CVIČENÍ K PŘEDNÁŠCE ALGEBRA I

Pavel Růžička

Obsah

Contents

Teorie grup

Cvičení 1
Relace a operace na množině

Binární relace

Definice. *Binární relací* na množině M rozumíme podmnožinu kartézského součinu $M \times M$.

Je-li R binární relace na množině M, budeme často psát aRb místo $(a, b) \in R$.

Definice. Nechť R, S jsou binární relace na množině M. *Součinem* RS relací R a S rozumíme relaci definovanou předpisem

$$aRSb \text{ právě když } \exists\, c \in M : aRc \text{ a zároveň } cSb.$$

Definice. Nechť R je binární relace na množině M. Relací *inverzní* k relaci R rozumíme relaci $R^{\mathbf{T}}$ definovanou předpisem

$$aR^{\mathbf{T}}b \text{ právě když } bRa.$$

Symbolem Δ označme relaci $\{(a, a) \mid a \in M\}$ ('diagonálu kartézského součinu $M \times M$').

Cvičení 1.1. *Nechť R, S a T jsou binární relace na množině M. Dokažte, že platí*

(1) $R(ST) = (RS)T$;
(2) $(ST)^{\mathbf{T}} = T^{\mathbf{T}}S^{\mathbf{T}}$;
(3) *jestliže* $R^{\mathbf{T}} \subseteq R$, *potom* $R^{\mathbf{T}} = R$.

Definice (vlastnosti relací). Nechť R je binární relace na množině M. Řekneme, že relace R je

(a) *reflexivní*, pokud aRa pro všechna $a \in M$;
(b) *tranzitivní*, pokud aRb a bRc implikuje aRc, pro všechna a, b, $c \in M$;
(c) *symetrická*, pokud aRb implikuje bRa, pro všechna a, $b \in M$;
(d) *antisymetrická*, pokud aRb a zároveň bRa implikuje $a = b$, pro všechna a, $b \in M$;
(e) *antireflexivní* právě když $(a, a) \notin R$ pro každé $a \in M$.

Cvičení 1.2. *Dokažte, že relace R je*

(1) *reflexivní právě když* $\Delta \subseteq R$;
(2) *tranzitivní právě když* $RR \subseteq R$;
(3) *symetrická právě když* $R^{\mathbf{T}} \subseteq R$;
(4) *jak podobným způsobem popsat antisymetrickou a antireflexivní relaci?*

Definice. Relace R se nazývá *ekvivalence*, je-li reflexivní, tranzitivní a symetrická.

Neostré uspořádání na množině M je relace, která je reflexivní, tranzitivní a antisymetrická.

Ostré uspořádání na množině M je relace, která je tranzitivní a antireflexivní.

Cvičení 1.3. *Nechť R, S jsou ekvivalence na množině M. Potom je relace RS ekvivalence právě když $RS = SR$. Dokažte!*

Operace na množině

Binární operace na množině M je zobrazení $M \times M \to M$. Obecně můžeme definovat n-ární operaci jako zobrazení

$$\underbrace{M \times \cdots \times M}_{n\times} \to M.$$

Speciálně *unární* operace je zobrazení $M \to M$ a *nulární* operace je předpis, který vybere z množiny M jeden prvek.

Operace obvykle značíme symboly $+$, $\cdot$, $\circ$, $*$, ... Připomeňme, že je zvykem používat *aditivní* značení "$+$" pro komutativní operace a *multiplikativní* značení "$\cdot$" pro obecně nekomutativní operace.

Množina M s jednou binární operací "$\cdot$", což značíme symbolem $(M, \cdot)$, se nazývá *grupoid*. Je-li operace "$\cdot$" *asociativní*, tj. platí-li

$$(a \cdot b) \cdot c = a \cdot (b \cdot c),$$

pro každé a, b, $c \in M$, nazveme dvojici $(M, \cdot)$ *pologrupou*. *Jednotkový prvek* je element $e \in M$ takový, že

$$a \cdot e = a = e \cdot a,$$

pro každé $a \in M$. Pologrupa s jednotkovým prvkem se nazývá *monoid*. V případě, že používáme aditivní značení, nazýváme prvek n s vlastností

$$a + n = a = n + a,$$

nulový prvek.

Cvičení 1.4. *Buď M libovolná množina. Označme*

$$P = \{f \in M^M \mid f \text{ je prosté }\}, \qquad N = \{f \in M^M \mid f \text{ je na }\}.$$

Ukažte, že

(a) *jestliže $f \in P$, potom pro každou dvojici g, h prvků M^M platí $f \circ g = f \circ h \Rightarrow g = h$;*
(b) *jestliže $f \in P$, potom pro každé $g \in M^M$ existuje $h \in M^M$ tak, že $h \circ f = g$;*
(c) *jestliže $f \in N$, potom pro každou dvojici g, h prvků M^M platí $g \circ f = h \circ f \Rightarrow g = h$;*
(d) *jestliže $f \in N$, potom pro každé $g \in M^M$ existuje $h \in M^M$ tak, že $f \circ h = g$.*

Definice. Řekneme, že grupoid $(G, \cdot)$ je

(a) s *pravým krácením* pokud $b \cdot a = c \cdot a \Rightarrow b = c$ pro každé a, b, $c \in G$;
(b) s *pravým dělením* pokud má rovnice $x \cdot a = b$ (s neznámou x), řešení v G pro každé a, $b \in G$;
(c) s *levým krácením* pokud $a \cdot b = a \cdot c \Rightarrow b = c$ pro každé a, b, $c \in G$;
(d) s *levým dělením* pokud má rovnice $a \cdot y = b$ (s neznámou y), řešení v G pro každé a, $b \in G$.

Je-li operace $\cdot$ komutativní, potom pravé a levé krácení, resp. dělení splývají. V tom případě říkáme jen, že grupoid G je *s krácením*, resp. *dělením*.

Množina přirozených čísel s nulou tvoří s operací sčítání komutativní monoid, který je s krácením, ale není s dělením.

Monoid $(P, \circ)$ je s levým krácením (Cvičení 1.4, (i)), ale obecně není s levým dělením, pravým krácením ani pravým dělením (Cvičení 1.4, (ii)). Podobně je monoid $(N, \circ)$ s pravý krácením (Cvičení 1.4, (iii)), ale obecně není s pravým dělením, levým krácením ani levým dělením (Cvičení 1.4, (iv)).

Cvičení 1.5. *Označme P' množinu všech prostých zobrazení $f : \mathbb{N} \to \mathbb{N}$ takových, že množina $\mathbb{N} \setminus f(\mathbb{N})$ je nekonečná. Buď $\circ$ operace skládání zobrazení. Dokažte, že $(P', \circ)$ je pologrupa s pravým dělením, která není s pravým krácením.*

Cvičení 1.6. *Nechť $(G, \cdot)$ je pologrupa s pravým i levým krácením a dělením. Potom v G existuje jednotkový prvek a ke každému prvku pologrupy G existuje prvek inverzní. Dokažte!*

Definice. Pologrupa s pravým i levým krácením a dělením se nazývá *grupa*.

Cvičení 1.7. *Nechť $(G, \cdot)$ je pologrupa ve které existuje prvek e tak, že pro všechna $a \in G$ platí*

$$a \cdot e = a$$

a ke každému $a \in G$ existuje $a^P \in G$ tak, že

$$a \cdot a^P = e.$$

Potom je $(G, \cdot)$ grupa. Dokažte!

Cvičení 1.8. *Konečná pologrupa $(G, \cdot)$ je s pravým krácením právě když je s pravým dělením. Dokažte!*

Poznámka. Podpologrupa pologrupy s pravým (levým) krácením je opět pologrupa s pravým (levým) krácením. Naproti tomu podpologrupa pologrupy s pravým (levým) dělením nemusí být pologrupou s pravým (levým) dělením (například přirozená čísla, obsažená v aditivní grupě celých čísel, jsou s krácením, ale ne s dělením). Obecně tedy podpologrupa grupy nemusí být grupou. Vzhledem k Cvičení 1.8 však platí:

Cvičení 1.9. *Konečná podpologrupa grupy G je její podgrupou. Dokažte!*

Cvičení 2
Homomorfismy grup a symetrické grupy

Definice. Nechť $(G, \cdot)$ a $(H, *)$ jsou grupy. Zobrazení $f : G \to H$ je *homomorfismus* těchto grup jestliže platí

$$f(ab) = f(a) * f(b)$$

pro každé a, $b \in G$. *Vnoření* je homomorfismus, který je prostý. Homomorfismus, který je prostý a na nazvame *izomorfismem*. Existuje-li izomorfismus z grupy G do grupy H, řekneme, že jsou grupy G a H izomorfní.

Cvičení 2.1. *Nechť $f : G \to H$ je homomorfismus grup. Dokažte, že*

(i) $f(1_G) = 1_H$ *(1_G, resp. 1_H značí jednotkový prvek grupy G, resp. H).*
(ii) $f(a^{-1}) = f(a)^{-1}$ *pro každé $a \in G$.*
(iii) $f(a^z) = f(a)^z$ *pro každé $a \in G$ a $z \in \mathbb{Z}$.*

Cvičení 2.2. *Uvažme množinu $\mathcal{P}(M)$ všech podmnožin množiny M. Na množině $\mathcal{P}(M)$ definujme operaci Δ předpisem*

$$A \Delta B = (A \setminus B) \cup (B \setminus A) = (A \cup B) \setminus (A \cap B),$$

kde A, B jsou podmnožiny M. Ověřte, že $(\mathcal{P}(M), \Delta)$ je grupa. Jak vypadá jednotkový prvek této grupy? Jak vypadá inverzní prvek k $A \in \mathcal{P}(M)$?

Symetrická grupa

Symbolem S_n označíme grupu všech permutací množiny $\{1, \ldots, n\}$ s operací skládání. Tuto grupu nazýváme *symetrická grupa* řádu n. Snadno nahlédneme, že grupa S_n má $n!$ prvků, a že pro $n \geq 3$ není grupa S_n komutativní.

Připomeňme, že každou permutaci můžeme rozložit v součin nezávislých cyklů. Tak například rozklad v součin nezávislých cyklů permutace π šestiprvkové množiny definované po prvcích takto:

$$\pi(1) = 4,\ \pi(2) = 6,\ \pi(3) = 1,\ \pi(4) = 3,\ \pi(5) = 5,\ \pi(6) = 2$$

je $\pi = (1, 4, 3)(2, 6)$. Cykly délky 1 odpovídající pevným bodům permutace π v zápisu pro jednoduchost vynecháváme. Permutaci π můžeme znázornit také tabulkou:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 6 & 1 & 3 & 5 & 2 \end{pmatrix}.$$

Nyní popíšeme multiplikativní tabulku grupy S_3. Grupa S_3 má šest prvků. Jsou to identická permutace, která je jednotkovým prvkem a kterou budeme značit i, tři transpozice $(1, 2)$, $(1, 3)$ a $(2, 3)$ a dva trojcykly $(1, 2, 3)$ a $(1, 3, 2)$. Multiplikativní tabulka grupy S_3 vypadá takto:

$$\begin{array}{cccccc} i & (1,2) & (1,3) & (2,3) & (1,2,3) & (1,3,2) \\ (1,2) & i & (1,3,2) & (1,2,3) & (2,3) & (1,3) \\ (1,3) & (1,2,3) & i & (1,3,2) & (1,2) & (2,3) \\ (2,3) & (1,3,2) & (1,2,3) & i & (1,3) & (1,2) \\ (1,2,3) & (1,3) & (2,3) & (1,2) & (1,3,2) & i \\ (1,3,2) & (2,3) & (1,2) & (1,3) & i & (1,2,3) \end{array}.$$

Všiměme si, že v každém sloupci, resp. každém řádku této tabulky se vyskytuje každý prvek grupy S_3 právě jednou. To odpovídá pravému, resp. levému krácení a dělení (v konečném případě stačí jen jedna z těchto vlastností, v nekonečném odpovídá pravé krácení tomu, že se každý prvek vyskytuje v každém sloupci nejvýše jednou a pravé dělení odpovídá tomu, že se tam vyskytuje alespoň jednou).

