7 Z pralesa těles do oceánu grup

Řešení
Cvičení 3. a 4. dubna, verze ze dne 18. dubna 2024.

Cíle cvičení: Dnes si uvědomíme, že kořenová a rozkladová nadtělesa můžeme hledat nejen pomocí faktorizace, nýbrž i jako podtělesa vhodných větších (nejlépe algebraicky uzavřených) těles. Všimneme si toho, že mezi oběma konstrukcemi najdeme izomorfismus, což, jak se později ukáže, vůbec není náhoda. A poté se střemhlav vrhneme do teorie grup a na začátek se ponoříme do struktury grupy z nejspletitějších, jíž je grupa permutací.

Úlohy, které bychom určitě měli umět řešit:

Úloha 7.1. Napište všechna kořenová a rozkladová nadtělesa nad tělesem $\mathbb{Q}$ obsažená v $\mathbb{C}$ následujících polynomů z $\mathbb{Q}[x]$:

(a) $x^2 - 2$,

(b) $x^3 - 2x^2 - 2x - 3$.

Řešení. (a) Polynom $x^2 - 2$ má dva reálné kořeny $\pm\sqrt{2}$, o kvadratických rozšířeních tělesa racionálních čísel víme, že tvoří těleso, tudíž máme jediné kořenové nadtěleso $\mathbb{Q}(\sqrt{2}) = \mathbb{Q}(-\sqrt{2})$, která je zároveň i rozkladovým nadtělesem $\mathbb{Q}(\sqrt{2}, -\sqrt{2}) = \mathbb{Q}(\sqrt{2})$ polynomu $x^2 - 2$ nad tělesem $\mathbb{Q}$.

(b) Nejprve si všimneme, že má polynom $x^3 - 2x^2 - 2x - 3$ racionální kořen 3 (už umíme zjistit, že v úvahu připadají pouze hodnoty ± 1, ± 3, a ty zkusíme dosadit). To znamená, že triviální rozšíření $\mathbb{Q}(3) = \mathbb{Q}$ je kořenovým nadtělesem tohoto polynomu. Dále standardním postupem spočítáme kořeny polynomu

$$\frac{x^3 - 2x^2 - 2x - 3}{x - 3} = x^2 + x + 1 = \left(x + \frac{1}{2} - \frac{i\sqrt{3}}{2}\right)\left(x + \frac{1}{2} + \frac{i\sqrt{3}}{2}\right),$$

odkud dostáváme druhé možné kořenové nadtěleso $\mathbb{Q}(-\frac{1}{2} + \frac{i\sqrt{3}}{2}) = \mathbb{Q}(-\frac{1}{2} - \frac{i\sqrt{3}}{2}) = \mathbb{Q}(i\sqrt{3})$. Toto těleso je zřejmě i rozkladovým nadtělesem polynomu $x^3 - 2x^2 - 2x - 3$, neboť se zde rozkládá na kořenové činitele

$$x^3 - 2x^2 - 2x - 3 = (x - 3)\left(x + \frac{1}{2} - \frac{i\sqrt{3}}{2}\right)\left(x + \frac{1}{2} + \frac{i\sqrt{3}}{2}\right).$$

Úloha 7.2. Dokažte, že jsou izomorfní páry těles

(a) $\mathbb{Q}[\alpha]/(\alpha^3 - 2)$ a $\mathbb{Q}(\sqrt[3]{2})$,

(b) $\mathbb{Q}[\alpha]/(\alpha^2 - 3)$ a $\mathbb{Q}(\sqrt{3})$,

(c) $\mathbb{R}[\alpha]/(\alpha^2 + \alpha + 2)$ a $\mathbb{C}$.

Řešení. Ve všech úlohách zkonstruujeme dosvědčující izomorfismus.

