostaneme $f(g) = id'$, a tedy $f(g) = f(id)$. Protože f je injektivní zobrazení, musí platit, že $g = id$, a tedy $ker(f) = \{id\}$.

Nyní dokážeme opačnou implikaci. Předpokládejme, že $ker(f) = \{id\}$. Pakliže g_1 a g_2 jsou dva prvky grupy G takové, že $f(g_1) = f(g_2)$, postupnými úpravami dostáváme (přičemž využíváme faktu, že f je homomorfismus):

$$f(g_1 g_2^{-1}) = f(g_1) f(g_2^{-1}) = f(g_1) f(g_2)^{-1} = f(g_1) f(g_1)^{-1} = id'.$$

A tedy $g_1 g_2^{-1} \in ker(f) = \{id\}$, a tudíž $g_1 g_2^{-1} = id$. Z toho již vyplývá, že $g_1 = g_2$, a tedy f je injektivní zobrazení.

Kapitola 6

Přímý součin grup

Nechť H a K jsou grupy. Potom přímý součin je grupa $H \times K$ definovaná na množině všech uspořádaných dvojic (h, k), kde $h \in H$ a $k \in K$ s binární operací definovanou po složkách: $(h_1, k_1)(h_2, k_2) = (h_1h_2, k_1k_2)$.

Zřejmě přiřazení $h \mapsto (h, 1)$ a $k \mapsto (1, k)$ jsou monomorfismy $H \to H \times K$ a $K \to H \times K$. Obráceně, projekce $p_1 \colon (h, k) \to h$ a $p_2 \colon \to k$ na první a druhou složku jsou epimorfismy $H \times K \to H$ a $H \times K \to K$. Všimněme si rovněž, že zobrazení $(h, k) \mapsto (k, h)$ je izomorfismus $H \times K \to K \times H$, tedy $H \times K \cong K \times H$.

Lemma 6.1. *Grupy $H \times 1_K \cong H$ a $1_H \times K \cong K$ jsou normální podgrupy přímého součinu splňující $(H \times 1_K) \cap (1_H \times K) = \{(1_H, 1_K)\} = 1_{H \times K}$.*

Důkaz. Jádro $\ker(p_1) = 1_H \times K$ a jádro $\ker(p_2) = H \times 1_K$. Podle 1. věty o izomorfismu platí $1_H \times K \lhd H \times K$ a $H \times 1_K \lhd H \times K$. Druhá část tvrzení je triviální.

Zajímavou otázka je, zda je možné tvrzení předchozího lemma obrátit. Ukazuje se, že to možné je. Dostáváme tak následující rozkladovou větu. □

Věta 6.2. *Nechť grupa G obsahuje dvě normální podgrupy $H \lhd G$ a $K \lhd G$ takové, že $H \cap K = 1$ a $HK = G$. Potom $G \cong H \times K$.*

Důkaz. Protože $G = HK$, tak každý prvok $a \in G$ se dá vyjádřit v tvaru $a = hk$, kde $h \in H$ a $k \in K$. Tvrdíme, že toto vyjádření je jednoznačné. Dokazujme sporem. Nechť a se dá navíc vyjádřit takto $a = h_1k_1$, kde $h_1 \in H$ a $k_1 \in K$. Potom $hk = a = h_1k_1$, a po úpravě $h_1^{-1}h = k^{-1}k_1 \in H \cap K = 1_G$. Proto $k_1 = k$ a $h_1 = h$. Uvažujme funkci $f \colon G \to H \times K$ danou předpisem $f(a) = f(hk) = (h, k)$. Z předešlého vyplývá, že f je dobře definovaná. Chceme dokázat, že f je hledaný izomorfismus. Nejdříve dokážeme, že f je homomorfismus. Chceme, aby platilo, že $f(ab) = f(a)f(b)$. Vzhledem k tomu, že $f(ab) = f(h_1k_1h_2k_2)$, potřebujeme, aby $k_1h_2 = h_2k_1$. Uvažujme komutátor $[h_2, k_1] = h_2k_1h_2^{-1}k_1^{-1} = (h_2k_1h_2^{-1})k_1^{-1} \in K$, ale aj $[h_2, k_1] = h_2(k_1h_2^{-1}k_1^{-1}) \in H$. Protože $H \cap K = 1$,

tak $[h_2, k_1] = 1$. Odtud $h_2k_1 = k_1h_2$. Potom platí

$$f(ab) = f(h_1k_1h_2k_2) = f(ab) = f(h_1h_2k_1k_2) = f(h_1h_2)f(k_1k_2) = f(a)f(b).$$

Triviálně f je surjektivní. Pro $a = hk \in \ker(f)$ platí $f(hk) = (h, k) = (1, 1)$. Proto $h = 1$ i $k = 1$, a tedy $a = 1$. Odtud je f injektivní.

Žádný z předpokladů nemůžeme vynechat. Uvažujme například podgrupy $H = \langle(1, 2, 3)\rangle \leq S_3$ a $K = \langle(1, 2)\rangle \leq S_3$. Platí $H \lhd S_3$, $H \cap K = 1$, ale S_3 není izomorfní $H \times K \cong Z_3 \times Z_2$. □

Věta 6.3. *Nechť $A \lhd H$, $B \lhd K$. Potom $A \times B \lhd H \times K$ a platí $(H/A) \times (K/B) \cong (H \times K)/(A \times B)$.*

Důkaz. Definujme epimorfismus $H \times K \to (H/A) \times (K/B)$ předpisem $(h, k) \mapsto (hA, kB)$. Nechť $a \in A$, $b \in B$. Vzhledem k tomu, že $f(a, b) = f(aA, bB) = (A, B) = (1_{H/A}, 1_{H/B}) = 1_{H/A \times H/B}$, jádro epimorfismu f je grupa $A \times B$. Z toho vyplývá, že $A \times B \lhd H \times K$. Dále pak použijeme 1. větu o izomorfismu. □

Cvičení

6.1. Dokažte, že pokud $\gcd(m, n) = 1$, je $Z_{mn} \cong Z_m \times Z_n$.

6.2. Dokažte, že abelovská grupa řádu p^2, kde p je prvočíslo, je buď cyklická, nebo je izomorfní s $Z_p \times Z_p$.

6.3. Najděte příklad grupy G a $H \lhd G$ takový, že G neobsahuje podgrupu izomorfní s G/H.

6.4. Definujte přímý součin tří a více grup. Pokuste se zformulovat tvrzení analogické větě 6.2 pro vícenásobné součiny.

6.5. Nechť V je n-dimenzionální vektorový prostor nad polem F. Dokažte, že pro aditivní grupu $V = (V, +)$ platí $V = F_1 \times F_2 \times \cdots \times F_n$, kde $F_i \cong (F, +)$.

6.6. Dokažte, že grupu D_4 nelze vyjádřit přímým součinem dvou vlastních podgrup.

6.7. Nechť H, K jsou podgrupy grupy G. Pokud $G = HK$ a $g = hk$, kde $g \in G, h \in H$ a $k \in K$, existuje nějaký vztah mezi $|g|, |h|$ a $|k|$? A co když $G = H \times K$?

6.8. V grupě $\mathbb{Z}$ nechť $H = \langle 5\rangle$ a $K = \langle 7\rangle$. Dokažte, že $\mathbb{Z} = HK$. Je $\mathbb{Z} = H \times K$?

Nápověda k vybraným cvičením

6.3 Příkladem může být kvaternionová grupa $Q_8 = G$ a grupa $\{-1, 1\} = H$. Určete grupu Q_8/H. S jakou známou grupou je tato grupa izomorfní? Zapište grupy Q_8 a Q_8/H Cayleyho tabulkou a grupovou reprezentací.

Řešení vybraných cvičení

6.1 Uvažujme prvek $(1,1) \in \mathbb{Z}_{mn}$. Pokud $k(1,1) = (0,0)$, musí být k násobkem m i n, a tedy $\operatorname{lcm}(m,n)$ dělí k. Protože $\gcd(m,n) = 1$, je $\operatorname{lcm}(m,n) = mn$. A proto $|\langle(1,1)\rangle| = mn = |\mathbb{Z}_m \times \mathbb{Z}_n|$. A tedy grupa $\mathbb{Z}_m \times \mathbb{Z}_n$ je rovněž cyklická grupa a je izomorfní s grupou $\mathbb{Z}_{mn}$.

6.6 Pokud $D_4 = H \times K$, pak protože $|D_4| = 8$, je $|H| = 4$ a $|K| = 2$ (nebo naopak). Pak $K \cong \mathbb{Z}_2$ a $H \cong \mathbb{Z}_4$ nebo $\mathbb{Z}_2 \oplus \mathbb{Z}_2$. Ať tak či tak, obě podgrupy K i H jsou abelovské. Protože $D_4 = H \times K \cong H \oplus K$, grupa D_4 musí být rovněž abelovská. Protože ale grupa D_4 abelovská není, nelze ji vyjádřit přímým součin dvou vlastních podgrup.

Kapitola 7

Akce grup

7.1 Konjugace

Definice 7.1. Dva prvky $a, b \in G$ se nazývají konjugované, jestliže existuje prvek $g \in G$ takový, že $b = gag^{-1}$. Konjugace je relace ekvivalence. Třídu ekvivalence konjugace obsahující prvek a budeme označovat a^G.

Zřejmě $a^G = \{gag^{-1};\ g \in G\}$.

Definice 7.2. Centrum grupy G, značíme $Z(G)$, je podgrupa těch prvků, které komutují se všemi prvky grupy G, $Z(G) \lhd G$. Centralizátor $C_G(a)$ prvku a je podgrupa těch prvků $g \in G$, které komutují s a.

Věta 7.3. *Pro každé $a \in G$ platí $|a^G| = [G : C_G(a)]$. Navíc, je-li G konečná, $|a^G|$ dělí řád G.*

Důkaz. Definujme funkci $f\colon a^G \to G/C_G(a)$ předpisem $gag^{-1} = gC$. Dokážeme, že f je dobře definovaná bijekce. Pokud $hah^{-1} = gag^{-1}$, platí $g^{-1}hah^{-1}g = a$. Proto $g^{-1}h, h^{-1}g \in C$. Odtud $g = gc^{-1}$ pro nějaké $c \in C$. Potom

$$f(hah^{-1}) = f(gc^{-1}acg^{-1}) = gc^{-1}C = gC.$$

A tedy f je dobře definovaná.

Nechť $x = gag^{-1}$, $y = hah^{-1}$ a nechť $f(x) = f(y)$. Potom $gC = hC$ a máme $h = gc$ pro nějaké $c \in C$. Odtud $y = hah^{-1} = gcac^{-1}g^{-1} = gag^{-1} = x$. Proto f je injektivní. Zřejmě f je i surjektivní.

Druhá část tvrzení je důsledkem Lagrangeovy věty. □

Definice 7.4. Vzhledem k tomu, že konjugace prvkem je automorfismus grupy, pokud $H \leq G$ je podgrupa, potom $H^a = aHa^{-1} \leq G$ je rovněž podgrupa. Potom $N_G(H) = \{a \in G;\ H^a = H\}$ je podgrupa G, kterou nazýváme normalizátor podgrupy H v grupě G. Normalizátor H je maximální podgrupa $K \leq G$ taková, že $H \lhd K \leq G$.

Věta 7.5. *Pro každou podgrupu $H \leq G$ platí $|H^G| = [G : N_G(H)]$. Navíc, pokud je G konečná, $|H^G|$ dělí řád G.*

Důkaz. Definujme funkci $f\colon H^G \to G/N$ předpisem $H^g \mapsto gN$, kde $N = N_G(H)$. Třeba dokázat, že f je dobře definovaná bijekce. Dále dokazujeme obdobně jako v důkazu předchozí věty. □

7.2 Konjugace v symetrické grupě

Definice 7.6. Dvě permutace $\alpha, \beta \in S_n$ mají stejnou cyklovou strukturu, pokud v úplných cyklových rozkladech α a β je počet cyklů délky r stejný pro každé $r \geq 1$.

Lemma 7.7. *Konjugované permutace mají stejnou cyklovou strukturu.*

Důkaz. Nechť $\alpha = \rho_1\rho_2 \dots \rho_k$ je úplný rozklad na disjunktní cykly. Potom $\alpha^\beta = \rho_1^\beta\rho_2^\beta \dots \rho_k^\beta$ je úplný rozklad na disjunktní cykly permutacie α^β. Konjugace permutací β je automorfismus S_n, proto $|\rho_i| = |\rho_i^\beta|$. □

Věta 7.8. *Dvě permutace v S_n jsou konjugované, mají-li stejnou cyklovou strukturu.*

Důkaz. Jednu implikaci jsme již dokázali v lemmatu 7.7. Nechť α a β mají stejnou cyklovou strukturu a nechť $\alpha = \rho_1 \dots \rho_k$, $\beta = \delta_1 \dots \delta_k$. Můžeme předpokládat, že cykly jsou uspořádané tak, že postupnosti $\{|\rho_i|\}_{i=1}^k$ a $\{|\delta_i|\}_{i=1}^k$ jsou neklesající. Potom pro každé $i = 1, \dots, k$ platí $|\rho_i| = |\delta_i|$. Napíšeme ρ_i a δ_i pod sebe. Položíme $\gamma(a) = (b)$, pokud a i b jsou na stejných pozicích v zápise ρ_i a δ_i. Potom $\gamma\alpha\gamma^{-1}(b) = \gamma\alpha(a) = \gamma\rho_i(a) = \delta_i(b) = \beta(b)$. Proto $\beta = \alpha^\gamma$. □

Důsledek 7.9. *Podgrupa $H \leq S_n$ je normální právě tehdy, když s každou permutací $\alpha \in H$ podgrupa H obsahuje všechny permutace se stejnou cyklovou strukturou jako α.*

Důkaz. Stačí si uvědomit, že každá normální podgrupa je disjunktním sjednocením ekvivalentních tříd podle relace konjugace.

Definice 7.10. Partice čísla n je posloupnost $m_1, m_2, \dots, m_r$, $1 \leq m_1 \leq m_2 \leq \dots \leq m_r$ splňující podmínku $m_1 + m_2 + \dots + m_r = n$.

□

Důsledek 7.11. *Počet tříd konjugace v S_n je rovný počtu partic čísla n.*

Lemma 7.12. *Nechť H je normální podgrupa grupy G s prvočíselným indexem. Nechť x je takový prvek grupy H, že centralizátor prvku x v grupě H je vlastní podgrupa centralizátoru prvku x v grupě G, tj. $C_H(x) < C_g(x)$. Potom je-li prvek $y \in H$ konjugovaný s prvkem x v grupě G, je konjugovaný s prvkem x i v grupě H.*

Cvičení

7.1. Dokažte, že symetrická grupa pro $n \geq 3$ má triviální centrum.

7.2. Dokažte, že A_4 má triviální centrum.

7.3. Dokažte, že pokud G není abelovská, $G/Z(G)$ není cyklická.

7.4. Dokažte, že $Z(H \times K) = Z(H) \times Z(K)$.

7.5. Dokažte, že A_4 nemá normální podgrupu řádu 6.

7.6. Identifikujte třídy konjugace v S_5 a A_5.

7.3 Jednoduchost A_n

Některé objekty se na první pohled zdají být jednoduché, jiné se jeví jako složité. Při podrobnějším pohledu na věc se ale někdy situace úplně otočí. Zjistíme, že původně jednoduché objekty jsou ve skutečnosti složité, a složité objekty se po pochopení jejich struktury stanou jednoduchými.
V této sekci chceme dokázat, že grupa sudých permutací A_n je pro $n \geq 5$ jednoduchá.

Definice 7.13. Grupa se nazývá jednoduchá, pokud nemá vlastní normální podgrupy.

Tvrzení 7.14. *Nechť G je abelovská grupa. Potom G je jednoduchá právě tehdy, když G je cyklická prvočíselného řádu.*

Důkaz. ($\Leftarrow$) Je-li grupa G cyklická prvočíselného řádu, z věty 5.11 vyplývá, že G nemá žádné vlastní podgrupy, a tedy G je jednoduchá.
($\Rightarrow$) Z definice normální grupy vidíme, že v abelovské grupě je každá podgrupa normální. Vzhledem k tomu, že G je jednoduchá abelovská grupa, pro každý prvek $a \in G$, $a \neq 1$, platí $\langle a \rangle = G$. Proto G je cyklická grupa. Z věty 4.8 vyplývá, že $|G|$ nemá netriviálního dělitele. Proto G je prvočíselného řádu. □

Lemma 7.15. *Grupa A_4 má normální podgrupu indexu 3.*

Důkaz. Označme $\alpha = (12)(34)$ a $\beta = (13)(24)$ dvě permutace v A_4. Všimněme si, že $\alpha\beta = \beta\alpha$, proto $H = \langle \alpha, \beta \rangle$ je izomorfní s grupou $Z_2 \times Z_2$. Dokážeme, že $\langle \alpha, \beta \rangle$ je normální podgrupa grupy A_4. Jinými slovy musíme dokázat, že pro každé $g \in A_4$ platí, že $\langle \alpha, \beta \rangle^g = \langle \alpha, \beta \rangle$. Kromě prvků grupy $\langle \alpha, \beta \rangle$, obsahuje grupa A_4 jen 8 dalších prvků, a to permutace typu $\gamma = (abc)(d)$. Pro každý 3-cyklus γ ověříme, že $H^\gamma = H$. □

Lemma 7.16. *A_5 je jednoduchá.*

Důkaz. Důkaz rozdělíme na několik částí.

(1) Dokážeme, že všechny 3-cykly jsou v A_5 konjugované. Z věty 7.8 víme, že jsou konjugované v S_5. Nechť $x = (123)(4)(5)$. Všimněme si, že x komutuje s

lichou permutací $(45)(1)(2)(3)$. Z toho vyplývá, že $C_{A_5}(x) < C_{S_5}(x)$. Použitím věty 7.12 dostáváme dokazované tvrzení.

(2) Dokážeme, že permutace typu $(ab)(cd)(e)$ jsou v A_5 konjugované. Všimněme si, že permutace $(12)(34)(5)$ komutuje s lichou permutací $(12)(3)(4)(5)$, a postupujeme analogicky jako v předchozím případě.

(3) Dokážeme, že permutace typu $(abcde)$ tvoří v A_5 dvě třídy konjugace. Nechť $\alpha = (12345)$. Z asociativity operace skládání permutací vyplývá, že α musí komutovat se všemi svými mocninami. Vzhledem k tomu, že α má řád 5 a všechny 5-cykly patří do grupy A_5, platí, že $|C_{A_5}(\alpha)| \geq 5$. Všech 5-cyklů je 24. V grupě S_5 jsou všechny 5-cykly konjugované, a tedy $|\alpha^{S_5}| = 24$. Podle věty 7.3 platí $[S_5 \colon C_{S_5}(\alpha)] = |\alpha^{S_5}| = 24$. Z toho je jasné, že $|C_{S_5}(\alpha)| = |S_5|/[S_5 \colon C_{S_5}(\alpha)] = 120/24 = 5$. Vzhledem k tomu, že $|C_{S_5}(\alpha)| = 5$, je $|C_{A_5}(\alpha)| \leq 5$. Dokázali jsme, že $|C_{A_5}(\alpha)| = 5$. Z věty 7.3 dostaneme $|\alpha^{A_5}| = [A_5 \colon C_{A_5}(\alpha)] = |A_5|/|C_{A_5}(\alpha)| = 60/5 = 12$. Vzhledem k tomu, že stejný výpočet platí pro libovolný 5-cyklus a grupa A_5 obsahuje 24 5-cyklů, permutace typu $(abcde)$ tvoří v A_5 dvě třídy konjugace.

Velikost grupy A_5 je $A_5 = S_5/2 = 60$. Grupa A_5 obsahuje identitu, $\frac{\binom{4}{2}}{2} = 15$ permutací typu $(ab)(cd)(e)$, $\binom{5}{3} * 2 = 20$ permutací typu $(abc)(d)(e)$ a $5!/5 = 24$ permutací typu $(abcde)$. Permutace typu $(abcde)$ tvoří dvě třídy konjugace. Ostatní typy tvoří jen jednu třídu konjugace. Grupa A_5 se tedy rozpadne na 5 tříd konjugací s velikostmi $1, 15, 20, 12$ a 12. Každá normální podgrupa je sjednocením tříd konjugací a každá podgrupa musí obsahovat neutrální prvek, tedy identitu. Nechť vezmeme libovolné netriviální sjednocení tříd konjugace, jeho velikost nikdy nebude vlastním dělitelem $|A_5| = 60$, a tedy nemůže tvořit podgrupu (Lagrangeova věta). Tím jsme dokázali, že $|A_5|$ je jednoduchá.

□

Lemma 7.17. *Nechť $H \lhd A_n$, $n \geq 5$. Pokud H obsahuje 3-cyklus, platí $H = A_n$.*

Důkaz. Protože $H \lhd A_n$ a v grupě A_n jsou všechny 3-cykly konjugované, s 3-cyklem $\gamma \in H$ obsahuje grupa H všechny 3-cykly.

