

Abstraktní algebra

Úvodní kurz

Roman Nedela a Roman Čada

Abstraktní algebra

Úvodní kurz

Roman Nedela a Roman Čada

Kniha byla napsána použitím typografického systému L^AT_EX.

Obsah

| | | |
|-----------|--|-----------|
| 1 | Permutace | 1 |
| 2 | Grupy | 9 |
| 3 | Podgrupy | 15 |
| 4 | Cyklické grupy | 21 |
| 5 | Homomorfismy a izomorfismy | 27 |
| 5.1 | Lagrangeova věta | 29 |
| 5.2 | Normální podgrupy | 33 |
| 5.3 | Věty o izomorfismu | 37 |
| 6 | Přímý součin grup | 41 |
| 7 | Akce grup | 45 |
| 7.1 | Konjugace | 45 |
| 7.2 | Konjugace v symetrické grupě | 46 |
| 7.3 | Jednoduchost A_n | 48 |
| 7.4 | Reprezentace grup | 50 |
| 7.5 | Akce grupy na množině | 52 |
| 7.6 | Počítání orbit | 54 |
| 7.7 | Grupy geometrických transformací | 56 |
| 8 | Sylovovy věty | 65 |
| 8.1 | p -grupy | 65 |
| 8.2 | Sylovovy věty | 69 |
| 8.3 | Grupy malého řádu | 71 |
| 9 | Konečné abelovské grupy | 75 |
| 10 | Normální řetězce podgrup | 79 |
| 10.1 | Jordan-Hölderova věta | 79 |
| 10.2 | Řešitelné grupy | 82 |

| | |
|--|------------|
| 11 Okruhy | 87 |
| 11.1 Okruhy | 87 |
| 11.2 Obory integrity | 89 |
| 11.3 Pole | 89 |
| 11.4 Charakteristika okruhu | 90 |
| 11.5 Ideály a faktorové okruhy | 91 |
| 11.6 Prvočíselné a maximální ideály | 92 |
| 11.7 Homomorfizmy okruhů | 93 |
| 11.8 Podílové pole | 95 |
| 12 Polynomy | 97 |
| 12.1 Základní vlastnosti | 97 |
| 12.2 Dělení polynomů se zbytkem | 98 |
| 12.3 Rozklady polynomů | 99 |
| 12.4 Dělitelnost v oboru integrity | 102 |
| 12.5 Gaussovy obory integrity | 103 |
| 12.6 Eukleidovy obory | 104 |
| 13 Pole | 107 |
| 13.1 Rozkladová pole | 107 |
| 13.2 Konečná pole | 110 |
| 14 Galoisova teorie | 113 |
| 14.1 Řešitelnost Galoisovy grupy polynomu | 113 |
| 14.2 Řešitelnost polynomických rovnic v radikálech | 117 |
| 14.3 Neřešitelný polynom stupně 5 | 119 |

Kapitola 1

Permutace

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

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:

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

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 $M = \{i_0, i_1, \dots, i_{r-1}\} \subseteq \{1, 2, \dots, n\}$ je r -prvková podmnožina, $r > 1$. Nechť $\alpha \in S_n$ je permutace taková, že $\alpha(i_j) = i_{j+1}$, $j = 0, 1, \dots, r-1$ a $\alpha(k) = k$ pro $k \in \{1, 2, \dots, n\} \setminus M$. Potom permutaci α nazveme *cyklus* délky r a budeme ji zapisovat $\alpha = (i_0, i_1, \dots, i_{r-1})$. Všimněme si, že zápis $\alpha = (i_1, i_2, \dots, i_{r-1}, i_0)$ 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 $\underbrace{\alpha \circ \alpha \circ \dots \circ \alpha}_m$.

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 $j \in \{1, 2, \dots, n\}$, 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 $(i, \phi(i), \phi^2(i), \dots, \phi^{m-1}(i))$, přičemž m je nejmenší číslo takové, že $\phi^m(i) = i$. \square

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

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

Uvažujme součin transpozic

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

Toto pozorování 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 $\alpha = \beta_1 \beta_2 \dots \beta_t$ je úplný rozklad permutace $\alpha \in S_n$. Označme $\text{sgn}(\alpha) = (-1)^{n-t}$.

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

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

Důkaz. Uvažujme rozklad $\beta = \gamma_1 \gamma_2 \dots \gamma_t$ 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!) \square

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

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

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

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

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

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 $\text{sgn}(\alpha) = 1$.

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 $\text{sgn}(\alpha)$ 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 dānu množinu S_n , kde $n \geq 3$. Kolik fixovaných prvků k může existovat v nějaké permutaci v S_n ? Jak vypadā inverzní permutace k permutaci α , v níž je fixováno právě $n - 2$ prvků?

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

1.7. Nechť jsou dāny 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 dāna 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 vypadā permutace α v S_n , pro níž $\alpha^2 = id$? A jak vypadā 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. Necht' $\alpha = (i_1 i_2 \cdots i_r)$ a $\beta = (j_1 j_2 \cdots j_s)$. Dokažte, že α a β jsou disjunktní permutace právě tehdy, když $\{i_1, i_2, \dots, i_r\} \cap \{j_1, j_2, \dots, j_s\} = \emptyset$.

1.17. Necht' 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. Necht' α, β jsou permutace v S_n . Pokud α i β mají stejnou paritu, je $\text{sgn}(\alpha\beta) = 1$, pokud α a β mají rozdílnou paritu, je $\text{sgn}(\alpha\beta) = -1$. 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. Necht' 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. Necht' 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. Necht' 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. Necht' 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. Necht' o permutaci β víme následující: $\beta \in S_7$ a $\beta^4 = (2, 1, 4, 3, 5, 6, 7)$. Určete permutaci β .

1.28. Necht' $\beta = (1, 2, 3)(1, 4, 5)$. 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 řady 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-cykklus. Pro jaké přirozené číslo $i = \{2, 3, \dots, 10\}$ je δ^i rovněž 10-cykklus?
- 1.36.** Najděte jednu cyklickou a jednu necyklickou podgrupu grupy A_8 , jež má řád 4.
- 1.37.** Nechtě 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 $\text{sgn}(\alpha) = (-1)^{n-t}$, 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. Provéřte, pro kolik z 15 variant platí $\alpha \cdot \beta = \beta \cdot \alpha$. Vratíme-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 $\text{sgn}(\alpha) = -1^{n-t}$, 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 proved'te 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 Nechtě α, β, γ a δ jsou permutace v S_3 . Dále nechtě $\beta = id$ a $\gamma = \delta \neq id$ (tzn., že existuje právě jeden fixní prvek). Naleznete α a γ a přesvědčete se, že daná věta neplatí.

1.12 Položme $\beta = \alpha^{-1}$.

1.13 Připomeňme, že dvě funkce $f, g : A \rightarrow B$ 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 $\binom{6}{4} = \binom{6}{2} = \frac{6 \cdot 5}{2 \cdot 1} = 15$ 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 zbývajících prvky. Poslední prohození je již dáno dvěma zbývajících 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, $\frac{n(n-1)(n-2)(n-3)}{2^2 \cdot 2}$ součinů dvou disjunktních 2-cyklů a obecně $\frac{n(n-1)\dots(n-2k+1)}{2^k \cdot k!}$ součinů k disjunktních 2-cyklů, kde $2k \leq n$.

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

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

Kapitola 2

Grupy

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

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 $G \times G \rightarrow G$ 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 $GL(2, \mathbb{R})$, $GL(2, \mathbb{Q})$, $GL(2, \mathbb{C})$.

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

(i) Multiplikatívni grupy $U(n)$.

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

(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 $x_1x_2 \dots x_m$ je v grupě G dobře definován pro každé přirozené m . Nechť G je grupa a x je prvek. Pro přirozené číslo m definujeme $x^m = xx \dots x$, m -krát. Mocninu můžeme rozšířit na celá čísla následovně: $x^0 = 1$ a $x^m = (x^{-m})^{-1} = x^{-1}x^{-1} \dots x^{-1}$ 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 dihedralní grupy D_4 splňující rovnici $x^2 = 1$.
- 2.4.** Zkonstruuje 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 $f : Z_{11} \rightarrow Z_{11}$ 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 necht' $a_1, \dots, a_n \in G$. 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 necht' m, n jsou nesoudělná čísla. Jestliže $a^m = 1$, ukažte, že existuje $b \in G$, pro něž je $a = b^n$.
- 2.13.** Zkonstruuje Cayleyho tabulku pro grupu D_4 (což je dihedralní 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.** Necht' r_1, r_2, r_3 reprezentují tři rotace v D_n a necht' 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.** Necht' 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.** Číslo 5 a 15 patří do seznamu dvanácti přirozených čísel, která tvoří grupu při násobení modulo 56. Nalezněte všech dvanáct čísel patřících 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 $ab = ba$.

Náповěda k vybraným cvičením

2.1

- $\mathbb{Z}_{20} = \{0, 1, \dots, 19\}$. Najděte mocninu m čísla 13 takovou, že $a^m = 1$. Prvek a^{m-1} je pak inverzním prvkem k prvku a .
- $U(14) = \{1, 3, 5, 9, 11, 13\}$. 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 $0, \dots, 11$ 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 $0, \dots, 11$ je právě jednou vzorem a právě jednou obrazem, je $f = \alpha$ permutací.

Permutace α vypadá následovně:

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

Zapišeme 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). Necht' $g \in G$ 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 $(\mathbb{Z}, +)$ 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). Necht' 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). Necht' 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 .

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

Věta 3.8. Necht' G je grupa a necht' $a \in G$. Potom $\langle a \rangle$ je podgrupa.

Příklad 3.9. Necht' D_n je dihedralní 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. Necht' G je grupa a necht' $G_i, i \in I$, je systém podgrup grupy G . Potom $\bigcap_{i \in I} G_i$ je podgrupa G .

Definice 3.11. Necht' 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). Necht' $\{1, i\} \subset \mathbb{C}$. Potom $\langle 1, i \rangle = \{a + bi; a, b \in \mathbb{Z}\}$ je podgrupa $(\mathbb{C}, +)$. Pokud použijeme standardní reprezentaci komplexních čísel v Euklidovské rovině, tak Gaussova čísla odpovídají bodům s celočíselnými souřadnicemi.

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

Věta 3.14. Necht' G je grupa. Centrum grupy je abelovská podgrupa grupy G .

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

Definice 3.15. Necht' $a \in G$. 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 dihedralní 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. Necht' 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. Necht' k je pole. Ukažte, že $SL(n, k)$, množina všech $n \times n$ matic přes k majících determinant 1, je podgrupa grupy $GL(n, k)$.

- 3.8.** Necht' $n > 2$. 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.** Necht' 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.** Necht' H, K jsou podgrupy grupy G . Ukažte, že $H \cap K$ je rovněž podgrupa grupy G .
- 3.21.** Necht' 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.** Necht' G je grupa a $a \in G$. Ukažte, že $C(a) = C(a^{-1})$.
- 3.24.** Necht' a, b jsou dva různé prvky grupy G . Dokažte, že buď $a^2 \neq b^2$ nebo $a^3 \neq b^3$.
- 3.25.** Necht' je dána grupa G a její podgrupa H . Dokažte, že $C(H)$ je podgrupa 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.** Spočítejte 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. Spočítejte $|U(4)|, |U(10)|$ a $|U(40)|$. Odporuje tento příklad Vaší hypotéze z předchozího cvičení? Pokud ano, revidujte tuto hypotézu.

3.30. Nechť $H = \{a + bi \mid a, b \in \mathbb{R}, ab \geq 0\}$. 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 vyladíte 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 $\alpha_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix}$. Máme tedy dvě triviální možnosti:

$x_1 = 1$ a $x_2 = \alpha_1$. Dále je zřejmé, že α komutuje s $x_3 = (3, 4)$ a tedy i s $x_2 x_3$.

Proto $\{(1), (1, 2), (3, 4), (1, 2)(3, 4)\} \subseteq C((1, 2))$.

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 $b^j a = a b^j$. 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 $a^i b = b a^i = a^{n-1} b$. 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 $|a^k| = n / \gcd(n, k)$.*

Důkaz: Označme $d = \gcd(n, k)$. Chceme dokázat, že $\langle a^d \rangle = \langle a^k \rangle$. Protože $d \mid k$, je $\langle a^d \rangle \geq \langle a^k \rangle$. Existují celé čísla s a t takové, že $d = \gcd(n, k) = ns + kt$ (Euklidův algoritmus). Užitím substituce dostaneme $a^d = a^{ns+kt} = (a^k)^t \in \langle a^k \rangle$. Tedy i $\langle a^d \rangle \leq \langle a^k \rangle$. Dokázali jsme $\langle a^k \rangle = \langle a^{\gcd(n,k)} \rangle$.

Pro řády prvků platí: $(a^d)^{n/d} = 1$, proto $|a^d| \mid \frac{n}{d}$. Z druhé strany, minimální i takové, že $a^{di} = 1$, nemůže být menší než $\frac{n}{d}$, jinak bychom se dostali do sporu s $|a| = n$. Proto $|a^d| = \frac{n}{d}$. Z rovnosti $\langle a^d \rangle = \langle a^k \rangle$, vyplývá $|a^k| = |a^d| = \frac{n}{d}$.

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 $m > t$, existují celá čísla $q \geq 1$ a r , $0 \leq r < t$, takové, že $m = qt + r$. 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 $a^m = a^{qt} \in \langle a^t \rangle$. Tím jsme ověřili platnost $H \leq \langle a^t \rangle$, tedy $H = \langle a^t \rangle$.

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. \square

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 role 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

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

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

Důkaz. Dokážeme jen poslední rovnost. Nechť C_n je cyklická grupa řádu n . Z věty 4.8 víme, že pro každý dělitel $d | n$ 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

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

\square

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 $H = \{g \in G \mid |g| \text{ dělí } 12\}$. Dokažte, že H je grupa. Číslo 12 můžete nahradit i jiným číslem. Pokuste se zformulovat obecné tvrzení.
- 4.7. Najděte maximální řetězec podgrup $H_1 < H_2 < \dots < H_m$ v cyklické grupě \mathbb{Z}_{240} . Pokuste se zformulovat všeobecné tvrzení pro cyklickou grupu řádu n .
- 4.8. Vypište podgroupy $(\mathbb{Z}, +)$.
- 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 podgroupy grupy \mathbb{Z}_{30} a určete jejich řád.
- 4.12. Najděte příklad nocyklické grupy, jejíž všechny vlastní podgroupy jsou cyklické.
- 4.13. Nechť a je prvek grupy G a nechť $|a| = 15$. Spočítejte 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 podgroupy, z nichž jedna je řádu 7. Kolik je $|G|$? Co můžeme říci, nahradíme-li číslo 7 libovolným prvočíslem?
- 4.17. Doplněte následující tvrzení, aby bylo pravdivé: $|a| = |a^2|$ právě tehdy, když $|a| \dots$
- 4.18. Nechť cyklická grupa obsahuje prvek nekonečného řádu. Kolik tato grupa obsahuje prvků konečného řádu?
- 4.19. Vypište cyklické podgroupy 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.** Necht' d je přirozené číslo různé od dvou a necht' 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.** Necht' p je prvočíslo. Pokud grupa G obsahuje více než $p - 1$ prvků řádu p , nemůže být grupa G cyklická. Dokažte.
- 4.26.** Necht' 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.** Necht' 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.** Necht' $|a^5| = 12$. Jaké možnosti připadají v úvahu pro $|a|$? A jak to bude pro $|a^4| = 12$?
- 4.31.** Necht' a je prvek grupy G takový, že $|a^{28}| = 10$ a $|a^{22}| = 20$. Určete $|a|$.
- 4.32.** Dokažte, že grupa $H = \left\{ \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \mid n \in \mathbb{Z} \right\}$ je cyklická podgrupa grupy $GL(2, \mathbb{R})$.
- 4.33.** Necht' a, b jsou prvky grupy G a necht' $|a| = 12$, $|b| = 22$ 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 $2m$ a $-m$ být rovněž v K . Jeden z nich (v závislosti na tom, zda je m kladné či záporné), je však určitě větší než m 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

- $\langle 1 \rangle = \{0, 1, 2, \dots, 29\}$ – řádu 30,
- $\langle 2 \rangle = \{0, 2, 4, \dots, 28\}$ – řádu 15,
- $\langle 3 \rangle = \{0, 3, 6, \dots, 27\}$ – 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. Necht' (G, \cdot) a $(H, *)$ jsou grupy. Zobrazení $\varphi : G \rightarrow H$ je homomorfismem, pokud pro každé dva prvky $a, b \in G$ platí $\varphi(a \cdot b) = \varphi(a) * \varphi(b)$. Izomorfismus $G \rightarrow H$ je homomorfismus, který je bijekcí. Surjektivní homomorfismus se nazývá epimorfismus. Injektivní homomorfismus se nazývá monomorfismus (nebo vnoření).

Věta 5.2. Necht' (G, \cdot) a $(H, *)$ jsou grupy. Necht' $\varphi : G \rightarrow H$ 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 $\text{sgn} : S_n \rightarrow U(3) \cong (\{1, -1\}, \cdot)$ je homomorfismem.

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

Definice 5.4. Necht' $\varphi : G \rightarrow H$ je homomorfismus grup. Označme $\ker(\varphi) = \{g \in G \mid \varphi(g) = 1_H\}$ jádro homomorfismu φ a $\text{Im}(\varphi) = \{h \in H \mid \text{existuje } g \in G, \varphi(g) = h\}$ obraz homomorfismu φ .

Tvrzení 5.5. Necht' $\varphi : G \rightarrow H$ je homomorfismus grup. Platí $\ker(\varphi) \leq G$ a $\text{Im}(\varphi) \leq H$ jsou podgrupami.

Tvrzení 5.6 (Test monomorfismu). Necht' $\varphi : G \rightarrow H$ je homomorfismus grup. Potom φ je injektivní právě tehdy, když jádro $\ker(\varphi) = 1_G$ je triviální.

Cvičení

Cílem důkazu je porozumět dokazovanému tvrzení, ne jen prověřit jeho platnost!

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

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

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 $(\mathbb{R}, +) \rightarrow (T, \cdot)$.

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 $\text{Aut}(\mathbb{Z})$.

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 $G \not\cong H$, ale $\text{Aut}(G) \cong \text{Aut}(H)$.

5.11. Najděte $\text{Aut}(\mathbb{Z}_6)$.

5.12. Jestliže Ψ a Φ 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 $\Phi : \mathbb{Z}_{50} \rightarrow \mathbb{Z}_{50}$ 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 $f : X \rightarrow Y$ je bijekce mezi množinami X a Y . Ukažte, že $\alpha \mapsto f \circ \alpha \circ f^{-1}$ je izomorfismus $S_X \rightarrow S_Y$.

Nápověda k vybraným cvičením

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

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

5.8 Vezměme bijektivní zobrazení $\Phi : U(8) \rightarrow U(12)$ 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 $\text{Aut}(\mathbb{Z}) = \{id, \Phi\}$, 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

Při studiu konečných cyklických grup jsme dokázali, že řád podgrupy dělí řád cyklické grupy. Ukážeme, že se jedná o speciální případ všeobecně platné teoremů.

Definice 5.7. Necht' G je grupa a $H \leq G$ je podgrupa. Množinu $Hg = \{hg \mid h \in H\}$ nazýváme pravou třídou rozkladu podle podgrupy $H \leq G$. Podobně $gH = \{gh \mid h \in H\}$ nazýváme levou třídou rozkladu podle podgrupy $H \leq G$. Libovolný prvek třídy Hg (gH) se nazývá reprezentant třídy rozkladu.

Příklad 5.8. Necht' $H = \{m \cdot n \mid n \in \mathbb{Z}\} \leq \mathbb{Z}$ je podgrupa celých čísel, které jsou násobky čísla $m > 0$. Potom $H, H + 1, H + 2, \dots, H + m - 1$ jsou pravé třídy rozkladu. Navíc, $\mathbb{Z} = \cup_{i=0}^{m-1} H + i$.

Příklad 5.9. Necht' $\tau = (1, 2) \in S_3$ a $H = \langle \tau \rangle$. Určete množinu pravých a levých tříd rozkladu S_3 podle H . Jak je to s rovností $gH = Hg$?

Věta 5.10 (Vlastnosti tříd rozkladu). *Necht' $H \leq G$ 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 5.11. Počet tříd rozkladu G podle podgrupy $H \leq G$ nazýváme index podgrupy a označujeme jej $[G : H]$.

Věta 5.12 (Lagrange). *Necht' G je konečná grupa a $H \leq G$ je podgrupa. Potom $|H|$ dělí $|G|$.*

Důkaz. Ukážeme, že všechny třídy rozkladu jsou stejně velké. Nechť $f : Hg \rightarrow H$ je funkce daná $hg \mapsto h$. Toto zobrazení je prosté (injektivní), neboť $f(h_1g) = f(h_2g)$ 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 $g_i \in G$, $i = 1, \dots, m$ takoví, že platí $G = Hg_1 \cup \dots \cup Hg_m$ a $Hg_i \cap Hg_j = \emptyset$ pro $i \neq j$. Proto $|G| = \sum_{i=1}^m |Hg_i| = \sum_{i=1}^m |H| = m|H|$. \square

Důsledek 5.13. Řád libovolného prvku grupy G dělí řád grupy G .

