13.10.

1. Aritmetika ideálů a prvoideály

1.1. Obory hlavních ideálů.

1.1. Mějme $\mathcal{R} = (R, +, -, \cdot, 0, 1)$ obecný obor hlavních ideálů a $a, b \in R$.

(a) Určete $(a)(b)$, $(a) + (b)$, $(a) \cap (b)$.
(b) Jak vypadají prvoideály a maximální ideály oboru $\mathcal{R}$?
(c) Ukažte, že faktor $\mathcal{R}$ podle nenulového prvoideálu je nutně těleso.

(a) Z přednášky víme, že $(a)(b) = (ab)$. Označme $d = \mathrm{GCD}(a, b)$, $n = \mathrm{lcm}(a, b)$. Protože $d/a, b/n$, dostáváme, že $(a)+(b) \subseteq (d)$ a $(n) \subseteq (a) \cap (b)$. Naopak, vezmeme-li c, pro které $(c) = (a) + (b)$ a $m \in (a) \cap (b)$, pak d/c a $a, b/m$, proto $c/a, b/m$, tedy $(d) \subseteq (a) + (b)$ a $(m) \subseteq (a) \cap (b)$. Tím jsme ověřili rovnosti $(d) = (a) + (b)$ $(n) = (a) \cap (b)$.

(b) a (c) Z popisu hlavních prvoideálů plyne, že jsou vedle nulového ideálu prvoideály právě ideály generované ireducibilním prvkem. Vezmeme-li ireducibilní prvek p a nějaký prvek $r \notin (p)$, pak $(p) + (r) = \mathrm{GCD}(r, p) = R$, proto existují prvky a, b, pro něž $1 = \mathrm{GCD}(r, p) = ar + bp$. To znamená, že je faktor $R/(p)$ těleso a tudíž je (p) maximální ideál. Zjistili jsme, že maximální ideály jsou právě ideály generované ireducibilním prvkem. □

1.2. V oboru celých čísel $\mathcal{Z} = (\mathbb{Z}, +, -, \cdot, 0, 1)$ uvažujme ideály $I = (168)$ a $J = (288)$.

(a) Určete $I + J$, IJ, $I \cap J$, $I^2 + J$.
(b) Jak vypadají maximální ideály oboru celých čísel?
(c) Napište všechny prvoideály, které obsahují ideály, I, J, IJ, $I \cap J$ a J^2.

(a) Víme, že všechny ideály $\mathcal{Z}$ jsou hlavní, proto generátor $I + J$ musí být společným dělitelem prvků 168 a 288, tedy a díky Eukleidově algoritmu víme (protože $\mathrm{GCD}(168, 288) = 168x + 288y \in (168, 288)$), že se bude jednat právě o největšího společného dělitele. Obdobnou úvahou nahlédneme, že $I \cap J$ generuje právě nejmenší společný násobek čísel 168 a 288. Pro násobení hlavních ideálů obecně víme, že $(m)(n) = (mn)$. Protože $\mathrm{GCD}(168, 288) = 24$ a $\mathrm{lcm}(168, 288) = \frac{168 \cdot 288}{/} 24 = 2016$, dostáváme

$$I + J = (24), \ I \cap J = (2016), \ IJ = (168 \cdot 288) = (48384).$$

Konečně podle předchozích pozorování nám pro určení $I^2 + J$ stačí spočítat největší společný dělitel $\mathrm{GCD}(168^2, 288)$, tedy $I^2 + J = (\mathrm{GCD}(168^2, 288)) = (288) = J$.

(b) Z přednášky víme, že v oboru hlavních ideálů jsou prvoideály kromě nuly právě ideály generované prvočinitelem a že každý maximální ideál je prvoideálem. Nulový ideál zjevně není maximální a zbývá si uvědomit, že ostatní prvoideály už maximální jsou. Je-li p prvočíslo a uvážíme ideál (i), pro který $(p) \subset (i)$, pak i/p. Protože je p prvočíslo, je buď $(i) = (1) = \mathbb{Z}$ nebo $(i) = (p)$, což jsme měli dokázat.

Maximální ideály jsou tedy právě ideály generované prvočíslem.

(c) Stačí využít vztahu dělitelnosti a inkluze ideálů, tj. $(a) \subseteq (p) \Leftrightarrow p/a$, a najít prvočísla obsažená v prvočíselném rozkladu generátorů daných ideálů. Protože $168 = 2^3 \cdot 3 \cdot 7$ a $288 = 2^5 \cdot 3^2$ dostáváme, že

- I, IJ a $I \cap J$ jsou obsažené právě v prvoideálech (2), (3) a (7),

- J a J^2 jsou obsažené právě v prvoideálech (2) a (3).

$\square$

1.3. V oboru polynomů s racionálními koeficienty $(\mathbb{Q}[x], +, -, \cdot, 0, 1)$ uvažujme ideály $I = (x^3 + x^2 + 2x + 2)$ a $J = (x^3 - 2x^2 + 2x - 4)$.

(a) Určete $I + J$, IJ, $I \cap J$, $I^2 + J^3$.
(b) Které faktory modulo ideál z bodu a) jsou obory?
(c) Napište všechny prvoideály, které obsahují ideály, I, J, IJ, $I \cap J$ a J^2.

Nejprve (v tomto případě) snadno zjistíme ireducibilní rozklady polynomů

$$x^3 + x^2 + 2x + 2 = (x^2 + 2)(x + 1), \quad x^3 - 2x^2 + 2x - 4 = (x^2 + 2)(x - 2).$$

Protože je $(\mathbb{Q}[x], +, -, \cdot, 0, 1)$ stejně jako okruh celých čísel oborem hlavních ideálů, postupujeme obdobně jako v předchozí úloze.

(a) Ze stejných důvodů jsou součty ideálů generovány největším společným dělitelem a jejich průniky nejmenším společným násobkem:

$$I + J = (\mathrm{GCD}(x^3 + x^2 + 2x + 2, x^3 - 2x^2 + 2x - 4)) = (x^2 + 2),$$
$$I \cap J = (\mathrm{lcm}(x^3 + x^2 + 2x + 2, x^3 - 2x^2 + 2x - 4)) = ((x^3 + x^2 + 2x + 2)(x - 2))$$
$$IJ = ((x^3 + x^2 + 2x + 2)(x^3 - 2x^2 + 2x - 4)).$$
$$I^2 + J^3 = (\mathrm{GCD}((x^3 + x^2 + 2x + 2)^2, (x^3 - 2x^2 + 2x - 4)^3)) = (x^2 + 2)^2.$$

(b) Víme, že pouze faktory modulo ideál generovaný ireducibilním polynomem, což nastává pouze pro modulo ideál $I + J$.

(c) Ze vztahu $(a) \subseteq (p) \Leftrightarrow p/a$ plyne, že použijeme ireducibilní faktory generujících polynomů:

- I, IJ jsou obsažené právě v prvoideálech $(x^2 + 2)$ a $(x + 1)$,
- J a J^2 jsou obsažené právě v prvoideálech $(x^2 + 2)$ a $(x - 2)$,
- IJ a $I \cap J$ jsou obsažené právě v prvoideálech $(x^2 + 2)$, $(x + 1)$ a $(x - 2)$.

$\square$

1.2. **Noetherovské okruhy.**

1.4. Uvažujme obor polynomů s celočíselnými koeficienty $\mathcal{Z}[x] = (\mathbb{Z}[x], +, -, \cdot, 0, 1)$ a jeho ideál $I = (2) + (x)$.

(a) Najděte $\mathrm{GCD}(2, x)$ a rozhodněte, zda je I hlavní ideál.
(b) Ověřte, že $\mathcal{Z}[x]$ je noetherovský a není obor hlavních ideálů.
(c) Je I prvoideál?

(a) Ukážeme, že I není hlavní.

Předpokládejme, že tomu tak není je, tedy že existuje jeho generátor a, což znamená, že $I = (a)$. Protože $2\mathbf{Z}[x] \subseteq (a)$, vidíme, že $a/2$, tj. $a \in \{1, -1, 2, -2\}$. Podobně $(x) \subseteq (a)$, a proto a/x a $a \in \{1, -1, x, -x\}$. Tedy a je nutně invertibilní prvek, tudíž $I = (a) = \mathbf{Z}[x]$. Protože zřejmě $1 \notin I$, dostáváme spor, tedy ideál I nemůže být hlavní.

Už jsme zjistili, že společní dělitelé prvků 2 a x jsou jen 1 a -1 oba prvky jsou tedy podle definice největší společní dělitelé 2 a x.

(b) Protože je okruh celých čísel obor hlavních ideálů, tedy noetherovský okruh, je $\mathcal{Z}[x]$ noetherovský podle Hilbertovy věty o bázi.

(c) Stačí si všimnout, že $\mathcal{Z}[x]/I \cong \mathbb{Z}_2$, což je těleso. Podle tvrzení z přednášky je I maximální a tedy prvoideál. $\square$

20.10.

1.5. Rozhodněte, zda jsou následující ideály okruhu $(\mathbf{Z}[x], +, -, \cdot, 0, 1)$ hlavní a zda se jedná o prvoideály:

(a) $\{\sum_i p_i x^i \in \mathbf{Z}[x] |\ \sum_i p_i = 0\}$ (tzv. fundamentální ideál),
(b) $\{p \in \mathbf{Z}[x] |\ p(\frac{1}{2}) = 0\}$,
(c) $(x^2 - 1) + (x^2 + 3x + 2)$.

