1. Izomorfismy

Jsou-li $(G,\cdot,^{-1},1)$ a $(H,\cdot,^{-1},1)$ dvě grupy, pak se zobrazení $\varphi: G \to H$ nazývá (grupový) izomorfismus, jestliže je to bijekce a pro každé $a,b \in G$

$\varphi(a\cdot b) = \varphi(a)\cdot\varphi(b)$,
$\varphi(a^{-1}) = \varphi(a)^{-1}$,
$\varphi(1) = \varphi(1)$.

Obecně pro algebry $\mathcal{A}$ a $\mathcal{B}$ a zobrazení $\varphi: A \to B$ mezi jejich nosnými množinami platí, že je to izomorfismus, jestliže je φ bijekce a pro každý operační symbol σ arity n a každou dvojici jeho realizací $\sigma_{\mathcal{A}}$ a $\sigma_{\mathcal{B}}$jako operací na algebrách $\mathcal{A}$ a $\mathcal{B}$ platí

$$\varphi(\sigma_{\mathcal{A}}(a_1,\ldots,a_n)) = \sigma_{\mathcal{B}}(\varphi(a_1),\ldots,\varphi(a_n)) \quad \forall a_1,\ldots,a_n \in A.$$

1.1. Co znamená podmínka izomorfismu pro nulární operace?

Podle definice uvažujme pro prvky určené nulárními operacemi $\sigma_{\mathcal{A}}$, $\sigma_{\mathcal{B}}$, že se převedou zobrazí jeden na druhý, tedy $\varphi(\sigma_{\mathcal{A}}) = \sigma_{\mathcal{B}}$. □

1.2. Dokažte, že bijekce $f: G \to H$ dvou grup $(G,\cdot,^{-1},1)$ a $(H,\cdot,^{-1},1)$ je grupový izomorfismus právě když $f(a\cdot b) = f(a)\cdot f(b)$ pro každé $a,b \in G$.

Protože podmínka na levé straně ekvivalence je jednou ze tří definitorických podmínek, je přímá implikace triviální.

Předpokládejme, že $f(a\cdot b) = f(a)\cdot f(b)$ pro každé $a,b \in G$. Protože $f(1) = f(1\cdot 1) = f(1)\cdot f(1)$, stačí rovnost $f(1) = f(1)\cdot f(1)$ přenásobit prvkem $f(1)^{-1}$, abychom dostali $1 = f(1)\cdot f(1)^{-1} = f(1)\cdot f(1)\cdot f(1)^{-1} = f(1)$. Dále $1 = f(1) = f(a^{-1}\cdot a) = f(a^{-1})\cdot f(a)$ a podobně $1 = f(a)\cdot f(a^{-1})$, proto $f(a^{-1}) = (f(a))^{-1}$. □

1.3. Nechť $(G,\cdot,^{-1},1)$ a $(H,\cdot,^{-1},1)$ jsou grupy. Dokažte, že bijekce $f: G \to H$ je izomorfismus algeber $(G,\cdot,^{-1},1)$ a $(H,\cdot,^{-1},1)$ právě když je to izomorfismus algeber $(G,\cdot)$ a $(H,\cdot)$.

Tvrzení je jen reformulace předchozího tvrzení do jazyka algeber. □

1.4. Máme-li dvě algebry (A,Σ), (B,Σ) stejného typu s množinou operačních symbolů Σ a buď $f: A \to B$ je izomorfismus algeber (A,Σ), (B,Σ). Jestliže $\Omega \subseteq \Sigma$, dokažte, že je f izomorfismus algeber (A,Ω), (B,Ω)

Jde o úvahu stejného druhu jako u předchozích přímých implikací: je-li podmínka splněna pro všechny operace ze Σ, je splněna i pro všechny operace z množiny Ω. □

1.5. Dokažte, že izomorfismus grup i algeber tvoří (třídovou) ekvivalenci.

Stačí si všimnout, že identita je vždy izomorfismus, složení dvou izomorfismů (které lze skládat) a inverz k izomorfismu jsou opět izomorfismy. □

Jestliže mezi dvěma grupami $(G,\cdot,^{-1},1)$ a $(H,\cdot,^{-1},1)$ existuje izomorfismus, říkáme, že jsou *izomorfní* a píšeme $(G,\cdot,^{-1},1) \cong (H,\cdot,^{-1},1)$ nebo zkráceně $G_1 \cong G_2$.

1.6. Rozhodněte, zda jsou izomorfní následující dvojice grup.

(a) $(\mathbb{R}^2, +, -, 0)$ a $(\mathbb{C}, +, -, 0)$,
(b) $(\mathbb{R}, +, -, 0)$ a $(\mathbb{R}^+, \cdot, ^{-1}, 1)$,
(c) $(\mathbb{Z}_n, +, -, 0)$ a $(\{c \in (\mathbb{C}|\ c^n = 1\}, \cdot, ^{-1}, 1)$

(a) Ano, $\mathbb{R}^2$ a $\mathbb{C}$ jsou izomorfní dokonce jako reálné vektorové prostory, které mají vždy aditivní strukturu abelovské grupy, izomorfismem je tedy například zobrazení $(a, b) \to a + bi$.

(b) Ano, stačí uvážit exponenciálu $x \to e^x$.

(c) Ano, stačí uvážit komplexní exponenciálu $k \to e^{\frac{2\pi ik}{n}} = \cos\frac{2\pi k}{n} + i \sin\frac{2\pi k}{n}$. □

1.7. Rozhodněte, zda jsou izomorfní následující dvojice grup.

(a) $(\mathbb{Z}, +, -, 0)$ a $(\mathbb{R}, +, -, 0)$,
(b) $(\mathbb{Z}, +, -, 0)$ a $(\mathbb{Q}, +, -, 0)$,
(c) $(\mathbb{S}_4, \circ, ^{-1}, \mathrm{Id})$ a $(\mathbb{Z}_{24}, +, -, 0)$,
(c) $(\mathbb{S}_4, \circ, ^{-1}, \mathrm{Id})$ a $(\mathbb{Z}_2^3 \times \mathbb{Z}_3, +, -, 0)$,

(a) Ne, množiny $\mathbb{Z}$ a $\mathbb{R}$ nemají stejnou mohutnost, proto mezi nimi neexistuje bijekce.

(b) Ne, zatímco je grupa $(\mathbb{Z}, +, -, 0)$ cyklická, grupa $(\mathbb{Q}, +, -, 0)$ cyklická není, tj. $\langle q \rangle \neq \mathbb{Q}$ pro žádné racionální q. Kdyby existoval izomorfismus $g : \mathbb{Z} \to \mathbb{Q}$, pak by platilo, že

$$\mathbb{Q} = g(\mathbb{Z}) = g(\langle 1 \rangle) = \langle g(1) \rangle,$$

což je spor s faktem, že $(\mathbb{Q}, +, -, 0)$ cyklická není.

(c) Ne, grupa $(\mathbb{Z}_{24}, +, -, 0)$ je cyklická, zatímco $(\mathbb{S}_4, \circ, ^{-1}, \mathrm{Id})$ cyklická není. Dál bychom uvažovali stejně jako v předchozí úloze.

(d) Ne, grupa $(\mathbb{Z}_2^3 \times \mathbb{Z}_3, +, -, 0)$ je komutativní, zatímco $(\mathbb{S}_4, \circ, ^{-1}, \mathrm{Id})$ komutativní není. Předpokládejme, že existuje izomorfismus $h : \mathbb{S}_4 \to \mathbb{Z}_2^3 \times \mathbb{Z}_3$. Pak

$$h((12) \circ (23)) = h((12)) + h((23)) = h((23)) + h((12)) = h((23) \circ (12)),$$

tudíž díky prostotě h bychom měli $(12) \circ (23) = (23) \circ (12)$, což není pravda. □

9./11.3.

