MV008 — Algebra I — Cvičení

Podstatná část příkladů je převzata od kolegů, jmenovitě Prof. Kučery, Doc. Poláka a Doc. Kunce, se kterými jsem v minulosti při přípravě cvičení spolupracoval. Sbírka vznikla modifikací sbírek, které používám při cvičení k předmětu Algebra I na PřF, který ovšem nemá úplně identický obsah.

Veškeré připomínky, opravy a komentáře jsou vítány na adrese `klima@math.muni.cz`.

Hvězdičkou jsou označeny doplňující úlohy, které přesahují sylaby předmětu nebo jsou obtížnější.

Sbírku budu aktualizovat, zejména ji doplním o příklady na látku z druhé poloviny semestru.

Ondřej Klíma

Verze z 12. prosince 2016

0 Opakování modulární aritmetiky (z předmětu MB104)

Příklad 0.1: Určete největšího společného dělitele dvojice čísel:
1) $2016, 2017$, 2) $1000, 1024$, 3) $153, 221$.

Příklad 0.2: Nalezněte koeficienty do Bezoutovy rovnosti pro dvojice čísel
1) $1000, 1024$, 2) $153, 221$, 3) $49, 225$.

Příklad 0.3*: Pro libovolné přirozené číslo k, určete největšího společného dělitele dvojice čísel:
1) $2^k + 1, 2^{2k} + 1$, 2) $k^3 - 1, k^2 - k + 1$.

Příklad 0.4*: Pro libovolné přirozené číslo k, určete koeficienty do Bezoutovy rovnosti pro dvojici k^3, $k^2 - 1$.

Příklad 0.5: Určete hodnotu Eulerovy funkce pro následující čísla n:
1) $n = 24$, 2) $n = 306$, 3) $n = 5225$.

Příklad 0.6: Ukažte, že pro libovolné $n > 2$ je $\varphi(n)$ sudé číslo.

Příklad 0.7*: Určete všechna přirozená čísla m, pro která platí $\varphi(m) = 18$.

Příklad 0.8*: Určete všechna přirozená čísla n taková, že $\varphi(n) \mid n$.

Příklad 0.9: Určete zbytek po dělení daných čísel číslem 17.
1) $2^{50} + 3^{50} + 4^{50}$, 2) $5^{40} + 6^{40} + 7^{40} + 8^{40}$, 3) $4^{4^4} + 5^{5^5}$, 4) $13^{13^{13}} + 15^{15^{15}}$.

Příklad 0.10: Ukažte, že číslo $2^{60} + 7^{30}$ je dělitelné číslem 13.

Příklad 0.11: Určete zbytek po dělení čísla $a^{9^9 - 3^{10}}$ číslem 44, pro $a = 8, 9, 10, 11$.

Příklad 0.12: Určete poslední dvě cifry čísla $15^{15^{15}}$.

Příklad 0.13: Určete poslední tři cifry čísla $15^{15^{15}}$.

Příklad 0.14: Určete poslední dvě cifry čísla $13^{13^{13}}$.

Příklad 0.15*: Dokažte, že pro libovolné $n \in \mathbb{N}$ je $2^{2^{2n+1}} + 3$ číslo složené.

Příklad 0.16*: Dokažte Čínskou zbytkovou větu: Nechť je dáno $k \in \mathbb{N}$ a k-tice $m_1, \cdots, m_k$ po dvou nesoudělných přirozených čísel. Pak pro libovolnou k-tici $c_1, \cdots, c_k$ přirozených čísel existuje $x \in \mathbb{N}$ takové, že $x \equiv c_i (\mathrm{mod}\, m_i)$ pro $i = 1, \ldots, k$. Navíc je toto x určeno jednoznačně $\mathrm{mod}\, m_1 \cdot \cdots \cdot m_k$; přesněji, všechna tato čísla dávají stejný zbytek po dělení číslem $m_1 \cdot \cdots \cdot m_k$.

1 Pologrupy

Příklad 1.1: Rozhodněte, zda dané předpisy zadávají operaci f na množině všech racionálních čísel $\mathbb{Q}$, případně na množině všech nenulových racionálních čísel $\mathbb{Q}^* = \mathbb{Q} - \{0\}$.

1) $f(x, y) = \frac{x}{y}$, pro $x, y \in \mathbb{Q}$,
2) $f(\frac{p}{q}, \frac{r}{s}) = \frac{p+r}{q+s}$, pro $p, q, r, s \in \mathbb{Z}$, $q \neq 0 \neq s$.
3) $f(x, y) = \sqrt{2} \cdot x + y$, pro $x, y \in \mathbb{Q}$,
4) $f(\frac{p}{q}, \frac{r}{s}) = \frac{p+r}{q+s}$, pro $p, r \in \mathbb{Z}$, $q, s \in \mathbb{N}$.
5) $f(\frac{p}{q}, \frac{r}{s}) = \frac{p}{q}$, pro $p, q, r, s \in \mathbb{Z}$, $q \neq 0 \neq s$.
6) $f(\frac{p}{q}, \frac{r}{s}) = \sqrt{\frac{p}{q}}$, pro $p, q, r, s \in \mathbb{Z}$, $q \neq 0 \neq s$.
7) $f(\frac{p}{q}, \frac{r}{s}) = \frac{p \cdot s}{q \cdot r}$, pro $p, q, r, s \in \mathbb{Z} \setminus \{0\}$.

Příklad 1.2: Rozhodněte, zda daný grupoid je pologrupa, případně monoid a zda je operace komutativní.

1) Celá čísla s operací sčítání.
2) Reálná čísla s operací násobení.
3) Celá čísla s operací odečítání.
4) Přirozená čísla s operací největší společný dělitel.

Příklad 1.3: Pro dané množiny matic typu 2 krát 2 nad reálnými čísly rozhodněte, zda je sčítání, resp. násobení, matic operací na této množině. Pokud se jedná o operaci, zjistěte, zda je operace asociativní či komutativní a zda obsahuje neutrální prvek.

1) Množina všech matic nad celými čísly.
2) Množina všech matic nad racionálními čísly.
3) Množina všech regulárních matic nad racionálními čísly.
4) Množina všech matic s nulou v levém dolním rohu a s jedničkami na diagonále.
5) Množina všech regulárních matic nad celými čísly.

Příklad 1.4: Pro množinu X značíme $\mathcal{P}(X)$ množinu všech podmnožin množiny X. Pro následující operace určete, zda grupoid $\mathcal{P}(X)$ je pologrupou, zda je operace komutativní a zda existuje neutrální prvek.

1) Průnik.
2) Sjednocení.
3) Množinový rozdíl. ($Y \setminus Z = \{x \in Y \mid x \notin Z\}$)
4) Symetricky rozdíl. ($Y \div Z = (Y \setminus Z) \cup (Z \setminus Y)$)

Příklad 1.5: Určete, zda operace na tříprvkové množině $\{a, b, c\}$ daná tabulkou je komutativní, asociativní a zda má neutrální prvek.

1)

$\circ$	a	b	c
a	b	a	a
b	a	b	a
c	a	a	a

2)

$\circ$	a	b	c
a	b	a	a
b	a	b	c
c	a	c	a

3)

$\circ$	a	b	c
a	a	a	a
b	b	b	b
c	c	c	c

Příklad 1.6*: Prvek e pologrupy $(G, \cdot)$ se nazývá idempotent, jestliže $e \cdot e = e$. Ukažte, že každá konečná pologrupa obsahuje aspoň jeden idempotent.

Příklad 1.7: Pro množinu X označme $\mathcal{R}(X)$ množinu všech relací na X, tj. $\mathcal{R}(X) = \mathcal{P}(X \times X)$. Na $\mathcal{R}(X)$ definujeme operaci $\circ$ takto:

$$\rho \circ \sigma = \{(x, y) \in X \times X \mid (\exists z \in X)((x, z) \in \sigma \wedge (z, y) \in \rho)\} .$$

Dokažte, že $(\mathcal{R}(X), \circ)$ je monoid.

Víme, že speciálním případem relací jsou zobrazení, pro které je operace $\circ$ skládání zobrazení. Označme $\mathcal{T}(X)$ množinu všech transformací množiny X (zobrazení z X do X), tj.

$$\mathcal{T}(X) = \{f \in \mathcal{R}(X) \mid (\forall x \in X)(\exists y \in X)((x, y) \in f \wedge (\forall y')((x, y') \in f \implies y' = y))\} .$$

Rozhodněte, zda je $(\mathcal{T}(X), \circ)$ monoid.

Podobně značíme $\mathcal{PT}(X)$ množinu všech parciálních transformací na X, tj.

$$\mathcal{PT}(X) = \{f \in \mathcal{R}(X) \mid (\forall x, y, z \in X)(((x, y) \in f \wedge (x, z) \in f) \implies y = z)\} .$$

(Všimněme si, že $\mathcal{T}(X) \subseteq \mathcal{PT}(X)$ a že prázdná relace patří do $\mathcal{PT}(X)$.)

Rozhodněte, zda je $\mathcal{PT}(X)$ podpologrupa/podmonoid pologrupy/monoidu $(\mathcal{R}(X), \circ)$.

Příklad 1.8: Uvažujme monoid všech transformací množiny přirozených čísel: $(\mathcal{T}(\mathbb{N}), \circ)$. Rozhodněte, zda dané podmnožiny tvoří podpologrupu, resp. podmonoid.

1) I – podmnožina všech injektivních zobrazení z $\mathbb{N}$ do $\mathbb{N}$.
2) S – podmnožina všech surjektivních zobrazení z $\mathbb{N}$ do $\mathbb{N}$.
3) B – podmnožina všech bijektivních zobrazení z $\mathbb{N}$ do $\mathbb{N}$.
4) $C = \{f \in \mathcal{T}(\mathbb{N}) \mid f(1) = 1\}$.
5) $D = \{f \in \mathcal{T}(\mathbb{N}) \mid f^2 = id_{\mathbb{N}}\}$.
6) $E = \{f \in \mathcal{T}(\mathbb{N}) \mid \forall n \in \mathbb{N} : f(n) > n\}$.
7) $F = \{f \in \mathcal{T}(\mathbb{N}) \mid \forall n \in \mathbb{N} : 2 | f(n) - n\}$.
8) $G = \{f \in \mathcal{T}(\mathbb{N}) \mid \forall n \in \mathbb{N} : 2 \not| f(n) - n\}$.

Příklad 1.9: Uvažujme monoidy všech matic 2 krát 2 nad reálnými čísly $(Mat_2(\mathbb{R}), +)$ a $(Mat_2(\mathbb{R}), .)$. Pro každou podmnožinu množiny $Mat_2(\mathbb{R})$ z následujícího seznamu rozhodněte, zda tvoří podpologrupu, resp. podmonoid $(Mat_2(\mathbb{R}), +)$ či $(Mat_2(\mathbb{R}), .)$.

1) $M_1 = Mat_2(\mathbb{Q})$.
2) $M_2 = \{A \in Mat_2(\mathbb{R}) \mid |A| = 0\}$.
3) $M_3 = \{A \in Mat_2(\mathbb{R}) \mid |A| \neq 0\}$.
4) $M_4 = \{A \in Mat_2(\mathbb{R}) \mid |A| \in \mathbb{Q}\}$.
5) $M_5 = \{A \in Mat_2(\mathbb{R}) \mid |A| > 1\}$.
6) $M_6 = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \mid a, b, d \in \mathbb{R} \right\}$.
7) $M_7 = \left\{ \begin{pmatrix} a & 0 \\ c & d \end{pmatrix} \mid a, c, d \in \mathbb{R} \right\}$.

8) $M_8 = \left\{ \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} \mid a, d \in \mathbb{R} \right\}$.

9) $M_9 = \left\{ \begin{pmatrix} a & b \\ c & 0 \end{pmatrix} \mid a, b, c \in \mathbb{R} \right\}$.

V případě 8) zkuste využít odpovědí z části 6) a 7).

Příklad 1.10: Doplňte následující tabulku operace na tříprvkové množině tak, aby výsledný grupoid byl pologrupou.

$\circ$	a	b	c
a	b	a	c
b			
c			

Příklad 1.11: Následující tabulku je možno jediným způsobem doplnit na tabulku operace $\cdot$ v pologrupě $(S, \cdot)$, kde $S = \{a, b, c, d, e, f\}$.

$\cdot$	a	b	c	d	e	f
a	a	b	c	d		f
b	b	e	c	d	b	f
c	c	c	f	c	c	d
d	d		c	d	d	f
e	e	b	c	d	e	f
f	f	f	d	f	f	c

1) Určete, kterému prvku z množiny S se rovná $d \cdot b$, resp. $a \cdot e$, v pologrupě $(S, \cdot)$.

2)* Určete všechny idempotenty.

3)* Vypište všechny pravé neutrální prvky.

4)* Vypište všechny levé nulové prvky.

5) Lze původní tabulku doplnit tak, aby byla operace $\cdot$ v grupoidu $(S, \cdot)$ komutativní?

Příklad 1.12*: V monoidu $\mathcal{T}(X)$ z příkladu 1.7. určete počet všech idempotentů.

Příklad 1.13*: V monoidu matic $(Mat_2(\mathbb{R}), \cdot)$ typu 2 krát 2 nad reálnými čísly s operací násobení matic určete všechny idempotenty. (Zkuste kromě aritmetického postupu zapojit i geometrickou představu a znalosti z MB101.)