Cvičení 2.3. *Nechť $(G, *)$ je grupa a nechť $a \in G$.*

(i) *Dokažte, že pro každé $a \in G$ jsou funkce $L_a : G \to G$, resp. $R_a : G \to G$ definované předpisy $x \mapsto a * x$, resp. $x \mapsto x * a^{-1}$ bijekce.*
(ii) *Dokažte, že pro každé $a, b \in G$ platí $L_{a*b} = L_a \circ L_b$ a $R_{a*b} = R_a \circ R_b$.*
(iii) *Z předchozího odvoďte, že každou n-prvkovou grupu je možné vnořit do grupy S_n.*

Permutace je sudá právě když se dá vyjádřit jako součin sudého počtu transpozic a lichá v opačném případě. Pro každou permutaci $\pi \in S_n$ definujme

$$\operatorname{sgn}(\pi) = \begin{cases} 0 & : \pi \text{ je sudá.} \\ 1 & : \pi \text{ je lichá.} \end{cases}$$

Protože platí $\operatorname{sgn}(\pi\sigma) = \operatorname{sgn}(\pi) + \operatorname{sgn}(\sigma)$ pro každou dvojici permutací z množiny S_n, je zobrazení sgn homomorfismus z grupy S_n na grupu $\mathbb{Z}_2$. Jádrem tohoto homomorfismu je *alternující* grupa A_n všech sudých permutací množiny $\{1, \ldots, n\}$.

Cvičení 2.4. *Spočtěte znaménko permutace α zapsané tabulkou*

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

Cvičení 2.5. *Dokažte, že permutace π je sudá právě když je součinem trojcyklů.*

Cvičení 2.6. *Nechť n je přirozené číslo.*

(1) *Dokažte, že transpozice $(1,2)$, $(2,3)$, $\ldots$, $(n-1,n)$ generují grupu S_n.*
(2) *Dokažte, že transpozice $(1,2)$, $(1,3)$, $\ldots$, $(1,n)$ generují grupu S_n.*
(3) *Dokažte, že cykly $(1,\ldots,n-1)$, $(n-1,n)$ generují grupu S_n.*
(4) *Dokažte, že grupa S_n je generovaná dvojicí cyklů $(1,2)$ a $(1,2,\ldots,n)$.*
(5) *Dokažte, že grupa S_4 není generovaná cykly $(1,3)$ a $(1,2,3,4)$.*
(6) *Dokažte, že prvky $(1,2,3)$, $(1,2,4)$, $\ldots$, $(1,2,n)$ generují grupu A_n pro každé $n \geq 3$.*

Cvičení 3
Cyklické grupy

Definice. Nechť a je prvek grupy G. Jsou-li všechny mocniny prvku a různé, řekneme, že a má nekonečný řád a píšeme $\mathbf{o}(a) = \infty$. V opačném případě řekneme, že prvek a má konečný řád. v tomto případě existují celá čísla $k > l$ tak, že

$$a^k = a^l.$$

Odtud plyne, že $a^{k-l} = 1$. To znamená, že existují mocniny prvku a s přirozenými exponenty, které jsou rovny jednotkovému prvku. Nejmenší takové přirozené číslo n je řádem prvku a. Píšeme $\mathbf{o}(a) = n$.

Cvičení 3.1. *Nechť a, b jsou prvky grupy G takové, že $ab = ba$. Potom je řád prvku ab dělitelem nejmenšího společného násobku řádů prvků a a b. Navíc jsou-li řády $\mathbf{o}(a)$, $\mathbf{o}(b)$ nesoudělné, platí $\mathbf{o}(ab) = \mathbf{o}(a)\mathbf{o}(b)$. Dokažte!*

Nyní toto jednoduché pozorování: Je-li G grupa a $\mathcal{A}$ libovolná množina podgrup grupy G, potom je $\bigcap \mathcal{A}$ podgrupou grupy G. Proto můžeme definovat pro každou podmnožinu X grupy G podgrupu $\langle X \rangle$ grupy G *generovanou množinou* X jako průnik všech podgrup grupy G, které množinu X obsahují. Tj.

$$\langle X \rangle = \{H \mid H \leq G \ \& \ X \subseteq H\}.$$

Je-li množina X jednoprvková obsahující prvek a, budeme psát $\langle a \rangle$ místo $\langle \{a\} \rangle$. Grupa G je **cyklická**, jestliže exituje prvek $a \in G$ takový, že $\langle a \rangle = G$. Rozmyslete si, že cyklická grupa generovaná prvkem a se skládá právě z celočíselných mocnin prvku a.

Pro přirozené číslo n a celé číslo z označme $z \mod n$ zbytek čísla z po dělení číslem n. Množina $\{0, 1, \ldots, n-1\}$ na které je definovaná operace $+_n$ předpisem

$$a +_n b = a + b \mod n$$

je grupou, kterou označíme symbolem $\mathbb{Z}_n$.

Cvičení 3.2. *Ukažte, že všechny podgrupu grupy $(\mathbb{Z}, +)$ celých čísel jsou tvaru $n\mathbb{Z} = \{nz \mid z \in \mathbb{Z}\}$, kde n je nezáporné celé číslo. Dále ukažte, že $\mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}_n$.*

Tvrzení 3.1. *Buď a prvek grupy G konečného řádu n. Potom je $a^z = 1$ právě když $n \mid z$, pro každé celé číslo z.*

Důkaz. Pokud n dělí z, existuje celé číslo y tak, že $ny = z$. Odtud dostáváme $a^z = a^{ny} = (a^n)^y = 1^y = 1$.

Nyní naopak předpokládejme, že $a^z = 1$. Po vydělení čísla z číslem n se zbytkem dostaneme $z = ny + r$, kde $0 \leq r < n$. Podle našeho předpokladu platí

$$1 = a^z = a^{ny+r} = a^{ny}a^r = a^r.$$

Protože n je nejmenší přirozené číslo takové, že $a^n = 1$, je nutně $r = 0$ a tedy $n \mid z$. $\square$

Důsledek 3.2. *Buď a prvek grupy G konečného řádu n. Potom pro celá čísla y, z platí $a^y = a^z$ právě když $y \equiv z \pmod{n}$.*

Důkaz. Podle Tvrzení 3.1 je $a^{y-z} = 1$ právě když $n \mid (y - z)$. Rovnost $a^{y-z} = 1$ je ekvivalentní tomu, že $a^y = a^z$ a $n \mid (y - z)$ právě když je $y \equiv z \pmod{n}$. □

Buď a prvek grupy G. Definujme zobrazení $\varphi_a : \mathbb{Z} \to G$ předpisem $\varphi(z) = a^z$. Obrazem zobrazení φ_a je množina všech celočíselných mocnin prvku a, která je právě cyklickou podgrupou generovanou prvkem a. Je-li prvek a nekonečného řádu, je zobrazení φ_a prosté a grupa $\langle a \rangle$ je izomorfní $\mathbb{Z}$. Je-li řád prvku a konečný, roven n, je podle Tvrzení 3.1 jádrem homomorfismu φ_a množina $n\mathbb{Z}$. Odtud a z Cvičení 3.2 plyne, že cyklická grupa generovaná prvkem nekonečného řádu je izomorfní grupě celých čísel a cyklická grupa generovaná prvkem konečného řádu n je izomorfní grupě $\mathbb{Z}_n$.

Cvičení 3.3. *Buď n přirozené číslo. Dokažte, že všechny podgrupy grupy $\mathbb{Z}_n$ jsou tvaru $m\mathbb{Z}_n = \{mk \mod n \mid k \in \mathbb{Z}_n\}$, kde m je nějaký celočíselný dělitel prvku n, a že platí*

$$\mathbb{Z}_n/m\mathbb{Z}_n \simeq \mathbb{Z}_m \qquad a \qquad m\mathbb{Z}_n \simeq \mathbb{Z}_{n/m}.$$

Z Cvičení 3.2 a 3.3 odvoďte tato tvrzení:

Tvrzení 3.3. *Každá podgrupa a každá faktorová grupa cyklické grupy je opět cyklická grupa.*

Tvrzení 3.4. *Pro každý dělitel m čísla n existuje právě jedna m prvková podgrupa n prvkové cyklické grupy. Jiné podgrupy n prvkové cyklické grupy neexistují.*

Cvičení 3.4. *Dokažte, že grupa $\mathbb{Z}_n \times \mathbb{Z}_m$ je cyklická právě když jsou čísla m, n nesoudělná. (Návod: Použijte Cvičení 3.1.)*

Cvičení 4
Eulerova funkce

Symbolem $\mathrm{NSD}(n, m)$ označíme největší společný dělitel přirozených čísel m, n.

Definice. *Eulerova funkce* φ je definována takto:

(i) $\varphi(1) = 1$;
(ii) Je-li $n > 1$, je

$$\varphi(n) = |\{k \mid 1 \leq k < n \ \ \& \ \ \mathrm{NSD}(k, n) = 1\}|,$$

tj. $\varphi(n)$ je rovno počtu čísel menších než n, které jsou s číslem n nesoudělné.

Lemma 4.1. *Nechť m, n je dvojice přirozených čísel a $d = \mathrm{NSD}(n, m)$ je jejich největší společný dělitel. Potom existují celá čísla u, v tak, že $nu + mv = d$.*

Důkaz. Lemma ukážeme indukcí podle velikosti součtu $m+n$. Je-li $n = m$, položíme $u = 1$, $v = 0$. Předpokládejme, že $n > m$ a že pro každou dvojici přirozených čísel n', m' takovou, že $n' + m' < n + m$ tvrzení platí. Potom vzhledem k tomu, že $d = \mathrm{NSD}(n - m, m)$, existují celá čísla u, v' tak, že $d = u(n - m) + v'm$. Položme $v = v' - u$. □

Tvrzení 4.2. *Nechť C_a je cyklická grupa generovaná prvkem a konečného řádu n. Potom přirozená mocnina a^k generuje grupu C_a právě když jsou čísla n, k nesoudělná.*

Důkaz. Nejprve předpokládejme, že je prvek a^k generátorem grupy C_a. Potom existuje přirozené číslo u takové, že

$$(a^k)^u = a,$$

odkud plyne, že $ku - 1 = nv$, pro některé celé číslo v. Proto $1 = ku + nv$, odkud plyne, že jsou čísla k, n nesoudělná.

Nyní předpokládejme, že jsou čísla k, n nesoudělná. Potom podle Lemmatu 4.1 existují celá čísla u, v tak, že

$$1 = ku + nv.$$

Potom

$$a = a^{ku+nv} = (a^k)^u (a^n)^v = (a^k)^u,$$

odkud plyne, že prvek a^k generuje grupu C_a. □

Tvrzení 4.3. *Počet různých generátorů n-prvkové cyklické grupy je $\varphi(n)$.*

Cvičení 4.1. *Dokažte, že jsou-li m, n nesoudělná přirozená čísla, potom platí*

$$\varphi(mn) = \varphi(m)\varphi(n).$$

Cvičení 4.2. *Dokažte, že je-li p prvočíslo, potom platí*

$$\varphi(p^k) = p^k - p^{k-1}$$

pro každé $k \in \mathbb{N}$.