1.8. Rozhodněte, zda jsou izomorfní následující dvojice grup.

(a) $(\mathbb{Z}_6, +, -, 0)$ a $(\mathbb{Z}_2 \times \mathbb{Z}_3, +, -, (0, 0))$,
(b) $(\mathbb{Z}_9, +, -, 0)$ a $(\mathbb{Z}_3 \times \mathbb{Z}_3, +, -, (0, 0))$,
(c) $(\mathbb{Z}^2, +, -, (0, 0))$ a $(\mathbb{Z}^3, +, -, (0, 0, 0))$,
(d) $(\mathbb{Q}, +, -, (0, 0))$ a $(\mathbb{Q}^2, +, -, (0, 0))$,
(e) $(\mathbb{R}, +, -, (0, 0))$ a $(\mathbb{R}^2, +, -, (0, 0))$,

(a) Ano, stačí buď použít Čínské věty o zbytcích nebo si všimnout, že je grupa $(\mathbb{Z}_2 \times \mathbb{Z}_3, +, -, (0, 0))$ cyklická řádu 6 (s generátorem $(1, 1)$) stejně jako grupa $(\mathbb{Z}_6, +, -, 0)$.

(b) Ne, protože řád každého prvku grupy $(\mathbb{Z}_3 \times \mathbb{Z}_3, +, -, (0, 0))$ je nejvýše 3, zatímco grupa $(\mathbb{Z}, +, -, 0)$ je cyklická

(c) Ne, $(\mathbb{Z}^2, +, -, (0, 0))$ je generována dvěma prvky , ovšem, abychom dostali $(\mathbb{Z}^3, +, -, (0, 0, 0))$ potřebujeme aspoň 3 generátory (což plyne z vlastností bází ve vektorovém prostoru $\mathbb{Q}^3$, který $\mathbb{Z}^3$ obsahuje jako podgrupu). Snadno bychom

nahlédli, že izomorfní obraz množiny generátorů grupy je opět množina generátorů, tedy uvedená vlastnost je invariant.

(d) Ne, všimneme si, že grupa $(\mathbb{Q}^2, +, -, (0,0))$ obsahuje podgrupu izomorfní grupě $(\mathbb{Z}^2, +, -, (0,0))$ a že grupa $(\mathbb{Q}, +, -, (0,0))$ takovou podgrupu neobsahuje. I tentokrát je obvyklým způsobem verifikovatelné, že je tato vlastnost invariantem.

(e) Ano. Protože jsou $(\mathbb{R}, +, -, (0,0))$ a $(\mathbb{R}^2, +, -, (0,0))$ racionální vektorové prostory se stejně mohutnou (nespočetnou) bází, musí být izomorfní jako vektorové prostory, tudíž i jako grupy. □

1.9. Dokažte, že je invariantem pro každou algebru $(A, \circ)$ s binární operací $\circ$ vlastnost

a) existuje $a \in A$, pro něž platí $a \circ a = a$,
b) pro každé $a \in A$ platí $a \circ a = a$,
c) $|\{a \in A |\ a \circ a = a\}| = 2$,
d) $|\{a \in A |\ a \circ a = a\}| > 5$.

Uvážíme-li algebru s jednou binární operací $(B, \circ)$ a izomorfismus $\varphi : A \to B$ algebry $(A, \circ)$ do algebry $(B, \circ)$, pak prvek $a \in A$ splňující $a \circ a = a$ platí, že

$$\varphi(a) = \varphi(a \circ a) = \varphi(a) \circ \varphi(a)$$

a protože je zobrazení φ^{-1} je také izomorfismus platí pro každé $b \in B$ splňující $b \circ b = b$ i

$$\varphi(b)^{-1} = \varphi^{-1}(b \circ b) = \varphi^{-1}(b) \circ \varphi^{-1}(b).$$

Tudíž $a \circ a = a$, právě když $\varphi(a) \circ \varphi(a) = \varphi$. Odtud dostáváme, že všechny čtyři výroky jsou invarianty. □

Každé a algebry $(A, \circ)$ s binární operací $\circ$ splňující podmínku $a \circ a = a$ se nazývá *idempotentním* prvkem.

1.10. Dokažte, že

(a) $(\mathbb{R}, \cdot) \not\simeq (\mathbb{R}^2, \cdot)$,
(b) $(\mathbb{Z}, \cdot) \not\simeq (\mathbb{N}, \cdot)$,
(c) $(\mathbb{Q}, \cdot) \not\simeq (\mathbb{Q}^+, \cdot)$.

(a) Protože $(a,b) \cdot (a,b) = (a,b)$, právě když $a, b \in \{0,1\}$, obsahuje $(\mathbb{R}^2, \cdot)$ právě čtyři idempotentní prvky $(0,0), (0,1), (1,0), (1,1)$, zatímco $(\mathbb{R}, \cdot)$ je dva $(0,1)$. Dle předchozí úlohy tudíž nemůže jít o izomorfní algebry.

(b) Použijeme opět 1.9. Tentokrát $(\mathbb{Z}, \cdot)$ obsahuje právě idempotenty $0, 1$ a $(\mathbb{N}, \cdot)$ jen idempotent 1.

(c) Argumentace je stejná jako v (b). □

1.11. Rozhodněte, které dvojice následujících algeber jsou izomorfní:

$$(\mathbb{R}, +), \quad (\mathbb{R}, \cdot), \quad (\mathbb{R}^+, +), \quad (\mathbb{R}^+, \cdot).$$

Nejprve si všimneme, že $(\mathbb{R}, +) \simeq (\mathbb{R}^+, \cdot)$ podle 1.6 a že $(\mathbb{R}, +)$ obsahuje neutrální prvek a inverzní prvky, neboť má strukturu grupy. To ovšem znamená, že $(\mathbb{R}, +) \not\simeq (\mathbb{R}, \cdot)$ a $(\mathbb{R}, +) \not\simeq (\mathbb{R}^+, +)$ a tudíž i $(\mathbb{R}^+, \cdot) \not\simeq (\mathbb{R}, \cdot)$ a $(\mathbb{R}^+, \cdot) \not\simeq (\mathbb{R}^+, +)$. Konečně protože $(\mathbb{R}, \cdot)$ obsahuje dva idempotenty, zatímco $(\mathbb{R}^+, +)$ žádný i tentokrát dostáváme $(\mathbb{R}, \cdot) \not\simeq (\mathbb{R}^+, +)$. □

2. Homomorfismy a faktorizace

2.1. Najděte všechny homomorfismy aditivních grup:

a) $\mathbb{Z}_2 \to \mathbb{Z}_4$,
b) $\mathbb{Z}_4 \to \mathbb{Z}_2$,

Všimněme si, že homomorfismus cyklické grupy je určen obrazem generátoru a že homomorfní obraz 0 je opět 0. Homomorfismem je dále vždy zobrazení na neutrální prvek grupy, tj. na 0

(a) Jediným nenulovým homomorfismem je zobrazení určené obrazem $1 \to 2$, protože je řád prvku 1 v $\mathbb{Z}_2$ roven 2 a řád jeho obrazu musí číslo 2 dělit.

(b) Jediný možný nenulový homomorfismus je zobrazení dané obrazem jednotky, tedy $1 \to 1$. □

23./25.3.

2.2. Ověřte, že je $\mathcal{H}$ normální podgrupa $\mathcal{G}$ a rozhodněte, se kterou „známou" grupou je izomorfní faktorová grupa $\mathcal{G}/\mathcal{H}$, jestliže $n \in \mathbb{N}$ a

a) $\mathcal{G} = (\mathbb{S}_n, \circ, ^{-1}, \mathrm{Id})$ a $\mathcal{H} = (\mathbb{A}_n, \circ, ^{-1}, \mathrm{Id})$,
b) $\mathcal{G} = (\mathbb{Z}, +, -, 0)$ a $\mathcal{H} = (\langle n \rangle, +, -, 0)$,
c) $\mathcal{G} = (\mathbb{C}, +, -, 0)$ a $\mathcal{H} = (\mathbb{R}, +, -, 0)$,
d) $\mathcal{G} = (\mathbb{C}^*, \cdot, ^{-1}, 1)$ a $\mathcal{H} = (\mathbb{R}^+, \cdot, ^{-1}, 1)$,
e) $\mathcal{G} = (GL_n(\mathbb{R}), \cdot, ^{-1}, I_n)$ (reálné regulární matice stupně n) a $\mathcal{G} = (\{A \in GL_n(\mathbb{R}) | \det(A) = 1\}, \cdot, ^{-1}, I_n)$.