(a) Všimněme si, že $x-1 \in J_a = \{\sum_i p_i x^i \in \mathbf{Z}[x] |\ \sum_i p_i = 0\}$, tedy máme inkluzi $(x-1) \subseteq J_1$. Zvolíme-li $p \in \mathbf{J}_a$, můžeme p vydělit se zbytkem polynomem $x-1$, tj. existují polynomy $q, z \in \mathbf{Z}[x]$, pro které $p = q\cdot(x-1)+z$ a $\deg(z) < \deg(x-1) = 1$. Vidíme, že $z = p - q \cdot (x-1) \in J_1$, protože z má nejvýše jeden nenulový koeficient (u x^0) a ten musí být podle definice J_1 nulový, dostáváme, že $p \in (x-1)$.

Protože je polynom $x-1$ ireducibilní, je $(x-1)$ prvoideál.

(b) Rovněž tentokrát snadno najdeme polynom nejnižšího možného nezáporného stupně, který leží v množině $J_b = \{p \in \mathbf{Z}[x] |\ p(\frac{1}{2}) = 0\}$, konkrétně $2x-1 \in J_b$. Poznamenejme, že důkaz faktu, že je J_b ideál je zcela přímočarý. Vidíme tedy, že $(2x-1)\mathbf{Z}[x] \subseteq J_b$ a ukážeme obrácenou inkluzi. Zvolme proto $p \in \mathbf{J}_a$. Tentokrát ovšem nemůžeme vydělit se zbytkem bezprostředně v okruhu $(\mathbf{Z}[x], +, -, 0, \cdot, 1)$, protože vedoucí koeficient polynomu $2x-1$ není v $\mathbf{Z}$ invertibilní, ovšem můžeme vydělit se zbytkem v okruhu $(\mathbf{Q}[x], +, -, 0, \cdot, 1)$.

To znamená, že existují polynomy $q, z \in \mathbf{Q}[x]$, pro které $p = q \cdot (2x-1) + z$ a $\deg(z) < \deg(x-1) = 1$. Dosadíme-li $x = \frac{1}{2}$, vidíme, že $z = 0$, a proto $p = q\cdot(2x-1)$. Nyní uvážíme, že $q = \sum_i q_i x^i \in \mathbf{Z}[x]$, tj. že $q_i \in \mathbf{Z}$ pro všechna i. Dokažme to indukcí. Nejprve označme $p = \sum_i p_i x^i$ a všimněme si, že $q_0 = p_0$ a $p_i = q_i - 2q_{i-1}$ pro každé $i > 0$. To jednak znamená, že $q_0 \in \mathbf{Z}$ a předpokládáme-li, že $q_{i-1} \in \mathbf{Z}$, pak $q_i = p_i + 2q_{i-1} \in \mathbf{Z}$. Tím jsme ověřili, že $J_b = (2x-1)\mathbf{Z}[x]$ je hlavní ideál.

(c) Ptáme se, zda existuje polynom $p \in J_2 = (x^2-1)+(x^2+3x+2)$, který generuje J_2, tedy zda existují polynomy $a, b \in \mathbf{Z}[x]$, že $p = (x^2-1)\cdot a + (x^2+3x+2)\cdot b$ a $J_2 = (p)$. Předpokládejme, že je tato podmínka splněna. Protože $p = (x+1)[(x-1)\cdot a+(x+2)\cdot b]$, vidíme, že $J_c = (p)$, právě když $((x-1)\cdot a+(x+2)\cdot b) = (x-1)+(x+2)$. Dále můžeme argumentovat stejně jako v předchozí úloze: $q = (x-1)\cdot a + (x+2)\cdot b$ musí být společným dělitelem polynomů $x-1$ a $x+2$, a 1 a -1 jsou jedinými společnými děliteli. Protože ovšem $q(1) = 3 \cdot b(1)$ je číslo dělitelné trojkou. To znamená $\mathbf{Z}[x] \neq (x-1)+(x+2)$, hledané q, a tudíž ani p neexistuje, proto ideál J_c není hlavní. □

1.6. Dokažte pro každé n, že je ideál $I = (x^{n-1}, x^{n-2}y, x^{n-3}y^2, \dots, xy^{n-2}, y^{n-1})$ okruhu $T[x,y]$ je generován nejméně n generátory.

Vezměme si ideál $J = (x^n, x^{n-1}y, x^{n-2}y^2, \dots, xy^{n-1}, y^n)$ a uvážíme, že ideál I/J faktorového okruhu $T[x,y]/J$ má strukturu vektorového prostoru nad tělesem $T[x,y]/(x,y) \cong T$. Protože není těžké ověřit, že bázi tohoto vektorového prostoru tvoří množina $\{x^{n-1}+J, x^{n-2}y+J, \dots, y^{n-1}+J\}$, jedná se o vektorový prostor dimenze n. Kdyby byla v ideálu I přítomna generující množina G o nejvýše n prvcích, pak by množina $\{g+J, g \in G\}$ generovala celý vektorový prostor $T[x,y]/J$, což by bylo ve sporu s hodnotou jeho dimenze. □

1.7. Nechť $R = \{\sum_i p_i x^i \in \mathbf{Q}[x] |\ p_0 \in \mathbf{Z}\} \subseteq \mathbf{Q}[x]$.

(a) Dokažte, že je $\mathcal{R} = (R, +, -, \cdot, 0, 1)$ podokruh okruhu polynomů s racionálními koeficienty a že jde o obor integrity,
(b) rozhodněte, zda je R noetherovský.

(a) Protože součet, rozdíl i součin polynomů s celočíselným absolutním členem má tutéž vlastnost a $0, 1 \in R$, je R podokruh okruhu $(\mathbf{Q}[x], +, -, 0, \cdot, 1)$.

Protože je $\mathbf{Q}[x]$ obor , je každý jeho podokruh opět obor.

(b) Uvědomme si, že $2^{-n}x \in R$, $(2^{-n}x) \subseteq (2^{-(n+1)}x)$, protože $2^{-n}x = 2 \cdot 2^{-(n+1)}x$, a $(2^{-n}x) \neq (2^{-(n+1)}x)$, protože $2^{-(n+1)}x \notin (2^{-n}x)$, čímž jsme našli nekonečnou posloupnost vlastních dělitelů $\dots 2^{-(n+1)}x/2^{-n}x \dots x/2^{-1}x$ a máme tak rostoucí posloupnost ideálů

$$(2^{-1}x) \subset (2^{-2}x) \subset \cdots \subset (2^{-n}x) \subset (2^{-n-1}x) \subset \dots .$$

Protože jsme našli rostoucí posloupnost ideálů, R není noetherovský. Všimněme si navíc, že ideál $I = \bigcup_{n \in \mathbf{N}} 2^{-n}xR$ není konečně generovaný. $\square$

27.10.

2. Lokalizace a faktorizace

2.1. **Lokalizace.**

2.1. Mějme multiplikativní množinu S komutativního okruhu $\mathcal{R} = (R, +, -, 0, \cdot, 1)$. Na $R \times S$ definujme relaci $\sim$ vztahem

$$(r, s) \sim (p, t) \Leftrightarrow \exists u \in S : u \cdot (r \cdot t - p \cdot s) = 0$$

Ověřte, že

(a) $\sim$ je ekvivalence na $R \times S$
(b) $\mathcal{R}S^{-1} = (R \times S/\sim, +, -, \cdot, 0, 1)$ je komutativní okruh s operacemi zavedenými stejně jako pro lokalizace v oborech,
(c) zobrazení $\nu : R \to R \times S/\sim$ dané předpisem $\nu(r) = \frac{r}{1}$ je homomorfismus (opět značíme $\frac{r}{1} = [(r, s)]_\sim$),
(d) $\mathrm{Ker}(\nu) = \{r \in R | \ \exists u \in S : ru = 0\}$.

(a) reflexivita a symetrie $\sim$ plyne okamžitě z definice relace.

Nechť $(r_0, s_0) \sim (r_1, s_1) \sim (r_2, s_2)$. Pak existují $u_1, u_2 \in S$, pro která

$$u_0(r_0s_1 - r_1s_0) = 0 \quad \text{a} \quad u_1(r_1s_2 - r_2s_1) = 0.$$

Přenásobením dostáváme:

$$s_2u_1u_0(r_0s_1 - r_1s_0) = 0 \quad \text{a} \quad s_0u_0u_1(r_1s_2 - r_2s_1) = 0$$

Nyní stačí rovnice sečíst

$$s_1u_1u_0(r_0s_2 - r_2s_0) = s_2u_1u_0(r_0s_1 - r_1s_0) + s_0u_0u_1(r_1s_2 - r_2s_1) = 0$$

a uvážit, že $s_1u_1u_0 \in S$.

(b) Postupujeme obdobně jako v důkazu konstrukce podílového tělesa pomocí obvyklé ekvivalence krácení, tj. postupně přímočaře ověříme platnost všech axiomů komutativního okruhu.

(c) Stačí nahlédnout, že $\nu(r + s) = \frac{r+s}{1} = \frac{r}{1} + \frac{s}{1}$, $\nu(rs) = \frac{r}{1} \cdot \frac{s}{1}$ a $\nu(1) = 1$.

(d) Vidíme, že $r \in \mathrm{Ker}(\nu) \Leftrightarrow \frac{r}{1} = \frac{0}{1} \Leftrightarrow (r, 1) \sim (0, 1) \Leftrightarrow \exists u \in S : ru = 0.$ $\square$

2.2. Nechť p je prvočíslo, tedy (p) prvoideál oboru $(\mathbb{Z}, +, -, \cdot, 0, 1)$ a uvažujme multiplikativní množinu $S = \mathbb{Z} \setminus (p)$. Ověřte, že nenulové ideály lokalizace $\mathbb{Z}S^{-1}$ jsou právě tvaru (p^i) a že je svaz všech ideálů lineárně uspořádán inkluzí.

