Cvičení 3, 2.11.2020

Příklady označené (!) jsou zásadní a nutně musíte pochopit řešení. Příklady označené (*) jsou těžší.

Kořenová a rozkladová nadtělesa

1. (!) Určete kořenové a rozkladové nadtěleso polynomu x^2+3 nad tělesem $\mathbb{R}$.
   Návod: Je to $\mathbb{C}$. Ale nemohlo by to být nějaké menší těleso $\mathbb{R} < T < \mathbb{C}$?
2. (!) Určete všechna možná kořenová nadtělesa pro f nad $\mathbb{Q}$ obsažená v $\mathbb{C}$ (existují i jiná než obsažená v $\mathbb{C}$?), nějaké rozkladové nadtěleso pro f nad $\mathbb{Q}$, stupně rozšíření všech těchto těles a popište jejich Galoisovy grupy nad $\mathbb{Q}$ (vypište její prvky a určete, které známé grupě je izomorfní).
   a) $f(x) = x^2 - 1$
   Řešení: $\mathbb{Q}$ stupně 1, $\mathbb{Q}$ stupně 1, Gal triviální
   b) $f(x) = x^3 - 1$
   Řešení: koř. $\mathbb{Q}$ stupně 1, koř. i rozkl. $\mathbb{Q}(e^{2\pi i/3})$ stupně 2, $Gal = \{id, x \mapsto \bar{x}\}$.
   c) $f(x) = x^2 + 3$
   Řešení: koř. i rozkl. $\mathbb{Q}(\sqrt{3}i)$ stupně 2, $Gal = \{id, x \mapsto \bar{x}\}$.
   d) $f(x) = x^4 - 1$
   Řešení: koř. $\mathbb{Q}$, koř. i rozkl. $\mathbb{Q}(i)$ stupně 2, $Gal = \{id, x \mapsto \bar{x}\}$.
   e) $f(x) = x^4 + 1$
   Návod: Je to ireducibilní polynom a dokažte, že čtyři různé kořeny generují to samé těleso tvaru $\mathbb{Q}(a)$. Gal má nejvýše čtyři prvky, protože $a \mapsto$ jeden ze čtyř kořenů, Gal má aspoň čtyři prvky, protože je tranzitivní na kořenech. Přitom všechny netriviální automorfismy mají řád 2, protože $a \mapsto$něco$\mapsto a$ (pokud nechápete, co z toho plyne, napište si obraz obecného prvku $r + sa + ta^2 + ua^3$ v daném automorfismu).
   Řešení: koř. i rozkl. $\mathbb{Q}(e^{2\pi i/8})$ stupně 4, $Gal \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$.
   f) $f(x) = x^3 - 2$
   Řešení: Koř. $\mathbb{Q}(\sqrt[3]{2})$, $\mathbb{Q}(\sqrt[3]{2}e^{2\pi i/3})$ stupně 3, Gal je cyklická tříprvková. Rozkl. $\mathbb{Q}(\sqrt[3]{2}, e^{2\pi i/3})$, Gal se vnořuje do S_3, obsahuje prvek $x \mapsto \bar{x}$ řádu 2, obsahuje aspoň tři prvky díky tranzitivitě, takže musí být izomorfní S_3. Z toho je vidět, že všech 6 permutací kořenů musí dát automorfismus, vzorce si snadno explicitně napíšete.
3. Popište Galoisovu grupu rozšíření $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ nad $\mathbb{Q}$.
   Řešení: Aplikací Tvrzení 2.11 na polynomy x^2-2 a x^2-3 vidíme, že každý $\varphi \in$ Gal splňuje $\varphi(\sqrt{2}) = u\sqrt{2}$ a $\varphi(\sqrt{3}) = v\sqrt{3}$ pro nějaká $u, v \in \{\pm 1\}$, čili $\mathbb{Q}$-automorfismy jsou nejvýše čtyři a lze je zapsat vzorcem
   $$\varphi(a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}) = a + ub\sqrt{2} + vc\sqrt{3} + uvd\sqrt{6}.$$
   Z vzorce také vidíme, že $\varphi^2 = id$ pro všechny volby u, v. Pokud dokážeme, že existují pouze čtyři automorfismy, Gal musí být izomorfní $\mathbb{Z}_2 \times \mathbb{Z}_2$.
   Jsou to skutečně $\mathbb{Q}$-automorfismy? Je možné, ale velmi pracné, to ověřit přímo z definice. Jednodušší je využít tranzitivity: není těžké nahlédnout, že $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$ a aplikací tranzitivity na minimální polynom $m_{\sqrt{2}+\sqrt{3},\mathbb{Q}}$ vidíme, že $|Gal| \geq 4$.