Cvičení 4.3. *Dokažte, že pro* $m = p_1^{k_1} \dots p_n^{k_n}$ *platí*

$$\varphi(m) = m\left(1 - \frac{1}{p_1}\right)\dots\left(1 - \frac{1}{p_n}\right).$$

Označme symbolem $\mathbb{Z}_n^*$ množinu všech generátorů cyklické grupy $\mathbb{Z}_n$. Snadno ověříme, že tato množina s operací $\cdot_n$ definovanou předpisem

$$k \cdot_n m = km \mod n$$

pro každé k, $m \in \mathbb{Z}_n^*$ tvoří grupu. Toto pozorování spolu s Tvrzením 4.3 má několik zajímavých důsledků.

Tvrzení 4.4 (Eulerova věta). *Je-li* a *číslo nesoudělné s přirozeným číslem* n*, potom je*

$$a^{\varphi(n)} \equiv 1 \pmod{n}.$$

Důkaz. Grupa $\mathbb{Z}_n^*$ má $\varphi(n)$ prvků. Proto je řád prvku $a \mod n$ dělitelem čísla $\varphi(n)$. Odtud plyne dokazované tvrzení. □

Důsledek 4.5 (Fermatova věta). *Nechť* p *je prvočíslo které nedělí celé číslo* a*. Potom*

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

Cvičení 4.4 (Wilsonova věta). *Nechť* p *je přirozené číslo. Potom je*

$$p \mid (p-1)! + 1$$

právě když je p *prvočíslo. Dokažte!*

Tvrzení 4.6. *Pro každé přirozené číslo* n *je*

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

kde sčítáme přes všechna přirozená čísla, které dělí číslo n*.*

Důkaz. Nechť G je libovolná grupa. Pro cyklickou podgrupu C grupy G označme symbolem C^* množinu všech jejích generátorů. Uvědomte si, že platí

$$G = \bigcup C^*,$$

kde sjednocení bereme přes všechny cyklické podgrupy grupy G (každý prvek grupy G je generátorem právě jedné její cyklické podgrupy).

Pro každý přirozený dělitel d přirozeného čísla n existuje právě jedna d prvková cyklická podgrupa C_d grupy $\mathbb{Z}_n$. Proto platí

$$\mathbb{Z}_n = \bigcup_{d|n} C_d^*.$$

Protože $\varphi(d) = |C_d^*|$ pro každý dělitel d čísla n, je

$$n = |\mathbb{Z}_n| = \sum_{d|n} \varphi(d).$$

□

Cvičení 5
Normální podgrupy a rozkladové třídy

Rozkladové třídy podle podgrupy

Nechť G je pologrupa a S, T jsou její podmnožiny. Součin podmnožin S, T je množina

$$ST = \{st \mid s \in S,\ t \in T\}.$$

Snadno ověříme, že takto definované násobení je asociativní. V případě, že je množina S jednoprvková, $S = \{s\}$, píšeme sT místo $\{s\}T$. Podobně budeme psát St místo $S\{t\}$, pokud je $T = \{t\}$.

Cvičení 5.1. *Nechť G je konečná grupa a S, T jsou neprázdné podmnožiny G. Dokažte, že jestliže $|S| + |T| > |G|$, potom $ST = G$. (Definujeme $ST = \{st \mid s \in S,\ t \in T\}$.)*

Dokažte, že každý prvek konečného tělesa je součtem dvou čtverců.

Definice. Nechť H je podgrupa grupy G a nechť $g \in G$. Levou, resp. pravou, *rozkladovou třídou* podle podgrupy H určenou prvkem g rozumíme množinu gH, resp. Hg.

Cvičení 5.2. *Dokažte, že*

(a) *je-li H podmnožina grupy G taková, že $hH = H$ pro každé $h \in H$, potom je H podgrupa grupy G;*
(b) *je-li H podgrupa grupy G, potom je $hH = H$ právě když $h \in H$;*
(c) *je-li H podgrupa grupy G, potom pro každou dvojici prvků g, k z grupy G platí $gH = kH$ právě když $k^{-1}g \in H$.*

Cvičení 5.3. *Dokažte, že podmnožina H grupy G je její podgrupou právě když $HH = H$.*

Tvrzení 5.1. *Každá levá (pravá) rozkladová třída podle podgrupy H je určena libovolným ze svých prvků, tj. $g \in kH$ právě když $gH = kH$ ($g \in Hk$ právě když $Hg = Hk$), pro každou dvojici prvků g, k z grupy G.*

Důkaz. Tvrzení ukážeme pro levé rozkladové třídy. Nechť g, $k \in G$. Potom $g \in kH$ právě když $k^{-1}g \in H$. Podle Cvičení 5.2, (c), to nastane právě tehdy když $gH = kH$. □

Důsledek 5.2. *Levé (pravé) rozkladové třídy grupy G podle její podgrupy H tvoří rozklad grupy G.*

Buď G konečná grupa. Označme symbolem $[G : H]$ počet levých rozkladových tříd podle podgrupy H grupy G. Protože jsou všechny levé rozkladové třídy podle H stejně velké a počet jejich prvků je roven počtu prvků podgrupy H, dostáváme rovnost

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

Ukázali jsme tak Lagrangeovu větu, že počet prvků libovolé podgrupy konečné grupy G dělí počet prvků G.

Definice. Podgrupa H grupy G se nazývá *normální* (značíme $H \triangleleft G$), jestliže $gHg^{-1} = H$, pro každé $g \in G$.

Z asociativity násobení podmnožin grupy G plyne, že $gHg^{-1} = H$ právě když $gH = Hg$. Proto, pokud je H normální podgrupa grupy G, nemusíme rozlišovat mezi pravými a levými rozkladovými třídami podle H a budeme tedy mluvit pouze o rozkladových třídách. Je-li H normální podgrupa grupy G, je pro každé g, $h \in G$,

$$(gH)(hH) = g(Hh)H = (gh)(HH) = (gh)H$$

a množina rozkladových tříd podle H tvoří spolu s operací násobení grupu (s jednotkou H a s inverzí $g^{-1}H$ k prvku gH), kterou budeme nazývat faktorová grupa podle H a značit G/H. Zobrazení $\pi_H : G \to G/H$ určené předpisem $g \mapsto gH$ je grupový homomorfismus na grupu G/H; budeme ho nazývat *přirozená projekce na grupu* G/H. Jádrem přirozené projekce na grupu G/H je grupa H.

Cvičení 5.4. *Buď K jádro grupového homomorfismu $\varphi : G \to H$. Ověřte, že K je normální podgrupou grupy G.*

Důsledek 5.3. *Jádra grupových homomorfismů jsou právě normální podgrupy.*

Cvičení 5.5. *Nechť H a K jsou podgrupy grupy G. Je-li alespoň jedna z těchto podgrup normální v G, je také součin HK podgrupa grupy G. Dokažte!*

Nechť H, K, J jsou normální podgrupy grupy G a platí $H \subseteq K$. Dokažte, že

$$K \cap (HJ) = H(K \cap J).$$

Cvičení 5.6. *Je-li H podgrupa grupy G taková, že $[G : H] = 2$, potom je H normální. Dokažte! (Návod: Využijte toho, že existují jen dvě levé, resp. pravé rozkladové třídy podle H.)*

Cvičení 5.7. *Položme $V = \{\mathrm{id},\ (1,2)(3,4),\ (1,3)(2,4),\ (1,4)(2,3)\}$. Dokažte, že V je normální podgrupa grupy A_4.*

Poznámka. Pro $n \geq 5$ nemá grupa A_n žádnou netriviální normální podgrupu!

Cvičení 5.8*. *Buď p nejmenší prvočíslo, které dělí počet prvků konečné grupy G. Je-li H podgrupa grupy G taková, že $[G : H] = p$, potom je H normální. Dokažte!*

Cvičení 6
Akce grupy na množině a barvení těles

Definice. Nechť M je nějaká množina a G je grupa. *Levou akcí* grupy G na množině M rozumíme zobrazení, které dvojici $(g, m) \in G \times M$ přiřadí prvek $gm \in M$ takový, že platí

(1) $(gh)m = g(hm)$ pro každé g, $h \in G$ a $m \in M$;
(2) $1m = m$ pro každé $m \in M$.

Symetricky definujeme *pravou akci* grupy G na množině M. Až do konce této kapitoly se budeme zabývat výhradně levou akcí, v případě pravé akce bychom postupovali obdobně.

Pro m, $n \in M$, položme $m \sim_G n$ pokud $m = gn$ pro nějaké $g \in G$.

Lemma 6.1. *Relace $\sim_G$ je ekvivalence na množině M.*

Důkaz. Ukážeme, že relace $\sim_G$ je reflexivní, symetrická a tranzitivní. Podle definice je $m = 1m$ pro každé $m \in M$ a tedy $m \sim_G m$, tj. relace $\sim_G$ je reflexivní. Jestliže, pro některá m, $n \in M$, platí $m \sim_G n$, existuje $g \in G$ tak, že $m = gn$. Potom $g^{-1}m = g^{-1}(gn) = (g^{-1}g)n = 1n = n$ a tedy $n \sim_G m$. Proto je relace $\sim_G$ symetrická. Nakonec, nechť pro některá m, n, $k \in M$ platí $m \sim_G n$ a $n \sim_G k$. Potom existují g, $h \in G$ tak, že $m = gn$ a $n = hk$. Odtud $m = g(hk) = (gh)k$ a tedy $m \sim_G k$. Ukázali jsme, že relace $\sim_G$ je i tranzitivní a tedy je to ekvivalence na M. □

Symbolem M/G označíme množinu rozkladových tříd ekvivalence $\sim_G$ a pro $m \in M$ položíme $Gm = \{gm \mid g \in G\}$, tj. Gm je rozkladová třída ekvivalence $\sim_G$ obsahující prvek m.

Cvičení 6.1. *Nechť m, n jsou prvky množiny M. Dokažte, že $n \in Gm$ právě když $Gn = Gm$.*

Pro $m \in M$ označme dále $G_m = \{g \in G \mid gm = m\}$.

Cvičení 6.2. *Dokažte, že pro každé $m \in M$ je G_m podgrupa grupy G.*

Tvrzení 6.2. *Buď dána levá akce grupy G na množině M. Potom pro každé $m \in M$ platí*

$$|G| = |Gm||G_m|.$$

Důkaz. Pro každé $n \in Gm$ zvolme $g_n \in G$ tak, že $n = g_n m$. Označme $\Gamma_m = \{g_n \mid n \in Gm\}$. Předpisem $(g_n, h) \mapsto g_n h$ definujme zobrazení $\varphi_m : \Gamma_m \times G_m \to G$. Ukážeme, že zobrazení φ_m je bijekce.

Buď $g \in G$. Označme $n = gm$. Potom $g_n^{-1}g \in G_m$ a $g = \varphi_m(g_n, g_n^{-1}g)$, odkud plyne, že je zobrazení φ_m na.

Pokud $g_n h = g_{n'} h'$ pro n, $n' \in Gm$ a h, $h' \in G_m$, tak

$$n = g_n hm = g_{n'} hm = n',$$

a tedy také $h = h'$. Proto je zobrazení φ_m prosté.