Připomeňme, že $\mathbb{Z}S^{-1}$ je stejně jako $\mathbb{Z}$ obor hlavních ideálů a generátor nenulového ideálu oboru $\mathbb{Z}S^{-1}$ lze vzít kladný z oboru $k \in \mathbb{Z}$. Nyní stačí uvážit prvočíselný rozklad k, přesněji řečeno valoaci prvočísla p v k. Vezmeme-li tedy takové nezáporné celé j, že $k = p^j \cdot v$, kde $\mathrm{GCD}(p, v) = 1$. Potom $v \in S$, proto $(p^j) = (k)$.
Nyní je zřejmé, že $(p^{j+1}) \subseteq (p^j)$ navíc $p^j \notin (p^{j+1})$, tedy $(p^{j+1}) \neq (p^j)$. $\square$

2.3. Jak vypadají lokalizace v prvoideálu oboru hlavních ideálů?

Uvážíme-li nulový ideál, pak je lokalizací právě podílové těleso tohoto oboru.
Nenulový prvoideál, je podobně jako v předchozí úloze generován nějakým prvočinitelem p. To opět znamená,že každý nenulový prvek lokalizace lze jednoznačně zapsat ve tvaru $p^i \cdot u$ pro invertibilní u. Tedy ideály jsou opět lineárně uspořádány a nenulové jsou generovány prvkem p^i pro vhodné nezáporné i. $\square$

2.4. Uvažme v oboru $(\mathbb{Z}[x], +, -, 0, \cdot, 1)$ množinu $S = \{x^i |\ i \in \mathbb{N} \cup \{0\}\}$. Dokažte, že je S multiplikativní a popište obor $\mathbb{Z}[x]S^{-1}$

Zřejmě $x^i \cdot x^j = x^{i+j} \in S$ a $1 = x^0$.
Potřebujeme invertovat právě polynomy x^i, proto

$$\mathbb{Z}[x]S^{-1} \cong \mathbb{Z}[x, x^{-1}] = \{\sum_{i=a}^{b} c_i x^i |\ a \leq b \in \mathbb{Z}\}.$$

$\square$

2.5. Popište lokalizace $\mathcal{R}S^{-1}$ pro

(a) $\mathcal{R} = (\mathbb{Z} \times \mathbb{Z}, +, -, 0, \cdot, 1)$ a $S = \{(a, b) |\ b \neq 0\}$,
(b) $\mathcal{R} = (\mathbb{Z} \times \mathbb{Z}, +, -, 0, \cdot, 1)$ a $S = \{(0, b) |\ b \neq 0\} \cup \{(1, 1)\}$,
(c) $\mathcal{R} = (\mathbb{Q}[x, y]/(xy), +, -, 0, \cdot, 1)$ a $S = \{x^i |\ i \in \mathbb{N}\}$.

(a) Všimněme si, že multiplikativní množina S je doplňkem prvoideálu $\mathbb{Z} \times \{0\}$. Dále poznamenejme, že $(a, 0) \cdot (0, 1) = 0$, proto všechny prvky tvaru $(a, 0)$ splynou s nulou. Nyní už je snadné dopočítat, že hledaná lokalizace je izomorfní tělesu racionálních čísel.
(b) I tentokrát lokalizace vynuluje všechny prvky tvaru $(a, 0)$ a tudíž je hledaná lokalizace i tentokrát izomorfní tělesu racionálních čísel.
(c) Tentokrát ztratíme monom y, proto podobně jako v úloze 2.4 dostáváme, že $\mathcal{R}S^{-1} \cong \mathbb{Q}[x, x^{-1}] = \{\sum_{i=a}^{b} c_i x^i |\ a \leq b \in \mathbb{Q}\}$. $\square$

2.2. **Čínská věta o zbytcích.** Uvažujme pro po dvou nesoudělná n_i zobrazení

$$f : \mathbf{Z}_{\prod_i n_i} \to \prod_i \mathbf{Z}_{n_i}$$

předpisem $f(k) = (k \bmod n_1, k \bmod n_2, \dots)$.

2.6. Pro $f : \mathbb{Z}_{45} \to \mathbb{Z}_5 \times \mathbb{Z}_9$ (tj.$f(a) = (a \bmod 5, a \bmod 9)$) spočítejte (jednoznačně určené) $a \in \mathbf{Z}_{45}$, pro které $f(a) = (2, 4)$.

Využijeme úvahu důkazu Čínské věty o zbytcích. Zapíšeme ji ovšem pomocí kongruencí, tedy hledáme $a \in \mathbb{Z}_{45}$, pro

$$a \equiv 2 (\mathrm{mod}\ 5), \quad a \equiv 4 (\mathrm{mod}\ 9)$$

To znamená, že $a = 2 + 5s$ a

$$2 + 5s \equiv 4 (\mathrm{mod}\ 9) \quad \Rightarrow \quad 5s \equiv 2 (\mathrm{mod}\ 9) \quad \Rightarrow \quad s \equiv 2 \cdot 5s \equiv 2 \cdot 2 \equiv 4 (\mathrm{mod}\ 9).$$

Proto $s = 4$ a $a = 2 + 5 \cdot 4 = 22$. □

2.7. Pro $f : \mathbb{Z}_{720} \to \mathbb{Z}_5 \times \mathbb{Z}_9 \times \mathbb{Z}_{16}$ najděte $b \in \mathbb{Z}_{720}$, pro které $f(b) = (2, 4, 5)$.

Nyní využijeme indukce, abychom navázali na úvahu předchozí úlohy. Tedy víme, že $a \equiv 22 (\mathrm{mod}\ 45)$, proto $a = 22 + 45t$ a $a \equiv 5 (\mathrm{mod}\ 16)$, tudíž

$$22{+}45t \equiv 5 (\mathrm{mod}\ 16) \Rightarrow -3t \equiv -1 (\mathrm{mod}\ 16) \Rightarrow t \equiv 5{\cdot}(-3)t \ \equiv 5{\cdot}(-1) \equiv 11 (\mathrm{mod}\ 16).$$

Vidíme, že $t = 11$ a $a = 22 + 45 \cdot 11 = 517$ □

2.8. Najděte všechna řešení rovnice $x^2 + 1 = 0$ v okruzích a) $\mathbb{Z}_{45}$ a b) $\mathbb{Z}_{65}$.

a) Kdyby existovalo řešení rovnice $x^2 + 1 = 0$ v $\mathbb{Z}_{45}$, muselo by existovat i okruhu $\mathbb{Z}_9$, to znamená, že bychom měli prvek $x \in \mathbb{Z}_9$, pro který $x^2 = -1$, a proto $x^4 = 1$. Tudíž by x byl prvek řádu 4 multiplikativní grupy $\mathbb{Z}_9^*$. Protože je $\mathbb{Z}_9^*$ řádu 6, podle Lagrangeovy věty žádný prvek řádu čtyři nemůže obsahovat a $x^2 + 1$ v $\mathbb{Z}_9$ ani $\mathbb{Z}_{45}$ nemá žádné řešení.

b) Tentokrát využijeme k řešení Čínskou větu o zbytcích. Nejprve vyřešíme rovnici $x^2 + 1$ v tělesech $\mathbb{Z}_5$ a $\mathbb{Z}_{13}$, tedy

$$x \equiv 2 (\mathrm{mod}\ 5) \quad \text{nebo} \quad x \equiv -2 \equiv 3 (\mathrm{mod}\ 5),$$

$$x \equiv 5 (\mathrm{mod}\ 13) \quad \text{nebo} \quad x \equiv -5 \equiv 8 (\mathrm{mod}\ 13),$$

Dále postupujeme obdobně jako v předchozích příkladech. Nejprve položíme $x = \pm 5 + 13s$ a dosadíme:

$$\pm 5 + 13s \equiv 3s \equiv \pm 2 (\mathrm{mod}\ 5) \quad \Rightarrow \quad s \equiv 2 \cdot 3s \equiv \pm 4 (\mathrm{mod}\ 5).$$

Dosazením za $s = 1, 4$ dostáváme právě čtyři řešení rovnice $x^2 + 1$ v okruhu $\mathbb{Z}_{65}$: $8, 18, 47, 57$. □

10.11.

3. Radikály

3.1. **Odmocniny a radikály v okruzích hlavních ideálů.**

3.1. Určete v oboru celých čísel $(\mathbb{Z}, +, -, 0, \cdot, 1)$

(a) $\sqrt{(0)}$, $J(\mathbb{Z})$,
(b) $\sqrt{(25)}$, $\sqrt{(125)}$, $\sqrt{(50)}$, $\sqrt{(100)}$, $\sqrt{(\prod_i p_i^{r_i})}$ pro různá prvočísla $\{p_i\}$,
(c) $J(\mathbb{Z}/(100))$,
(d) kdy je $(\mathbb{Z}/(n))/J(\mathbb{Z}/(n))$ těleso.

(a) Protože je (0) prvoideál, nutně $\sqrt{(0)} = (0)$. Vezmeme-li pro libovolné nenulové celé n prvočíslo p, které nedělí n, pak n neleží v maximálním ideálu (p), proto n neleží v $J(\mathbb{Z})$. Tím jsme dokázali, že $J(\mathbb{Z}) = (0)$ (odtud samozřejmě také plyne, že $\sqrt{(0)} = (0)$).

(b) Stačí si všimnout, že $Var((25)) = Var((125)) = \{(5)\}$, proto

$$\sqrt{(25)} = \sqrt{(125)} = (5).$$

Podobně $Var((50)) = Var((100)) = \{(5), (2)\}$, tudíž

$$\sqrt{(50)} = \sqrt{(100)} = (5)(2) = (10).$$

Z téhož důvodu $\sqrt{(\prod_i p_i^{r_i})} = \bigcap_i (p_i) = \prod_i (p_i) = (\prod_i p_i)$.