4. * V závislosti na n popište Galoisovu grupu rozkladového nadtělesa polynomu x^n-1. Na základě pár příkladů si tipněte, kolik bude stupeň rozšíření, ale bez další teorie se vám váš odhad nejspíš nepovede dokázat.

   Návod: Označme $\zeta = e^{2\pi i/n}$. Rozkladové nadtěleso je $\mathbb{Q}(\zeta)$, to má $\varphi(n)$ generátorů ζ^k, k nesoudělné s n. Galoisova grupa je izomorfní $\mathbb{Z}_n^*$, prvku k odpovídá automorfismu danému předpisem $\zeta \mapsto \zeta^k$. Stupeň je $\varphi(n)$, časem budeme mít větu, že za jistých předpokladů je stupeň roven $|Gal|$.
5. Buď $0 \neq a \in \mathbb{Q}$. Dokažte, že rozkladovým nadtělesem polynomu $f = x^n - a$ nad tělesem $\mathbb{Q}$ je těleso $Q(e^{2\pi i/n}, b)$, kde b je libovolný komplexní kořen polynomu f.
6. Spočtěte prvky Galoisovy grupy $Gal(\mathbb{R}/\mathbb{Q})$.

   Návod: Dokažte nejprve, že každý prvek $Gal(\mathbb{R}/\mathbb{Q})$ je rostoucí funkce (to je specifická vlastnost rozšíření $\mathbb{Q} \leq \mathbb{R}$, pro jiná tělesa to typicky pravda nebude). Zbytek je úloha z elementární analýzy na úrovni prváku: najděte všechny rostoucí reálné funkce, které fixují racionální čísla.

T-homomorfismy

1. (!) Buďte T, U tělesa charakteristiky 0. Pak $\mathbb{Q} \subset T, U$ (co to přesně znamená?) a každý nenulový okruhový homomorfismus $\varphi : T \to U$ je prostým $\mathbb{Q}$-homomorfismem. (Nulovým homomorfismem rozumíme zobrazení $x \mapsto 0$.)

   Návod: Přesně to znamená, že racionální číslo $\frac{a}{b}$ ztotožníme s prvkem $(a\times 1)(b\times 1)^{-1}$, kde $u \times 1 = 1 + ... + 1$ u-krát pro $u > 0$, resp. 0 pro $u = 0$, resp. $-(1 + ... + 1)$ pro $u < 0$. Zbytek pak je jasný z toho, že $\varphi(1) = 1$ a $\varphi(a^{-1}) = \varphi(a)^{-1}$, ovšem tyto dvě vlastnosti musíte dokázat z definice okruhového homomorismu. Prostost: $\mathrm{Ker}(\varphi)$ je ideál, tedy 0 nebo T.
2. (!) Buď S_1, S_2 rozkladová nadtělesa pro polynom f nad tělesem T a buď ψ T-izomorfismus těchto těles. Dokažte, že $Gal(S_1/T) \to Gal(S_2/T)$, $\varphi \mapsto \psi\varphi\psi^{-1}$ je izomorfismus příslušných Galoisových grup.
3. Buď $T \subset U$ algebraické rozšíření těles a $U \subset K$ (ne nutně algebraické). Pak K je algebraický uzávěr U, právě když K je algebraický uzávěr T.
4. Pro která $m, n \in \mathbb{Z}$ jsou tělesa $\mathbb{Q}(\sqrt{m})$, $\mathbb{Q}(\sqrt{n})$ $\mathbb{Q}$-izomorfní?

   Návod: Aplikujte tvrzení o tom, že kořen polynomu f se zobrazí na kořen polynomu f.

Algebraický uzávěr

1. Žádné konečné těleso není algebraicky uzavřené.

   Návod: Euklides si všimnul: "Kdyby bylo jen konečně mnoho prvočísel, vemte jejich součin plus 1, ten není dělitelný žádným prvočíslem, spor."Stejnou myšlenku proveďte pro polynomy $x - a$.
2. * Algebraický uzávěr nekonečného tělesa T má stejnou mohutnost jako T.

   Návod: Pokud jste neměli teorii množin, na úlohu zapomeňte. Jinak si rozeberte konstrukci uzávěru a aplikujte poznatky o tom, kolik je polynomů a jaká je mohutnost sjednocení řetězce množin.