Protože $|\Gamma_m| = |Gm|$, dostáváme dokazovanou rovnost. □

Lemma 6.3. *Buď dána levá akce grupy G na množině M. Potom*

$$|M/G| = \sum_{m \in M} \frac{1}{|Gm|}$$

Důkaz. Buď Δ_G množina reprezentantů rozkladových tříd relace $\sim_G$. Potom

$$|M/G| = |\Delta_G| = \sum_{m \in \Delta_G} \frac{|Gm|}{|Gm|} = \sum_{m \in \Delta_G} \left(\sum_{n \in Gm} \frac{1}{|Gm|} \right) = \sum_{m \in M} \frac{1}{|Gm|}.$$

□

Lemma 6.4. *Buď dána levá akce grupy G na množině M. Potom*

$$|M/G| = \frac{1}{|G|} \sum_{m \in M} |G_m|$$

Důkaz. Pro každé $m \in M$ je podle Tvrzení 6.2

$$\frac{1}{|Gm|} = \frac{|G_m|}{|G|}.$$

□

Nyní pro každé $g \in G$ ozbnačme $M_g = \{m \in M \mid gm = m\}$.

Věta 6.5. *Buď dána levá akce grupy G na množině M. Potom*

$$|M/G| = \frac{1}{|G|} \sum_{g \in G} |M_g|.$$

Důkaz. Věta plyne z toho, že

$$\sum_{m \in M} |G_m| = |\{(g, m) \mid gm = m\}| = \sum_{g \in G} |M_g|.$$

□

Příklad 6.6. *Určete kolika způsoby je možné obarvit stěny pravidelného čtyřstěnu n různými barvami. Přitom dvě obarvení považujeme za shodná, můžeme-li jedno získat z druhého otočením čtyřstěnu.*

Řešení. Buď G grupa všech otočení čtyřstěnu a M množina všech obarvení "fixního" čtyřstěnu. Pro obarvení $m \in M$ a otočení $g \in G$ označíme symbolem gm obarvení, které vznikne z m otočíme-li čtyřstěn pomocí g. Dostaneme tak levou akci grupy G na množině M. Potom je hledaný počet obarvení roven počtu prvků množiny M/G. Podle Věty 6.5 platí

$$|M/G| = \frac{1}{|G|} \sum_{g \in G} |M_g|.$$

Protože je každé otočení čtyřstěnu určeno polohou jedné stěny a jednoho vrcholu v této stěně, je $|G| = 4 \cdot 3 = 12$. Očíslujeme stěny čtyřstěnu čísly 1, 2, 3, 4 a každé otočení reprezentujeme jako permutaci této čtveřice. Grupa G se skládá z těchto prvků:

- Identické otočení, kterému odpovídá permutace (1)(2)(3)(4).
- Trojice otočení okolo osy procházející středy protilehlých stran čtyřstěnu. Těmto otočením odpovídají následující permutace: (12)(34), (13)(24), (14)(23).
- Otočení okolo osy procházejicí vrcholem a středem protější stěny. Takových otočení je osm a jsou reprezentovány permutacemi: (123)(4), (132)(4),(124)(3), (142)(3), (134)(2), (143)(2), (234)(1), (243)(1).

Je-li otočení $g \in G$ reprezentováno permutací, která má k cyklů, je $|M_g| = n^k$. Proto

$$|M/G| = \frac{1}{12}\left(n^4 + 3n^2 + 8n^2\right) = \frac{1}{12}\left(n^4 + 11n^2\right).$$

Cvičení 6.3. *Určete kolika způsoby je možné obarvit stěny krychle n různými barvami. Přitom dvě obarvení považujeme za shodná, můžeme-li jedno získat z druhého otočením krychle.*

Cvičení 6.4. *Kolika způsoby je možné obarvit políčka šachovnice 8×8 dvěma barvami.*

Cvičení 6.5. *Kolik lze vytvořit náhrdelníků z osmi korálků, máme-li k dispozici*

(i) *čtyři červené a čtyři bílé korálky,*
(ii) *libovolný počet červených a bílých korálků.*

Cvičení 6.6. *Buď p prvočíslo, G grupa, která má p^n prvků a M množina taková, že $p \nmid |M|$. Je-li dána akce grupy G na množině M, potom $G_m = G$ pro některé $m \in M$. Dokažte!*

Cvičení 6.7*. *Buď G grupa regulárních $n \times n$-matic nad tělesem $\mathbb{Z}_p$, která má p^k ($k \in \mathbb{N}$) prvků. Dokažte, že existuje nenulový vektor $\mathbf{v} \in \mathbb{Z}_p^n$ takový, že $\mathbf{Av} = \mathbf{v}$ pro každou matici $\mathbf{A}$ z grupy G.*

Cvičení 7
Konjugace, p-grupy a třídová formule

Třídová formule

Definice. Prvky g, h grupy G nazveme *konjugované* (značíme $g \sim_G h$) pokud existuje $x \in G$ tak, že $g = x^{-1}hx$.

Pro $g, x \in G$ označíme $g^x = x^{-1}gx$. Všimněme si, že předpisem $(x, g) \mapsto g^x = x^{-1}gx$ je definována pravá akce grupy G na množině G. Je totiž $g^{xy} = (xy)^{-1}g(xy) = y^{-1}x^{-1}gxy = y^{-1}g^xy = (g^x)^y$ a platí $g^1 = g$, pro každé g, x, $y \in G$. Podobně jako v šesté kapitole uvažme pro každé $g \in G$ množiny $G_g = \{x \in G \mid g^x = g\}$ a $g^G = \{g^x \mid x \in G\}$. Potom je G_g podgrupa grupy G a platí (Tvrzení 6.2)

$$|G| = |G_g||g^G|. \tag{7.1}$$

Označme symbolem Δ_G množinu reprezentantů tříd ekvivalence $\sim_G$. Potom je

$$G = \dot{\bigcup}_{g \in \Delta_G} g^G,$$

odkud dostaneme, že

$$|G| = \sum_{g \in \Delta_G} |g^G|. \tag{7.2}$$

Definice. Buď G grupa. Položme $\mathrm{Z}(G) = \{g \in G \mid \forall x \in G : gx = xg\}$. Množina $\mathrm{Z}(G)$ ze nazývá *centrum* grupy G.

Snadno nahlédneme, že $g \in \mathrm{Z}(G)$ právě když $|g^G| = 1$. Speciálně je $\mathrm{Z}(G) \subseteq \Delta_G$. Položme $\Delta'_G = \Delta_G \setminus \mathrm{Z}(G)$. Dosazením do (7.2) dostaneme

$$|G| = |\mathrm{Z}(G)| + \sum_{g \in \Delta'_G} |g^G|. \tag{7.3}$$

Vzorec (7.3) se často nazývá *třídová formule*. Pomocí tohoto vzorce ukážeme následující klasické tvrzení.

Tvrzení 7.1 (Cauchy 1845). *Buď G konečná grupa. Jestliže $p \mid |G|$, potom v grupě G existuje prvek řádu p.*

Důkaz. Je-li G cyklická grupa generovaná prvkem g, je řád prvku g roven pm pro nějaké $m \in \mathbb{N}$. Potom je řád prvku g^m roven právě p. Nyní pro spor předpokládejme, že Tvrzení 7.1 neplatí. Zvolme nejmenší grupu G takovou, že prvočíslo p dělí počet prvků této grupy a přitom v G neexistuje prvek řádu p. Nejprve předpokládejme, že je grupa G komutativní. Buď $1 \neq h$ nějaký prvek grupy G a označme H cyklickou grupu generovanou prvkem h. Podle našeho předpokladu prvočíslo p nedělí $|H|$ a tedy, podle Lagrangeovy věty, $p \mid |G/H| < |G|$. Proto grupa G/H obsahuje prvek gH řádu p. Potom p dělí řád prvku g a tedy v cyklické grupě generované prvkem g, a tedy i v G, existuje prvek řádu p, což je spor. Tedy grupa G není komutativní. Prvočíslo p nedělí počet prvků žádné vlastní podgrupy grupy G, speciálně p nedělí $|G_g|$ pro žádné $g \in \Delta'_G$. Podle (7.2) potom $p \mid |g^G|$ pro každé $g \in \Delta'_G$ a protože $p \mid |G|$, dostáváme, že p dělí

$$|G| - \sum_{g \in \Delta'_G} |g^G| = |\mathrm{Z}(G)|.$$

Odtud plyne, že $G = \mathrm{Z}(G)$, což znamená, že grupa G je komutativní – spor. □

p-GRUPY

Definice. Buď p prvočíslo. Konečná grupa, která má p^n prvků ($n \in \mathbb{N}$) se nazývá *p-grupa.*

Cvičení 7.2. *Dokažte, že konečná grupa G je p-grupa právě když řád každého jejího prvku je mocninou prvočísla p.*

Tvrzení 7.2. *Každá p-grupa má netriviální centrum.*

Důkaz. Buď G grupa, která má p^n prvků. Pro každý prvek g grupy G, který neleží v jejím centru je, vzhledem k (7.1),

$$1 < |g^G| = \frac{|G|}{|G_g|} = p^k \quad \text{pro nějaké} \quad 0 < k < n.$$

Použijem třídovou formuli (7.3) a dostaneme

$$p \mid (|G| - \sum_{g \in \Delta'_G} |g^G|) = |\mathrm{Z}(G)|,$$

odkud plyne, že $\mathrm{Z}(G)$ má alespoň p prvků. □

Cvičení 7.3. *Buď p prvočíslo. Dokažte, že každá grupa která má p^2 je nutně komutativní. Odvoďte odtud, že, až na izomorfismus, exitují právě dvě grupy, které mají p^2 prvků a to $\mathbb{Z}_{p^2}$ a $\mathbb{Z}_p \times \mathbb{Z}_p$.*

Cvičení 7.4. *Dokažte, že pro každé prvočíslo p existuje grupa, která má p^3 prvků a která není komutativní. [Návod: Ukažte, že horní trojůhelníkové matice tvaru*

$$\begin{pmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{pmatrix}$$

nad tělesem $\mathbb{Z}_p$ tvoří grupu.]

Cvičení 7.5*. *Dokažte, že je-li H netriviální normální podgrupa p-grupy G, potom $H \cap \mathrm{Z}(G) \neq \{1\}$ (Návod: Uvažte akci konjugace grupy G na množině $H \setminus \{1\}$ a použijte Cvičení 6.6).*

Cvičení 7.6. *Nechť p je prvočíslo a G je nekomutativní grupa, která má p^3 prvků. Potom $\mathrm{Z}(G) \simeq \mathbb{Z}_p$ a $G/\mathrm{Z}(G) \simeq \mathbb{Z}_p \times \mathbb{Z}_p$. Dokažte!*

Třídy konjugovaných prvků v grupě S_n

Připomeňme, že každou permutaci σ z grupy S_n můžeme zapsat (jednoznačně až na pořadí) jako součin nezávislých cyklů. *Typem* $\mathrm{t}(\sigma)$ permutace σ rozumíme n-tici nezáporných celých čísle $(\mathrm{t}_1(\sigma), \mathrm{t}_2(\sigma), \ldots, \mathrm{t}_n(\sigma))$ takovou, že $\mathrm{t}_i(\sigma)$ je rovno počtu cyklů délky i ve vyjádření permutace σ jako součinu nezávislých cyklů. Je-li například

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

tj. $\sigma = (1,2,5)(3,8,4,6)(7)$, je

$$\mathrm{t}(\sigma) = (1,0,1,1,0,0,0).$$

Tvrzení 7.3. *Permutace σ, $\rho \in S_n$ jsou konjugované právě když* $\mathrm{t}(\sigma) = \mathrm{t}(\rho)$.