Ve všech případech bude užitečné použít 1.větu o izomorfismus. Vždy se pokusíme najít (známý) homomorfismus grupy $\mathcal{G}$ na (známou) grupu jehož jádro je právě podgrupa $\mathcal{H}$. Protože je jádro homomorfismu normální podgrupa, odpadne nám také problém s dokazováním normality $\mathcal{H}$:

(a) Stačí uvážit grupový homomorfismus znaménko $\mathrm{sgn} : \mathbb{S}_n \to \{-1, 1\}$. Navíc si uvědomíme, že je grupa $(\{-1, 1\}, \cdot, ^{-1}, 1)$ dvouprvková cyklická, tedy izomorfní aditivní grupě $\mathbb{Z}_2$.

(b) Tentokrát uvážíme homomorfismus $\mathbb{Z} \to \mathbb{Z}_n$ daný předpisem $z \to (z) \mathrm{mod}\ n$. Proto $\mathcal{G}/\mathcal{H} \cong (\mathbb{Z}_n, +, -, 0)$.

(c) Nyní stačí vzít projekci komplexních čísel na jejich imaginární část, tudíž $\mathcal{G}/\mathcal{H} \cong (\mathbb{R}, +, -, 0)$.

(d) Vezmeme-li zobrazení $c \to \frac{c}{\|c\|}$ dostáváme právě projekci na jednotkovou kružnici v $\mathbb{C}^*$ což je tedy v tomto případě grupa izomorfní $\mathcal{G}/\mathcal{H}$.

(e) Uvědomíme-li si, že determinant je homomorfismus grupy $(GL_n(\mathbb{R}), \cdot, ^{-1}, I_n)$ do $(\mathbb{R}^*, \cdot, ^{-1}, 1)$, vidíme, že hledanou izomorfní grupou je právě $(\mathbb{R}^*, \cdot, ^{-1}, 1)$. □

2.3. Označíme-li $\mathcal{C}^* = (\mathbb{C}^*, \cdot, ^{-1}, 1)$ grupu nenulových komplexních čísel s násobením, a položme $\mathbb{C}_n = \{z \in \mathbb{C}^* \mid z^n = 1\}$, dokažte, že platí $\mathcal{C}^*/\mathcal{C}_n \simeq \mathcal{C}^*$

Opět využijeme 1.větu o izomorfismu aplikovanou na homomorfismus $(-)^n : \mathcal{C}^*\mathcal{C}^*$ daný vztahem $c \to (c)^n$. □

2.4. Najděte všechny homomorfismy grupy $\mathcal{G}$ do grupy $\mathcal{H}$, jestliže:

a) $\mathcal{G} = \mathcal{H} = (\mathbb{Z}, +, -, 0)$,
b) $\mathcal{G} = (\mathbb{Z}, +, -, 0)$ a $\mathcal{H} = (\mathbb{Z}_n, +, -, 0)$,
c) $\mathcal{G} = (\mathbb{Z}_n, +, -, 0)$ a $\mathcal{H} = (\mathbb{Z}, +, -, 0)$,

d) $\mathcal{G} = (\mathbb{Z}_n, +, -, 0)$ a $\mathcal{H} = (\mathbb{Z}_m, +, -, 0)$,
e) $\mathcal{G} = (\mathbb{S}_n, \circ, ^{-1}, \mathrm{Id})$ a $\mathcal{H} = (\mathbb{Z}_m, +, -, 0)$ pro $n > 4$.
f) $\mathcal{G} = (\mathbb{Z}_n, +, -, 0)$ a $\mathcal{H} = (\mathbb{S}_m, \circ, ^{-1}, \mathrm{Id})$,

(a) Homomorfismus cyklické grupy je určen obrazem generátoru, tedy homomorfismy jsou tvaru $f_z(x) = zx$ pro libovolné $z \in \mathbb{Z}$.

(b) Platí úvaha s omezením, že $f_z(x) = (zx) \mathrm{mod}\ n$ pro $z \in \mathbb{Z}_n$.

(c) Podle 1.věty o izomorfismu je homomorfní obraz podgrupou izomorfní faktoru $(\mathbb{Z}_n, +, -, 0)$. Ovšem grupa $(\mathbb{Z}, +, -, 0)$ obsahuje pouze triviální konečnou grupu, proto je jediným homomorfismem $\mathbb{Z}_n \to \mathbb{Z}$ nulový homomorfismus.

(d) Podle 1.věty o izomorfismu stačí uvažovat jen faktory grupy $(\mathbb{Z}_n, +, -, 0)$ jejichž řád dělí řád grupy $(\mathbb{Z}_m, +, -, 0)$, největším takovým je faktor izomorfní $(\mathbb{Z}_d, +, -, 0)$, kde $d = \gcd(n, m) = 4$. Protože každý homomorfismus $(\mathbb{Z}_d, +, -, 0)$ do $(\mathbb{Z}_m, +, -, 0)$ je určen obrazem generátoru do jednoznačně určené podgrupy grupy $(\mathbb{Z}_m, +, -, 0)$ řádu d (ta je generovaná prvkem $a = \frac{m}{d}$), existuje homomorfismů $(\mathbb{Z}_d, +, -, 0)$ do $(\mathbb{Z}_m, +, -, 0)$ právě d a jsou tvaru $g_z(x) = (zax) \mathrm{mod}\ m$ pro $z \in \mathbb{Z}_d$. Uvážíme-li, že je zobrazení $\mathbb{Z}_n \to \mathbb{Z}_d$ daný vztahem $y \to (y) \mathrm{mod}\ d$ homomorfismus na $\mathbb{Z}_d$, pak je každý homomorfismus $(\mathbb{Z}_n, +, -, 0)$ do $(\mathbb{Z}_m, +, -, 0)$ právě tvaru $f_z(x) = g_z((x) \mathrm{mod}\ d) = (za \cdot (x) \mathrm{mod}\ d) \mathrm{mod}\ m$ pro $z \in \mathbb{Z}_d$.

(e) Připomeneme-li, že všechny podgrupy cyklické grupy jsou opět cyklické, musí být homomorfní obraz $(\mathbb{S}_n, \circ, ^{-1}, \mathrm{Id})$ také cyklický. Připomeneme-li, že $\{1\}$, $\mathbb{A}_n$ a $\mathbb{S}_n$ jsou jediné normální podgrupy $(\mathbb{S}_n, \circ, ^{-1}, \mathrm{Id})$ pro všechna $n \neq 4$ a že $\mathbb{S}_n/\{1\} \cong \mathbb{S}_n$ není komutativní, a proto ani cyklická, zbývají jen dvouprvkové cyklické faktory $\mathbb{S}_n/\mathbb{A}_n$. Tedy pro n lichá máme pouze triviální homomorfismus a pro n sudá přibude ještě homomorfismus $\sigma \to \frac{-(\mathrm{sgn}\ +1) \cdot n}{2 \cdot 2}$.

8./20.4.

(f) Tentokrát víme, že jsou homomorfismy určeny obrazem generátoru, který je podle 1.věty o izomorfismu právě prvek řádu, který dělí řád n. Stačí nám tedy vzít všechny prvky grupy $\mathbb{S}_m, \circ, ^{-1}, \mathrm{Id})$ řádu, který dělí řád n, označme je A. Potom je je každý homomorfismus $(\mathbb{Z}_n, +, -, 0)$ do $\mathbb{S}_m, \circ, ^{-1}, \mathrm{Id})$ právě tvaru $\varphi_a(x) = a^x$ pro $x \in \mathbb{Z}_n$. □

2.5. Kolik existuje homomorfismů mezi každou z dvojic grup
$(\mathbb{Z}_{140}, +, -, 0)$, $(\mathbb{Z}_{72}, +, -, 0)$ $(\mathbb{Z}, +, -, 0)$ a $(\mathbb{S}_4, \circ, ^{-1}, \mathrm{Id})$?