Příklad 1.14*: Dokažte, že pro pologrupu $(S, \cdot)$ jsou následující podmínky ekvivalentní:

(i) $(\forall a, b \in S)\ a \cdot b \cdot a = a$,

(ii) $(\forall a \in S)\ a \cdot a = a \quad \wedge \quad (\forall a, b, c \in S)\ a \cdot b \cdot c = a \cdot c$,

(iii) $(\forall a, b \in S)\ a \cdot b = b \cdot a \implies a = b$.

Poznamenejme, že pologrupa splňující tyto podmínky se nazývá rektangulární band.

Příklad 1.15*: Buď A konečná abeceda a uvažujme množinu všech jazyků nad A, tj. množinu $\mathcal{P}(A^*)$. Podmnožiny této množiny tvořené všemi regulárními, resp. všemi bezkontextovými jazyky, označíme $\mathcal{REG}(A)$, resp. $\mathcal{CF}(A)$. Rozhodněte, zda $\mathcal{REG}(A)$, resp. $\mathcal{CF}(A)$, jsou podmonoidy monoidů $(\mathcal{P}(A^*), \cdot)$, $(\mathcal{P}(A^*), \cup)$, resp. $(\mathcal{P}(A^*), \cap)$. Pokud je pro Vás příklad příliš jednoduchý, uvažujte podmnožinu tvořenou lineárními jazyky (to jsou jazyky dané bezkontextovou gramatikou, kde každé pravidlo na pravé straně obsahuje nejvýše jeden neterminál) nebo si zvolte svoji vlastní složitější třídu jazyků.

Příklad 1.16: Určete podpologrupu pologrupy $(\mathbb{N}, +)$, resp. $(\mathbb{N}, \cdot)$, generovanou dvojicí prvků 5 a 7. Totéž pro dvojici 10 a 15 a dvojici 12 a 18.

Příklad 1.17: uvažujme množinu $Mat_2(\mathbb{R})$ všech matic typu 2 krát 2 nad reálnými čísly. V pologrupách $(Mat_2(\mathbb{R}), +)$, resp. $(Mat_2(\mathbb{R}), \cdot)$, určete podpologrupy generované následující množinou prvků X.

1) $X = \left\{ \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \right\}$,

2) $X = \left\{ \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} \right\}$,

3) $X = \left\{ \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \right\}$,

4) $X = \left\{ \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \right\}$,

5) $X = \left\{ \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \right\}$.

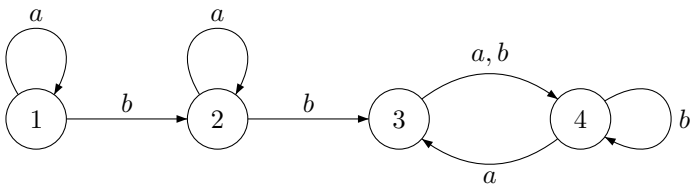
Příklad 1.18: Buď $(S, \cdot)$ pologrupa a $M = \{m_1, m_2, \ldots, m_k\}$ její neprázdná konečná podmnožina taková, že její prvky po dvou komutují (tj. platí $\forall s, t \in M : s \cdot t = t \cdot s$). Dokažte, že potom podpologrupa generovaná množinou M je rovna množině

$$\{m_1^{\epsilon_1} m_2^{\epsilon_1} \ldots m_k^{\epsilon_k} \mid \epsilon_1, \epsilon_2, \ldots, \epsilon_k \in \mathbb{N}_0, \epsilon_1 + \epsilon_2 + \cdots + \epsilon_k > 0\}.$$

Příklad 1.19: Určete všechny konečné podpologrupy pologrupy: 1) $(\mathbb{R}, \cdot)$, 2)$^*(\mathbb{C}, \cdot)$.

Příklad 1.20: Určete podmonoid monoidu $\mathcal{T}(\{1, 2, 3\})$ generovaný prvky f a g, kde transformace jsou zadány takto: $f(1) = 2, f(2) = 1, f(3) = 2, g(1) = 2, g(2) = 3, g(3) = 3$.

Příklad 1.21: Určete všechny prvky přechodového monoidu následujícího automatu.



Příklad 1.22: Dokažte, že zobrazení $\alpha : (\mathbb{C}, \cdot) \to (Mat_2(\mathbb{R}), \cdot)$ dané předpisem $\alpha(a + bi) = \begin{pmatrix} a & -b \\ b & a \end{pmatrix}$, pro libovolná $a, b \in \mathbb{R}$, je injektivní homomorfismus pologrup.

Příklad 1.23: Určete, které z následujících předpisů zadávají homomorfismus φ z pologrupy $(Mat_2(\mathbb{R}), +)$, resp. $(Mat_2(\mathbb{R}), \cdot)$, do pologrupy $(\mathbb{R}, +)$, resp. $(\mathbb{R}, \cdot)$.

1) $\varphi(A) = |A|$, kde $|A|$ značí determinant matice A,

2) $\varphi(A) = tr(A)$, kde $|A|$ značí stopu matice A, tj. $tr(\begin{pmatrix} a & b \\ c & d \end{pmatrix}) = a + d$,

3) $\varphi(\begin{pmatrix} a & b \\ c & d \end{pmatrix}) = a$, pro $a, b, c, d \in \mathbb{R}$,

4) $\varphi(\begin{pmatrix} a & b \\ c & d \end{pmatrix}) = a + 3b - 4c - d$, pro $a, b, c, d \in \mathbb{R}$,

5) $\varphi(\begin{pmatrix} a & b \\ c & d \end{pmatrix}) = a^2$, pro $a, b, c, d \in \mathbb{R}$.

Pokud se jedná o homomorfismus pologrup, rozhodněte, zda se jedná i o homomorfismus monoidů. Rozmyslete si dále, zda je zobrazení injektivní, surjektivní či dokonce bijektivní.

Příklad 1.24: Rozhodněte, zda zadané zobrazení je homomorfismem příslušných pologrup nebo monoidů.

1) $\alpha : (\mathbb{Z}, +) \to (\mathbb{N}_0, +)$, $\alpha(n) = |n|$.

2) $\beta : (\mathbb{N}, +) \to (\mathbb{C}, \cdot)$, $\beta(n) = i^n$.

3) $\gamma : (\mathcal{P}(\mathbb{N}), \cap) \to (\mathcal{P}(\mathbb{N}), \cup)$, $\gamma(X) = X^c = \mathbb{N} \setminus X$.

4) $\delta : (\mathbb{N}, \cdot) \to (\mathbb{N}, \cdot)$, $\delta(n) = n^2$.

5) $\epsilon : (\mathbb{N}, \mathrm{nsd}) \to (\mathbb{N}, \mathrm{nsd})$, $\epsilon(n) = n^2$.

6) $\zeta : (A^*, \cdot) \to (A^*, \cdot)$, $\zeta(u) = u^2$, kde A je konečná abeceda a u libovolné slovo.

7) $\eta : (\mathcal{P}(A), \div) \to (\mathbb{N}_0, +)$, $\eta(X) = |X|$. Zde A je konečná množina a $|X|$ značí počet prvků množiny X.

8) $\theta : (\mathcal{P}(A), \div) \to (\mathbb{Z}_2, +)$, $\theta(X) = [|X|]_2$. Zde A je konečná množina a $|X|$ značí počet prvků množiny X.

Pokud je odpověď pozitivní, tj. jedná se o homomorfismus, rozhodněte, zda je zobrazení také izomorfismus.

Příklad 1.25: Rozhodněte, zda jsou následující dvojice pologrup izomorfní.

1) $(\mathbb{C}, \cdot)$ a $(\mathbb{R}, \cdot)$.

2) $(\mathbb{R}, \cdot)$ a $(\mathbb{Z}, +)$.

3) $(\mathbb{N}, +)$ a $(\mathbb{N}, \cdot)$.

4) $(\mathbb{N}, +)$ a $(\mathbb{Z}^-, +)$, kde $\mathbb{Z}^-$ je množina všech záporných celých čísel.

5) $(\mathbb{Q}, +)$ a $(\mathbb{Q}, \cdot)$.

6) $(\mathbb{Q}, \cdot)$ a $(\mathbb{R}, \cdot)$.

7) $(\{0, 1\}, \cdot)$ a $(\mathcal{P}(\{0\}), \cup)$.

8) $(Mat_2(\mathbb{R}), +)$ a $(\mathbb{C}, \cdot)$.

9) $(Mat_2(\mathbb{R}), +)$ a $(\mathbb{R}, \cdot)$.

10)* $(\mathbb{N}, \cdot)$ a $(\mathbb{L}, \cdot)$, kde $\mathbb{L}$ je množina všech lichých přirozených čísel.

11) $(\{a\}^+, \cdot)$ a $(\mathbb{N}, +)$.

12) $(S, \cdot)$ a $(\{a, b, c, d\}^+, \cdot)$, kde S je podpologrupa pologrupy $(\{a, b\}^+, \cdot)$ tvořená slovy sudé délky.

Příklad 1.26: Dejte příklad injektivního homomorfismu z pologrupy $(\mathbb{N}, +) \times (\mathbb{N}, +)$ do pologrupy $(\mathbb{N}, \cdot)$.

Příklad 1.27*: Dejte příklad izomorfismu z pologrupy $(\mathbb{N}, \cdot) \times (\mathbb{N}, \cdot)$ do pologrupy $(\mathbb{N}, \cdot)$.

Příklad 1.28: Dokažte, že neexistuje injektivní homomorfismus z pologrupy $(\mathbb{N}, +) \times (\mathbb{N}, +)$ do pologrupy $(\mathbb{Z}, +)$.

Příklad 1.29*: Dokažte, že neexistuje injektivní homomorfismus z pologrupy $(\mathbb{N},+)\times(\mathbb{N},+)$ do pologrupy $(\{a,b\}^+,\cdot)$.

Příklad 1.30: Nalezněte injektivní homomorfismus

1) z pologrupy $(\{a,b,c\}^+,\cdot)$ do pologrupy $(\{a,b\}^+,\cdot)$;
2) z pologrupy $(\mathbb{Z},+)$ do pologrupy $(Mat_2(\mathbb{R}),+)$;
3) z pologrupy $(\mathbb{Z},+)$ do pologrupy $(Mat_2(\mathbb{R}),\cdot)$;
4) z pologrupy $(\mathbb{N},\cdot)$ do pologrupy $(Mat_2(\mathbb{R}),+)$;
5) z pologrupy $(\mathbb{N},\cdot)$ do pologrupy $(Mat_2(\mathbb{R}),\cdot)$.

Příklad 1.31: U každého z následujících předpisů (kde $a,b\in\mathbb{Z}$, $x,y\in\mathbb{N}$, $p,q\in\mathbb{Z}\setminus\{0\}$) rozhodněte, zda zadává zobrazení. Pokud ano, rozhodněte, zda se jedná o homomorfismus či dokonce izomorfismus pologrup. Určete dále, které z nich jsou homomorfismy či dokonce izomorfismy monoidů.

$$\alpha,\overline{\alpha}:(\mathbb{Z}_4,+)\times(\mathbb{Z}_3,+)\to(\mathbb{Z}_{12},+)$$

$$\alpha(([a]_4,[b]_3))=[6a+4b]_{12}$$
$$\overline{\alpha}(([a]_4,[b]_3))=[a-b]_{12}$$

$$\beta:(\mathbb{N}_0,+)\times(\mathbb{N},\cdot)\to(\mathbb{N},\cdot)$$
$$\beta((x,y))=y^x$$

$$\gamma:(\mathbb{Q}\setminus\{0\},\cdot)\to(\mathbb{Q}\setminus\{0\},\cdot)$$
$$\gamma(p/q)=q/p$$

$$\delta:(\mathbb{Z}_{15},\cdot)\to(\mathbb{Z}_5,\cdot)\times(\mathbb{Z}_3,\cdot)$$
$$\delta([a]_{15})=([a]_5,[a]_3)$$

Příklad 1.32*: Určete všechny dvouprvkové pologrupy (až na izomorfismus, tj. přejmenování prvků).

2 Grupy

2.1 Definice a základní vlastnosti

Příklad 2.1: Rozhodněte, zda daný grupoid $(G,\circ)$ je grupa.

1) G je množina nenulových racionálních čísel a operace $\circ$ je dána předpisem $x\circ y=|x\cdot y|$.
2) G je interval $\langle 0,1)$ a operace $\circ$ je dána předpisem $x\circ y=x+y-[x+y]$, kde $[z]$ značí celou část z čísla z, tj. největší celé číslo menší nebo rovno z.
3) G je množina celých čísel a operace $\circ$ je dána předpisem $x\circ y=x+(-1)^x y$.
4) $G=\mathbb{R}\times\mathbb{R}-\{(0,0)\}$ je množina všech dvojic reálných čísel z nichž aspoň jedno je nenulové, a operace $\circ$ je dána předpisem $(x,y)\circ(u,v)=(xu-yv,xv+yu)$.
5) $G=(\mathbb{R}-\{0\})\times\mathbb{R}$ je množina uspořádaných dvojic reálných čísel, přičemž první z nich není 0, a operace $\circ$ je dána předpisem $(x,y)\circ(u,v)=(xu,xv+y)$.