Důsledek 5.14. 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 $\{a^n \mid n \in \mathbb{Z}\} = G$. \square

Věta 5.15 (Fermat). Nechť p je prvočíslo a $x \in \mathbb{Z}$ je celé číslo. Potom $x^p \equiv x \pmod{p}$.

Důkaz. Uvažujme unitární grupu $U(p) = \{1, 2, \dots, p-1\}$ řádu $p-1$. Podle důsledku 5.13 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 $\{[1], [2], \dots, [p-1]\}$ 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 $x^p \equiv x \pmod{p}$. \square

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 $d = \text{lcm}(n, m)$.

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 $\text{gcd}(r, s) = 1$, 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.** Necht' $H \subset G$ má index 2. Dokažte, že $a^2 \in H$ pro všechny prvky $a \in G$.
- 5.27.** Necht' $H = \{(1), (1, 2)(3, 4), (1, 3)(2, 4), (1, 4)(2, 3)\}$. Nalezněte levou třídu rozkladu H v A_4 . Kolik těchto tříd existuje?
- 5.28.** Necht' $H = \{\pm 0, \pm n, \pm 2n, \pm 3n, \dots\}$, 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.** Necht' $a, b \neq id$ 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.** Necht' 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.** Necht' 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.** Necht' 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.** Necht' H je podgrupa grupy S_4 a H obsahuje prvky $(1, 2)$ a $(2, 3, 4)$. Dokažte, že $H = S_4$.
- 5.37.** Necht' 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 prvočíslu.
- 5.39.** Necht' $|G| = 15$. 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.** Necht' $|G| = 8$. Ukažte, že grupa G musí obsahovat prvek řádu 2.
- 5.41.** Může grupa řádu 55 obsahovat právě dvacet prvků řádu 11? Svě rozhodnutí zdůvodněte.
- 5.42.** Necht' G je grupa řádu p^n , kde p je prvočíslu. Dokažte, že centrum grupy G nemůže být řádu p^{n-1} .
- 5.43.** Necht' $G = GL(2, \mathbb{R})$ a $H = SL(2, \mathbb{R})$. Necht' $\mathbb{A} \in G$ a předpokládejme, že $\det \mathbb{A} = 2$. Ukažte, že $\mathbb{A}H$ je množina matic 2×2 v G mající determinant 2.
- 5.44.** Necht' G je grupa s méně než sto prvky obsahující podgrupy řádu 10 a 25. Určete řád grupy G .

Nápověda k vybraným cvičením

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

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 $H, 1 + H, 2 + H, \dots, (n - 1) + H$ 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: $H = \{1, 11\}$, $7H = \{7 \cdot 1, 7 \cdot 11\} = \{7, 17\}$, $13H = \{13 \cdot 1, 13 \cdot 11\} = \{13, 23\}$ 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

Při zkoumání struktury grup použijeme redukce grupy pomocí vhodných operací na grupy menší. Snad nejdůležitější redukce je faktorizace grupy podle normální podgrupy, kterou zdefinujeme této sekci.

Definice 5.16. Nechť $S, T \subseteq G$ jsou neprázdné podmnožiny grupy G . Označme $ST = \{st; s \in S, t \in T\} \subseteq G$.

Věta 5.17 (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 $\varphi: S \times T \rightarrow ST$ 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

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

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 $\varphi(y_0)^{-1} \subseteq M$. \square

Definice 5.18. Podgrupa $K \leq G$ se nazývá normální, značíme $K \triangleleft G$, platí-li pro každé $g \in G$ rovnost $gKg^{-1} = K$.

Lemma 5.19. *Jádro homomorfismu $\varphi: G \rightarrow H$ je normální podgrupa.*

Důkaz. Nechť $K = \ker(\varphi) = \{x \in G; \varphi(x) = 1_H\}$ je jádro. Pro $x \in K$ a $g \in G$ platí

$$\varphi(gxg^{-1}) = \varphi(g)\varphi(x)\varphi(g^{-1}) = \varphi(g)\varphi(x)\varphi^{-1}(g) = \varphi(g) \cdot 1_H \cdot \varphi^{-1}(g) = 1_H.$$

Proto $gxg^{-1} \in K$. \square

Lemma 5.20. *Je-li $K \triangleleft G$ normální, pro každé $x \in G$ platí $xK = Kx$. Odtud dostaneme, že množiny levých a pravých tříd rozkladu podle normální podgrupy se rovnají.*

Definice 5.21. Necht $a \in G$. Zobrazení $\gamma_a: x \mapsto axa^{-1}$ nazýváme konjugace prvkem x .

Lemma 5.22. 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 5.23 (Faktorová grupa). *Pokud $N \triangleleft G$ 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 $(Nx)^{-1} = Nx^{-1}$. \square

Lemma 5.24. Necht $N \triangleleft G$. Přirozená projekce $\nu: x \mapsto Nx$ je homomorfismus $G \rightarrow G/N$ 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 5.25. 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 5.26. Platí $G' \triangleleft G$. Navíc, je-li $N \triangleleft G$, je G/N abelovská právě tehdy, když $G' \leq N$.

Důkaz. Necht $f: G \rightarrow G$ 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 $G' \triangleleft G$.

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

Cvičení

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

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

5.47. Grupa kvaternionů. Necht $G = \langle A, B \rangle \leq GL(2, \mathbb{C})$, 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 $A_n \triangleleft S_n$.

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

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

5.51. Dokažte, že pokud $N \triangleleft G$ 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 $H = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix}; a, b, d \in \mathbb{R}, ad \neq 0 \right\}$. 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 našli 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 $N \triangleleft G$. 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 5.27 (1. věta o izomorfismu: každý homomorfismus odpovídá přirozené projekci). *Pokud $f: G \rightarrow H$ je homomorfismus, $\text{Im}(f) \cong G/\ker(f)$.*

Důkaz. Označme $K = \ker(f)$ a nechť $\varphi: G/K \rightarrow H$ je zobrazení $\varphi: Ka \mapsto f(a)$.

Nejprve dokážeme, že φ je dobře definované: pokud $Ka = Kb$, potřebujeme dokázat $f(a) = f(b)$. 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 $Ka = K$. \square

Lemma 5.28. *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 $ST \triangleleft G$ normální.*

Důkaz. Nechť $T \triangleleft G$. Potom

$$s_1 t_1 (s_2 t_2)^{-1} = s_1 (t_1 t_2^{-1}) s_2^{-1} = s_1 s_2^{-1} (s_2 (t_1 t_2^{-1}) s_2^{-1}) = s_1 s_2^{-1} t' \in ST.$$

Proto $ST \leq G$. A podobně

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

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 $ST = TS$.

Nechť $S \triangleleft G$ a $T \triangleleft G$. Potom pro každé $g \in G$

$$g(st)g^{-1} = (gsg^{-1})(gtg^{-1}) = s't' \in ST.$$

□

Věta 5.29 (2. věta o izomorfismu). *Nechť $N \triangleleft G$ a $T \leq G$. Potom $N \cap T \triangleleft T$ a $T/(N \cap T) \cong NT/N$.*

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

Věta 5.30 (3. věta o izomorfismu). *Nechť $K \leq H \leq G$, kde $K \triangleleft G$ i $H \triangleleft G$. Potom $H/K \triangleleft G/K$ a platí $(G/K)/(H/K) \cong G/H$.*

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

Věta 5.31 (Věta o korespondenci). *Nechť $K \triangleleft G$ 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 $[S : T] = [S^* : T^*]$,
- $K \leq T \triangleleft S$ právě tehdy, když $T^* \triangleleft S^*$ a $S/T \cong S^*/T^*$.

Poznámka: Tuto větu můžeme interpretovat tak, že funkce $S \rightarrow S^*$ 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 $\nu^* : S \mapsto S/K = S^*$ 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 $\text{sgn}(\alpha)$. 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 $f : G \rightarrow H$ 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 $f : G \rightarrow H$ 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):

$$f(g_1g_2^{-1}) = f(g_1)f(g_2^{-1}) = f(g_1)f(g_2)^{-1} = f(g_1)f(g_1)^{-1} = id'.$$

A tedy $g_1g_2^{-1} \in \ker(f) = \{id\}$, a tudíž $g_1g_2^{-1} = id$. Z toho již vyplývá, že $g_1 = g_2$, a tedy f je injektivní zobrazení.

Kapitola 6

Přímý součin grup

V předešlé sekci jsme zavedli pojem faktorové grupy. Faktorizace je cesta k analýze struktury konečných grup. Grupy, které nelze netriviálně faktorizovat se nazývají jednoduché. Pokud dokážeme klasifikovat jednoduché grupy a pochopíme jak zrekonstruovat grupu z její normální podgrupy $1 \neq N \triangleleft G$ a z faktorové grupy G/N dostaneme rekurzivní charakterizaci všech konečných grup. Oba problémy, jak klasifikace jednoduchých grup, tak problém rekonstrukce G z informací o $N \triangleleft G$ a G/N jsou složité. Problém rekonstrukce je v literatuře znám pod názvem “problém rozšíření normální podgrupy N pomocí grupy $H \cong G/N$ ”. Nejjednodušší typ rozšíření je přímý součin grup, kterému je věnována tato sekce.

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 $H \rightarrow H \times K$ a $K \rightarrow H \times K$. Obráceně, projekce $p_1: (h, k) \rightarrow h$ a $p_2: (h, k) \rightarrow k$ na první a druhou složku jsou epimorfismy $H \times K \rightarrow H$ a $H \times K \rightarrow K$. Všimněme si rovněž, že zobrazení $(h, k) \mapsto (k, h)$ je izomorfismus $H \times K \rightarrow K \times H$, tedy $H \times K \cong K \times H$. Následující lemma shrnuje důležité vlastnosti přímého součinu grup.

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. Jádrem $\ker(p_1) = 1_H \times K$ a jádrem $\ker(p_2) = H \times 1_K$. Podle 1. věty o izomorfismu platí $1_H \times K \triangleleft H \times K$ a $H \times 1_K \triangleleft H \times K$. Druhá část tvrzení je triviální.

Zajímavou otázkou je, zda je možné tvrzení předchozího lemma obrátit. Ukazuje se, že to možné je. Dostáváme tak následující rozkladovou větu. \square

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

Důkaz. Protože $G = HK$, tak každý prvek $a \in G$ se dá vyjádřit v tvaru $a = hk$, kde $h \in H$ a $k \in K$. Tvrdíme, že toto vyjádření je jednoznačné. Dokazujeme 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 $h_1^{-1}h = k_1k^{-1} \in H \cap K = 1_G$. Proto $k_1 = k$ a $h_1 = h$. Uvažujme funkci $f: G \rightarrow H \times K$ 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 $f(ab) = f(a)f(b)$, kde $a = h_1k_1$, $b = h_2k_2$. Vzhledem k tomu, že $f(ab) = f(h_1k_1h_2k_2)$, potřebujeme, aby $k_1h_2 = h_2k_1$. Uvažujme komutátor $[h_2, k_1] = h_2k_1h_2^{-1}k_1^{-1} = (h_2k_1h_2^{-1})k_1^{-1} \in K$, zároveň $[h_2, k_1] = h_2(k_1h_2^{-1}k_1^{-1}) \in H$. Protože $H \cap K = 1$, tak $[h_2, k_1] = 1$. Odtud $h_2k_1 = k_1h_2$. Potom platí

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

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. \square

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 $H \triangleleft S_3$, $H \cap K = 1$, ale $S_3 = HK$ není izomorfní $H \times K \cong Z_3 \times Z_2$.

Následující teoréma ukazuje, že binární operace přímého součinu komutuje s faktorizací podle normálních podgrup.

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

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

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 $H \triangleleft G$ 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} necht' $H = \langle 5 \rangle$ 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 $\text{lcm}(m, n)$ dělí k . Protože $\text{gcd}(m, n) = 1$, je $\text{lcm}(m, n) = mn$. 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 součinem dvou vlastních podgrup.

Kapitola 7

Akce grup

Akce grupy je důležitý koncept nejen v teorii grup, ale i v širším matematickém kontextu, uvažujeme například akce lineárních grup na vektorových prostorech, nebo grupy topologických a geometrických transformací. Akce grup úzce souvisí s reprezentacemi grup v permutačních grupách. Aplikace můžeme najít v enumeracích konečných struktur.

7.1 Konjugace

Akce grupy G konjugací na prvcích G a na podgrupách G je důležitá pro studium struktury grupy G .

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 .

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

Definice 7.2. Centrum grupy G , značíme $Z(G)$, je podgrupa těch prvků, které komutují se všemi prvky grupy G , $Z(G) \triangleleft G$. 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. Označme $C = C_G(a)$. Definujme funkci $f: a^G \rightarrow G/C_G(a) = G/C$ 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 $h = gc^{-1}$ pro nějaké $c \in C$. Potom

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

A tedy f je dobře definovaná.

Nechť $x = gag^{-1}$, $y = hah^{-1}$ a necht' $f(x) = f(y)$. Potom $gC = hC$ a máme $h = gc$ pro nějaké $c \in C$. Protože $C = C_G(a)$, platí

$$y = hah^{-1} = gac^{-1}g^{-1} = gag^{-1} = x.$$

Proto f je injektivní. Zřejmě f je i surjektivní.

Druhá část tvrzení je důsledkem Lagrangeovy věty (Index podgrupy dělí řád grupy). \square

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 $H \triangleleft K \leq G$.

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 $f: H^G \rightarrow G/N$ 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. \square

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. Necht' $\alpha = \rho_1\rho_2 \dots \rho_k$ 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 $|\rho_i| = |\rho_i^\beta|$. Tedy řady permutací jsou stejné. Navýše, ρ_i^β je cyklus délky $|\rho_i|$. Kdyby tomu tak nebylo, tak existuje x_0 takové, že pro vlastního dělitele $m \mid |\rho_i|$ platí: $x_0 = id(x_0) = id^{\beta^{-1}}x_0 = (\rho_i)^m x_0$, spor. \square

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. Necht' α a β mají stejnou cyklovou strukturu a necht' $\alpha = \rho_1 \dots \rho_k$, $\beta = \delta_1 \dots \delta_k$. 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 $\beta = \alpha^\gamma$. \square

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 .

Důkaz. Označme $H, g_1H, \dots, g_{p-1}H$ třídy rozkladu G/H , kde p je prvočíslo. Buď třída g_iH obsahuje prvek z $C_G(x)$, nebo $C_G(x) \cap g_iH = \emptyset$. V prvním případě můžeme předpokládat, že reprezentant $g_i \in C_G(x)$. Potom třída $g_iC_H(x) \subset C_G(x)$. Navyš, třídy g_iH takové, že $g_i \in C_G(x)$ tvoří podgrupu $K = \eta(C_G(x)) \leq G/H$, kde η je přitozená projekce $y \mapsto yH$. Podobně, grupa $C_H(x)$ se zobrazí na grupu $L = \eta(C_H(x)) < K \leq G/H$. Protože $|G/H| = p$, z Lagrange-ovy teoremů a $1 \leq L < K \leq G/H$, máme $C_H(x) \leq H$, $K = G/H$ a $|C_G(x)| = p \cdot |C_H(x)|$. Proto

$$|x^G| = \frac{|G|}{|C_G(x)|} = \frac{p|H|}{p|C_H(x)|} = \frac{|H|}{|C_H(x)|} = |x^H|,$$

a platí $x^G = x^H$.

□

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 5.12 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. \square

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-cykklus γ ověříme, že $H^\gamma = H$. \square

Lemma 7.16. *A_5 je jednoduchá.*

Důkaz. Hlavní myšlenka důkazu je založena na jednoduchém důsledku definice normální podgrupy: každá normální podgrupa je disjunktním sjednocením orbit v akci grupy konjugací na svých prvcích.

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 platí $C_{A_5}(x) < C_{S_5}(x)$ a $[S_5 : A_5] = 2$. Použitím Lemy 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 $[S_5 : C_{S_5}(\alpha)] = |\alpha^{S_5}| = 24$. Z toho je jasné, že $|C_{S_5}(\alpha)| = |S_5|/[S_5 : C_{S_5}(\alpha)] = 120/24 = 5$. 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 $|\alpha^{A_5}| = [A_5 : C_{A_5}(\alpha)] = |A_5|/|C_{A_5}(\alpha)| = 60/5 = 12$. Vzhledem k tomu, že stejný výpočet platí pro libovolný 5-cyklos 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, $\binom{4}{2} = 15$ 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. \square

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

Důkaz. Protože $H \triangleleft A_n$ a v grupě A_n jsou všechny 3-cykly konjugované, s 3-cyklem $\gamma \in H$ obsahuje grupa H všechny 3-cykly. Zde používáme stejný argument jako pro A_5 .

Nechť $\alpha = \tau_1 \tau_2 \dots \tau_m$ 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, opakovaním 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 $A_n = H$. \square

Lemma 7.18. *A_6 je jednoduchá.*

Důkaz. Nechť $1 \neq H \triangleleft A_6$ 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 $H \cap F \triangleleft F$. 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-cyklos. Z lemmatu 7.17 vyplývá $H = A_6$.

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

Dokážeme, že tenhle případ se nestane. 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 položíme $\beta = (j, k, l)$. 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. \square

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

Důkaz. Vzhledem k Lemě 7.16 a 7.18 budeme předpokládat $n \geq 7$. Nechť $1 \neq H \triangleleft A_n$ je normální podgrupa. Naším cílem je dokázat, že H obsahuje 3-cykklus. Nechť $\beta \in H$, $\beta(i) = j \neq i$. Dále předpokládejme, že β není 3-cykklus. Kdyby všechny ostatní body byly fixovány, tak β je transpozice. Pokud jenom jeden, ze zvyšných bodů je nefixován, tak β je 3-cykklus. Proto existují k a l tak, že $\beta(k) \neq k$, $\beta(l) \neq l$ a $\{j, k, l\}$ je 3-prvková množina neobsahující i . Nechť $\alpha = (i)(j, k, l) \cdots \in A_n$ je 3-cykklus. 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 α a $\beta\alpha^{-1}\beta^{-1}$. Nechť $F \leq A_n$ je podgrupa, která fixuje všechny prvky s výjimkou těch, které se nacházejí ve dvou 3-cyklech rozkladu γ . Protože α a $\beta\alpha^{-1}\beta^{-1}$ jsou disjunktí 3-cykly, tak $F \cong A_6$ a $H \cap F \triangleleft F$. Z Lemy 7.18 vyplývá $H \cap F = F$ a H obsahuje 3-cykklus. Z lematu 7.17 vyplývá $H = A_n$. \square

Cvičení

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

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

7.4 Rerezentace 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 $L_a: g \mapsto ag$. 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 $\phi: a \mapsto L_a$ je hledaný monomorfismus $G \rightarrow S_G$. Je to morfismus, neboť $\phi(ab) = L_{ab} = L_a L_b = \phi(a)\phi(b)$. Navíc, $\phi(a) = 1$ implikuje $ag = g$ pro každé $g \in G$. Odtud, $a = gg^{-1} = 1$. \square

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

Důsledek 7.22. Necht' $|G| = n$ a necht' \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 $\psi: S_n \rightarrow GL(n, \mathbb{F})$ 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. \square

Věta 7.23. Necht' G je grupa a necht' $H \leq G$ je podgrupa indexu n . Potom existuje homomorfismus $\rho: G \rightarrow S_n$ s jádrem $\ker(\rho) \leq H$.

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

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 $G \rightarrow S_n$. Grupa G je jednoduchá, proto $\ker(\rho) = 1$ nebo $G = \ker(\rho) \leq H$. Ve druhém případě $G = H$ a $[G : H] = 1$. \square

Věta 7.26. Necht' $H \leq G$ a necht' X je množina všech podgrup konjugovaných s H . Potom existuje homomorfismus $\Psi: G \rightarrow S_X$ s jádrem $\ker(\Psi) \leq N_G(H)$.

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

Cvičení

7.9. Dokažte, že přiřazení $\alpha \mapsto M_\alpha$ je vnoření $S_n \rightarrow GL(n, \mathbb{F})$, 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 injektivní homomorfismus $G \rightarrow S_G$.

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. Necht' G je grupa a necht' X je množina. Zobrazení $\alpha: G \times X \rightarrow X$, 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 $\alpha: G \times X \rightarrow X$ je akce, je $\tilde{\alpha}: g \mapsto (x \mapsto gx)$ homomorfismus $G \rightarrow S_X$.

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

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

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

a podobně

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

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) Necht' $\theta: G \rightarrow S_X$ 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. Necht' 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. Necht' 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 $f: gx \mapsto gG_x$. Toto zobrazení je dobře definované. Dále $gG_x = hG_x$ implikuje $h = gc$, kde $c \in G_x$. Potom $h \cdot x = (gc) \cdot x = g \cdot (c \cdot x) = g \cdot x$ je ten samý prvek orbity $O(x)$. Proto f je injektivní. Pokud $gG_x \in G/G_x$, pro $y = g \cdot x$ platí $f(y) = gG_x$. \square

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 $G_x = C_G(x)$. \square

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 $G_H = N_G(H)$. \square

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 $\varphi: X \rightarrow Y$ 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

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

\square

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 $\theta: G \rightarrow H$ a bijekce $\varphi: X \rightarrow Y$ 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 $\text{Cor}(G) = \bigcap_{x \in X} G_x \leq G$.