Využijeme-li předchozí úlohu a označíme $\mathrm{Hom}(G, H)$ množinu všech homomorfismů $\mathcal{G} \to \mathcal{H}$, snadno spočítáme, že

- $|\mathrm{Hom}(\mathbb{Z}_{140}, \mathbb{Z}_{72})| = \gcd(140, 72) = 4$,
- $|\mathrm{Hom}(\mathbb{Z}_{140}, \mathbb{Z})| = 1$,
- $|\mathrm{Hom}(\mathbb{Z}_{140}, S_4)| = 1 + \frac{4 \cdot 3}{2!} + \frac{4!}{4} = 13$,
- $|\mathrm{Hom}(\mathbb{Z}_{72}, \mathbb{Z}_{140})| = \gcd(140, 72) = 4$,
- $|\mathrm{Hom}(\mathbb{Z}_{72}, \mathbb{Z})| = 1$,
- $|\mathrm{Hom}(\mathbb{Z}_{72}, S_4)| = |\mathbb{S}_4| = 24$,
- $|\mathrm{Hom}(\mathbb{Z}, \mathbb{Z}_{140})| = 140$,
- $|\mathrm{Hom}(\mathbb{Z}, \mathbb{Z}_{72})| = 72$,
- $|\mathrm{Hom}(\mathbb{Z}, S_4)| = |\mathbb{S}_4| = 24$,
- $|\mathrm{Hom}(\mathbb{S}_4, \mathbb{Z}_{140})| = 2$,
- $|\mathrm{Hom}(\mathbb{S}_4, \mathbb{Z}_{72})| = 2$,
- $|\mathrm{Hom}(\mathbb{S}_4, Z| = 1$.

□

2.6. Spočítejte kolika způsoby lze obarvit stěny krychle (bez ohledu na její polohu) pomocí n barev.

Nejprve definujme množinu X jako množinu všech obarvení krychle v pevné pozici (tj. přiřazujeme barvu 6 pozicím s ohledem na jejich polohu) a G grupu všech otočení krychle. Konečně otočení g přiřadí obarvení x příslušně otočení krychle $g(x)$. Zřejmě jde o působení G na množině X. Všimněme si, že dvě obarvení z množiny X jsou ekvivalentní vzhledem k ekvivalenci $\sim$, pokud lze jedno převést na druhé nějakým otočením krychle. To znamená, že počet všech obarvení krychle bez ohledu na její otočení je právě roven počtu rozkladových tříd $|X/\sim|$. Nyní využijeme Burnsideova lemmatu $|X/\sim| = \frac{1}{|G|}\sum_{g\in G}|X_g|$, kde $X_g = xzX|g(x) = x$.

Uvědomme si, že grupa otočení G obsahuje právě 24 prvků (otočení můžeme reprezentovat zobrazením stěny na jednu z 6 stěn ve 4 pozicích, případně zobrazením jednoho vrcholu na 8 vrcholů s trojicí hran, které z něj vybíhají). Každé otočení můžeme reprezentovat jako permutaci stěn, které se k tomuto účelu očíslujeme čísly 1,...,6 (tedy grupu G chápeme jako podgrupu S_6). Konečně poznamenejme, že má-li zůstat při konkrétním otočení zachováno obarvení krychle, musí být obarvení všech stěn v jednom cyklu stejné. Tedy potřebujeme zjistit, kolik cyklů každá z permutací odpovídající danému otočení obsahuje (je-li jich v permutaci g právě k, pak $|X_g| = n^k$. Probereme jednotlivé případy:

(1) 6 cyklů obsahuje pouze $g = \mathrm{Id}$, tedy $|X_g| = n^6$,
(2) 4 cykly obsahují 3 osové symetrie podle os procházejících středy protilehlých stěn, tj.
$$g \in \{(13)(24), (13)(53), (24)(56)\}$$
a $|X_g| = n^4$,
(3) 3 cykly obsahuje 6 otočení o 90 stupňů vpravo a vlevo podle os procházejících středy protilehlých stěn, tj
$$g \in \{(1234), (1432), (1635), (1536), (2645), (2546)\}$$
a 6 překlopení podle os procházejících středy protilehlých hran, tedy g leží v množině
$$\{(13)(64)(25), (13)(26)(45), (24)(16)(35), (24)(15)(36), (56)(14)(23), (56)(12)(34)\}$$
a $|X_g| = n^3$,
(4) 2 cykly obsahuje 8 otočení o 120 stupňů vpravo a vlevo podle os procházejících protilehlými vrcholy, tj. g leží v množině $\{(164)(235), (146)(253), (126)(345), (162)(354), (145)(263), (154)(236), (125)(634), (125)(634)\}$ a $|X_g| = n^2$,

Tedy zjistili jsme, že $|X/\sim| = \frac{1}{24}(n^6 + 3n^4 + 12n^3 + 8n^2)$. □

22.4.

2.7. Určete kolika způsoby lze krychli obarvit (bez ohledu na její polohu) pomocí 3 barev

Stačí dosadit do odvozeného vzorečku: $\frac{1}{24}(3^6 + 3\cdot 3^4 + 12\cdot 3^3 + 8\cdot 3^2) = 57$. □

3. Okruhy a tělesa

3.1. Uvažujme okruh $\mathcal{Z} = (\mathbb{Z}, +, -, \cdot, 0, 1)$ a zvolme $n \in \mathbb{Z}$.

a) Dokažte, že $(n) = \{nz |\ z \in \mathbb{Z}\}$ je ideál $\mathcal{Z}$,
b) popište všechny ideály $\mathcal{Z}$,
c) kolik prvků má faktor $\mathcal{Z}/(n)$?

(a) Víme, že (n) je podgrupa komutativní grupy $(\mathbb{Z}, +, -, 0)$, zbývá si všimnout, že pro každé $z, t \in \mathbb{Z}$ $nzt \in (n)$¨.

(b) Protože je každý ideál podgrupou aditivní grupy okruhu a $(\mathbb{Z}, +, -, 0)$ obsahuje právě cyklické podgrupy, tvoří množinu všech ideálů okruhu $\mathcal{Z}$ podle (a) právě systém $\{(n) |\ n \in \mathbb{N} \cup \{0\}\}$

(c) Podle První věty o izomorfismu je $\mathcal{Z}/(n) \cong Z_n$, proto $|\mathbb{Z}/(n)| = |Z_n| = n$. □

3.2. Najděte všechny ideály okruhů $\mathcal{Z}_n = (\mathbb{Z}_n, +, -, \cdot, 0, 1)$ pro $n = 5, 8, 15$ a pro obecné n.

Stejně jako v předchozím příkladě stačí prozkoumat podgrupy příslušných cyklických grup. Tedy generátory jsou právě dělitelé čísla n. Konkrétně

podgrupy $\mathbb{Z}_5$ jsou jen $\{0\}, \mathbb{Z}_5$,
podgrupy $\mathbb{Z}_8$ jsou $\{0\}, 2\mathbb{Z}_8, 4\mathbb{Z}_8, \mathbb{Z}_8$,
a podgrupy $\mathbb{Z}_{15}$ jsou $\{0\}, 3\mathbb{Z}_{15}, 5\mathbb{Z}_{15}, \mathbb{Z}_{15}$.

□

3.3. Spočtěte prvky nejmenšího ideálu okruhu $(\mathbb{Z}, +, -, \cdot, 0, 1)$ obsahujícího a) $28, 63$, b) $15, 18, 40$.