6) G je množina komplexních čísel, jejichž reálná i imaginární část je celočíselná, a operace $\circ$ je sčítání komplexních čísel.

7) $G = \mathbb{R}$ je množina všech reálných čísel a operace $\circ$ je dána vztahem

$$x \circ y = \begin{cases} -xy, & x < 0, y < 0 \\ |xy|, & \text{jinak} \end{cases} \qquad \text{pro } x, y \in \mathbb{R}.$$

8) $G = \{(a, b) \in \mathbb{R} \times \mathbb{R} \mid a^2 + b^2 = 1\}$ a operace $\circ$ je dána předpisem $(a, b) \circ (c, d) = (ad + bc, bd - ac)$ pro $(a, b), (c, d) \in G$.

9) $G = \{(a, b) \in \mathbb{R} \times \mathbb{R} \mid a^2 + b^2 \geq 1\}$ a operace $\circ$ je dána předpisem $(a, b) \circ (c, d) = (ad + bc, bd - ac)$ pro $(a, b), (c, d) \in G$.

10) $G = \{(a, b) \in \mathbb{Z} \times \mathbb{Z} \mid a^2 - 5b^2 = 1\}$ a operace $\circ$ je dána předpisem $(a, b) \circ (a', b') = (aa' + 5bb', ab' + a'b)$ pro $(a, b), (a', b') \in G$.

Příklad 2.2: Popište multiplikativní tabulku grupy $(\mathbb{Z}_n^\times, \cdot)$ pro následující n:
1) $n = 5$, 2) $n = 7$, 3) $n = 8$.

Příklad 2.3: Spočtěte 1) $[4]_{15}^{-1}$ v $\mathbb{Z}_{15}^\times$, 2) $[17]_{181}^{-1}$ v $\mathbb{Z}_{181}^\times$, 3) $[49]_{226}^{-1}$ v $\mathbb{Z}_{226}^\times$, 4) $[49]_{225}^{-1}$ v $\mathbb{Z}_{225}^\times$, 5) $[125]_{1296}^{-1}$ v $\mathbb{Z}_{1296}^\times$.

Příklad 2.4:

1) Dokažte, že v libovolné grupě platí tzv. *zákony o krácení*

$$(\forall a, b, c)\ (ab = ac \implies b = c) \quad \wedge \quad (\forall a, b, c)\ (ba = ca \implies b = c)\ .$$

2) Popište, jak lze z multiplikativní tabulky operace poznat, že v grupoidu platí zákony o krácení.

3)* Dokažte, že konečná pologrupa, v které platí zákony o krácení, je grupa.

4) Udejte příklad nekonečné pologrupy, která není grupou, ale platí v ní zákony o krácení.

5) Udejte příklad tříprvkového grupoidu, který není grupou, ale platí v něm zákony o krácení. Ukažte, že grupoid není pologrupou.

6) Udejte příklad pětiprvkového grupoidu s neutrálním prvkem, který není grupou, ale platí v něm zákony o krácení. Ukažte, že grupoid není pologrupou.

Příklad 2.5: Určete, kolik je dvouprvkových, resp. tříprvkových, resp. čtyřprvkových grup (až na izomorfismus, tj. přejmenování prvků).

Příklad 2.6: Dokažte, že v konečné grupě o sudém počtu prvků existuje prvek, který je inverzní k sobě samému a není to neutrální prvek.

Příklad 2.7: Doplňte tabulku operace $*$ tak, aby vznikla grupa $(\{a, b, c\}, *)$:

$\circ$	a	b	c
a			
b	c	a	
c			

Příklad 2.8: Nechť $(G, \circ)$ je grupa a a nějaký její pevně zvolený prvek. Dokažte, že potom $(G, \square)$ je také grupa, kde operace $\square$ je definována předpisem $g \square h = g \circ a \circ h$.

Příklad 2.9*: Dokažte, že grupy jsou právě ty pologrupy, pro něž platí:

$$(\forall a, b)\ (\exists x, y)\ (ax = b,\ ya = b)\ .$$

2.2 Grupa permutací

Příklad 2.10: Nechť

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

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

1) Rozložte permutace s, t, u na součin nezávislých cyklů.
2) Spočtěte součiny $s \circ t$, $t \circ s$, $s \circ u \circ t$. Použijte jak "dvojřádkový"zápis, tak rozklad na nezávislé cykly.
3) Spočtěte $s^3, s^{20}, t^{53}, t^{103}, u^{211}$.
4) Určete inverzní prvky s^{-1}, t^{-1}, u^{-1}.
5) Spočtěte permutace $(s^{120} \circ t^{-3})^{17} \circ u^{23}$ a $(u^{-23} \circ s)^{134} \circ t^4$.
6) Permutace s, t, u rozložte na součin transpozic a určete jejich paritu.

Příklad 2.11: Napište permutace $f = (2,3,4,5) \circ (1,3,6,8)$ a $g = (1,4,6) \circ (2,7,4,8,3) \circ (1,5)$ jako součin 10 transpozic.

Příklad 2.12: Dokažte že permutace $(s^3 \circ t^{-17})^{18} \circ s^{10}$ je sudá permutace pro libovolné permutace $s, t \in \mathbb{S}_9$.

Příklad 2.13: Rozhodněte, zda existuje permutace $s \in \mathbb{S}_9$ taková, že $s \circ (1,2,3) = (1,2) \circ s$.

Příklad 2.14: Určete všechny permutace a z grupy $\mathbb{S}_8$ takové, že $a^2 = (1,2,3)(4,5,6)$. Podobně určete b takové, že $b^4 = (1,2,3,4,5,6,7)$, c takové, že $c^3 = (1,2,3,4)(5,6,7,8)$, d takové, že $d^2 = (1,2,3,4)(5,6,7,8)$ a e takové, že $e^2 = (1,2,3,4)$.

Příklad 2.15: Určete všechny permutace f z grupy $\mathbb{S}_8$ takové, že $f^3 = (1,2)(3,4)(5,6)$.

Příklad 2.16: Určete, pro která přirozená čísla $n \in \mathbb{N}$ existuje permutace $s \in \mathbb{S}_6$ taková, že $s \circ (1,2,3,4,5) \circ s = (1,2)^n$. Pro tato n popište všechny takové permutace s.

Příklad 2.17: Buď $a \in \mathbb{S}_m$ cyklus délky n.Dokažte, že pro libovolné $k \in \mathbb{N}$ platí:

1) $a^k = id$ právě když n dělí k,
2) pokud n nedělí k pak je a^k součinem d nezávislých cyklů délky $\frac{n}{d}$, kde d je největší společný dělitel n a k.

Příklad 2.18*:

1) Ukažte, že libovolnou permutaci v $\mathbb{S}_n$ lze rozložit na součin transpozic tvaru $(1, i)$.
2) Ukažte, že libovolnou sudou permutaci v $\mathbb{S}_n$ lze rozložit na součin cyklů tvaru $(1, 2, i)$.

Příklad 2.19*: Ukažte, že libovolnou permutaci v $\mathbb{S}_n$ lze rozložit na součin cyklů $(1,2)$ a $(1,2,\ldots,n)$.

Příklad 2.20*: Dokažte, že pro každou konečnou množinu X existuje trojice f, g, h transformací této množiny taková, že podmnožina $\{f, g, h\}$ generuje celou pologrupu $\mathcal{T}(X)$.

Příklad 2.21*: Určete, které prvky $a \in \mathbb{S}_n$ lze psát ve tvaru b^2c^2 pro vhodné $b, c \in \mathbb{S}_n$.

2.3 Řád prvku

Příklad 2.22: Určete řád permutace $(1,2,4,5) \circ (3,7,8) \circ (6,9)$ resp. $(1,2,4,5,3,6,7,9) \circ (3,7,8) \circ (6,2,9)$.

Příklad 2.23: Určete největší $k \in \mathbb{N}$ takové, že v grupě $\mathbb{S}_{10}$ existuje prvek řádu k.

Příklad 2.24: Nalezněte nějaké $k \in \mathbb{N}$ takové, že v grupě $\mathbb{S}_{15}$ existuje prvek řádu k, ale v grupě $\mathbb{S}_{14}$ prvek řádu k neexistuje.

Příklad 2.25: Určete řád prvku $[k]_n$ v grupě $(\mathbb{Z}_n, +)$.

Příklad 2.26: Určete řády všech prvků v grupě $(\mathbb{Z}_n^\times, \cdot)$ pro $n = 7, 8, 12, 13$.

Příklad 2.27: Určete řády prvků $[2]_{17}$ a $[13]_{17}$ v $(\mathbb{Z}_{17}^\times, \cdot)$.

Příklad 2.28: V $GL_2(\mathbb{Z}_3)$ (grupa regulárních matic nad $\mathbb{Z}_3$) určete řády prvků $\begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}$ a $\begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}$.

2.4 Podgrupy

Příklad 2.29: Ukažte, že podmnožina kladných reálných čísel, resp. kladných racionálních čísel, resp. $\mathbb{Q}(\sqrt{3}) = \{a + b\sqrt{3} \mid a, b \in \mathbb{Q}, a^2 + b^2 > 0\}$ je podgrupa grupy $(\mathbb{R}^*, \cdot)$.

Příklad 2.30: Ukažte, že množina sudých permutací tvoří podgrupu grupy $\mathbb{S}_n$ pro libovolné $n \in \mathbb{N}$.

Příklad 2.31: Popište všechny podgrupy grupy $(\mathbb{Z}_{10}, +)$.

Příklad 2.32: Popište všechny podgrupy grupy $(\mathbb{Z}, +)$.

Příklad 2.33: Popište všechny podgrupy grupy $(\mathbb{Z}_n, +)$.

Příklad 2.34: Popište všechny podgrupy grupy $\mathbb{S}_3$, respektive grupy $\mathbb{A}_4$.

Příklad 2.35*: Popište všechny podgrupy grupy symetrií $\mathbb{D}_n$ (alespoň pro $n = 3, 4$).

Příklad 2.36: Uvažujme grupu $(\mathbb{S}_\mathbb{N}, \circ)$ všech permutací množiny $\mathbb{N}$. Rozhodněte, zda dané podmnožiny tvoří podgrupu grupy $(\mathbb{S}_\mathbb{N}, \circ)$:

1) $H_1 = \{f \in \mathbb{S}_\mathbb{N} \mid \forall n \in \mathbb{N} : f(n) > n\}$.
2) $H_2 = \{f \in \mathbb{S}_\mathbb{N} \mid f^2 = id\}$.
3) $H_3 = \{f \in \mathbb{S}_\mathbb{N} \mid \exists n \in \mathbb{N} : f^n = id\}$.
4) $H_4 = \{f \in \mathbb{S}_\mathbb{N} \mid \forall n \in \mathbb{N} : f(2n) = 2n\}$.

Příklad 2.37: Pro libovolnou podmnožinu X množiny $\mathbb{N}$ označíme dvě podmnožiny $\mathbb{S}_\mathbb{N}$ takto:

$$S_X = \{f \in \mathbb{S}_\mathbb{N} \mid \forall x \in X : f(x) = x\}, \quad T_X = \{f \in \mathbb{S}_\mathbb{N} \mid \forall x \in \mathbb{N} : x \in X \iff f(x) \in X\}.$$

Rozhodněte, zda podmnožina S_X, resp. T_X, tvoří podgrupu grupy $(\mathbb{S}_\mathbb{N}, \circ)$.

Příklad 2.38: Určete podgrupu $\mathbb{S}_8$ generovanou množinou X:

1) $X = \{(4,5,2,1) \circ (4,6,3,1,5,2), (4,5,2,1) \circ (4,5,6) \circ (2,1,3)\}$,

2) $X = \{(1,5,8) \circ (1,4,2,5) \circ (1,5,2), (1,2,6,4,8,5) \circ (1,4,6,2)\}$,

3) $X = \{(1,8,2,3,5) \circ (1,2,6,7,8), (4,7,6,2) \circ (2,4,8)\}$,

4) $X = \{(1,2)(3,4), (2,3)(4,5)\}$.

5)* $X = \{(2,4,6), (4,7,2), (3,2,4)\}$.

Příklad 2.39*: Určete podgrupu $\mathbb{S}_n$ generovanou množinou $\{(1,2), (1,2,3,\ldots,n)\}$.

Příklad 2.40: V $(\mathbb{Z}, +)$ určete podgrupu generovanou množinou $\{8, 30\}$.

Příklad 2.41: V $(\mathbb{Z}_{60}, +)$ určete podgrupu generovanou množinou $\{[6]_{60}, [15]_{60}\}$. Podobně v $(\mathbb{Z}_{50}, +)$ určete podgrupu generovanou množinou $\{[24]_{50}, [30]_{50}\}$.

Příklad 2.42: V grupě $(\mathbb{R}, +)$, resp. $(\mathbb{R}^*, \cdot)$, určete podgrupu generovanou prvkem $\sqrt[3]{2}$.