Věta 7.39. *Nechť (G, X) je akce. Potom $K = \text{Cor}(G) \triangleleft G$ 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 $\text{Cor}(G) = 1$.

Důkaz. Uvažujme homomorfismus $\theta: G \rightarrow S_X$ definovaný přiřazením $g \mapsto (x \mapsto g \cdot x)$. Potom $\ker(\theta) = \text{Cor}(G) = K$, a proto $K \triangleleft G$.

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 $G/K \cong \text{Im}(\theta) \leq S_X$. □

Cvičení

7.13. Symetrická grupa S_n má akci na množině polynomů n proměnných definovanou $\sigma \cdot f(x_1, x_2, \dots, x_n) = f(x_{\sigma 1}, x_{\sigma 2}, \dots, x_{\sigma n})$. Nechť $D = D(x_1, \dots, x_n) = \prod_{i < j} (x_i - x_j)$. 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 $\text{Orb}(G, X)$ počet G -orbit a $\text{Fix}(g)$ počet bodů X fixovaných $g \in G$. Potom*

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

Důkaz. Použijeme princip počítání dvěma způsoby. Prvky grupy G i množinu X můžeme lineárně uspořádat. Uvažujme matici A dimenze $|G| \times |X|$ s prvky $a_{i,j} = 1$ právě tehdy, když $g_i \cdot x_j = x_j$, kde $g_i \in G$ a $x_j \in X$. V opačném případě $a_{i,j} = 0$. Potom součet hodnot i -tého řádku je $\sum_{j=1}^{|X|} a_{i,j} = \text{Fix}(g_i)$. Součet hodnot j -tého sloupce je $\sum_{i=1}^{|G|} a_{i,j} = |G_{x_j}|$.

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 $G_y \rightarrow G_x$ a $G_x \rightarrow G_y$, proto $G_x \cong G_y$. 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 roven $[G : G_x]$. Proto každá orbita O přispívá k součtu $\sum_{x \in X} |G_x|$ hodnotou $|G_y|[G : G_y] = |G|$, kde $y \in O$ je vybraný reprezentant orbity O , a tedy platí

$$\sum_{g \in G} \text{Fix}(g) = \sum_{i,j} a_{i,j} = \sum_{x \in X} |G_x| = \sum_O |G_y|[G : G_y] = \sum_O |G| = |G| \cdot \text{Orb}(G, X).$$

□

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

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

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

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, \dots, 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 $i = 1, 2, \dots, n$. 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 $\text{Fix}(1) = |X| = q^n$ a $\text{Fix}(\tau) = q^{\lfloor n+1/2 \rfloor}$. Ve druhém vztahu jsme využili to, že $\tau \cdot x = x$ právě tehdy, když x je palindrom. Potom $\text{Orb}(G, X) = \frac{1}{2}(q^n + q^{\lfloor n+1/2 \rfloor})$.

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

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

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

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

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

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

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

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

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

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

A na druhou stranu je

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

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 Grupy geometrických transformací

Felix Klein v roce 1872 publikoval Erlangenský program, v kterém navrhl klasifikovat různé geometrie podle prostoru a příslušné grupy geometrických transformací. V následovném textu budeme studovat dvě klasické geometrické grupy: grupu izometrií a afinní grupu.

Skalární součin vektorů $x = (x_1, \dots, x_n)$ a $y = (y_1, \dots, y_n)$ z \mathbb{R}^n je číslo $(x, y) = \sum_{i=1}^n x_i y_i$. Funkci $\mathbb{R}^n \rightarrow \mathbb{R}^+$ definovanou vztahem

$$\|x\| = \|(x_1, \dots, x_n)\| = \sqrt{(x, x)} = \sqrt{\sum_{i=1}^n x_i^2},$$

nazýváme *norma vektora* $x = (x_1, \dots, x_n)$. V následujícím textu budeme využívat některé hezké vlastnosti skalárního součinu a normy.

Definice 7.46. *Izometrie* je funkce $T: \mathbb{R}^n \rightarrow \mathbb{R}^n$, 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 $S: \mathbb{R}^n \rightarrow \mathbb{R}^n$ je *ortogonální*, jestliže platí $\|Sx\| = \|x\|$.

Zřejmě každá ortogonální transformace je izometrie fixující nulový vektor nebo

$$\|S(x) - S(y)\| = \|S(x - y)\| = \|x - y\|.$$

Definice 7.48. Pro $i = 1, \dots, n$ označme ϵ_i vektor vektorového prostoru \mathbb{R}^n , který má i -tou souřadnici rovnou jedna a všechny ostatní souřadnice jsou 0. Monožina $\{\epsilon_i; i = 1, \dots, n\}$ se nazývá *standartní ortonormální báze* prostoru \mathbb{R}^n . Obecně, báze \mathcal{B} vektorového prostoru je *ortonormální*, když pro každé dva vektory $x, y \in \mathcal{B}$ platí, $(x, y) = 0$ pokud $x \neq y$ a $(x, x) = 1$. Symbol $\lambda_{i,j} = 1$ pro $i = j$, a $\lambda_{i,j}$ když $i \neq j$. V literatuře se $\lambda_{i,j}$ nazývá Kroneckerovo lambda.

Lemma 7.49. *Lineární transformace S je ortogonální právě tehdy, když $\{S(\epsilon_i)\}$, $i = 1, 2, \dots, n$ je ortonormální báze.*

Z definice vyplývá, že ortogonální transformace tvoří podgrupu grupy lineárních transformací. Tato grupa může být interpretována jako grupa symetrií jednotkové n -dimenzionální sféry tvořenou body \mathbb{R}^{n+1} ve vzdálenosti jedna od nulového vektoru. Pro $n = 2$ tvoří sféra povrch koule s poloměrem 1 se středem v počátku souřadnicového systému.

Důkaz. (\Rightarrow) Chceme dokázat, že pro skalární součin platí $(Sx, Sy) = (x, y)$. Nejdříve si všimneme, že ze vztahu $(x_i + y_i)^2 = x_i^2 + 2x_i y_i + y_i^2$ 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) Necht' $x = \sum_i x_i \epsilon_i$. Potom $Sx = \sum_i x_i S(\epsilon_i)$ a s použitím vlastností skalárního součinu dostaneme

$$\begin{aligned} \|Sx\|^2 &= (Sx, Sx) = \left(\sum_i x_i S(\epsilon_i), \sum_j x_j S(\epsilon_j) \right) = \sum_{i,j} (x_i S(\epsilon_i), x_j S(\epsilon_j)) = \\ &= \sum_{i,j} x_i x_j (S(\epsilon_i), S(\epsilon_j)) = \sum_{i,j} x_i x_j \lambda_{i,j} = (x, x) = \|x\|^2. \end{aligned}$$

□

Lemma 7.50. *Ortogonální transformace tvoří podgrupu grupy lineárních transformací.*

Lemma 7.51. *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 $x = (x_1, \dots, x_n)$ je libovolný vektor a $T(x) = y = (y_1, \dots, y_n)$. Máme

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

Proto

$$y_1^2 + y_2^2 + \dots + y_n^2 = x_1^2 + \dots + x_n^2.$$

Z předpokladů plyne

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

A odtud

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

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

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

Věta 7.52. *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 7.51 je R ortogonální transformace. Ale $T = S^{-1}R$. \square

Věta 7.53. *Funkce $T: \mathbb{R}^n \rightarrow \mathbb{R}^n$ fixující 0 je izometrie právě tehdy, když zachovává skalární součin, tedy $(Tx, Ty) = (x, y)$.*

Důkaz. (\Rightarrow) Z předpokladů $\|x + y\|^2 = \|T(x + y)\|^2$. Z definice normy a použitím vlastností skalárního součinu máme

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

$$\begin{aligned} \|T(x + y)\|^2 &= (T(x + y), T(x + y)) = (Tx + Ty, Tx + Ty) = \\ &= (Tx, Tx) + 2(Tx, Ty) + (Ty, Ty) = \|Tx\|^2 + 2(x, y) + \|Ty\|^2. \end{aligned}$$

Protože T fixuje 0, použitím $\|Tx\| = \|x\|$ a $\|Ty\| = \|y\|$ dostaneme $(Tx, Ty) = (x, y)$.

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

$$\begin{aligned} \|T(x) - T(y)\|^2 &= (Tx - Ty, Tx - Ty) = (Tx, Tx) - 2(Tx, Ty) + (Ty, Ty) = \\ &= (x, x) - 2(x, y) + (y, y) = (x - y, x - y) = \|x - y\|^2. \end{aligned}$$

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

V geometrii se úhel mezi dvěma vektory definuje vztahem

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

Důsledek 7.54. *Nechť T je funkce $T: \mathbb{R}^n \rightarrow \mathbb{R}^n$ 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 7.51 a věty 7.53. Použijeme Lemma 7.49. 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 $A^t A = E$.

A naopak, jestliže platí $A^t A = E$, platí i $(u_i, u_j) = \lambda_{i,j}$ a báze $\{u_i\}$ je ortonormální. Podle lemmatu 7.49 je T izometrií. \square

Definice 7.55. 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 determinanem 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 vyjádřena. V lineární algebře se relace konjugace v lineární grupě nazývá podobnost.

Izometrie $\varphi: x \mapsto Tx + w$ 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 $H = \langle x_1, \dots, x_{n-1} \rangle \subset \mathbb{E}_n$, 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, \dots, x_{n-1}, a vyjádření

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

Věta 7.56. *Reflexe fixující 0 je orientaci měnící izometrie.*

Příklad 7.57. 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 $\theta \in (-\pi, \pi)$. 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 $\det(T^-) = -1$. 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 přímkou 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 $Aut(\Delta)$ a podgrupu orientaci zachovávající izometrii označíme $Aut^+(\Delta)$.

Lemma 7.58. *Nechť φ je izometrie \mathbb{E}_n , necht' A_1, \dots, A_k jsou body a necht' $x = \sum_{i=1}^k \lambda_i A_i$ je konvexní kombinace. Potom $\varphi(x) = \sum_{i=1}^k \lambda_i \varphi(A_i)$.*

Lemma 7.58 dokážeme v rámci obecnějšího tvrzení, viz lemma 7.62.

Věta 7.59. *Nechť Δ je pravidelný konvexní n -úhelník s těžištěm v $(0, 0)$, $n \geq 3$. Potom $\text{Aut}(\Delta)$ je řádu $2n$ a $\text{Aut}(\Delta) = \langle T, S \rangle$, přičemž $|T| = n$, $|S| = 2$ a $STS = T^{-1}$.*

Důkaz. Důkaz spočívá v několika krocích.

Krok 1. Zřejmě každá izometrie $\varphi \in \text{Aut}(\Delta)$ zobrazuje vrchol na vrchol. Vzhledem k tomu, že každý bod Δ je konvexní kombinací vrcholů, z lemmatu 7.58 vyplývá, že obraz každého bodu je jednoznačně určený obrazy vrcholů Δ . Z toho plyne, že $\text{Aut}(\Delta) \hookrightarrow S_n$.

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 . Necht' e je hrana, potom $|G_e| = 2$, podle kroku 1. Podle Věty 7.31 je $|\text{Orb}(e)| = [G : G_e] = |G|/|G_e|$. Po dosažení dostaneme $n = |G|/2$, a proto $|G| = 2n$.

Krok 3. Necht' 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 $|G| = 2n$, $\langle T \rangle \triangleleft G$ je normální podgrupa indexu 2. Odtud plyne $STS = T^i$ pro nějaké i , $\text{gcd}(n, i) = 1$. Ztotožníme $T = (1, 2, \dots, n)$ 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 $i = -1$. \square

Všimněme si, že $G = \langle T \rangle \cup S\langle T \rangle$ a pro prvky typu ST^i platí $(ST^i)^2 = ST^i ST^i = T^{-i} T^i = 1$. Tedy všechny n prvky třídy $S\langle T \rangle$ jsou involuce. *Involuce* v grupě G je prvek řádu 2. Grupu symetrií pravidelného n -úhelníku 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 7.59 triviálně platí.

Věta 7.60. *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 $b \mapsto S$ je izomorfismus $\langle a, b \rangle \rightarrow D_{2n}$. \square

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. Necht' $\text{Aut}(\Delta)$ 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 7.61. 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 $\text{Aff}(n, \mathbb{R})$.

Následující lemma hovoří o vlastnostech grupy afinních transformací.

Lemma 7.62. *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, \dots, A_k je množina bodů, potom $A_2 - A_1, \dots, A_k - A_1$ jsou lineární nezávislé vektory právě tehdy, když $\varphi(A_2 - A_1), \dots, \varphi(A_k - A_1)$ 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

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

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

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

což jsme chtěli dokázat. □

Důsledek 7.63. *Grupa $\text{Aff}(2, \mathbb{R})$ je tranzitivní na množině všech trojúhelníků v rovině.*

Věta 7.64. *V každém trojúhelníku se všechny tři těžnice protínají v jednom bodě, přičemž tento bod je dělí v poměru 2 : 1.*

Důkaz. Z Důsledku 7.63 vyplývá, že tvrzení stačí dokázat pro rovnostranný trojúhelník $\triangle ABC$ s hranou jednotkové délky. Označme t_A , t_B a t_C těžnice spojující po řadě bod A se středem BC , bod B se středem AC , a bod C se středem AB . Označme $\{T\} = t_A \cap t_B$. Reflexe ρ_A a ρ_B fixující těžnice t_A a t_B , generují grupu symetrií $\triangle ABC$, tedy T je bod fixovaný každou symetrií $\triangle ABC$. Speciálně reflexe $\rho_C = \rho_B \rho_A \rho_B$ fixuje T , a tedy všechny tři těžnice se protínají v bodě T . Tři těžnice t_A , t_B a t_C tvoří orbitu v akci $\text{Aut}(\triangle ABC)$, proto jsou stejné délky. Osobitně platí $|TA| = |TB| = |TC|$, tedy bod T dělí těžnice ve stejném poměru $t = \sin(30^\circ) = 1/2$. Alternativně je možné hodnotu t vypočítat využitím Pythagorovy věty. □

V duchu Kleina můžeme i topologii považovat za geometrii. Jestliže Δ je pravidelný n -úhelník, grupa homeomorfizmů roviny zobrazující Δ na sebe je tranzitivní na množině bodů Δ . Věta o pevném bodě hovoří o tom, že každý prvek této grupy fixuje v akci na Δ nějaký bod. To je v protikladu k tomu, co jsme dokázali o akci tranzitivní grupy na konečné množině bodů (Důsledek 7.41).

Cvičení

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

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

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

Cílem této sekce je prozkoumat možnost obrácení implikace Lagrangeovy teorémy. Bude nás tedy zajímat následovná otázka: Nechť d je dělitel řádu $|G|$ nějaké konečné grupy G . Existuje podgrupa $H \leq G$ řádu $|H| = d$? Pozitivní odpověď na tuto otázku jsme nahlédly v případě, že G je cyklická grupa. Z druhé strany, alternující grupa A_4 má dělitele $d = 6$, ale podgrupu velikosti 6 bychom v A_4 hledali marně. Užitím Bertrandovho postulátu (“Pro každé k existuje prvočíslo p takové, že $k \leq p < 2k$ ”) můžeme výše uvedený příklad zobecnit na libovolnou alternující grupu.

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 $\langle x \rangle \triangleleft G$ 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 $\nu: G \rightarrow G/\langle x \rangle$. Nechť $y \in \nu^{-1}(y^*)$. Restrikce $\nu|_{\langle y \rangle}: \langle y \rangle \rightarrow \langle y^* \rangle$ je epimorfismus cyklických grup, proto p dělí řád y a jsme v případě 1. \square

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:

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

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 $[G : C_G(x)]$ je mocnina p^e , $0 \leq e < n$. Pokud pro nějaké $x \neq 1$ platí, $[G : C_G(x)] = 1$, potom $x \in Z(G)$ a $|Z(G)| > 1$ a z Lagrangeovy věty $p \mid |Z(G)|$. V opačném případě je index $[G : G_x]$ dělitelný p pro každé netriviální $x \in G$. 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 $Z(G) \triangleleft G$ a faktorová grupa $G/Z(G) \cong Z_p$. Nechť $y \notin Z(G)$, potom $G/Z(G) = \{Z(G), Z(G)y, \dots, Z(G)y^{p-1}\}$. Tedy každý prvek $g \in G$ má tvar $g = x^i y^j$, kde $Z(G) = \langle x \rangle$. Potom $y^g = y^{-j} x^{-i} y x^i y^j = y^{-j} y y^j = y$ 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 $H \triangleleft G$.*

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 akci 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 $H \triangleleft G$.

□

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 $x, y \in H$. Z Lagrangeovy věty $p^e = |H| = |X \cap H| + 1$ pro nějaké $e \geq 1$. Odtud $|X \cap H| = p^e - 1$. Velikost orbity $x^G = [G : G_x]$ 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 $(H, K_1), \dots, (H, K_a)$ jsou všechny takové dvojice, které obsahují H . Podle věty 8.6 je $H \triangleleft K_j$, a tedy $K_j \leq N_G(H) = N$. Uvažujme přirozenou projekci $\nu: N \rightarrow N/H$. 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 $(H_1, K), \dots, (H_b, K)$ jsou všechny dvojice pro fixovanou podgrupu K řádu p^{s+1} . Podle věty 8.6 je $H_i \triangleleft K$. 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 $D_j \triangleleft K$, 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 $H_j \mapsto H_j/D_j$ 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 $r_s \equiv r_{s+1} \pmod{p}$. Proto pro každé $s \leq n$ platí $r_1 \equiv r_s \pmod{p}$. Nyní už tvrzení vyplývá z Lemmatu 8.7. \square

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 $1 \pmod{p}$. 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 $1 \pmod{p}$. \square

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, \dots, m_n) , $m_i > 0$, $i = 1, \dots, n$, 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 $m_1 \leq m_2 \leq \dots \leq m_n$. 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, \dots, m_k) takových, že

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

Odtud pro $k = 1, \dots, \lfloor n/q \rfloor$ dostaneme konečně mnoho n -tic splňujících podmínky. \square

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 $|C_G(x_j)|$, $j = m+1, \dots, n$. Je však jen konečně mnoho konečných grup daného řádu. \square

Cvičení

8.1. Nechť $H \triangleleft G$ 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 $1 < H \triangleleft G$. Dokažte, že $H \cap Z(G) \neq 1$.

8.4. Nechť G je konečná p -grupa a $H \triangleleft G$, $|H| = p$. 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 $\nu: N_G(P) \rightarrow N_G(P)/P$ je přirozená projekce. Uvažujme $\nu^{-1}(yP)$. 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). \square

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 necht' $X = \{P_1, P_2, \dots, P_r\}$ je množina podgrup konjugovaných s P . Grupa G má akci na X , $a \cdot P_i = P_i^a$. Necht' 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 $a^{-1}P_i a = P_i$. 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 $P \triangleleft G$.

A naopak, necht' $P \triangleleft G$ 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. Necht' P je Sylowova p -grupa. Chceme dokázat, že p nedělí $[G : P]$. Necht' $N = N_G(P)$, 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 prvočísl a necht' G je konečná grupa. Necht' p^k dělí řád $|G|$. Potom G obsahuje podgrupu řádu p^k .*

Důkaz. Necht' 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 $k < e$, tak existence podgrupy řádu p^k v P vyplývá z tvrzení, že počet podgrup řádu p^k v P je $\equiv 1 \pmod{p}$ (věta 8.8). □

Věta 8.19 (Frattiniho argument). *Nechť $K \triangleleft G$ je normální podgrupa v konečné grupě. Necht' 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. Necht' X je konečná G -množina a necht' 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. Necht' pro každé prvočísl 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 dihedralní.*

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 $H \triangleleft G$. A proto $tst = s^i$ pro nějaké i . Dále

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

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

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

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

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 $\psi: G \rightarrow S_q$ 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 $P \triangleleft G$.

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 $Q \triangleleft G$, $G = P \times Q = \langle ab \rangle \cong C_{pq}$.

Ve druhém případě $q|p - 1$ a Q není normální podgrupa. Protože $P \triangleleft G$, 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 $a^j ba^{-j} = b^{m^j}$. Pro $j = q$ dostaneme požadovaný vztah. \square

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 $\langle a \rangle \triangleleft G$ 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 $\langle a \rangle \triangleleft G$ 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 dihedralní. Pokud $b^2 = a^2$, G je grupa kvaternionů. \square

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:

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_{15} |

Na následujícím příkladu si ukážeme další aplikaci Sylowových vět.

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 a $r|30$. Z jednoduchosti, G máme $r \neq 1$. Jediný vhodný dělitel je 6. Počet netriviálních prvků v těchto grupách je $6 \cdot 4$. Podobně musí být 10 Sylowových 3-grup, což dává 20 netriviálních prvků. Protože grupy řádů 3 a 5 mají triviální průnik, počet prvků v G je alespoň $1 + 20 + 24 = 45 > 30$.