(a) Nejprve poznamenejme, že kubick7 polynom $x^3 - 2$ nemá racionální kořeny, proto je ireducibilní v $\mathbb{Q}[x]$ a definujeme zobrazení $\Omega : \mathbb{Q}[\alpha]/(\alpha^3 - 2) \to \mathbb{Q}[\sqrt[3]{2}]$ předpisem

$$\Omega(a\alpha^2 + b\alpha + c) = a\sqrt[3]{4} + b\sqrt[3]{2} + c.$$

Přímo z definice vidíme, že se jedná o o dobře zavedené lineární zobrazení nad tělesem $\mathbb{Q}$ na celé $\mathbb{Q}[\sqrt[3]{2}]$. Ukážeme, že jde o prosté zobrazení. Jestliže je $r \in \mathbb{Q}[x]$ polynom stupně menšího než 3, jehož kořenem je $\sqrt[3]{2}$, pak i pro $s = \mathrm{NSD}_{\mathbb{Q}[x]}(r, x^3 - 2)$ platí, že je $\sqrt[3]{2}$ jeho kořenem. Protože je $\deg(r) < 3$ a $x^3 - 2$ je ireducibilní, musí nutně $r = 0$. Proto pokud pro $a, b, c \in \mathbb{Q}$

$$a(\sqrt[3]{2})^2 + b\sqrt[3]{2} + c = 0,$$

dostáváme, že $a = b = c = 0$. Tedy Ω má triviální jádro a jedná se o prosté zobrazení. Už jsme si všimli, že je Ω lineární, tedy slučitelné se sčítáním, a musíme ověřit pro všechna $r, s \in \mathbb{Q}[\alpha]$ stupně nejvýše 2 a takové $t(\alpha) = (r(\alpha)s(\alpha)) \pmod{\alpha^3 - 2}$, že $r(\sqrt[3]{2}) \cdot s(\sqrt[3]{2}) = t(\sqrt[3]{2})$. Protože existuje $q \in \mathbb{Q}[\alpha]$ splňující $t = rs - q(\alpha^3 - 2)$, dostáváme, že

$$t(\sqrt[3]{2}) = r(\sqrt[3]{2})s(\sqrt[3]{2}) - q(\sqrt[3]{2})((\sqrt[3]{2})^3 - 2) = r(\sqrt[3]{2}) \cdot s(\sqrt[3]{2}),$$

tedy zobrazení Ω je okruhový izomorfismus. Zbývá si všimnout, že obor $\mathbb{Q}[\sqrt[3]{2}]$ je izomorfní obraz tělesa, tedy opět těleso, což znamená, že $\mathbb{Q}[\sqrt[3]{2}] = \mathbb{Q}(\sqrt[3]{2})$ a Ω představuje dosvědčující izomorfismus těles $\mathbb{Q}[\alpha]/(\alpha^3 - 2)$ a $\mathbb{Q}(\sqrt[3]{2})$

(b) Opět díky neexistenci racionálního kořene je kvadratický polynom $x^2 - 3$ v oboru $\mathbb{Q}[x]$ ireducibilní a dále postupujeme stejně jako v (a). Definujeme lineární zobrazení $\Omega : \mathbb{Q}[\alpha]/(\alpha^2 - 3) \to \mathbb{Q}[\sqrt{3}] = \mathbb{Q}(\sqrt{3})$ předpisem

$$\Omega(a\alpha + b) = a\sqrt{2} + b,$$

o němž stejný argument jako v (a) ukáže, že se jedná o okruhový izomorfismus

(c) Vidíme, že polynom $x^2 + x + 2$ má komplexní kořeny $\frac{-1 \pm i\sqrt{7}}{2}$, tudíž je v $\mathbb{R}[x]$ nerozložitelný a opět můžeme definovat zjevně lineární zobrazení $\Omega : \mathbb{R}[\alpha]/(\alpha^2 + 2) \to \mathbb{C}$, tentokrát například podmínkou $\Omega(a\alpha + b) = a\frac{i\sqrt{7}-1}{2} + b$. Protože se zjevně jedná o prosté lineární zobrazení mezi reálnými vektorovými prostory dimenze 2, jde o bijekci, u níž stejně jako v (a) a (b) nahlédneme slučitelnost s operacemi.