Příklad 2.43: Nechť je dána grupa G a její dvě podgrupy H a K. Dokažte, že

$$\langle H \cup K \rangle = \{a_1 b_1 \ldots a_n b_n \mid n \in \mathbb{N}, a_i \in H, b_i \in K\}.$$

2.5 Homomorfismy a izomorfismy grup

Příklad 2.44: Dokažte, že $(\mathbb{Z}_7^\times, \cdot)$ je izomorfní s $(\mathbb{Z}_6, +)$ a $(\mathbb{Z}_8^\times, \cdot)$ je izomorfní s $(\mathbb{Z}_2, +) \times (\mathbb{Z}_2, +)$. (Ukažte, že předpis $f([a]_6) = [3]_7^a$ definuje izomorfismus $f : (\mathbb{Z}_6, +) \to (\mathbb{Z}_7^\times, +)$.)

Příklad 2.45: U homomorfismů z příkladu 1.23 určete jádro a obraz homomorfismu a rozmyslete si znovu otázku, zda je dané zobrazení izomorfismem..

Příklad 2.46: Dokažte, že předpis $f([a]_{20}) = (1,2,3,4,5)^a$ definuje homomorfismus grup $f : (\mathbb{Z}_{20}, +) \to (\mathbb{S}_7, \circ)$. Určete jeho jádro a obraz.

Příklad 2.47: Nechť $f : G \to H$ je izomorfismus grup. Ukažte, že řády prvků a a $f(a)$ jsou stejné. Co lze říci o řádech prvků a a $f(a)$ v případě, že $f : G \to H$ je (injektivní) homomorfismus?

Příklad 2.48: Popište všechny homomorfismy z grupy $(\mathbb{Z}_3, +)$ do grupy $(\mathbb{A}_4, \circ)$.

Příklad 2.49: Popište všechny injektivní homomorfismy z grupy $(\mathbb{Z}_2, +) \times (\mathbb{Z}_2, +)$ do grupy $(\mathbb{A}_4, \circ)$, respektive $(\mathbb{S}_4, \circ)$.

Příklad 2.50: Pro libovolnou grupu $(G, \cdot)$ označme $\mathrm{Aut}(G) = \{f : G \to G \mid f \text{ izomorfismus}\}$ množinu všech automorfismů grupy G a $\mathrm{End}(G) = \{f : G \to G \mid f \text{ homomorfismus}\}$ množinu všech endomorfismů grupy G. Ukažte, že $(\mathrm{End}(G), \circ)$, kde $\circ$ je skládání zobrazení, je monoid a $\mathrm{Aut}(G)$ je podmnožina invertibilních prvků, tj. $(\mathrm{Aut}(G), \circ)$ je grupa.

Příklad 2.51: Popište všechny endomorfismy a automorfismy grupy $(\mathbb{Z}, +)$. Určete, čemu je izomorfní monoid $\mathrm{End}(\mathbb{Z})$ a grupa $\mathrm{Aut}(\mathbb{Z})$.

Příklad 2.52: Popište všechny endomorfismy a automorfismy grupy $(\mathbb{Z}_n, +)$. Určete, čemu je izomorfní monoid $\mathrm{End}(\mathbb{Z}_n)$ a grupa $\mathrm{Aut}(\mathbb{Z}_n)$.

Příklad 2.53*: Pro libovolnou dvojici čísel $n, k \in \mathbb{N}$ popište všechny homomorfismy z grupy $(\mathbb{Z}_n, +)$ do grupy $(\mathbb{Z}_k, +)$.

Příklad 2.54: Dokažte, že zobrazení $f : G \to G$ definované předpisem $f(x) = x^{-1}$ je izomorfismus právě tehdy, když grupa G je komutativní.

Příklad 2.55: Dokažte, že pro libovolné grupy G a H jsou grupy $G \times H$ a $H \times G$ izomorfní.

Příklad 2.56: Uvažme grupu $(G, \cdot)$ matic typu 3 krát 3 nad $\mathbb{Z}$, které jsou v horním trojúhelníkovém tvaru s jedničkami na hlavní diagonále, tj.

$$G = \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \mid a, b, c \in \mathbb{Z} \right\} ,$$

kde $\cdot$ je násobení matic. Definujme nyní zobrazení $f : (G, \cdot) \to (\mathbb{Z}, +)$, které matici

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

přiřadí číslo $a - c$. Dokažte, že zobrazení f je homomorfismus grup.

Příklad 2.57*: Nechť $X = \{1, \ldots, n\}$. Ukažte, že grupa $(P(X), \div)$ z příkladu 1.4-4 je izomorfní grupě $(\mathbb{Z}_2^n, +)$. ($(\mathbb{Z}_2^n, +)$ je součin n kopií grupy $(\mathbb{Z}_2, +)$.)

Příklad 2.58*: Nechť $(G, \cdot)$ je grupa.

i) Dokažte, že pro libovolný prvek $a \in G$ je zobrazení ρ_a automorfismus grupy G, kde $\rho_a : G \to G$ je definováno vztahem $\rho_a(x) = axa^{-1}$. (Hovoříme o vnitřních automorfismech.)

ii) Ukažte, že množina všech vnitřních automorfismů $\mathrm{Inn}(G) = \{\rho_a \mid a \in G\}$ je podgrupa grupy $(\mathrm{Aut}(G), \circ)$.

iii) Dokažte, že zobrazeni $\rho : G \to \mathrm{Aut}(G)$ dané předpisem $\rho(a) = \rho_a$ je homomorfismus grup.

Příklad 2.59: Buď α homomorfismus grupy $(\mathbb{Z}_{30}, +)$ do grupy $(\mathbb{Z}_{20}, +)$ definovaný předpisem $\alpha([a]_{30}) = [6a]_{20}$. Dále nechť β je homomorfismus grupy $(\mathbb{Z}_{20}, +)$ do grupy $(\mathbb{S}_5, \circ)$ daný předpisem $\beta([b]_{20}) = (1, 2, 3, 4, 5)^b$. Určete jádra homomorfismů α, β a $\beta \circ \alpha$.

Příklad 2.60: U následujících předpisů (kde $a, b \in \mathbb{Z}$, $s \in \mathbb{S}_6$) rozhodněte, zda zadávájí zobrazení. Pokud ano, rozhodněte, zda se jedná o homomorfismus či dokonce izomorfismus grup. Odpovědi zdůvodněte!

1) $\alpha : (\mathbb{Z}_2, +) \times (\mathbb{Z}_5, +) \to (\mathbb{Z}_{10}, +)$, $\alpha(([a]_2, [b]_5)) = [a + b]_{10}$;
2) $\alpha : (\mathbb{Z}_2, +) \times (\mathbb{Z}_5, +) \to (\mathbb{Z}_{10}, +)$, $\alpha(([a]_2, [b]_5)) = [5a + 2b]_{10}$;
3) $\alpha : (\mathbb{Z}_4, +) \to (\mathbb{C}^*, \cdot)$, $\alpha([a]_4) = i^a$;
4) $\alpha : (\mathbb{Z}_5, +) \to (\mathbb{C}^*, \cdot)$, $\alpha([a]_5) = i^a$;

$\beta : (\mathbb{S}_6, \circ) \to (\mathbb{S}_6, \circ)$, $\beta(s) = (1, 2) \circ s \circ (1, 2)$.
$\beta : (\mathbb{S}_6, \circ) \to (\mathbb{S}_6, \circ)$, $\beta(s) = s^2$.
$\beta : (\mathbb{Z}, +) \to (\mathbb{Z}_3, +)$, $\beta(a) = [|a|]_3$.
$\beta : (\mathbb{Z}, +) \to (\mathbb{Z}_2, +)$, $\beta(a) = [|a|]_2$.

Příklad 2.61: U následujících předpisů (kde $p, q \in \mathbb{Z}$, $q \neq 0 \neq p$) rozhodněte zda zadávájí zobrazení. Pokud ano, rozhodněte, zda se jedná o homomorfismus či dokonce izomorfismus grup. Odpovědi zdůvodněte!

1) $\alpha : (\mathbb{Q}^*, \cdot) \to (\mathbb{Q}^*, \cdot)$, $\alpha(\frac{p}{q}) = \frac{p^3}{q^3}$,
2) $\beta : (\mathbb{Q}^*, \cdot) \to (\mathbb{Q}^*, \cdot)$, $\beta(\frac{p}{q}) = (-1)^{pq} \cdot \frac{p}{q}$,
3) $\gamma : (\mathbb{Q}^*, \cdot) \to (\mathbb{Q}^*, \cdot)$, $\gamma(\frac{p}{q}) = (-1)^{p(p+q)q} \cdot \frac{q}{p}$.

Příklad 2.62*: Ukažte, že libovolná podgrupa grupy $\mathbb{S}_n$, která není podgrupou grupy $\mathbb{A}_n$, obsahuje právě polovinu sudých permutací a má tudíž sudý počet prvků.

2.6 Konečné komutativní grupy

Příklad 2.63: Určete všechny (až na izomorfismus) komutativní grupy, které mají $n = 24$ prvků. Totéž pro $n = 18, 24, 30, 36$.

Příklad 2.64: Pro libovolnou dvojici přirozených čísel m, n dokažte, že předpis $\alpha([a]_{m\cdot n}) = ([a]_n, [a]_m)$ zadává homorfismus z grupy $\mathbb{Z}_{mn}$ do grupy $\mathbb{Z}_n \times \mathbb{Z}_m$. Rozhodněte, pro která m, n je α izomorfismus.

Příklad 2.65: Určete, pro které dvojice čísel m, n jsou grupy $\mathbb{Z}_{mn}$ a $\mathbb{Z}_n \times \mathbb{Z}_m$ izomorfní.

Příklad 2.66: Určete rozklad grupy $(\mathbb{Z}_{21}^\times, \cdot)$ na součin netriviálních cyklických grup. Dejte příklad příslušného izomorfismu. Totéž pro $(\mathbb{Z}_{34}^\times, \cdot)$ a $(\mathbb{Z}_{40}^\times, \cdot)$.

Příklad 2.67: Dokažte, že grupa, v níž pro každý prvek x platí $x \cdot x = 1$, je komutativní.

2.7 Normální podgrupy

Příklad 2.68: Pro libovolné $n \in \mathbb{N}$ je $\mathbb{A}_n$ normální podgrupa grupy $\mathbb{S}_n$. Dokažte.

Příklad 2.69: Popište všechny normální podgrupy grup $(\mathbb{S}_3, \circ)$ a $(\mathbb{A}_4, \circ)$. (Povšimněte si, že existuje normální podgrupa N grupy H — normální podgurpy grupy $(\mathbb{A}_4, \circ)$ — která není normální podgrupou $(\mathbb{A}_4, \circ)$.)

Příklad 2.70: Označme následující podgrupy grupy $(\mathbb{S}_6, \circ)$: $G = \{f \in \mathbb{S}_6 \mid f \text{ sudá}\}$ a $H = \{f \in G \mid f(3) = 3\}$, tj. $H \subseteq G \subseteq \mathbb{S}_6$. Rozdodněte, zda
a) H je normální podgrupa grupy $(G, \circ)$;
b) H je normální podgrupa grupy $(\mathbb{S}_6, \circ)$;
c) G je normální podgrupa grupy $(\mathbb{S}_6, \circ)$.
Odpovědi zdůvodněte!

Příklad 2.71*: Nechť $n \in \mathbb{N}$, $n > 4$. Dokažte, že $\mathbb{A}_n$ nemá vlastní normální podgrupy a že je to jediná netriviální normální podgrupa $\mathbb{S}_n$.

Příklad 2.72: Uvažme grupu $(\mathbb{GL}_2(\mathbb{Q}), \cdot)$ regulárních matic dva krát dva nad racionálními čísly. Buďte dále G, H a N následující množiny matic:

$$G = \left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \mid a \in \mathbb{Q}^*, b \in \mathbb{Q} \right\}, \quad H = \left\{ \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \mid a, b \in \mathbb{Q}^* \right\}, \quad N = \left\{ \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \mid a \in \mathbb{Q}^* \right\}.$$

Určete, zda se jedná o normální podgrupy grupy $(\mathbb{GL}_2(\mathbb{Q}), \cdot)$.

Příklad 2.73: Buď dána následující grupa $(G, \cdot)$ matic ve speciálním tvaru s operací násobení matic a její podgrupa H:

$$G = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \mid a, c \in \mathbb{R}^*, b \in \mathbb{R} \right\}, \qquad H = \left\{ \begin{pmatrix} a & 0 \\ 0 & c \end{pmatrix} \mid a, c \in \mathbb{R}^* \right\}.$$

Dokažte, že H je podgrupa grupy $(G, \cdot)$. Rozhodněte, zda H je normální podgrupa $(G, \cdot)$. Odpověď zdůvodněte!

Příklad 2.74*: Dokažte, že množina vnitřních automorfismů $\mathrm{Inn}(G)$ v 2.56 je normální podgrupa grupy všech automorfismů $\mathrm{Aut}(G)$.

Příklad 2.75: Buď dána grupa $(G, \circ)$ nekonstantních afinních zobrazení reálných čísel

$$G = \{f : \mathbb{R} \to \mathbb{R} \mid f(x) = ax + b, \text{ pro vhodná } a \in \mathbb{R}^*, b \in \mathbb{R}\}$$

s operací skládání zobrazení $\circ$. Uvažme v této grupě dvě podgrupy:

$$T = \{f : \mathbb{R} \to \mathbb{R} \mid f(x) = ax, a \in \mathbb{R}^*\},$$

$$S = \{f : \mathbb{R} \to \mathbb{R} \mid f(x) = x + b, b \in \mathbb{R}\}.$$

Která z nich je normální podgrupou grupy $(G, \circ)$? Popište u obou pravý i levý rozklad.