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 $\psi: G \rightarrow S_4$ 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, $|G| = \prod_{i=1}^n p_i^{n_i}$, 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 $H = G$. \square

Poznámka: 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 $b \notin \langle a \rangle$. Potom existuje také b minimálního řádu 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 z minimality i řád $|b| = p$. Potom $\langle a \rangle \cap \langle b \rangle = 1$. Uvažujme přirozenou projekci $\psi: G \rightarrow G/\langle b \rangle$. 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 $\langle a \rangle = \psi^{-1}(\langle \bar{a} \rangle)$ a $K = \psi^{-1}(\bar{K})$ jsou disjunktní normální podgrupy, přičemž $|G| = |\langle a \rangle| \cdot |K|$. Proto $G = \langle a \rangle \times K$. \square

Důsledek 9.4. *Nechť G je abelovská p -grupa. Potom G je izomorfní přímému součinu na na cyklické p -grupy.*

Důkaz. Rozklad získáme opakovaným použitím Lemmy 9.3. \square

Lemma 9.5. *Nechť G je abelovská p -grupa. Nechť $G = H_1 \times H_2 \times \dots \times H_m$ a $G = K_1 \times K_2 \times \dots \times K_n$ jsou rozklady na netriviální cyklické podgrupy, přičemž $|H_1| \geq |H_2| \geq \dots \geq |H_m|$ a $|K_1| \geq |K_2| \geq \dots \geq |K_n|$.*

Potom $m = n$ a $|H_i| = |K_i|$, $i = 1, \dots, m$.

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 $G^p = H_1^p \times H_2^p \times \dots \times H_{m'}^p$, $G^p = K_1^p \times K_2^p \times \dots \times K_{n'}^p$, 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

$$|H_1||H_2|\dots|H_{m'}|p^{m-m'} = |G| = |K_1||K_2|\dots|K_{m'}|p^{n-n'}.$$

Odtud $m = n$ a zbylé grupy H_i, K_i pro $i > m' = n'$ jsou cyklické grupy řádu p . \square

Definice 9.6. 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 9.7. Najděte rozklad multiplikativní grupy $U(65)$ na cyklické p -grupy. 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 multiplikativní řád $||2|| = 12$. Potom $2^4 = 16$ generuje cyklickou Sylowovu 3-grupu v $U(65)$ řádu 3. 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 |
| Rád | 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 9.8. Pro každého dělitele d řádu $|G|$ konečné abelovské grupy G existuje podgrupa grupy G řádu d .

Příklad 9.9. Nechť G je abelovská grupa řádu $|G| = 72 = 2^3 \cdot 3^2$. 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

$$G = G_0 \geq G_1 \geq \dots \geq G_n = 1,$$

kde pro každé $i = 0, \dots, n-1$ platí $G_{i+1} \triangleleft G_i$. *Podílové grupy* normálního řetězce jsou grupy G_i/G_{i+1} , $i = 0, 1, \dots, n-1$; jeho *délka* je počet vlastních inkluzí (nebo jinak délka je počet jeho netriviálních podílových grup).

Definice 10.2. Normální řetězec

$$G = H_0 \geq H_1 \geq \dots \geq H_m = 1$$

je *zjemněním* normálního řetězce

$$G = G_0 \geq G_1 \geq \dots \geq G_n = 1,$$

jestliže G_0, G_1, \dots, G_n je vybraná posloupnost z postupnosti H_0, H_1, \dots, H_m .

Definice 10.3. *Kompoziční řetězec* je normální řetězec

$$G = G_0 \geq G_1 \geq \dots \geq G_n = 1,$$

ve kterém pro všechny $i = 0, \dots, n-1$, 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 $A \triangleleft A^*$ a $B \triangleleft B^*$ jsou čtyři podgrupy grupy G . Potom

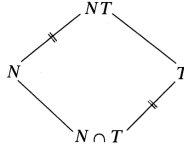
$$A(A^* \cap B) \triangleleft A(A^* \cap B^*),$$

$$B(B^* \cap A) \triangleleft B(B^* \cap A^*),$$

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 $N \triangleleft G$ a $T \leq G$. Potom $N \cap T \triangleleft T$ a $T/(N \cap T) \cong NT/N$.



Ve druhé větě o izomorfismu položíme $G = A^*$, $N = A \triangleleft A^*$ a $T = A^* \cap B^*$. Potom

$$N \cap T = A \cap (A^* \cap B^*) = A \cap A^* \cap B^* = A \cap B^* \triangleleft A^* \cap B^* = T.$$

Pokud položíme $N = B \triangleleft B^*$, podobnou úvahou dostaneme $B \cap A^* \triangleleft A^* \cap B^*$. Vzhledem k tomu, že $A \triangleleft A^*$ i $B \triangleleft B^*$, je $A(A^* \cap B) \triangleleft A(A^* \cap B^*)$ i $B(B^* \cap A) \triangleleft B(B^* \cap A^*)$. Protože $A \cap B^* \triangleleft A^* \cap B^*$ i $A^* \cap B \triangleleft A^* \cap B^*$, je $D = (A \cap B^*)(A^* \cap B) \triangleleft A^* \cap B^*$.

Dalším krokem důkazu je konstrukce epimorfismu

$$f: B(B^* \cap A^*) \rightarrow (A^* \cap B^*)/D.$$

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 $B \triangleleft B^*$ dostaneme

$$b_1c_1b_2c_2 = b_1(c_1b_2c_1^{-1})c_1c_2 = b_1b'_2c_1c_2,$$

kde $b'_2 \in B$.

Potom

$$f(xy) = f(b_1c_1b_2c_2) = f(b_1b'_2c_1c_2) = c_1c_2D = c_1Dc_2D = f(x)f(y).$$

Zřejmě $f(x) = D$ právě tehdy, když $x = bc_1c_2$, kde $b \in B$, $c_1 \in A^* \cap B$ a $c_2 \in A \cap B^*$. Takoveto 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. Necht

$$G = H_0 \geq H_1 \geq \dots \geq H_m = 1,$$

$$G = G_0 \geq G_1 \geq \dots \geq G_n = 1$$

jsou normální řetězce pro grupu G . Položme $G_{i,j} = G_{i+1}(G_i \cap H_j)$ pro všechny $j = 0, 1, \dots, m$. 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 $j = 0, \dots, m-1$. 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

$$G_i = G_{i,0} \geq G_{i,1} \geq \dots \geq G_{i,m-1} \geq G_{i,m} = G_{i+1} = G_{i+1,0}$$

pro $i = 0, \dots, n-1$ a $j = 0, \dots, m$.

Položíme v Zassenhausově lemmatu $A = G_{i+1}$, $A^* = G_i$, $B = H_{j+1}$ a $B^* = H_j$. Potom dostaneme $G_{i,j+1} \triangleleft G_{i,j}$. Proto posloupnost $\{G_{i,j}\}$ (s lexikálním uspořádáním dvojitých indexů) tvoří normální řetězec podgrup grupy G , který je zjemněním řetězce $\{G_i\}$.

Podobně položíme $H_{i,j} = H_{j+1}(H_j \cap G_i) \geq H_{j+1}(H_j \cap G_{i+1}) = H_{i+1,j}$,

$$H_j = H_{0,j} \geq H_{1,j} \geq \dots \geq H_{n-1,j} \geq H_{n,j} = H_{j+1}$$

pro $i = 0, 1, \dots, n$ a $j = 0, \dots, m-1$. 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 $G_{i,j}/G_{i,j+1} \rightarrow H_{i,j}/H_{i+1,j}$, 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. \square

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 .

Důkaz. Uvažujme cyklickou grupu $G = \langle x \rangle$ řádu $n = p_1 p_2 \dots p_t$ (prvočísla v rozkladu se mohou opakovat). Potom

$$G = \langle x \rangle \triangleright \langle x^{p_1} \rangle \triangleright \langle x^{p_1 p_2} \rangle > \dots \langle x^{p_1 p_2 \dots p_{t-1}} \rangle \triangleright \langle x^{p_1 p_2 \dots p_t} \rangle = 1$$

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 . \square

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 $S_n \triangleright A_n \triangleright 1$ je kompoziční řetězec s podílovými grupami Z_2 a A_n . \square

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 $G = G_0 \triangleright G_1 \triangleright \dots \triangleright G_k = 1$. 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 K je podgrupa společného zjemnění $G_i \triangleright K \triangleright G_{i+1}$. Potom existuje epimorfismus z abelovské grupy $\Phi : G_i/G_{i+1} \rightarrow$

K/G_{i+1} daný $gG_{i+1} \mapsto gK$, $g \in G_i$. Proto všechny podílové grupy zjemnění jsou abelovské a tedy i podílové grupy kompozičního řetězce jsou abelovské. Necht' H_i/H_{i+1} není cyklická prvočíselného řádu. Potom $H_i/H_{i+1} = A \times B$, kde A je cyklická prvočíselného řádu a $A > 1$ i $B > 1$ (Cauchyho teoréma). Označme $N = \Phi^{-1}(A)$. Potom $H_i \triangleleft N \triangleleft H_{i+1}$ je netriviální zjemnění, spor s maximalitou $\{H_j\}_{j=0}^m$. Proto každá faktorová grupa je cyklická prvočíselného řádu. \square

Věta 10.14. *Každá podgrupa $H \leq G$ řešitelné grupy G je řešitelná.*

Důkaz. Pokud $G = G_0 \geq G_1 \geq \dots \geq G_n = 1$ je řešitelný řetězec, je $H = H_0 \geq H \cap G_1 \geq \dots \geq H \cap G_n = 1$ 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

$$H \cap G_{i+1} = (H \cap G_i) \cap G_{i+1} \triangleleft H \cap G_i.$$

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. \square

Věta 10.15. *Každý kvocient G/N řešitelné grupy G je řešitelný.*

Důkaz. Dokážeme následující tvrzení: Necht' G je řešitelná s řešitelným řetězcem $\{G_i\}_{i=0}^t$. Pokud $f: G \rightarrow H$ je epimorfismus, je $\{f(G_i)\}_{i=0}^t$ řešitelný řetězec grupy H .

Tvrzení dostaneme, jestliže položíme $H = G/N$, kde $N \triangleleft G$. Necht' $x_i \in G_i$, $i = 0, 1, \dots, t-1$.

Necht' $h_i = f(x_i) \in f(G_i)$. Potom

$$h_i f(x_{i+1}) h_i^{-1} = f(x_i) f(x_{i+1}) (f(x_i))^{-1} = f(x_i x_{i+1} x_i^{-1}) \leq f(G_{i+1}).$$

Proto $f(G_{i+1}) \triangleleft f(G_i)$ 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 $p: f(G_i) \rightarrow f(G_i)/f(G_{i+1})$ přirozenou projekcí $f(x_i) \mapsto f(x_i)f(G_{i+1})$. Potom $\varphi: x_i \mapsto f(x_i)f(G_{i+1})$ je epimorfismus $G_i \rightarrow f(G_i)/f(G_{i+1})$, neboť φ je složení epimorfismů f a p . Zřejmě $G_{i+1} \leq \ker(\varphi)$, proto φ indukuje epimorfismus $\varphi^*: G_i/G_{i+1} \rightarrow f(G_i)/f(G_{i+1})$. Protože G_i/G_{i+1} je abelovská, i $f(G_i)/f(G_{i+1})$ je abelovská. \square

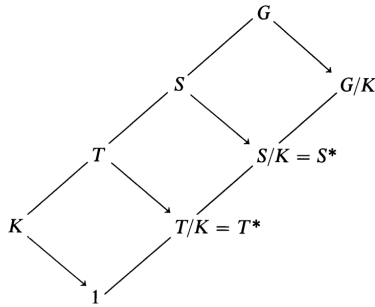
Následující tvrzení budeme potřebovat k důkazu další věty o řešitelných grupách.

Věta 10.16 (Korespondenční věta). *Necht' $K \triangleleft G$ jsou grupy, $K \leq T \leq S \leq G$ jsou podgrupy a $\nu: G \rightarrow G/K$ 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) $T \triangleleft S$ právě tehdy, když $T^* \triangleleft S^*$, 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 $\alpha: sT \mapsto \nu(s)T^*$ je bijekce $S/T \rightarrow S^*/T^*$. Jestliže G je konečná, alternativně platí

$$[S^* : T^*] = |S^*|/|T^*| = |S/K|/|T/K| = (|S|/|K|)/(|T|/|K|) = |S|/|T| = [S : T].$$

(iii) Jestliže $T \triangleleft S$, třetí věta o izomorfismu implikuje $T^* = T/K \triangleleft S/K = S^*$ a navíc $S^*/T^* = (S/K)/(T/K) \cong S/T$. Zbývá dokázat, že $T^* \triangleleft S^*$ implikuje $T \triangleleft S$. Nechť $\mu: S^* \rightarrow S^*/T^*$ je přirozená projekce a $\nu_S = \nu|_S$ je restrikce ν na S . Potom $\Phi = \mu\nu_S: S \rightarrow S^*/T^*$ 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 $K \triangleleft G$. Podobně pro svaz normálních podgrup G/K . Speciálně, korespondenční věta zaručuje, že k normálnímu řetězci grupy

$$G/K = G^* \geq K_1^* \geq K_2^* \geq \dots \geq K_n^* = 1$$

existuje částečný normální řetězec

$$G \geq K_1 \geq K_2 \geq \dots \geq K_n \geq K$$

s izomorfními odpovídajícími podílovými grupami.

Věta 10.17. *Nechť $H \triangleleft G$ a nechť H i G/H jsou řešitelné grupy. Potom G je řešitelná.*

Důkaz. Nechť $G/H \geq K_1^* \geq K_2^* \geq \dots \geq K_n^* = 1$ je řešitelný řetězec. Použitím korespondenční věty zkonstruujeme podgrupy $G \geq K_1 \geq K_2 \geq \dots \geq K_n \geq H$ 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 . \square

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 $K_1 \cong K$, $H_1 \triangleleft G$ a $K_1 \triangleleft G$, $H_1 \cap K_1 = 1$ a $G = H_1 K_1$. Z první věty o izomorfismu dostaneme $K_1 \cong G/H_1$. Nyní už tvrzení získáme použitím věty 10.19. \square

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. \square

Kapitola 11

Okruhy a obory integrity

11.1 Okruhy

Definice 11.1. *Okruh* $(R; +, \cdot)$ je množina s dvěma operacemi sčítání a násobení, kde $(R; +)$ je aditivní abelovská grupa, $(R; \cdot)$ je pologrupa a platí levý a pravý distributivní zákon: Pro každé tři prvky $a, b, c \in R$

- $a(b + c) = ab + ac$,
- $(b + c)a = ba + ca$.

Je-li (R, \cdot) komutativní pologrupa, potom $(R; +, \cdot)$ je komutativní okruh. Pologrupa (R, \cdot) může a nemusí obsahovat neutrální prvek, který (pokud existuje) nazýváme *jednotkou* okruhu R . Analogicky jako pro přirozená čísla zavedeme v komutativním okruhu R relaci *dělitelnosti*: pro prvky $a, b \in R$ řekneme, že a dělí b , označíme $a|b$ právě tehdy, když existuje $c \in R$ takové, že $b = ac$. Podobně jako pro grupy označíme $na = a + a + \dots + a$ (n sčítanců) a $a^n = a \cdot a \dots a$ (n -tá mocnina). *Dělitelem jednotky* v komutativním okruhu s jednotkou R rozumíme prvek u , který dělí každý prvek R . Množina dělitelů jednotky tvoří vzhledem k operaci násobení grupu.

Příklad 11.2. Následují základní příklady okruhů:

- $(\mathbb{Z}; +, \cdot)$ je komutativní okruh celých čísel s jednotkou, přičemž ± 1 jsou dělitelé jednotky \mathbb{Z} ,
- $(\mathbb{Z}_n; +, \cdot)$ je komutativní okruh s jednotkou, přičemž dělitelé jednotky \mathbb{Z}_n tvoří grupu $U(n)$,
- $(\mathbb{Z}[x]; +, \cdot)$ je komutativní okruh polynomů s koeficienty v \mathbb{Z} , přičemž neutrální prvek na násobení je polynom $f(x) = 1$ a dělitelé jednotky jsou polynomy $f(x) = \pm 1$,

- Matice $M_2(\mathbb{Z})$ typu 2×2 s celočíselnými koeficienty tvoří nekomutativní okruh s jednotkou.
- Okruh $2\mathbb{Z}$ sudých celých čísel je komutativní okruh bez jednotky.
- Spojité reálné funkce reálné proměnné s operacemi $(f + g)(a) = f(a) + g(a)$, $(fg)(a) = f(a)g(a)$, které splňují rovnost $f(1) = 0$ tvoří komutativní okruh bez jednotky.

Přímý součin okruhů: Necht' R_1, R_2, \dots, R_n jsou okruhy.

Potom $R_1 \oplus R_2 \oplus \dots \oplus R_n = \{(a_1, a_2, \dots, a_n); a_i \in R_i\}$ s operacemi

$$(a_1, a_2, \dots, a_n) + (b_1, b_2, \dots, b_n) = (a_1 + b_1, a_2 + b_2, \dots, a_n + b_n),$$

$$(a_1, a_2, \dots, a_n)(b_1, b_2, \dots, b_n) = (a_1 b_1, a_2 b_2, \dots, a_n b_n),$$

je okruh.

Označme $b - c = b + (-c)$. V okruhu platí běžná pravidla počítání. Necht' a, b, c jsou prvky okruhu R . Potom platí:

1. $a0 = 0a = 0$,
2. $a(-b) = (-a)b = -(ab)$,
3. $(-a)(-b) = ab$,
4. $a(b - c) = ab - ac$ a $(b - c)a = ba - ca$.
5. Pokud R je okruh s jednotkou, pak platí $(-1)a = -a$, $(-1)(-1) = 1$.

Podmnožina $S \subseteq R$ okruhu $(R; +, \cdot)$ je *podokruh*, pokud $(S; +, \cdot)$ je okruh.

Lemma 11.3 (Kritérium podokruhu). *Necht' $(R; +, \cdot)$ je okruh. Potom $S \subseteq R$ je podokruh právě tehdy, když pro každé dva prvky $a, b \in S$ platí $a - b \in S$ a $ab \in S$.*

Příklad 11.4. $S = \{0, 2, 4\}$ je podokruh $(\mathbb{Z}_6; +, \cdot)$. Všimněme si, že 1 je jednotka \mathbb{Z}_6 , ale 4 je jednotka $(S; +, \cdot)$.

Příklad 11.5. $n\mathbb{Z} \subset \mathbb{Z}$ je pro každé přirozené číslo n podokruh okruhu celých čísel; Gaussovská celá čísla $\mathbb{Z}[i] = \{a + bi; a, b \in \mathbb{Z}\}$ jsou podokruhem komplexních čísel \mathbb{C} ; diagonální matice typu 2×2 nad okruhem \mathbb{Z} tvoří podokruh okruhu $M_2(\mathbb{Z})$.

Cvičení

11.1. Relace „být podokruh“ je částečným uspořádáním na množině okruhů. Určete Hasseův diagram této relace pro množinu okruhů \mathbb{Z} , \mathbb{Q} , \mathbb{R} , \mathbb{C} , $\mathbb{Z}[i]$, $\mathbb{Z}(\sqrt{2})$.

11.2. Určete maximální prvky uspořádání „být podokruhem“ pro množinu podokruhů \mathbb{Z} .

11.3. Určete grupu dělitelů jednotky pro okruh $\mathbb{Z}[i]$.

11.4. Necht' $R = \mathbb{Z} \oplus \mathbb{Z} \oplus \mathbb{Z}$ a $S = \{(a, b, c); a + b = c\}$. Dokažte, nebo vyvráťte, že S je podokruh R .

11.5. Určete nejmenší podokruh \mathbb{Q} obsahující číslo $\frac{1}{2}$.

11.2 Obory integrity

Okruh byl zavedený jako abstrakce celých čísel. V obecném pohledu to není odpovídající abstrakce, protože kromě přirozených požadavků na komutativitu násobení a existenci jednotky existuje ještě jedna vlastnost celých čísel, kterou okruhy obecně nemusí splňovat. Jedná se o zákon krácení. Tyto úvahy vedou k definici oboru integrity.

Definice 11.6 (Dělitelé nuly). Dělitel nuly je nenulový prvek a komutativního okruhu R , pro nějž existuje nenulový prvek b takový, že $ab = 0$.

Definice 11.7 (Obor integrity). Obor integrity je komutativní okruh s jednotkou bez dělitelů nuly.

V oboru integrity tedy platí: $ab = 0$ implikuje $a = 0$ nebo $b = 0$.

Příklad 11.8. Následující okruhy jsou obory integrity \mathbb{Z} , $\mathbb{Z}[x]$, $\mathbb{Z}[i]$, $\mathbb{Z}[\sqrt{2}]$, \mathbb{Z}_p , p je prvočíslo.

Příklad 11.9. Následující okruhy nejsou obory integrity \mathbb{Z}_n , kde n je číslo složené, $\mathbb{Z} \oplus \mathbb{Z}$, $M_2(\mathbb{Z})$.

Lemma 11.10 (Pravidlo krácení). Necht' a, b, c jsou prvky oboru integrity. Potom $ab = ac$, kde $a \neq 0$, implikuje $b = c$.

Důkaz. Rovnost $ab = ac$ implikuje $ab - ac = 0$. Odtud $a(b - c) = 0$. Protože $a \neq 0$, platí $b - c = 0$. Tedy $b = c$. \square

11.3 Pole

Definice 11.11 (Pole). Pole je komutativní okruh s jednotkou, ve kterém je každý nenulový prvek dělitelem jednotky.

Lemma 11.12. Každé pole F je oborem integrity. Netriviální okruh F je polem právě tehdy, když $(F \setminus \{0\}; \cdot)$ je komutativní grupa.