(c) Protože maximální ideály splývají s nenulovými prvoideály, máme

$$J(\mathbb{Z}/(100)) = \sqrt{(100)}/(100) = (10)/(100).$$

(d) Zopakujeme-li úvahu (c) pro obecné číslo (n) s použitím úvahy (b), vidíme, že $\mathbb{Z}/J(\mathbb{Z}/(n))$ těleso, právě když je $\sqrt{(n)}$ maximální ideál, což nastává právě tehdy, když je n mocninou prvočísla. □

3.2. Uvažujme okruh $(\mathbb{Z}_n, +, -, 0, \cdot, 1)$, kde $n = \prod_{i \leq k} p_i^{r_i}$ je pro prvočíselný rozklad pro p_i jsou různá prvočísla

(a) Popište všechny prvoideály, nilradikál a Jacobsonův radikál okruhu pro libovolné kladné,
(b) spočítejte nilradikál a Jacobsonův radikál pro $n = 162$,
(c) rozhodněte, kdy $\sqrt{(0)} = 0$.

Určete nilradikál a Jacobsonův radikál okruhu pro libovolné kladné n a speciálně pro $n = 162$.

(a) Stačí pro faktorový okruh $\mathbb{Z}/(n) \cong \mathbb{Z}_n$ využít 3.1. Dostáváme tak, že pro prvočíselný rozklad $n = \prod_i p_i^{r_i}$, kde p_i jsou různá prvočísla je $Var(0) = \{(p_i) | \, i \leq k\}$ a oba radikály jsou tvaru $(\prod_i p_i)$.

(b) Protože $162 = 2 \cdot 3^4$, v okruhu $(\mathbb{Z}_{162}, +, -, \cdot, 0, 1)$ máme jediné maximální ideály i prvoideály (2) a (3), proto $J(\mathbb{Z}_{162}) = \sqrt{(0)} = (2) \cap (3) = (2)(3) = (6)$.

(c) Tvrdíme, že $\sqrt{(0)} = 0$, právě když je n bez čtverců, tj. $r_i = 1$ pro všechna $i \leq k$. V (a) jsme zjistili, že $\sqrt{(0)} = (\prod_i p_i)$, což se rovná nulovému ideálu, právě když $r_i = 1$ pro všechna $i \leq k$. □

3.3. V oboru polynomů nad komplexními čísly $(\mathbb{C}[x], +, -, \cdot, 0, 1)$

(a) spočítejte $\sqrt{(0)}$, $J(\mathbb{C}[x])$, $\sqrt{(x-3)^5(x-1)^4(x^3+2)}$, $\sqrt{(x^6 - x^4 - x^2 + 1)}$,
(b) dokažte, že $\sqrt{(p)} = (\frac{p}{\mathrm{GCD}(p,p')})$, kde $p \in \mathbb{C}[x]$.

(a) Obdobná argumentace jako v předchozí úloze dokazuje, že
$\sqrt{(0)} = J(\mathbb{C}[x]) = 0$,
$\sqrt{(x-3)^5(x-1)^4(x^3+2)} = ((x-3)(x-1)(x^3+2))$ a
$\sqrt{(x^6 - x^4 - x^2 + 1)} = \sqrt{(x^2-1)^2(x^2+1)} = (x^2-1)(x^2+1)$.

(b) Stačí si uvědomit, že polynom $\frac{p}{\mathrm{GCD}(p,p')}$ ve svém ireducibilním rozkladu obsahuje všechny kořenové činitele polynomu p ve stupni jedna, zbytek argumentace už je shodný s argumentací 3.1(b). □

3.2. **Radikály v lokalizacích.**

3.4. Spočítejte nilradikál a Jacobsonův radikál lokalizace $\mathbb{Z}(\mathbb{Z}\setminus(p))^{-1}$ oboru celých čísel $(\mathbb{Z},+,-,\cdot,0,1)$ v prvoideálu (p) daného prvočíslem p.

Lokalizace obsahuje jediný maximální ideál (p), tudíž je $J(R)=(p)$. Protože je v každém oboru (0) prvoideál, opět nutně dostáváme, že $\sqrt{(0)}=(0)$. Vidíme tedy, že v tomto případě $\sqrt{(0)}\neq J(R)$. □

3.5. Spočítejte nilradikál a Jacobsonův radikál kvazilokálního komutativního oboru $\mathcal{R}$ s jediným maximálním ideálem M. Kdy oba radikály splývají?

Ze stejného důvodu jako v předchozí úloze je $J(R)=M$. Navíc $\sqrt{(0)}=(0)$, neboť uvažujeme obor. Odtud plyne, že $J(R)=\sqrt{(0)}$, právě když je $\mathcal{R}$ těleso. □

3.6. Najděte všechny prvoideály, nilradikál a Jacobsonův radikál lokalizace $\mathcal{R}:=\mathbb{Z}S^{-1}$ oboru celých čísel $(\mathbb{Z},+,-,0,\cdot,1)$ v multiplikativní množině $S:=\mathbb{Z}\setminus((2)\cup(3)\cup(5))$.

Podobně jako v úlohách 2.2 a 3.4 zjistíme, že obecný ideál okruhu $\mathcal{R}$ je tvaru $(2^i3^j5^k)$ pro i,j,k nezáporná celá, a proto $Var(0)=\{(0),(2),(3),(5)\}$. Potom zřejmě $\sqrt{(0)}=(0)$ a $J(R)=(2)\cap(3)\cap(5)=(2)(3)(5)=(30)$. □

3.3. **Radikály v obecných okruzích.**

3.7. Pro komutativní okruhy $\mathcal{R}$ a $\mathcal{S}$ a ideály I a j okruhu $\mathcal{R}$ dokažte, že

(a) $\sqrt{I\cap J}=\sqrt{I}\cap\sqrt{J}$,

(b) nilradikál okruhu $\mathcal{R}\times\mathcal{S}$ je právě kartézský součin nilradikálů obou okruhů,

(c) $J(R\times S)=J(R)\times J(S)$.

(a) Postupujme podle definice

$$a\in\sqrt{I\cap J}\Leftrightarrow\exists n: a^n\in I\cap J\Leftrightarrow\exists n: a^n\in I, a^n\in J\Leftrightarrow a\in\sqrt{I}\cap\sqrt{J}.$$

(b) Označme K_R a K_S příslušné nilradikály a dokážeme opět jen s využitím definice, že je $K_R\times K_S$ nilradikál součinu okruhů:

$$(a_1,a_2)\in\sqrt{0}\Leftrightarrow\exists n(a_1,a_2)^n=(0,0)\Leftrightarrow\exists n: a_1^n=0, a_2^n=0\Leftrightarrow(a_1,a_2)\in K_R\times K_S$$

(c) Využijeme charakterizace Jacobsonova ideálu a stejného postupu jako v případu (b)

$$(a_1,a_2)\in J(R\times S)\Leftrightarrow\forall(r_1,r_2)\in R\times S:(1,1)-(a_1,a_2)\cdot(r_1,r_2)\in(R\times S)^*\Leftrightarrow$$
$$\Leftrightarrow\forall r_1\in R,\forall r_s\in S: 1-a_1r_1\in R^*, 1-a_2r_2\in S^*\Leftrightarrow(a_1,a_2)\in J(R)\times J(S)$$

□

3.8. Spočítejte nilradikál a Jacobsonův radikál oborů polynomů $(\mathbb{Z}[x],+,-,\cdot,0,1)$ a $(T[\mathbb{X}],+,-,\cdot,0,1)$, kde T je těleso a $\mathbb{X}$ (libovolně velká) množina neznámých.

V obou případech se jedná o obory, tedy nilradikály jsou nulové. Navíc můžeme pro výpočet Jacobsonova radikálu obou okruhů s úspěchem použít charakterizační Poznámku 4.6, podle níž příslušnost prvku a do Jacobsonova radikálu implikuje, že $1-ar$ je pro každý prvek r okruhu invertibilní. To ovšem v obou případech znamená, že nutně $a=0$ a proto jsou Jacobsonovy radikály obou okruhů nulové. □

4. Konečně generované moduly

4.1. **Nerozložitelné rozklady modulů nad $\mathbb{Z}$.**

4.1. Rozhodněte, zda je faktorový Z-modul $\mathbb{Z}^3/N$ cyklický, jestliže
(a) $N = (5) \oplus (7) \oplus (12)$,
(b) $N = (10) \oplus (11) \oplus (12)$,
(c) $N = (a) \oplus (b) \oplus (c)$ pro a, b, c po dvou nesoudělná
(d) $N = (0) \oplus (1) \oplus (a)$ pro $a \neq 0$.

Poté, co využijeme pozorování z přednášky, že

$$\mathbb{Z}^3/((a) \oplus (b) \oplus (c)) \cong \mathbb{Z}/(a) \oplus \mathbb{Z}/(b) \oplus \mathbb{Z}(c) \cong \mathbb{Z}_{|a|} \times \mathbb{Z}_{|b|} \times \mathbb{Z}_{|c|}$$

stačí využít Čínskou větu o zbytcích, protože $\mathbb{Z}_{|a|} \times \mathbb{Z}_{|b|} \times \mathbb{Z}_{|c|}$ je cyklický Z-modul (tedy cyklická grupa), právě když je izomorfní $\mathbb{Z}_{abc}$, tedy právě když jsou prvky a, b, c po dvou nesoudělné. Proto
(a) pro $N = (5) \oplus (7) \oplus (12)$ je modul $\mathbb{Z}^3/N$ cyklický,
(b) pro $N = (10) \oplus (11) \oplus (12)$ není modul $\mathbb{Z}^3/N$ cyklický,
(c) pro $N = (a) \oplus (b) \oplus (c)$, kde a, b, c po dvou nesoudělná je modul $\mathbb{Z}^3/N$ cyklický.
V případě (d) vidíme, že $\mathbb{Z}^3/N \cong \mathbb{Z} \oplus \mathbb{Z}/(a) \cong \mathbb{Z} \times \mathbb{Z}_{|a|}$, což pro nenulové a nemůže být cyklický modul. □

O modulu (nebo podmodulu) M řekneme, že je direktně nerozložitelný, jestliže $A \oplus B = M$ implikuje , že $A = 0$ nebo $B = 0$.