I tentokrát využijeme toho, že ideály okruhu $(\mathbb{Z}, +, -, \cdot, 0, 1)$ a podgrupy grupy $(\mathbb{Z}, +, -, 0)$ splývají. Generátory ideálů jsou tedy generátory cyklických podgrup, které najdeme jako největší společné dělitele. To znamená, že

$$(28) + (63) = (\gcd(28, 63))\mathbb{Z} = 7\mathbb{Z}, (15) + (18) + (40) = (\gcd(15, 18, 40))\mathbb{Z} = 1\mathbb{Z} = \mathbb{Z}.$$

□

3.4. Spočtěte prvky nejmenšího ideálu okruhu $\mathbb{Q}$ obsahujícího $\frac{3}{4}$.

Protože je $\mathbb{Q}$ těleso, tak nejmenšího ideálu $(\frac{3}{4})$ obsahující $\frac{3}{4}$ je celé $\mathbb{Q}$ □

3.5. Popište všechny ideály okruhů a) $(\mathbb{Q}[x], +, -, \cdot, 0, 1)$, b) $(\mathbb{Z}_p[x], +, -, \cdot, 0, 1)$ pro p prvočíslo. Které z nich jsou maximální?

Protože jsou okruhy $(\mathbb{Q}, +, -, \cdot, 0, 1)$ i $(\mathbb{Z}_p, +, -, \cdot, 0, 1)$ tělesa, víme, že $(\mathbb{Q}[x], +, -, \cdot, 0, 1)$ i $(\mathbb{Z}_p[x], +, -, \cdot, 0, 1)$ jsou Ekleidovské obory, tedy obory hlavních ideálů, tedy všechny ideály jsou tvaru $u\mathbb{Q}[x]$, resp. $u\mathbb{Z}_p[x]$ pro nějaký polynom u.

Máme dokázáno, že hlavní ideál generovaný prvkem u jakéhokoli oboru hlavních ideálů je maximální, právě když je u ireducibilní. To znamená , že $u\mathbb{Q}[x]$, resp. $u\mathbb{Z}_p[x]$ je maximální právě pro u ireducibilní polynomy. □

3.6. Rozhodněte, zda je ireducibilní

a) polynom $x^2 - 2$ v oboru $(\mathbb{Q}[x], +, -, \cdot, 0, 1)$,
b) polynom $x^2 + 1$ v oboru $(\mathbb{Z}_5[x], +, -, \cdot, 0, 1)$.

a) x^2-2 umíme rozložit nad reálnými čísly na součin $x^2-2=(x-\sqrt{2})(x+\sqrt{2})$, ale protože $\sqrt{2}\notin\mathbb{Q}$, je polynom x^2-2 v oboru $(\mathbb{Q}[x],+,-,\cdot,0,1)$ ireducibilní.

b) protože v $(\mathbb{Z}_5[x],+,-,\cdot,0,1)$ máme $x^2+1=x^2-4=(x-2)(x-3)$, je tento polynom reducibilní. □

3.7. Dokažte, že je $\mathbb{Q}[x]/(x^2-2)\mathbb{Q}[x]$ těleso izomorfní tělesu $\mathbb{Q}[\sqrt{2}]$.

Stačí uvážit dosazovací homomorfismus $\Omega_{\sqrt{2}}\mathbb{Q}[x]\to\mathbb{R}$ daný předpisem $\Omega_{\sqrt{2}}(f)=f(\sqrt{2})$. Potom snadno nahlédneme, že $\operatorname{Ker}\Omega_{\sqrt{2}}=(x^2-2)\mathbb{Q}[x]$ a díky První větě o izomorfismu dostáváme

$$\mathbb{Q}[x]/(x^2-2)\mathbb{Q}[x]=\mathbb{Q}[x]/\operatorname{Ker}\Omega_{\sqrt{2}}\cong\Omega_{\sqrt{2}}(\mathbb{Q}[x])=\mathbb{Q}[\sqrt{2}]$$

□

3.8. Uvažujme tělesa reálných čísel $\mathbf{R}$ a jeho podtěleso racionálních čísel $\mathbf{Q}$.

(a) Dokažte , že je prvek $\sqrt{3}$ algebraický nad $\mathbf{Q}$,
(b) spočítejte stupeň rozšíření $[\mathbf{Q}(\sqrt{3}):\mathbf{Q}]$,
(c) najděte nad $\mathbf{Q}$ minimální polynom prvku $\sqrt{3}$,
(d) ověřte, že je prvek $2+5\sqrt{3}$ algebraický nad $\mathbf{Q}$ a najděte jeho minimální polynom nad $\mathbf{Q}$,
(e) ověřte, že $\frac{2-\sqrt{3}}{3+\sqrt{3}}$ je algebraický prvek nad $\mathbf{Q}$ a najděte jeho minimální polynom nad $\mathbf{Q}$,
(f) dokažte , že je prvek $\sqrt[3]{2}$ algebraický nad $\mathbf{Q}$,
(g) najděte nad $\mathbf{Q}$ minimální polynom prvku $\sqrt[3]{2}$ a spočítejte stupeň rozšíření $[\mathbf{Q}(\sqrt[3]{2}):\mathbf{Q}]$,
(h) ověřte, že $[\mathbf{Q}(\sqrt[3]{2},\sqrt[5]{5}):\mathbf{Q}]\leq 15$,
(i) najděte nějakou generující množinu vektorového prostoru $\mathbf{Q}(\sqrt[3]{2},\sqrt[5]{5})$ nad tělesem $\mathbf{Q}$.

(a) Prvek α je podle definice algebraický nad $\mathbf{Q}$, právě když existuje polynom $p\in\mathbf{Q}[x]$, jehož je α kořenem. V našem případě okamžitě vidíme, že $\sqrt{3}^2=3$, a proto je $\sqrt{3}$ kořenem polynom $x^2-3\in\mathbf{Q}[x]$.

(b) Nahlédneme, že je těleso $\mathbf{Q}(\sqrt{3})$, tedy nejmenší podtěleso tělesa $\mathbf{R}$ obsahující množinu $\mathbf{Q}\cup\{\alpha\}$, rovno množině $A=\{a+b\sqrt{3}\in\mathbf{R}|\ a,b\in\mathbf{Q}\}$. Protože pro každé $a,b\in\mathbf{Q}$, máme z uzavřenosti na operace $a,b,b\sqrt{3},a+b\sqrt{3}\in,Q(\sqrt{3})$, proto $A\subseteq Q(\sqrt{3})$. Přitom je A zjevně množina uzavřená na sčítání, odčítání a násobení a $0,1\in A$, tedy je A podokruh okruhu $\mathbf{R}$. Vezmeme-li nenulové $a+b\sqrt{3}\in A$, potom $(a+b\sqrt{3})^{-1}=\frac{(a-b\sqrt{3})}{(a+b\sqrt{3})(a-b\sqrt{3})}=\frac{a}{a^2-3b^2}-\frac{b}{a^2-3b^2}\sqrt{3}\in A$, protože $\frac{a}{a^2-3b^2}\in\mathbf{Q}$ a $-\frac{b}{a^2-3b^2}\in\mathbf{Q}$. To znamená, že je A podtěleso tělesa $\mathbf{Q}(\sqrt{3})$ obsahující $\mathbf{Q}\cup\{\alpha\}$, proto $A=\mathbf{Q}(\sqrt{3})$.

Tím jsme ukázali, že $\mathbf{Q}(\sqrt{3})$ je jako racionální vektorový prostor generováno prvky 1 a $\sqrt{3}$. Ověříme, že jde o lineárně nezávislou množinu. Předpokládejme, že je $\sqrt{3}$ racionální, tj. existují nesoudělná přirozená c a j, pro která $\sqrt{3}=\frac{c}{j}$, a proto $c^2=3j^2$. Potom $3/c$, tedy $9/c^2$, a proto $3/j$, spor s nesoudělností c a j. Protože je prvek $\sqrt{3}$ iracionální, není racionálním násobkem prvku 1, tudíž je lineárně nezávislý na 1. Našli jsme dvouprvkovou bázi $\mathbf{Q}(\sqrt{3})$ chápaného jako vektorový prostor nad tělesem $\mathbf{Q}(\sqrt{3})$, tedy $[\mathbf{Q}(\sqrt{3}):\mathbf{Q}]=\dim_{\mathbf{Q}}\mathbf{Q}(\sqrt{3})=2$.