Nechť $\alpha = \tau_1\tau_2 \ldots \tau_m$ je rozklad nějaké sudé permutace na transpozice. Nechť $\tau_1 = (i, j)$ a $\tau_2 = (k, \ell)$. Pokud tyto transpozice jsou disjunktní, $(i, j)(k, \ell) = (i, j, k)(j, k, \ell)$; pokud nejsou disjunktní (a například $\tau_2 = (j, k)$), $(i, j)(j, k) = (i, j, k)$. V každém případě můžeme nahradit $\tau_1\tau_2$ ve vyjádření α jedním nebo dvěma 3-cykly. Protože m je sudé, opakováním postupu nahradíme ve vyjádření α všechny transpozice a dostaneme vyjádření α jako součin 3-cyklů. Proto $\alpha \in H$ a $A_n \leq H$. Z předpokladů pak dostáváme $A_n = H$. □

Lemma 7.18. *A_6 je jednoduchá.*

Důkaz. Nechť $1 \neq H \lhd A_6$ je normální podgrupa. Nechť $\alpha \in H$, $\alpha \neq 1$. Rozlišíme 2 případy.

Případ I: $\alpha(i) = i$ pro nějaké $i \in \{1, 2, 3, 4, 5, 6\}$. Označme $F \leq A_6$ podgrupu $F = \{\gamma \in A_6;\ \gamma(i) = i\}$. Zřejmě $F \cong A_5$ a podle 2. věty o izomorfismu je

$H \cap F \lhd F$. Ale $\alpha \in H \cap F$, proto $H \cap F > 1$. Z lemmatu 7.16 máme $H \cap F = F$. Proto $F \leq H$ a H obsahuje 3-cyklus. Z lemmatu 7.17 vyplývá $H = A_6$.

Případ II: Pro každý prvek $\alpha \in H$ kromě jedničky a pro každé i platí $\alpha(i) \neq i$.

Protože α je sudá permutace, $\alpha = (i,j)(k,l,m,r)$ nebo $\alpha = (i,j,k)(l,m,r)$. V prvním případě $\alpha^2(i) = (i)$ a $\alpha^2 \neq 1$, dostáváme tedy spor.

Ve druhém případě položme $\beta = (j,k,l)$. Permutace $\gamma = [\alpha,\beta] = \alpha(\beta\alpha^{-1}\beta^{-1}) \in H$. Navíc $\gamma = (i,m,k,j,l)(r)$, a proto $\gamma(r) = r$, dostáváme tedy spor.

□

Věta 7.19. *Pro každé $n \geq 5$ je A_n jednoduchá grupa.*

Důkaz. Nechť $1 \neq H \lhd A_n$ je normální podgrupa. Nechť $\beta \in H$, $\beta(i) = j \neq i$. Nechť $\alpha = (i)(j,k,l)\ldots$ je 3-cyklus. Potom $\beta\alpha(i) = j \neq k = \alpha\beta(i)$, proto $\gamma = [\alpha\beta] \neq 1$, ale $\gamma \in H$. Navíc, $\gamma = (\alpha\beta\alpha^{-1})\beta^{-1}$ je součin dvou 3-cyklů. Nechť $F \leq A_n$ je podgrupa, která fixuje všechny prvky s výjimkou těch, které se nacházejí ve dvou 3-cyklech rozkladu γ. Zřejmě $F \cong A_6$ a $H \cap F \lhd F$. Proto $H \cap F = F$ a H obsahuje 3-cyklus. Z lemmatu 7.17 vyplývá $H = A_n$. □

Cvičení

7.7. Dokažte, že symetrická grupa pro $n \neq 4$ má jedinou normální podgrupu $A_n \lhd S_n$.

7.8. Nechť $G \leq S_n$ obsahuje lichou permutaci. Potom řád $|G|$ je sudý a přesně polovina prvků G je lichá.

7.4 Reprezentace grup

V této části se budeme zabývat reprezentací abstraktních grup v symetrických a lineárních grupách. Ukážeme, že symetrické i lineární grupy jsou univerzální v tom smyslu, že pro každou (konečnou) grupu řádu n můžeme najít izomorfní podgrupu v symetrické grupě S_n i v grupě lineárních transformací n-dimenzionálního vektorového prostoru.

Věta 7.20 (Cayley, 1878)**.** *Každá grupa G je izomorfní nějaké podgrupě S_G. Pokud $|G| = n$, je G je izomorfní podgrupě S_n.*

Důkaz. Pro každý prvek $a \in G$ definujme funkci $L_a \colon g \mapsto ag$. Tvrdíme, že L_a je permutace prvků grupy G. Nechť $L_a(g) = L_a(h)$. Potom $ag = ah$, odtud pak $g = h$. Pro každé $h \in G$ existuje $g = a^{-1}h$ takové, že $L_a(g) = h$.

Dále, zobrazení $\phi \colon a \mapsto L_a$ je hledaný monomorfismus $G \to S_G$. Je to morfismus, neboť $\phi(ab) = L_{ab} = L_aL_b = \phi(a)\phi(b)$. Navíc, $\phi(a) = 1$ implikuje $ag = g$ pro každé $g \in G$. Odtud, $a = gg^{-1} = 1$. □

Definice 7.21. Zobrazení $\phi \colon G \to S_G$, $a \mapsto L_a$ se nazývá levá regulární reprezentace grupy G.

Důsledek 7.22. *Nechť $|G| = n$ a nechť $\mathbb{F}$ je pole. Potom G můžeme vnořit do $GL(n, \mathbb{F})$.*

Důkaz. Z Cayleyho věty vyplývá, že G můžeme reprezentovat jako podgrupu S_n. Dále S_n můžeme reprezentovat v $GL(n, \mathbb{F})$. Toto vnoření $\psi\colon S_n \to GL(n, \mathbb{F})$ je dané zobrazením $\alpha \mapsto M_\alpha$, kde $M_\alpha = (m_{i,j})$, $n \times n$ je permutační matice se složkami $m_{i,j} \in \{0, 1\}$, přičemž $m_{i,j} = 1$ právě tehdy, když $\alpha(i) = j$. Potom složení $\psi \circ \phi$ je hledaná reprezentace. □

Věta 7.23. *Nechť G je grupa a nechť $H \leq G$ je podgrupa indexu n. Potom existuje homomorfismus $\rho\colon G \to S_n$ s jádrem $\ker(\rho) \leq H$.*

Důkaz. Položme $L_a(gH) = agH$. Potom L_a je permutace G/H. Dále $\varphi\colon a \mapsto L_a$ je homomorfismus $G \to S_{G/H} \cong S_n$. Pokud $a \in \ker(\varphi)$, je $L_a(H) = aH = H$. Proto $a \in H$ a $\ker(\varphi) \leq H$. □

Definice 7.24. Zobrazení $a \mapsto L_a$ se nazývá reprezentace grupy G na třídách podgrupy H.

Pokud $H = 1$, získáme levou regulární reprezentaci z Cayleyho věty.

Důsledek 7.25. *Jestliže jednoduchá grupa G obsahuje podgrupu indexu $n > 1$, existuje vnoření G do S_n.*

Důkaz. Uvažujme homomorfismus ρ grupy $G \to S_n$. Grupa G je jednoduchá, proto $\ker(\rho) = 1$ nebo $G = \ker(\rho) \leq H$. Ve druhém případě $G = H$ a $[G : H] = 1$. □

Věta 7.26. *Nechť $H \leq G$ a nechť X je množina všech podgrup konjugovaných s H. Potom existuje homomorfismus $\Psi\colon G \to S_X$ s jádrem $\ker(\Psi) \leq N_G(H)$.*

Důkaz. Označme $\psi_a\colon X \to X$ zobrazení $gHg^{-1} \mapsto agHg^{-1}a^{-1}$. Potom $\psi_a \in S_X$ a $\Psi\colon a \mapsto \psi_a$ je homomorfismus. Pokud $a \in \ker(\Psi)$, je $\psi_a(H) = aHa^{-1}$, a proto $a \in N_G(H)$. Odtud pak plyne $\ker(\Psi) \leq N_G(H)$. □

Cvičení

7.9. Dokažte, že přiřazení $\alpha \mapsto M_\alpha$ je vnoření $S_n \to GL(n, \mathbb{F})$, kde $\mathbb{F}$ je libovolné pole a M_α je permutační matice.

7.10. Dokažte, že A_6 nemá podgrupu prvočíselného indexu.

7.11. Položme $R_a(g) = ga$. Potom $a \mapsto R_a$ je pravá regulární reprezentace. Dokažte, že pravá regulární reprezentace je injektívní homomorfismus $G \to S_G$.

7.12. Dokažte, že pravá a levá regulární reprezentace grupy S_3 v grupě S_6 tvoří konjugované podgrupy.

7.5 Akce grupy na množině

Definice 7.27. Nechť G je grupa a nechť X je množina. Zobrazení $\alpha\colon G\times X \to X$, značíme $\alpha(g,x) = g\cdot x$, nazveme *akce grupy*, a množinu X nazveme *G-množina*, jestliže platí:

- $1\cdot x = x$, pro každé $x\in X$,
- $g\cdot(h\cdot x) = (gh)\cdot x$ pro každé $g,h\in G$ a pro každé $x\in X$.

Akce S_n na množině $\{1,2,\dots,n\}$, akce grupy G na G a na množině levých tříd G/H levým násobením, akce grupy G na G a na množině podgrup G konjugací jsou příklady akcí.

Věta 7.28. *Pokud $\alpha\colon G\times X\to X$ je akce, je $\tilde\alpha\colon g\mapsto (x\mapsto gx)$ homomorfismus $G\to S_X$.*

Je-li $\theta\colon G\to S_X$ homomorfismus, G má akci na X definovanou $\alpha(g,x) = g\cdot x = \theta(g)(x)$.

Důkaz. a) Nejprve ověříme, že $\alpha_g\colon x\mapsto gx$ je permutace. Nechť $\alpha_g(x) = \alpha_g(y)$, potom $g\cdot x = g\cdot y$. Máme

$$g^{-1}\cdot(g\cdot x) = (gg^{-1})\cdot x = 1\cdot x = x$$

a podobně

$$g^{-1}\cdot(g\cdot y) = (gg^{-1})\cdot y = 1\cdot y = y,$$

což implikuje $x = y$. Dále, ke každému $y\in X$ existuje $x = g^{-1}\cdot y$ takové, že $\alpha_g(x) = y$.

Ověříme, že $\tilde\alpha$ je homomorfismus:

$$\tilde\alpha(gh) = \alpha_{gh} = \alpha_g\alpha_h = \tilde\alpha(g)\tilde\alpha(h).$$

b) Nechť $\theta\colon G\to S_X$ je homomorfismus. Potom $1\cdot x = \theta(1)(x) = id(x) = x$. Dále

$$(gh)\cdot x = \theta(gh)(x) = \theta(g)(\theta(h)(x)) = \theta(g)(h\cdot x) = g\cdot(h\cdot x).$$

□

Definice 7.29. Nechť X je G-množina. Množinu $O(x) = \{y\in X;\ y = g\cdot x, g\in G\}$ budeme nazývat *G-orbita* bodu x.

Pokud je G pevně zvolená, $O(x)$ budeme stručně nazývat orbita bodu x. Množina všech orbit tvoří rozklad množiny X.

Definice 7.30. Nechť X je G-množina. Podgrupu $G_x = \{g\in G;\ g\cdot x = x\}$ budeme nazývat *stabilizátor* prvku x.

V akci grupy G na G je konjugací $O(a) = a^G$ a $G_a = C_G(a)$. V akci grupy G na množině podgrup je konjugací $O(H) = H^G$ a $G_H = N_G(H)$.

Akce G levým násobením na G/H má jedinou orbitu. Stabilizátor $G_H = H$.

Věta 7.31. *Nechť X je G-množina. Potom $|O(x)| = [G : G_x]$.*

Důkaz. Nechť $f\colon gx \mapsto gG_x$. Toto zobrazení je dobře definované. Pokud $y = gx = hx$, je $gG_x = hG_x$. Dále $gG_x = hG_x$ implikuje $h = gc$, kde $c \in G_x$. Potom $hx = gcx = gx$ je ten samý prvek orbity $O(x)$. Proto f je injektivní. Pokud $gG_x \in G/G_x$, pro $y = g \cdot x$ platí $f(y) = gG_x$. □

Důsledek 7.32. *Pokud X je G-množina a G je řádu n, je $|O(x)|$ dělitelem n.*

Důsledek 7.33. *Nechť G je konečná grupa. Potom počet prvků konjugovaných s x se rovná $[G : C_G(x)]$.*

Důkaz. Ve větě 7.31 položíme $X = G$ a akce G na X je daná konjugací. Potom $G_x = C_G(x)$. □

Důsledek 7.34. *Nechť G je konečná grupa. Potom počet podgrup konjugovaných s $H \leq G$ se rovná $[G : N_G(H)]$.*

Důkaz. Ve větě 7.31 vezmeme za X množinu všech podgrup a akce G na X je daná konjugací. Potom $G_H = N_G(H)$. □

Definice 7.35. Akce grupy G na X se nazývá *tranzitivní*, jestliže má jen jednu orbitu. Jinými slovy, pro každé $x, y \in X$ existuje $g \in G$ takové, že $g \cdot x = y$.

Definice 7.36. Budeme hovořit, že G-množiny X a Y jsou *izomorfní*, existuje-li bijekce $\varphi\colon X \to Y$ splňující pro každé $g \in G$ a $x \in X$ rovnost $\varphi(g \cdot x) = g \cdot \varphi(x)$.

Věta 7.37. *Každá tranzitivní akce (G, X) je izomorfní akci G s násobením na levých třídách rozkladu podle nějaké podgrupy H. Navíc, dvě akce dané násobením na třídách rozkladu podle $K \leq G$ a podle $H \leq G$ jsou izomorfní právě tehdy, když podgrupy K, H jsou konjugované.*

Důkaz. Položme $H = G_x \leq G$ pro nějaký prvek $x \in X$ a $\varphi(y) = aG_x$, pokud $y = a \cdot x$. Z tranzitivity akce také umíme $a \in G$ vždy najít.

Je to dobře definovaná funkce, protože $y = a' \cdot x = a \cdot x$ implikuje $a^{-1}a' \in G_x$. Proto $a' = ah$ pro nějaké $h \in G_x$ a $\varphi(y) = \varphi(a' \cdot x) = ahG_x = aG_x$. Je to injektivní zobrazení, neboť $\varphi(y) = \varphi(z)$ pro $y = a \cdot x$, $z = b \cdot x$, to implikuje $aG_x = bG_x$. Odtud existuje $h \in G_x$ takové, že $b = ah$. Proto $z = b \cdot x = ah \cdot x = a \cdot x = y$. Tedy φ je injektivní a φ je rovněž surjekce, neboť pro třídu hG_x platí $\varphi(h \cdot x) = hG_x$.

Nechť $z = g \cdot y$, $y = a \cdot x$ a $z = b \cdot x$. Potom $\varphi(g \cdot y) = b \cdot G_x$ a $g \cdot \varphi(y) = gaG_x$. Potom $b \cdot G_x = gaG_x$ právě tehdy, když $b^{-1}ga \in G_x$. Platí

$$b^{-1}ga \cdot x = b^{-1}g \cdot y = b^{-1} \cdot z = b^{-1}b \cdot x = x.$$

□

Zajímavou otázkou je, zda každou akci grupy na nějakém prostoru X je možné představit si jako přirozenou akci podgrupy S_X. Abychom tuto otázku mohli zformulovat jako matematický problém, potřebujeme jej formalizovat.

Definice 7.38. Dvě akce (G, X) a (H, Y) jsou *ekvivalentní*, existuje-li izomorfismus $\theta\colon G \to H$ a bijekce $\varphi\colon X \to Y$ takové, že $\varphi(g \cdot x) = \theta(g) \cdot \varphi(x)$.

Akce grupy G na X se nazývá *permutační*, jestliže je ekvivalentní přirozené akci podgrupy S_X.

Nechť (G, X) je akce. Označme $\mathrm{Cor}(G) = \cap_{x\in X} G_x \leq G$.

Věta 7.39. *Nechť (G, X) je akce. Potom $K = \mathrm{Cor}(G) \lhd G$ je normální podgrupa. Navíc $(G/K, X)$ definovaná předpisem $gK \cdot x = g \cdot x$ je permutační akce.*

Speciálně (G, X) je permutační akce právě tehdy, když $\mathrm{Cor}(G) = 1$.

Důkaz. Uvažujme homomorfismus $\theta\colon G \to S_X$ definovaný přiřazením $g \mapsto (x \mapsto g \cdot x)$. Potom $\ker(\theta) = \mathrm{Cor}(G) = K$, a proto $K \lhd G$.

Dokážeme, že G/K má akci na X. Nejdříve ověříme, že zobrazení $gK \cdot x = g \cdot x$ je dobře definované. Nechť $gK = g'K$. Potom $g' = gk$ pro nějaké $k \in K$. Potom

$$g'K \cdot x = gkK \cdot x = gK \cdot x.$$

Zřejmě $1K \cdot x = 1 \cdot x = x$. Dále

$$(gKhK) \cdot x = ghK \cdot x = (gh) \cdot x = g \cdot (h \cdot x) = gK \cdot (hK \cdot x).$$

Tedy se jedná o dobře definovanou akci.

Z 1. věty o izomorfismu dostáváme $G/K \cong Im(\theta) \leq S_X$. □

Cvičení

7.13. Symetrická grupa S_n má akci na množině polynomů n proměnných definovanou $\sigma \cdot f(x_1, x_2, \ldots, x_n) = f(x_{\sigma 1}, x_{\sigma 2}, \ldots, x_{\sigma n})$. Nechť $D = D(x_1, \ldots, x_n) = \prod_{i<j}(x_i - x_j)$. Zjistěte stabilizátor G_D akce $G = S_n$ na množině polynomů s n proměnnými.

7.14. Nechť G má akci na X. Dokažte, že pokud x a y patří do stejné orbity, platí $G_x \cong G_y$.

7.6 Počítání orbit

Věta 7.40 (Burnside)**.** *Nechť X je konečná G-množina. Označme $O(G)$ počet G-orbit a $\mathrm{Fix}(g)$ počet bodů X fixovaných $g \in G$. Potom*

$$\mathrm{Orb}(G, X) = \frac{1}{|G|} \sum_{g\in G} \mathrm{Fix}(g).$$

Důkaz. Nechť x, y jsou ve stejné orbitě. Existuje $g \in G$ takové, že $y = g \cdot x$. Nechť $h \in G_y$, potom $g^{-1}hg(x) = x$, proto $\gamma_g(G_y) = G_y^g \leq G_x$. Podobně $\gamma_{g^{-1}}(G_x) = G_x^{g^{-1}} \leq G_y$. Zkonstruovali jsme vzájemně inverzní monomorfismy $G_y \to G_x$ a $G_x \to G_y$.

Každý bod x přispívá do sumy na pravé straně $|G_x|$. Jestliže x, y jsou ve stejné orbitě, $G_x \cong G_y$, a tedy $|G_x| = |G_y|$. Podle věty 7.31 je počet prvků orbity obsahující x rovný $[G : G_x]$. Proto každá orbita přispívá $|G| = |G_x|[G : G_x]$, a tedy platí $\sum_{g\in G} \mathrm{Fix}(g) = |G| \cdot \mathrm{Orb}(G)$.

□

Důsledek 7.41. *Nechť (G, X) je tranzitivní akce a nechť $|X| > 1$. Potom existuje prvek $g \in G$ takový, že* $\mathrm{Fix}(g) = 0$.

Důkaz. Z tranzitivity akce plyne $\mathrm{Orb}(G) = 1$. Předpokládejme, že $\mathrm{Fix}(g) \geq 1$ pro každé $g \in G$. Z Burnsidovy věty plyne

$$|G| = \sum_{g\in G} \mathrm{Fix}(g) = \mathrm{Fix}(1) + \sum_{g\in G, g\neq 1} \mathrm{Fix}(g) \geq |G| + (|G| - 1) > |G|$$

a dostáváme spor. □

Příklad 7.42. Uvažujme vlajku složenou z n stejně dlouhých pásů obarvených q barvami. Každé takové vlajce můžeme přiřadit vektor barev $(c_1, \ldots, c_n)$. Dvě takové postupnosti definují stejnou vlajku, jestliže se rovnají nebo pokud druhá vznikne z první reflexí danou permutací $\tau(i, n - i + 1)$ pro $i = 1, 2, \ldots n$. Kolik různých vlajek můžeme vytvořit?

Úlohu vyřešíme pomocí Burnsidovy věty. Položme $G = \langle\tau\rangle$ a nechť X je prostor všech vektorů délky n vytvořených z q barev. Potom grupa G má akci na X definovanou permutací indexů. Nyní je třeba spočítat počet orbit. Grupa G má jen 2 prvky, platí $\mathrm{Fix}(1) = |X| = q^n$ a $\mathrm{Fix}(\tau) = q^{\lfloor n+1/2\rfloor}$. Ve druhém vztahu jsme využili to, že $\tau \cdot x = x$ právě tehdy, když x je palindrom. Potom $O(G) = \frac{1}{2}(q^n + q^{\lfloor n+1/2\rfloor})$.

Příklad zobecníme následovně. Nechť $G \leq S_n$ a nechť C je množina q-barev. Potom G má akci na množině všech barevných vektorů $X = C^n$ dimenze n definovanou

$$\sigma \cdot (c_1, c_2, \ldots, c_n) = (c_{\sigma 1}, c_{\sigma 2}, \ldots, c_{\sigma n}).$$

Orbitu v akci G na X budeme nazývat (G, q) obarvení množiny $\{1, 2, \ldots, n\}$.