Důkaz. Buď α libovolná permutace z grupy S_n a nechť

$$\sigma = (a_{1,1}, \ldots, a_{1,n_1})(a_{2,1}, \ldots, a_{2,n_2}) \ldots (a_{k,1}, \ldots, a_{k,n_k})$$

je vyjádření permutace σ jako součinu nezávislých cyklů. Všimněme si, že je-li $\sigma(a) = b$, je

$$\sigma^\alpha(\alpha^{-1}(a)) = \alpha^{-1}(\sigma(\alpha(\alpha^{-1}(a)))) = \alpha^{-1}(\sigma(a)) = \alpha^{-1}(b).$$

Proto

$$\sigma^\alpha = (\alpha^{-1}(a_{1,1}), \ldots, \alpha^{-1}(a_{1,n_1}))(\alpha^{-1}(a_{2,1}), \ldots, \alpha^{-1}(a_{2,n_2})) \ldots (\alpha^{-1}(a_{k,1}), \ldots, \alpha^{-1}(a_{k,n_k}))$$

a $\mathrm{t}(\sigma) = \mathrm{t}(\sigma^\alpha)$. Ukázali jsme, že jsou-li dvě permutace konjugované, potom mají stejný typ.

Předpokládejme nyní, že $\mathrm{t}(\sigma) = \mathrm{t}(\rho)$ a nechť

$$\rho = (b_{1,1}, \ldots, b_{1,n_1})(b_{2,1}, \ldots, b_{2,n_2}) \ldots (b_{k,1}, \ldots, b_{k,n_k})$$

je rozklad permutace ρ v součin nezávislých cyklů. Buď $\alpha \in S_n$ permutace taková, že $\alpha(b_{i,j}) = a_{i,j}$ pro každé $i \leq k$, $j \leq n_i$. Potom

$$\sigma^\alpha(b_{i,j}) = \sigma^\alpha(\alpha^{-1}(a_{i,j})) = \alpha^{-1}(a_{i,(j+1 \mod n_i)}) = b_{i,(j+1 \mod n_i)} = \rho(b_{i,j})$$

pro každé $i \leq k$, $j \leq n_i$ a tedy $\sigma^\alpha = \rho$. □

Cvičení 7.7. *Dokažte, že počet c rozkladových tříd relace konjugace v grupě G je*

$$c = \frac{1}{|G|} \sum_{g \in G} |G_g|.$$

Cvičení 7.8. *Třídy konjugovaných prvků v grupě S_4 můžeme popsat takto:*

Typ	**Příklad**	**Počet prvků**
$(4,0,0,0)$	*identita*	1
$(2,1,0,0)$	$(1,2)$	6
$(0,2,0,0)$	$(1,2)(3,4)$	3
$(1,0,1,0)$	$(1,2,3)$	8
$(0,0,0,1)$	$(1,2,3,4)$	6

Sestrojte podobnou tabulku pro grupu S_5.

Okruhy a dělitelnost

Cvičení 8
Okruhy a ideály

Definice a základní vlastnosti okruhů

Definice. *Okruh* je množina R se dvěma binárními operacemi $+, \cdot$ a dvojicí prvků $0 \neq 1$ taková, že

(1) $(R, +, 0)$ je komutativní grupa;
(2) $(R, \cdot, 1)$ je monoid;
(3) $a(b + c) = ab + ac$ a $(a + b)c = ac + bc$ pro každé a, b, $c \in R$.

Okruh R je *komutativní* splňuje-li navíc podmínku

(4) $ab = ba$ pro každé a, $b \in R$.

Podívejme se na několik příkladů okruhů: Mezi okruhy patří všechna tělesa a okruh $(\mathbb{Z}, +, .)$ celých čísel. Dále okruh $(\mathbb{Z}_n, +, .)$ se sčítáním a násobením modulo n (okruh $\mathbb{Z}_n$ je těleso právě když je p prvočíslo). Další příklady získáme následujícími konstrukcemi z již známých okruhů: jsou to okruh $R[x]$ polynomů v neurčité x s koeficienty v okruhu R a okruh $\mathbb{M}_n(R)$ čtvercových matic řádu n s prvky z okruhu R.

Cvičení 8.1. *Buď R komutativní okruh v němž pro každý prvek a různý od 1 existuje b tak, že $a + b - ab = 0$. Dokažte, že R je těleso.*

Definice. Prvek e okruhu R je *invertibilní*, jestliže existuje $f \in R$ tak, že

$$ef = 1 = fe.$$

Všechny invertibilní prvky okruhu R tvoří grupu, kterou označíme symbolem R^*.

Cvičení 8.2. *Ověřte, že $\mathbb{Z}^* = \{1, -1\}$ a pro libovolné těleso je $T^* = T[x]^* = T^* = T \setminus \{0\}$[1]. Jak vypadá $\mathbb{Z}_p^*$?*

Cvičení 8.3. *Označme*

$$\mathbb{Z}[i] = \{a + ib \mid a, b \in \mathbb{Z}\}.$$

Pro $\alpha = a + ib$ položme $\overline{\alpha} = a - ib$, a definujme $\mathbf{N}(\alpha) = \alpha\overline{\alpha} = a^2 + b^2$.

(a) *Dokažte, že $\mathbf{N}(\alpha\beta) = \mathbf{N}(\alpha)\mathbf{N}(\beta)$ pro všechna α, $\beta \in \mathbb{Z}[i]$;*
(b) *Dokažte, že $\alpha \in \mathbb{Z}[i]^*$ právě když $\mathbf{N}(\alpha) = 1$;*
(c) *Popište grupu $\mathbb{Z}[i]^*$.*

Ideály a okruhové homomorfismy

Definice. Zobrazení f z okruhu R do okruhu S je *okruhový homomorfismus* pokud platí

(1) $f(a + b) = f(a) + f(b)$, pro každé a, $b \in R$;
(2) $f(a.b) = f(a)f(b)$, pro každé a, $b \in R$;
(3) $f(1) = 1$.

Okruhový homomorfismus, který je prostý a na nazveme *izomorfismem*. Okruhy R, S jsou *izomorfní*, jestliže existuje izomorfismus z okruhu R na okruh S.

[1] Polynomy stupně 0 chápeme jako prvky tělesa T

Cvičení 8.4. *Dokažte, že okruh* $C = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \mid a, b \in \mathbb{R} \right\}$ *je izomorfní tělesu komplexních čísel.*

Cvičení 8.5. *Dokažte, že okruh matic* $T = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \mid a, b \in \mathbb{Z}_3 \right\}$ *je izomorfní devítiprvkovému tělesu.*

Cvičení 8.6. *Buď R okruh a x, y neurčité. Dokažte, že*

$$(R[x])[y] \simeq R[x, y].$$

Cvičení 8.7. *Buď R okruh a n, $m \in \mathbb{N}$. Dokažte, že*

$$\mathbb{M}_n(\mathbb{M}_m(R)) \simeq \mathbb{M}_{nm}(R).$$

Definice. *Ideálem* okruhu R rozumíme podgrupu I aditivní grupy okruhu R takovou, že pro každé r, $s \in R$ platí $rIs \subseteq I$.

Cvičení 8.8. *Dokažte, že*

(1) *Pokud ideál okruhu R obsahuje* 1*, je roven celému okruhu R;*
(2) *Je-li okruh R komutativní, je podgrupa I aditivní grupy $(R, +, 0)$ ideálem R právě když pro každé $r \in R$ platí $rI \subseteq I$.*

Buď R komutativní okruh. Pro $a \in R$ položme $(a) = \{ra \mid r \in R\}$. Ideál (a) budeme nazývat *hlavní ideál* generovaný prvkem a.

Definice. Buď R komutativní okruh a nechť a, b jsou dva nenulové prvky R. Řekneme, že prvek a *dělí* b jestliže existuje $c \in R$ tak, že $ac = b$. To, že a dělí b zapíšeme symbolem $a \mid b$.

Cvičení 8.9. *Buď R komutativní okruh. Dokažte, že (a) je nejmenší ideál okruhu R, který obsahuje prvek a. Dále ukažte, že jsou-li a, b dva nenulové prvky okruhu R, potom $a \mid b$ právě když $(b) \subseteq (a)$.*

Cvičení 8.10. *Popište ideály okruhů $\mathbb{Z}$ a $\mathbb{Z}_{p^n}$, kde p je prvočíslo a $n \in \mathbb{N}$.*

Cvičení 9
Dělitelnost

Obor integrity je komutativní okruh R , ve kterém $ab = 0$ implikuje $a = 0$ nebo $b = 0$.

Cvičení 9.1. *Dokažte, že komutaivní okruh R je oborem integrity právě když je v něm možné krátit nenulovými prvky.*

Definice. Řekneme, že prvek a okruhu R dělí prvek b, značíme $a \mid b$, jestliže existuje $c \in R$ tak, že $ac = b$. Pokud $a \mid b$ a zároveň $b \mid a$, budeme říkat, že prvky a, b jsou *asociovány* (značíme $a \sim b$).

Je zřejmé, že relace $\sim$ je reflexivní a symetrická a snadno nahlédneme, že je také tranzitivní. Je to tedy ekvivalence na množině R.

Cvičení 9.2. *Dokažte, že nenulové prvky a, b oboru integrity R jsou asociovány právě tehdy když exituje invertibilní prvek e okruhu R tak, že $a = eb$.*

Definice. Nenulový prvek a oboru integrity R, který není invertibilní, nazveme *nerozložitelný*, jestliže $a = bc$ implikuje, že jeden z prvků b, c je invertibilní (a tedy druhý je s a asociován). Nenulový prvek $a \in R$ se nazývá *prvočinitel*, jestliže $a \mid bc$ implikuje, že $a \mid b$ nebo $a \mid c$.

Je-li a prvočinitel a $a = bc$, potom $a \mid b$ nebo $a \mid c$. V prvním případě máme $a \sim b$, (neboť také $b \mid a$) a tedy $c \in R^*$, ve druhém $c \mid a$ a tedy $b \in R^*$. Odtud je vidět, že je *každý prvočinitel nerozložitelný*. V okruhu $\mathbb{Z}$ celých čísel je každý nerozložitelný prvek prvočinitel. Obecně to však neplatí, jak si ukážeme v následujícím příkladu.

Příklad 9.1. *Uvažme obor integrity*

$$\mathbb{Z}[\sqrt{5}] = \{a + \sqrt{5}b \mid a,\ b \in \mathbb{Z}\}.$$

V tomto okruhu existuje nerozložitelný prvek, který není prvočinitelem.