Příklady polí: \mathbb{Q} , \mathbb{R} , \mathbb{C} . Grupy, okruhy, obory integrity a pole jsou nejdůležitější algebraické struktury.

Věta 11.13. Konečný obor integrity je pole.

Důkaz. Nechť D je konečný obor integrity. Stačí dokázat, že každý nenulový prvek je dělitel jednotky. Ak $a = 1$, potom $1 \cdot 1 = 1$. Nechť $a \neq 1$. Uvažujme posloupnost mocnin $\{a^n\}_{n=1}^{\infty}$. Z konečnosti D vyplývá: existují $i > j$ taková, že $a^i = a^j$. Protože D je obor integrity, zkrácením dostaneme $a^{i-j} = 1$. Jelikož $a \neq 1$, máme $i - j > 1$ a platí

$$a \cdot a^{i-j-1} = a^{i-j} = 1$$

a proto a^{i-j-1} je inverzní prvek k a . □

Důsledek 11.14. *Pro každé prvočíslo p je okruh $(\mathbb{Z}_p; +, \cdot)$ pole.*

Důkaz. Stačí dokázat, že $(\mathbb{Z}_p; +, \cdot)$ nemá dělitele nuly. Nechť $ab = 0$. Potom $p|ab$ a odtud $p|a$ anebo $p|b$. Potom $a = 0 \pmod{p}$ anebo $b = 0 \pmod{p}$. □

11.4 Charakteristika okruhu

Definice 11.15. *Charakteristika okruhu $\text{char } R$ je nejmenší přirozené číslo n takové, že $nx = 0$ pro každý prvek $x \in R$. Pokud takové n neexistuje, položíme $\text{char } R = 0$.*

Zřejmě $\text{char } \mathbb{Z} = 0$, $\text{char } \mathbb{Z}_n = n$ a $\text{char } \mathbb{Z}_2[x] = 2$.

Lemma 11.16. *Má-li okruh R jednotku, potom platí*

- $\text{char } R = n$, je-li n je aditivní řád jednotky,
- $\text{char } R = 0$, má-li jednotka nekonečný řád.

Důkaz. Pro každé číslo n platí

$$n \cdot x = x + x + \dots + x = 1x + 1x + \dots + 1x = (1 + 1 + \dots + 1)x = (n \cdot 1)x$$

Teda $nx = 0$ pro nějaké $x \in R$ právě tehdy, když $n1 = 0$. Z toho plyne, že $\text{char } R = n$ právě tehdy, když n je aditivní řád 1. □

Věta 11.17. *Charakteristika oboru integrity je nula anebo prvočíslo.*

Důkaz. Nechť $n = st$ je řád 1. Potom

$$0 = n \cdot 1 = (st) \cdot 1 = (s \cdot 1)(t \cdot 1).$$

Protože počítáme v oboru integrity, tak $s \cdot 1 = 0$ anebo $t \cdot 1 = 0$. Jelikož n je minimální přirozené číslo s vlastností $n \cdot 1 = 0$, máme $s = n$ anebo $t = n$. Proto je n prvočíslo. □

Příklad 11.18. Uvažujme kořeny polynomu $f(x) = x^2 - 4x + 3 = (x-3)(x-1)$. Pokud $f(x)$ je polynom nad okruhem \mathbb{Z} , potom jsou jeho jediné kořeny 3 a 4. Pokud $f(x) \in \mathbb{Z}_{12}[x]$, pak rozklady $0 = 3 \cdot 4 = 2 \cdot 6$ dávají další kořeny $x = 5, 6, 7, 9$. Je zřejmé, že za nárůstem počtu kořenů stojí fakt, že $(\mathbb{Z}_{12}; +, \cdot)$ není oborem integrity.

Cvičení

11.6. Dokažte, že Gaussovy čísla $\mathbb{Z}_3[i]$ modulo 3 tvoří pole s 9 prvky.

11.7. Dokažte, že $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2}; a, b \in \mathbb{Q}\}$ je pole.

11.5 Ideály a faktorové okruhy

Normální podgrupy mají speciální roli v teorii grup, hlavně proto, že umožňují konstrukci faktorových grup. V teorii okruhů zavedeme analogický pojem speciálních podokruhů, které budeme nazývat ideály.

Definice 11.19. Podokruh A okruhu R nazýváme ideál, když pro každý prvek $r \in R$ a $a \in A$ platí $ra \in A$ a $ar \in A$.

Lemma 11.20 (Kriterium ideálu). *Podmnožina $A \subseteq R$ okruhu R je ideál právě tehdy, když pro každé $a, b \in A$ a $r \in R$ platí $a - b \in A$, $ra \in A$ a $ar \in A$.*

Příklad 11.21. Následující podmnožiny jsou ideály:

- $n\mathbb{Z} \subset \mathbb{Z}$ je ideál.
- Je-li R komutativní okruh s jednotkou, potom se $\langle a \rangle = \{ra; r \in R\} \leq R$ nazývá *hlavní ideál* generovaný $a \in R$. Například, $\langle x \rangle \subset \mathbb{Z}[x]$ je hlavní ideál tvořený polynomy s nulovým konstantním členem.
- Ak R je komutativní okruh s jednotkou, potom $\langle a_1, \dots, a_n \rangle = \{r_1a_1 + r_2a_2 + \dots + r_na_n; r \in R\} \leq R$ se nazývá ideál generovaný $\{a_1, \dots, a_n\} \subseteq R$. Například, $\langle 2, x \rangle \subset \mathbb{Z}[x]$ je ideál tvořený polynomy se sudým konstantním členem.
- Diferencovatelné funkce tvoří podokruh okruhu reálných funkcí reálné proměnné, který není ideálem.

Věta 11.22. *Nechť $A \subset R$ jsou okruhy. Potom množina tříd rozkladu $R/A = \{r + A; r \in R\}$ s operacemi $(s + A) + (t + A) = (s + t) + A$ a $(s + A)(t + A) = st + A$ je okruh právě tehdy, když A je ideál.*

Důkaz. (\Leftarrow) Jelikož $(A; +) \triangleleft (R; +)$ je normální podgrupa, tak je sčítání dobře definované a $(R/A; +)$ je komutativní grupa. Nechť $s' + A = s + A$ a $t' + A = t + A$. Potom existují $a, b \in A$ takové, že $s' = s + a$, $t' = t + b$. Máme $s't' = (s + a)(t + b) = st + at + sb + ab$. Potom

$$(s' + A)(t' + A) = s't' + A = st + at + sb + ab = st + A,$$

nebo $at + sb + ab \in A$.

(\Rightarrow) Nechť $r \in R$ a $a \in A$ jsou takové, že $ra \notin A$ nebo $ar \notin A$. Předpokládejme $ra \notin A$ a nechť násobení je dobře definované. Potom $(a + A)(r + A) = ar + A$, ale $(0 + A)(r + A) = 0 \cdot r + A = A$. Z předpokladů $ar + A \neq A$, proto násobení není dobře definované. \square

Příklad 11.23. Uvažujme okruh $R = \mathbb{Z}[i]/\langle 2 - i \rangle$ Gaussovských čísel faktorizovaný hlavním ideálem $I = \langle 2 - i \rangle$. Jeho prvky mají tvar $a + bi + \langle 2 - i \rangle$. Otázkou je, zda je umíme rozlišit. Z rovnosti $2 - i + \langle 2 - i \rangle = 0 + \langle 2 - i \rangle$ dostáváme, že modulo I platí rovnost $i = 2$. Potom také $-1 = 4$ modulo I , tedy $5 = 0 \pmod{I}$. Použitím rovnice $i \equiv 2$ umíme nalézt celočíselný reprezentant c v každé třídě, tedy každá třída má tvar $c + I$. Použitím vztahu $5 \equiv 0 \pmod{I}$ získáme $c \in \{0, 1, 2, 3, 4\}$, tedy R má nejvýše 5 prvků. Protože $5(1 + I) = I$, tak $1 + I$ má aditivní řád 1 anebo 5. Pokud by byl 1, tak $1 \in I$. Potom $1 = (2 - i)(a + bi) = 2a + b + (2b - a)i$. Tedy $a = 2b$ a $1 = 2a + b$. Odtud, $b = 1/5$, spor. Tedy R je okruh o 5 prvcích. Existuje ale jen jediná abelovská grupa na 5 prvcích a to \mathbb{Z}_5 . Snadno tedy vidíme, že přiřazení $x \mapsto x + I$ je izomorfismus $(\mathbb{Z}_5; +, \cdot) \rightarrow R$.

Příklad 11.24. Uvažujme faktorový okruh $R = \mathbb{R}[x]/\langle x^2 + 1 \rangle$ polynomů s reálnými koeficienty modulo hlavní ideál $I = \langle x^2 + 1 \rangle$. Prvky R jsou tvaru $g(x) + I$. Jelikož $x^2 \equiv -1 \pmod{I}$, můžeme $g(x)$ redukovat na lineární polynom. Asi není žádným překvapením, že R je izomorfní okruhu komplexních čísel.

11.6 Prvočíselné a maximální ideály

Definice 11.25 (Prvočíselný a maximální ideál). *Prvočíselný ideál* A komutativního okruhu R je vlastní ideál, ve kterém pro každé dva prvky $a, b \in R$, $ab \in A$ implikuje $a \in A$ anebo $b \in A$. Vlastní ideál A je maximální, když pro každý ideál B ze vztahu $A \subseteq B \subseteq R$ vyplývá $B = A$ anebo $B = R$.

Příklad 11.26. Ideál $p\mathbb{Z}$ je prvočíselný, neboť $ab = px$ implikuje $p|a$ anebo $p|b$. Tedy $a \in p\mathbb{Z}$ anebo $b \in p\mathbb{Z}$.

Příklad 11.27. Ideál $I = \langle x^2 + 1 \rangle$ je maximální v $\mathbb{R}[x]$. Necht' existuje ideál A , $I \subsetneq A$, a necht' $f(x) \in A \setminus I$. Dokážeme, že $A = \mathbb{R}[x]$. Potom $f(x) = q(x)(x^2 + 1) + r(x)$, $r(x) \neq 0$ a $\deg(r(x)) \leq 1$. Teda $r(x) = ax + b$, pro nějaké $a, b \in \mathbb{R}$. Navíc $r(x) = f(x) - q(x)(x^2 + 1) \in A$. Potom $(ax - b)(ax + b) = a^2x^2 - b^2 \in A$ a současně $a^2(x^2 + 1) = a^2x^2 + a^2 \in A$. Potom $a^2x^2 + a^2 - (a^2x^2 - b^2) = a^2 + b^2 \in A$. Pokud nějaký prvek $c = a^2 + b^2 \neq 0$ je v A , potom $1 \in A$, a tedy i každý polynom z $\mathbb{R}[x]$ je v A .

Věta 11.28. *Necht' R je komutativní okruh s jednotkou a I je ideál R . Potom R/I je obor integrity tehdy a jen tehdy, když I je prvočíselný.*

Důkaz. (\Rightarrow) Necht' R/I je obor integrity a necht' $ab \in I$. Potom $(a + I)(b + I) = ab + I = I$. Potom $a + I = I$ anebo $b + I = I$, tedy $a \in I$ anebo $b \in I$.

(\Leftarrow) Necht' I je prvočíselný. Necht' $(a + I)(b + I) = ab + I = I$. Proto $ab \in I$. Proto $a \in I$ anebo $b \in I$. Tedy aspoň jeden z $a + I$, $b + I$ je nulový prvek v R/I . \square

Věta 11.29. *Necht' R je komutativní okruh s jednotkou a A je ideál R . Potom R/A je pole tehdy a jen tehdy, když A je maximální.*

Důkaz. (\Rightarrow) Nechť R/A je pole, a nechť B je ideál $A \subset B \subseteq R$. Potom existuje $b \in B - A$. Tedy $b + A$ je nenulový prvek R/A . Potom existuje inverzní prvek $c + A$ takový, že $1 + A = (b + A)(c + A) = bc + A$. Potom $1 - bc \in A$, tedy $1 = (1 - bc) + bc \in B$. Potom pro každé $r \in R$, $r = r \cdot 1 \in B$, tedy $B = R$ a A je maximální.

(\Leftarrow) Nechť A je maximální ideál a nechť $b \in R - A$. Potřebujeme dokázat, že $b + A$ má multiplikativní inverzi. Uvažujme ideál $B = \{br + a \mid r \in R, a \in A\}$. Zřejmé $A \subset B$ a z maximality A vyplývá $B = R$. Proto $1 = bc + a'$, pro nějaké $c \in R$ a $a' \in A$. Potom

$$1 + A = bc + a' + A = bc + A = (b + A)(c + A).$$

□

Důsledek 11.30. *Nechť R je komutativní okruh s jednotkou a I je ideál R . Pokud I je maximální, potom I je prvočíselný.*

Příklad 11.31. Ideál $\langle x \rangle$ je prvočíselný ideál v $Z[x]$, ale není maximální, neboť $\langle x \rangle \subset \langle x, 2 \rangle \subset Z[x]$. Je-li $f(x)g(x) \in \langle x \rangle$, pak $f(0)g(0) = 0$. Potom pro aspoň jeden z polynomů máme $f(0) = 0$ anebo $g(0) = 0$. Tedy $\langle x \rangle$ je prvočíselný ideál. Na druhé straně $\langle x, 2 \rangle$ je tvořený polynomy se sudým absolutním členem.

11.7 Homomorfizmy okruhů

Definice 11.32 (Homomorfizmus okruhů). Homomorfizmus $\phi: R \rightarrow S$ je zobrazení splňující pro každé $a, b \in R$ identity $\phi(a + b) = \phi(a) + \phi(b)$, $\phi(ab) = \phi(a)\phi(b)$.

Příklad 11.33. Příklady homomorfizmů:

- $k \mapsto k \pmod{n}$ je epimorfizmus $Z \rightarrow Z_n$,
- $a + bi \mapsto a - bi$ je automorfizmus $C \rightarrow C$,
- $f(x) \mapsto f(1)$ je homomorfizmus $R[x] \rightarrow R$,
- $a \mapsto a^2$, je homomorfizmus $R \rightarrow R$, kde R je komutativní okruh charakteristiky 2.

Věta 11.34 (Vlastnosti homomorfismů okruhů). *Bud' ϕ homomorfizmus okruhu R do okruhu S . Bud' A podokruh R a bud' B ideál S . Pak platí:*

- Pro $r \in R$ a kladné celé n je $\phi(nr) = n\phi(r)$ a $\phi(r^n) = \phi^n(r)$.
- $\phi(A) = \{\phi(a) \mid a \in A\}$ je podokruh S .
- Je-li A ideál a ϕ je na S , pak $\phi(A)$ je ideál.
- $\phi^{-1}(B) = \{r \in R \mid \phi(r) \in B\}$ je ideál R .

- Je-li R komutativní okruh, pak $\phi(R)$ je rovněž komutativní.
- Má-li R jednotku 1 , $S \neq \{0\}$, a ϕ je na, pak $\phi(1)$ je jednotka S a dělitelé jednotky R se zobrazují na dělitele jednotky S .
- ϕ je izomorfismus právě tehdy, když ϕ je na a $\ker \phi = \{r \in R \mid \phi(r) = 0\} = \{0\}$.

Věta 11.35. *Bud' ϕ homomorfismus okruhů z R do S . Pak $\ker \phi = \{r \in R \mid \phi(r) = 0\}$ je ideál R .*

Věta 11.36 (První věta o izomorfismu okruhů). *Bud' ϕ homomorfismus okruhů z R do S . Pak zobrazení z $R/\ker \phi$ do $\phi(R)$ dané předpisem $r + \ker \phi \rightarrow \phi(r)$ je izomorfismus. Symbolicky $R/\ker \phi \cong \phi(R)$.*

Věta 11.37. *Každý ideál okruhu R je jádrem nějakého homomorfismu okruhu R . Speciálně, ideál A je jádrem zobrazení $r \rightarrow r + A$ z R do R/A .*

Věta 11.38. *Bud' R okruh s jednotkou 1 . Zobrazení $\phi: \mathbb{Z} \rightarrow R$ dané $n \rightarrow n \cdot 1$ je homomorfismus okruhů.*

Důkaz. Máme $\phi(m + n) = (m + n) \cdot 1 = m \cdot 1 + n \cdot 1$, tj. ϕ zachovává součet. Podobně $\phi(mn) = (mn) \cdot 1 = (mn) \cdot ((1)(1)) = (m \cdot 1)(n \cdot 1) = \phi(m)\phi(n)$, tj. ϕ zachovává součin. \square

Důsledek 11.39. *Je-li R okruh s jednotkou a charakteristikou $n > 0$, pak R obsahuje podokruh izomorfní \mathbb{Z}_n . Je-li charakteristika R rovna 0 , pak R obsahuje jako podokruh \mathbb{Z} .*

Důkaz. Bud' 1 jednotka v R a bud' $S = \{k \cdot 1 \mid k \in \mathbb{Z}\}$. Z věty 11.38 máme, že zobrazení $\phi: \mathbb{Z} \rightarrow S$ dané $\phi(k) = k \cdot 1$ je homomorfismus a tedy $\mathbb{Z}/\ker \phi \cong S$. Zřejmě ale $\ker \phi = \langle n \rangle$, kde n je aditivního řádu 1 a n je rovněž charakteristika R . Tedy $S \cong \mathbb{Z}/\langle n \rangle \cong \mathbb{Z}_n$. Je-li R charakteristiky 0 , je $S \cong \mathbb{Z}/\langle 0 \rangle \cong \mathbb{Z}$. \square

Příklad 11.40. Bud' $R = \{0, 2, 4, 6, 8\}$ se sčítáním a násobením modulo 10 . Prvek 6 je jednotka R a jelikož $5x = 0$ pro všechna $x \in R$, je $\text{char } R = 5$. Zobrazení $\phi(n) = n \cdot 6 = 6n$ je izomorfismus s $\ker \phi = \langle 5 \rangle$. Proto $R \cong \mathbb{Z}/\langle 5 \rangle \cong \mathbb{Z}_5$ a R je těleso.

Důsledek 11.41. *Pro každé přirozené m je zobrazení $\phi: \mathbb{Z} \rightarrow \mathbb{Z}_m$ dané $x \rightarrow x \bmod m$ je homomorfismem okruhů.*

Důsledek 11.42. *Bud' F pole charakteristiky p , pak F obsahuje podpole izomorfní \mathbb{Z}_p . Je-li F pole charakteristiky 0 , pak F obsahuje podpole izomorfní racionálním číslům.*

Důkaz. První dva fakty jsou zřejmé. Je-li nyní $T = \{ab^{-1} \mid a, b \in S, b \neq 0\}$, je T izomorfní racionálním číslům. \square

Jelikož je průnik všech podpolí pole rovněž podpole, každé pole obsahuje nejmenší podpole. To se nazývá *prvopole* daného pole. Prvopole pole charakteristiky p je izomorfní \mathbb{Z}_p , zatímco pro charakteristiku 0 je izomorfní \mathbb{Q} .

11.8 Podílové pole

Obor integrity \mathbb{Z} není pole, ale je obsažen v poli racionálních čísel. V dalším vyjdeme z myšlenky konstrukce racionálních čísel z celých čísel pomocí jejich podílů.

Věta 11.43. *Bud' D obor integrity. Pak existuje pole F (zvané podílové pole D) obsahující podokruh izomorfní D .*

Důkaz. Bud' $S = \{(a, b) \mid a, b \in D, b \neq 0\}$. Definujme relaci ekvivalence na S $(a, b) \equiv (c, d)$ pokud $ad = bc$. Bud' F množina příslušných tříd ekvivalence S . Třídu ekvivalence obsahující prvek (x, y) označíme x/y . Na F zavedeme sčítání a násobení

$$a/b + c/d = (ad + bc)/(bd), \quad a/b \cdot c/d = (ac)/(bd).$$

(Zde potřebujeme uzavřenost násobení danou oborem integrity, tj. že $bd \neq 0$ pokud $b \neq 0$ a $d \neq 0$.) Snadno se ověří, že takto definované operace jsou dobře definované a nezávisí na volbě reprezentantů tříd. F je zřejmě pole. Bud' 1 jednotka D . Pak $0/1$ je aditivní jednotka F . Aditivní inverze a/b je $-a/b$, multiplikativní inverze nenulového prvku a/b je b/a . Zobrazení $\phi: D \rightarrow F$ dané $x \rightarrow x/1$ je homomorfismus okruhů z D do $\phi(D)$. \square

Je-li F pole, podílové pole pro $F[x]$ označíme $F(x)$.

Příklad 11.44. • Bud' $D = \mathbb{Z}[x]$. Pak podílové pole D je $\{f(x)/g(x) \mid f(x), g(x) \in D, g(x) \text{ není nulový polynom}\}$.

• Bud' p prvočíslo. Pak $\mathbb{Z}_p(x) = \{f(x)/g(x) \mid f(x), g(x) \in \mathbb{Z}_p[x], g(x) \neq 0\}$ je nekonečné pole charakteristiky p .