Lemma 7.43. *Jestliže $\sigma \in G \leq S_n$, platí* $\mathrm{Fix}(\sigma) = q^{t(\sigma)}$*, kde $t(\sigma)$ je počet cyklů v úplném rozkladu σ na disjunktní cykly.*

Důkaz. Nechť $x = (c_1, c_2, \ldots, c_n) \in \mathrm{Fix}(\sigma)$. Potom $\sigma^k(x) = x$ pro každé $k \in \mathbb{Z}$. Speciálně, $\sigma^k(x_i) = x_i$ pro každé $i = 1, 2, \ldots, n$. Nechť $\sigma = \beta_1\beta_2 \ldots \beta_k$, $k = t(\sigma)$ je úplný rozklad na disjunktní cykly. Pokud i je v orbitě definované β_j, potom všechny barvy na indexech $o(\beta_j)$ jsou stejné. Tedy máme $q^{t(\sigma)}$ možností jak zvolit barvy v x. □

Definice 7.44. Nechť je počet cyklů délky r v úplném rozkladu permutace $\alpha \in S_n$ na disjunktní cykly $e_r \geq 0$. Potom cyklový index $\mathrm{ind}(\sigma) = \prod_{i=1}^n x_i^{e_i}$. Jestliže $G \leq S_n$, platí $P_G(x_1, \ldots, x_n) = \frac{1}{|G|} \sum_{\sigma\in G} \mathrm{ind}(\sigma)$.

Například $\mathrm{ind}(\mathrm{id}) = x_1^n$ a $\mathrm{ind}(\beta) = x_1^{n-r}x_r$, kde β je cyklus délky r.

Důsledek 7.45. *Počet (G,q) obarvení množiny $\{1,2,\ldots,n\}$ je $P_G(q,q,\ldots,q)$.*

Důkaz. Z Burnsidovy věty a z lemmatu 7.43 vyplývá, že počet (G,q) obarvení je

$$\mathrm{Orb}(G,X) = \frac{1}{|G|}\sum_{\sigma\in G}\mathrm{Fix}(\sigma) = \frac{1}{|G|}\sum_{\sigma\in G} q^{t(\sigma)}.$$

A na druhou stranu je

$$\begin{aligned} P_G(q,q,\ldots,q) &= \frac{1}{|G|}\sum_{\sigma\in G}\mathrm{ind}(\sigma)(q,q,\ldots,q) = \frac{1}{|G|}\sum_{\sigma\in G} q^{e_1(\sigma)}q^{e_2(\sigma)}\ldots q^{e_n(\sigma)} \\ &= \frac{1}{|G|}\sum_{\sigma\in G} q^{t(\sigma)}. \end{aligned}$$

□

Cvičení

7.15. Dokažte, že počet tříd relace konjugace na konečné grupě G je

$$\frac{1}{|G|}\sum_{g\in G}|C_G(g)|.$$

Najděte analogický vzorec pro počet tříd konjugace na podgrupách.

7.16. Kolik obarvení šachovnice $n\times n$ vznikne použitím q barev? Dvě šachovnice považujeme za totožné, jestliže jedna vznikne z druhé rotací o 90, 180 nebo 270 stupňů.

7.7 Geometrické grupy

Definice 7.46. *Izometrie* je funkce $T\colon \mathbb{R}^n \to \mathbb{R}^n$, která zachovává vzdálenost, platí tedy $||T(x)-T(y)|| = ||x-y||$ pro každé $x,y\in\mathbb{R}^n$. *Translace* určená $w\in\mathbb{R}^n$ je izometrie $T_w(x) = x+w$.

Definice 7.47. Lineární transformace $S\colon \mathbb{R}^n \to \mathbb{R}^n$ je ortogonální, jestliže platí $||Sx|| = ||x||$.

Zřejmě každá ortogonální transformace je izometrie nebo $||S(x)-S(y)|| = ||S(x-y)|| = ||x-y||$.

Lemma 7.48. *Lineární transformace S je ortogonální právě tehdy, když $\{S(\epsilon_i)\}$, $i=1,2,\ldots,n$ je ortonormální báze.*

Důkaz. ($\Rightarrow$) Chceme dokázat, že pro skalární součin platí $(Sx,Sy) = (x,y)$. Nejdříve si všimneme, že ze vztahu $(x_i+y_i)^2 = x_i^2+2x_iy_i+y_i^2$ vyplývá $||x+y||^2 - ||x||^2 - ||y||^2 = 2(x,y)$ i $||S(x)+S(y)||^2 - ||S(x)||^2 - ||S(y)||^2 = 2(S(x),S(y))$. Z

ortogonality S dostaneme $(Sx, Sy) = (x, y)$. Potom $(S\epsilon_i, S\epsilon_j) = (\epsilon_i, \epsilon_j) = \lambda_{i,j}$, a tedy báze $\{S(\epsilon_i)\}$ je ortonormální.

($\Leftarrow$) Nechť $x = \sum_i x_i\epsilon_i$. Potom $Sx = \sum_i x_i S(\epsilon_i)$ a s použitím vlastností skalárního součinu dostaneme

$$||Sx||^2 = (Sx, Sx) = (\sum_i x_i S(\epsilon_i), \sum_j x_j S(\epsilon_j)) = \sum_{i,j} (x_i S(\epsilon_i), x_j S(\epsilon_j)) =$$

$$\sum_{i,j} x_i x_j (S(\epsilon_i), S(\epsilon_j)) = \sum_{i,j} x_i x_j \lambda_{i,j} = (x, x) = ||x||^2.$$

□

Lemma 7.49. *Ortogonální transformace tvoří podgrupu grupy lineárních transformací.*

Lemma 7.50. *Každá izometrie, která fixuje nulový vektor, je ortogonální transformace.*

Důkaz. Nejprve dokážeme, že izometrie fixující nulový vektor a zároveň každé ϵ_j ve standardní bázi, je identita. Nechť $x = (x_1, \ldots, x_n)$ je libovolný vektor a $T(x) = y = (y_1, \ldots, y_n)$. Máme

$$||y|| = ||T(x)|| = ||T(x) - T(0)|| = ||x - 0|| = ||x||.$$

Proto

$$y_1^2 + y_2^2 + \ldots y_n^2 = x_1^2 + \cdots + y_n^2.$$

Z předpokladů plyne

$$||T(x - \epsilon_1)|| = ||T(x) - T(\epsilon_1)|| = ||T(x) - \epsilon_1|| = ||x - \epsilon_1||.$$

A odtud

$$(y_1 - 1)^2 + y_2^2 + \cdots + y_n^2 = (x_1 - 1)^2 + \cdots + y_n^2.$$

Porovnáním vztahů $1 - 2y_1 = 1 - 2x_1$ dostaneme $y_1 = x_1$. Opakováním tohoto postupu pro $i = 2, 3, \ldots, n$ získáme požadovaný výsledek.

Předpokládejme, že $T\epsilon_i = u_i$. Nechť S je ortonormální transformace $S\epsilon_i = u_i$ pro každé $i = 1, \ldots, n$. Potom $S^{-1}T$ je izometrie fixující každý vektor standardní báze. Podle předchozího platí $S^{-1}T = \mathrm{id}$. A proto $T = S$. □

Věta 7.51. *Každá izometrie je složením ortogonální transformace a translace.*

Důkaz. Nechť T je izometrie $T(0) = w$. Označme S translaci $x \mapsto x - w$. Potom $R = ST$ je izometrie fixující 0. Podle lemmatu 7.50 je R ortogonální transformace. Ale $T = S^{-1}R$. □

Věta 7.52. *Funkce $T\colon \mathbb{R}^n \to \mathbb{R}^n$ fixující 0 je izometrie právě tehdy, když zachovává skalární součin, tedy $(Tx, Ty) = (x, y)$.*

Důkaz.

$$||x+y||^2 = (x+y, x+y) = (x,x) + 2(x,y) + (y,y) = ||x||^2 + 2(x,y) + ||y||^2.$$

$$||T(x+y)||^2 = (T(x+y), T(x+y)) = (Tx+Ty, Tx+Ty) =$$

$$(Tx,Tx) + 2(Tx,Ty) + (Ty,Ty) = ||Tx||^2 + 2(x,y) + ||Ty||^2.$$

Použitím $||Tx|| = ||x||$ a $||Ty|| = ||y||$ dostaneme $(Tx, Ty) = (x, y)$.

Naopak nechť pro každé x,y platí $(Tx, Ty) = (x, y)$.

$$||T(x) - T(y)||^2 = (Tx - Ty, Tx - Ty) = (Tx,Tx) - 2(Tx,Ty) + (Ty,Ty) =$$

$$(x,x) - 2(x,y) + (y,y) = (x-y, x-y) = ||x-y||^2.$$

Navíc $||T(0)|| = (T(0), T(0)) = (0,0) = 0$. A proto $T(0) = 0$. □

V geometrii se úhel mezi dvěma vektory definuje vztahem

$$(x,y) = ||x|| \cdot ||y|| \cdot \cos(\theta).$$

Důsledek 7.53. *Nechť T je funkce $T\colon \mathbb{R}^n \to \mathbb{R}^n$ fixující 0. Potom následující tvrzení jsou ekvivalentní:*

1. *T zachovává úhly.*
2. *T je izometrie (zachovává vzdálenosti).*
3. *T je ortogonální transformace.*
4. *T je lineární transformace definovaná maticí A, pro kterou platí $AA^t = E$.*

Důkaz. Důkaz ekvivalence prvních tří tvrzení vyplývá z lemmatu 7.50 a věty 7.52. Použijeme lemma 7.48. Jestliže T je izometrie fixující 0, je T lineární transformace, která zobrazuje standardní bázi na ortonormální bázi $\{u_i\}$. Proto i-tý řádek příslušné matice A je u_i a j-tý sloupec transponované matice A^t je u_j. Prvek $s_{i,j}$ součinu je $s_{i,j} = (u_i, u_j) = \lambda_{i,j}$. Proto $A^tA = E$.

A naopak, jestliže platí $A^tA = E$, platí i $(u_i, u_j) = \lambda_{i,j}$ a báze $\{u_i\}$ je ortonormální. Podle lemmatu 7.48 je T izometrií. □

Definice 7.54. Reálná regulární matice A dimenze n se nazývá ortogonální, jestliže platí $AA^t = E$.

Pokud je A ortogonální, platí

$$1 = \det(E) = \det(AA^t) = \det(A)\det(A^t) = (\det A)^2.$$

Proto $\det(A) \in \{1, -1\}$. Zřejmě matice s determinantem 1 tvoří podgrupu ortogonální grupy. Tuto podgrupu indexu 2 nazýváme *grupa rotací*. Zobrazení s $\det(A) = -1$ nazýváme zobrazení orientaci měnící.

Protože determinant se při konjugaci nemění, jeho hodnota nezávisí od toho, vzhledem ke které bázi je daná lineární transformace vyjádřená. V lineární algebře se relace konjugace v lineární grupě nazývá podobnost.

Izometrie $\varphi\colon x \mapsto Tx + w$ je izometrie *orientaci zachovávající*, jestliže T je rovněž orientaci zachovávající ($\det T = 1$). Pokud $\det T = -1$, je φ je orientaci měnící izometrie.

Nadrovina ve vektorovém prostoru $\mathbb{E}_n$ je množina $Y = H + w$, kde H je nějaký $(n-1)$-dimenzionální podprostor a $w \in \mathbb{E}_n$ je vektor.

Reflexe je orientaci měnící izometrie, která bodově fixuje nějakou nadrovinu $Y \subseteq \mathbb{E}^n$ a vyměňuje dvojice samodružných bodů ortogonálního 1-dimenzionálního podprostoru. Samodružná dvojice bodů je dvojice typu $w+x, w-x$, kde $x \in H^\perp$ a $w \in H$, kde $w \perp x$.

Uvažujme reflexi ρ nadroviny H, která je podprostorem $H = \langle x_1, \ldots, x_{n-1}\rangle \subset \mathbb{E}_n$, a nechť $a \perp H$ je vektor jednotkové velikosti. Tedy translace $w = 0$. Potom ρ je lineární transformace, která má vzhledem na bázi $x_1, \ldots, x_{n-1}, a$ vyjádření

$$\rho = \begin{pmatrix} 1 & 0 & 0 & \ldots & 0 & 0 \\ 0 & 1 & 0 & \ldots & 0 & 0 \\ 0 & 0 & 1 & \ldots & 0 & 0 \\ \cdot & \cdot & \cdot & \ldots & \cdot & \cdot \\ 0 & 0 & 0 & \ldots & 1 & 0 \\ 0 & 0 & 0 & \ldots & 0 & -1 \end{pmatrix}.$$

Věta 7.55. *Reflexe fixující* 0 *je orientaci měnící izometrie.*

Příklad 7.56. Uvažujme izometrii T fixující $\vec{0} = (0,0) \in \mathbb{E}_2$ v Eukleidovské rovině. Daná je ortogonální maticí $T = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. Potom $u_1 = (a,b)$ a $u_2 = (c,d)$ je ortonormální báze. Tyto vektory odpovídají bodům na jednotkové kružnici. Potom můžeme vyjádřit $(a,b) = (\cos\theta, \sin\theta)$ pro nějaký úhel $\theta \in (-\pi, \pi\rangle$. Protože $u_1 \perp u_2$, je $(c,d) = (\cos(\theta \pm \frac{\pi}{2}), \sin(\theta \pm \frac{\pi}{2}))$. A odtud $(c,d) = (-\sin\theta, \cos\theta)$, nebo $(c,d) = (\sin\theta, -\cos\theta)$.

Tedy T má tvar

$$T^+ = \begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix}, \quad \text{nebo} \quad T^- = \begin{pmatrix} \cos\theta & \sin\theta \\ \sin\theta & -\cos\theta \end{pmatrix}.$$

Použitím $\sin^2\theta + \cos^2\theta = 1$ vypočítáme $\det(T^+) = 1$ a $\det(T^{-1}) = -1$. Můžeme dokázat, že

$$(T^+)^n = \begin{pmatrix} \cos(n\theta) & \sin(n\theta) \\ -\sin(n\theta) & \cos(n\theta) \end{pmatrix}.$$

Tedy T^+ je rotace o úhel θ fixující $\vec{0}$. Dále $(T^-)^2 = E$. Dokážeme, že T^- je reflexe fixující přímku p procházející $(0,0)$ pod úhlem $\theta/2$. Na to stačí dokázat,

že bod $T^-(\cos\beta, \sin\beta)^t = (\cos\beta, \sin\beta)^t$ právě tehdy, když $\beta = \theta/2$. Použitím substituce $\beta = -\alpha$ máme

$$\begin{pmatrix}\cos\theta & \sin\theta \\ \sin\theta & -\cos\theta\end{pmatrix}\begin{pmatrix}\cos\beta \\ \sin\beta\end{pmatrix} = \begin{pmatrix}\cos\theta & \sin\theta \\ \sin\theta & -\cos\theta\end{pmatrix}\begin{pmatrix}\cos\alpha \\ -\sin\alpha\end{pmatrix} = \begin{pmatrix}\cos(\theta+\alpha) \\ \sin(\theta+\alpha)\end{pmatrix}.$$

Nechť $\begin{pmatrix}\cos(\theta+\alpha) \\ \sin(\theta+\alpha)\end{pmatrix} = \begin{pmatrix}\cos(\alpha) \\ -\sin(\alpha)\end{pmatrix}$. Porovnáním po souřadnicích a vydělením druhé rovnice první získáme $\tan(\theta+\alpha) = -\tan(\alpha) = \tan(-\alpha)$. To je v pořádku, pokud $\alpha \neq \pm(\pi/2)$ a současně $\alpha + \theta \neq \pm\pi/2$. Případy, kdy to neplatí, můžeme řešit zvlášť. Z poslední rovnosti dostaneme $\theta = -2\alpha = 2\beta$, což jsme potřebovali ověřit. Vzhledem k tomu, že všechny úpravy byly ekvivalentní, tvrzení je dokázané.

Nechť Δ je konvexní rovinný útvar. Označme $Sym(\Delta)$ podgrupu grupy izometrií roviny složenou z transformací $T(\Delta) = \Delta$. Tuto grupu označíme $\mathrm{Aut}(\Delta)$ a podgrupu orientaci zachovávající izometrii označíme $\mathrm{Aut}^+(\Delta)$.

Lemma 7.57. *Nechť φ je izometrie $\mathbb{E}_n$, nechť $A_1, \ldots, A_k$ jsou body a nechť $x = \sum_{i=1}^k \lambda_i A_i$ je konvexní kombinace. Potom $\varphi(x) = \sum_{i=1}^k \lambda_i \varphi(A_i)$.*

Lemma 7.57 dokážeme v rámci obecnějšího tvrzení, viz lemma 7.61.

Věta 7.58. *Nechť Δ je pravidelný konvexní n-úhelník s těžištěm v $(0,0)$, $n \geq 3$. Potom $\mathrm{Aut}(\Delta)$ je řádu $2n$ a $\mathrm{Aut}(\Delta) = \langle T, S\rangle$, přičemž $|T| = n$, $|S| = 2$ a $STS = T^{-1}$.*

Důkaz. Důkaz spočívá v několika krocích.

Krok 1. Zřejmě každá izometrie $\varphi \in \mathrm{Aut}(\Delta)$ zobrazuje vrchol na vrchol. Vzhledem k tomu, že každý bod Δ je konvexní kombinací vrcholů, z lemmatu 7.57 vyplývá, že obraz každého bodu je jednoznačně určený obrazy vrcholů Δ. Z toho plyne, že $\mathrm{Aut}(\Delta) \hookrightarrow S_n$.

Krok 2. Uvažujme rotaci T o úhel $2\pi/n$ se středem otáčení v $(0,0)$. Zřejmě $T(\Delta) = \Delta$, $|T| = n$ a $\langle S\rangle$ je tranzitivní na hranách Δ. Nechť e je hrana, potom $|G_e| = 2$, podle kroku 1. Podle věty 7.31 je $|Orb(e)| = |[G : G_e] = |G|/|G_e|$. Po dosazení dostaneme $n = |G|/2$, a proto $|G| = 2n$.

Krok 3. Nechť S je generátor G_e. Zřejmě $\langle T, S\rangle \leq G$. Určitě $S \notin \langle T\rangle$, neboť žádná netriviální mocnina nefixuje e. Protože $|G| = 2n$, $\langle T\rangle \lhd G$ je normální podgrupa indexu 2. Odtud plyne $STS = T^i$ pro nějaké i, $\gcd(n, i) = 1$. Ztotožníme $T = (1, 2, \ldots, n)$ a $e = [1, 2]$. Vzhledem k tomu, že $S(e) = e$, platí $S(1) = 2$, $S(2) = 1$, $S(3) = n$ a $S(n) = 3$ pro $n \geq 3$. Potom $STS(1) = ST(2) = S(3) = n = T^i(1)$ pro $n \geq 3$. Proto $i = -1$. □

Všimněme si, že $G = \langle T\rangle \cup S\langle T\rangle$ a pro prvky typu ST^i platí $(ST^i)^2 = ST^iST^i = T^{-i}T^i = 1$. Tedy všechny n prvky třídy $S\langle T\rangle$ jsou involuce. *Involuce* v grupě G je prvek řádu 2. Grupu symetrií pravidelného n-úholníku nazýváme *dihedrální grupa,* značíme D_{2n}. Můžeme rozšířit definici dihedrální grupy pro $n \leq 2$ tak, že položíme $D_2 \cong Z_2$ pro $n = 1$ a $D_4 \cong Z_2 \times Z_2$ pro $n = 2$. Potom vztahy pro generátory T, S z věty 7.58 triviálně platí.

Věta 7.59. *Nechť a, b jsou dvě involuce v konečné grupě G. Potom $\langle a, b\rangle$ je dihedrální.*

Důkaz. Položme $t = ab$. Potom $btb = ba = t^{-1}$. Pokud $|t| = n$, $t \mapsto T$ a $b \to S$ je izomorfismus $\langle a, b\rangle \to D_{2n}$. □

Poznámka. Ne každá volba dvou involucí a, b v dihedrální grupě D_{2n} vygeneruje celou D_{2n}.

Podobnou úvahu jako s pravidelným n-úhelníkem můžeme udělat v dimenzi 3. Otázka je, co bude "pravidelný n-úhelník" v dimenzi 3. Mějme konvexní těleso Δ s těžištěm v počátku, které má n oblastí a každá je ohraničená pravidelným k-úhelníkem. Nechť $\mathrm{Aut}(\Delta)$ je tranzitivní na oblastech Δ, přičemž stabilizátor oblasti je D_{2k}. Z Eulerovy věty můžeme dokázat, že existuje přesně 5 takovýchto těles, které se nazývají Platónská tělesa. Jejich grupy automorfismů jsou známé a jsou izomorfní: $A_5 \times Z_2$, $S_4 \times Z_2$ a S_4. To vede k obecnější otázce klasifikace konečných podgrup $O(3, \mathbb{R})$. Takovéto grupy se nazývají sférické grupy. Klasifikace sférických grup je známa. Jako abstraktní grupy jsou to podgrupy $A_5 \times Z_2$, $S_4 \times Z_2$, $D_{2n} \times Z_2$. Klasifikace akcí sférických grup na jednotkové sféře je známa též, ale její prezentace a důkaz je nad rámec tohoto textu.

Definice 7.60. Afinní transformace v $\mathbb{E}_n$ je zobrazení tvaru $x \mapsto Tx + z$, kde T je lineární transformace a z je vektor.