(c) Připomeňme, že minimální polynom $m \in \mathbf{Q}[x]$ prvku α je ireducibilní monický polynom, jehož kořenem je α, ekvivalentně je m monický polynom nejmenšího možného stupně, jehož kořenem je α. Navíc bylo na přednášce dokázáno, že $\deg(\sqrt{3}) = [\mathbf{Q}(\sqrt{3}) : \mathbf{Q}]$. Využijeme-li pozorování $[\mathbf{Q}(\sqrt{3}) : \mathbf{Q}] = 2$ a všimneme-li, že jsme v (a) už polynom stupně 2 s kořenem $\sqrt{3}$ našli, tedy nutně musí jít o minimální polynom. Tedy $x^2 - 3$ je minimální polynom prvku $\sqrt{3}$ nad $\mathbf{Q}$.

(d,e) Na přednášce bylo dokázáno, že každé rozšíření konečného stupně je algebraické, tedy díky (b) je každý prvek $\mathbf{Q}(\sqrt{3})$ algebraický nad $\mathbf{Q}$. Protože $2 + 5\sqrt{3}, \frac{2-\sqrt{3}}{3+\sqrt{3}} \in \mathbf{Q}(\sqrt{3})$, jde o prvky algebraické nad $\mathbf{Q}$.

Dále víme, že každé tři prvky vektorového prostoru dimenze 2 musí být lineárně závislé, tedy existuje netriviální racionální lineární kombinace $q_0 + q_1(2 + 5\sqrt{3}) + q_2(2 + 5\sqrt{3})^2 = q_1 + q_2(2 + 5\sqrt{3}) + q_2(79 + 20\sqrt{3}) = 0$. Vyjádřeno v souřadnicích vzhledem k bázi $1, \sqrt{3}$ řešíme homogenní soustavu lineárních rovnic $q_0 + 2q_1 + 79q_2 = 0$, $5q_1 + 20q_2 = 0$ s maticí $\begin{pmatrix} 1 & 2 & 79 \\ 0 & 5 & 20 \end{pmatrix}$. Tedy řešením je například vektor $(q_0, q_1, q_2) = (-71, -4, 1)$, což znamená, že je algebraický prvek $2 + 5\sqrt{3}$ kořenem polynomu $m_1 = x^2 - 4x - 71$.

Podobně budeme uvažovat o prvku $\frac{2-\sqrt{3}}{3+\sqrt{3}}$. Nejprve ho ovšem vyjádříme v bázi $1, \sqrt{3}$, tedy $\frac{2-\sqrt{3}}{3+\sqrt{3}} = \frac{(2-\sqrt{3})(3-\sqrt{3})}{(3+\sqrt{3})(3-\sqrt{3})} = \frac{9-5\sqrt{3}}{6}$ a opět hledáme $q_i \in \mathbf{Q}$, aby $q_0 + q_1\frac{9-5\sqrt{3}}{6} + q_2(\frac{9-5\sqrt{3}}{6})^2 = 0$, tedy $36q_0 + q_1(54 - 30\sqrt{3}) + q_2(156 - 90\sqrt{3}) = 0$. Řešíme proto soustavu s maticí

$$\begin{pmatrix} 36 & 54 & 156 \\ 0 & -30 & -90 \end{pmatrix} \sim \begin{pmatrix} 6 & 0 & -1 \\ 0 & 1 & 3 \end{pmatrix}.$$

Tedy snadno najdeme řešení $(q_0, q_1, q_2) = (-\frac{1}{6}, -3, 1)$, jemuž odpovídá monický polynom $m_2 = x^2 - 3x - \frac{1}{6}$ s kořenem $\frac{2-\sqrt{3}}{3+\sqrt{3}}$. Protože jsou oba polynomy m_1 a m_2 monické stupně dva a ani jedno z uvažovaných iracionálních čísel není kořenem racionálního polynomu stupně jedna, je m_1 minimální polynom prvku $2 + 5\sqrt{3}$ nad $\mathbf{Q}$ a m_2 minimální polynom prvku $\frac{2-\sqrt{3}}{3+\sqrt{3}}$ nad $\mathbf{Q}$.

(f) Jako v (a) stačí uvážit, že $\sqrt[3]{2}$ je kořenem polynom $x^3 - 2 \in \mathbf{Q}[x]$.

(g) Protože minimální polynom určitě dělí $x^3 - 2$ v oboru $\mathbf{Q}[x]$, máme $[\mathbf{Q}(\sqrt[3]{2}) : \mathbf{Q}] \leq \deg(x^3 - 2) = 3$. To znamená, že mocniny prvku $(\sqrt[3]{2})^0 = 1$, $(\sqrt[3]{2})^1 = \sqrt[3]{2}$ a $(\sqrt[3]{2})^2 = \sqrt[3]{4}$ generují vektorový prostor $\mathbf{Q}(\sqrt[3]{2})$ nad tělesem $\mathbf{Q}$. Ukážeme, že se jedná o bázi $\mathbf{Q}(\sqrt[3]{2})$.

6.5.

(h) Uvážíme-li, že podle (b) je $[\mathbf{Q}(\sqrt{3}) : \mathbf{Q}] = 3$ a že prvek $\sqrt[5]{5}$ je kořenem polynomu $x^5 - 5$, který můžeme chápat jako polynom nad tělesem $\mathbf{Q}(\sqrt[3]{2})$, tedy stupeň minimálního polynomu prvku $\sqrt[5]{5}$ nad $\mathbf{Q}(\sqrt[3]{2})$ je nejvýše 5, proto $[\mathbf{Q}(\sqrt[3]{2}, \sqrt[5]{5}) : \mathbf{Q}(\sqrt[3]{2})] \leq 5$. Podle pozorování z přednášky je

$$[\mathbf{Q}(\sqrt[3]{2}, \sqrt[5]{5}) : \mathbf{Q}] = [\mathbf{Q}(\sqrt[3]{2}, \sqrt[5]{5}) : \mathbf{Q}(\sqrt[3]{2})] \cdot [\mathbf{Q}(\sqrt{3}) : \mathbf{Q}] \leq 5 \cdot 3 = 15.$$

(i) Stačí si podrobněji prohlédnout důkazy tvrzení využívaných v (h), abychom zjistili, že množina $\{\sqrt[3]{2}^i \cdot \sqrt[5]{5}^j \mid i = 0, 1, 2; j = 0, 1, 2, 3, 4\}$, protože $1, \sqrt[3]{2}, \sqrt[3]{2}^2$ generuje $\mathbf{Q}(\sqrt[3]{2})$ nad $\mathbf{Q}$ $1, \sqrt[5]{5}, \sqrt[5]{5}^2, \sqrt[5]{5}^3, \sqrt[5]{5}^4$ generuje $\mathbf{Q}(\sqrt[3]{2}, \sqrt[5]{5})$ nad $\mathbf{Q}(\sqrt[3]{2})$. □

3.9. Uvažujme faktorový okruh $\mathbf{Q}[x]/(x^3-2)\mathbf{Q}[x]$ okruhu polynomů $(\mathbf{Q}[x],+,-,0,\cdot,1)$.

(a) Dokažte, že je $\mathbf{Q}[x]/(x^3-2)\mathbf{Q}[x]$ těleso,
(b) ověřte, že $\mathbf{Q}[x]/(x^3-2)\mathbf{Q}[x] \cong Q(\sqrt[3]{2})$,
(c) ověřte, že $(x+1)+(x^3-2)\mathbf{Q}[x] = (x^3+x-1)+(x^3-2)\mathbf{Q}[x]$,
(d) najděte v $\mathbf{Q}[x]/(x^3-2)\mathbf{Q}[x]$ inverzní prvek k prvku $x+1+(x^3-2)\mathbf{Q}[x]$.