4.2. Najděte rozklad $\mathbb{Z}$-modulů M na direktní sumu nerozložitelných podmodulů jestliže
(a) $M = \mathbb{Z}_8 \times \mathbb{Z}_6$,
(b) $M = \mathbb{Z}_{10} \times \mathbb{Z}_{12} \times \mathbb{Z}_{15}$,
(c) $M = \mathbb{Z}_{20} \times \mathbb{Z}_{15} \times \mathbb{Z}$,
(d) $M = \mathbb{Z}^{(n)}/(\bigoplus_{i=1}^{r} \bigoplus_{j=1}^{k_i} (p_i^{n_{ij}}))$ pro různá prvočísla $p_1, \dots, p_r$, přirozená čísla $n_{ij} \geq n_{ij+1}$ a $n = \sum_{i=1}^{r} k_i$.

(a) Stačí pomocí Čínské věty o zbytcích určit

$$M = \mathbb{Z}_8 \times \mathbb{Z}_6 \cong \mathbb{Z}_8 \times \mathbb{Z}_3 \times \mathbb{Z}_2 \cong \mathbb{Z}_2 \times \mathbb{Z}_{24}.$$

(b) Postupujeme stejně jako v (b):

$$M = \mathbb{Z}_{10} \times \mathbb{Z}_{12} \times \mathbb{Z}_{15} \cong \mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_3^2 \times \mathbb{Z}_5^2.$$

(c) Nejprve stejně jako v (a) a (b) spočítáme konečných cyklických grup:

$$\mathbb{Z}_{20} \times \mathbb{Z}_{15} \cong \mathbb{Z}_4 \times \mathbb{Z}_5 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \cong \mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_5^2.$$

Nyní dostáváme $M \cong \mathbb{Z} \times \mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_5^2$.
(d) Položme $k := \max\{k_i\}$ a $s_{k-\nu+1} := \prod_{i=1}^{n} p_i^{n_{i\nu}}$, kde nedefinovaná $n_{i\nu}$ mají hodnotu 0. Nyní nám Čínská věta o zbytcích zaručuje, že $M \cong \bigoplus_i \mathbb{Z}/(s_i)$.
Výpočty už jsme uskutečnili v předchozí úloze pomocí Čínské věty o zbytcích:

$$\mathbb{Z}_8 \times \mathbb{Z}_6 \cong \mathbb{Z}_8 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_2, \qquad \mathbb{Z}_{10} \times \mathbb{Z}_{12} \times \mathbb{Z}_{15} \cong \mathbb{Z}_2 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_3^2 \oplus \mathbb{Z}_5^2,$$

$$\mathbb{Z}_{20} \times \mathbb{Z}_{15} \times \mathbb{Z} \cong \mathbb{Z}/(5) \oplus \mathbb{Z}/(60) \oplus \mathbb{Z}/(0), \qquad \mathbb{Z}^2/(\mathbb{Z}a) \cong \mathbb{Z}/(2) \oplus \mathbb{Z}/(0).$$

(d) Využijeme-li opět pozorování, že $M \cong \bigoplus_{i=1}^{r} \bigoplus_{j=1}^{k_i} \mathbb{Z}/(p_i^{n_{ij}})$ a zjevný fakt, že $\mathbb{Z}/(p_i^{n_{ij}})$ má lineárně uspořádané podmoduly a tedy jde direktně nerozložitelný modul, je modul $\bigoplus_{i=1}^{r} \bigoplus_{j=1}^{k_i} \mathbb{Z}/(p_i^{n_{ij}})$ přímo ireducibilní rozkladem modulu M. □

4.2. **Nerozložitelné rozklady modulů nad okruhem polynomů.** Máme-li φ lineární operátor na vektorovém prostoru V nad tělesem T zavedeme na V strukturu $T[x]$-modulu předpisem $(\sum_i a_i x^i)v = \sum_i a_i \varphi^i(v)$ $\sum_i a_i x^i \in T[x]$ a $v \in V$.

4.3. Uvažujme lineární operátor φ na $\mathbb{C}^2$ s maticí vzhledem ke kanonické bázi $\mathbf{X} = \begin{pmatrix} 3 & 1 \\ 4 & 3 \end{pmatrix}$.

(a) Najděte všechny podmoduly $\mathbb{C}^2$ jako modulu nad okruhem $\mathbb{C}[x]$,
(b) rozhodněte, zda je $\mathbb{C}[x]$-modul $\mathbb{C}^2$ cyklický a najděte minimální množinu jeho generátorů.

(a) Nejprve poznamenejme, že určitě $\{(0,0)^T\}$ a $\mathbb{C}^2$ jsou (triviální) podmoduly $\mathbb{C}[x]$-modulu $\mathbb{C}^2$. Dále si všimněme, že každý P podmodul $\mathbb{C}[x]$-modulu je jeho $\mathbb{C}$-podprostor, zbývá tedy prozkoumat, které komplexní přímky v $\mathbb{C}^2$ jsou $\mathbb{C}[x]$-podmoduly. Protože pro podmodul P platí, že $xP = \varphi(P) = XP \subseteq P$, vidíme, že podmodulem budou právě přímky invariantní vzhledem k φ, tedy přímky generované vlastním vektorem.

Snadno spočítáme, že lineární operátor má právě dvě vlastní čísla 1 a 5 (například jako kořeny charakteristického polynomu $\det(\mathbf{X} - \lambda \mathbf{I}_2)$). Nyní najdeme vlastní vektory, t.j. řešení homogenních soustav lineárních rovnic s maticí $\mathbf{X} - \lambda \mathbf{I}_2$:

$$\lambda = 1 : \begin{pmatrix} 2 & 1 \\ 4 & 2 \end{pmatrix}, \qquad \lambda = 5 : \begin{pmatrix} -2 & 1 \\ 4 & -2 \end{pmatrix},$$

Spočítáme, že hledané invariantní přímky tvoří $U_1 = \langle (1,-2)^T \rangle$ a $U_2 = \langle (1,2)^T \rangle$, což znamená, že $\{(0,0)^T\}$, $\mathbb{C}^2$, U_1 a U_2 jsou právě všechny podmoduly $\mathbb{C}[x]$-modul $\mathbb{C}^2$.

(b) Všimněme si, že pro každý vektor $\mathbf{v} \in \mathbb{C}^2$ je zobrazení $\psi : \mathbb{C}[x] \to \mathbb{C}^2$ dané vztahem $\psi(p) = p\mathbf{v}$ homomorfismus, a proto podle 1. věty o izomorfismu je $\mathbb{C}[x]/\ker\psi \cong \mathbb{C}[x]\mathbf{v}$. Aplikujeme-li to na vlastní vektory, že $\mathbb{C}[x]/(x-1) \cong \mathbb{C}[x](1,-2)^T = U_1$ a $\mathbb{C}[x]/(x-5) \cong \mathbb{C}[x](1,2)^T = U_2$. Využijeme-li nyní Čínskou větu o zbytcích, dostaneme

$$\mathbb{C}^2 = U_1 \oplus U_2 \cong \mathbb{C}[x]/(x-1) \oplus \mathbb{C}[x]/(x-5) \cong \mathbb{R}[x]/((x-1)(x-5)),$$

neboť ideály $(x-1)$ a $(x-5)$ jsou komaximální. Zjistili jsme, že modul $\mathbb{C}[x]$-modul $\mathbb{C}^2$ je cyklický. Jeho generátorem je každý (nenulový) vektor, který není vlastní, například vektor $(1,0)^T$. □

4.4. Nechť je V konečně dimenzionální vektorový prostor nad tělesem T a φ lineární operátor na V. Uvažujme V jako $T[x]$-modul určený operátorem φ. Dokažte, že

(a) podmoduly V jsou právě invariantní podprostory φ,
(b) existuje nenulový polynom p, který anihiluje V, tj. $pV = 0$.

(a) Je-li U invariantní podprostor, pak pro každé $u \in U$ máme $\varphi(u) \in U$, proto i $\sum_i a_i \varphi^i(u) \in U$. tedy U je uzavřen na násobení polynomem. Protože jde o podprostor je uzavřen i na sčítání, tudíž jde o $T[x]$-podmodul.

Naopak $T[x]$-podmodul U je určitě T-podprostorem a platí, že $\varphi(U) = xU \subseteq U$, tedy jde o invariantní podprostor.