Lehce ověříme, že složení dvou afinních transformací je afinní transformace. Navíc, inverzní prvek k $x \mapsto Tx + z$ je afinní transformace $x \mapsto T^{-1}x - T^{-1}z$. Proto afinní transformace s operací skladní tvoří grupu $\mathrm{Aff}(n, \mathbb{R})$.

Následující lemma hovoří o vlastnostech grupy afinních transformací.

Lemma 7.61. *Nechť φ je afinní transformace. Potom*

(P1) *φ zachovává konvexní kombinace,*

(P2) *φ zobrazuje úsečky na úsečky a trojúhelník na trojúhelník,*

(P3) *φ zobrazuje t bod úsečky na t-bod úsečky,*

(P4) *φ zobrazuje množinu kolineárních bodů na množinu kolineárních bodů,*

(P5) *nechť $A_1, A_2, \ldots, A_k$ je množina bodů, potom $A_2 - A_1, \ldots, A_k - A_1$ jsou lineární nezávislé vektory právě tehdy, když $\varphi(A_2 - A_1), \ldots, \varphi(A_k - A_1)$ jsou lineární nezávislé vektory.*

Důkaz. Dokážeme jen (P1). Ostatní tvrzení jsou triviálními důsledky.

Nechť $x = \sum_{i=1}^{k} \lambda_i A_i$ je konvexní kombinace a nechť $\varphi(x) = Tx + w$ je afinní transformace. Potom

$$\varphi(x) = \varphi(\sum_{i=1}^{k} \lambda_i A_i) = T(\sum_{i=1}^{k} \lambda_i A_i) + w = \sum_{i=1}^{k} \lambda_i T(A_i) + w.$$

Z druhé strany

$$\sum_{i=1}^{k} \lambda_i \varphi(A_i) = \sum_{i=1}^{k} (\lambda_i (T(A_i) + w)) = \sum_{i=1}^{k} \lambda_i T(A_i) + \sum_{i=1}^{k} \lambda_i w = \sum_{i=1}^{k} \lambda_i T(A_i) + w \sum_{i=1}^{k} \lambda_i.$$

Použitím $\sum_{i=1}^{k} \lambda_i = 1$ dostaneme

$$\varphi(\sum_{i=1}^{k} \lambda_i A_i) = \sum_{i=1}^{k} \lambda_i \varphi(A_i),$$

což jsme chtěli dokázat. □

Důsledek 7.62. *Grupa* $\mathrm{Aff}(2, \mathbb{R})$ *je tranzitivní na množině všech trojúhelníků v rovině.*

Věta 7.63. *V každém trojúhelníku se všechny tři těžnice protínají v jednom bodě, přičemž tento bod je dělí v poměru* $2 : 1$.

Kleinova definice geometrie. Grupa izometrií a afinní grupa jsou příklady podgrup grupy homeomorfismů roviny.

Jiným příkladem může byt grupa homeomorfismů, která zobrazuje konvexní obal množiny bodů na sebe. Například, jestliže Δ je pravidelný n-úhelník, tato grupa je tranzitivní na množině bodů Δ. Věta o pevném bodě hovoří o tom, že každý prvek této grupy má fixovaný bod. To je v protikladu k tomu, co jsme dokázali o akci tranzitivní grupy na konečné množině bodů.

Cvičení

7.17. Nechť Q_3 je kostka. Dokažte, že $\mathrm{Aut}(Q_3) \cong S_4 \times Z_2$ a $\mathrm{Aut}^+(Q_3) \cong S_4$.

7.18. Nechť I je ikosaedr. Dokažte, že $\mathrm{Aut}(I) \cong A_5 \times Z_2$ a $\mathrm{Aut}^+(I) \cong A_5$.

7.19. Umíme dokázat, že každá izometrie v $T \in O(3, \mathbb{R})$ má vlastní vektor v takový, že $Tv = v$. Dokažte, že T má vzhledem na vhodnou bázi tvar

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & a & b \\ 0 & c & d \end{pmatrix},$$

kde $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in O(2, \mathbb{R})$.

7.20. Dokažte, že $O(2, \mathbb{R})$ je izomorfní grupě automorfismů jednotkového kruhu.

Kapitola 8

Sylowovy věty

8.1 p-grupy

Grupa G se nazývá p-grupa, jestliže řád každého prvku je p^n, kde p je prvočíslo a n je přirozené číslo.

Lemma 8.1. *Nechť G je konečná abelovská grupa taková, že řád G je dělitelný prvočíslem p. Potom G obsahuje prvek řádu p.*

Důkaz. Nechť $|G| = pm$. Budeme postupovat indukcí podle m. Pokud $m = 1$, je $|G|$ cyklická řádu p a tvrzení platí.

Nechť $m > 1$. Nechť x je prvek řádu t.

Případ 1: $p|t$. Potom $x^{t/p}$ je řádu p.

Případ 2: p nedělí t. Protože G je abelovská, platí $\langle x\rangle \lhd G$ a $|G/\langle x\rangle| = pm/t = pm'$, kde $m' = m/t < m$. Podle indukčního předpokladu existuje prvek $y^* \in G/\langle x\rangle$ řádu p. Uvažujme přirozenou projekci $\nu\colon G \to G/\langle x\rangle$. Nechť $y \in \nu^{-1}(y^*)$. Restrikce $\nu|_{\langle y\rangle}\colon \langle y\rangle \to \langle y^*\rangle$ je epimorfismus cyklických grup, proto p dělí řád y a jsme v případě 1. □

Věta 8.2 (Cauchy)**.** *Nechť G je konečná grupa taková, že řád G je dělitelný prvočíslem p. Potom G obsahuje prvek řádu p.*

Důkaz. Z důsledku 7.33 je počet prvků konjugovaných s x rovný $[G : C_G(x)]$. Jestliže $x \notin Z(G)$, třída $|x^G| > 1$. Jestliže p dělí řád $C_G(x)$ a $C_G(x) < G$, tvrzení vyplývá z indukčního předpokladu. Jestliže by pro každé x platilo $C_G(x) = G$, je G abelovská grupa a tvrzení vyplývá z lemmatu 8.1.

Nechť p nedělí $C_G(x)$ pro každé $x \in G$.

Z tranzitivity akce G na x^G platí $|G| = [G : C_G(x)]|C_G(x)|$. Proto p dělí $[G : C_G(x)]$ pro každé $x \in G \setminus Z(G)$. Třídy konjugace tvoří rozklad grupy, přičemž prvky z centra jsou fixované prvky. Rozepíšeme:

$$|G| = |Z(G)| + \sum_i [G : C_G(x_i)], \tag{8.1}$$

kde x_i jsou reprezentanti tříd mimo centrum. Vzhledem k tomu, že p dělí levou stranu i každý index v sumě, p dělí $|Z(G)|$. Ale $Z(G)$ je abelovská a tvrzení vyplývá z lemmatu 8.1.

□

Důsledek 8.3. *Konečná grupa G je p-grupa právě tehdy, když řád G je p^n pro nějaké $n > 0$.*

Důkaz. Jestliže řád G je p^n, z Lagrangeovy věty plyne, že řád každého prvku je mocnina p.

Předpokládejme, že G je p-grupa. Nechť existuje prvočíslo $q \neq p$ takové, že q dělí $|G|$. Podle Cauchyho věty v G existuje prvek řádu q. Dostáváme spor.

□

Věta 8.4. *Každá konečná netriviální p-grupa má netriviální centrum.*

Důkaz. Uvažujme rovnost (8.1). Podle důsledku 8.3 je $|G| = p^n$ a index $[G : G_x]$ je mocnina p^e, $0 < e < n$. Proto i $|Z(G)|$ je dělitelný p.

□

Nechť G je konečná jednoduchá p-grupa. Potom $G = Z(G)$, a proto G je abelovská. Ve skutečnosti platí $G \cong (Z_p, +)$.

Důsledek 8.5. *Nechť G je grupa řádu p^2. Potom G je cyklická nebo $G \cong Z_p \times Z_p$.*

Důkaz. Jestliže grupa G není cyklická, všechny netriviální prvky mají řád p. Předpokládejme, že G není abelovská. Potom $|Z(G)| < p^2$ a $1 \neq Z(G) \cong Z_p$. Potom $Z(G) \lhd G$ a faktorová grupa $G/Z(G) \cong Z_p$. Nechť $y \notin Z(G)$, potom $G/Z(G) = \{Z(G), Z(G)y, \ldots, Z(G)y^{p-1}\}$. Tedy každý prvek $g \in G$ má tvar $g = x^i y^j$, kde $Z(G) = \langle x \rangle$. Potom $y^g = y^{-j}x^{-i}yx^i y^j = y^{-j}yy^j = y$ a $y \in Z(G)$, dostáváme spor. Proto G je abelovská. Nechť $x \neq y$ jsou dva netriviální prvky, $y \notin \langle x \rangle$. Tvrdíme, že $\langle x \rangle \cap \langle y \rangle = 1$. Nechť existuje $z \neq 1$, $z \in \langle x \rangle \cap \langle y \rangle$. Potom $\langle z \rangle \leq \langle y \rangle$, $\langle z \rangle \leq \langle x \rangle$. Ale $p = |z| = |y| = |x|$ a $\langle x \rangle = \langle y \rangle$, dostáváme spor s výběrem y. A podle věty 6.2

$$G \cong \langle x \rangle \times \langle y \rangle \cong Z_p \times Z_p.$$

□

Věta 8.6. *Nechť G je konečná p-grupa. Nechť $H < G$ je vlastní podgrupa. Potom $H < N_G(H)$. A navíc, je-li H maximální, platí $H \lhd G$.*

Důkaz. Označme $X = H^G$ množinu podgrup konjugovaných s grupou H. Podle důsledku 7.34 platí $|X| = [G : N_G(H)]$. Podgrupa H má na X akci konjugací. V této akci je velikost každé orbity mocnina p. Zároveň $\{H\}$ je orbita. Z dělitelnosti číslem p vyplývá, že existuje aspoň dalších $p - 1$ podgrup konjugovaných s H,

které jsou fixované akcí H. Nechť $H^g = gHg^{-1} \neq H$ je jedna taková konjugovaná podgrupa. Tedy pro každé $a \in H$ platí $agHg^{-1}a^{-1} = g^{-1}Hg$. Protože $H^g \neq H$, existuje $a \in H$ takové, že $g^{-1}ag \notin H$. Potom

$$g^{-1}agHg^{-1}a^{-1}g = g^{-1}gHg^{-1}g = H,$$

a tedy $g^{-1}ag \in N_G(H)$. Proto $N_G(H) > H$.

Jestliže H je maximální vlastní podgrupa, $N_G(H) = G$ a $H \lhd G$.

□

Lemma 8.7. *Počet podgrup řádu p v konečné p-grupě je $r_1 \equiv 1 \pmod p$.*

Označme X množinu prvků řádu p. Spočítáme $|X|$ dvěma způsoby. Vzhledem k tomu, že každé dvě různé podgrupy řádu p mají triviální průnik, počet prvků řádu p je $|X| = r_1(p-1)$.

Na druhé straně, uvažujme akci konjugací na množině X prvků řádu p. Centrální prvky řádu p tvoří spolu s 1 podgrupu $H \leq Z(G)$. Toto vyplývá z faktu $(xy)^i = x^i y^i$ pro $x, y \in H$. Proto $p^e = |H| = |X \cap H| + 1$ pro nějaké $e \geq 1$. Odtud $|X \cap H| = p^e - 1$. Velikost orbity x^G v akci konjugací pro $x \notin Z(G)$ je netriviální mocnina p. Proto $|X| = pm + p^e - 1$ pro nějaké m. Porovnáním dostaneme

$$r_1(p-1) = |X| = pm + p^e - 1.$$

Pokud vezmeme poslední rovnici modulo p, dostaneme $r_1 \equiv 1 \pmod p$.

Věta 8.8. *Počet podgrup řádu p^m v konečné p-grupě je $r_m \equiv 1 \pmod p$.*

Důkaz. Nechť $|G| = p^n$, $n \geq 2$. Spočítáme dvěma způsoby počet dvojic (H, K) podgrup grupy G takových, že $H < K$, $|H| = p^s$ a $|K| = p^{s+1}$ pro $1 \leq s < n$.

Nechť $(H, K_1), \ldots, (H, K_a)$ jsou všechny takové dvojice, které obsahují H. Podle věty 8.6 je $H \lhd K_j$, a tedy i $K_j \leq N_G(H) = N$. Uvažujme přirozenou projekci $\nu\colon N \to N/H$. Potom bijekce $K_j \mapsto K_j/H$ přiřadí podgrupě K_j podgrupu $K_j/H \leq N/H$, která je řádu p. Počet takových podgrup v N/H je $a \equiv 1 \pmod p$, (viz lemma 8.7).

Nechť $(H_1, K), \ldots, (H_b, K)$ jsou všechny dvojice pro fixovanou podgrupu K řádu p^{s+1}. Podle věty 8.6 je $H_i \lhd K$. Zřejmě $H_1 H_j = K$ pro $j > 1$, proto $|H_1 H_j| = p^{s+1}$ a z produktové rovnosti

$$|H_1 H_j| \cdot |H_1 \cap H_j| = |H_1| \cdot |H_j|$$

dostaneme $|H_1 \cap H_j| = p^{s-1}$. Označme $D_j = H_1 \cap H_j$. Zřejmě $D_j \lhd K$, neboť je průnikem dvou normálních podgrup. Potom $[K : D_j] = p^2$ a $K/D_j \cong H_1/D_j \times H_j/D_j \cong Z_p \times Z_p$. Proto K/D_j má $p^2 - 1$ prvků řádu p a $p + 1 = \frac{p^2-1}{p-1}$ podgrup řádu p. Bijekce $H \mapsto H/D_j$ nám dá $p+1$ podgrup grupy K řádu p^s obsahujících D_j. Dvě takové množiny podgrup pro $i \neq j$ jsou buď totožné, nebo mají společnou pouze H_1. Tedy pro $j = 2$ máme $p+1$ podgrup a další systémy podgrup přispívají p podgrupami. Proto $b \equiv 1 \pmod p$.

Počet dvojic (H, K) je $\sum_{i=1}^{r_s} a_i = \sum_{j=1}^{r_{s+1}} b_j$. Dosazením $a_i \equiv 1 \pmod{p}$ a $b_j \equiv 1 \pmod{p}$ dostaneme $r_s \equiv r_{s+1} \pmod{p}$. Nyní už tvrzení vyplývá z lemmatu 8.7. □

Důsledek 8.9. *V p-grupě G řádu p^n existuje pro každé $1 \leq s \leq n$ podgrupa řádu p^s. Navíc, pro každou podgrupu $H < G$ řádu p^s existuje grupa K řádu p^{s+1} taková, že $H < K \leq G$.*

Důkaz. Z věty 8.8 víme, že počet podgrup řádu p^s je kongruentní s 1 (mod p). Proto musí existovat alespoň jedna podgrupa takového řádu. V první části důkazu věty 8.8 jsme zjistili, že počet podgrup řádu p^{s+1} obsahující zvolenou grupu H řádu p^s je kongruentní s 1 (mod p). □

Lemma 8.10 (Landau, 1906)**.** *Nechť $q \in \mathbb{Q}$ je racionální číslo. Potom pro dané n existuje jen konečně mnoho n-tic $(m_1, \ldots, m_n)$, $m_i > 0$, $i = 1, \ldots, n$, takových, že $q = \sum_{j=1}^{n} \frac{1}{m_j}$.*

Důkaz. Budeme postupovat indukcí podle n. Jestliže $n = 1$, existuje nejvíce jedna 1-tice (m_1) taková, že $q = \frac{1}{m_1}$.

Můžeme předpokládat, že $m_1 \leq m_2 \leq \cdots \leq m_n$. Dále

$$q = \sum_{j=1}^{n} \frac{1}{m_j} \leq n \frac{1}{m_1}.$$

Odtud $m_1 \leq n/q$. Z indukčního předpokladu pro každé $k \leq n/q$ a $q' = q - \frac{1}{k}$ existuje jen konečně $(n-1)$-tic $(m_2, \ldots, m_k)$ takových, že

$$q - \frac{1}{k} = \sum_{j=2}^{n} \frac{1}{m_j}.$$

Odtud pro $k = 1, \ldots, \lfloor n/q \rfloor$ dostaneme konečně mnoho n-tic splňující podmínky. □

Věta 8.11. *Existuje jen konečně mnoho konečných grup s předepsaným počtem tříd konjugace.*

Důkaz. Nechť n je počet tříd konjugace a nechť $m = |Z(G)|$. Předělíme rovnost (8.1) řádem $|G|$. Tak dostaneme

$$1 = \sum_{j=1}^{m} \frac{1}{|G|} + \sum_{j=m+1}^{n} \frac{1}{|C_G(x_j)|}.$$

Z lemmatu 8.10 vyplývá, že existuje jen konečně mnoho možností pro výběr $|G|$ a $|C_G(x_j)|$, $j = m+1, \ldots, n$. Je však jen konečně mnoho konečných grup daného řádu. □

Cvičení

8.1. Nechť $H \lhd G$ a G/H jsou p-grupy. Dokažte, že i G je p-grupa.

8.2. Nechť $|G| = p^n$, kde p je prvočíslo. Dokažte, že pro každé k, $1 \leq k \leq n$, grupa G obsahuje normální podgrupu řádu p^k.

8.3. Nechť G je konečná p-grupa a $1 < H \lhd G$. Dokažte, že $H \cap Z(G) \neq 1$.

8.4. Nechť G je konečná p-grupa a $H \lhd G$, $|H| = p$. Dokažte, že $H \leq Z(G)$.

8.2 Sylowovy věty

Z Lagrangeovy věty vyplývá, že řád podgrupy dělí řád grupy. Zajímavý inverzní problém se ptá, zda pro daného dělitele d řádu konečné grupy G existuje podgrupa řádu d. V předchozím textu jsme ověřili platnost tohoto tvrzení pro cyklické grupy a pro p-grupy. Na druhé straně A_4 neobsahuje podgrupu řádu 6. Sylowovy věty tvoří základ pro studium struktury konečných grup. V této podkapitole budeme předpokládat, že všechny uvažované grupy jsou konečné.

Definice 8.12. Nechť p je prvočíslo. Potom Sylowova p-grupa grupy G je maximální p-podgrupa grupy G.

Lemma 8.13. *Nechť P je Sylowova podgrupa grupy G. Potom*

(i) $|N_G(P)/P|$ není dělitelné p,

(ii) jestliže řád $a \in G$ je mocnina p a zároveň $a^{-1}Pa = P$, nutně $a \in P$.

Důkaz. Předpokládejme, že p dělí $|N_G(P)/P|$. Potom z Cauchyho věty vyplývá, že existuje prvek $yP \in N_G(P)/P$. Nechť $\nu\colon N_G(P) \to N_G(P)/P$ je přirozená projekce. Uvažujme $\nu^{-1}\langle yP\rangle$. To je p-grupa $H > P$, dostáváme spor s maximalitou P.

Uvažujme vhodnou mocninu b prvku a, která je řádu p. Zřejmě $a \in N_G(P)$. Uvažujme $aP \in N_G(P)/P$. Potom řád $|aP| = p$, dostali jsme spor s (i). □

Věta 8.14 (Sylow, 1872)**.** *Nechť p je prvočíslo.*

- *Pokud P je Sylowova p-podgrupa grupy G, všechny Sylowovy podgrupy grupy G jsou konjugované s P.*
- *Nechť r je počet Sylowových p-podgrup. Potom r dělí $|G|$ a $r \equiv 1 \pmod{p}$.*

Důkaz. Označme $P_1 = P$ a nechť $X = \{P_1, P_2, \ldots, P_r\}$ je množina podgrup konjugovaných s P. Grupa G má akci na X, $a \cdot P_i = P_i^a$. Nechť Q je Sylowova p-podgrupa. Potom Q má akci konjugací na X, která je restrikcí akce G. Uvažujme orbity akce Q na X. Podle věty 7.31 je velikost orbity rovna indexu stabilizátoru. Proto velikost každé orbity je mocnina p. Předpokládejme, že orbita obsahující P_i má velikost 1. To znamená, že pro každé $a \in Q$, platí $a^{-1}P_ia = P_i$. Podle lemmatu 8.13(ii) každé $a \in Q$ patří do P_i, proto $Q \leq P_i$. Z maximality Q

plyne $Q = P_i$. Jestliže položíme $Q = P_1$, všechny orbity s výjimkou $\{P_1\}$ mají velikost nějakého násobku p. Proto $r \equiv 1 \pmod{p}$. Předpokládejme, že existuje Sylowova p-podgrupa Q, která se nenachází v X. Potom velikost každé orbity akce Q na X je násobkem p. Vzhledem k tomu, že X je disjunktní sjednocení orbit, $r \equiv 0 \pmod{p}$, a dostáváme spor s předchozím.

Máme $r = |X| = |P^G| = [G : N_G(P)]$, a proto r dělí $|G|$.