Příklad 2.76: Popište pravé a levé rozklady grupy $\mathbb{S}_3$ podle všech podgrup.

Příklad 2.77: Popište levý rozklad grupy $(\mathbb{A}_4, \circ)$ sudých permutací na množině $\{1, 2, 3, 4\}$ podle podgrupy generované permutací $(2, 1, 4)$.

Příklad 2.78: Určete počet levých tříd grupy $(\mathbb{Z}, +) \times (\mathbb{Z}, +)$ podle podgrupy $H = \{(m, n) \ ; \ 6 \mid (m - 2n)\}$.

Příklad 2.79: Nechť konečná grupa $(G, \cdot)$ má sudý počet prvků $2n$ a H je její n prvková podgrupa. Dokažte, že H je normální podgrupa grupy $(G, \cdot)$.

2.8 Faktorizace grup

Příklad 2.80: Určete faktorgrupu z příkladu 2.73.

Příklad 2.81: Faktorizujte grupu $\mathbb{Z}$ podgrupou $k\mathbb{Z} = \{ka \mid a \in \mathbb{Z}\}$.

Příklad 2.82: Faktorizujte grupu $\mathbb{Z}_n$ podgrupou $k\mathbb{Z}_n = \{kz \mid z \in \mathbb{Z}_n\} = \{[kz]_n \mid z \in \mathbb{Z}\}$, kde k dělí n.

Příklad 2.83: Víme, že množina

$$G = \left\{ \begin{pmatrix} \varepsilon & a \\ 0 & 1 \end{pmatrix} \mid \varepsilon \in \{1, -1\}, a \in \mathbb{Z} \right\}$$

společně s operací násobení matic tvoří grupu $(G, \cdot)$. Označme

$$H = \left\{ \begin{pmatrix} 1 & 2b \\ 0 & 1 \end{pmatrix} \mid b \in \mathbb{Z} \right\}$$

podmnožinu G. Ukažte, že H je normální podgrupa grupy G. Popište rozklad G/H, tj. charakterizujte, kdy dvě matice $\begin{pmatrix} \varepsilon & a \\ 0 & 1 \end{pmatrix}$ a $\begin{pmatrix} \varepsilon' & a' \\ 0 & 1 \end{pmatrix}$ náleží do stejné třídy rozkladu. Určete počet tříd rozkladu G/H. Určete, které grupě $(K, \cdot)$ je izomorfní faktorgrupa G/H, tj. popište grupu $(K, \cdot)$ a definujte vhodné zobrazení $\alpha : G \to K$ pro něž dokažte, že α je surjektivní homomorfismus grup, jehož jádrem je H.

Příklad 2.84: Uvažme množiny reálných čísel $G = \{15^p 5^q \mid p, q \in \mathbb{Z}\}$ a $H = \{3^r \mid r \in \mathbb{Z}\}$ a operaci $\cdot$ (násobení reálných čísel). Zřejmě $(G, \cdot)$ je grupa.

1. Ukažte, že H je normální podgrupa grupy $(G, \cdot)$.
2. Pro $p, \overline{p}, q, \overline{q} \in \mathbb{Z}$ doplňte podmínku $(\cdots)$ tak, aby platilo:

$$15^p 5^q \text{ a } 15^{\overline{p}} 5^{\overline{q}} \text{ náleží do stejné třídy rozkladu } {}^{G}\!/_{H} \iff \cdots.$$

3. Určete, které grupě je izomorfní faktorgrupa G/H, tj. popište grupu $(K, \cdot)$ a definujte vhodné zobrazení $\alpha : G \to K$, pro něž dokažte, že α je surjektivní homomorfismus grup, jehož jádrem je H.

Řešte stejné zadání pro množinu $H_1 = \{45^r \mid r \in \mathbb{Z}\}$ a $H_2 = \{25^r 27^s \mid r, s \in \mathbb{Z}\}$.

Příklad 2.85: Uvažme množiny reálných čísel $G = \{2^p 3^q 5^r \mid p, q, r \in \mathbb{Z}\}$ a $H = \{20^x \mid x \in \mathbb{Z}\}$ a operaci $\cdot$ (násobení reálných čísel). Zřejmě $(G, \cdot)$ je grupa.

1. Ukažte, že H je normální podgrupa grupy $(G, \cdot)$.
2. Pro $p, \overline{p}, q, \overline{q}, r, \overline{r} \in \mathbb{Z}$ doplňte podmínku $(\cdots)$ tak, aby platilo:

$$2^p 3^q 5^r \text{ a } 2^{\overline{p}} 3^{\overline{q}} 5^{\overline{r}} \text{ náleží do stejné třídy rozkladu } {}^{G}\!/_{H} \iff \cdots.$$

3. Určete, které grupě je izomorfní faktorgrupa G/H, tj. popište grupu $(K, \cdot)$ a definujte vhodné zobrazení $\alpha : G \to K$, pro něž dokažte, že α je surjektivní homomorfismus grup, jehož jádrem je H.

Řešte stejné zadání pro množinu $H = \{8^x 15^y \mid x, y \in \mathbb{Z}\}$.

Příklad 2.86: Faktorizujte aditivní grupu komplexních čísel podgrupou všech reálných čísel. $((\mathbb{C}, +)/\mathbb{R} \cong ?)$

Příklad 2.87: Určete, čemu je izomorfní faktorgrupa regulárních matic nad reálnými čísly podle podgrupy matic jejichž determinant je roven 1. $(\mathbb{GL}_n(\mathbb{R})/\mathbb{SL}_n(\mathbb{R}) \cong ?)$

Příklad 2.88: Nechť je dána grupa matic

$$G = \left\{ \begin{pmatrix} a & 0 \\ b & c \end{pmatrix} \mid a, c \in \mathbb{Q}^*, b \in \mathbb{Q} \right\}$$

s operací nasobení. Dokažte, že podgrupa

$$H = \left\{ \begin{pmatrix} a & 0 \\ b & c \end{pmatrix} \mid a, b, c \in \mathbb{Q}, a, c > 0 \right\}$$

je normální a určete faktorgrupu.

Příklad 2.89: Uvažujme normální podgrupu grupy $(G, +) = (\mathbb{Z}, +) \times (\mathbb{Z}, +)$ definovanou takto:

$$(a) : H = \{(a, b) \in \mathbb{Z} \times \mathbb{Z}; 5 \mid a, 2 \mid b\},$$

$$(b) : H = \{(a, b) \in \mathbb{Z} \times \mathbb{Z}; 7 \mid 2a + 3b\},$$

Určete, které grupě je izomorfní faktorgrupa G/H, tj. popište grupu $(K, \cdot)$ a definujte vhodné zobrazení $\alpha : G \to K$, pro něž dokažte, že α je surjektivní homomorfismus grup, jehož jádrem je H.

Příklad 2.90*: V příkladu 2.67 jsme spočítali jednu netriviální normální podgrupu v $\mathbb{S}_4$ resp. $\mathbb{A}_4$, označme ji $\mathbb{V}_4$. Spočtete příslušné faktorgrupy. $(\mathbb{S}_4/\mathbb{V}_4 \cong ?, \mathbb{A}_4/\mathbb{V}_4 \cong ?)$

Příklad 2.91*: Dokažte, že až na izomorfismus existují pouze dvě $2p$ prvkové grupy a popište je. (Zde p je prvočíslo.)

Příklad 2.92*: Určete faktorgrupy z příkladu 2.70.

2.9 Doplňující příklady z teorie grup

Příklad 2.93*:

i) Ukažte, že libovolný automorfismu grupy $\mathbb{S}_n$ zachovává paritu permutace.

ii) Dokažte, že pro $n > 2$ je grupa vnitřních automorfismů $\mathrm{Inn}(\mathbb{S}_n)$ izomorfní grupě $\mathbb{S}_n$.

iii) Dokažte, že $\mathrm{Aut}(\mathbb{S}_n) \cong \mathbb{S}_n$ pro $n = 3, 4, 5$.

Příklad 2.94*: Buď $(G,\cdot)$ komutativní grupa. Ukažte, že pro dané $n \in \mathbb{N}$ tvoří množina $G_n = \{a \in G \mid a^n = 1\}$ podgrupu grupy $(G,\cdot)$. Ukažte dále, že množina všech prvků konečného řádu $\overline{G} = \bigcup_{n=1}^{\infty} G_n = \{a \in G \mid \exists n \in \mathbb{N} : a^n = 1\}$ je taktéž podgrupou grupy $(G,\cdot)$.

Příklad 2.95*: Nechť je dána grupa G a její dvě podgrupy H a K. Definujme nyní podmnožinu HK grupy G:

$$HK = \{hk \mid h \in H,\ k \in K\}.$$

Dokažte, že pokud je K normální podgrupa grupy G, potom je podmnožina HK podgrupou grupy G. Dále dokažte, že pokud jsou obě podgrupy H i K normální, potom je normální i podgrupa HK.

Příklad 2.96*: Nechť $(G,\cdot)$ je grupa, $n \in \mathbb{N}$ a předpokládejme, že grupa G obsahuje jedinný prvek řádu n (označme jej a). Dokažte, že tento prvek komutuje s libovolným prvkem grupy G, tj. $xa = ax$ pro libovolné $x \in G$.

Příklad 2.97*: Nechť G je grupa a označme G' podgrupu generovanou množinou prvků tvaru $[x,y] = x^{-1}y^{-1}xy$, tj.

$$G' = \{[x_1,y_1][x_2,y_2]\dots[x_n,y_n] \mid n \in \mathbb{N}, x_i, y_i \in G\}.$$

i) Dokažte, že G' je normální podgrupa grupy G.

ii) Ukažte, že faktorgrupa G/G' je komutativní grupa.

iii) Ukažte, že G/G' je „největší“ komutativní faktorgrupa grupy G, tj. ukažte, že pokud H je normální podgrupa grupy G taková, že G/H je komutativní grupa, potom $G' \subseteq H$.

iv) Určete „největší“ komutativní faktorgrupu pro grupu

$$G = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \mid a, c \in \mathbb{Q}^*, b \in \mathbb{Q} \right\}.$$

Totéž pro $\mathbb{GL}_2(\mathbb{Q})$.

Příklad 2.98*:

i) Nechť $(G,\cdot)$ a $(H,\star)$ jsou grupy a nechť $\varphi : (H,\star) \to (\mathrm{Aut}(G),\circ)$ je homomorfismus grup. Definujme na $G \times H$ operaci $\diamond$ vztahem: $(a,b) \diamond (c,d) = (a \cdot \varphi(b)(c), b \star d)$. Dokažte, že $(G \times H, \diamond)$ je grupa.

ii) Ukažte, že součin grup $(G,\cdot) \times (H,\star)$ je speciálním případem $(G \times H, \diamond)$ pro vhodné φ.

iii) Nechť $(G,\cdot)$ je grupa. Definujme na $G \times G$ operaci $\diamond$ vztahem: $(a,b) \diamond (c,d) = (abcb^{-1}, bd)$. Dokažte, že $(G \times G, \diamond)$ je grupa.

Příklad 2.99*: Ukažte, že libovolná konečná grupa je izomorfní s podgrupou grupy $\mathbb{A}_n$ pro vhodné $n \in \mathbb{N}$.

3 Polynomy nad $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ a $\mathbb{C}$

3.1 Dělení v okruzích polynomů, Euklidův aloritmus, Bezoutova rovnost

Příklad 3.1: V $\mathbb{Q}[x]$ dělte se zbytkem polynomy
a) $(x^5 + x^3 - 2x + 1) : (-x^3 + x + 1)$,
b) $(3x^3 + 10x^2 + 2x - 3) : (5x^2 + 25x + 30)$,
c) $(12x^4 + 3x^3 - 4x + 3) : (2x^2 - 1)$,
d) $(x^6 + x^4 + x^2 + 1) : (x^2 - x + 1)$.

Příklad 3.2: V $\mathbb{Q}[x]$ dělte se zbytkem polynomy:
a) $(2x^3 + 3x^2 - 4x + 5) : (x - 2)$,
b) $(4x^4 - 3x^2 - x + 2) : (3x + 1)$.

Příklad 3.3: Nalezněte polynomy $f(x), g(x) \in \mathbb{Q}[x]$, které jsou stupně 3, každý z nich má alespoň jeden alespoň dvojnásobný kořen a jejich největší společný dělitel je:
a) $x^2 + x - 6$,
b) $x^2 + x - 2$,
c) $x^2 + 2x - 3$.
Vyjádřete největší společný dělitel polynomů f, g Bezoutovou rovností.

Příklad 3.4: Nalezněte polynomy $f(x), g(x) \in \mathbb{Q}[x]$, které jsou stupně 4, každý z nich má alespoň jeden alespoň trojnásobný kořen a jejich největší společný dělitel je:
a) $x^2 + x - 2$,
b) $x^2 + 2x - 3$,
c) $x^2 - 2x - 3$.
Vyjádřete největší společný dělitel polynomů f, g Bezoutovou rovností.