Cvičení

11.8. Určete podokruh $\mathbb{Z} \oplus \mathbb{Z}$, který není ideál.

11.9. Ukažte, že průnik libovolné množiny ideálů okruhu je opět ideál.

11.10. Bud' A, B ideály okruhu. Ukažte, že pak $AB \subseteq A \cap B$.

11.11. Ukažte, že $I = \{f(x) \in \mathbb{Z}[x] \mid f(1) \text{ je sudé}\}$ je ideál $\mathbb{Z}[x]$.

11.12. Určete řád $\mathbb{Z}[i]/\langle i \rangle$.

11.13. V $\mathbb{Z}_5[x]$ bud' $I = \langle x^2 + x + 2 \rangle$. Určete multiplikativní inverzi $2x + 3 + I$ v $\mathbb{Z}_5[x]/I$.

11.14. Ukažte, že $\mathbb{Z}_3[x]/\langle x^2 + x + 1 \rangle$ není pole.

Kapitola 12

Okruhy polynomů

12.1 Základní vlastnosti

Definice 12.1. Necht R je komutativní okruh. Množina formálních výrazů tvaru

$$R[x] = \{a_n x^n + a_{n-1} x^{n-1} \dots a_1 x + a_0 \mid a_i \in R \text{ pro } 0 \leq i \leq n, a_n \neq 0\}$$

kde n je libovolné přirozené číslo, se nazývá *okruh polynomů na R s proměnnou x* .

Definice 12.2. Říkáme, že polynom $f(x) = a_n x^n + a_{n-1} x^{n-1} \dots a_1 x + a_0$ je stupně n , píšeme $\deg(f(x)) = n$. Koeficient $a_n \neq 0$ budeme nazývat vedoucí koeficient.

Definice 12.3. Dva polynomy $f(x) = \sum_{i \geq 0}^n a_i x^i$ a $g(x) = \sum_{i \geq 0}^m b_i x^i$ se rovnají, pokud $n = m$ a $a_i = b_i$ pro $i = 0, 1, \dots, n$.

Poznámka 12.4. Množinu $R[x]$ a množinu polynomických funkcí $R \rightarrow R$ není možné ztotožnit, neboť jedna polynomická funkce může odpovídat různým polynomům. Například $f(x) = x$ a $g(x) = x^3$ nad \mathbb{Z}_3 definují stejnou funkci. Mohli bychom definovat prvky $R[x]$ jako posloupnosti $\{a_i\}_{i=0}^{\infty}$ s konečným počtem nenulových prvků $a_i \in R$ a celou teorii vybudovat bez použití proměnné x . Z technických důvodů je však užitečnější používat zápis s proměnnou x . Zároveň je možné v případě potřeby doplnit koeficienty na pozicích větších než je stupeň polynomu nulami.

Definice 12.5. Necht $f(x) = \sum_{i \geq 0}^n a_i x^i$ a $g(x) = \sum_{i \geq 0}^m b_i x^i$ jsou dva polynomy nad okruhem R . Potom $h(x) = f(x) + g(x)$ je polynom $\sum_{i \geq 0}^k (a_i + b_i) x^i$, kde $k = \max\{m, n\}$. Součin polynomů je polynom $h(x) = f(x)g(x) = \sum_{k=0}^{m+n} c_k x^k$, kde $c_k = \sum_{i=0}^k a_i b_{k-i}$.

Věta 12.6. *Je-li D obor integrity, potom $D[x]$ je obor integrity.*

Důkaz. Stačí dokázat, že v $D[x]$ neexistují dělitelé nuly. Nechť $h(x) = f(x)g(x) \equiv 0$, kde $n = \deg(f(x))$ a $m = \deg(g(x))$. Potom vedoucí koeficient $a_n b_m$ polynomu $h(x)$ je nulový. Tedy $a_n b_m = 0$. Protože D je obor integrity, máme $a_n = 0$ anebo $b_m = 0$. Odtud $f(x) \equiv 0$ anebo $g(x) \equiv 0$. \square

12.2 Dělení polynomů se zbytkem

Věta 12.7. *Nechť F je pole, $f(x), g(x) \in F[x]$ a $g(x) \neq 0$. Potom existují jednoznačně určené polynomy $q(x), r(x) \in F[x]$ takové, že $f(x) = q(x)g(x) + r(x)$ a $r(x) = 0$ anebo $\deg(r(x)) < \deg(g(x))$.*

Důkaz. Existence. Je-li $f(x) = 0$ anebo $\deg(f(x)) < \deg(g(x))$, potom položíme $q(x) = 0$ a $r(x) = f(x)$.

Nechť $\deg(f(x)) \geq \deg(g(x))$ a nechť $f(x) = \sum_{i=0}^n a_i x^i$ a $g(x) = \sum_{i=0}^m b_i x^i$. Použijeme indukci podle $n = \deg(f(x))$. Příklad $n = 0$ jsme již řešili. Nechť tedy $n > 0$. Utvořme polynom $f_1(x) = f(x) - a_n b_m^{-1} x^{n-m} g(x)$. Zřejmě $f_1(x) = 0$ anebo $\deg(f_1(x)) < \deg(f(x))$. Podle indukčního předpokladu existují polynomy $q_1(x)$ a $r_1(x)$ tak, že $f_1(x) = q_1(x)g(x) + r_1(x)$ a $r_1(x) = 0$ anebo $\deg(r_1(x)) < \deg(g(x))$. Potom

$$f(x) = f_1(x) + a_n b_m^{-1} x^{n-m} g(x) = q_1(x)g(x) + r_1(x) + a_n b_m^{-1} x^{n-m} g(x) = \\ (q_1(x) + a_n b_m^{-1} x^{n-m})g(x) + r_1(x).$$

Položíme-li $q(x) = q_1(x) + a_n b_m^{-1} x^{n-m}$ a $r(x) = r_1(x)$, tak je existence dokázána.

Jednoznačnost. Nechť $f(x) = q(x)g(x) + r(x) = q_1(x)g(x) + r_1(x)$. Můžeme předpokládat $\deg(f(x)) \geq \deg(g(x))$. Potom $0 = (q(x) - q_1(x))g(x) + r(x) - r_1(x)$. Pokud $q(x) \neq q_1(x)$, potom $\deg((q(x) - q_1(x))g(x)) > \deg(r(x) - r_1(x))$. Proto je vedoucí koeficient $q(x) - q_1(x)$ nula, tedy $q(x) - q_1(x) = 0$. Tím i $r(x) - r_1(x) = 0$. \square

Existuje algoritmus na dělení polynomů se zbytkem, který jste se naučili na střední škole.

Definice 12.8. Nechť D je obor integrity a nechť $f(x), g(x) \in D[x]$. Říkáme, že $g(x)$ *dělí polynom* $f(x)$ (píšeme $g(x) \mid f(x)$), pokud existuje polynom $h(x) \in D[x]$ takový, že platí $f(x) = g(x)h(x)$. V takovém případě polynom $g(x)$ nazýváme *dělitel* polynomu $f(x)$.

Nechť $f(x) \neq 0$. Prvek $a \in F$, kde F je pole, nazýváme *kořen polynomu* $f(x) = \sum_{i=0}^n a_i x^i$, platí-li $f(a) = \sum_{i=0}^n a_i a^i = 0$.

Důsledek 12.9. *Nechť F je pole, $a \in F$. Potom $f(x) \in F[x]$ je polynom stupně aspoň 1. Potom $f(a)$ je zbytek po dělení $f(x)$ polynomem $x - a$. Speciálně, a je kořen $f(x)$ právě tehdy, když $(x - a)$ dělí $f(x)$.*

Důkaz. Podle věty 12.7 existují $q(x)$ a $r(x)$ tak, že $f(x) = q(x)(x - a) + r(x)$, přičemž $\deg(r(x)) = 0$. Tedy $r(a) = f(a) - q(a)(a - a) = f(a)$. Jelikož $r(x)$ je konstantní polynom, je $r(x) = f(a)$.

Je-li a je kořen, potom ze vztahu $f(x) = q(x)(x - a) + f(a)$ vyplývá, $(x - a) \mid f(x)$. Naopak, pokud $(x - a) \mid f(x)$, tak zbytek po dělení $f(x)$ polynomem $(x - a)$ je nula. Tedy $f(a) = 0$. \square

Definice 12.10. Kořen a polynomu $f(x) \in F[x]$ má násobnost $k \geq 1$, pokud $(x - a)^k$ dělí $f(x)$, ale $(x - a)^{k+1}$ nedělí $f(x)$. Z technických důvodů v dalším předpokládáme, že polynom $f(x) = 0$ nemá kořeny.

Věta 12.11. Polynom stupně n nad polem má nejvýše n kořenů (při započtení jejich násobností).

Důkaz. Necht' $f(x) \in F[x]$. Je-li $f(x) = 0$, potom $f(x)$ nemá žádný kořen. Dále použijeme indukci. Necht' a je kořen $f(x)$ násobnosti $k \leq n$. Potom $f(x) = (x - a)^k q(x)$. Zřejmě $\deg(q(x)) = n - k < n$. Pokud $f(x)$ nemá jiné kořeny, tak tvrzení platí. Každý kořen $b \neq a$ polynomu $f(x)$, je i kořenem $q(x)$. Podle indukčního předpokladu je těchto kořenů nejvýše $n - k$. Celkem má tedy $f(x)$ nejvýše $k + (n - k) = n$ kořenů. \square

Příklad 12.12. Necht' $f(x) = x^n - 1 \in \mathbb{C}[x]$. Potom z de Moivroy věty vyplývá

$$z_k^n = \cos \frac{2k\pi}{n} + \mathbf{i} \sin \frac{2k\pi}{n} = \cos 2k\pi + \mathbf{i} \sin 2k\pi = 1,$$

pro každé $k \in \mathbb{Z}$. Tedy pro $k = 0, 1, \dots, n - 1$ dostáváme n různých kořenů polynomu $x^n - 1$ v oboru komplexních čísel. Podle věty 12.11 jsme získali všechny kořeny.

Definice 12.13. Okruh hlavních ideálů je obor integrity R , ve kterém je každý ideál hlavní, tj. má tvar $\langle a \rangle = \{ra \mid r \in R\}$.

Věta 12.14. Okruh polynomů nad polem je okruh hlavních ideálů.

Důkaz. Z věty 12.6 vyplývá, že $R[x]$ je obor integrity. Necht' $\{0\} \neq I \neq R[x]$ je ideál, necht' $g(x) \in I$ je nenulový polynom minimálního stupně. Necht' $f(x) \in I$ je libovolný polynom. Potom existují $q(x), r(x) \in R[x]$ tak, že $f(x) = q(x)g(x) + r(x)$, kde $\deg(r(x)) < \deg(g(x))$. Zřejmě $\deg(f(x)) \geq \deg(g(x))$. Z minimality $g(x)$ plyne $r(x) = 0$. Tedy $I = \langle g(x) \rangle$. \square

Z důkazu předchozí věty plyne, že nenulový ideál $I \subset F[x]$ je generovaný libovolným polynomem minimálního stupně.

12.3 Rozklady polynomů

Definice 12.15. Necht' D je obor integrity a $f(x) \in D[x]$, $f(x) \neq 0$, $f(x) \neq 1$. Potom $f(x)$ je *nerozložitelný polynom*, pokud rovnost $f(x) = g(x)h(x)$ implikuje $g(x)$ anebo $h(x)$ je dělitelem jednotky.

Je-li F pole, tak nerozložitelnost $f(x) \in F[x]$ je ekvivalentní podmínce, že $f(x)$ není možné vyjádřit jako součin dvou polynomů menšího stupně.

Příklad 12.16. Polynom $f(x) = 2x^2 + 4$ je nerozložitelný nad \mathbb{Q} , ale rozložitelný nad \mathbb{Z} , $f(x) = 2(x^2 + 2)$. Polynom $x^2 - 2 = (x + \sqrt{2})(x - \sqrt{2})$ je rozložitelný nad \mathbb{R} , ale nerozložitelný nad \mathbb{Q} . Polynom $f(x) = x^2 + 1$ má nad polem \mathbb{Z}_5 rozklad $f(x) = (x + 2)(x + 3)$, ale nad polem \mathbb{Z}_3 je nerozložitelný.

Jak zjišťovat nerozložitelnost polynomu nad oborem integrity D není zřejmé. Pokud D má konečnou charakteristiku, můžeme vyzkoušet všechny možnosti rozkladu daného polynomu stupně n . Pro obory charakteristiky nula je situace komplikovanější. V následujícím uvedeme několik částečných výsledků o rozkladech polynomů.

Věta 12.17. *Nechť F je pole, $f(x) \in F[x]$ je stupně dva nebo tři. Potom $f(x)$ je rozložitelný právě tehdy, když má kořen.*

Definice 12.18. Nechť $f(x) = \sum_{j=0}^n a_j x^j \in \mathbb{Z}[x]$ je nenulový. Označme $\text{cont}(f(x)) = \text{gcd}(a_0, \dots, a_n)$. Polynom $f(x)$ nazveme *primitivní*, pokud $\text{cont}(f(x)) = 1$.

Lemma 12.19 (Gauss). *Součin primitivních polynomů nad \mathbb{Z} je primitivní.*

Věta 12.20. *Nechť $f(x) \in \mathbb{Z}[x]$. Je-li $f(x)$ je rozložitelný nad \mathbb{Q} , potom $f(x)$ je rozložitelný nad \mathbb{Z} .*

Příklad 12.21.

$$f(x) = 6x^2 + x - 2 = \left(3x - \frac{3}{2}\right)\left(2x + \frac{4}{3}\right) = (2x - 1)(3x + 2).$$

Nechť $f(x) \in \mathbb{Z}[x]$ a necht' p je prvočíslo. Označme $\bar{f}(x)$ polynom v $\mathbb{Z}_p[x]$, který vznikne z $f(x)$ redukcí každého koeficientu modulo p .

Věta 12.22 (Kriterium ireducibility mod p). *Nechť $f(x) \in \mathbb{Z}[x]$ a necht' p je prvočíslo. Je-li $\bar{f}(x)$ nerozložitelný nad \mathbb{Z}_p a $\deg(f(x)) = \deg(\bar{f}(x))$, potom $f(x)$ je nerozložitelný nad \mathbb{Q}*

Důkaz. Necht' $f(x)$ je rozložitelný nad \mathbb{Q} . Z věty 12.20 vyplývá, že existují $g(x), h(x) \in \mathbb{Z}[x]$ tak, že $f(x) = g(x)h(x)$. Z předpokladů plyne $\deg(\bar{g}(x)) \leq \deg(g(x)) < \deg(f(x)) = \deg(\bar{f}(x))$ a podobně $\deg(\bar{h}(x)) \leq \deg(h(x)) < \deg(f(x)) = \deg(\bar{f}(x))$. To je ve sporu s nerozložitelností $\bar{f}(x)$. \square

Příklad 12.23. Necht' $f(x) = 21x^3 - 3x^2 + 2x - 9$. Potom jeho redukce modulo 2 je polynom $\bar{f}(x) = x^3 + x^2 + 1$. Polynom $\bar{f}(x)$ nemá kořen v \mathbb{Z}_2 , proto $f(x)$ je nerozložitelný nad \mathbb{Q} .

Věta 12.24 (Eisenstein). *Nechť $f(x) = \sum_{j=0}^n a_j x^j \in \mathbb{Z}[x]$. Necht' existuje prvočíslo p takové, že $p \nmid a_n$, $p \mid a_j$, pro $j = 0, 1, \dots, n-1$, $p^2 \nmid a_0$. Potom $f(x)$ je nerozložitelný nad \mathbb{Q} .*

Důkaz. Necht' $f(x)$ je rozložitelný nad \mathbb{Q} . Z věty 12.20 vyplývá, že existují $g(x), h(x) \in \mathbb{Z}[x]$ tak, že $f(x) = g(x)h(x)$, $1 \leq \deg(g(x)) < n$ a $1 \leq \deg(h(x)) < n$. Necht' $g(x) = \sum_{j=1}^r b_j x^j$, $h(x) = \sum_{j=1}^s c_j x^j$. Protože $p \mid a_0$, $p^2 \nmid a_0$, z

vyjádření $a_0 = b_0 c_0$ plyne, že p dělí právě jedno z čísel b_0, c_0 . Nechť $p \mid b_0$ a $p \nmid c_0$. Protože $p \nmid a_n = b_r c_s$, tak $p \nmid b_r$. Takže existuje nejmenší t takové, že $p \nmid b_t$. Uvažujme

$$a_t = b_t c_0 + b_{t-1} c_1 + \cdots + b_0 c_t.$$

Z předpokladů $p \mid a_t$ a z výběru $t, p \nmid b_i c_{t-i}$ pro $i < t$. Potom $p \mid b_t c_0$, spor. \square

Důsledek 12.25. Pro každé prvočíslo p je polynom

$$\Phi_p(x) = x^{p-1} + x^{p-2} + \cdots + x + 1 = \frac{x^p - 1}{x - 1}$$

ireducibilní nad \mathbb{Q} .

Důkaz. Použitím substituce $x \mapsto x + 1$ a binomické věty dostaneme

$$f(x) = \Phi_p(x + 1) = \frac{(x + 1)^p - 1}{(x + 1) - 1} = \frac{1}{x} \left(-1 + \sum_{j=0}^p \binom{p}{j} x^{p-j} \right) = \sum_{j=0}^{p-1} \binom{p}{j} x^{p-j-1}.$$

Každý koeficient $f(x)$ kromě vedoucího koeficientu je dělitelný p a konstantní člen je $p = \binom{p}{p-1}$, tedy p^2 ho nedělí. Podle Eisensteinova kritéria je $f(x)$ ireducibilní nad \mathbb{Q} . Kdyby existoval rozklad $\Phi_p(x) = g(x)h(x)$ nad \mathbb{Q} , potom $f(x) = \Phi_p(x + 1) = g(x + 1)h(x + 1)$ by byl rozklad $f(x)$. Proto $\Phi_p(x)$ je nerozložitelný. \square

Věta 12.26. Nechť F je pole a $p(x) \in F[x]$. Potom ideál $\langle p(x) \rangle$ je maximální právě tehdy, když $p(x)$ je nerozložitelný.

Důkaz. Nechť $I = \langle p(x) \rangle$ je maximální ideál. Nechť $p(x) = g(x)h(x)$. Zřejmě $\langle p(x) \rangle \subseteq \langle g(x) \rangle \subseteq F[x]$. Z maximality I víme, že platí $\langle g(x) \rangle = I$ anebo $\langle g(x) \rangle = F[x]$. V prvním případě $\deg(p(x)) = \deg(g(x))$ a $h(x)$ je konstanta. Ve druhém případě je $g(x)$ konstantní a $\deg(p(x)) = \deg(h(x))$. V každém z případů není možné $p(x)$ vyjádřit jako součin polynomů menšího stupně.

Nechť je $p(x)$ nerozložitelný a $\langle p(x) \rangle \subset I \subset F[x]$. Z věty 12.14 vyplývá, že $I = \langle g(x) \rangle$ pro nějaký polynom $g(x)$. Proto $p(x) \in \langle g(x) \rangle$, $p(x) = g(x)h(x)$. Protože je $p(x)$ nerozložitelný, tak $\deg(g(x)) = \deg(p(x))$ anebo $g(x)$ je konstantní. V prvním případě $I = \langle p(x) \rangle$, v druhém případě $I = F[x]$. Proto $\langle p(x) \rangle$ je maximální ideál. \square

Důsledek 12.27. Nechť F je pole a $p(x)$ je nerozložitelný. Potom $F[x]/\langle p(x) \rangle$ je pole.

Příklad 12.28. $\mathbb{Z}_3[x]/\langle x^2 + 1 \rangle$ 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 redukuje modulo 3. Při operaci násobení redukuje modulo $x^2 + 1$. Například

$$(2x + 1)(2x + 2) = 4x^2 + 6x + 2 = x^2 + 2 = (x^2 + 1) + 1 = 1.$$

Důsledek 12.29. *Nechť F je pole a nechť $p(x), g(x), h(x) \in F[x]$, přičemž $p(x)$ je nerozložitelný nad F . Je-li $p(x) \mid g(x)h(x)$, potom $p(x) \mid g(x)$ anebo $p(x) \mid h(x)$.*

Důkaz. Protože $p(x)$ je nerozložitelný, tak $F[x]/\langle p(x) \rangle$ je pole a tedy i obor integrity. Z věty 11.28 vyplývá, že $\langle p(x) \rangle$ je prvočíselný. Protože $p(x) \mid g(x)h(x)$, tak $g(x)h(x) \in \langle p(x) \rangle$. Odtud $p(x) \mid g(x)$ anebo $p(x) \mid h(x)$. \square

Příklad 12.30. Konstrukce 8 prvkového pole. Vezmeme $\mathbb{Z}_2[x]/\langle x^3 + x + 1 \rangle$. Dosazováním zjistíme, že $x^3 + x + 1$ je nerozložitelný nad \mathbb{Z}_2 . Prvky pole jsou $0, 1, x, x+1, x^2, x^2+x, x^2+1, x^2+x+1$. Násobení je definované modulo x^3+x+1 . Multiplikativní grupa má 7 prvků a je izomorfní cyklické grupě.

Věta 12.31 (Věta o jednoznačnosti rozkladu). *Každý polynom v $\mathbb{Z}[x]$ různý od nuly a ± 1 je možné jednoznačně rozložit na součin ireducibilních polynomů a to až na permutaci činitelů a přenásobení -1 .*

Důkaz. (Existence.) Nechť $f(x) \in \mathbb{Z}[x]$. Použijeme indukci podle $\deg(f(x))$. Ak $\deg(f(x)) = 0$, potom tvrzení plyne z fundamentální věty aritmetiky.