□

Příklad 8.15. Řád grupy S_4 je $24 = 2^3 \cdot 3$. Zřejmě $D_8 \leq S_4$ (uvažujeme grupu symetrií čtverce), tedy D_8 je Sylowova 2-grupa v S_4. Sylowova věta říká, že všechny Sylowovy 2-grupy jsou konjugované, a tedy izomorfní, a jejich počet r je lichým dělitelem 24. Jestliže například $H = \langle (1,2,3,4), (2,4) \rangle \cong D_8$, je $H^{(1,2)} = \langle (1,2,3,4)^{(1,2)}, (2,4)^{(1,2)} \rangle = \langle (1,3,4,2), (1,4) \rangle$ jiná Sylowova 2-grupa. Proto $r > 1$. Jediný netriviální lichý dělitel 24 je 3. Proto S_4 obsahuje přesně tři Sylowovy 2-grupy. Sylowovy 3-grupy jsou cyklické, generované 3-cykly. Lehce nalezneme $4 \equiv 1 \pmod{3}$ takovéto podgrupy.

Důsledek 8.16. *Grupa G má jedinou Sylowovu p-grupu právě tehdy, když G má normální Sylowovu p-grupu.*

Důkaz. Jestliže existuje jediná Sylowova p-grupa $P \leq G$, je $P^g = P$ pro každý prvek $g \in G$, a tedy $P \lhd G$.

A naopak, nechť $P \lhd G$ je normální Sylowova p-grupa. Jestliže Q je Sylowova p-grupa, z věty 8.14 vyplývá, že existuje $g \in G$ takové, že $Q = P^g = P$.

□

Věta 8.17. *Nechť G je konečná grupa řádu $p^e m$, $\gcd(p, m) = 1$. Potom každá Sylowova p-grupa má řád p^e.*

Důkaz. Nechť P je Sylowova p-grupa. Chceme dokázat, že p nedělí $[G : P]$. Nechť $N = N_G(P)$, potom $[G : P] = [G : N][N : P]$. Z důsledku 7.34 je index $[G : N]$ roven počtu podgrup konjugovaných s P. Podle věty 8.14 je $[G : N] \equiv 1 \pmod{p}$. Z lemmatu 8.13 p nedělí $[N : P]$. Tedy p nedělí $[G : N][N : P] = [G : P]$.

Z Lagrangeovy věty plyne $|P| = p^k$ pro nějaké $k \leq e$. Z rovnosti $mp^e = |G| = |P| \cdot [G : P]$, $\gcd(m, p) = 1 = \gcd([G : P], p)$, vyplývá, že p^e dělí $|P|$. Proto $|P| = p^e$.

□

Následující věta dává odpověď na otázku existence podgrupy daného řádu v případě, že tento předepsaný řád je mocninou prvočísla. Obecně ale není možné dokázat více.

Věta 8.18. *Nechť p je prvočíslo a nechť G je konečná grupa. Nechť p^k dělí řád $|G|$. Potom G obsahuje podgrupu řádu p^k.*

Důkaz. Nechť p^e je maximální mocnina p taková, že p^e dělí $|G|$. Jestliže $k = e$, tvrzení vyplývá z věty 8.18. Uvažujme Sylowovu p-grupu P řádu p^e. Jestliže $k < e$, existence podgrupy řádu p^k v P vyplývá z věty 8.8. □

Věta 8.19 (Frattiniho argument)**.** *Nechť $K \lhd G$ je normální podgrupa v konečné grupě. Nechť P je Sylowova p-grupa grupy K. Potom $G = KN_G(P)$.*

Důkaz. Z normálnosti K pro každé $g \in G$ platí $P^g \leq K^g = K$. Proto P^g je Sylowova p-grupa grupy K. Z věty 8.14 vyplývá, že existuje $k \in K$ takové, že $gPg^{-1} = kPk^{-1}$, a proto $k^{-1}gPg^{-1}k = P$. Z poslední rovnosti dostáváme $k^{-1}g \in N_G(P)$. Proto $g = k(k^{-1}g)$ je hledaný rozklad. □

Cvičení

8.5. Nechť X je konečná G-množina a nechť H má tranzitivní akci na X. Potom $G = HG_x$. Dokažte pomocí tohoto tvrzení Frattiniho argument.

8.6. Dokažte, že Sylowovy podgrupy grupy G generují G.

8.7. Nechť pro každé prvočíslo p, které dělí řád G, má G jedinou Sylowovu p-grupu. Dokažte, že G je přímým součinem svých Sylowových p-grup, kde p bereme přes všechna prvočísla, které dělí $|G|$.

8.8. Najděte všechny Sylowovy 2-grupy pro A_5.

8.3 Grupy malého řádu

Věta 8.20. *Každá grupa řádu $2p$ je cyklická nebo dihedrální.*

Důkaz. Jestliže $p = 2$, je $|G| = 4$ a tvrzení vyplývá z důsledku 8.5. Jestliže $p > 2$, z Cauchyho věty vyplývá, že G obsahuje prvek s řádu p a prvek t řádu 2. Podgrupa $H = \langle s \rangle$ je indexu 2, proto $H \lhd G$. A proto $tst = s^i$ pro nějaké i. Dále

$$s = t^2st^2 = t(tst)t = ts^it = (tst)^i = s^{i^2},$$

proto $i^2 \equiv 1 \pmod{p}$. Navíc $(Z_p; +, \cdot)$ je pole, proto máme jen dvě řešení $i = \pm 1$.

Jestliže $i = 1$, je G komutativní grupa a prvek st má řád $2p$. Potom $G = \langle st \rangle$ je cyklická.

Jestliže $i = -1$, je $G = \langle s, t \rangle$ izomorfní dihedrální grupě. □

Věta 8.21. *Jestliže $|G| = pq$, kde $p > q$ jsou prvočísla, je G buď cyklická, nebo*

$$G = \langle a, b; b^p = 1, a^q = 1, aba^{-1} = b^m \rangle,$$

kde q dělí $p - 1$, $m^q \equiv 1 \pmod{p}$ a současně $m \not\equiv 1 \pmod{p}$.

Důkaz. Z Cauchyho věty G obsahuje prvek b řádu p, podgrupa $P = \langle b \rangle$ má index q. Uvažujme homomorfismus $\psi\colon G \to S_q$ daný levým násobením na levých třídách rozkladu podle P. Potom $\ker(\psi) \leq P$. Proto $\ker(\psi) = P$ nebo $\ker(\psi) = 1$. Pokud by $\ker(\psi) = 1$, je ψ monomorfismus a $\psi(b)$ je prvek řádu $p > q$ v S_q. Takový prvek grupa S_q neobsahuje. Proto $\ker(\psi) = P$ a $P \lhd G$.

Z Cauchyho věty G obsahuje prvek a řádu q. Označme $Q = \langle a \rangle$. Protože Q je Sylowova q-grupa, počet konjugantů je dělitelem $|G| = pq$ a $c = 1 + kq$ pro nějaké k. Buď $k = 0$ a $c = 1$ nebo $c = p = 1 + kq$.

V prvním případě je $Q \lhd G$, $G = P \times Q = \langle ab \rangle \cong C_{pq}$.

Ve druhém případě $q|p-1$ a Q není normální podgrupa. Protože $P \lhd G$, pro nějaké m platí $aba^{-1} = b^m$. Dále můžeme předpokládat $m \not\equiv 1 \pmod{p}$, jinak dostaneme předchozí abelovský případ. Indukcí dokážeme, že $a^j b a^{-j} = b^{m^j}$. Pro $j = q$ dostaneme požadovaný vztah.

□

Definice 8.22. Grupa kvaternionů je grupa $Q = \langle a, b \rangle$ řádu 8 splňující podmínky $a^4 = 1$, $b^2 = a^2$ a $bab^{-1} = a^{-1}$.

Poznámka: Ve cvičeních v kapitole 5 jsme definovali grupu kvaternionů jako podgrupu $GL(2, \mathbb{C})$ generovanou pomocí matic

$$A = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}, B = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

Dá se dokázat, že přiřazení $a \mapsto A$ a $b \mapsto B$ definuje izomorfismus grup. Jedná se tedy o tu samou grupu.

Věta 8.23. *Grupy Q a D_8 jsou jediné neabelovské grupy řádu 8.*

Důkaz. Nechť G je neabelovská grupa řádu 8. Jestliže $x \neq 1$, platí $|x| \in \{2, 4, 8\}$.

Pokud existuje $x \in G$, $|x| = 8$, je G cyklická a dostáváme spor.

Nechť všechny netriviální prvky mají řád 2. Pokud x a y, $x \neq y$, jsou dva takové prvky, pro $z = xy$ platí: $z \neq x$, $z \neq y$, $z \neq 1$ a $1 = z^2 = (xy)^2$. Proto $\langle x, y \rangle \cong C_2 \times C_2$. Nechť $z \notin \langle x, y \rangle$. Potom opakováním úvahy je $\langle x, z \rangle \cong C_2 \times C_2$ a $\langle z, y \rangle \cong C_2 \times C_2$. Proto x, y, z vzájemně komutují a $G \cong C_2 \times C_2 \times C_2$.

Tedy v G existuje prvek a takový, že $|a| = 4$. Potom $\langle a \rangle \lhd G$ a $G/\langle a \rangle \cong Z_2$. Pokud $b \notin \langle a \rangle$, platí $b^2 \in \langle a \rangle$. Pokud $b^2 = a$ nebo $b^2 = a^3 = a^{-1}$, platí $|b| = 8$, dostáváme spor. Proto $b^2 = a^2$ nebo $b^2 = 1$. Dále $\langle a \rangle \lhd G$ dává dvě možnosti: $bab^{-1} = a$ nebo $bab^{-1} = a^{-1}$. V prvním případě je G abelovská a dostáváme spor. Pokud $b^2 = 1$, je G dihedrální. Pokud $b^2 = a^2$, G je grupa kvaternionů. □

Definice 8.24. $T = \langle a, b; a^6 = 1, b^2 = a^3 = (ab)^2 \rangle$.

Není úplně jasné, zda T splňující podmínky řádu 12, existuje.

Posloupnost σ definující počet grup daného řádu má komplikované chování související s vlastnostmi přirozených čísel. Je známé, že "skoro všechny" grupy jsou 2-grupy. Například $\sigma(2^4) = 14$, $\sigma(2^5) = 51$, $\sigma(2^6) = 267$ a $\sigma(2^7) = 2328$.

Grupy malých řádů jsou uvedeny v tabulce:

Na následujícím příkladu si ukážeme další aplikaci Sylowových vět.

Tabulka 8.1: Malé grupy

Řád	**Počet**	**Grupy**
4	2	Z_4, $Z_2 \times Z_2$
6	2	Z_6, S_3
8	5	Z_8, $Z_4 \times Z_2$, Z_2^3, D_8, Q
9	2	Z_9, Z_3^2
10	2	Z_{10}, D_{10}
12	2	Z_{12}, $Z_6 \times Z_2$, D_{12}, A_4, T
14	2	Z_{14}, D_{14}
15	2	Z_{10}

Příklad 8.25. Neexistuje jednoduchá grupa řádu $n = 30$ a $n = 36$.

Nechť $n = 30 = 5 \cdot 3 \cdot 2$. V G existuje $r \equiv 1 \pmod 5$ Sylowových 5-grup, $r \neq 1$ a $r|30$. Jediný vhodný dělitel je 6. Počet prvků v těchto grupách je $6 \cdot 4 \neq 1$. Podobně musí být 10 Sylowových 3-grup, což dává 20 netriviálních prvků. A tedy triviálně $20 + 24 > 30$.

Nechť $n = 36 = 9 \cdot 4$. Ze Sylowových vět víme, že G obsahuje 4 Sylowovy 3-grupy. Nechť P je jedna z nich. Grupa P je indexu 4, proto existuje homomorfismus $\psi\colon G \to S_4$ daný akcí G na levých třídách P s jádrem $\ker(\psi) \leq P$. Jelikože je ale G jednoduchá, je $\ker(\psi) = 1$, což znamená, že S_4 obsahuje kopii G. A tedy triviálně $|G| = 36 > 24 = |S_4|$.

Cvičení

8.9. Identifikujte všechny vlastní podgrupy S_4.

8.10. Dokažte, že pro každý dělitel d čísla 24 existuje v S_4 podgrupa řádu d.

8.11. Dokažte, že neexistuje jednoduchá grupa řádu p^2q, kde p, q jsou prvočísla.

8.12. Najděte příklad dvou neizomorfních grup takový, že pro každé přirozené číslo d jsou počty prvků řádu d stejné.

Kapitola 9

Fundamentální věta o konečných abelovských grupách

Věta 9.1. *Každá konečná abelovská grupa G je přímým součinem cyklických grup, jejichž řád je mocnina prvočísla. Počet takovýchto cyklických grup v rozkladu G je jednoznačně určen grupou G. Rovněž i jejich řády jsou jednoznačně určené grupou G.*

Důkaz rozdělíme do několika pomocných lemmat.

Lemma 9.2. *Nechť G je konečná abelovská grupa, $|G| = \prod p_i^n$, kde p_i jsou po dvou různá prvočísla, $n_i \geq 1$. Potom $G = G(p_1) \times G(p_2) \times \cdots \times G(p_n)$, kde $|G(p_i)| = p_i^{n_i}$.*

Důkaz. Ze Sylowových vět vyplývá, že v G existují Sylowovy podgrupy $G(p_i)$ příslušných řádů. Vzhledem k tomu, že G je abelovská, grupy $G(p_i)$ jsou normální. Z Lagrangeovy věty vyplývá, že $G(p_i) \cap G(p_j) = 1$ pro $i \neq j$. Proto $H = G(p_1) \times G(p_2) \times \cdots \times G(p_n) \leq G$. Ale $|H| = |G|$, proto $H = G$. □

Poznámka: jednu Sylowovu p-grupu $G(p) \leq G$ je snadné identifikovat. Jestliže $|G| = p^e m$, $\gcd(p, m) = 1$, je $G(p) = \{x \in G; x^{p^e} = 1\}$.

Lemma 9.3. *Nechť G je abelovská p-grupa a nechť a je prvek maximálního řádu. Potom existuje vlastní podgrupa $K < G$ taková, že $G = \langle a \rangle \times K$.*

Důkaz. Nechť $|G| = p^n$. Budeme postupovat indukcí podle n. Pokud $n = 1$, je $|G| = \langle a \rangle \times \langle 1 \rangle$. Nechť $n > 1$. Pokud $|a| = p^k$ a $k = n$, je $|G| = \langle a \rangle \times \langle 1 \rangle$. Takže dále budeme předpokládat $k < n$. Zřejmě existuje $b \neq \langle a \rangle$. Potom existuje také b minimálního rádu p^m.

Tvrdíme, že $\langle a\rangle \cap \langle b\rangle = 1$. Z výběru b dostaneme $b^p \in \langle a\rangle$, proto $b^p = a^i$ pro nějaké i. Máme

$$1 = b^{p^m} = (b^p)^{p^{m-1}} = (a^i)^{p^{m-1}}.$$

A dále máme $|a^i| \leq p^{m-1} < |b| \leq |a|$, proto a^i není generátor $\langle a\rangle$. Odtud existuje j takové, že $i = pj$. Uvažujme $c = a^{-j}b$. Potom $c \notin \langle a\rangle$ a platí

$$c^p = a^{-jp}b^p = a^{-i}b^p = b^{-p}b^p = 1.$$

Proto $|c| = p$, a tedy i řád $|b| = p$. Potom $\langle a\rangle \cap \langle b\rangle = 1$. Uvažujme přirozenou projekci $\psi\colon G \to G/\langle b\rangle$. Faktorová grupa $\bar{G}$ má menší řád a $\bar{a} = a\langle b\rangle$ má řád $p^k = |a|$. Proto $\bar{a}$ je prvek maximálního řádu a podle indukčního předpokladu $\bar{G} = \langle \bar{a}\rangle \times \bar{K}$. Potom $\langle a\rangle = \psi^{-1}(\bar{a})$ a $K = \psi^{-1}(\bar{K})$ jsou disjunktní normální podgrupy, přičemž $|G| = |\langle a\rangle| \cdot |K|$. Proto $G = \langle a\rangle \times K$. □

Lemma 9.4. *Nechť G je abelovská p-grupa. Nechť $G = H_1 \times H_2 \times \cdots \times H_m$ a $G = K_1 \times K_2 \times \cdots \times K_n$ jsou rozklady na netriviální cyklické podgrupy, přičemž $|H_1| \geq |H_2| \geq \cdots \geq |H_m|$ a $|K_1| \geq |K_2| \geq \cdots \geq |K_n|$.*

Potom $m = n$ a $|H_i| = |K_i|$, $i = 1, \ldots, m$.

Důkaz. Budeme postupovat indukcí podle $|G|$. Jestliže $|G| = p$, tvrzení platí.

Nechť $|G| > p$. Uvažujme grupu $G^p = \{x^p; x \in G\} < G$. Zřejmě $G^p = H_1^p \times H_2^p \times \cdots \times H_{m'}^p$, $G = K_1 \times K_2 \times \cdots \times K_{n'}$, kde $m' \leq m$ a $n' \leq n$ jsou maximální přirozená čísla $m' \leq m$ a $n' \leq n$ taková, že řád $|H_{m'}| > p$ a řád $|H_{n'}| > p$. Podle indukčního předpokladu je $m' = n'$ a $|H_i^p| = |K_i^p|$ pro $1 \leq i \leq m' = n'$. Potom $|H_i| = |H_i^p|p$, $|K_i| = |K_i^p|p$, proto $H_i = K_i$ pro $i \leq m'$. Nakonec

$$|H_1||H_2|\ldots|H_{m'}|p^{m-m'} = |G| = |K_1||K_2|\ldots|K_{m'}|p^{n-n'}.$$

Odtud $m = n$ a zbylé grupy H_i, K_i pro $i > m' = n'$ jsou cyklické grupy řádu p. □

Definice 9.5. Pro dané číslo n označme $U(n) = \{x;\ 1 \leq x < n, \gcd(n, x) = 1\}$ multiplikativní grupu jednotek modulo n s násobením $z = x \cdot y \pmod n$.

Příklad 9.6. Uvažujme multiplikativní grupu $U(65)$. Její řád je $|U(65)| = \varphi(5 \cdot 13) = \varphi(5)\varphi(13) = 4 \cdot 12 = 48 = 3 \cdot 16$. Zjistíme multiplikativní řád 2. Protože $2^3 \cdot 2^3 = 64 \equiv -1 \pmod{65}$, je $||2|| = 12$. Potom $2^4 = 16$ generuje Sylowovu 3-grupu. Komplementární 2-grupu řádu 16 najdeme tak, že identifikujeme prvky, jejichž multiplikativní řád je mocnina 2. Jsou to následující prvky:

Tabulka 9.1: $S(2) \leq U(65)$

Prvek	1	8	12	14	18	21	27	31	34	38	44	47	51	53	57	64
Řád	1	4	4	2	4	4	4	4	4	4	4	4	2	4	4	2

Maximální řád prvků v $G = S(2)$ je 4. To dává dvě možnosti: $G \cong Z_4 \times Z_4$ a $G \cong Z_4 \times Z_2 \times Z_2$. Grupa $Z_4 \times Z_2 \times Z_2$ obsahuje 7 prvků řádu dva, ale podle tabulky 9.1, má G jen 3 prvky řádu dva. Proto $G \cong Z_4 \times Z_4$. Jeden možný rozklad je $G = \langle 8 \rangle \times \langle 31 \rangle$ a

$$U(65) = \langle 16 \rangle \times \langle 8 \rangle \times \langle 31 \rangle \cong Z_3 \times Z_4 \times Z_4.$$

Důsledek 9.7. *Pro každého dělitele d řádu $|G|$ konečné abelovské grupy G existuje podgrupa grupy G řádu d.*

Příklad 9.8. Nechť $|G| = 72 = 2^3 \cdot 3^2$. Najděte v G podgrupy řádu 12. Podle fundamentální věty je G izomorfní jedné ze šesti grup. Z každého rozkladu lehce najdeme podgrupu daného řádu, viz tabulka 9.2.

Tabulka 9.2: Abelovské grupy řádu 72 a jejich podgrupy řádu 12

Grupa	Podgrupa řádu 12
$Z_8 \times Z_9$	$Z_4 \times Z_3 \cong Z_{12}$
$Z_8 \times Z_3 \times Z_3$	$Z_4 \times Z_3 \times 1 \cong Z_{12}$
$Z_4 \times Z_2 \times Z_9$	$Z_4 \times 1 \times Z_3 \cong Z_{12}$
$Z_4 \times Z_2 \times Z_3 \times Z_3$	$Z_4 \times 1 \times Z_3 \times 1 \cong Z_{12}$
$Z_2 \times Z_2 \times Z_2 \times Z_9$	$Z_2 \times Z_2 \times 1 \times Z_3 \cong Z_2 \times Z_6$
$Z_2 \times Z_2 \times Z_2 \times Z_3 \times Z_3$	$Z_2 \times Z_2 \times 1 \times Z_3 \times 1 \cong Z_2 \times Z_6$

Rozklady grup můžeme úsporněji zapsat v tzv. Smithově formě jako součin cyklických grup $\prod C_i$, kde $|C_{i+1}|$ dělí $|C_i|$. Například, $Z_2 \times Z_2 \times Z_2 \times Z_3 \times Z_3 \cong Z_6 \times Z_6 \times Z_2$ a $Z_4 \times Z_2 \times Z_3 \times Z_3 \cong Z_{12} \times Z_6$.

Cvičení

9.1. Zjistěte počty prvků řádu 2 a řádu 4 v následujících grupách: Z_{16}, $Z_8 \times Z_2$, $Z_4 \times Z_4$ a $Z_4 \times Z_2 \times Z_2$.