(b) Stačí vzít bázi $v_1, \dots, v_n$ vektorového prostoru V a všimnout si, že První věta o izomorfismu aplikovaná na přirozený modulový homomorfismus $T[x] \to V$ daný vztahem $p \to pv_i$, indukuje izomorfismus $T[x]v_i \cong T[x]/\{p \mid pv_i = 0\}$. Protože je $T[x]$ nekonečně dimenzionální jako vektorový prostor nad T, zatímco $T[x]v_i$ je konečně dimenzionální, musí být hlavní ideál $\{p \mid pv_i = 0\}$ netriviální, tedy musí existovat $p_i \neq 0$, pro které $p_i v_i \neq 0$. Nyní zbývá vzít polynom $p := \prod_i p_i$. $\square$

4.5. Uvažujme lineární operátor φ na $\mathbb{R}^4$ s maticí vzhledem ke kanonické bázi
$$\mathbf{A} = \begin{pmatrix} 2 & 3 & 2 & 1 \\ 0 & 2 & 2 & 1 \\ 0 & 0 & 1 & -1 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

(a) Najděte ireducibilní rozklad $\mathbb{R}^4$ jako modulu nad okruhem $\mathbb{R}[x]$,
(b) rozhodněte, zda je $\mathbb{R}[x]$-modul $\mathbb{R}^4$ cyklický,
(c) dokažte, že charakteristický polynom φ anihiluje $\mathbb{R}[x]$-modul $\mathbb{R}^4$.

(a) Okamžitě vidíme, že lineární operátor má dvě vlastní čísla 1 a 2, obě algebraické násobnosti 2 a geometrické násobnosti 1. Najdeme nyní vlastní vektory a vektory určující invariantní podprostor odpovídající příslušné Jordanově buňce. Tedy řešíme nejprve homogenní a poté nehomogenní soustavu:

$$\lambda = 1: \quad \begin{pmatrix} 1 & 3 & 2 & 1 \\ 0 & 1 & 2 & 1 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 4 \\ -2 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \quad \begin{pmatrix} 1 & 3 & 2 & 1 \\ 0 & 1 & 2 & 1 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 8 \\ -1 \\ 0 \\ -1 \end{pmatrix} = \begin{pmatrix} 4 \\ -2 \\ 1 \\ 0 \end{pmatrix},$$

$$\lambda = 2: \quad \begin{pmatrix} 0 & 3 & 2 & 1 \\ 0 & 0 & 2 & 1 \\ 0 & 0 & -1 & -1 \\ 0 & 0 & 0 & -1 \end{pmatrix} \cdot \begin{pmatrix} 3 \\ 0 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \quad \begin{pmatrix} 0 & 3 & 2 & 1 \\ 0 & 0 & 2 & 1 \\ 0 & 0 & -1 & -1 \\ 0 & 0 & 0 & -1 \end{pmatrix} \cdot \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 3 \\ 0 \\ 0 \\ 0 \end{pmatrix},$$

Položme $u_1 = \begin{pmatrix} 4 \\ -2 \\ 1 \\ 0 \end{pmatrix}$, $u_2 = \begin{pmatrix} 8 \\ -1 \\ 0 \\ -1 \end{pmatrix}$, $v_1 = \begin{pmatrix} 3 \\ 0 \\ 0 \\ 0 \end{pmatrix}$ a $v_2 = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}$. Pak jsou podprostory $U = \langle u_1, u_2 \rangle$ a $V = \langle v_1, v_2 \rangle$ invariantní, tedy jde o $\mathbb{R}[x]$ moduly, navíc $\mathbb{R}^4 = U \oplus V$. Konečně $(\varphi - \mathrm{id})^2 U = 0$ a $(\varphi - 2\mathrm{id})^2 V = 0$ (tj. $U = \tau_{x-1}$ je takzvaná torzní komponenta příslušná ireducibilnímu polynomu $x - 1$ a $V = \tau_{x-2}$ je torzní komponenta příslušná ireducibilnímu polynomu $x - 2$).

(b) Protože $u_1 = (x-1)u_2$ a $v_1 = (x-2)v_2$, je $\mathbb{R}[x]u_2 = U$ a $\mathbb{R}[x]v_2 = V$. Výška obou prvků je právě 2, využijeme-li s tímto faktem ještě Čínskou větu o zbytcích dostáváme

$$\mathbb{R}^4 = \mathbb{R}[x]u_2 \oplus \mathbb{R}[x]v_2 \cong \mathbb{R}[x]/(x-1)^2 \oplus \mathbb{R}[x]/(x-2)^2 \cong \mathbb{R}[x]/((x-1)^2(x-2)^2).$$

(c) To, že charakteristický polynom φ, tedy polynom $(x-1)^2(x-2)^2$ anihiluje $\mathbb{R}^4$ plyne z předchozího pozorování. $\square$

15.12.

5. Volné a beztorzní moduly

5.1. **Homomorfismy volných modulů.** Je-li $\mathbf{A} \in \mathbb{Z}^{m\times n}$ budeme v následujícím značit $\varphi_{\mathbf{A}} : \mathbb{Z}^n \to \mathbb{Z}^m$ zobrazení dané předpisem $\varphi_{\mathbf{A}}(\mathbf{v}) = \mathbf{A}\mathbf{v}$.

5.1. Nechť $\mathbf{A} \in \mathbb{Z}^{m\times n}$ buď $\varphi : \mathbb{Z}^n \to \mathbb{Z}^m$ homomorfismus $\mathbb{Z}$-modulů $\mathbb{Z}^n$ a $\mathbb{Z}^m$. Dokažte, že

(a) $\varphi_{\mathbf{A}}$ je modulový homomorfismus,
(b) existuje matice $\mathbf{B} \in \mathbb{Z}^{m\times n}$, pro niž $\varphi_{\mathbf{B}} = \varphi$,
(c) $\varphi_{\mathbf{A}} = \varphi_{\mathbf{B}}$, právě když $\mathbf{A} = \mathbf{B}$.

Platí obdobná tvrzení i pro volné moduly konečného ranku, homomorfismy a matice nad obecným komutativním okruhem?

(a) Na celočíselné matice můžeme pohlížet jako na racionální matice, proto funguje stejný argument jako v lineární algebře, tj. distributivita násobení matic vzhledem ke sčítání a komutativita pro násobení skalárem.

(b) Stejně jako v lineární algebře stačí vzít matici složenou z obrazů vektorů kanonické báze jako sloupcových vektorů, tedy $\mathbf{B} = (\varphi(\mathbf{e}_1), \dots, \varphi(\mathbf{e}_n))$

(c) Stačí uvážit, že je homomorfismus na volném modulu jednoznačně určen hodnotami na libovolné bázi. Tyto hodnoty jsou ovšem determinovány údaji v matici $\mathbf{A}$, resp. $\mathbf{B}$.

Konečně, uvážíme-li, že se maticové násobení chová nad obecným komutativním okruhem obdobně jako nad tělesem (tedy především platí distributivita násobení matic vzhledem ke sčítání a komutativita pro násobení skalárem), pak vidíme, že předchozí tvrzení i v této situaci zůstávají v platnosti. □

5.2. Nechť $\mathbf{A} = \begin{pmatrix} 1 & 3 \\ 2 & 5 \end{pmatrix}$.

(a) Rozhodněte, zda je $\varphi_{\mathbf{A}}$ modulový izomorfismus,
(b) existuje-li najděte matici $\mathbf{B} \in \mathbb{Z}^{m\times n}$, pro kterou $\varphi_{\mathbf{B}} = \varphi_{\mathbf{A}}^{-1}$
(c) ověřte, že je $\{\begin{pmatrix} 1 \\ 2 \end{pmatrix}, \begin{pmatrix} 3 \\ 5 \end{pmatrix}\}$ volná báze $\mathbb{Z}^2$,
(d) určete, které z množin
$$X = \{\begin{pmatrix} 1 \\ 2 \end{pmatrix}, \begin{pmatrix} 3 \\ 4 \end{pmatrix}\},\quad Y = \{\begin{pmatrix} 4 \\ 5 \end{pmatrix}, \begin{pmatrix} 3 \\ 4 \end{pmatrix}\},\quad \varphi_{\mathbf{A}}(X),\quad \varphi_{\mathbf{A}}(X)$$
jsou volné báze $\mathbb{Z}^2$.

(a) Najdeme-li inverzní zobrazení k $\varphi_{\mathbf{A}}$, půjde o izomorfismus. V předchozí úloze jsme si uvědomili, že případný inverz by musel být tvaru $\varphi_{\mathbf{B}}$ pro vhodnou čtvercovou matici $\mathbf{B}$ a muselo by tudíž platit, že $\mathbf{AB} = \mathbf{BA} = \mathbf{I}_2$. $\varphi_{\mathbf{A}}$ je tedy invertibilní zobrazení, právě když existuje inverz matice $\mathbf{B}$, jehož všechny hodnoty jsou celočíselné, a to (díky vlastnosti adjungovaných matici) nastává právě když je $\det \mathbf{A} \in \mathbb{Z}^* = \{1, -1\}$.

Protože $\det \begin{pmatrix} 1 & 3 \\ 2 & 5 \end{pmatrix} = 5 - 6 = -1$, je $\varphi_{\mathbf{A}}$ modulový izomorfismus.

(b) Už jsme si uvědomili, že $\mathbf{B} = \mathbf{A}^{-1} = \begin{pmatrix} -5 & 3 \\ 2 & -1 \end{pmatrix}$.

(c) Protože je izomorfní obraz volné báze opět volná báze, je $\{\begin{pmatrix}1\\2\end{pmatrix}, \begin{pmatrix}3\\5\end{pmatrix}\} = \varphi(\{\mathbf{e}_1, \mathbf{e}_2\})$ volná báze $\mathbb{Z}^2$.

(d) Protože obraz volné báze (například kanonické) na volnou bázi lze vždy rozšířit na izomorfismus, stačí naopak uvážit homomorfismus $\varphi(\mathbf{e}_1) = \begin{pmatrix}1\\2\end{pmatrix}$, $\varphi(\mathbf{e}_2) = \begin{pmatrix}3\\4\end{pmatrix}$, tedy homomorfismus $\varphi_{\mathbf{C}}$ určený maticí $\mathbf{C} = \begin{pmatrix}1 & 3\\2 & 4\end{pmatrix}$. Protože $\det \mathbf{C} = -2 \notin \{1, -1\}$, nejedná se o izomorfismus, tedy množiny X ani $\varphi_{\mathbf{A}}(X)$ netvoří volné báze $\mathbb{Z}^2$.