Nechť $\deg(f(x)) > 0$. Označme $b = \text{cont}(f(x))$ s rozkladem na prvočísla $b = b_1 b_2 \dots b_s$. Potom $f(x) = b_1 b_2 \dots b_s g(x)$, kde $g(x)$ je primitivní polynom stupně > 1 . Je-li $g(x)$ ireducibilní, potom jsme získali rozklad. Nechť $g(x) = h(x)q(x)$ má netriviální rozklad. Z Gaussova lemmatu, $h(x)$ i $q(x)$ jsou primitivní stupně $< \deg(g(x)) = \deg(f(x))$. Z indukčního předpokladu, existují rozklady $h(x)$ a $q(x)$ na ireducibilní polynomy. Proto existuje rozklad $f(x)$ na ireducibilní polynomy.

(Jednoznačnost.) Mějme dva rozklady polynomu $f(x)$.

$$b_1 b_2 \dots b_s p_1(x) \dots p_m(x) = c_1 c_2 \dots c_t q_1(x) \dots q_n(x).$$

Z Gaussova lemmatu $p_1(x) \dots p_m(x)$ a $q_1(x) \dots q_n(x)$ jsou primitivní. Z rovnice $b_1 b_2 \dots b_s = \text{cont}(f(x)) = c_1 c_2 \dots c_t q_1(x)$ vyplývá, že $r = s$ a prvočísla b_i a c_j jsou až na permutaci vyjádření stejná. Protože $p_1(x)$ je ireducibilní, tak existuje i takové, že $p_1(x) \mid q_i(x)$, dle důsledku 12.29. Protože $q_i(x)$ je ireducibilní, tak $q_i(x) = \pm 1 p_1(x)$. Přečíslujeme polynomy $q_j(x)$, $j = 1, \dots, n$ tak, aby $q_i(x) := q_1(x)$. Vydělíme rovnici $p_1(x)$ a opakujeme postup pro rovnici $p_2(x) \dots p_m(x) = q_2(x) \dots q_n(x)$. Takto postupně najdeme bijekci $\psi: \{1, \dots, m\} \rightarrow \{1, \dots, n\}$ splňující $p_i(x) = \pm q_{\psi(i)}$, $i = 1, \dots, m$. \square

12.4 Dělitelnost v oboru integrity

Definice 12.32. Bud' D obor integrity. Prvky $a, b \in D$ nazveme *asociované*, pokud $a = ub$, kde u je dělitel jednotky D . Nenulový prvek a oboru integrity D nazveme *ireducibilní*, pokud a není dělitelem jednotky a pokud pro nějaká $b, c \in D$ platí $a = bc$, pak b nebo c je dělitel jednotky. Nenulový prvek $a \in D$ nazveme *prvočinitel*, pokud a není dělitelem jednotky a $a \mid bc$ implikuje $a \mid b$ nebo $a \mid c$.

Zřejmě $\langle a \rangle$ je prvočinitel, právě když $\langle a \rangle$ je prvoideál. Poznamenejme, že na rozdíl od čísel, jsou obecně pojmy prvočinitele a ireducibilního prvku odlišné.

Věta 12.33. *V oboru integrity je každý prvočinitel ireducibilní.*

Důkaz. Nechť a je prvočinitel v oboru integrity a $a = bc$. Ukážeme, že b nebo c je dělitel jednotky. Z definice prvočinitele $a|b$ nebo $a|c$. Nechť např. $at = b$. Pak $1b = b = at = (bc)t = b(ct)$ a zkrácením $1 = ct$. Tedy c je dělitel jednotky. \square

Věta 12.34. *V hlavním oboru integrity je prvek ireducibilní, právě když je prvočinitel.*

Důkaz. Z věty 12.33 máme, že prvočinitel je ireducibilní. Bud' proto a ireducibilní prvek hlavního oboru integrity D a předpokládejme $a|bc$. Ukážeme, že $a|b$ nebo $a|c$. Uvažme ideál $I = \{ax + by \mid x, y \in D\}$ a bud' $\langle d \rangle = I$. Jelikož $a \in I$, je $a = dr$, a jelikož je a ireducibilní, je d nebo r dělitel jednotky. Je-li d dělitel jednotky, je $I = D$ a můžeme psát $1 = ax + by$. Pak $c = acx + bcy$ a jelikož a dělí oba členy výrazu na pravé straně, $a|c$.

Je-li r dělitel jednotky, pak $\langle a \rangle = \langle d \rangle = I$ a jelikož $b \in I$, existuje prvek $t \in D$ tak, že $at = b$. Proto $a|b$. \square

Příklad 12.35. $\mathbb{Z}[x]$ není hlavní obor integrity. Uvažujme totiž ideál $I = \langle 2, x \rangle$. Ukážeme, že $I(x)$ není tvaru $\langle h(x) \rangle$. Pokud sporem ano, existují $f(x), g(x) \in \mathbb{Z}[x]$ tak, že $2 = h(x)f(x)$ a $x = h(x)g(x)$. Podle počítání stupňů polynomů $0 = \deg 2 = \deg h(x) + \deg f(x)$, takže $h(x)$ je konstantní polynom. Je $2 = h(1)f(1)$, proto $h(1) = \pm 1$ nebo ± 2 . Jelikož $1 \notin I$, $h(x) = \pm 2$. Pak ale $x = \pm 2g(x)$, spor.

12.5 Gaussovy obory integrity

Přirozená čísla větší než 1 se dají jednoznačně rozložit (až na pořadí) na součin prvočísel. Obdobně nenulový nejednotkový polynom lze jednoznačně rozložit na ireducibilní polynomy. V dalším ukážeme, že obecně je rozdíl mezi prvočiniteli a ireducibilními prvky.

Otázka jednoznačného rozkladu v oborech integrity se objevila v souvislosti s Fermatovo větou (Fermat's Last Theorem).

Definice 12.36 (Gaussův obor integrity [Unique Factorization Domain, UFD]).
] Obor integrity D nazveme Gaussův, platí-li že

- každý nenulový prvek D různý od dělitele jednotky lze vyjádřit jako součin ireducibilních prvků D a
- faktorizace na ireducibilní prvky je jednoznačná až na asociovanost prvků a pořadí prvků v rozkladu.

Příklad 12.37. Okruhy \mathbb{Z} a $\mathbb{Z}[x]$ jsou Gaussovy.

Lemma 12.38. *V hlavním oboru integrity je každý ostře rostoucí řetězec ideálů $I_1 \subset I_2 \subset \dots$ konečný.*

Důkaz. Bud' $I_1 \subset I_2 \subset \dots$ uvažovaný řetězec v oboru integrality D a bud' I sjednocení všech ideálů tohoto řetězce. I je ideál (proč?). Jelikož D je hlavní, existuje $a \in D$ tak, že $I = \langle a \rangle$. Jelikož $a \in I$, $I = \bigcup_i I_i$, je a prvkem nějakého I_n . Pro libovolné I_i je $I_i \subseteq I = \langle a \rangle \subseteq I_n$, tj. I_n musí být poslední člen řetězce. \square

Věta 12.39. *Každý hlavní obor integrality je Gaussův.*

Důkaz. Bud' D hlavní obor integrality a bud' a_0 nenulový prvek D , který není dělitelem jednotky. Ukážeme, že a_0 je součin ireducibilních prvků (případně jen s jedním faktorem).

Nejprve ukážeme, že a_0 má alespoň jeden ireducibilní faktor rozkladu. Pokud je a_0 ireducibilní, jsme hotovi. Necht' tedy $a_0 = b_1 a_1$, přičemž ani jedno z b_1 , a_1 není dělitel jednotky a a_1 není nulové. Pokud dále a_1 není ireducibilní, máme $a_1 = b_2 a_2$ a b_2 , a_2 nejsou děliteleé jednotky a a_2 je nenulové. Získáme posloupnost b_1, b_2, \dots prvků v D , které nejsou děliteli jednotky, a posloupnost a_0, a_1, a_2, \dots nenulových prvků D , kde $a_n = b_{n+1} a_{n+1}$ pro každé n . Pak je $\langle a_0 \rangle \subset \langle a_1 \rangle \subset \dots$ ostře rostoucí řetězec ideálů, který dle lemmatu 12.38 je konečný s posledním členem $\langle a_r \rangle$. Tím je a_r hledaný ireducibilní faktor a_0 .

Ukážeme, že rozklad je jednoznačný až na asociovanost prvků rozkladu a jejich pořadí. Necht' pro nějaké $a \in D$ platí

$$a = p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s,$$

kde p_i a q_j jsou ireducibilní (povolujeme opakování). Použijeme indukci podle r . Pro $r = 1$ je a ireducibilní a $s = 1$, $p_1 = q_1$. Předpokládejme, že každý prvek vyjádřitelný jako součin méně než r ireducibilních faktorů má jednoznačný rozklad (až na pořadí a asociovanost). D je hlavní obor integrality, každý ireducibilní faktor p_i ve vyjádření $p_1 p_2 \cdots p_r$ je prvočinitel (věta 12.34). Jelikož p_1 dělí $q_1 q_2 \cdots q_s$, musí p_1 dělit nějaké q_i , necht' $p_1 | q_1$. Pak $q_1 = u p_1$, kde u je dělitel jednotky D . Jelikož

$$u p_1 p_2 \cdots p_r = u q_1 q_2 \cdots q_s = q_1 (u q_2) \cdots q_s \quad \text{a} \quad u p_1 = q_1,$$

krácením získáme

$$p_2 \cdots p_r = (u q_2) \cdots q_s.$$

Z indukčního předpokladu jsou tyto dvě faktorizace identické až na pořadí a asociovanost faktorů. To platí i pro obě faktorizace a . \square

Jelikož je $F[x]$ hlavní obor integrality, máme

Důsledek 12.40. *Bud' F pole. Pak $F[x]$ je Gaussův obor.*

12.6 Eukleidovy obory

Definice 12.41 (Eukleidův obor). Obor integrality D nazveme Eukleidův, pokud existuje funkce (*míra*) zobrazující nenulové prvky D do nezáporných celých čísel tak, že

- $d(a) \leq d(ab)$ pro všechna nenulová $a, b \in D$ a
- pokud $a, b \in D, b \neq 0$, pak existují prvky $q, r \in D$ tak, že $a = bq + r$, kde $r = 0$ anebo $d(r) < d(b)$.

Příklad 12.42. Eukleidovy okruhy jsou

- \mathbb{Z} pro $d(a) = |a|$
- je-li F pole, je $F[x]$ Eukleidův obor pro $d(f(x)) = \deg f(x)$
- okruh Gaussových čísel $\mathbb{Z}[\mathbf{i}] = \{a + b\mathbf{i} \mid a, b \in \mathbb{Z}\}$ je Eukleidův obor pro $d(a + b\mathbf{i}) = a^2 + b^2$.

První podmínka definice plyne z $d(xy) = d(x)d(y)$ a tím $d(x) \leq d(xy)$ (ukážte) pro $x, y \in \mathbb{Z}[\mathbf{i}]$. Druhá podmínka plyne z následujícího. Pro $x, y \in \mathbb{Z}[\mathbf{i}], y \neq 0$ je $x, y \in \mathbb{Q}[\mathbf{i}]$ (ukážte). K vyjádření $xy^{-1} = s + t\mathbf{i}$ zvolme (případně libovolně) $m, n \in \mathbb{Z}$ tak, že m je nejbližší s a n k t (liší se tak nejvýše o $\frac{1}{2}$). Podmínka $x = qy + r$ na dělitelnost je pak splněna pro $q = m + n\mathbf{i}, r = [(s - m) + (t - n)\mathbf{i}]y$. Konečně $d(r) = [(s - m)^2 + (t - n)^2]d(y) \leq \frac{1}{2}d(y) < d(y)$.

Věta 12.43. Každý Eukleidův obor je hlavní obor integrity.

Důkaz. Buď D Eukleidův obor a I jeho nenulový ideál. Buď a nenulový prvek I s minimálním $d(a)$. Pak $I = \langle a \rangle$. Pokud totiž $b \in I$, existují q, r tak, že $b = aq + r$ a $r = 0$ nebo $d(r) < d(a)$. Ale $r = b - aq \in I$, tj. $d(r)$ není menší než $d(a)$. Tedy $r = 0$ a $b \in \langle a \rangle$. Nulový ideál je tedy $\langle 0 \rangle$. \square

Existují hlavní obory integrity, které nejsou Eukleidovy obory.

Důsledek 12.44. Každý Eukleidův obor je Gaussův.

Věta 12.45. Je-li D Gaussův obor, pak $D[x]$ je rovněž Gaussův.

Důkaz je obdobný jako ve speciálním případě $D = \mathbb{Z}$.

Příklad 12.46. Okruh $\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\}$ je obor integrity ale není Gaussův. Pro $d(a + b\sqrt{-5}) = a^2 + 5b^2$ je $d(xy) = d(x)d(y)$ a $d(x) = 1$, právě když x je dělitel jednotky. Tj. dělitelé jednotky jsou ± 1 . Ve faktorizacích $2 \cdot 23 = 46 = (1 + 3\sqrt{-5})(1 - 3\sqrt{-5})$ jsou všechny faktory ireducibilní.

Cvičení

12.1. Ukažte, že sjednocení prvků řetězce $I_1 \subset I_2 \subset \dots$ ideálů okruhu R je ideál R .

12.2. Buď D Eukleidův obor s mírou d . Ukažte, že u je dělitel jednotky, právě když $d(u) = d(1)$.

12.3. Buď D Eukleidův obor s mírou d . Ukažte, že pro asociované prvky a, b je $d(a) = d(b)$.

- 12.4.** Bud' D hlavní obor integrity. Ukažte, že každý vlastní ideál D je obsažený v maximálním ideálu.
- 12.5.** Stanovte dělitele jednotky v $\mathbb{Z}[i]$.
- 12.6.** Ukažte, že $\mathbb{Z}[\sqrt{-6}]$ není Gaussův obor.
- 12.7.** Ukažte, že $\mathbb{Z}[\sqrt{-2}]$, $\mathbb{Z}[\sqrt{2}]$ jsou Gaussovy obory.
- 12.8.** Ukažte, že $\mathbb{Z}[\sqrt{-3}]$ není hlavní obor integrity.

Kapitola 13

Pole

13.1 Rozkladová pole

Definice 13.1. Pole E nazýváme *rozšířením pole* F , pokud $E \supset F$ a operace F jsou zúžením operací na E .

Příklad 13.2. $\mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$.

Věta 13.3 (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 $p(x) \mid f(x)$. Stačí najít rozšíření E , ve kterém má $p(x)$ kořen. Kandidátem je pole $E = F[x]/\langle p(x) \rangle$. Nechť $\Phi: F \rightarrow E$ 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

$$p(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0.$$

Po dosazení dostaneme $p(\alpha) = p(x) + \langle p(x) \rangle = \langle p(x) \rangle = 0$.

□

Příklad 13.4. Nechť $f(x) = x^2 + 1 \in \mathbb{Q}[x]$. Podle důkazu věty 13.3 je $\alpha = x + \langle x^2 + 1 \rangle$ kořen $f(x)$ v rozšíření $E = \mathbb{Q}[x]/\langle x^2 + 1 \rangle$. 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 13.5. Nechť $a_1, a_2, \dots, a_n \in E \supset F$. Označme $F(a_1, a_2, \dots, a_n)$ nejmenší podpole E obsahující F i prvky a_1, a_2, \dots, a_n . Pak $F(a_1, a_2, \dots, a_n)$ je průnikem všech podpolí E obsahujících F a současně $\{a_1, a_2, \dots, a_n\}$.

Definice 13.6. Necht' $E \supseteq F$ 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 $a_1, a_2, \dots, a_n \in E$ takové, že

$$f(x) = a(x - a_1)(x - a_2) \dots (x - a_n).$$

Pole E se nazývá *rozkladové pole* pro $f(x)$, pokud $E = F(a_1, a_2, \dots, a_n)$.

Příklad 13.7. 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 $g(x) = x^2 - 2 \in \mathbb{Q}[x]$ se rozkládá nad \mathbb{R} . Ale rozkladové pole nad \mathbb{Q} je

$$\mathbb{Q}(\sqrt{2}) = \{r + s\sqrt{2}; r, s \in \mathbb{Q}\}.$$

Věta 13.8. 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 $\deg(f(x)) \geq 1$. 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 13.3 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, \dots, a_n polynomu $g(x)$. Proto všechny kořeny $\{a_1, a_2, \dots, a_n\} \subset K$. Potom $F(a_1, \dots, a_n) \subseteq K$. \square

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 13.9. 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 13.10. Necht' $f(x) = x^2 + x + 2 \in \mathbb{Z}_3[x]$. Dosazením $0, 1, 2 \in \mathbb{Z}_3$ 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 $\mathbb{Z}_3(\mathbf{i})$.

Pokud použijeme konstrukci z Kroneckerovy věty, získáme rozkladové pole $E = \mathbb{Z}_3[x]/\langle x^2 + x + 2 \rangle$. Je to 9-prvkové pole charakteristiky 3. Pokud označíme $1 + \langle x^2 + x + 2 \rangle := 1$ a $x + \langle x^2 + x + 2 \rangle := \beta$, 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 13.11 (jednoznačnost elementárního rozšíření). *Nechť $p(x) \in F[x]$ je ireducibilní polynom. Nechť $a \in E \setminus F$ je kořen $p(x)$ v rozšíření E . Potom $F(a) \cong F[x]/\langle p(x) \rangle$.*

Jestliže navíc $\deg(p(x)) = n$, platí

$$F(a) = \{c_{n-1}a^{n-1} + c_{n-2}a^{n-2} + \cdots + c_1a + c_0; c_0, c_1, \dots, c_{n-1} \in F\}.$$

Důkaz. Zobrazení $\Phi: F[x] \rightarrow F(a)$ 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 13.11 vyplývá, že rozšíření $F(a)$ tvoří nad F vektorový prostor dimenze $\deg(p(x))$.

Důsledek 13.12. *Nechť $p(x) \in F[x]$ je ireducibilní polynom stupně n . 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 13.13. *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 13.11 platí $F(a) \cong F[x]/\langle p(x) \rangle \cong F(b)$. Opakovaným použitím vět 13.11 dokážeme jednoznačnost. □

Poznámka: Věta 13.13 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 13.14. 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:

$$a^{1/n}, \omega a^{1/n}, \dots, \omega^{n-1} a^{1/n}.$$

Tyto kořeny se nacházejí v poli $\mathbb{Q}(a^{1/n}, \omega)$, což je zároveň i rozkladovým polem.

Věta 13.15. *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. Nechtě $f(x)$ 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, $(x - a) \mid 1$, což je spor. □

13.2 Konečná pole

Podle Lemy 11.16 a Věty 11.17 platí: charakteristika konečného pole F , zapisujeme $\text{char } F$, je rovna aditivnímu řádu 1, navyše $\text{char } F = p$ je prvočíslo.

Lemma 13.16. *V poli s $\text{char } F = p$ má každý nenulový prvek aditivní řád p .*

Důkaz. Nechtě $x \in F$. Máme

$$\begin{aligned} p \cdot x &= \underbrace{x + x + \dots + x}_{p \text{ sčítanců}} = \underbrace{1 \cdot x + 1 \cdot x + 1 \cdot x + \dots + 1 \cdot x}_{p \text{ sčítanců}} \\ &= \underbrace{(1 + 1 + \dots + 1)}_{p \text{ sčítanců}} \cdot x = (p \cdot 1) \cdot x = 0 \cdot x = 0. \end{aligned}$$

Tedy $|x|$ dělí p . Ale p je prvočíslo, proto $|x| = p$. □

Věta 13.17. *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 13.16 vyplývá $\text{char}(F) = p$ pro nějaké prvočíslo p . Uvažujme aditivní grupu pole $(F; +)$. Z lemmatu 13.16 vyplývá, že řád každého prvku je mocnina p , proto $(F; +)$ je p -grupa. Z důsledku 8.3 vyplývá, že $|(F; +)|$ je mocnina p . □

Z fundamentální věty o abelovských grupách (věta 9.1) vyplývá

Důsledek 13.18. *Aditivní grupa pole charakteristiky p je elementární abelovská p -grupa $(F; +) \cong Z_p^n$.*

Věta 13.19. *Pro každé prvočíslo p a pro každé přirozené číslo existuje, až na izomorfismus, jediné konečné pole řádu p^n .*

Důkaz. (Existence) Uvažujme rozkladové pole E pro polynom $f(x) = x^{p^n} - x \in Z_p[x]$. 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 13.15 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 $|E| = |K| = p^n$.

(Jednoznačnost) 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 13.13 vyplývá $E' \cong E$. \square

Definice 13.20. Konečné pole řádu p^n budeme označovat $\text{GF}(p^n)$.

Věta 13.21 (struktura konečného pole). *Aditivní grupa* $(\text{GF}(p^n), +) \cong Z_p^n$.
Multiplikativní grupa $(\text{GF}(p^n) - \{0\}, \cdot) \cong Z_{p^n-1}$ je cyklická řádu $p^n - 1$.

Důkaz. První část tvrzení je Důsledek 13.18.