9.2. Množina $G = \{1, 9, 16, 22, 29, 53, 74, 79, 81\}$ je grupa s násobením modulo 91. Najděte kanonický rozklad G na cyklické grupy.

9.3. Dokažte, že neexistuje jednoduchá grupa řádu p^2q, kde p, q jsou prvočísla.

9.4. Nechť G je grupa diagonálních matic typu $n \times n$ s hodnotami ± 1 na diagonále. Najděte kanonický rozklad G.

Kapitola 10

Normální řetězce podgrup

10.1 Jordan-Hölderova věta

Definice 10.1. *Normální řetězec* v grupě G je posloupnost podgrup

$$G = G_0 \geq G_1 \geq \cdots \geq G_n \geq 1,$$

kde pro každé $i = 0, \ldots, n-1$ platí $G_{i+1} \triangleleft G_i$. *Podílové grupy* normálního řetězce jsou grupy G_i/G_{i+1}, $i = 0, 1, \ldots, n-1$; jeho *délka* je počet vlastních inkluzí (nebo jinak délka je počet jeho netriviálních podílových grup).

Definice 10.2. Normální řetězec

$$G = H_0 \geq H_1 \geq \cdots \geq H_m = 1$$

je *zjemněním* normálního řetězce

$$G = G_0 \geq G_1 \geq \cdots \geq G_n = 1,$$

jestliže $G_0, G_1, \ldots, G_n$ je vybraná posloupnost z postupnosti $H_0, H_1, \ldots, H_m$.

Definice 10.3. *Kompoziční řetězec* je normální řetězec

$$G = G_0 \geq G_1 \geq \cdots \geq G_n = 1,$$

ve kterém pro všechny $i = 0, \ldots, n-1$, je G_{i+1} maximální vlastní normální podgrupa grupy G_i nebo $G_{i+1} = G_i$.

Definice 10.4. Dva normální řetězce grupy G jsou *ekvivalentní*, jestliže existuje bijekce mezi jejich netriviálními podílovými grupami taková, že odpovídající podílové grupy jsou izomorfní.

Zřejmě ekvivalentní normální řetězce mají stejnou délku.

Lemma 10.5. (Zassenhaus)
Nechť $A \lhd A^*$ a $B \lhd B^*$ jsou čtyři podgrupy grupy G. Potom

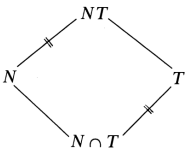
$$A(A^* \cap B) \lhd A(A^* \cap B^*),$$

$$B(B^* \cap A) \lhd B(B^* \cap A^*),$$

a existuje izomorfismus

$$\frac{A(A^* \cap B^*)}{A(A^* \cap B)} \cong \frac{B(B^* \cap A^*)}{B(B^* \cap A)}.$$

Důkaz. Všimněme si, že tvrzení je symetrické na záměnu symbolů A a B. Připomeňme si druhou větu o izomorfismu: Nechť $N \lhd G$ a $T \leq G$. Potom $N \cap T \lhd T$ a $T/(N \cap T) \cong NT/N$.



Ve druhé větě o izomorfismu položíme $G = A^*$, $N = A \lhd A^*$ a $T = A^* \cap B^*$. Potom

$$N \cap T = A \cap (A^* \cap B^*) = A \cap A^* \cap B^* = A \cap B^* \lhd A^* \cap B^* = T.$$

Pokud položíme $N = B \lhd B^*$, podobnou úvahou dostaneme $B \cap A^* \lhd A^* \cap B^*$. Vzhledem k tomu, že $A \lhd A^*$ i $B \lhd B^*$, je $A(A^* \cap B) \lhd A(A^* \cap B^*)$ i $B(B^* \cap A) \lhd B(B^* \cap A^*)$. Protože $A \cap B^* \lhd A^* \cap B^*$ i $A^* \cap B \lhd A^* \cap B^*$, je $D = (A \cap B^*)(A^* \cap B) \lhd A^* \cap B^*$.

Dalším krokem důkazu je konstrukce epimorfismu

$$f\colon B(B^* \cap A^*) \to (A^* \cap B^*)/D.$$

Jestliže $x \in B(B^* \cap A^*)$, je $x = bc$, kde $b \in B$ a $c \in B^* \cap A^*$. Položíme $f(x) = f(bc) = cD$. Zobrazení f je dobře definované, neboť jestliže $x = b_1c_1 = b_2c_2$, je $c_2 = b_2^{-1}b_1c_1$, a proto platí: $f(b_1c_1) = c_1D = f(b_2b_2^{-1}b_1c_1) = f(b_2c_2)$. Zřejmě f je surjekce. Dále nechť $x = b_1c_1$, $y = b_2c_2$. Použitím $c_1 \in B^* \cap A^*$ a $B \lhd B^*$ dostaneme

$$b_1c_1b_2c_2 = b_1(c_1b_2c_1^{-1})c_1c_2 = b_1b_2'c_1c_2,$$

kde $b_2' \in B$.

Potom

$$f(xy) = f(b_1c_1b_2c_2) = f(b_1b_2'c_1c_2) = c_1c_2D = c_1Dc_2D = f(x)f(y).$$

Zřejmě $f(x) = D$ právě tehdy, když $x = bc_1c_2$, kde $b \in B$, $c_1 \in A^* \cap B$ a $c_2 \in A \cap B^*$. Takovéto prvky tvoří množinu $B(A^* \cap B)(A \cap B^*) = B(A \cap B^*)$.

Tedy f je epimorfismus s jádrem $\ker(f) = B(B^* \cap A)$. Podle první věty o izomorfismu platí

$$\frac{B(B^* \cap A^*)}{B(B^* \cap A)} \cong \frac{A^* \cap B^*}{D}.$$

Záměnou A a B dostaneme

$$\frac{A(A^* \cap B^*)}{A(A^* \cap B)} \cong \frac{A^* \cap B^*}{D}.$$

□

Věta 10.6. (Schreierova zpřesňovací věta – Schreier Refinement Theorem)
Pro každé dva normální řetězce existují jejich zjemnění, která jsou ekvivalentní.

Důkaz. Nechť

$$G = H_0 \geq H_1 \geq \cdots \geq H_m = 1,$$

$$G = G_0 \geq G_1 \geq \cdots \geq G_n = 1$$

jsou normální řetězce pro grupu G. Položme $G_{i,j} = G_{i+1}(G_i \cap H_j)$ pro všechny $j = 0, 1, \ldots, m$. Ze vztahu $H_j \geq H_{j+1}$ platí

$$G_{i,j} = G_{i+1}(G_i \cap H_j) \geq G_{i+1}(G_i \cap H_{j+1})$$

pro $j = 0, \ldots, m-1$. Dále

$$G_{i,0} = G_{i+1}(G_i \cap H_0) = G_{i+1}(G_i \cap G) = G_{i+1}G_i = G_i$$

a rovněž

$$G_{i,m} = G_{i+1}(G_i \cap H_m) = G_{i+1}(G_i \cap 1) = G_{i+1}.$$

Proto

$$G_i = G_{i,0} \geq G_{i,1} \geq \ldots G_{i,m-1} \geq G_{i,m} = G_{i+1} = G_{i+1,0}$$

pro $i = 0, \ldots, n-1$ a $j = 0, \ldots, m$.

Položíme v Zassenhausově lemmatu $A = G_{i+1}$, $A^* = G_i$, $B = H_{j+1}$ a $B^* = H_j$. Potom dostaneme $G_{i,j+1} \lhd G_{i,j}$. Proto posloupnost $\{G_{i,j}\}$ (s lexikálním uspořádáním dvojitých indexů) tvoří normální řetězec podgrup grupy G, který je zjemněním řetězce $\{G_i\}$.

Podobně položíme $H_{i,j} = H_{j+1}(H_j \cap G_i) \geq H_{j+1}(H_j \cap G_{i+1}) = H_{i+1,j}$,

$$H_j = H_{0,j} \geq H_{1,j} \geq \ldots H_{n-1,j} \geq H_{n,j} = H_{j+1}$$

pro $i = 0, 1, \ldots, n$ a $j = 0, \ldots, m-1$. Ze Zassenhausova lemmatu vyplývá, že $\{H_{i,j}\}$ s uspořádáním indexů $(i,j) < (s,t)$, jestliže $j < t$, nebo $j = t$ a $i < s$, tvoří normální řetězec podgrup grupy G, který je zjemněním řetězce $\{H_j\}$. Navíc bijekce $G_{i,j}/G_{i,j+1} \to H_{i,j}/H_{i+1,j}$, páruje izomorfní faktorové grupy.

□

Definice 10.7. Podílové grupy v kompozičním řetězci se nazývají *kompoziční faktory* grupy G.

Věta 10.8. (Jordan-Hölder)
Každé dva kompoziční řetězce jsou ekvivalentní.

Důkaz. Kompoziční řetězce jsou normální řetězce maximální délky. Podle Schreierovy věty existují zjemnění, která jsou ekvivalentní. Zjemnění řetězce maximální délky však musí být ekvivalentní původnímu řetězci. Proto i původní řetězce musí být ekvivalentní. □

Jordan-Hölderovu větu můžeme považovat za zobecnění fundamentální věty aritmetiky.

Důsledek 10.9. (Fundamentální věta aritmetiky – Fundamental Theorem of Arithmetic)
Prvočísla a jejich mocniny vyskytující se při faktorizaci přirozeného čísla $n \geq 2$ jsou jednoznačně určeny právě číslem n.

The primes and their multiplicities occurring in the factorization of an integer $n \geq 2$ are determined by n.

Důkaz. Uvažujme cyklickou grupu $G = \langle x \rangle$ řádu $n = p_1 p_2 \dots p_t$. Potom

$$G = \langle x \rangle \rhd \langle x^{p_1} \rangle \rhd \langle x^{p_1 p_2} \rangle > \dots \langle x^{p_1 p_2 \cdots p_{t-1}} \rangle \rhd \langle x^{p_1 p_2 \cdots p_t} \rangle = 1$$

je kompoziční řád s podílovými grupami $G_i/G_{i+1} \cong Z_{p_{i+1}}$, $i = 0, 1, \dots, t-1$. Jordan-Hölderova věta tvrdí, že čísla p_i závisí jen na n. □

10.2 Řešitelné grupy

Definice 10.10. Konečná grupa G se nazývá **řešitelná**, jestliže existuje normální řetězec pro G, pro který všechny podílové grupy jsou cyklické prvočíselných řádů. Ekvivalentně, G je řešitelná, jestliže existuje kompoziční řetězec grupy G, pro který všechny podílové grupy jsou cyklické prvočíselných řádů.

Věta 10.11. *Pokud $n \geq 5$, S_n není řešitelná.*

Důkaz. Zřejmě $S_n \rhd A_n \rhd 1$ je kompoziční řetězec s podílovými grupami Z_2 a A_n. □

Definice 10.12. Normální řetězec grupy G se nazývá *řešitelný*, jestliže existuje normální řetězec grupy G takový, že všechny podílové grupy jsou abelovské.

Lemma 10.13. *Grupa G je řešitelná právě tehdy, když má řešitelný řetězec.*

Důkaz. Pokud G je řešitelná, její kompoziční řetězec je řešitelný.

Nechť G má řešitelný řetězec $G = G_0 \rhd G_1 \rhd \cdots \rhd G_k = 1$. Nechť $\{H_j\}$ je kompoziční řetězec. Podle Schreierovy věty existuje zjemnění $\{G_i\}_{i=0}^{k}$, které je ekvivalentní $\{H_j\}_{j=0}^{m}$.

Nechť G má řešitelný řetězec. Nechť K je podgrupa zjemnění $G_i \rhd K \rhd G_{i+1}$. Potom existuje epimorfismus z abelovské grupy $G_i/G_{i+1} \to K/G_{i+1}$. Proto všechny podílové grupy zjemnění jsou abelovské, a tedy i podílové grupy kompozičního řetězec jsou cyklické prvočíselného řádu. □

Věta 10.14. *Každá podgrupa $H \leq G$ řešitelné grupy G je řešitelná.*

Důkaz. Pokud $G = G_0 \geq G_1 \geq \cdots \geq G_n = 1$ je řešitelný řetězec, je $H = H_0 \geq H \cap G_1 \geq \cdots \geq H \cap G_n = 1$ rovněž řešitelný řetězec. To vyplývá z druhé věty o izomorfismu pro $G = G_i$, $N = G_{i+1}$, $T = H \cap G_i$ a výpočtu

$$H \cap G_{i+1} = (H \cap G_i) \cap G_{i+1} \lhd H \cap G_i.$$

Dále

$$(H \cap G_i)/(H \cap G_{i+1}) \cong G_{i+1}(H \cap G_i)/G_{i+1} \leq G_i/G_{i+1}.$$

Protože G_i/G_{i+1} je abelovská, i $(H \cap G_i)/(H \cap G_{i+1})$ je abelovská. □

Věta 10.15. *Každý kvocient G/N řešitelné grupy G je řešitelný.*

Důkaz. Dokážeme následující tvrzení: Nechť G je řešitelná s řešitelným řetězcem $\{G_i\}_{i=0}^t$. Pokud $f\colon G \to H$ je epimorfismus, je $\{f(G_i)\}_{i=0}^t$ řešitelný řetězec grupy H.

Tvrzení dostaneme, jestliže položíme $H = G/N$, kde $N \lhd G$. Nechť $x_i \in G_i$, $i = 0, 1, \ldots, t-1$.

Nechť $h_i = f(x_i) \in f(G_i)$. Potom

$$h_i f(x_{i+1}) h_i^{-1} = f(x_i) f(x_{i+1}) f(x_i) = f(x_i x_{i+1} x_i^{-1}) \leq f(G_{i+1}).$$

Proto $f(G_{i+1}) \lhd f(G_i)$ a $f(G_0) = f(G) = H$. Tedy $\{f(G_i)\}_{i=0}^t$ je normální řetězec grupy H. Zbývá dokázat, že tento řetězec je řešitelný. Označme $p\colon f(G_i) \to f(G_i)/f(G_{i+1})$ přirozenou projekci $f(x_i) \mapsto f(x_i)f(G_{i+1})$. Potom $\varphi\colon x_i \mapsto f(x_i)f(G_{i+1})$ je epimorfismus $G_i \to f(G_i)/f(G_{i+1})$, neboť φ je složení epimorfismů f a p. Zřejmě $G_{i+1} \leq \ker(\varphi)$, proto φ indukuje epimorfismus $\varphi^*\colon G_i/G_{i+1} \to f(G_i)/f(G_{i+1})$. Protože G_i/G_{i+1} je abelovská, i $f(G_i)/f(G_{i+1})$ je abelovská. □

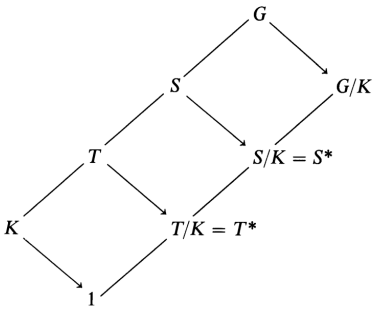
Následující tvrzení budeme potřebovat k důkazu další věty o řešitelných grupách.

Věta 10.16 (Korespondenční věta)**.** *Nechť $K \lhd G$ jsou grupy, $K \leq T \leq S \leq G$ jsou podgrupy a $\nu\colon G \to G/K$ je přirozená projekce $x \mapsto xK$. Potom*

(i) $S \mapsto \nu(S) = S/K = S^*$ je bijekce z množiny podgrup obsahujících grupu K do množiny všech podgrup grupy G/K;

(ii) $T \leq S$ právě tehdy, když $T^* \leq S^*$, a platí $[S : T] = [S^* : T^*]$;

(iii) $T \lhd S$ právě tehdy, když $T^* \lhd S^*$, a platí $S/T \cong S^*/T^*$.



Důkaz. (i) (ν je injektivní). Nechť $\nu(S) = S/K = T/K = \nu(T)$.

Potom pro sK existuje tK takové, že $sK = tK$, $s \in S$, $t \in T$. Tedy $t^{-1}s \in K$, $t = sk$, $k \in K$. Proto $s = tk \in TK = T$. Odtud $S \subseteq T$. Opačnou inkluzi získáme podobným postupem.

(ν je surjektivní) Nechť $A \leq G/K$ je podgrupa. Nechť $x, y^{-1} \in \nu^{-1}(A)$. Potom $xKy^{-1}K = xy^{-1}K \in A$, proto $xy^{-1} \in \nu^{-1}(A)$. Odtud vyplývá, že $\nu^{-1}(A)$ je podgrupa. Proto ν je surjektivní.

Obecně $\nu(\nu^{-1}(A)) \subseteq A$. Vzhledem k tomu, že ν je injektivní i surjektivní, je $\nu(\nu^{-1}(A)) = A$.

(ii) Triviálně $K \leq T \leq S$ implikuje $T/K \leq S/K$. Dále se dá dokázat, že $\alpha\colon sT \mapsto \nu(s)T^*$ je bijekce $S/T \to S^*/T^*$. Jestliže G je konečná, alternativně platí

$$[S^* : T^*] = |S^*|/|T^*| = |S/K|/|T/K| = (|S|/|K|)/(|T|/|K|) = |S|/|T| = [S : T].$$

(iii) Jestliže $T \lhd S$, třetí věta o izomorfismu implikuje $T^* = T/K \lhd S/K = S^*$ a navíc $S^*/T^* = (S/K)/(T/K) \cong S/T$. Zbývá dokázat, že $T^* \lhd S^*$ implikuje $T \lhd S$. Nechť $\mu\colon S^* \to S^*/T*$ je přirozená projekce a $\nu_S = \nu|_S$ je restrikce ν na S. Potom $\Phi = \mu\nu_S\colon S \to S^*/T^*$ je epimorfismus grup. Máme $\Phi(T) = T^*/T^* = 1 \in S^*/T^*$, proto $T \leq \ker(\Phi)$. Z druhé strany $s \in \ker(\Phi)$ implikuje $\Phi(s) = s^*T^* = T^*$. Proto $s^* \in T^*$, a odtud $s \in T$.

□

Poznámka: V jazyce teorie uspořádaných množin věta 10.16 hovoří, že svaz podgrup faktorové grupy G/K je izomorfní intervalu ve svazu podgrup grupy G ohraničenému grupami $K \lhd G$. Podobně pro svaz normálních podgrup G/K. Speciálně, korespondenční věta zaručuje, že k normálnímu řetězci grupy

$$G/K = G^* \geq K_1^* \geq K_2^* \geq \cdots \geq K_n^* = 1$$

existuje částečný normální řetězec

$$G \geq K_1 \geq K_2 \geq \cdots \geq K_n \geq K$$

s izomorfními odpovídajícími podílovými grupami.

Věta 10.17. *Nechť $H \lhd G$ a nechť H i G/H jsou řešitelné grupy. Potom G je řešitelná.*

Důkaz. Nechť $G/H \geq K_1^* \geq K_2^* \geq \cdots \geq K_n^* = 1$ je řešitelný řetězec. Použitím korespondenční věty zkonstruujeme podgrupy $G \geq K_1 \geq K_2 \geq \cdots \geq K_n \geq H$ tvořící částečný normální řetězec splňující $K_i/K_{i+1} \cong K_i^*/K_{i+1}^*$. Vzhledem k tomu, že K_i^*/K_{i+1}^* je abelovská, i K_i/K_{i+1} je abelovská. Pokud tento řetězec rozšíříme o řešitelný řetězec grupy H, dostaneme řešitelný řetězec grupy G. □

Důsledek 10.18. *Přímý součin dvou řešitelných grup je řešitelná grupa.*

Důkaz. Nechť $G \cong H \times K$, kde H i K jsou řešitelné. Potom existují podgrupy $H_1 \cong H$ a $K_1 \cong K$, $H_1 \lhd G$ a $K_1 \lhd G$, $H_1 \cap K_1 = 1$ a $G = H_1K_1$. Z první věty o izomorfismu dostaneme $K_1 \cong G/H_1$. Nyní už tvrzení získáme použitím věty 10.19. □

Věta 10.19. *Konečná p-grupa je řešitelná.*

Důkaz. Nechť G je konečná p-grupa. Budeme postupovat indukcí podle $|G|$. Triviální grupa je řešitelná. Nechť tvrzení platí pro p-grupy řádu $< |G|$. Z věty 8.4 dostaneme, že pro $G > 1$ je centrum $H = Z(G) > 1$. Protože $K = G/Z(G)$, je p podle indukčního předpokladu řešitelná. Použitím věty 10.19 dostaneme, že G je řešitelná. □

Kapitola 11

Řešitelnost polynomických rovnic v radikálech

11.1 Rozkladová pole

Pro začátek připomeňme některé definice a tvrzení z okruhů polynomů.

Definice 11.1. Polynom $f(x)$ nad oborem integrity D je ireducibilní (nerozložitelný), jestliže $f(x) = g(x)h(x)$ implikuje, že $g(x)$ nebo $h(x)$ je jednotka v D.

Příklad 11.2. Polynom $f(x) = 2x^2 + 4 = 2(x^2 + 2)$ je ireducibilní nad Q, ale je rozložitelný nad Z.

Věta 11.3. *Nechť F je pole, $f(x) \in F[x]$ a $p(x)$ je ireducibilní nad F. Potom $F(x)/\langle p(x)\rangle$ je pole.*

Poznámka: $\langle p(x)\rangle$ označuje ideál generovaný $p(x)$.