Příklad 3.5: Pro dané dvojice polynomů $f, g \in \mathbb{R}[x]$ najděte normovaný polynom, který je jejich největším společným dělitelem. Najděte koeficienty do příslušné Bezoutovy rovnosti.
a) $f = x^4 + 1, g = x^3 - 1$
b) $f = x^4 + 3x^3 - x^2 - 4x - 3, g = 3x^3 + 10x^2 + 2x - 3$
c) $f = x^5 - 5x^4 + 4x^3 + 8x^2 - 8x - 3, g = x^4 - 2x^3 - 7x^2 + 8x + 3$

3.2 Kořeny polynomů

Příklad 3.6: Uvažme polynom $f(x) = x^6 - 6x^5 + 9x^4 + 8x^3 - 24x^2 + 16 \in \mathbb{Q}[x]$. Dokažte, že $c = 2$ je kořenem polynomu f a určete jeho násobnost n.

Příklad 3.7: Určete hodnotu koeficientu $a \in \mathbb{Q}$ tak, aby polynom $f = x^5 - ax^2 - ax + 1 \in \mathbb{Q}[x]$ měl dvojnásobný kořen $c = -1$.

Příklad 3.8: Dokažte, že pro každé $n \in \mathbb{N}$ je $c = 1$ dvojnásobným kořenem polynomu $nx^{n+1} - (n+1)x^n + 1 \in \mathbb{Z}[x]$.

3.3 Taylorův rozvoj polynomu

Příklad 3.9: Vyjádřete polynom $f(x) = x^4 + 2x^3 - 3x^2 - 4x + 1$ v mocninách lineárního polynomu $x + 1$.

Příklad 3.10: Vyjádřete polynom $f(x) = (x - 2)^4 + 4(x - 2)^3 + 6(x - 2)^2 + 10(x - 2) + 20$ bez počítání jednotlivých mocnin polynomu $x - 2$.

3.4 Racionální kořeny polynomů

Příklad 3.11: Nalezněte všechny racionální kořeny polynomu v $\mathbb{C}[x]$ a určete jejich násobnost.
a) $12x^6 + 8x^5 - 85x^4 + 15x^3 + 55x^2 + x - 6$
b) $4x^7 - 16x^6 + x^5 + 55x^4 - 35x^3 - 38x^2 + 12x + 8$
c) $4x^7 - 23x^5 + 17x^4 + 31x^3 - 49x^2 + 24x - 4$
d) $2x^7 - 3x^6 - 20x^5 - x^4 + 66x^3 + 91x^2 + 48x + 9$
e) $4x^5 + 8x^4 - 27x^3 - 79x^2 - 56x - 12$
f) $4x^5 - 35x^3 + 15x^2 + 40x + 12$
g) $x^3 - \frac{5}{6}x^2 - \frac{1}{2}x + \frac{1}{3}$
h) $5x^3 - 8x^2 + 11x + 6$
i) $12x^4 - 7x^3 - 19x^2 - 3x + 2$

j) $3x^5 - x^4 + \frac{1}{3}x^3 - \frac{8}{3}x^2 + \frac{4}{3}x$
k) $6x^4 + x^3 + x^2 - 16x - 12$
l) $9x^6 - 21x^5 - 17x^4 + 15x^3 - 42x^2 - 34x - 6$
m) $4x^6 - 12x^5 + 9x^4 - 12x^2 + 36x - 27$
n) $2x^7 - 3x^6 - 8x^5 + 6x^4 + 10x^3 + x^2 + 4x + 4$
o) $x^4 + x^3 - 2x^2 - 3x - 1$
p) $x^5 - 4x^4 + 4x^3 + 2x^2 - 5x + 2$
q) $f = 12x^7 - 56x^6 + 115x^5 - 141x^4 + 103x^3 - 35x^2 - 3x + 9$
r) $g = 8x^7 - 44x^6 + 70x^5 - 17x^4 - 24x^3 + 10x^2 + 2x - 1$

Příklad 3.12: Určete takové $a \in \mathbb{C}$, pro něž má polynom $f = 2x^6 - x^5 - 11x^4 - x^3 + ax^2 + 2ax + 8 \in \mathbb{C}[x]$ kořen 2. Pro toto a určete všechny racionální kořeny polynomu f včetně násobností.

Příklad 3.13: Určete všechna $a \in \mathbb{Z}$, pro něž má polynom $x^4 + 2x^3 - 3x^2 + ax - 4$ racionální kořen.

3.5 Komplexní kořeny polynomů

Příklad 3.14: Určete všechna komplexní řešení rovnice $x^n = 2$ pro $n \in \mathbb{N}$.

Příklad 3.15: Nalezněte rovnici, jejíž všechna komplexní řešení tvoří v Gaussově rovině rovnostranný trojúhelník se středem v nule a jedním vrcholem v i.

Příklad 3.16: Řešte v $\mathbb{C}$ kvadratickou rovnici $x^2 + (1 + 3i)x + i - 2 = 0$.

Příklad 3.17: Určete všechna komplexní řešení rovnice $x^4 + x^3 + x^2 + x + 1 = 0$.

3.6 Rozklad polynomů

Příklad 3.18: Napište rozklad polynomu na součin ireducibilních faktorů postupně nad $\mathbb{Q}, \mathbb{R}, \mathbb{C}$:
a) $x^3 - \frac{5}{6}x^2 - \frac{1}{2}x + \frac{1}{3}$
b) $5x^3 - 8x^2 + 11x + 6$
c) $12x^4 - 7x^3 - 19x^2 - 3x + 2$
d) $3x^5 - x^4 + \frac{1}{3}x^3 - \frac{8}{3}x^2 + \frac{4}{3}x$
e) $6x^4 + x^3 + x^2 - 16x - 12$
f) $4x^6 - 12x^5 + 9x^4 - 12x^2 + 36x - 27$
g) $9x^6 - 21x^5 - 17x^4 + 15x^3 - 42x^2 - 34x - 6$

Příklad 3.19: Napište rozklady na součin ireducibilních polynomů postupně nad $\mathbb{C}, \mathbb{R}, \mathbb{Q}$ těch polynomů z Příkladu 3.11, u kterých znáte dostatek racionálních kořenů.

Příklad 3.20: Určete všechny kořeny polynomu f, víte-li, že má tři kořeny racionální. Rozložte f na ireducibilní faktory postupně nad $\mathbb{Q}, \mathbb{R}, \mathbb{C}$:
a) $f(x) = 4x^5 - 4x^4 - 5x^3 - 7x^2 + x + 2 \in \mathbb{C}[x]$,
b) $f(x) = 4x^5 - 12x^4 - 13x^3 - 13x^2 + 3x + 4 \in \mathbb{C}[x]$.

3.7 Komplexně sdružené kořeny

Příklad 3.21: Určete všechny kořeny polynomu $f = x^7 - 4x^6 + 8x^5 - 7x^4 + 8x^2 - 8x + 4 \in \mathbb{C}[x]$, víte-li, že má dvojnásobný kořen $1 + i$. Rozložte tento polynom na ireducibilní faktory postupně nad $\mathbb{Q}, \mathbb{R}, \mathbb{C}$.

Příklad 3.22: Mezi všemi normovanými polynomy s reálnými koeficienty, které mají jednoduchý kořen $-\frac{1}{3}$ a dvojnásobný kořen $3 + 2i$, nalezněte polynom nejmenšího stupně. Rozložte tento polynom na ireducibilní polynomy nad $\mathbb{Q}, \mathbb{R}, \mathbb{C}$.

Příklad 3.23: Určete všechny kořeny polynomu $f = x^6 - 7x^5 + 20x^4 - 30x^3 + 37x^2 - 55x + 50 \in \mathbb{C}[x]$, víte-li, že má dvojnásobný kořen $2 - i$. Rozložte jej na ireducibilní faktory postupně nad $\mathbb{Q}, \mathbb{R}, \mathbb{C}$.

Příklad 3.24: Mezi všemi normovanými polynomy s reálnými koeficienty, které mají dvojnásobný kořen $\frac{1}{2}$ a dvojnásobný kořen k nalezněte polynom nejmenšího stupně. Zapište rozklad tohoto polynomu na ireducibilní faktory postupně nad $\mathbb{Q}, \mathbb{R}, \mathbb{C}$:
a) $k = 1 - i$,
b) $k = 1 - 2i$.

Příklad 3.25: Nalezněte všechny kořeny polynomu $x^4 + 4x^2 + x + 6 \in \mathbb{C}[x]$ a určete jejich násobnost, víte-li, že jedním z kořenů je číslo $\frac{-1+i\sqrt{7}}{2}$.

Příklad 3.26: Víme, že polynom $f = 4x^6 - 4x^5 + 4x^4 - 4x^3 + 5x^2 - 3x + 1 \in \mathbb{C}[x]$ má dvojnásobný kořen $\frac{1}{2} + \frac{1}{2}i$. Určete zbývající kořeny polynomu f.

Příklad 3.27: Uveďte příklad polynomu v $\mathbb{R}[x]$, resp. v $\mathbb{Z}[x]$, jehož kořenem je
a) $1 + i$,
b) $2 + \sqrt{3}i$,
c) $\sqrt{3} - 5i$.

3.8 Eisensteinovo kritérium a ireducibilita nad $\mathbb{Q}$

Příklad 3.28: Ukažte, že polynom $f(x)$ je ireducibilní nad $\mathbb{Q}$:
a) $f(x) = x^n + p$; $n \in \mathbb{N}$, p je prvočíslo,
b) $f(x) = x^6 + x^3 + 1$.

Příklad 3.29: Najděte $n \in \mathbb{N}$ takové, že polynom $x^2 - n$ je ireducibilní nad $\mathbb{Q}$, ale nesplňuje podmínku Eisensteinova kritéria.

Příklad 3.30: Najděte $n \in \mathbb{N}$ tak, aby polynom $p(x) = x^n + n$
a) byl ireducibilní nad $\mathbb{Q}$,
b) nebyl ireducibilní nad $\mathbb{Q}$.

Příklad 3.31: Určete, který z polynomů $f(x) = x^5 + 3x^3 - 9x + 3 \in \mathbb{Z}[x]$ a $g(x) = x^4 + 4x^3 + 5x^2 - 3 \in \mathbb{Z}[x]$ je ireducibilní nad $\mathbb{Z}$ a který lze nad $\mathbb{Z}$ rozložit na součin polynomů nižšího stupně. Napište rozklady polynomů f a g na ireducibilní faktory nad $\mathbb{Z}$.

Příklad 3.32: Dokažte, že polynom $x^4 + x^3 + x^2 + x + 1$ je ireducibilní nad $\mathbb{Q}$. *Návod: Použijte Taylorův rozvoj ve vhodném bodě.*

Příklad 3.33: Dokažte, že polynom $x^4 + x + 1$ je ireducibilní nad $\mathbb{Q}$. *Návod: Použijte metodu neurčitých koeficientů.*

3.9 Minimální polynom

Příklad 3.34: Určete minimální polynomy prvku $\sqrt{2 + \sqrt{2}}$ nad $\mathbb{Q}$ a nad $\mathbb{Q}(\sqrt{2})$.

Příklad 3.35: Určete minimální polynomy prvků nad $\mathbb{Q}$:

$$\alpha = \sqrt[3]{4} + \sqrt[3]{2} - 1, \quad \beta = \sqrt{\sqrt{2 + \sqrt{2}} + \sqrt{2}}, \quad \gamma = \sqrt{2} + \sqrt{3}, \quad \delta = \sqrt{7 + 4\sqrt{3}} + \sqrt{7 - 4\sqrt{3}}.$$

Příklad 3.36: Určete minimální polynom prvku $\sqrt{7 + 4\sqrt{3}}$ nad $\mathbb{Q}$.

Příklad 3.37: Určete minimální polynom prvku $\sqrt[3]{16+8\sqrt{5}}$ nad $\mathbb{Q}$.

Příklad 3.38: Určete minimální polynom prvku $\cos\frac{2\pi}{3}+i\sin\frac{2\pi}{3}=\xi_3$ nad $\mathbb{Q}$.

Příklad 3.39: Určete minimální polynomy prvků nad $\mathbb{Q}$:

$$\alpha=\sqrt[3]{3}-1,\quad \beta=\sqrt{2}+\sqrt{3}+\sqrt{6},\quad \gamma=\sqrt{2}i+\sqrt[6]{2}i,\quad \delta=\sqrt{7}i.$$

4 Okruhy a tělesa

4.1 Okruh, podokruh

Příklad 4.1: Rozhodněte, zda $(M,\oplus,\odot)$ je okruh:
a) $M=\mathbb{Z}, x\oplus y=x+y-1, x\odot y=x\cdot y-1$
b) $M=\mathbb{Z},\ x\oplus y=x+y-1,\ x\odot y=x+y-xy$
c) $M=\mathbb{Q}$, operace jako v b)
d) $M=\mathbb{Q}\times\mathbb{Q},\ (x,y)\oplus(u,v)=(x+u,y+v),\ (x,y)\odot(u,v)=(xu+2yv,xv+yu)$
e) $M=\mathbb{Z}_2\times\mathbb{Z}_2,\ (x,y)\oplus(u,v)=(x+u,y+v),\ (x,y)\odot(u,v)=(xu+yv,xv+yu+yv)$

Příklad 4.2: Nechť $(R,+,\cdot)$ je komutativní okruh. Rozhodněte, zda je okruh také
a) $(R,+,\square)$, kde $\square$ je operace definovaná vztahem $a\square b=a\cdot b+b\cdot a$ pro libovolné $a,b\in R$,
b) $(R,+,+)$.