Naopak matice $\mathbf{D} = \begin{pmatrix}4 & 3\\5 & 4\end{pmatrix}$ má determinant 1, proto jsou množiny Y i $\varphi_{\mathbf{A}}(Y)$ volné báze $\mathbb{Z}^2$ □

5.3. Uvažujme matice $\mathbf{A} = \begin{pmatrix}1 & 3 & 2\\1 & 1 & 1\\2 & 4 & 3\end{pmatrix}$ s $\mathbf{B} = \begin{pmatrix}1 & 3 & 2\\1 & 1 & 0\\3 & 0 & 0\end{pmatrix}$ nad okruhem $\mathbb{Z}$.

(a) Rozhodněte, jsou $\varphi_{\mathbf{A}}, \varphi_{\mathbf{B}} : \mathbb{Z}^3 \to \mathbb{Z}^3$ prosté a zda jsou na,
(b) rozhodněte, zda jsou $\varphi_{\mathbf{A}}(\mathbb{Z}^3)$ a $\varphi_{\mathbf{B}}(\mathbb{Z}^3)$ volné a určete jejich rank.

(a) Snadno spočítáme, že je nad tělesem racionálních čísel hodnost matice $\mathbf{A}$ rovna dvěma a že je matice $\mathbf{B}$ regulární. Navíc determinant $\det \mathbf{B} = 3$, proto ani jedno ze zobrazení $\varphi_{\mathbf{A}}$ ani $\varphi_{\mathbf{B}}$ není na. Zobrazení $\varphi_{\mathbf{A}}$ navíc není ani prosté protože vhodným přenásobením nenulového racionálního vektoru z jádra matice dostaneme nenulový celočíselný vektor z jádra homomorfismu $\varphi_{\mathbf{A}}$. Konečně $\varphi_{\mathbf{B}}$ je prosté.

(b) Protože je $\varphi_{\mathbf{B}}$ prosté, dostáváme izomorfismus $\varphi_{\mathbf{B}} : \mathbb{Z}^3 \to \varphi_{\mathbf{B}}(\mathbb{Z}^3)$, tedy $\varphi_{\mathbf{B}}(\mathbb{Z}^3)$ je stejně jako $\mathbb{Z}^3$ volný modul ranku 3. Zbývá nahlédnout, že

$$\begin{pmatrix}1\\1\\2\end{pmatrix} = 2\begin{pmatrix}2\\1\\3\end{pmatrix} - \begin{pmatrix}3\\1\\4\end{pmatrix}, \quad \text{proto} \quad \varphi_{\mathbf{A}}(\mathbb{Z}^3) = \mathbb{Z}\begin{pmatrix}2\\1\\3\end{pmatrix} + \mathbb{Z}\begin{pmatrix}3\\1\\4\end{pmatrix}.$$

Z lineární nezávislosti zbylých dvou generátorů vidíme, že $\varphi_{\mathbf{A}}(\mathbb{Z}^3)$ je volný modul ranku 2. □

5.4. Uvažme volný modul $\mathbb{F}$ konečného ranku n nad oborem $\mathcal{R}$.

(a) Je-li $F = R^n$ a $\varphi : F \to F$, dokažte, že φ je modulový izomorfismus, právě když existuje taková matice $\mathbf{A} \in R^{n\times n}$, že $\det \mathbf{A} \in R^*$ a $\varphi = \varphi_{\mathbf{A}}$.
(b) Dokažte je grupa automorfismů na $\mathbb{F}$ (tj. izomorfismů $\mathbb{F}$ do $\mathbb{F}$) izomorfní grupě čtvercových matic nad oborem $\mathcal{R}$ s invertibilním determinantem.

(a) Protože je $\mathcal{R}$ obor, můžeme ho chápat jako podokruh jeho podílového tělesa $\mathcal{Q}$ a využívat všechny lineárně algebraické pojmy zavedené pro těleso $\mathcal{Q}$. Samotná myšlenka důkazu je uvedena v předchozí úloze.

(b) Stačí se omezit na volný modul R^n a využít bodu (a). Tedy hledaným izomorfismem je zobrazení, které izomorfismu $\varphi_{\mathbf{A}}$ přiřadí matici $\mathbf{A}$. Podle (a) jde o bijekci a tvrzení maticích složeného homomorfismu z lineární algebry (které jsme nad tělesem $\mathcal{Q}$ oprávněni použít) říká, že $\varphi_{\mathbf{A}} \circ \varphi_{\mathbf{B}} = \varphi_{\mathbf{AB}}$. □

5.2. **Podmoduly a faktory volných modulů.**

5.5. Ve volném $\mathbb{Z}$-modulu $\mathbb{Z}^2$ s prvky $a = \begin{pmatrix}4\\6\end{pmatrix}$ a $b = \begin{pmatrix}4\\3\end{pmatrix}$, $c = \begin{pmatrix}3\\3\end{pmatrix}$ určete:

(a) obsahy prvků a, b, c,
(b) volné báze f_1, f_2 a g_1, g_2 tak, aby $a = sf_1$ a $b = rg_1$ pro $(s) = c(a)$, $(r) = c(b)$
(c) strukturu modulů $\mathbb{Z}^2/(\mathbb{Z}a)$, $\mathbb{Z}^2/(\mathbb{Z}b)$, $\mathbb{Z}^2/(\mathbb{Z}a + \mathbb{Z}b)$ a $\mathbb{Z}^2/(\mathbb{Z}a + \mathbb{Z}c)$,
(d) torzní část modulu $\mathbb{Z}^2/(\mathbb{Z}a + \mathbb{Z}b)$.

(a) Využijeme-li kanonickou volnou bázi dostaneme $c(a) = (\mathrm{GCD}(4,6)) = (2)$, $c(b) = (\mathrm{GCD}(4,3)) = (1) = \mathbb{Z}$ a $c(c) = (\mathrm{GCD}(3,3)) = (3)$.

(b) Položíme (až na znaménko nutně) $f_1 = \begin{pmatrix}2\\3\end{pmatrix}$, pak stačí vzít Bezoutovy koeficienty, které nám dají největší společný dělitel $1 = -1 \cdot 2 + 1 \cdot 3$ a pomocí nich zkonstruovat vektor $f_2 = \begin{pmatrix}1\\1\end{pmatrix}$, aby byl determinant matice $(f_1 f_2)$ invertibilní.

Podobně zvolíme $g_1 = \begin{pmatrix}4\\3\end{pmatrix}$ a opět $g_2 = \begin{pmatrix}1\\1\end{pmatrix}$.

(c) Nalezené volné báze z úlohy (b) ukazují, že $\mathbb{Z}^2/(\mathbb{Z}a) \cong \mathbb{Z}_2 \oplus \mathbb{Z}$ a $\mathbb{Z}^2/(\mathbb{Z}b) \cong \mathbb{Z}$. Protože je obsah prvku b největší mezi všemi obsahy, stačí, abychom našli průnik $(\mathbb{Z}a + \mathbb{Z}b) \cap \mathbb{Z}g_2$, tj. hledáme celočíselná řešení rovnice

$$4x + 4y = 6x + 3y \Rightarrow y = 2x \Rightarrow (\mathbb{Z}a + \mathbb{Z}b) \cap \mathbb{Z}g_2 = \mathbb{Z}(\begin{pmatrix}4\\6\end{pmatrix} + 2\begin{pmatrix}4\\3\end{pmatrix}) = \mathbb{Z}\begin{pmatrix}12\\12\end{pmatrix}$$

Spočítali jsme, že $\mathbb{Z}a + \mathbb{Z}b = \mathbb{Z}g_1 \oplus \mathbb{Z}g_2 12 = \mathbb{Z}\begin{pmatrix}4\\3\end{pmatrix} \oplus \mathbb{Z}\begin{pmatrix}12\\12\end{pmatrix}$, proto

$$\mathbb{Z}^2/(\mathbb{Z}a + \mathbb{Z}b) = (\mathbb{Z}g_1 \oplus \mathbb{Z}g_2)/(\mathbb{Z}g_1 \oplus \mathbb{Z}g_2 12) \cong \mathbb{Z}/(12) \cong \mathbb{Z}_{12}$$

Protože jsou obsahy obou prvků vlastní ideály, víme, že největší možný obsah prvku je roven $c(a) + c(c) = (2) + (3) = \mathbb{Z}$. Snadno prvek s tímto obsahem, například $d = a - c = \begin{pmatrix}1\\3\end{pmatrix}$. Nyní vidíme, že dvojice d, c tvoří volnou bázi podmodulu $\mathbb{Z}a + \mathbb{Z}c$ a že že dvojice d, e_2 $\begin{pmatrix}0\\1\end{pmatrix}$ tvoří volnou bázi celého modulu $\mathbb{Z}^2$. Opět zbývá najít průnik $(\mathbb{Z}d + \mathbb{Z}c) \cap \mathbb{Z}e_2$, tj. hledáme celočíselná řešení soustavy rovnic $x + 3y = 0$, $3x + 3y = z$, proto

$$x = -3y, -9y + 3y = z \Rightarrow z = -6y \Rightarrow (\mathbb{Z}d + \mathbb{Z}c) \cap \mathbb{Z}e_2 = \mathbb{Z}\begin{pmatrix}0\\6\end{pmatrix}$$

(d) Zřejmě jde o torzní modul, tedy torzní část je celý modul $\mathbb{Z}^2/(\mathbb{Z}a + \mathbb{Z}b)$. $\square$