Příklad 11.4. $Z_3[x]/\langle x^2 + 1\rangle$ je pole řádu 9. Jeho prvky jsou $\{0, 1, 2, x, x + 1, x + 2, 2x, 2x + 1, 2x + 2\}$. Operace sčítání je sčítání polynomů, kde koeficienty redukujeme modulo 3. Při operaci násobení redukujeme součin modulo $x^2 + 1$. Například

$$(2x + 1)(2x + 2) = 4x^2 + 6x + 2 = x^2 + 2 = (x^2 + 1) + 1 = 1.$$

Definice 11.5. Pole E nazýváme rozšířením pole F, pokud $E \supset F$ a operace F jsou zúžením operací na E.

Příklad: $\mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$.

Věta 11.6 (Kronecker, 1887)**.** *Nechť F je pole a $f(x) \in F[x]$ je polynom stupně aspoň 1. Potom existuje rozšíření $E \supset F$, ve kterém $f(x)$ má kořen.*

Důkaz. (Náčrt.) $F[x]$ je obor integrity s jednoznačným rozkladem. Proto existuje ireducibilní polynom $p(x) \in F[x]$ takový, že $p(x)|f(x)$. Stačí najít rozšíření E, ve kterém má $p(x)$ kořen. Kandidátem je pole $E = F[x]/\langle p(x)\rangle$. Nechť $\Phi\colon F \to E$ je definované předpisem $\Phi(a) = a + \langle p(x)\rangle$. Potom $\Phi(F) \subset E$ je podpole izomorfní F. Tvrdíme, že $\alpha = x + \langle p(x)\rangle$ je kořen. Nechť

$$p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0.$$

Po dosazení dostaneme $p(\alpha) = p(x) + \langle p(x)\rangle = \langle p(x)\rangle = 0$.

□

Příklad 11.7. Nechť $f(x) = x^2 + 1 \in \mathbb{Q}[x]$. Podle důkazu věty 11.6 je $\alpha = x + \langle x^2 + 1\rangle$ kořen $f(x)$ v rozšíření $E = Q[x]/\langle x^2 + 1\rangle$. Přímý výpočet dá:

$$f(\alpha) = f(x+\langle x^2+1\rangle) = (x+\langle x^2+1\rangle)^2+1 = x^2+1+\langle x^2+1\rangle = \langle x^2+1\rangle = 0 \in E.$$

Poznámka: Víme, že v komplexních číslech má $f(x)$ kořen $\mathbf{i} = \sqrt{-1}$, ale chceme najít rozšíření a kořen v něm bez použití komplexních čísel.

Definice 11.8. Nechť $a_1, a_2, \ldots, a_n \in E \supset F$. Označme $F(a_1, a_2, \ldots, a_n)$ nejmenší podpole E obsahující F i prvky $a_1, a_2, \ldots, a_n$. Pak $F(a_1, a_2, \ldots, a_n)$ je průnikem všech podpolí E obsahujících F a současně $\{a_1, a_2, \ldots, a_n\}$.

Definice 11.9. Nechť $E \supseteq F$ je rozšíření pole F, $f(x) \in F[x]$ a $n = deg(f(x)) \geq 1$. Polynom $f(x)$ je rozložitelný v poli E, jestliže existuje $a \in F$ a $a_1, a_2, \ldots, a_n \in E$ takové, že

$$f(x) = a(x - a_1)(x - a_2)\ldots(x - a_n).$$

Pole E se nazývá rozkladové pole pro $f(x)$, pokud $E = F(a_1, a_2, \ldots, a_n)$.

Příklad 11.10. Polynom $f(x) = x^2 + 1 \in \mathbb{Q}[x]$ se rozkládá v $\mathbb{C}$, $f(x) = (x + \mathbf{i})(x - \mathbf{i})$. Ale rozkladové pole pro $f(x) \in \mathbb{Q}[x]$ je pole

$$\mathbb{Q}(\mathbf{i}) = \{r + s\mathbf{i}; r, s \in \mathbb{Q}\}.$$

Pokud uvažujeme $f(x) \in \mathbb{R}[x]$, rozkladové pole je $\mathbb{C}$. Tedy rozkladové pole závisí nejen na polynomu, ale i na poli, ve kterém uvažujeme jeho koeficienty. Podobně rozkladové pole pro $g(x) = x^2 - 2 \in \mathbb{R}$ je $\mathbb{R}$. Ale rozkladové pole pro $g(x) \in \mathbb{R}$ je

$$\mathbb{Q}(\sqrt{2}) = \{r + s\sqrt{2}; r, s \in \mathbb{Q}\}.$$

Věta 11.11. *Pro každý polynom $f(x) \in F[x]$ stupně aspoň 1 existuje rozkladové pole.*

Důkaz. Stačí dokázat, že existuje rozšíření $E \supseteq F$, ve kterém se $f(x)$ rozkládá. Budeme postupovat indukcí podle $def(f(x)) \geq 1$. Jestliže $\deg(f(x)) = 1$, platí $f(x) = a(x - a_1)$ a rozkladové pole je F. Pokud $n = \deg(f(x)) > 1$, z věty 11.6 vyplývá, že existuje pole $E \supseteq F$ a $a_1 \in E$ takové, že $f(x) = a(x - a_1)g(x)$, $g(x) \in E[x]$ a vedoucí koeficient $g(x)$ je 1. Zřejmě $\deg(g(x)) = n-1 < \deg(f(x)$. Z indukčního předpokladu vyplývá, že existuje $K \supseteq E$ takové, že K obsahuje kořeny $a_2, \ldots, a_n$ polynomu $g(x)$. Proto všechny kořeny $\{a_1, a_2, \ldots, a_n\} \subset K$. Potom $F(a_1, \ldots, a_n) \subseteq K$. □

Čtenář znající fundamentální věty algebry se možná zeptá, proč jsme jednoduše nepoložili v předešlém důkaze $K = \mathbb{C}$. Důvody jsou dva: existují pole, která nejsou obsažena v $\mathbb{C}$, například konečná pole. Druhý důvod je, že pokud to není nevyhnutné, chceme mít naši teorii nezávislou od fundamentální věty algebry. Ostatně, fundamentální věta algebry byla dokázána o mnoho let později v rámci komplexní analýzy. Její čistě algebraický důkaz nebyl dlouho znám.

Příklad 11.12. Uvažujme polynom $f(x) = x^4 - x^2 - 2 = (x^2 - 2)(x^2 + 1)$, který má nad $\mathbb{C}$ kořeny $\pm\sqrt{2}$ a $\pm\mathbf{i}$. Jeho rozkladové pole nad $\mathbb{Q}$ je $\mathbb{Q}(\sqrt{2}, \mathbf{i})$. Platí

$$\mathbb{Q}(\sqrt{2}, \mathbf{i}) = \{\alpha + \beta\mathbf{i};\ \alpha, \beta \in \mathbb{Q}(\sqrt{2})\} = \{(a + b\sqrt{2}) + (c + d\sqrt{2})\mathbf{i};\ a, b, c, d \in \mathbb{Q}\}.$$

Příklad 11.13. Nechť $f(x) = x^2 + x + 2 \in Z_3[x]$. Dosazením $0, 1, 2 \in Z_3$ zjistíme, že $f(x)$ je ireducibilní. Na druhé straně $f(x) = (x-(1+\mathbf{i}))(x-(1-\mathbf{i}))$, proto $f(x)$ se rozkládá v poli $Z_3(\mathbf{i})$.

Pokud použijeme konstrukci z Kroneckerovy věty, získáme rozkladové pole $E = Z_3[x]/\langle x^2+x+2\rangle$. Je to 9-prvkové pole charakteristiky 3. Pokud označíme $1 + \langle x^2 + x + 1\rangle := 1$ a $x + \langle x^2 + x + 1\rangle := \beta$, pole

$$E = \{0, 1, 2, \beta, 2\beta, \beta + 1, 2\beta + 1, \beta + 2, 2\beta + 2\}.$$

Sčítání v E je modulo 3. Při násobení používáme redukci modulo $\beta^2 + \beta + 2$. Speciálně po vynásobení dvou prvků použijeme substituci $\beta^2 = -\beta-2 = 2\beta+1$. Dělením $x - \beta$ dostaneme rozklad $x^2 + x + 2 = (x - \beta)(x + \beta + 1)$. Máme tedy 2 rozkladové pole polynomu $f(x) \in Z_3[x]$ a vzniká problém jednoznačnosti.

Věta 11.14 (jednoznačnost elementárního rozšíření)**.** *Nechť $p(x) \in F[x]$ je ireducibilní polynom. Nechť $a \in E \supseteq F$ je kořen $p(x)$ v rozšíření E. Potom $F(a) \cong F[x]/\langle p(x)\rangle$.*

Jestliže navíc $\deg(p(x)) = n$*, platí*

$$F(a) = \{c_{n-1}a^{n-1} + c_{n-2}a^{n-2} + \cdots + c_1a + c_0;\ c_0, c_1, \ldots, c_{n-1} \in F\}.$$

Důkaz. Zobrazení $\Phi\colon F[x] \to F(a)$ definované předpisem $\Phi(f(x)) = f(a)$ je homomorfismus okruhů s jádrem $\ker(\Phi) = \langle p(x)\rangle = \{r(x)p(x);\ r(x) \in F[x]\}$. Zřejmě $\Phi(p(x)) = p(a) = 0$, proto $\langle p(x)\rangle \subset \ker(\Phi)$. Ale $\langle p(x)\rangle$ je maximální ideál různý od $F[x]$, proto $\ker(\Phi) = \langle p(x)\rangle$. Z první věty o izomorfismu dostaneme $F[x]/\langle p(x)\rangle \cong F(a)$. Dále, každý prvek $F[x]/\langle p(x)\rangle$ má tvar $c_{n-1}x^{n-1} + c_{n-2}x^{n-2} + \cdots + c_1x + c_0 + \langle p(x)\rangle$. Tento prvek se izomorfismem indukovaným Φ zobrazí na

$$c_{n-1}a^{n-1} + c_{n-2}a^{n-2} + \cdots + c_1a + c_0.$$

□

Z věty 11.14 vyplývá, že rozšíření $F(a)$ tvoří nad F vektorový prostor dimenze $\deg(p(x))$.

Důsledek 11.15. *Nechť $p(x) \in F[x]$ je ireducibilní polynom. Nechť $a \in E \supseteq F$ je kořen $p(x)$ v rozšíření E. Potom $F(a) \subset E$ je n-dimenzionální vektorový prostor nad F.*

Věta 11.16. *Rozkladové pole $f(x) \in F[x]$ je jednoznačně určené polynomem $f(x)$ a polem F.*

Důkaz. Nechť $f(x) = p(x)g(x)$, kde $p(x)$ je ireducibilní polynom. Nechť $F(b)$ a $F(a)$ jsou rozšíření F obsahující kořeny a, b. Podle věty 11.14 platí $F(a) \cong F[x]/\langle p(x)\rangle \cong F(b)$. Opakovaným použitím vět 11.14 dokážeme jednoznačnost. □

Poznámka: Věta 11.16 nám potvrzuje, že rozkladové pole pro polynom $f(x) \in \mathbb{Q}[x]$ můžeme hledat tak, že najdeme kořeny $f(x)$ v $\mathbb{C}$ a potom najdeme minimální množinu kořenů, která vygeneruje rozkladové pole.

Příklad 11.17. Uvažujme $f(x) = x^n - a \in \mathbb{Q}[x]$. Označme $\omega = \cos(2\pi/n) + \sin(2\pi/n)\mathbf{i}$ primitivní řešení rovnice $\omega^n = 1$ v $\mathbb{C}$. Kořeny polynomu $f(x)$ v $\mathbb{C}$ jsou:

$$a^{1/n}, \omega a^{1/n}, \ldots, \omega^{n-1} a^{1/n}.$$

Tyto kořeny se nacházejí v poli $\mathbb{Q}(a^{1/n}, \mathbf{i})$, což je zároveň i rozkladovým polem.

Věta 11.18. *Polynom $f(x)$ nad polem F má násobný kořen v nějakém rozšíření $E \supseteq F$ tehdy a jen tehdy, když $f(x)$ a $f'(x)$ mají společného dělitele v $F[x]$ stupně ≥ 1.*

Důkaz. ($\Rightarrow$) Jestliže a je násobný kořen $f(x)$, platí $f(x) = (x-a)^2 g(x)$ a $f'(x) = 2(x-a)g(x) + (x-a)^2 g'(x)$. Tedy $(x-a)$ je společným dělitelem $f(x)$ a $f'(x)$.
($\Leftarrow$) Důkaz sporem. Nechť $f(x)$ a $f'(x)$ nemá společného netriviálního dělitele a současně a je násobný kořen. Z Euklidova algoritmu na výpočet $\gcd(f(x), f'(x))$ vyplývá, že existují polynomy $g(x)$ a $h(x)$ takové, že $1 = g(x)f(x) + h(x)f'(x)$. Uvažujme $g(x)f(x) + h(x)f'(x) \in E[x]$. Potom $(x-a)$ dělí $f(x)$ i $f'(x)$. Odtud, $(x-a)|1$, což je nesmysl.

□

11.2 Konečná pole

Definice 11.19. Pokud aditivní řád $1 \in F$ je konečný, charakteristika pole F, zapisujeme $\operatorname{char} F$, je rovna aditivnímu řádu 1. Pokud aditivní řád 1 je nekonečný, položíme $\operatorname{char} F = 0$.

Lemma 11.20. *Pokud $\infty > \operatorname{char} F > 0$, charakteristika $\operatorname{char} F = p$ je prvočíslo.*

Důkaz. Nechť $\operatorname{char} F = n$ a nechť $n = st$. Potom $0 = n \cdot 1 = (st)\cdot 1 = (s\cdot 1)(t\cdot 1)$. Protože F je obor integrity, je $s\cdot 1 = 0$ nebo $t\cdot 1 = 0$. Ale n je nejmenší přirozené číslo splňující $0 = n\cdot 1$, tedy $s = n$ nebo $t = n$. To znamená, že n nemá netriviální rozklad, tedy n je prvočíslo. □

Lemma 11.21. *V poli s* $\operatorname{char} F = p$ *má každý nenulový prvek aditivní řád* p.

Důkaz. Nechť $x \in F$. Máme

$$p \cdot x = \underbrace{x + x + \ldots + x}_{p \text{ sčítancov}} = \underbrace{1 \cdot x + 1 \cdot x + 1 \cdot x + \ldots + 1 \cdot x}_{p \text{ sčítancov}}$$
$$= \underbrace{(1 + 1 + \ldots + 1)}_{p \text{ sčítancov}} \cdot x = (p \cdot 1) \cdot x = 0 \cdot x = 0.$$

Tedy $|x|$ dělí p. Ale p je prvočíslo, proto $|x| = p$.

□

Věta 11.22. *Pokud* F *je konečné pole, existuje prvočíslo* p *a přirozené číslo* n *takové, že* $|F| = p^n$.

Důkaz. Vzhledem k tomu, že pole F je konečné, z lemmatu 11.21 vyplývá $\operatorname{char}(F) = p$ pro nějaké prvočíslo p. Uvažujme aditivní grupu pole $(F; +)$. Z lemmatu 11.21 vyplývá, že řád každého prvku je mocnina p, proto $(F; +)$ je p-grupa. Z důsledku 8.3 vyplývá, že $|(F; +)|$ je mocnina p. □

Poznámka: Jestliže F je charakteristiky p, z fundamentální věty o abelovských grupách (věta 9.1) vyplývá, že $(F; +) \cong Z_p^n$ je elementární abelovská p-grupa.

Věta 11.23. *Pro každé prvočíslo* p *a pro každé přirozené číslo existuje, až na izomorfismus, jediné konečné pole řádu* p^n.

Důkaz. Uvažujme rozkladové pole E pro $f(x) = x^{p^n} - x \in Z_p[x]$. Dokážeme, že $|E| = p^n$. V rozkladovém poli E má $f(x)$ p^n kořenů (se započtením násobností). Ale $f'(x) = p^n x^{p^n - 1} - 1$ a polynomy $f(x)$, $f'(x)$ jsou nesoudělné. Podle věty 11.18 jsou všechny kořeny $f(x)$ po dvou různé.

Nechť K je množina kořenů $f(x)$ v E. Podle předchozí úvahy je $|K| = p^n$. Dokážeme, že K je podpole E. Pokud a, b jsou kořeny, z binomické věty

$$(a - b)^{p^n} = \sum_{j=0}^{p^n} \binom{p^n}{j} a^j (-b)^{p^n - j}$$

můžeme dokázat, že p dělí $\binom{p^n}{j}$ pro $j \neq 0, j \neq p^n$. Protože pole je charakteristiky p, je $(a-b)^{p^n} = a - b$. Odtud $f(a-b) = (a-b)^{p^n} - (a-b) = 0$. A dále $f(a) = 0$ a $f(b) = 0$ implikuje $a^{p^n} = a$, $b^{p^n} = b$. Po dosazení $f(ab) = a^{p^n} b^{p^n} - ab = 0$ a také

$$f(1/a) = (1/a)^{p^n} - 1/a = 1/a^{p^n} - 1/a = 1/a - 1/a = 0.$$

Protože E je rozkladové pole, musí být $E = K$ a $|E| = |K| = p^n$.

Nechť E' je nějaké pole řádu p^n. Potom obsahuje pole izomorfní Z_p (generované 1). Nenulové prvky K tvoří multiplikativní grupu řádu $p^n - 1$, proto pro každé $x \in K$ platí $x^{p^n - 1} = 1$, tedy i $x^{p^n} = x$. Odtud $f(x) = 0$ pro každé $x \in K$. Z toho vyplývá, že E' je rozkladové pole pro $f(x) = x^{p^n} - x$. Z věty 11.16 vyplývá $E' \cong E$. □

Definice 11.24. Konečné pole řádu p^n budeme označovat $\mathrm{GF}(p^n)$.

Věta 11.25 (struktura konečného pole)**.** *Aditivní grupa* $(\mathrm{GF}(p^n), +) \cong Z_p^n$.
Multiplikativní grupa $(\mathrm{GF}(p^n) - \{0\}, \cdot) \cong Z_{p^n-1}$ *je cyklická řádu* $p^n - 1$.

Důkaz. První část tvrzení vyplývá z fundamentální věty o abelovských grupách, (věta 9.1) a faktu, že každý nenulový prvek $\mathrm{GF}(p^n)$ má aditivní řád p (lemma 11.21).

Grupa $GF^*(p^n) = (\mathrm{GF}(p^n) - \{0\}, \cdot)$ je abelovská. Z věty 9.1 vyplývá, že existuje rozklad $GF^*(p^n)$ na cyklické grupy. Grupa $\mathrm{GF}^*(p^n)$ je cyklická právě tehdy, když řády faktorů rozkladu jsou po dvou nesoudělné. Kvůli sporu předpokládejme, že $\mathrm{GF}^*(p^n)$ není cyklická. Potom v rozkladu existují dvě různé cyklické grupy se společným dělitelem $d > 1$. To znamená, že $\mathrm{GF}^*(p^n)$ obsahuje dvě různé cyklické podgrupy $H \neq K$ řádu d. Potom každý prvek H i K je kořen polynomu $x^d - 1 \in \mathrm{GF}(p^n)[x]$. Potom počet jeho kořenů je aspoň $|H| \cup |K| > d$, dostáváme spor. □

Cvičení

11.1. Určete svaz podpolí GF(64).

11.2. Nechť α je kořen $f(x) = x^3 + x^2 + 1 \in Z_2[x]$ v nějakém rozšíření GF(2). Vypočítejte $1/\alpha$.

11.3. Dokažte, že $GF^*(32)$, je generovaná každým netriviálním prvkem.

11.4. Dokažte, že $x \mapsto x^p$ je automorfismus $\mathrm{GF}(p^n)$ řádu n.

11.3 Řešitelnost Galoisovy grupy polynomu

Definice 11.26. Nechť $E \supset F$ je rozšíření pole F. Automorfismus E je automorfismus okruhu E. Galoisova grupa $\mathrm{Gal}(E/F)$ je podgrupa grupy automorfismů bodově fixující F.

Nechť $H \leq \mathrm{Gal}(E/F)$. Potom $E_H = \{x \in E; \Phi(x) = x \text{ pro každé } \Phi \in H\}$ se nazývá pole fixované H.

Jedna z klíčových myšlenek Galoisovy teorie spočívá v pozorovaní, že svaz podpolí $\langle F, E\rangle$ a svaz podgrup $\mathrm{Gal}(E/F)$ jsou antiizomorfní.

Příklad 11.27. (Q) Uvažujme $E = \mathbb{Q}(2^{1/4}, \mathbf{i})$. Dá se dokázat, že $\mathrm{Gal}(E/\mathbb{Q})$ je 8-prvková grupa izomorfní grupě kvaternionů. Její generátory jsou $\alpha\colon \mathbf{i} \mapsto \mathbf{i}, 2^{1/4} \mapsto -\mathbf{i}2^{1/4}$; $\beta\colon \mathbf{i} \mapsto -\mathbf{i}, 2^{1/4} \mapsto 2^{1/4}$. Svaz podpolí vypadá takto: obrázek.

Svaz podgrup $\mathrm{Gal}(E/\mathbb{Q} \cong \langle \alpha, \beta\rangle$ vypadá takto: obrázek.