Příklad 4.3: Rozhodněte, zda daná množina M je podokruhem okruhu $(\mathbb{C},+,\cdot)$:
a) $M=\{a+2i\mid a\in\mathbb{R}\}$,
b) $M=\{a+2i\mid a\in\mathbb{C}\}$,
c) $M=\{a+bi\mid a\in\mathbb{R},b\in\mathbb{N}\}$,
d) $M=\{3a+bi\mid a\in\mathbb{Z},b\in\mathbb{Z}\}$,
e) $M=\{a+2bi\mid a\in\mathbb{Z},b\in\mathbb{Z}\}$,
f) $M=\{\frac{a}{2^k}\mid a\in\mathbb{Z},k\in\mathbb{N}\}$.

Příklad 4.4: Rozhodněte, zda daná podmnožina A okruhu racionálních čísel $(\mathbb{Q},+,\cdot)$ je okruh, případně obor integrity. Jde-li o okruh, charakterizujte jeho invertibilní prvky.
a) $A=\{\frac{p}{q}\mid p\in\mathbb{Z},q\in\mathbb{N},3\nmid q\}$
b) $A=\{\frac{m}{3^n}\mid m\in\mathbb{Z},n\in\mathbb{N}\}$
c) $A=\{\frac{m}{6^n}\mid m\in\mathbb{Z},n\in\mathbb{N}\}$

Příklad 4.5: Určete, které prvky náleží nejmenšímu podokruhu okruhu $(\mathbb{C},+,\cdot)$ obsahujícímu číslo a pro
a) $a=\sqrt{3}$,
b) $a=\sqrt[5]{2}$,
c) $a=i$,
d) $a=\cos\frac{2\pi}{3}+i\sin\frac{2\pi}{3}=\xi_3$,
e) $a=\cos\frac{2\pi}{7}+i\sin\frac{2\pi}{7}=\xi_7$,
f) $a=\pi$,
g) $a=\sqrt{n}$,
h) $a=\sqrt[3]{n}$,
i) $a=\sqrt{n}i$.

4.2 Homomorfismy okruhů

Příklad 4.6: Rozhodněte, zda zobrazení $f : \mathbb{C} \to \mathbb{C}$ je homomorfismus okruhu $(\mathbb{C}, +, \cdot)$ do okruhu $(\mathbb{C}, +, \cdot)$, je-li pro $a, b \in \mathbb{R}$ dáno:

a) $f(a + b\,\mathrm{i}) = a + b$,
b) $f(a + bi) = a^2 + b^2$,
c) $f(a + bi) = a - bi$.

Příklad 4.7: Určete, zda je okruh $(\mathbb{Z}_2, +, \cdot) \times (\mathbb{Z}_3, +, \cdot)$ oborem integrity. Je izomorfní s okruhem $(\mathbb{Z}_6, +, \cdot)$?

Příklad 4.8: Dokažte, že okruh $(\mathbb{Z}, \oplus, \odot)$ z příkladu 4.1 b) je izomorfní s okruhem $(\mathbb{Z}, +, \cdot)$.

Příklad 4.9: Určete všechny čtveřice $(a, b, c, d) \in \mathbb{R}^4$ takové, že předpis $\alpha(r + s\,\mathrm{i}) = (ar + bs) + (cr + ds)\,\mathrm{i}$, pro $r, s \in \mathbb{R}$, definuje homomorfismus $\alpha : \mathbb{C} \to \mathbb{C}$ okruhu $\mathbb{C}$ do sebe. Pro které z nich se jedná o izomorfismus?

Příklad 4.10: Buď $\mathbb{Q}(\sqrt{3}) = \{a + b\sqrt{3} \mid a, b \in \mathbb{Q}\}$ podokruh okruhu $(\mathbb{R}, +, \cdot)$. Dokažte, že libovolný okruhový homomorfismus $\alpha : \mathbb{Q}(\sqrt{3}) \to \mathbb{C}$ je identický na množině racionálních čísel, tj. $\forall r \in \mathbb{Q} : \alpha(r) = r$. Popište všechny okruhové homomorfismy $\alpha : \mathbb{Q}(\sqrt{3}) \to \mathbb{C}$. Které z nich jsou izomorfismy?

4.3 Obory integrity, invertibilní prvky okuhů, tělesa

Příklad 4.11: Rozhodněte, zda následující podmnožina M okruhu komplexních čísel $(\mathbb{C}, +, \cdot)$ je okruh, obor integrity, případně těleso. Jde-li o okruh, charakterizujte jeho invertibilní prvky.

a) $M = \{a + bi \mid a, b \in \mathbb{Z}\}$
b) $M = \{a + b \cdot \sqrt{5} \mid a, b \in \mathbb{Q}\}$
c) $M = \{a + b \cdot \sqrt[3]{5} \mid a, b \in \mathbb{Q}\}$
d) $M = \{a + b \cdot \frac{1+\sqrt{3}i}{2} \mid a, b \in \mathbb{Q}\}$

Příklad 4.12: Nalezněte invertibilní prvky okruhu $(\{a + b \cdot \frac{1+\sqrt{3}i}{2} \mid a, b \in \mathbb{Z}\}, +, \cdot)$

Příklad 4.13: Pro okruhy v příkladech 4.1 a 4.4 rozhodněte, zda se jedná o obor integrity a těleso. V okruzích, které nejsou tělesem, charakterizujte invertibilní prvky. Dále rozhodněte, zda invertibilní prvky tvoří podokruh.

Příklad 4.14: Pro prvky z příkladu 4.5 najděte nejmenší podtěleso tělesa $(\mathbb{C}, +, \cdot)$ obsahující daný prvek.

4.4 Polynomy nad $\mathbb{Z}_p$

Příklad 4.15: Nalezněte všechny kořeny polynomu $x^5 + 5x^4 - x^2 - x + 3$ v $\mathbb{Z}_7$.

Příklad 4.16: Určete všechny ireducibilní polynomy nad

a) $\mathbb{Z}_2$ stupně menšího než 5,
b) $\mathbb{Z}_3$ stupně menšího než 4.

Příklad 4.17: S využitím příkladu 4.16a) dokažte, že polynomy $x^4 + x^3 + x^2 + x + 1$, $x^4 + x^3 + x^2 + x + 3$ a $x^4 + x^3 - x^2 + x + 1$ jsou ireducibilní nad $\mathbb{Z}$.

Příklad 4.18: Nalezněte všechny kořeny polynomu $x^6 - x^5 - x^4 - x^3 - x^2 - x + 1 \in \mathbb{Z}_3[x]$ v $\mathbb{Z}_3[x]$ a určete jejich násobnost.

Příklad 4.19: Určete nějaký prvek $a \in \mathbb{Z}_5$ takový, že polynom $x^3 + x^2 + ax + 1$ je ireducibilní nad $\mathbb{Z}_5$.

Příklad 4.20: Určete všechny prvky $a \in \mathbb{Z}_7$, pro které je polynom $x^3 + x^2 + x + a$ ireducibilní nad $\mathbb{Z}_7$.

Příklad 4.21: Metodou neurčitých koeficientů rozhodněte, zda je polynom $x^4 + x^3 + x^2 + x + 2$ ireducibilní nad $\mathbb{Z}_5$. Totéž pro polynom $x^4 + x^3 + 3x + 1$.

Příklad 4.22: Udejte příklad polynomu
a) $g \in \mathbb{Z}_5[x]$, který je stupně 5, má dvojnásobný kořen 2 a žádné jiné kořeny nemá,
b) $g \in \mathbb{Z}_2[x]$, který je stupně 5, není ireducibilní a nemá žádný kořen,
c) $g \in \mathbb{Z}_3[x]$, který je stupně 4, není ireducibilní a nemá žádný kořen,
d) $g \in \mathbb{Z}_3[x]$, který je stupně 5, není ireducibilní a nemá žádný kořen,
e) $g \in \mathbb{Z}_5[x]$, který je stupně 6, má dvojnásobný kořen 2, jednoduchý kořen 4 a který nemá žádné další kořeny.

Příklad 4.23: Rozložte polynomy na ireducibilní faktory.
a) $x^6 + x^5 + x^2 + 1 \in \mathbb{Z}_2[x]$
b) $x^7 + 3x^6 + 2x^5 - x^4 + 3x^3 - x^2 + x + 1 \in \mathbb{Z}_5[x]$
c) $x^5 + x^4 + x^3 + x^2 + x + 1 \in \mathbb{Z}_2[x]$
d) $x^7 - x^6 + 2x^4 + x^3 - x^2 + 2 \in \mathbb{Z}_5[x]$
e) $x^5 + x^4 + x^3 - x^2 + 1 \in \mathbb{Z}_3[x]$
f) $x^4 + x^3 + x + 1 \in \mathbb{Z}_2[x]$
g) $x^5 + 3x^3 + x + 3 \in \mathbb{Z}_5[x]$
h) $x^5 + x^3 + 2x^2 + 2$

Příklad 4.24: Pro následující polynomy $f, g \in \mathbb{Z}_5[x]$ najděte normovaný polynom, který je jejich největším společným dělitelem. Najděte koeficienty do příslušné Bezoutovy rovnosti:
a) $f = x^3 + x^2 + x + 1$, $g = x^2 + 2x + 2$;
b) $f = x^3 + x^2 + x$, $g = x^2 + 2x + 2$;
c) $f = x^4 + x^2 + 1$, $g = x^3 + x^2 + x + 1$.

Příklad 4.25: Uvažujme okruh polynomů $\mathbb{Z}_4[x]$. Zdůrazněme nejdříve, že uvažované polynomy v tomto příkladu nejsou polynomy nad tělesem, ale polynomy nad okruhem $\mathbb{Z}_4$, který není obor integrity.
a) Popište jednotky okruhu $\mathbb{Z}_4[x]$.
b) Určete všechny prvky dělící prvek $2 \in \mathbb{Z}_4[x]$.
c) Ukažte, že $x \nmid x + 2$ a $x + 2 \nmid x$.
d) Dokažte, že $2 \cdot x = 2 \cdot (x + 2)$ jsou různé rozklady téhož prvku na ireducibilní prvky.
e) Dokažte, že prvky $2 \cdot x$ a $x(x + 2)$ nemají v $\mathbb{Z}_4[x]$ největšího společného dělitele.
Poznámka: v příkladu jde s úspěchem využít následujících dvou faktů. 1) Pro nenulový polynom f je jeho stupeň o jedna menší než stupeň polynomu $x \cdot f$. 2) Přirozené zobrazení $\mathbb{Z}_4[x] \to \mathbb{Z}_2[x]$ je homomorfismus okruhů, které jednotky zobrazuje na jednotky. Pokud tato nápověda nestačí, podívejte se na řešení do skript do odstavce 5.19.

4.5 Ideály a faktorokruhy

Příklad 4.26: Určete podgrupu grupy $(\mathbb{C}, +)$ generovanou prvkem i. Určete podokruh, podtěleso a ideál okruhu $(\mathbb{C}, +, \cdot)$ generovaný prvkem i. Totéž pro prvky $\sqrt[3]{2}$ a e.

Příklad 4.27: Popište všechny ideály okruhu $\mathbb{Z}_2 \times \mathbb{Z}_4$.

Příklad 4.28: Ukažte, že ideál $(x, 2)$ není hlavní ideál okruhu $\mathbb{Z}[x]$.

Příklad 4.29: Určete všechny ideály v okruhu $Mat_2(\mathbb{R})$ (okruh matic typu 2×2 nad reálnými čísly).

Příklad 4.30: Pro okruh R a jeho ideály I, J klademe $I + J = \{i + j \mid i \in I, j \in J\}$. Dokažte, že $\cap$ i $+$ jsou operace na množině všech ideálů okruhu R.

Příklad 4.31: Pro okruh R a jeho ideály I, J klademe $I \circ J = \{i \cdot j \mid i \in I, j \in J\}$. Rozhodněte, zda $\circ$ je operace na množině všech ideálů okruhu R.

Příklad 4.32: Dokažte, že v okruhu $\mathbb{Z}_n$ je každý ideál hlavní.

Příklad 4.33: Určete ideál generovaný prvkem $\sqrt{2}$ v okruhu $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}$. Čemu je izomorfní příslušný faktorokruh?

Příklad 4.34*: Určete, pro která $n \in \mathbb{N}$ je v okruhu $\mathbb{Z}_n[x]$ každý ideál hlavní.

Příklad 4.35*: Dokažte, že každý ideál okruhu $\mathbb{Z}[x]$ je konečně generovaný.

Příklad 4.36: Dokažte, že množina všech polynomů, které mají součet koeficintů dělitelný 3, tvoří v okruhu $\mathbb{Z}[x]$ ideál. Rozhodněte, zda se jedná o hlavní ideál. Určete, čemu je izomorfní příslušný faktorokruh.

Příklad 4.37: Dokažte, že množina všech polynomů, které mají všechny koeficinety sudé, tvoří v okruhu $\mathbb{Z}[x]$ ideál. Určete, čemu je izomorfní příslušný faktorokruh.