Důkaz. Podívejme se na to, jak vypadá v tomto okruhu sčítání a násobení:

$$(a + \sqrt{5}b) + (c + \sqrt{5}d) = (a + c) + \sqrt{5}(b + d),$$

$$(a \pm \sqrt{5}b)(c \pm \sqrt{5}d) = (ac + 5bd) \pm \sqrt{5}(ad + bc).$$

Pro $\alpha = a + \sqrt{5}b \in \mathbb{Z}[\sqrt{5}]$ položme $\overline{\alpha} = a - \sqrt{5}b$ a definujme

$$\mathbf{N}(\alpha) = \alpha\overline{\alpha} = a^2 - 5b^2.$$

Z definice násobení v oruhu $\mathbb{Z}[\sqrt{5}]$ snadno nahlédneme, že $\overline{\alpha}\overline{\beta} = \overline{\alpha\beta}$ pro každé α, $\beta \in \mathbb{Z}[\sqrt{5}]$, odkud

$$\mathbf{N}(\alpha\beta) = \mathbf{N}(\alpha)\mathbf{N}(\beta).$$

(Je totiž $\mathbf{N}(\alpha\beta) = \alpha\beta\overline{\alpha\beta} = \alpha\beta\overline{\alpha}\overline{\beta} = \alpha\overline{\alpha}\beta\overline{\beta} = \mathbf{N}(\alpha)\mathbf{N}(\beta)$.) Odtud plyne, že jestliže $\alpha \mid \beta$, potom $\mathbf{N}(\alpha) \mid \mathbf{N}(\beta)$. Nyní ověříme, že invertibilní prvky okruhu $\mathbb{Z}[\sqrt{5}]$ jsou právě ty $\alpha \in \mathbb{Z}[\sqrt{5}]$, pro které je $|\mathbf{N}(\alpha)| = 1$. Je-li $\alpha \in \mathbb{Z}[\sqrt{5}]^*$, potom $\mathbf{N}(\alpha) \mid \mathbf{N}(1) = 1$ a tedy $|\mathbf{N}(\alpha)| = 1$. Je-li $|(\mathbf{N}(\alpha)| = 1$, je

$$1 = \mathbf{N}(\alpha)^2 = \alpha\big(\overline{\alpha}\alpha\overline{\alpha}\big)$$

a tedy α je jednotkou.

Ukážeme, že 2 je nerozložitelný prvek okruhu $\mathbb{Z}[\sqrt{5}]$, který není prvočinitel. Nejprve ověříme, že prvek 2 je nerozložitelný. Pro spor předpokládejme, že existují prvky α, β okruhu $\mathbb{Z}[\sqrt{5}]$ tak, že

$$2 = \alpha\beta$$

a žádný z těchto prvků není invertibilní. Potom

$$4 = \mathbf{N}(2) = \mathbf{N}(\alpha)\mathbf{N}(\beta),$$

a tedy nutně $|\mathbf{N}(\alpha)| = |\mathbf{N}(\beta)| = 2$. Je-li $\alpha = a + \sqrt{5}b$, je potom $|a^2 - 5b^2| = 2$ a tedy

$$a^2 \equiv 2 \pmod 5 \quad \text{nebo} \quad a^2 \equiv 3 \pmod 5.$$

To však neplatí pro žádné celé číslo, jak snadno ověříme prozkoumáním všech možností:

$$\begin{aligned}(5k+1)^2 &\equiv 1 \pmod 5,\\ (5k+2)^2 &\equiv 4 \pmod 5,\\ (5k+3)^2 &\equiv 4 \pmod 5,\\ (5k+4)^2 &\equiv 1 \pmod 5,\\ (5k)^2 &\equiv 0 \pmod 5.\end{aligned}$$

Nyní ukážeme, že 2 není prvočinitel okruhu $\mathbb{Z}[\sqrt{5}]$. Platí totiž

$$2 \cdot 2 = 4 = (1 + \sqrt{5})(-1 + \sqrt{5}).$$

Kdyby, ve sporu s tím co máme dokázat, bylo číslo 2 prvočinitelem v okruhu $\mathbb{Z}[\sqrt{5}]$, platilo by

$$2 \mid 1 + \sqrt{5} \quad \text{nebo} \quad 2 \mid -1 + \sqrt{5}.$$

Nastala-li by například první z těchto možností, existovalo by $a + \sqrt{5}b \in \mathbb{Z}[\sqrt{5}]$ tak, že

$$2(a + \sqrt{5}b) = 2a + 2\sqrt{5}b = 1 + \sqrt{5},$$

odkud $2a \mid 1$, což není možné. Podobně ve druhém případě. □

Cvičení 9.3. *Ověřte, že obor integrity $\mathbb{Z}[\sqrt{5}]$ je izomorfní okruhu matic* $\begin{pmatrix} a & \sqrt{5}b \\ \sqrt{5}b & a \end{pmatrix}$, *kde a, $b \in \mathbb{Z}$.*

Cvičení 9.4. *Dokažte, že v oboru integrity $\mathbb{Z}[\sqrt{3}i] = \{a + \sqrt{3}ib \mid a, b \in \mathbb{Z}\}$ je 2 nerozložitelný prvek, který není prvočinitel.*

Definice. Nechť a, b jsou nenulové prvky oboru integrity R. Prvek $d \in R$ se nazývá největší společný dělitel a, b, značíme ho

$$d = \mathrm{NSD}(a, b),$$

jestliže je společným dělitelem prvků a, b a každý společný dělitel prvků a, b dělí d. Poznamenejme, že každý prvek asociovaný s d je opět největším společným dělitelem prvků a, b a největší společný dělitel je určen jednoznačně až na relaci "$\sim$".

Následující tvrzení nebudeme dokazovat.

Věta 9.2. *Buď R obor integrity. Existuje-li největší společný dělitel každé dvojice nenulových prvků $a, b \in R$, potom je každý nerozložitelný prvek okruhu R prvočinitelem.*

Všimněmě si, že z této věty plyne, že v okruhu $\mathbb{Z}[\sqrt{5}]$ existuje dvojice nenulových prvků, která nemá největší společný dělitel.

Cvičení 9.5*. *Dokažte, že prvky 4 a $2 + 2\sqrt{5}$ nemají v oboru integrity $\mathbb{Z}[\sqrt{5}]$ největší společný dělitel.*

Cvičení 10
Gaussovy a Eukleidovy obory

Připomeňme, že každé přirozené číslo je možné (až na pořadí) vyjádřit jako součin prvočísel. Nyní definujme analogii této vlastnosti přirozených čísel pro jakýkoliv obor integrity. Nejprve, nechť je R obor integrity a a nenulový prvek R. Řekneme, že dva rozklady

$$a = b_1 b_2 \dots b_n \quad \text{a} \quad a = c_1 c_2 \dots c_m$$

jsou *asociované*, jestliže je $n = m$ a po vhodné změně pořadí prvků ve druhém rozkladu je $b_i \sim c_i$ pro $i = 1, \dots, n$.

Definice. Obor integrity R nazveme *Gaussův obor* jestliže je možné každý nenulový prvek $a \in R$ rozložit v součin nerozložitelných prvků a každé dva takové rozklady jsou asociované.

Tvrzení 10.1. *Ke každé dvojici nenulových prvků Gaussova oborou existuje největší společný dělitel.*

Příklad 10.2. *V okruhu $\mathbb{Z}[i]$ určete největší společný dělitel čísel 85 a $1 + 13i$.*

Řešení. Největší společný dělitel najdeme pomocí Eukleidova algoritmu. Platí

$$\frac{85}{1+13i} = \frac{85(1-13i)}{170} = \frac{1}{2} - \frac{13}{2}i.$$

Prvky okruhu $\mathbb{Z}[i]$ tvoří čtvercovou síť a číslo $1/2 + 13/2i$ leží uprostřed čtverce s vrcholy $-6i$, $-7i$, $1-6i$, $1-7i$. Platí $85+(1+13i)6i = 7+6i$ a tedy $7+6i$ je zbytek po dělení čísla 85 číslem $1+13i$ (všimněme si, že $\mathbf{N}(7+6i) = 85 < 170 = \mathbf{N}(1+13i)$). Dále platí

$$\frac{1+13i}{7+6i} = \frac{(1+13i)(7-6i)}{85} = \frac{85+85i}{85} = 1+i.$$

Vidíme, že $(7+6i) \mid (1+13i)$ a tedy

$$\mathrm{NSD}(85, 1+13i) = 7+6i.$$

□

Cvičení 10.1. *V okruhu $\mathbb{Z}[i]$ určete největší společný dělitel čísel 100 a $7-4i$.*

Cvičení 10.2. *Nechť a, b, t jsou nenulové prvky Gaussova oboru R. Buď $d = \mathrm{NSD}(a, b)$ a nechť $a = a'd$. Položme $c = a'b$. Dokažte, že pokud $a \mid t$ a zároveň $b \mid t$ potom také $c \mid t$.*

Věta 10.3. *Je-li R Gaussův obor, potom je také okruh $R[x]$ polynomů s koeficienty z R Gaussův obor.*

Cvičení 10.3. *V okruhu $\mathbb{R}[x]$ určete největší společný dělitel polynomů $x^4 - x_3 + 2x^2 - x + 2$ a $x^3 - 3x^2 + 3x - 2$.*

Příklad 10.4 Výpočet Vandermondova determinantu. *Buď R Gaussův obor a nechť $x_0, \dots, x_{n-1}$ je množina neurčitých. Potom je*

$$\begin{vmatrix} 1 & x_0 & \dots & x_0^{n-1} \\ 1 & x_1 & \dots & x_1^{n-1} \\ \dots & \dots & \dots & \dots \\ 1 & x_{n-1} & \dots & x_{n-1}^{n-1} \end{vmatrix} = \prod_{i>j} (x_i - x_j). \tag{10.1}$$

Důkaz. Zkoumaný determinant je polynom v neurčitých $x_0, \dots, x_{n-1}$. Označme jej $D(x_0, \dots, x_{n-1})$. Z definice determinantu je vidět, že

$$D(x_0, \dots, x_{n-1}) = \sum c_{(a_0,\dots,a_{n-1})} x_0^{a_0} x_1^{a_1} \dots x_{n-1}^{a_{n-1}},$$

kde sčítáme přes všechny n-tice $(a_0, \dots, a_{n-1})$ různých nezáporných čísel takové, že $a_0 + \dots + a_{n-1} = \frac{n(n-1)}{2}$ ($c_{(a_0,\dots,a_{n-1})}$ jsou nějaké neznámé koeficienty).

Nechť $0 \le j < i \le n-1$. Odečteme-li v matici (10.1) od i-tého řádku j-tý řádek, dostaneme

$$\begin{vmatrix} 1 & x_0 & \dots & x_0^{n-1} \\ \dots & \dots & \dots & \dots \\ 1 & x_i & \dots & x_i^{n-1} \\ \dots & \dots & \dots & \dots \\ 1 & x_{n-1} & \dots & x_{n-1}^{n-1} \end{vmatrix} = \begin{vmatrix} 1 & x_0 & \dots & x_0^{n-1} \\ \dots & \dots & \dots & \dots \\ 0 & x_i - x_j & \dots & x_i^{n-1} - x_j^{n-1} \\ \dots & \dots & \dots & \dots \\ 1 & x_{n-1} & \dots & x_{n-1}^{n-1} \end{vmatrix} =$$

$$= (x_i - x_j) \begin{vmatrix} 1 & x_0 & \dots & x_0^{n-1} \\ \dots & \dots & \dots & \dots \\ 0 & 1 & \dots & \sum_{k=0}^{n-2} x_i^k x_j^{n-2-k} \\ \dots & \dots & \dots & \dots \\ 1 & x_{n-1} & \dots & x_{n-1}^{n-1} \end{vmatrix}.$$

Odtud vidíme, že $(x_i - x_j) \mid D(x_0, \dots, x_{n-1})$ pro každé $0 \le j < i \le n-1$. Je-li $0 \le j' < i' \le n-1$ dvojice různá od dvojice i, j, jsou plynomy $x_i - x_j$ a $x_{i'} - x_{j'}$ nesoudělné. Podle Cvičení 10.2 potom

$$\prod_{i>j} (x_i - x_j) \mid D(x_0, \dots, x_{n-1}).$$

Porovnáním stupnů obou polynomů dostaneme, že

$$\prod_{i>j} (x_i - x_j) = cD(x_0, \dots, x_{n-1}).$$

pro některé $c \in R^*$. Protože $c_{(0,1,2,\dots,n-1)} = 1$ (rozmyslete si) je $c = 1$. □

Definice. Buď R obor integrity.