(a) Protože je podle 3.8(c) polynom x^3-2 minimálním polynomem prvku $\sqrt[3]{2}$ nad $\mathbf{Q}$, jedná se o nerozložitelný polynom okruhu $(\mathbf{Q}[x],+,-,0,\cdot,1)$, tedy je hlavní ideál $(x^3-2)\mathbf{Q}[x]$ maximální. Nyní stačí připomenou, že faktor komutativního okruhu podle maximálního ideálu je těleso.

(b) Vezmeme-li dosazovací homomorfismus $\mathrm{Id}_{\sqrt[3]{2}} : \mathbf{Q}[x] \to \mathbf{Q}(\sqrt[3]{2})$, vidíme díky 3.8, že jde o homomorfismus na a jádro $\mathrm{Ker}(\mathrm{Id}_{\sqrt[3]{2}}) = (x^3-2)\mathbf{Q}[x]$. Díky první větě o izomorfismu dostáváme $\mathbf{Q}[x]/(x^3-2)\mathbf{Q}[x] = \mathbf{Q}[x]/\mathrm{Ker}(\mathrm{Id}_{\sqrt[3]{2}}) \cong Q(\sqrt[3]{2})$.

(c) Připomeňme, že dvě rozkladové třídy podle ideálu I splývají, jestliže rozdíl jejich reprezentantů leží v I. Tedy stačí nahlédnout, že $(x^3+x-1)-(x+1) = x^3-2 \in (x^3-2)\mathbf{Q}[x]$.

(d) Najdeme-li Eukleidovým algoritmem polynomy $q, r \in \mathbf{Q}[x]$, aby $(x+1)q + (x^3-2)r = c$, kde c je invertibilní, vidíme, že $c^{-1}q$ je prvek rozkladové třídy hledaného inverzu. Tedy vydělíme se zbytkem $x^3-2 = (x+1)(x^2-x+1)-3$, a proto $-3 = -(x+1)(x^2-x+1)+(x^3-2)$ a $1 = (x+1)\frac{1}{3}(x^2-x+1)-\frac{1}{3}(x^3-2)$. Tudíž $(x+1+(x^3-2)\mathbf{Q}[x])^{-1} = \frac{1}{3}(x^2-x+1)+(x^3-2)\mathbf{Q}[x]$. □

3.10. Najděte kořenové nadtěleso polynomu $p \in T[x]$ nad tělesem T, jestliže

(a) $T = \mathbf{Q}$ a $p = x^3-1$,
(b) $T = \mathbf{Q}$ a $p = x^3-2$,
(c) $T = \mathbf{Z}_2$ a $p = x^2+1$,
(d) $T = \mathbf{Z}_2$ a $p = x^2+x+1$.

(a) Protože je $1 \in \mathbf{Q}$ kořenem polynomu x^3-1, je samotné těleso $\mathbf{Q}$ už jeho kořenovým nadtělesem.

(b) V 3.8 jsme zjistili, že v tělese $\mathbf{Q}(\sqrt[3]{2})$ má polynom $p = x^3-2$ kořen $\sqrt[3]{2}$, navíc je $\mathbf{Q}(\sqrt[3]{2})$ nejmenší podtěleso $\mathbf{R}$ obsahující $\sqrt[3]{2}$ a $\mathbf{Q}$, proto jde právě o kořenové nadtěleso.

Také jsme mohli sestrojit kořenové nadtěleso stejně jako ve větě, která ukazuje jeho existenci, tj. mohli jsme uvážit, že je $p = x^3-2$ ireducibilní v $\mathbf{Q}[x]$ a vzít faktorový okruh $\mathbf{Q}[x]/(x^3-2)\mathbf{Q}[x]$.

(c) Podobně jako v (a) je Protože je $1 \in \mathbf{Z}_2$ kořenem polynomu x^2+1, je $\mathbf{Z}_2$ kořenovým nadtělesem tohoto polynomu.

(d) Tentokrát stejně jako v 2.konstrukci z (b) vezmeme těleso $\mathbf{Z}_2[x]/(x^2+x+1)\mathbf{Z}_2[x]$. Označíme-li $[a] = a+(x^2+x+1)\mathbf{Z}_2[x]$, všimněme si, že má těleso $\mathbf{Z}_2[x]/(x^2+x+1)\mathbf{Z}_2[x]$ právě 4 prvky: $[0]$, $[1]$, $[x]$, $[x+1]$. □

18./20.5.

3.11. Je-li U rozkladové nadtěleso polynomu x^3-2 nad tělesem $\mathbb{Q}$. Ukažte, že

(a) $U = \mathbb{Q}[\sqrt[3]{2}, e^{\frac{2\pi i}{3}}]$,
(b) $[U:\mathbb{Q}] = 6$,
(c) $\mathbf{Gal}(U/\mathbb{Q}) \cong \mathbb{S}_3$.

(a) Vidíme, že komplexní čísla $\sqrt[3]{2}$, $\sqrt[3]{2}e^{\frac{2\pi i}{3}}$ a $\sqrt[3]{2}e^{-\frac{2\pi i}{3}}$ jsou právě kořeny polynomu $p = x^3 - 2$, proto $U = \mathbb{Q}[\sqrt[3]{2}, \sqrt[3]{2}e^{\frac{2\pi i}{3}}, \sqrt[3]{2}e^{-\frac{2\pi i}{3}}]$. Nyní si stačí všimnout, že

$$\sqrt[3]{2}e^{\frac{2\pi i}{3}}, \sqrt[3]{2}e^{-\frac{2\pi i}{3}} = \sqrt[3]{2} \cdot (e^{\frac{2\pi i}{3}})^{-1} \in \mathbb{Q}[\sqrt[3]{2}, e^{\frac{2\pi i}{3}}],$$

proto $U \subseteq \mathbb{Q}[\sqrt[3]{2}, e^{\frac{2\pi i}{3}}]$, a že

$$e^{\frac{2\pi i}{3}} = \sqrt[3]{2}e^{\frac{2\pi i}{3}} \cdot (\sqrt[3]{2})^{-1} \in U,$$

odkud dostáváme, že $U = \mathbb{Q}[\sqrt[3]{2}, e^{\frac{2\pi i}{3}}]$.

(b) Využijeme-li tvrzení z přednášky a bod (a), víme, že pro každý prvek $\alpha \in U$ platí

$$[U : \mathbb{Q}] = [U : \mathbb{Q}[\alpha]] \cdot [\mathbb{Q}[\alpha] : \mathbb{Q}].$$

Položíme-li $\alpha = \sqrt[3]{2}$, pak

$$[\mathbb{Q}[\sqrt[3]{2}] : \mathbb{Q}] = \deg m_{\sqrt[3]{2},\mathbb{Q}} = \deg x^3 - 2 = 3$$

a protože minimální polynom prvku $e^{\frac{2\pi i}{3}}$ nad tělesem $\mathbb{Q}[\sqrt[3]{2}]$ dělí polynom $x^3 - 12$ a tudíž i $x^2 + x + 1$, a o lineární polynom se kvůli imaginárním hodnotám nemůže jednat, dostáváme

$$[U : \mathbb{Q}[\sqrt[3]{2}]] = [(Q[\sqrt[3]{2}])[e^{\frac{2\pi i}{3}}] : \mathbb{Q}[\sqrt[3]{2}]] = \deg m_{e^{\frac{2\pi i}{3}},Q[\sqrt[3]{2}]} = \deg x^2 + x + 1 = 2$$

Tedy $[U : \mathbb{Q}] = [U : \mathbb{Q}[\alpha]] \cdot [\mathbb{Q}[\alpha] : \mathbb{Q}] = 6$.