Úloha 7.3. Zapište následující permutace jako součin nezávislých cyklů a pro každou permutaci σ určete σ^{-1} a σ^{2020}:

(a) $\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 5 & 1 & 2 \end{pmatrix} \in \mathbf{S}_5$,

(b) $\tau = (4\,6\,5\,1\,2) \in \mathbf{S}_6$,

(c) $\sigma = (1\,5\,6)(2\,3\,8\,4\,7) \in \mathbf{S}_8$,

(d) $\rho = (4\,3\,5) \circ (5\,1\,2) \in \mathbf{S}_5$.

Řešení. Nejprve si uvědomíme veledůležitou vlastnost, že nezávislé cykly spolu komutují, tj. $c_1c_2 = c_2c_1$ pro každé dva nezávislé cykly (což pro obecné dvojice cyklů, natož permutací, neplatí). Pak v cyklickém zápisu $c_1 \dots c_k$ každou permutaci snadno umocníme i invertujeme

$$[c_1c_2 \dots c_k]^n = c_1^n c_2^n \dots c_k^n, \quad [c_1c_2 \dots c_k]^{-1} = c_1^{-1}c_2^{-1} \dots c_k^{-1}.$$

Dále si všimneme si, že $c^n = \mathrm{id}$ pro každé n dělitelné délkou cyklu c.

(a) Nejprve tedy zapíšeme permutaci π v cyklickém zápisu, tedy ve tvaru $\dots(\dots a\pi(a)\pi^2(a)\dots)\dots$. Dostáváme $\pi = (1\,4)(2\,3\,5)$. Abychom invertovali permutaci, stačí invertovat, tedy převrátit, každý z cyklů (samozřejmě si můžeme vybrat kterýkoli z n ekvivalentních zápisu jednoho cyklu délky n)

$$\pi^{-1} = (1\,4)^{-1}(2\,3\,5)^{-1} = (4\,1)(5\,3\,2) \quad (= (1\,4)(2\,5\,3) = \dots)$$

a podobně umocníme

$$\pi^{2020} = (1\,4)^{2020}(2\,3\,5)^{2020} = ((1\,4)^2)^{1010}((2\,3\,5)^3)^{673}(2\,3\,5) = \mathrm{id}^{1010}\,\mathrm{id}^{673}(2\,3\,5) = (2\,3\,5).$$

(b) Permutaci $\tau = (4\,6\,5\,1\,2)$ tvoří jeden cyklus délky 5 a poté jeden cyklus délky 1, který nemusíme (a obvykle nebudeme) zapisovat. Nakonec si snadno rozmyslíme, že $\tau^{-1} = (2\,1\,5\,6\,4)$ a $\tau^{2020} = \mathrm{id}$, protože délka cyklu 5 dělí 2020.

(c) Obdobně jako v předchozích úlohách dostáváme

$$\sigma = (1\,5\,6)(2\,3\,8\,4\,7), \quad \text{a} \quad \sigma^{-1} = (6\,5\,1)(7\,4\,8\,3\,2), \quad \sigma^{2020} = (1\,5\,6).$$

(d) Složíme oba cykly a dostaneme $\rho = (1\,2\,4\,3\,5)$ a $\rho^{-1} = (5\,3\,4\,2\,1)$. Ze stejného důvodu jako v (b) máme $\rho^{2020} = \mathrm{id}$.

Úloha 7.4. Buďte $\pi, \tau \in \mathbf{S}_n$.

(a) Ukažte, že je-li v cyklickém zápisu permutace π prvek b hned po prvku a, pak je v cyklickém zápisu permutace $\sigma = \tau\pi\tau^{-1}$ prvek $\tau(b)$ hned po prvku $\tau(a)$,

(b) určete $\pi\tau\pi^{-1}$ a $\tau\pi\tau^{-1}$ pro permutace π a τ z příkladu 7.3.

Řešení. (a) Stačí pro $b = \pi(a)$ konjugovat $\tau\pi\tau^{-1}(\tau(a)) = \tau\pi(a) = \tau(b)$.