(i) Řekneme, že R je *obor hlavních ideálů*, jestliže je každý ideál R hlavní.

(ii) Řekneme, že R je *Eukleidův obor*, jestliže je možné ke každému nenulovému prvku $a \in R$ přiřadit nezáporné celé číslo $\mathbf{N}(a)$ tak, že k libovolným dvěma prvkům a, $b \in R$, $b \neq 0$ existují v okruhu R prvky c, r tak, že

$$a = bc + r$$

a zároveň buď $r = 0$ a nebo $\mathbf{N}(r) < \mathbf{N}(b)$.

Věta 10.4. *Každý Eukleidův obor je oborem hlavních ideálů a každý obor hlavních ideálů je Gaussův obor.*

Tvrzení 10.5. *Okruh $\mathbb{Z}[i]$ je Eukleidův obor.*

Důkaz. Pro každé komplexní číslo σ definujme $\mathbf{N}(\sigma) = \sigma\overline{\sigma}$. Nechť a, $b \in \mathbb{Z}[i]$, b je nenulové. Položme $\alpha = \frac{a}{b}$. Prvky okruhu $\mathbb{Z}[i]$ tvoří v komplexní rovině čtverovou síť složenou ze čtverců se stranou délky 1. Číslo α padne do některého z těchto čtverců. Potom je vzdálenost α od některého z vrcholů tohoto čtverce menší než 1 a tedy existuje $c \in \mathbb{Z}[i]$ tak, že $N(\alpha - c) < 1$, odkud $N(a - bc) < N(b)$. Položme $r = a - bc$. □

Cvičení 10.4. *Dokažte, že obor $\mathbb{Z}[\sqrt{2}i]$ je Eukleidův.*

Cvičení 10.5. *Dokažte, že obory $\mathbb{Z}[\sqrt{3}i]$, $\mathbb{Z}[\sqrt{5}]$ nejsou Eukleidovy.*

(Návod: Použijte Příklad 9.1, Cvičení 9.4, Tvrzení 10.1 a Větu 10.4.)

Příklad 10.6. *Určete všechna celočíselná řešení rovnice*

$$a^2 + 4 = b^3. \tag{10.2}$$

Řešení. Rozložme nejprve výraz (10.2) v okruhu $\mathbb{Z}[i]$. Dostaneme

$$(a + 2i)(a - 2i) = b^3. \tag{10.3}$$

Nyní ukážeme, že z (10.3) plyne, že je $a + 2i$ třetí mocninou v okruhu $\mathbb{Z}[i]$. Zkoumejme největší společný dělitel čísel $a + 2i$ a $a - 2i$ v okruhu $\mathbb{Z}[i]$. Platí

$$\mathrm{NSD}(a + 2i, a - 2i) = \mathrm{NSD}(a + 2i, 4i).$$

Označme d_N největší společný dělitel norem $\mathbf{N}(a + 2i)$ a $\mathbf{N}(4i)$. Dostaneme

$$d_N = \begin{cases} 1 & : a = 2k + 1; \\ 4 & : a = 4k; \\ 8 & : a = 4k + 2. \end{cases}$$

Každý prvek v okruhu $\mathbb{Z}[i]$ jehož norma je mocninou čísla 2 je asociován s mocninou čísla $1+i$. Buď n, resp. m největší mocnina čísla $1+i$, která dělí $a+2i$, resp. $a-2i$. Protože $1+i \sim 1-i$, je $n = m$ a $\mathrm{NSD}(a+2i, a-2i) = (1+i)^n$. Z toho, že je součin $(a+2i)(a-2i)$ třetí mocninou, dostáváme, že $3 \mid 2n$ a tedy $3 \mid n$. Označme α, resp. β podíl čísla $a + 2i$, resp. $a - 2i$ a číslem $(1 + i)^n$. Čísla α a β jsou nesoudělná a jejich součin je třetí mocninou v okruhu $\mathbb{Z}[i]$, proto je každé z nich asociováno se třetí mocninou v okruhu $\mathbb{Z}[i]$. Odtud plyne, že je $a + 2i = \alpha(1 + i)^n$ asociováno se třetí mocninou v okruhu $\mathbb{Z}[i]$. Všimněme si, že je každý z invertibilních prvků okruhu $\mathbb{Z}[i]$ třetí mocninou ($i = (-i)^3$, $-i = i^3$, $-1 = (-1)^3$ a $1 = 1^3$) a proto je každé číslo asociované se třetí mocninou v $\mathbb{Z}[i]$ opět třetí mocninou v $\mathbb{Z}[i]$. Odtud

$$a+2i = (x+iy)^3 = x^3 - 3xy^2 + i3x^2y - iy^3 = x\left(x^2 - 3y^2\right) + iy\left(3x^2 - y^2\right). \tag{10.4}$$

Z rovnosti $2 = y\left(3x^2 - y^2\right)$ dostaneme čtyři možné řešení rovnice (10.4): $x = \pm 1$, $y = -2$ a $x = \pm 1$, $y = 1$, kterým odpovídají čtyři možné řešení rovnice (10.2): $a = \pm 11$, $b = 5$ a $a = \pm 2$, $b = 2$.

Cvičení 10.6*. *Určete všechna celočíselná řešení rovnice*

$$a^2 + 49 = b^3.$$

Cvičení 10.7. *Dokažte, že neexistují přirozená čísla a, b tak, že platí*

$$a^2 + 1 = b^3.$$

Cvičení 10.8.** *Určete všechna celočíselná řešení rovnice*

$$a^2 + 2 = b^3. \tag{10.5}$$

(Návod*: Výraz (10.5) rozložte v okruhu $\mathbb{Z}[\sqrt{2}i]$. Ověřte, že $\mathbb{Z}[\sqrt{2}i]$ je Eukleidův obor.*)

Algebraické rovnice

Cvičení 11
Řešení algebraických rovnic

Kvadratická rovnice

Uvažme polynom

$$f(x) = x^2 + bx + c. \tag{11.1}$$

Položíme $y = x + \frac{1}{2}b^2$ a tak transformujeme rovnici (11.1) na rovnici

$$g(y) = y^2 + c - b^2/4,$$

jejíž řešení určíme snadno: $\pm\frac{1}{2}\sqrt{b^2 - 4c}$. Kořeny rovnice (11.1) jsou potom

$$\frac{1}{2}(-b \pm \sqrt{b^2 - 4c}).$$

Kubická rovnice

Kubickou rovnici vyřešili *Scipione del Ferro (1465-1526), Nicolo Tartaglia (1499-1557) a Girolamo Cardano (1501-1576).* Uvažme rovnici

$$f(x) = x^3 + ax^2 + bx + c, \tag{11.2}$$

kterou transformujeme substitucí $y = x + \frac{1}{3}a$ na rovnici

$$g(y) = y^3 + qy + r. \tag{11.3}$$

Přitom α je kořenem rovnice (11.3) právě když je $\alpha - \frac{1}{3}a$ kořenem rovnice (11.2). Budeme hledat α ve tvaru $\alpha = \beta + \gamma$. Binomický rozklad dává

$$\alpha^3 = (\beta + \gamma)^3 = \beta^3 + \gamma^3 + 3(\beta^2\gamma + \beta\gamma^2) = \beta^3 + \gamma^3 + 3\alpha\beta\gamma.$$

Dosazením do (11.3) dostaneme

$$0 = g(\alpha) = \beta^3 + \gamma^3 + (3\beta\gamma + q)\alpha + r = 0. \tag{11.4}$$

Nyní budeme hledat dvojici β, γ tak, že $\beta\gamma = -q/3$. Z rovnice (11.4) dostaneme

$$\beta^3 + \gamma^3 = -r$$

a

$$\beta^3\gamma^3 = -\frac{q^3}{27},$$

odkud

$$\beta^3 - \frac{q^3}{27\beta^3} = -r \quad \text{a tedy } \beta^6 + r\beta^3 - \frac{q^3}{27} = 0.$$

Nyní vzorec pro kvadratickou rovnici dává

$$\beta^3 = \frac{1}{2}\left[-r \pm \sqrt{r^2 + 4q^3/27}\right]$$

a podobně

$$\gamma^3 = \frac{1}{2}\left[-r \mp \sqrt{r^2 + 4q^3/27}\right].$$

Je-li $\omega = e^{2\pi i/3}$ primitivní třetí odmocnina z jedné a

$$\beta = \sqrt[3]{\frac{1}{2}\left[-r + \sqrt{r^2 + 4q^3/27}\right]}, \quad \text{resp.} \quad \gamma = \sqrt[3]{\frac{1}{2}\left[-r - \sqrt{r^2 + 4q^3/27}\right]},$$

jsou kořeny rovnice $g(y)$ ve tvaru $\beta + \gamma$, $\omega\beta + \omega^2\gamma$ a $\omega^2\beta + \omega\gamma$.

Kvadrická formule

Vzorec pro kořeny kvadrické rovnice

$$f(x) = x^4 + ax^3 + bx^2 + cx + d \tag{11.5}$$

objevil Lodovici Ferrari (1522-1565). Substitucí $y = x + \frac{1}{4}a$ transformujeme rovnici (11.5) na rovnici

$$g(y) = y^4 + qy^2 + ry + s,$$

kterou můžeme rozložit v součin

$$g(y) = y^4 + qy^2 + ry + s = (y^2 + ky + l)(y^2 - ky + m).$$

Protože umíme řešit kvadratickou rovnici, stačí najít koeficienty k, l a m. Po roznásobení pravé strany dostaneme porovnáním koeficientů, že

$$\begin{aligned} l + m - k^2 &= q, \\ km - kl &= r, \\ lm &= s. \end{aligned} \tag{11.6}$$

První dvě z těchto rovnic přepišme do tvaru

$$\begin{aligned} l + m &= q + k^2, \\ m - l &= r/k, \end{aligned}$$

odkud dostaneme

$$\begin{aligned} 2m &= q + k^2 + r/k, \\ 2l &= q + k^2 - r/k. \end{aligned}$$

Nyní je vidět, že stačí nalézt k. Dosazením do (11.6) dostaneme

$$(q + k^2 + r/k)(q + k^2 - r/k) = 4ml = 4s,$$

odkud

$$k^6 + 2qk^4 + (q^2 - 4s)k^2 - r^2 = 0,$$

což je kubická rovnic s neznámou k^2.