(c) Protože je polynom $x^3 - 2$ nad tělesem racionálních čísel ireducibilní, víme z přednášky, že je grupa $\mathbf{Gal}(U/\mathbb{Q})$ izomorfní podgrupě grupy permutací všech kořenů polynomu $x^3 - 2$, která je izomorfní $\mathbb{S}_3$. Snadno nahlédneme, že zobrazení komplexního sdružení $\overline{\mathrm{id}}$ je prvek $\mathbf{Gal}(U/\mathbb{Q})$ řádu 2, což podle Lagrangeovy věty znamená, že $2/|\mathbf{Gal}(U/\mathbb{Q})|$. Dále nám za daných předpokladů tvrzení z přednášky zaručuje existenci prvku $\varphi \in \mathbf{Gal}(U/\mathbb{Q})$ splňujícího $\varphi(\sqrt[3]{2}) = \sqrt[3]{2}e^{\frac{2\pi i}{3}}$. Protože $\mathrm{id} \neq \varphi \neq \overline{\mathrm{id}}$, vidíme, že $|\mathbf{Gal}(U/\mathbb{Q})| = 6$. Protože je $\mathbf{Gal}(U/\mathbb{Q})$ izomorfní podgrupě $\mathbb{S}_3$, nutně už to znamená, že $\mathbf{Gal}(U/\mathbb{Q}) \cong \mathbb{S}_3$. □

3.12. Spočítejte Galoisovy grupy $\mathbf{Gal}(U/\mathbb{Q})$ je-li U rozkladové nadtěleso polynomu

(a) $x^4 + 4x^2 + 2$,

(b) $x^4 - 2$.

(a) Nejprve snadno najdeme komplexní kořeny $-2 \pm \sqrt{2}$ polynomu $y^2 + 4y + 2$, proto jsou $\pm i\sqrt{2 \pm \sqrt{2}}$ všechny kořeny polynomu $x^4 + 4x^2 + 2$. Dále si všimněme, $\sqrt{2} \in \mathbb{Q}[i\sqrt{2 + \sqrt{2}}]$, proto i

$$i\sqrt{2 - \sqrt{2}} = \frac{\sqrt{2}}{i\sqrt{2 + \sqrt{2}}} \frac{\sqrt{2 - \sqrt{2}}}{\sqrt{2 - \sqrt{2}}} \in \mathbb{Q}[i\sqrt{2 + \sqrt{2}}].$$

To znamená, že $U = \mathbb{Q}[i\sqrt{2 + \sqrt{2}}]$ každý $\mathbb{Q}$-automorfismus tělesa U je určen obrazem prvku $i\sqrt{2 + \sqrt{2}}$ na kterýkoli kořen $\pm i\sqrt{2 \pm \sqrt{2}}$. Navíc lze snadno přímočaře ukázat, že $x^4 + 4x^2 + 2$ je ireducibilní polynom nad tělesem racionálních čísel, což znamená, že $|\mathbf{Gal}(U/\mathbb{Q})| = 4$. Zbývá rozhodnout, zda $\mathbf{Gal}(U/\mathbb{Q}) \cong \mathbb{Z}_4$ nebo $\mathbf{Gal}(U/\mathbb{Q}) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$. Protože je $\overline{\mathrm{id}}$ opět prvek $\mathbf{Gal}(U/\mathbb{Q})$, stačí si všimnout, že existuje homomorfismus $\varphi \in \mathbf{Gal}(U/\mathbb{Q})$ určený podmínkou $\varphi(i\sqrt{2 + \sqrt{2}}) = i\sqrt{2 - \sqrt{2}}$ zřejmě splňuje $\varphi(-i\sqrt{2 + \sqrt{2}}) = -i\sqrt{2 - \sqrt{2}}$, proto jsou automorfismy $\overline{\mathrm{id}}$ a φ různé

prvky Galoisovy grupy řádu 2. Takovou vlastnost ovšem určitě žádná cyklická grupa nesplňuje, tudíž $\mathbf{Gal}(U/\mathbb{Q}) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.

(b) Obdobně jako v úloze 3.11 nejprve zjistíme, že $U = \mathbb{Q}[\sqrt[4]{2}, i]$. Protože $\mathbb{Q}[i]$ je rozkladové nadtěleso polynomu $x^2 + 1$ na tělesem $\mathbb{Q}$, říká nám Galoisova věta, že $\mathbf{Gal}(U/\mathbb{Q}[i])$ je normální podgrupa $\mathbf{Gal}(U/\mathbb{Q})$ a navíc platí, že

$$\mathbf{Gal}(U/\mathbb{Q})/\mathbf{Gal}(U/\mathbb{Q}[i]) \cong \mathbf{Gal}(\mathbb{Q}[i]/\mathbb{Q}).$$

Snadno spočítáme, že je polynom $x^4 - 2$ ireducibilní nad tělesem $\mathbb{Q}[i]$, proto platí, že $|\mathbf{Gal}(U/\mathbb{Q}[i])| = 4$, dokonce $\mathbf{Gal}(U/\mathbb{Q}[i]) \cong \mathbb{Z}_4$, neboť automorfismus $\varphi \in \mathbf{Gal}(U/\mathbb{Q})$ určený podmínkou $\varphi(\sqrt[4]{2}) = \sqrt[4]{2}i$ je prvek řádu 4. Protože $\mathbf{Gal}(\mathbb{Q}[i]/\mathbb{Q}) \cong \mathbb{Z}_2$, je grupa $\mathbf{Gal}(U/\mathbb{Q})$ izomorfní grupě D_8 symetrií čtverce. □

Další úlohy

(1) Popište všechny homomorfismy mezi symetrickou grupy $(S_n, \circ, ^{-1}, id)$ a obecnou konečnou komutativní grupou.

(2) Je-li $\mathbf{Q}$ osmiprvková kvaternionová grupa, ověřte, že $\{\pm 1\}$ tvoří normální podgrupu $\mathbf{N}$ a rozhodněte, zda je $\mathbf{Q}/\mathbf{N}$ izomorfní grupě $\mathbb{Z}_4$ nebo grupě $\mathbb{Z}_2 \times \mathbb{Z}_2$.

(3) Popište všechny kongruence na algebře a) $(\mathbb{Z}, +)$ b) $(\mathbb{Z}, +, \cdot)$ c) $(\mathbb{Z}, 0, 1)$ (tj. máme pouze nulární operace) d) $(\mathbb{Z}_n, +)$, e) $(\mathbb{Q}, +, \cdot)$.

(4) Najděte všechny ideály okruhu $(\mathbb{Z}_{10}, +, -, \cdot, 0, 1) \times (\mathbb{Z}_{10}, +, -, \cdot, 0, 1)$.

(5) Spočtěte prvky nejmenšího ideálu okruhu $\mathbb{Z}[x]$ obsahujícího a) x^2, x^3, b) $x^2 + 2, x$, c) $2, x^2$.

(6) Rozhodněte, zda množina $\{\sum_{i=0}^{n} a_i x^i \in \mathbb{Z}[x] : a_0 + a_1 + \ldots + a_n = 0\}$ tvoří ideál okruhu $\mathbb{Z}[x]$. Je to hlavní ideál? Pokud ano, najděte generátor.

(7) Rozhodněte, zda množina $\{x \cdot f + 3g : f, g \in \mathbb{Z}[x]\}$ tvoří ideál okruhu $\mathbb{Z}[x]$. Je to hlavní ideál? Pokud ano, najděte generátor.

(8) Popište operace a hledání inverzu a najděte primitivní prvky těles
(a) $\mathbb{F}_4 = \mathbb{Z}_2[x]/(x^2 + x + 1)$, (b) $\mathbb{F}_8 = \mathbb{Z}_2[x]/(x^3 + x + 1)$.
(c) $\mathbb{F}_9 = \mathbb{Z}_3[x]/(x^2 + 1)$.

(9) Najděte generátor hlavního ideálu v oboru $(\mathbb{Q}[x], +, -, \cdot, 0, 1)$
a) $(x^3 - 1)\mathbb{Q}[x] \cap (x^2 + 3)\mathbb{Q}[x]$,
b) $(x^3 - 1)\mathbb{Q}[x] + (x^2 + 3)\mathbb{Q}[x]$,
c) $(x^3 - 1)\mathbb{Q}[x] \cap (x^2 - 1)\mathbb{Q}[x]$,
d) $(x^3 - 1)\mathbb{Q}[x] + (x^2 - 1)\mathbb{Q}[x]$.