(b) Počítáme:

$$\pi\tau\pi^{-1} = (\pi(4)\,\pi(3)\,\pi(5)\,\pi(1)\,\pi(2)) = (1\,5\,2\,4\,3),$$
$$\tau\pi\tau^{-1} = (\tau(1)\,\tau(4))(\tau(2)\,\tau(3)\,\tau(5)) = (2\,3)(4\,5\,1).$$

Připomeňme, že operaci $\pi^\tau = \tau\pi\tau^{-1}$ se říká *konjugace prvku π prvkem τ* a prvek π^τ je pak s prvkem π *konjugovaný*.

Úloha 7.5. Ověřte, že je relace „být konjugovaný s“ ekvivalence.

Řešení. Protože $\pi^{\mathrm{id}} = \mathrm{id} \circ \pi \circ \mathrm{id}^{-1} = \pi$, jedná se o reflexivní relaci. Jestliže $\pi^\sigma = \sigma\pi\sigma^{-1} = \rho$, pak

$$\rho^{\sigma^{-1}} = \sigma^{-1}\rho(\sigma^{-1})^{-1} = \sigma^{-1}\rho\sigma = \sigma^{-1}\sigma\pi\sigma^{-1}\sigma = \pi,$$

tedy je naše relace symetrická. Konečně pokud $\pi^\sigma = \rho$ a $\rho^\tau = \theta$, pak

$$\pi^{\tau\sigma} = \tau\sigma\pi(\tau\sigma)^{-1} = \tau(\sigma\pi\sigma^{-1})\tau^{-1} = \tau\rho\tau^{-1} = \theta,$$

a proto je naše relace tranzitivní, čímž jsme dokončili důkaz.

A nakonec ještě trochu počítání pro radost a povzbuzení:

Úloha 7.6. Je-li $m \in \mathbb{Q}[x]$ ireducibilní polynom a $\beta \in \mathbb{C}$ jeho komplexní kořen, dokažte, že jsou tělesa $\mathbb{Q}[\alpha]/(m(\alpha))$ a $\mathbb{Q}(\beta)$ izomorfní.

Řešení. Obdobně jako v 7.2 sestrojíme izomorfismus $\Omega : \mathbb{Q}[\alpha]/(m(\alpha)) \to \mathbb{Q}[\beta]$ předpisem

$$\Omega(f(\alpha)) = f(\beta) \quad \forall\ f \in \mathbb{Q}[x],\ \deg(f) < \deg(m),$$

o němž se stejným postupem ukáže, že je izomorfismem. Protože je $\mathbb{Q}[\beta]$ izomorfním obrazem tělesa, jedná se rovněž o těleso, tedy máme zkonstruovaný izomorfismus $\mathbb{Q}[\alpha]/(m(\alpha)) \cong \mathbb{Q}[\beta] = \mathbb{Q}(\beta)$.

Úloha 7.7. Napište jako rozšíření $\mathbb{Q}$ v tělese $\mathbb{C}$ rozkladové nadtěleso polynomu $x^n - 1$.

Řešení. Nejprve uvážíme, že pro komplexní primitivní n-tou odmocni z jedné

$$e^{2\pi i/n} = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}$$

platí $(e^{2\pi i/n})^k = (e^{2k\pi i/n})$, což jsou pro $k = 0, 1, \ldots n-1$ jsou právě všechny kořeny polynomu $x^n - 1$. Proto existuje ireducibilní faktor $q \in \mathbb{Q}[x]$ polynomu $x^n - 1$, který má kořen $e^{2\pi i/n}$. Nyní z konstrukce tvrzení 9.4 a 9.5 z přednášky víme, že v tělese $\mathbb{Q}[x]/(m)$ máme kořen polynomu m. Vezmeme-li nyní zobrazení $\Omega : \mathbb{Q}[x]/(m) \to \mathbb{Q}[e^{2\pi i/n}]$ dané dosazením $\Omega(f) = f(e^{2\pi i/n})$, můžeme stejně jako v úlohách 7.2 a 7.6 dokázat, že se jedná o dobře definovaný izomorfismus. Tudíž je $\mathbb{Q}[e^{2\pi i/n}]$ těleso, které je právě kořenovým nadtělesem polynomu $x^n - 1$. Protože $(e^{2\pi i/n})^k = e^{2k\pi i/n} \in \mathbb{Q}[e^{2\pi i/n}]$ pro každé $k \in \mathbb{N}$, rozkládá se nám polynom