Cvičení 12
Galoisova teorie

Těleso C nazveme *algebraicky uzavřené*, jestliže má každý polynom $f(x) \in C[x]$ kořen v C, tedy existuje-li pro každé $f(x) \in C[x]$ prvek $c \in C$ tak, že $f(c) = 0$. Snadno indukcí ukážeme, že těleso C je algebraicky uzavřené právě když pro každé přirozené číslo n a každý plynom $f(x)$ stupně n existuje n-tice $c_1, c_2, \ldots, c_n$ (ne nutně různých) prvků tělesa C a $c \in C$ tak, že

$$f(x) = c(x - c_1)(x - c_2)\ldots(x - c_n).$$

Například těleso komplexních čísel je tělesem algebraicky uzavřeným. Každé těleso je možné vnořit do algebraicky uzavřeného tělesa (to budete ukazovat na přednášce; idea důkazu spočívá v postupném přidávání kořenů polynomů s koeficienty z tohoto tělesa). Například těleso reálných čísel je takto vnořeno do tělesa komplexních čísel. Je-li T podtěleso tělesa C a X podmnožina C, označíme symbolem $T(X)$ nejmenší podtěleso C obsahující $T \cup X$ (je rovno průniku všech podtěles C, která obsahují $T \cup X$). Například těleso $T(c)$ vzniklé *přidáním prvku $c \in C$ k tělesu T* je tvaru

$$T(c) = \left\{ \frac{f(c)}{g(c)} \mid f(x),\, g(x) \in T[x] \text{ a } g(c) \neq 0 \right\}.$$

Podobně můžeme k tělesu T přidat n-tici $c_1, c_2, \ldots, c_n$ prvků z C. Potom dostaneme těleso $T(c_1, c_2, \ldots, c_n)$ jehož prvky jsou zlomky

$$\frac{f(c_1, c_2, \ldots, c_n)}{g(c_1, c_2, \ldots, c_n)},$$

takové, že $f(x_1, x_2, \ldots, x_n)$, $g(x_1, x_2, \ldots, x_n) \in T[x_1, x_2, \ldots, x_n]$ a $g(c_1, c_2, \ldots, c_n) \neq 0$. Je-li $f(x) \in T[x]$ polynom stupně n a

$$f(x) = (x - c_1)(x - c_2)\ldots(x - c_n),$$

pro $c_1, c_2, \ldots, c_n \in C$, nazývá se těleso $T(c_1, c_2, \ldots, c_n)$ *rozkladové nadtěleso polynomu $f(x)$ (nad T)* a značí se T_f.

Definice 12.1. Buď T těleso, $f(x) \in T[x]$. Řekneme, že polynom $f(x)$ je *řešitelný pomocí radikálů* nad T, jestliže existuje řetězec těles

$$T = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_t$$

takový, že $T_f \subseteq K_t$ a $K_{i+1} = K_i(b_i)$ $(i = 0, \ldots, t_1)$, kde b_i je kořenem polynomu

$$x^{n_i} - d_i = 0$$

pro některé přirozené číslo n_i a $d_i \in K_i$.

Polynon

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$$

je *řešitelný pomocí radikálů*, je-li řešitelný pomocí radikálů nad tělesem $\mathbb{Q}(a_0, a_1, \ldots, a_n)$.

V jedanácté kapitole jsme odvodili vzorce pro řešení rovnic druhého, třetího a čtvrtého stupně. Nyní ukážeme, jak na základě těchto vzorců sestrojit posloupnost těles dosvědčující, že polynomy stupňe nejvýše čtyři jsou řešitelné pomocí radikálů.

Kvadratická rovnice.

$$f(x) = x^2 + bx + c. \tag{12.1}$$

Pro kvadratickou rovnici (12.1) máme $T = \mathbb{Q}(b, c)$ a řetězec

$$\mathbb{Q}(b, c) = K_0 \subseteq K_1 = K_0(\sqrt{b^2 - 4c}).$$

Všimněme si, že rozkladové nadtěleso rovnice $f(x)$ je rovno právě tělesu K_1.

Kubická rovnice.

$$g(y) = y^3 + py + q. \tag{12.2}$$

Pro kubickou rovnici ve tvaru (12.2) je $K_0 = T = \mathbb{Q}(p, q)$. Označme

$$b_0 = \sqrt{r^2 + \frac{4q^3}{27}}$$

a položme $K_1 = K_0(b_0)$. Všimněme si, že v tělese K_1 leží β^3 a γ^3. Nyní nechť

$$b_1 = \sqrt[3]{1/2(-r + b_0)}$$

a položme $K_2 = K_1(b_1)$. V tělese K_2 leží β a protože $\beta\gamma = -q/3$, leží tam i γ. Nakonec označme ω primitivní třetí odmocninu z jedné (tj. $\omega = e^{\frac{2\pi i}{3}}$) a položme $K_3 = K_0(\omega)$. Máme tedy posloupnost

$$\begin{aligned}\mathbb{Q}(p, q) = K_0 \subseteq K_0(\underbrace{\sqrt{r^2 + 4q^3/27}}_{b_0}) = K_1 \subseteq K_1(\sqrt[3]{1/2(-r + b_0)}) \\ = K_2 \subseteq K_2(e^{\frac{2\pi i}{3}}) = K_3.\end{aligned}$$

Těleso K_2 obsahuje alespoň jeden kořen polynomu $f(x)$ a těleso K_3 obsahuje rozkladové nadtěleso tohoto polynomu S. Uvědomme si však, že se může stát (například v případě, že jsou všechny kořeny polynomu $f(x)$ reálné), že $S \subsetneq K_3$.

Kvadrická rovnice.

$$g(y) = y^4 + qy^2 + ry + s. \tag{12.3}$$

Rovnici $g(y)$ ve tvaru (12.3) rozložíme

$$g(y) = (y^2 + ky + l)(y^2 - ky + m).$$

Podle vztahů odvozených na předchozím cvičení určíme k^2 jako kořen kubické rovnice

$$h(z) = z^3 + 2qz^2 + (q^2 - 4s)z - r^2.$$

Pro tuto rovnici máme, podobně jako v případě kubické rovnice (12.3) posloupnost těles

$$\mathbb{Q}(q, s, r) = K_0 \subseteq K_1 \subseteq K_2 \subseteq K_3,$$

splňující podmínky Definice 12.1 takovou, že K_3 obsahuje rozkladové nadtěleso $h(z)$, speciálně $k^2 \in K_3$. Položme $d_3 = k^2$ a $K_4 = K_3(\sqrt{d_3})$. Protože

$$2m = q + k^2 + \frac{r}{k},$$
$$2l = q + k^2 - \frac{r}{k},$$

leží v prvky k, l, m v tělese K_4. Nyní položme

$$K_5 = K_4(\sqrt{k^2 - 4l}) \quad \text{a} \quad K_6 = K_5(\sqrt{k^2 - 4m}).$$

Těleso K_6 obsahuje rozkladové nadtěleso polynomu $g(y)$ v K_0 a proto je rovnice (12.3) řešitelná pomocí radikálů.

Dvojici těles $T \subseteq S$ budeme nazývat *rozšíření* a značit S/T.

Definice 12.2. Buď S těleso. *Automorfismem* tělesa S rozumíme bijekci $\varphi : S \to S$ takovou, že pro každé a, $b \in S$ platí

(i) $\varphi(a + b) = \varphi(a) + \varphi(b)$,
(ii) $\varphi(ab) = \varphi(a)\varphi(b)$.

Buď S/T rozšíření. *T-automorfismem* tělesa S rozumíme automorfismus φ tělesa S takový, že $\varphi(a) = a$ pro každé $a \in T$ (tj. $\varphi \restriction T = \mathrm{id}_T$).

Lemma 12.3. *Buď S/T rozšíření, $f(x) \in T[x]$ polynom a φ T-automorfismus tělesa S. Je-li a kořen polynomu $f(x)$, je také $\varphi(a)$ kořenem polynomu $f(x)$.*

Definice 12.4. Buď S/T rozšíření. *Galoisova grupa* $\mathrm{Gal}(S/T)$ tohoto rozšíření je grupa všech T-automorfismů tělesa S s operací skládání. Je-li $f(x) \in T[x]$, budeme nazývat grupu $\mathrm{Gal}(T_f/T)$ *Galoisovou grupou polynomu $f(x)$ nad tělesem T.*

Lemma 12.5. *Buď $f(x) \in T[x]$ polynom a $A = \{a_1, a_2, \ldots, a_n\}$ množina všech jeho různých kořenů. Potom je zobrazení $\Phi : \mathrm{Gal}(T_f/T) \to S_A \simeq S_n$ určené předpisem $\Phi(\varphi) = \varphi \restriction A$ prostým grupovým homomorfismem. Tedy každý T-automorfismus tělesa T_f je jednoznačně určený jím indukovanou permutací kořenů polynomu $f(x)$.*

Lemma 12.6. *Nechť $K \subseteq T \subseteq S$ jsou tělesa taková, že S, T jsou rozkladová nadtělesa polynomů nad tělesem K. Potom je $\mathrm{Gal}(S/T) \triangleleft \mathrm{Gal}(S/K)$ a platí*

$$\mathrm{Gal}(S/K) \Big/ \mathrm{Gal}(S/T) \simeq \mathrm{Gal}(T/K).$$

Věta 12.7 (Galois 1831). *Nechť je $f(x) \in T[x]$ polynom stupně n nad tělesem T. Označme $G = \mathrm{Gal}(T_f/T)$ Galoisovu grupu polynomu $f(x)$ nad tělesem T. Rovnice $f(x) = 0$ je řešitelná pomocí radikálů nad tělesem T právě když existuje posloupnost*

$$1 = G_0 \leq G_1 \leq \cdots \leq G_t = G,$$

podgrup grupy G taková, že pro každé $i = 0, 1, \ldots, t-1$ je $G_i \triangleleft G_{i+1}$ a grupa G_{i+1}/G_i je cyklická, prvočíselného řádu.

Definice 12.8. *Normální řada* grupy G je posloupnost

$$1 = G_0 \leq G_1 \leq \cdots \leq G_t = G, \tag{12.4}$$

podgrup G taková, že pro každé $i = 0, 1, \ldots, t-1$ je $G_i \triangleleft G_{i+1}$.

Grupa G je *řešitelná*, jestliže exituje normální řada tvaru (12.4) taková, že faktorgrupy G_{i+1}/G_i, $i = 0, 1, \ldots, t-1$, jsou cyklické prvočíselného řádu.

Cvičení 12.1. *Ukažte, že podgrupa řešitelné grupy je opět řešitelná grupa.*

Pro grupy S_3, S_4 máme následující normální řady, které dokazují, že tyto grupy jsou řešitelné:

$$G_0 = 1 \leq G_1 = A_3 \leq G_2 = S_3$$

a

$$G_1/G_0 \simeq \mathbb{Z}_3,\ G_2/G_1 \simeq \mathbb{Z}_2;$$

$$G_0 = 1 \leq G_1 = \{\mathrm{id}, (1,2)(3,4)\} \leq G_2 = V \leq G_3 = A_4 \leq G_4 = S_3,$$

kde

$$V = \{\mathrm{id}, (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\}$$

a

$$G_1/G_0 \simeq \mathbb{Z}_2,\ G_2/G_1 \simeq \mathbb{Z}_2,\ G_3/G_2 \simeq \mathbb{Z}_3,\ G_4/G_3 \simeq \mathbb{Z}_2.$$

Důkaz následující věty naleznete například v [1, strana 60].

Věta 12.9. *Pro $n \geq 5$ nemá grupa A_n žádnou normální podgrupu.*

Důsledek 12.10. *Pro $n \geq 5$ není grupa A_n a tedy ani grupa S_n řešiteltelná.*

Lemma 12.11. *Buď $f(x) \in T[x]$ nerozložitelný polynom a buď a, b dvojice jeho kořenů. Buď S/T rozšíření takové, že a, $b \in S$. Potom existuje T-automorfismus φ tělesa S takový, že $\varphi(a) = b$.*

Tvrzení 12.12. *Buď $f(x) \in \mathbb{Q}[x]$ nerozložitelný polynom stupně 5, který má právě tři reálné kořeny. Potom je Galoisova grupu tohoto polynomu izomorfní grupě S_5.*

Cvičení 12.2. *Ukažte, že polynom $f(x) = x^5 - 4x + 2$ je nerozložitelný nad $\mathbb{Q}$, a že má právě tři reálné kořeny.*

Literatura:

1. A. G. Kuroš, *Kapitoly z obecné algebry*, Academia Praha, 1968 (1977).

HTTP://ADELA.KARLIN.MFF.CUNI.CZ/~RUZICKA/...
E-mail address: ruzicka@karlin.mff.cuni.cz