Příklad 11.28. (Z_2) Nechť $E = \mathbb{Q}\sqrt{2}$. Nechť $\Phi \in \mathrm{Gal}(E/\mathbb{Q}$. Potom

$$2 = \Phi(2) = \Phi(\sqrt{2}\sqrt{2}) = \Phi(\sqrt{2})^2.$$

Proto $\Phi(\sqrt{2}) = \pm\sqrt{2}$. Proto $\mathrm{Gal}(E/\mathbb{Q} = \langle\beta\rangle \cong Z_2$, kde β je automorfismus $\sqrt{2} \mapsto -\sqrt{2}$.

Příklad 11.29. (1) Uvažujme rozšíření $E = \mathbb{Q}(\sqrt[3]{2}) \supset \mathbb{Q}$ podobně jako v předchozím příkladu:

$$2 = \Phi(2) = \Phi(\sqrt[3]{2}\sqrt[3]{2}\sqrt[3]{2}) = (\Phi(\sqrt[3]{2}))^3.$$

Tato rovnice má jediné řešení $\Phi(\sqrt[3]{2}) = \sqrt[3]{2}$. Z definice, Φ fixuje všechny prvky $\mathbb{Q}$, proto $\mathrm{Gal}(F/\mathbb{Q})$ je triviální.

Příklad 11.30. (Z_4) Uvažujme rozšíření $E = \mathbb{Q}(\sqrt[4]{2}, \mathbf{i}) \supset \mathbb{Q}$. Jestliže $\Phi \in \mathrm{Gal}(E/\mathbb{Q})$ a zároveň fixuje $\mathbb{Q}(\mathbf{i})$, rovnice

$$2 = \Phi(2) = \Phi(\sqrt[4]{2}\sqrt[4]{2}\sqrt[4]{2}\sqrt[4]{2}) = (\Phi(\sqrt[4]{2}))^4$$

dává čtyři možnosti pro $\Phi(\sqrt[4]{2})$, konkrétně $\sqrt[4]{2}, \mathbf{i}\sqrt[4]{2}, -\sqrt[4]{2}, -\mathbf{i}\sqrt[4]{2}$. Pokud položíme $\alpha(\mathbf{i}) = \mathbf{i}$ a $\alpha(\sqrt[4]{2}) = \mathbf{i}\sqrt[4]{2}$, $\alpha \in \mathrm{Gal}(E/\mathbb{Q}(\mathbf{i}))$ má řád 4 a $\mathrm{Gal}(E/\mathbb{Q}(\mathbf{i}))$. Podgrupa $\langle\alpha^2\rangle \leq \mathrm{Gal}(E/\mathbb{Q}(\mathbf{i}))$ fixuje pole $(\mathbf{i}, \sqrt{2})$. Svaz podpolí je lineární $\mathbb{Q}(\mathbf{i}) \leq_2 (\mathbf{i}, \sqrt{2}) \leq_2 \mathbb{Q}(\sqrt[4]{2}, \mathbf{i})$, podobně jako svaz podgrup $1 \leq \langle\alpha^2\rangle \leq \langle\alpha\rangle = \mathrm{Gal}(E/\mathbb{Q}(\mathbf{i}))$.

Příklad 11.31. ($Z_2 \times Z_2$) Uvažujme rozšíření $E = \mathbb{Q}(\sqrt{3}, \sqrt{5}) \supset \mathbb{Q}$. Protože

$$E = \{a + b\sqrt{3} + c\sqrt{5} + d\sqrt{3}\sqrt{5}; a, b, c, d \in \mathbb{Q}\},$$

každý automorfismus $\Phi \in \mathrm{Gal}(E/\mathbb{Q}$ je určený obrazy $\Phi(\sqrt{3}) = \pm\sqrt{3}$ a $\Phi(\sqrt{5}) = \pm\sqrt{5}$. Potom $\mathrm{Gal}(E/\mathbb{Q}) \cong Z_2 \times Z_2$. Svazy podpolí a podgrup mají tvar diamantu.

Příklad 11.32. (S_3) Nechť $\omega = -1/2 + \mathbf{i}\sqrt{3}/2$. Přímým dosazením ověříme, že ω vyhovuje rovnicím $\omega^3 = 1$ a $\omega^2 + \omega + 1 = 0$. Uvažujme rozšíření $E = \mathbb{Q}(\omega, \sqrt[3]{2}) \supset \mathbb{Q}$. Podobně jako v předešlých úlohách automorfismus rozšíření je daný obrazem prvků ω a $\sqrt[3]{2}$. Najdeme dva automorfismy $\alpha \in \mathrm{Gal}(E/\mathbb{Q}(\sqrt[3]{2})$ a $\alpha \in \mathrm{Gal}(E/\mathbb{Q}(\omega)$. Podgrupa generovaná $\langle\alpha, \beta\rangle \cong S_3$. Ve skutečnosti je to už celá $\mathrm{Gal}(E/\mathbb{Q}$, neboť tyto podpole vygenerují E.

Tabulka 11.1: Automorfismy $\mathrm{Gal}(E/\mathbb{Q})$

id	α	β	β^2	$\alpha\beta$	$\alpha\beta^2$
$\omega \mapsto \omega$ $\sqrt[3]{2} \mapsto \sqrt[3]{2}$	$\omega \mapsto \omega^2$ $\sqrt[3]{2} \mapsto \sqrt[3]{2}$	$\omega \mapsto \omega$ $\sqrt[3]{2} \mapsto \omega\sqrt[3]{2}$	$\omega \mapsto \omega$ $\sqrt[3]{2} \mapsto \omega^2\sqrt[3]{2}$	$\omega \mapsto \omega^2$ $\sqrt[3]{2} \mapsto \omega^2\sqrt[3]{2}$	$\omega \mapsto \omega^2$ $\sqrt[3]{2} \mapsto \omega\sqrt[3]{2}$

Svazy podpolí a podgrup vypadají následovně:

obrázek

Věta 11.33 (Fundamentální věta Galoisovy teorie)**.** *Nechť E je pole charakteristiky 0 nebo konečné pole. Jestliže E je rozkladové pole nějakého polynomu $z\ F[x]$, zobrazení $\Theta\colon \langle F,E\rangle \to \mathrm{Sub}(\mathrm{Gal}(E/F))$ s předpisem $K \mapsto Gal(E/K)$ je antiizomorfismus svazů splňující následující vlastnosti:*

(1) $\dim[E:K] = |\operatorname{Gal}(E/K)|$ *a* $\dim[K:F] = [\operatorname{Gal}(E/F) : \operatorname{Gal}(E/K)]$.

(2) Jestliže K je rozkladové pole nějakého polynomu z $F[x]$, platí $\operatorname{Gal}(E/K) \lhd \operatorname{Gal}(E/F)$ *a* $\operatorname{Gal}(K/F) = \operatorname{Gal}(E/F)/\operatorname{Gal}(E/K)$.

(3) $K = E_{\mathrm{Gal}(E/K)}$, pole fixované $\operatorname{Gal}(E/K)$ *je K.*

(4) Jestliže $H \leq \operatorname{Gal}(E/F)$, platí $H = \operatorname{Gal}(E/E_H)$. Grupa automorfismů fixující E_H je H.

Příklad 11.34. Nechť $\omega = \cos(2\pi/7) + \mathbf{i}\sin(2\pi/7)$. Uvažujme pole $E = \mathbb{Q}(\omega)$. Určete svaz polí $\langle \mathbb{Q}, E\rangle$.

Zřejmě $\omega^7 = 1$, proto $\mathbb{Q}(\omega)$ je rozkladové pole polynomu $x^7 - 1 \in \mathbb{Q}[x]$. Můžeme aplikovat větu 11.33. Automorfismus $\alpha\colon \omega \mapsto \omega^3$ má řád 6, proto $|\dim(E:\mathbb{Q}| = |\operatorname{Gal}(E/\mathbb{Q}| \geq 6$. Platí $x^7-1 = (x-1)(x^6+x^5+x^4+x^3+x^2+x+1)$ a ω je kořen. Proto $\dim(E:\mathbb{Q}) \leq 6$. Proto $\operatorname{Gal}(E/\mathbb{Q}) = \langle\alpha\rangle$ je cyklická grupa řádu 6. Nyní již snadno identifikujeme svaz $\langle \mathbb{Q}, E\rangle$. Pole E obsahuje přesně dvě vlastní rozšíření, které jsou fixovanými poli podgrup $\langle\alpha^2\rangle$ a $\langle\alpha^3\rangle$. S trochou námahy je možné určit tyto pole explicitně. Podle věty 11.33 potřebujeme nelézt podpole fixované α^2 a α^3. Pole fixované α^3 je $\mathbb{Q}(\omega + \omega^{-1})$, pole fixované α^2 je $\mathbb{Q}(\omega^3 + \omega^5 + \omega^6)$.

11.4 Řešitelnost polynomických rovnic v radikálech

Kubický polynom $x^3 + bx + c = 0$ má tři kořeny: $A + B$, $-(A+B)/2 + (A - B)\sqrt{-3}/2$, a $-(A+B)/2 - (A-B)\sqrt{-3}/2$, kde

$$A = \sqrt[3]{\frac{-c}{2} + \sqrt{\frac{b^3}{27} + \frac{c^2}{4}}} \quad \text{a} \quad B = \sqrt[3]{\frac{-c}{2} - \sqrt{\frac{b^3}{27} + \frac{c^2}{4}}}.$$

Kořeny tedy můžeme vypočítat z koeficientů b a c pouhým použitím aritmetických operací a operací odmocňování. Takovému řešení rovnice $f(x) = 0$ říkáme řešení v radikálech.

Definice 11.35. Nechť F je pole a nechť $f(x) \in F[x]$. Říkáme, že $f(x)$ je řešitelný nad F v radikálech, jestliže se F rozkládá v nějakém rozšíření $F(a_1, \ldots, a_n)$ a existují přirozená čísla $k_1, \ldots, k_n$ taková, že $a_1^{k_1} \in F$, $a_i^{k_i} \in F(a_1, \ldots, a_{i-1})$ pro $i = 2, \ldots, n$.

Příklad 11.36. Polynom $f(x) = x^8 - 3 \in \mathbb{Q}[x]$ má kořeny $\sqrt[8]{3}$, $\sqrt[8]{3}\omega$, $\sqrt[8]{3}\omega^2, \ldots, \sqrt[8]{3}\omega^7$, kde $\omega = \cos(2\pi/8) + \mathbf{i}\sin(2\pi/8)$. Polynom $f(x)$ se tedy rozkládá v poli $\mathbb{Q}(\sqrt[8]{3}, \omega)$.

Protože $(\sqrt[8]{3})^8 = 3 \in \mathbb{Q}$ a $\omega^8 = 1 \in \mathbb{Q} \subset \mathbb{Q}(\omega)$,je $f(x)$ řešitelný v radikálech. Kořeny se dají přepsat do tvaru

$$\pm\sqrt[8]{3},\ \sqrt{-1}\sqrt[8]{3},\ \sqrt[8]{3}\left(\frac{\sqrt{2}}{2}+\frac{\sqrt{-2}}{2}\right),\ \sqrt[8]{3}\left(\frac{\sqrt{2}}{2}-\frac{\sqrt{-2}}{2}\right).$$

Věta 11.37. *Nechť F je pole charakteristiky 0 a nechť E je rozkladové pole pro $f(x) = x^n - a \in F[x]$. Potom* $\mathrm{Gal}(E/F)$ *je řešitelná grupa.*

Důkaz. Nechť b je kořen $f(x) = x^n - a$ a nechť ω je primitivní kořen rovnice $x^n = 1$. Pokud $b = 0$, je $a = 0$ a b je n-násobný kořen. V takovém případě $E = F$ a $\mathrm{Gal}(E/F) = 1$. Proto dále předpokládáme $b \neq 0$.

Případ 1: F obsahuje nějaký primitivní kořen ω rovnice $x^n = 1$. Potom všechny kořeny $f(x)$ mají tvar $b\omega^i$, kde $i = 0, 1, \ldots, n-1$. Proto $E = F(b)$. Dále pro automorfismus $\Phi \in \mathrm{Gal}(E/F)$ platí $0 = \Phi(0) = \Phi(f(b)) = f(\Phi(b))$, proto Φ zobrazuje kořen na kořen a Φ je jednoznačně určený $b \mapsto b\omega^i$. Označme $\Phi_i\colon b \mapsto b\omega^i$. Potom

$$\Phi_i\Phi_k(b) = \Phi_i(b\omega^k) = b\omega^{k+i} = \Phi_k(b\omega^i) = \Phi_k\Phi_i(b).$$

Proto pro každé $i, k \in Z_n$ platí $\Phi_i\Phi_k = \Phi_k\Phi_i$ a $\mathrm{Gal}(E/F)$ je abelovská.

Případ 2. F neobsahuje primitivní kořen rovnice $x^n = 1$. Zřejmě i $b\omega$ je kořen $f(x)$ a i $\omega = \omega b/b \in E$. Proto $F \subset F(\omega) \subset E$ a $F(\omega)$ je rozkladové pole polynomu $x^n - 1$, kde kořeny jsou ω^i, $i \in Z_n$. Jestliže v předchozí úvaze položíme $f(x) = x^n - 1$ a $b = 1$, dostaneme, že $\mathrm{Gal}(F(\omega)/F)$ je abelovská.

Dále, E je rozkladové pole $f(x) \in F(\omega)$ a $F(\omega)$ obsahuje primitivní kořen rovnice $x^n = 1$. Podle případu 1 je $\mathrm{Gal}(E/F(\omega))$ abelovská. Z věty 11.33(2) vyplývá, že $\mathrm{Gal}(E/F(\omega)) \lhd \mathrm{Gal}(E/F)$ a $\mathrm{Gal}(E/F)/\mathrm{Gal}(E/F(\omega)) \cong \mathrm{Gal}(F(\omega))/F)$. Potom řetězec $1 \lhd \mathrm{Gal}(E/F(\omega)) \lhd \mathrm{Gal}(E/F)$ je řešitelný.

□

Věta 11.38. *Nechť F je charakteristiky 0 a nechť $E = F(a_1, a_2, \ldots, a_t)$ je rozkladové pole pro $f(x) \in F[x]$, který je řešitelný v radikálech. Potom* $\mathrm{Gal}(E/F)$ *je řešitelná grupa.*

Důkaz. Budeme postupovat indukcí podle t.

Nechť $t = 1$. Z předpokladů vyplývá, že existuje n_1 takové, že $a_1^{n_1} = a \in F$. Tedy a_1 je kořen $x^{n_1} - a$. Nechť L je rozkladové pole pro $x^{n_1} - a$. Zřejmě $F \subseteq F(a_1) \subseteq L$. Z věty 11.33(2) vyplývá, že $\mathrm{Gal}(L/E) \lhd \mathrm{Gal}(L/F)$ a $\mathrm{Gal}(L/F)/\mathrm{Gal}(L/E) \cong \mathrm{Gal}(E/F)$. Podle věty 11.37 je $\mathrm{Gal}(L/F)$ řešitelná grupa. Podle věty 10.14 je i $\mathrm{Gal}(L/E)$ řešitelná, podle věty 10.15 je faktorová grupa $\mathrm{Gal}(E/F)$ řešitelná.

Nechť $t > 1$. Nechť L je rozkladové pole $x^{n_1} - a$ nad E a nechť $K \subseteq L$ je rozkladové pole $x^{n_1} - a$ nad F. Potom L je rozkladové pole $(x^{n_1} - a)f(x)$ nad F a L je rozkladové pole $f(x)$ polynomu $x^{n_1} - a$ nad E. Protože $F(a_1) \subseteq K$, rozkládá se $f(x)$ nad $K(a_2, \ldots, a_t)$. Z indukčního předpokladu je grupa $\mathrm{Gal}(L/K)$ řešitelná. Z věty 11.37 je $\mathrm{Gal}(K/F)$ řešitelná. Z věty 11.33(2) je

$\mathrm{Gal}(L/F)/\mathrm{Gal}(L/K) \cong \mathrm{Gal}(K/F)$ řešitelná. Z věty 10.19 je $\mathrm{Gal}(L/F)$ řešitelná. Potom z věty 10.14 je podgrupa $\mathrm{Gal}(L/E) \leq \mathrm{Gal}(L/F)$ řešitelná. Z věty 11.33(2) je $\mathrm{Gal}(L/E) \lhd \mathrm{Gal}(L/F)$ a faktorová grupa $\mathrm{Gal}(L/F)/\mathrm{Gal}(L/E) \cong \mathrm{Gal}(E/F)$. Podle věty 10.15 je $\mathrm{Gal}(E/F)$ řešitelná. □

Poznámka 11.39. Platí i obrácená implikace k větě 11.38: Nechť E je rozkladové pole pro polynom $f(x) \in F[x]$, $\mathrm{char}(F) = 0$. Jestliže $\mathrm{Gal}(E/F)$ je řešitelná, je $f(x) = 0$ řešitelná v radikálech.

Poznámka 11.40. Je známo, že každá konečná grupa je Galoisova grupa nad nějakým polem. Charakterizace konečných grup, které jsou Galoisovými grupami nad $\mathbb{Q}$, není známa. Není ani znám příklad konečné grupy, která by nebyla Galoisovou grupou nad $\mathbb{Q}$.

11.5 Neřešitelný polynom stupně 5

Uvažujme polynom $g(x) = 3x^5 - 15x + 5$. Prvočíslo 5 dělí všechny koeficienty s výjimkou prvního a $5^2 = 25$ nedělí c_0. Podle Eisensteinova kritéria je $g(x)$ ireducibilní nad $\mathbb{Q}$. V následující tabulce jsou hodnoty $g(x)$ ve vybraných celých číslech. Ze spojitosti $g(x)$ vyplývá, že $g(x)$ má v otevřených intervalech $(-2,-1)$, $(0,1)$ a $(1,2)$ tři různé reálné kořeny a_1, a_2 a a_3. Uvažujme derivaci $g'(x) = 15x^4 - 15 = 15(x^4 - 1)$.

Tabulka 11.2: Hodnoty $g(x)$

$g(-2)$	$g(-1)$	$g(0)$	$g(1)$	$g(2)$
-61	17	5	-7	56

Použitím Euklidova algoritmu zjistíme, že $g(x)$ a $g'(x)$ jsou nesoudělné. Odtud máme, že všechny kořeny $g(x)$ jsou násobnosti 1. Dokážeme, že $g(x)$ má přesně 3 reálné kořeny. Nechť $g(x)$ má aspoň 4 reálné kořeny. Z Rolleovy věty z kalkulu vyplývá, že mezi každými dvěma kořeny $g(x)$ se nachází kořen $g'(x)$. Odtud, $g'(x) = 15(x^4 - 1)$ má aspoň 3 reálné kořeny, ale derivace má kořeny $\pm 1, \pm\mathbf{i}$, dostáváme spor. Tedy zbylé dva kořeny a_4, a_5 jsou vzájemně sdružené komplexní čísla $a \pm b\mathbf{i}$, $b \neq 0$. Nechť $K = \mathbb{Q}(a_1, a_2, a_3, a_4, a_5)$ je rozkladové pole pro $g(x)$. Vzhledem k tomu, že $g(x)$ je ireducibilní polynom stupně 5, platí $\dim[\mathbb{Q}(a_1) : \mathbb{Q}] = 5$ (věta 11.14). Z věty 11.33(1) máme $5 = \dim[\mathbb{Q}(a_1) : \mathbb{Q}] = |\mathrm{Gal}(\mathbb{Q}(a_1)/\mathbb{Q})|$. Vzhledem k tomu, že $\mathrm{Gal}(\mathbb{Q}(a_1)/\mathbb{Q}) \leq \mathrm{Gal}(K/\mathbb{Q})$, z Lagrangeovy věty 5 dělí $|\mathrm{Gal}(K/\mathbb{Q})|$. Z definice $\mathrm{Gal}(K/\mathbb{Q})$ má akci na množině kořenů a $\mathrm{Gal}(K/\mathbb{Q}) \leq S_5$. Z Cauchyho věty $\mathrm{Gal}(K/\mathbb{Q})$ obsahuje prvek řádu 5. Navíc $\mathrm{Gal}(K/\mathbb{Q})$ obsahuje automorfismus $a_4 = a + b\mathbf{i} \mapsto a - b\mathbf{i} = a_5$ a fixuje ostatní kořeny. Podgrupa grupy S_5 generovaná transpozicí a cyklem délky 5 se rovná S_5. Proto $\mathrm{Gal}(K/\mathbb{Q}) \cong S_5$ není řešitelná. Podle věty 11.38 se kořeny $g(x)$ nedají nad $\mathbb{Q}$ vyjádřit v radikálech.

Cvičení

11.5. Určete grupu automorfismů konečného pole GF(4).

11.6. Nechť E je rozkladové pole polynomu $x^4+1 \in \mathbb{Q}[x]$. Určete $\mathrm{Gal}(E/\mathbb{Q}$. Najděte všechny podpole E. Najděte automorfismy v $\mathrm{Gal}(E/\mathbb{Q}$ fixující $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{-2})$, $\mathbb{Q}(\mathbf{i})$.

11.7. Nechť $f(x) \in F[x]$ je polynom stupně n a $a_1, a_2, \ldots, a_n$ jsou kořeny. Jestliže $K = \mathbb{Q}(a_1, a_2, \ldots, a_n)$, je $\mathrm{Gal}(K/F)$ izomorfní podgrupě S_n.

11.8. Určete Galoisovu grupu polynomu $f(x) = x^2 - 10x + 21$.