$$x^n - 1 = \prod_{k\in\mathbb{Z}_n} (x - e^{2k\pi i/n}) \in \mathbb{Q}[e^{2\pi i/n}][x]$$

na kořenové činitele, a těleso $\mathbb{Q}[e^{2\pi i/n}] = \mathbb{Q}(e^{2\pi i/n})$ je tudíž rozkladovým nadtělesem $x^n - 1$ nad $\mathbb{C}$.

Úloha 7.8. Najděte všechny permutace α na množině $\{1, 2, 3, 4\}$, pro něž platí $\alpha \circ (1\,2\,3) \circ \alpha^{-1} = (1\,2\,4)$.

Řešení. Tentokrát si pro pořádek přidáme do cyklického zápisu i cykly délky 1 a hledáme všechna α, pro něž

$$\alpha \circ (1\,2\,3) \circ \alpha^{-1} = (\alpha(1)\,\alpha(2)\,\alpha(3))(\alpha(4)) = (1\,2\,4)(3).$$

Vzhledem k tomu, že máme 3 způsoby, jak zapsat cyklus $(124) = (241) = (412)$, odečteme permutaci α v maticovém zápisu:

$$\begin{matrix}(1&2&3)&(4)\\(1&2&4)&(3)\end{matrix}\,, \qquad \begin{matrix}(1&2&3)&(4)\\(2&4&1)&(3)\end{matrix}\,, \qquad \begin{matrix}(1&2&3)&(4)\\(4&1&2)&(3)\end{matrix}$$

Z prvního zápisu vidíme, že $\alpha = \begin{pmatrix}1&2&3&4\\1&2&4&3\end{pmatrix} = (3\,4)$, z druhého $\alpha = \begin{pmatrix}1&2&3&4\\2&4&1&3\end{pmatrix} = (1\,2\,4\,3)$ a z posledního $\alpha = \begin{pmatrix}1&2&3&4\\4&1&2&3\end{pmatrix} = (1\,4\,3\,2)$. Našli jsme právě tři různé konjugující permutace $(3\,4)$, $(1\,2\,4\,3)$, $(1\,4\,3\,2)$.

Úloha 7.9. Je-li $\pi = \begin{pmatrix}1&2&3&4&5\\2&3&1&5&4\end{pmatrix}$, určete počet prvků množiny všech permutací $\alpha \in \mathbf{S}_5$,

(a) které jsou konjugované s permutací π,

(b) pro něž $\alpha\pi = \pi\alpha$.

Tvoří tyto množiny podgrupu $\mathbf{S}_5$?

Řešení. (a) Nejprve snadno spočítáme $\begin{pmatrix}1&2&3&4&5\\2&3&1&5&4\end{pmatrix} = (1\,2\,3)(4\,5)$. V předchozí úloze jsme si uvědomili, že konjugované permutace jsou právě ty se stejným cyklickým zápisem, tedy v našem případě takové, které se skládají z jednoho trojcyklu a jednoho dvojcyklu. Výběrem tří prvků z pěti zvolíme rozdělení permutace na trojcyklus a dvojcyklus, oba možné zápisy představují týž dvojcyklus, zatímco u trojcyků máme dvě možnosti, jak vytvořit různé (vzájemně inverzní) permutace. Tedy celkem dostáváme $2 \cdot \binom{5}{3}$ možností. Množina permutací se stejným cyklickým zápisem, s výjimkou té obsahující pouze identickou permutaci, netvoří podgrupu, například proto, že v ní neleží identická permutace.