5.6. Najděte posloupnost $s_1/s_2/\dots$ aby pro $\mathbb{Z}$-modul platilo $M \cong \bigoplus_i \mathbb{Z}/(s_i)$, jestliže

(a) $M = \mathbb{Z}_8 \times \mathbb{Z}_6$,
(b) $M = \mathbb{Z}_{10} \times \mathbb{Z}_{12} \times \mathbb{Z}_{15}$,
(c) $M = \mathbb{Z}_{20} \times \mathbb{Z}_{15} \times \mathbb{Z}$,
(d) $M = \mathbb{Z}^2/(\mathbb{Z}a)$ pro a z předchozí úlohy,

(a) Stačí pomocí Čínské věty o zbytcích určit

$$M = \mathbb{Z}_8 \times \mathbb{Z}_6 \cong \mathbb{Z}_8 \times \mathbb{Z}_3 \times \mathbb{Z}_2 \cong \mathbb{Z}_2 \times \mathbb{Z}_{24} \cong \mathbb{Z}/(2) \oplus \mathbb{Z}/(24).$$

(b) Postupujeme stejně jako v (b):

$$M = \mathbb{Z}_{10} \times \mathbb{Z}_{12} \times \mathbb{Z}_{15} \cong \mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_3^2 \times \mathbb{Z}_5^2 \cong \mathbb{Z}_{30} \times \mathbb{Z}_{60} \cong \mathbb{Z}/(30) \oplus \mathbb{Z}/(60).$$

(c) Nejprve stejně jako v (a) a (b) spočítáme dekompozici torzní části:

$$\mathbb{Z}_{20} \times \mathbb{Z}_{15} \cong \times\mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_5^2 \cong \mathbb{Z}_5 \times \mathbb{Z}_{60} \cong \mathbb{Z}/(5) \oplus \mathbb{Z}/(60).$$

Protože $\mathbb{Z} \cong \mathbb{Z}/(0)$, dostáváme $M \cong \mathbb{Z}/(5) \oplus \mathbb{Z}/(60) \oplus \mathbb{Z}/(0)$.

(d) Už jsme spočítali, že $\mathbb{Z}^2/(\mathbb{Z}a) \cong \mathbb{Z}_2 \oplus \mathbb{Z}$, tedy $M \cong \mathbb{Z}/(2) \oplus \mathbb{Z}/(0)$. □

5.1.

6. Galoisovy grupy, stopa a norma

6.1. **Galoisovy grupy.**

6.1. Uvažujme rozšíření $\mathbb{R} \leq \mathbb{C}$, určete $[\mathbb{C} : \mathbb{R}]_S$ a popište strukturu Galoisovy grupy rozšíření $\mathbb{R} \leq \mathbb{C}$. Jedná se o Galoisovo rozšíření?

Víme, že $\mathbb{C} = \mathbb{R}[i]$ a minimální polynom $m_i = x^2 + 1$. Protože je těleso $\mathbb{R}$ charakteristiky 0, je perfektní a tudíž $[\mathbb{C} : \mathbb{R}]_S = [\mathbb{C} : \mathbb{R}] = \deg m_i = 2$.

Protože každý $\mathbb{R}$-homomorfismus tělesa $\mathbb{C}$ je určen permutací kořenů polynomu $m_i = x^2+1$, je $\mathrm{Gal}(\mathbb{C}|\mathbb{R}) = \{\mathrm{id}, \overline{\mathrm{id}}\}$, kde $\overline{\mathrm{id}}(a+bi) = a-bi$ pro $a, b \in \mathbb{R}$. Rozšíření je zřejmě Galoisovo, jednak vidíme, že se $\mathbb{C}$ je rozkladové nadtěleso polynomu x^2+1 nebo můžeme argumentovat tím, že $|\mathrm{Gal}(\mathbb{C}|\mathbb{R})| = [\mathbb{C} : \mathbb{R}]_S$. □

6.2. Určete stupeň separability a popište strukturu Galoisovy grupy rozšíření $\mathbb{Q} \leq \mathbb{Q}[\sqrt{3}]$. Jedná se o Galoisovo rozšíření?

Protože minimální polynom prvku $\sqrt{3}$ nad $\mathbb{Q}$ je x^2-3 a těleso $\mathbb{Q}$ je opět perfektní, máme $[\mathbb{Q}[\sqrt{3}] : \mathbb{Q}]_S = [\mathbb{Q}[\sqrt{3}] : \mathbb{Q}] = \deg x^2 - 3 = 2$. Dále vidíme, že zobrazení $\varphi(a + b\sqrt{3}) = a - b\sqrt{3}$, kde $a, b \in \mathbb{Q}$, je $\mathbb{Q}$-automorfismus tělesa $\mathbb{Q}[\sqrt{3}]$, proto $\mathrm{Gal}(\mathbb{Q}[\sqrt{3}]|\mathbb{Q}) = \{\mathrm{id}, \varphi\}$ je opět dvou prvková (cyklická) grupa. Rozšíření je opět Galoisovo, neboť jde o rozkladové nadtěleso polynomu $x^2 - 3$. □

6.3. Určete stupeň separability a popište strukturu Galoisovy grupy rozšíření $\mathbb{Q} \leq \mathbb{Q}[\sqrt[3]{3}]$. Jedná se o Galoisovo rozšíření?

I tentokrát je stupeň separability roveň stupni rozšíření a $x^3 - 3$ je minimální polynom prvku $\sqrt{3}$, proto $[\mathbb{Q}[\sqrt[3]{3}] : \mathbb{Q}]_S = [\mathbb{Q}[\sqrt[3]{3}] : \mathbb{Q}] = \deg x^3 - 3 = 3$. Ovšem $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}[\sqrt[3]{3}]) = \{\mathrm{id}\}$, neboť zbývající dva prvky množiny $\mathrm{Hom}_{\mathbb{Q}}((\mathbb{Q}[\sqrt[3]{3}], \overline{\mathbb{Q}})$ nutně zobrazují prvek $\sqrt[3]{3}$ na ryze komplexní kořen polynomu $x^3 - 3$. To znamená, že rozšíření $\mathbb{Q} \leq \mathbb{Q}[\sqrt[3]{3}]$ není Galoisovo. □

6.4. Určete stupeň separability a popište strukturu Galoisovy grupy rozšíření konečných těles $\mathbb{F}_q \leq \mathbb{F}_{q^n}$. Jde o Galoisovo rozšíření?

I tentokrát pracujeme s perfektním tělesem, proto $[\mathbb{F}_{q^n} : \mathbb{F}_q]_S = [\mathbb{F}_{q^n} : \mathbb{F}_q] = n$. Dále snadno ověříme, že Frobeniův endomorfismus $f_q : \mathbb{F}_{q^n} \to \mathbb{F}_{q^n}$ daný vztahem $f_q(a) = a^q$ je $\mathbb{F}_q$-automorfismus tělesa $\mathbb{F}_{q^n}$, a proto $f_{q^i} = f_q^i$ jsou pro $i = 0, \ldots, n-1$ různé $\mathbb{F}_q$-automorfismus tělesa $\mathbb{F}_{q^n}$. Protože navíc $|\mathrm{Gal}(\mathbb{F}_{q^n}|\mathbb{F}_q)| \leq [\mathbb{F}_{q^n} : \mathbb{F}_q]_S = n$, dostáváme, že proto $\mathrm{Gal}(\mathbb{F}_{q^n}|\mathbb{F}_q) = \{\mathrm{id}, f_q, f_{q^2}, \ldots, f_{q^{n-1}}\}$ je n-prvková cyklická grupa. Protože $\mathbb{F}_{q^n}$ je rozkladové nadtěleso polynomu $x^{q^n} - x$, je rozšíření $\mathbb{F}_q \leq \mathbb{F}_{q^n}$ Galoisovo. $\square$

6.2. **Stopa a norma.**

6.5. Pro rozšíření $\mathbb{R} \leq \mathbb{C}$ a prvek $\alpha = a+bi$, kde $a, b \in \mathbb{R}$, spočítejte charakteristický polynom c_α prvku α, dále normu $\mathrm{N}_{\mathbb{C}|\mathbb{R}}(\alpha)$ a stopu $\mathrm{Tr}_{\mathbb{C}|\mathbb{R}}(\alpha)$.

Z dokázané věty plyne, že $c_\alpha = (x - a - bi)(x - a + bi) = x^2 - 2ax + a^2 + b^2$. Nyní z charakteristického polynomu dostávám, že $\mathrm{N}_{\mathbb{C}|\mathbb{R}}(\alpha) = a^2 + b^2 = |\alpha|^2$ a $\mathrm{Tr}_{\mathbb{C}|\mathbb{R}}(\alpha) = 2a = 2Re\alpha$ $\square$

6.6. Pro rozšíření $\mathbb{Q} \leq \mathbb{Q}[\sqrt{3}]$ a prvek $\alpha := a + b\sqrt{3}$, kde $a, b \in \mathbb{Q}$, spočítejte charakteristický polynom c_α prvku α, normu $\mathrm{N}_{\mathbb{Q}[\sqrt{3}]|\mathbb{Q}}(\alpha)$ a stopu $\mathrm{Tr}_{\mathbb{Q}[\sqrt{3}]|\mathbb{Q}}(\alpha)$.

Podobně jako v předchozí úloze spočítáme $c_\alpha = (x - a - b\sqrt{3})(x - a + b\sqrt{3}) = x^2 - 2ax + a^2 - 3b^2$, proto $\mathrm{N}_{\mathbb{C}|\mathbb{R}}(\alpha) = a^2 - 3b^2$ a $\mathrm{Tr}_{\mathbb{C}|\mathbb{R}}(\alpha) = 2a$. $\square$