Grupa $\text{GF}^*(p^n) = (\text{GF}(p^n) - \{0\}, \cdot)$ je abelovská. Z věty 9.1 vyplývá, že existuje rozklad $\text{GF}^*(p^n)$ na cyklické grupy. Grupa $\text{GF}^*(p^n)$ je cyklická právě tehdy, když řády faktorů rozkladu jsou po dvou nesoudělné. Kvůli sporu předpokládejme, že $\text{GF}^*(p^n)$ není cyklická. Potom v rozkladu existují dvě různé cyklické grupy se společným dělitelem $d > 1$. To znamená, že $\text{GF}^*(p^n)$ obsahuje dvě různé cyklické podgrupy $H \neq K$ řádu d . Potom každý prvek H i K je kořen polynomu $x^d - 1 \in \text{GF}(p^n)[x]$. Potom počet jeho kořenů je aspoň $|H| \cup |K| > d$, dostáváme spor. \square

Cvičení

13.1. Určete svaz podpolí $\text{GF}(64)$.

13.2. Nechť α je kořen $f(x) = x^3 + x^2 + 1 \in Z_2[x]$ v nějakém rozšíření $\text{GF}(2)$. Vypočítejte $1/\alpha$.

13.3. Dokažte, že $\text{GF}^*(32)$, je generovaná každým netriviálním prvkem.

13.4. Dokažte, že $x \mapsto x^p$ je automorfismus $\text{GF}(p^n)$ řádu n .

Kapitola 14

Řešitelnost polynomických rovnic v radikálech

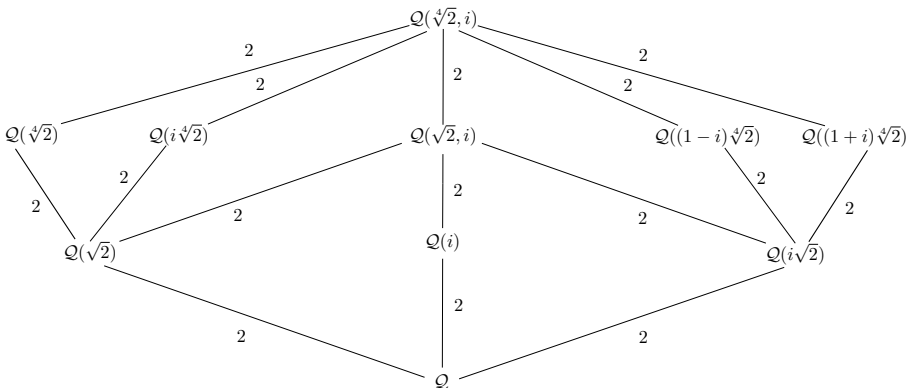
14.1 Řešitelnost Galoisovy grupy polynomu

Definice 14.1. Necht' $E \supset F$ je rozšíření pole F . Automorfismus E je automorfismus okruhu E . Galoisova grupa $\text{Gal}(E/F)$ je podgrupa grupy automorfismů bodově fixující F .

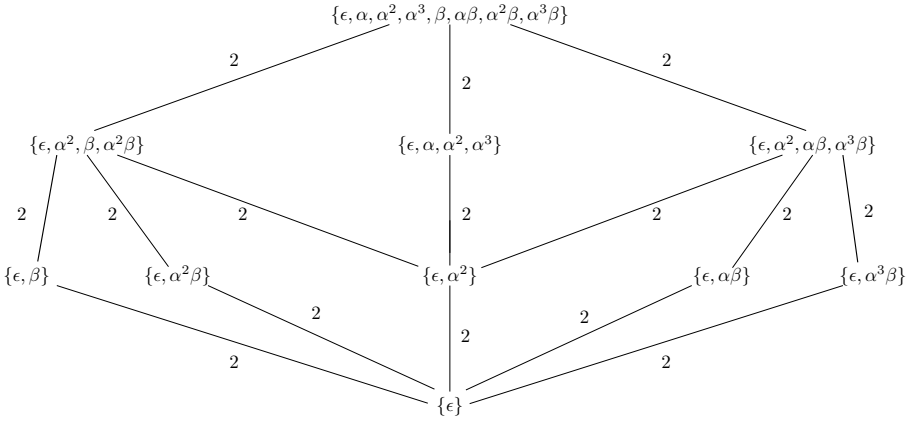
Necht' $H \leq \text{Gal}(E/F)$. Potom $E_H = \{x \in E; \Phi(x) = x \text{ pro každé } \Phi \in H\}$ se nazývá pole fixované H .

Jedna z klíčových myšlenek Galoisovy teorie spočívá v pozorování, že svaz podpolí $\langle F, E \rangle$ a svaz podgrup $\text{Gal}(E/F)$ jsou antiizomorfní.

Příklad 14.2. (Q) Uvažujme $E = \mathbb{Q}(2^{1/4}, i)$. Dá se dokázat, že $\text{Gal}(E/\mathbb{Q})$ je 8-prvková grupa izomorfní grupě kvaternionů. Její generátory jsou $\alpha: i \mapsto i, 2^{1/4} \mapsto -i2^{1/4}; \beta: i \mapsto -i, 2^{1/4} \mapsto 2^{1/4}$. Svaz podpolí vypadá takto:



Svaz podgrup $\text{Gal}(E/\mathbb{Q}) \cong \langle \alpha, \beta \rangle$ vypadá takto:



Příklad 14.3. (Z_2) Necht' $E = \mathbb{Q}\sqrt{2}$. Necht' $\Phi \in \text{Gal}(E/\mathbb{Q})$. Potom

$$2 = \Phi(2) = \Phi(\sqrt{2}\sqrt{2}) = \Phi(\sqrt{2})^2.$$

Proto $\Phi(\sqrt{2}) = \pm\sqrt{2}$. Proto $\text{Gal}(E/\mathbb{Q}) = \langle \beta \rangle \cong Z_2$, kde β je automorfismus $\sqrt{2} \mapsto -\sqrt{2}$.

Příklad 14.4. (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 $\text{Gal}(E/\mathbb{Q})$ je triviální.

Příklad 14.5. (Z_4) Uvažujme rozšíření $E = \mathbb{Q}(\sqrt[4]{2}, \mathbf{i}) \supset \mathbb{Q}$. Jestliže $\Phi \in \text{Gal}(E/\mathbb{Q})$ a zároveň fixuje $\mathbb{Q}(\mathbf{i})$, rovnice

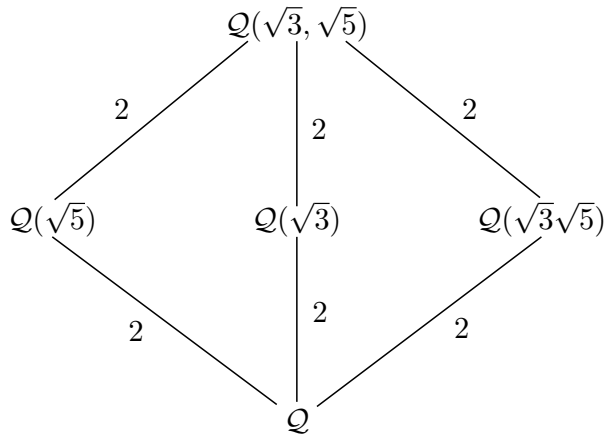
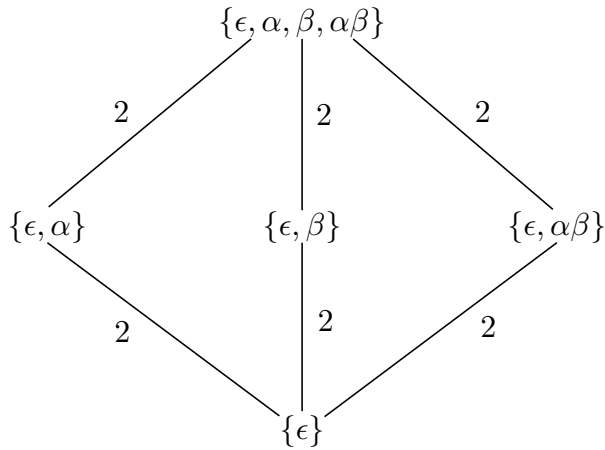
$$2 = \Phi(2) = \Phi(\sqrt[4]{2}\sqrt[4]{2}\sqrt[4]{2}\sqrt[4]{2}) = (\Phi(\sqrt[4]{2}))^4$$

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 $\alpha(\sqrt[4]{2}) = \mathbf{i}\sqrt[4]{2}$, $\alpha \in \text{Gal}(E/\mathbb{Q}(\mathbf{i}))$ má řád 4 a $\text{Gal}(E/\mathbb{Q}(\mathbf{i}))$. Podgrupa $\langle \alpha^2 \rangle \leq \text{Gal}(E/\mathbb{Q}(\mathbf{i}))$ 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 $1 \leq \langle \alpha^2 \rangle \leq \langle \alpha \rangle = \text{Gal}(E/\mathbb{Q}(\mathbf{i}))$.

Příklad 14.6. ($Z_2 \times Z_2$) 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 $\Phi \in \text{Gal}(E/\mathbb{Q})$ je určen obrazy $\Phi(\sqrt{3}) = \pm\sqrt{3}$ a $\Phi(\sqrt{5}) = \pm\sqrt{5}$. Potom $\text{Gal}(E/\mathbb{Q}) \cong Z_2 \times Z_2$. Svazy podpolí a podgrup mají tvar diamantu.

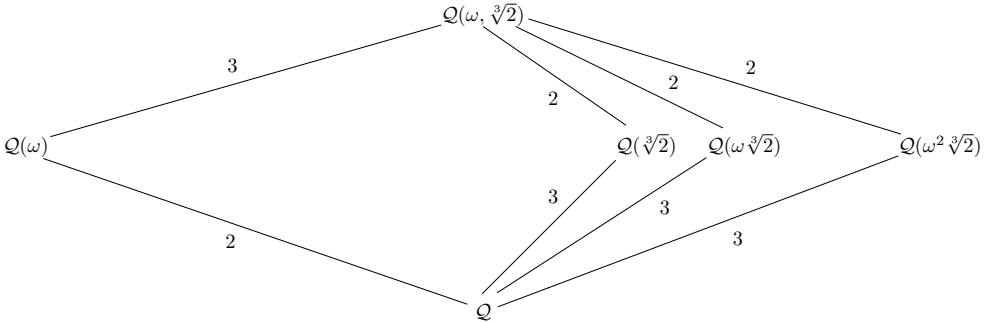
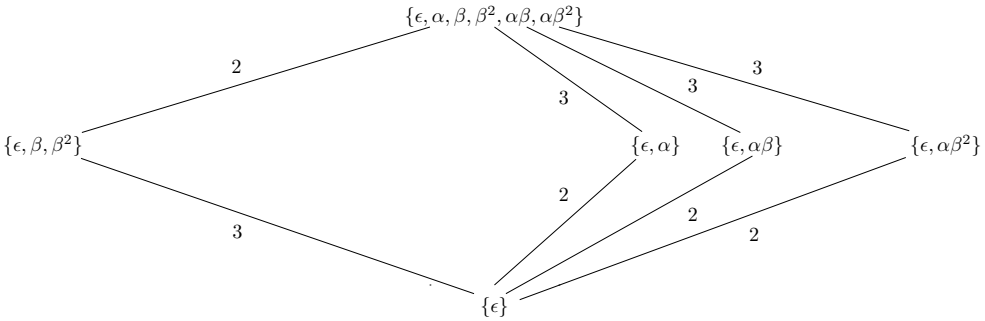


Příklad 14.7. (S_3) Necht $\omega = -1/2 + i\sqrt{3}/2$. Přímým dosazením ověříme, že ω vyhovuje rovnicím $\omega^3 = 1$ a $\omega^2 + \omega + 1 = 0$. Uvažujme rozšíření $E = \mathbb{Q}(\omega, \sqrt[3]{2}) \supset \mathbb{Q}$. Podobně jako v předešlých úlohách automorfismus rozšíření je daný obrazem prvků ω a $\sqrt[3]{2}$. Najdeme dva automorfismy $\alpha \in \text{Gal}(E/\mathbb{Q}(\sqrt[3]{2}))$ a $\alpha \in \text{Gal}(E/\mathbb{Q}(\omega))$. Podgrupa generovaná $\langle \alpha, \beta \rangle \cong S_3$. Ve skutečnosti je to už celá $\text{Gal}(E/\mathbb{Q})$, neboť tyto podpole vygenerují E .

Tabulka 14.1: Automorfismy $\text{Gal}(E/\mathbb{Q})$

| 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:



Nechť $E \subset F$ je rozšíření pole F . Označme $\mathbb{L}[F, E]$ svaz podpolí E obsahujících pole F .

Věta 14.8 (Fundamentální věta Galoisovy teorie). *Nechť F je pole charakteristiky 0 nebo konečné pole. Jestliže E je rozkladové pole nějakého polynomu z $F[x]$, zobrazení $\Theta: \mathbb{L}[F, E] \rightarrow \text{Sub}(\text{Gal}(E/F))$ s předpisem $K \mapsto \text{Gal}(E/K)$ je antiizomorfismus svazů splňující následující vlastnosti:*

- (1) $\dim[E : K] = |\text{Gal}(E/K)|$ a $\dim[K : F] = [\text{Gal}(E/F) : \text{Gal}(E/K)]$.
- (2) Jestliže K je rozkladové pole nějakého polynomu z $F[x]$, platí $\text{Gal}(E/K) \triangleleft \text{Gal}(E/F)$ a $\text{Gal}(K/F) \cong \text{Gal}(E/F) / \text{Gal}(E/K)$.
- (3) $K = E_{\text{Gal}(E/K)}$, pole fixované $\text{Gal}(E/K)$ je K .
- (4) Jestliže $H \leq \text{Gal}(E/F)$, platí $H = \text{Gal}(E/E_H)$. Grupa automorfismů fixující E_H je H .

Příklad 14.9. Necht' $\omega = \cos(2\pi/7) + i\sin(2\pi/7)$. 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 14.8. Automorfismus $\alpha: \omega \mapsto \omega^3$ má řád 6, proto $|\dim(E : \mathbb{Q})| = |\text{Gal}(E/\mathbb{Q})| \geq 6$. 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 $\text{Gal}(E/\mathbb{Q}) = \langle \alpha \rangle$ 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 14.8 potřebujeme nelézt podpole fixované α^2 a α^3 . Pole fixované α^3 je $\mathbb{Q}(\omega + \omega^{-1})$, pole fixované α^2 je $\mathbb{Q}(\omega^3 + \omega^5 + \omega^6)$.

14.2 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 14.10. Necht' F je pole a necht' $f(x) \in F[x]$. Říkáme, že $f(x)$ je řešitelný nad F v radikálech, jestliže se $f(x)$ rozkládá v nějakém rozšíření $F(a_1, \dots, a_n)$ a existují přirozená čísla k_1, \dots, k_n taková, že $a_1^{k_1} \in F$, $a_i^{k_i} \in F(a_1, \dots, a_{i-1})$ pro $i = 2, \dots, n$.

Příklad 14.11. Polynom $f(x) = x^8 - 3 \in \mathbb{Q}[x]$ má kořeny $\sqrt[8]{3}, \sqrt[8]{3}\omega, \sqrt[8]{3}\omega^2, \dots, \sqrt[8]{3}\omega^7$, kde $\omega = \cos(2\pi/8) + i\sin(2\pi/8)$. 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 14.12. Necht' F je pole charakteristiky 0 a necht' E je rozkladové pole pro $f(x) = x^n - a \in F[x]$. Potom $\text{Gal}(E/F)$ je řešitelná grupa.

Důkaz. Necht' b je kořen $f(x) = x^n - a$ a necht' 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 $\text{Gal}(E/F) = 1$. 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 $i = 0, 1, \dots, n - 1$. Proto $E = F(b)$.

Dále pro automorfismus $\Phi \in \text{Gal}(E/F)$ 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 $\Phi_i: b \mapsto b\omega^i$. 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 $\text{Gal}(E/F)$ 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 $\text{Gal}(F(\omega)/F)$ 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 $\text{Gal}(E/F(\omega))$ abelovská. Z věty 14.8(2) vyplývá, že $\text{Gal}(E/F(\omega)) \triangleleft \text{Gal}(E/F)$ a $\text{Gal}(E/F)/\text{Gal}(E/F(\omega)) \cong \text{Gal}(F(\omega)/F)$. Potom řetězec $1 \triangleleft \text{Gal}(E/F(\omega)) \triangleleft \text{Gal}(E/F)$ je řešitelný. \square

Věta 14.13. *Nechť F je charakteristiky 0 a necht' $f(x) \in F[x]$ s rozkladovým polem $E \supset F$. Necht' $f(x)$ se rozkládá v poli $F(a_1, a_2, \dots, a_t)$, a existují celé čísla n_i , takové, že $a^{n_1} \in F$, $a_i^{n_i} \in F(a_1, \dots, a_{i-1})$, pro $i = 2, \dots, t$. Potom $\text{Gal}(E/F)$ je řešitelná grupa.*

Důkaz. Budeme postupovat indukcí podle t .

Necht' $t = 1$. Z předpokladů vyplývá, že existuje n_1 takové, že $a_1^{n_1} = a \in F$. Tedy a_1 je kořen $x^{n_1} - a$. Necht' L je rozkladové pole pro $x^{n_1} - a$. Zřejmě $F \subseteq F(a_1) \subseteq L$. Z Věty 14.8(2) vyplývá, že $\text{Gal}(L/E) \triangleleft \text{Gal}(L/F)$ a $\text{Gal}(L/F)/\text{Gal}(L/E) \cong \text{Gal}(E/F)$. Podle věty 14.12 je $\text{Gal}(L/F)$ řešitelná grupa. Podle věty 10.14 je i $\text{Gal}(L/E)$ řešitelná, podle věty 10.15 je faktorová grupa $\text{Gal}(E/F)$ řešitelná.

Necht' $t > 1$. Necht' L je rozkladové pole $x^{n_1} - a$ nad E a necht' $K \subseteq L$ 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 $K(a_2, \dots, a_t)$. Z indukčního předpokladu je grupa $\text{Gal}(L/K)$ řešitelná. Z věty 14.12 je $\text{Gal}(K/F)$ řešitelná. Z věty 14.8(2) je $\text{Gal}(L/F)/\text{Gal}(L/K) \cong \text{Gal}(K/F)$ řešitelná. Z věty 10.19 je $\text{Gal}(L/F)$ řešitelná. Potom z věty 10.14 je podgrupa $\text{Gal}(L/E) \leq \text{Gal}(L/F)$ řešitelná. Z věty 14.8(2) je $\text{Gal}(L/E) \triangleleft \text{Gal}(L/F)$ a faktorová grupa $\text{Gal}(L/F)/\text{Gal}(L/E) \cong \text{Gal}(E/F)$. Podle věty 10.15 je $\text{Gal}(E/F)$ řešitelná. \square

Poznámka 14.14. Platí i obrácená implikace k větě 14.13: Necht' E je rozkladové pole pro polynom $f(x) \in F[x]$, $\text{char}(F) = 0$. Jestliže $\text{Gal}(E/F)$ je řešitelná, je $f(x) = 0$ řešitelná v radikálech.

Poznámka 14.15. 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} .

14.3 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 14.2: 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 $\pm 1, \pm i$, dostáváme spor. Tedy zbylé dva kořeny a_4, a_5 jsou vzájemně sdružené komplexní čísla $a \pm bi$, $b \neq 0$. 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 13.11). Z věty 14.8(1) máme $5 = \dim[\mathbb{Q}(a_1) : \mathbb{Q}] = |\text{Gal}(\mathbb{Q}(a_1)/\mathbb{Q})|$. Vzhledem k tomu, že $\text{Gal}(\mathbb{Q}(a_1)/\mathbb{Q}) \leq \text{Gal}(K/\mathbb{Q})$, z Lagrangeovy věty 5 dělí $|\text{Gal}(K/\mathbb{Q})|$. Z definice $\text{Gal}(K/\mathbb{Q})$ má akci na množině kořenů a $\text{Gal}(K/\mathbb{Q}) \leq S_5$. Z Cauchyho věty $\text{Gal}(K/\mathbb{Q})$ obsahuje prvek řádu 5. Navíc $\text{Gal}(K/\mathbb{Q})$ obsahuje automorfismus $a_4 = a + bi \mapsto a - bi = a_5$ a fixuje ostatní kořeny. Podgrupa grupy S_5 generovaná transpozicí a cyklem délky 5 se rovná S_5 . Proto $\text{Gal}(K/\mathbb{Q}) \cong S_5$ není řešitelná. Podle věty 14.13 se kořeny $g(x)$ nedají nad \mathbb{Q} vyjádřit v radikálech.

Cvičení

14.1. Určete grupu automorfismů konečného pole $\text{GF}(4)$.

14.2. Nechť E je rozkladové pole polynomu $x^4 + 1 \in \mathbb{Q}[x]$. Určete $\text{Gal}(E/\mathbb{Q})$. Najděte všechny podpole E . Najděte automorfismy v $\text{Gal}(E/\mathbb{Q})$ fixující $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{-2})$, $\mathbb{Q}(i)$.

14.3. Nechť $f(x) \in F[x]$ je polynom stupně n a a_1, a_2, \dots, a_n jsou kořeny. Jestliže $K = \mathbb{Q}(a_1, a_2, \dots, a_n)$, je $\text{Gal}(K/F)$ izomorfní podgrupě S_n .

14.4. Určete Galoisovu grupu polynomu $f(x) = x^2 - 10x + 21$.