(b) Všimněme si, že je podmínka $\alpha\pi = \pi\alpha$ ekvivalentní podmínce $\alpha\pi\alpha^{-1} = \pi$. Jak jsme nahlédli v minulé úloze, stačí si uvědomit kolika způsoby můžeme permutaci zapsat ve stejném cyklickém zápisu. Protože $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix} = (1\,2\,3)(4\,5)(6)$, mohu cyklus $(1\,2\,3) = (2\,3\,1) = (3\,1\,2)$ délky 3 napsat třemi způsoby a cyklus $(4\,5)$ délky 2 napsat dvěma způsoby, proto máme právě $2 \cdot 3 = 6$ permutací α splňujících podmínku.

Pokud $\alpha\pi = \pi\alpha$ a $\beta\pi = \pi\beta$, vidíme, že

$$(\alpha\beta)\pi = \alpha\beta\pi = \alpha\pi\beta = \pi\alpha\beta = \pi(\alpha\beta),$$

$$\pi\alpha^{-1} = \alpha^{-1}\alpha\pi\alpha^{-1} = \alpha^{-1}\pi, \qquad \mathrm{id}\,\pi = \pi = \pi\,\mathrm{id}$$

tedy uvažovaná množina tvoří podgrupu.

Úloha 7.10. Kolik ekvivalenčních tříd má ekvivalence „být konjugovaný“ na grupě $\mathbf{S}_6$?

Řešení. Díky úvahám předchozích dvou úloh si můžeme uvědomit, že se ptáme na to, kolik různých cyklických zápisů permutace na šesti prvcích existuje. Protože záleží jen na délkách jednotlivých cyklů, můžeme ekvivalentně spočítat počet neklesajících posloupností délek jednotlivých cyklů

$$\{(a_1, \ldots, a_2) \mid k, a_1 \ldots, a_k \in \mathbb{N},\ a_1 \leq \cdots \leq a_k,\ \sum_{i=1}^{k} a_i = 6\} =$$

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

kterých jsme hrubou silou našli právě jedenáct.

Úloha 7.11. Uvnitř tělesa $T = \mathbb{Z}_2[\alpha]/(\alpha^4 + \alpha + 1)$ nalezněte kořenové nadtěleso polynomu $x^2 + x + 1 \in \mathbb{Z}_2[x]$.

Řešení. V podstatě chceme v T najít kořen onoho polynomu. Jelikož T má charakteristiku 2, můžeme ekvivalentně hledat řešení β rovnice $x^2 = x + 1$; kromě toho mocnění mnohočlenu na druhou probíhá „člen po členu“ (smíšené členy jsou díky výskytu 2 rovny nule).

Předně si všimněme, že z Viètových vztahů bude součet řešení rovnice roven 1, tím pádem můžeme BÚNO hledat řešení β, jehož abs. člen je nulový (a druhé řešení bude se bude lišit jen v onom abs. členu).

Pokud si dále spočteme $(\alpha^3)^2 = \alpha^3 + \alpha^2$, vidíme, že β musí nutně obsahovat α^2, aby mělo β^2 nenulový abs. člen (stejně jako má $\beta + 1$). Jelikož ovšem $(\alpha^2)^2 = \alpha + 1$, je v β^2 nutně přítomen lineární člen α, tím pádem musí být i v β. Ze zbývajících dvou možností $\alpha^2 + \alpha$ a $\alpha^3 + \alpha^2 + \alpha$ snadno potvrdíme první a vyloučíme druhou.

Máme tedy $\beta = \alpha^2 + \alpha$, druhé řešení rovnice je tedy $\alpha^2 + \alpha + 1$. Hledané kořenové nadtěleso je $\mathbb{Z}_2(\alpha^2 + \alpha) \leq T$, které je zřejmě stejné jako $\mathbb{Z}_2(\alpha^2 + \alpha + 1)$. Toto těleso je i rozkladové a zadaný polynom se v něm rozkládá jako

$$x^2 + x + 1 = (x + \alpha^2 + \alpha)(x + \alpha^2 + \alpha + 1).$$