Příklad 4.38: Pro dané přirozené číslo n a celé číslo k označme $I(k, n) = \{f \in \mathbb{Z}[x] \mid n \mid f(k)\}$. Dokažte, že $I(k, n)$ je ideál okruhu $\mathbb{Z}[x]$. Rozhodněte, pro která n, k je tento ideál hlavní, pro která je maximální, pro která je to prvoideál. Nalezněte generátory tohoto ideálu.

Příklad 4.39: Určete, čemu je izomorfní faktorokruh $\mathbb{Q}[x]/(x - 2)$.

Příklad 4.40: Určete, čemu jsou izomorfní faktorokruhy
a) $\mathbb{Q}[x, y]/(x, y)$,
b) $\mathbb{Q}[x, y]/(x, y - 1)$,
c) $\mathbb{Q}[x, y]/(x)$,
d) $\mathbb{Q}[x, y]/I$, kde $I = \{f \in \mathbb{Q}[x, y] \mid f(x, x) = 0\}$.

Příklad 4.41: Určete, čemu je izomorfní faktorokruh $\mathbb{R}[x]/(x^2 + 1)$.

Příklad 4.42: Ukažte, že faktorokruh $\mathbb{Q}[x, y]/(x^2, y^2)$ je izomorfní okruhu čtvercových matic:

$$\left\{ \begin{pmatrix} d & 0 & 0 & 0 \\ c & d & 0 & 0 \\ b & 0 & d & 0 \\ a & b & c & d \end{pmatrix} \mid a, b, c, d \in \mathbb{Q} \right\}.$$

Příklad 4.43: Označme pro prvočíslo p okruh $M_p = \left\{ \frac{m}{n} \mid m, n \in \mathbb{Z},\ p \nmid n \right\}$. Popište všechny ideály tohoto okruhu. Určete, které z nich jsou hlavní, které prvoideály a které maximalní ideály.

Příklad 4.44*: Určete, čemu jsou izomorfní faktorokruhy příslušné ideálům z příkladu 4.43.

Příklad 4.45: Určete faktorokruh $\mathbb{Z}[x]/I(k, n)$ z příkladu 4.38.

4.6 Jednoduchá rozšíření

Příklad 4.46: Určete, které prvky patří do tělesa $\mathbb{Q}(i)$, $\mathbb{Q}(\sqrt{2 + \sqrt{2}})$. Určete stupně příslušných rozšíření (nad $\mathbb{Q}$).

Příklad 4.47: Buď $\alpha \in \mathbb{C}$ kořenem (ireducibilního) polynomu $x^3 - x - 2 \in \mathbb{Q}[x]$. Určete stupeň rozšíření tělesa $\mathbb{Q}(\alpha)$ nad tělesem $\mathbb{Q}$ a udejte bázi tohoto rozšíření. Vyjádřete prvky α^{-1}, $(1+\alpha)^3$ v této bázi.

Příklad 4.48: Určete, které prvky patří do tělesa $\mathbb{Q}(\pi)$.

Příklad 4.49: Určete všechny inkluze mezi následujícími podtělesy tělesa $\mathbb{C}$: $\mathbb{Q}$, $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{3})$, $\mathbb{Q}(\sqrt{6})$, $\mathbb{Q}(\sqrt{2},\sqrt{3})$, $\mathbb{Q}(\sqrt{2},\sqrt{6})$, $\mathbb{Q}(\sqrt{3},\sqrt{6})$, $\mathbb{Q}(\sqrt{2},\sqrt{3},\sqrt{6})$. Určete stupně rozšíření těchto těles nad $\mathbb{Q}$. Jsou tělesa $\mathbb{Q}(\sqrt{2})$ a $\mathbb{Q}(\sqrt{3})$ izomorfní?

Příklad 4.50: Určete, které prvky patří do tělesa $\mathbb{Q}(\sqrt{2}, \sqrt[3]{2})$. Určete stupeň rozšíření nad tělesem $\mathbb{Q}$ a rozhodněte, zda se jedná o jednoduché rozšíření.

Příklad 4.51*: Dokažte, že je v okruhu $\mathbb{Z}_n[x]$ každý ideál hlavní právě tehdy, když n není dělitelné druhou mocninou prvočísla. Postupně dokažte, že:

- Pokud existuje prvočíslo p takové, že $p^2 \mid n$, pak ideál (x, p) není hlavní ideál v $\mathbb{Z}_n[x]$.
- Pokud n je prvočíslo, pak $\mathbb{Z}_n[x]$ je okruhem hlavních ideálù.
- Pokud n je součinem rùzných prvočísel $p_1, p_2, \ldots, p_k$, pak okruh $\mathbb{Z}_n[x]$ je izomorfní součinu okruhů $\mathbb{Z}_{p_1}[x]$, $\mathbb{Z}_{p_2}[x]$, $\ldots$,$\mathbb{Z}_{p_k}[x]$.
- Každý ideál I v konečném součinu okruhù je součinem příslušných ideálů v jednotlivých komponentách součinu. Pokud jsou navíc tyto ideály hlavní, je hlavní i původní ideál I.

4.7 Konečná rozšíření a rozkladové těleso

Příklad 4.52: Ukažte, že tělesa $\mathbb{Q}(\sqrt{2})$ a $\mathbb{Q}(\sqrt{3})$ nejsou izomorfní.

Příklad 4.53: Je-li $\varphi : \mathbb{Q}(\alpha) \to \mathbb{Q}(\beta)$ izomorfismus, pak $\varphi(\alpha)$ má stejný minimální polynom jako α. Dokažte.

Příklad 4.54: Dokažte, že $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ je jednoduché rozšíření $\mathbb{Q}$. Určete stupeň tohoto rozšíření.

Příklad 4.55: Určete všechny automorfismy (izomorfismy na sebe) tělesa $\mathbb{Q}(\sqrt{2})$.

Příklad 4.56: Určete stupeň rozšíření rozkladového tělesa polynomu $x^4 - 2$ nad $\mathbb{Q}$.

Příklad 4.57: Určete stupeň rozšíření rozkladového tělesa polynomu $x^3 - 2$ nad $\mathbb{Q}$.

Příklad 4.58: Určete stupeň rozšíření rozkladového tělesa polynomu $x^n - 1$ nad $\mathbb{Q}$, pro $n = 3, 4, 5, 6$.

Příklad 4.59: Určete stupeň rozšíření rozkladového tělesa polynomu $x^n - 1$ nad $\mathbb{Q}$, pro n prvočíslo.

Příklad 4.60: Dokažte, že pro polynom stupně n nad $\mathbb{Q}$, je stupeň rozkladového tělesa tohoto polynomu menší nebo roven $n!$.

Příklad 4.61: Uvažujme ireducibilní polynom $f = x^3 + x + 1$ nad $\mathbb{Z}_2$. Popište těleso $\mathbb{Z}_2[x]/(f)$. Určete všechny jeho podtělesa.

Příklad 4.62: Určete všechny automorfismy tělesa $\mathbb{Q}(\sqrt{2}, \sqrt{3})$.

Příklad 4.63: Určete stupeň rozšíření rozkladového tělesa polynomu $x^3 - 5$ nad $\mathbb{Q}$.

Příklad 4.64: Uvažujme ireducibilní polynom f stupně 4 nad $\mathbb{Z}_2$. Popište těleso $\mathbb{Z}_2[x]/(f)$. Určete všechny jeho podtělesa.

Příklad 4.65*: Popište všechna konečná rozšíření tělesa $\mathbb{C}$.

4.8 Konečná tělesa, grupy automorfismů

Příklad 4.66: Uvažujme šestnáctiprvkové těleso $\mathbb{F}_{16}$. Buď β generátor jeho čtyřprvkového podtělesa.
a) Určete minimální polynom prvku β nad $\mathbb{Z}_2$. Napište jeho rozklad na ireducibilní polynomy nad $\mathbb{Z}_2(\beta)$.
b) Určete všechny ireducibilní polynomy stupně 2 nad $\mathbb{Z}_2(\beta)$.
c) Nechť f je nějaký ireducibilní polynom stupně 2 nad $\mathbb{Z}_2(\beta)$. Nalezněte jeho kořeny v $\mathbb{F}_{16}$. Popište izomorfismus $\mathbb{F}_{16}$ a $\mathbb{Z}_2(\beta)[x]/(f)$.

Příklad 4.67: Uvažujme těleso $\mathbb{F}_{p^n}$ o p^n prvcích a jeho grupu automorfismů $(Aut(\mathbb{F}_{p^n}), \circ)$. Nechť zobrazení $\iota : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ je definováno vztahem $\iota(x) = x^p$.
a) Dokažte, že ι je automorfismus tělesa $\mathbb{F}_{p^n}$.
b) Ukažte, že ι je prvek řádu n v grupě $(Aut(\mathbb{F}_{p^n}), \circ)$.
c) Ukažte, že $\mathbb{F}_{p^n}$ je jednoduché rozšíření tělesa $\mathbb{F}_p = \mathbb{Z}_p$ a proto existuje právě n automorfismů $\mathbb{F}_{p^n}$. tzn. $(Aut(\mathbb{F}_{p^n}), \circ)$ je n prvková cyklická grupa.

Příklad 4.68: Popište, kolik je homomorfismů z $\mathbb{F}_{p^n}$ do $\mathbb{F}_{q^m}$ a jak vypadají.

Příklad 4.69: Určete grupu automorfismů rozkladového tělesa polynomu $x^5 - 1$ nad $\mathbb{Q}$.

Příklad 4.70: Pro některou dvojici f, g různých ireducibilních polynomů stupně 2 nad $\mathbb{Z}_3$ popište všechny homomorfismy z $\mathbb{Z}_3[x]/(f)$ do $\mathbb{Z}_3[x]/(g)$.

Příklad 4.71*: Určete grupu automorfismů rozkladového tělesa polynomu $x^4 - 2$ nad $\mathbb{Q}$.

4.9 Počítání v jednoduchých rozšířeních těles

Příklad 4.72: Buď $\epsilon \in \mathbb{C}$ kořen polynomu $f = x^3 - x - 2 \in \mathbb{Q}[x]$. Dokažte, že f je ireducibilní polynom. Vyjádřete prvky ϵ^{-1} , $(1+\epsilon)^3$ a $(\epsilon^2 + 3\epsilon - 1)^{-2}$ ve tvaru $a_0 + a_1 \cdot \epsilon + a_2 \cdot \epsilon^2$, kde $a_0, a_1, a_2 \in \mathbb{Q}$.

Příklad 4.73: Buď $\epsilon \in \mathbb{C}$ kořen polynomu $f = x^4 + 2x^2 - 4x + 2 \in \mathbb{Q}[x]$. Vyjádřete čísla ϵ^{-1}, ϵ^6 a $(\epsilon^2 + \epsilon + 1)^{-1}$ ve tvaru $a_0 + a_1 \cdot \epsilon + a_2 \cdot \epsilon^2 + a_3 \cdot \epsilon^3$, kde $a_i \in \mathbb{Q}$ pro $i = 0, \ldots, 3$.

Příklad 4.74: Označme $a = \sqrt[4]{3}i + \sqrt{3}$. Dokažte, že $\mathbb{Q}(a) = \mathbb{Q}(\sqrt[4]{3}i)$. Vyjádřete komplexní číslo $\frac{1}{a}$ bez použití jiných než racionálních čísel ve jmenovateli.

Příklad 4.75: Buď $f = x^2 + [1]_3 \in \mathbb{Z}_3[x]$. Dokažte, že $\mathbb{F}_9 = \mathbb{Z}_3[x]/(f)$ je 9-prvkové těleso. Označme $\alpha \in \mathbb{F}_9$ prvek $\alpha = x + (f)$.
Určete $a_0, a = 1 \in \mathbb{Z}$ takové, že

i) $[a_0]_3 + [a_1]_3 \cdot \alpha = \alpha^4$;

ii) $[a_0]_3 + [a_1]_3 \cdot \alpha = (\alpha + [1]_3)^{-1}$.

Příklad 4.76: Buď $f = x^4 + x^3 + 1 \in \mathbb{Z}_2[x]$ a označme $\mathbb{F}_{16} = \mathbb{Z}_2[x]/(f)$ příslušné těleso. Označme $\alpha \in \mathbb{F}_{16}$ prvek $\alpha = x + (f)$.
Určete $a_i \in \mathbb{Z}_2$ pro $i = 0, 1, 2, 3$ takové, že

i) $a_0 + a_1 \cdot \alpha + \cdots + a_3 \cdot \alpha^3 = \alpha^6$;

ii) $a_0 + a_1 \cdot \alpha + \cdots + a_3 \cdot \alpha^3 = (\alpha^2 + 1)^{-1}$.

Příklad 4.77: Buď $f = x^3 - x + [2]_5 \in \mathbb{Z}_5[x]$ a nechť $\mathbb{F}_{125} = \mathbb{Z}_5[x]/(f)$ je 125-prvkové těleso. Označme $\alpha \in \mathbb{F}_{125}$ prvek $\alpha = x + (f)$. Určete $a, b, c \in \mathbb{Z}$ taková, že

i) $[a]_5 + [b]_5 \cdot \alpha + [c]_5 \cdot \alpha^2 = \alpha^5$,

ii) $[a]_5 + [b]_5 \cdot \alpha + [c]_5 \cdot \alpha^2 = (\alpha^4 + \alpha + 1)^{-1}$.