GALOISOVA TEORIE

DAVID STANOVSKÝ

Řešitelné grupy

Definice. Grupa $\mathbf{G}$ se nazývá *řešitelná*, pokud existuje číslo k a normální podgrupy $\mathbf{N}_0, \dots, \mathbf{N}_k \trianglelefteq \mathbf{G}$ takové, že $\{1\} = \mathbf{N}_0 \leq \mathbf{N}_1 \leq \dots \leq \mathbf{N}_k = \mathbf{G}$ a každá faktorgrupa $\mathbf{N}_i/\mathbf{N}_{i-1}$, $i = 1, \dots, k$, je abelovská. Nejmenšímu k, pro které taková řada podgrup existuje, se říká *stupeň řešitelnosti* grupy $\mathbf{G}$.

Vidíme, že grupa je řešitelná stupně 1 právě tehdy, když je abelovská. Řešitelné grupy stupně ≤ 2 se nazývají *metabelovské*.

Tvrzení 0.1. *Buď $\mathbf{G}$ grupa.*

(1) *Je-li $\mathbf{G}$ řešitelná a $\mathbf{H}$ její pogrupa, pak je $\mathbf{H}$ řešitelná.*
(2) *Je-li $\mathbf{G}$ řešitelná a $\mathbf{K}$ její normální podgrupa, pak je $\mathbf{G}/\mathbf{K}$ řešitelná.*
(3) *Pokud $\mathbf{G}$ obsahuje normální podgrupu $\mathbf{N}$ takovou, že jsou obě grupy $\mathbf{N}$ i $\mathbf{G}/\mathbf{N}$ řešitelné, pak je $\mathbf{G}$ řešitelná.*

Důsledek 0.2. *Buď $\mathbf{G}$ grupa a $\mathbf{N}_0, \dots, \mathbf{N}_k \trianglelefteq \mathbf{G}$ takové, že $\{1\} = \mathbf{N}_0 \leq \mathbf{N}_1 \leq \dots \leq \mathbf{N}_k = \mathbf{G}$ a každá faktorgrupa $\mathbf{N}_i/\mathbf{N}_{i-1}$, $i = 1, \dots, k$, je řešitelná. Pak je $\mathbf{G}$ řešitelná.*

1. Izomorfismy tělesových rozšíření

1.1. Galoisova grupa rozšíření.

Galoisova teorie studuje grupy symetrií tělesových rozšíření. Konkrétně, půjde o automorfismy většího tělesa, které zachovávají menší těleso.

Definice. Buď $\mathbf{T}, \mathbf{S}, \mathbf{U}$ tělesa taková, že $\mathbf{T} \leq \mathbf{S}$ a $\mathbf{T} \leq \mathbf{U}$. Okruhový izomorfismus $\varphi : \mathbf{S} \to \mathbf{U}$ se nazývá $\mathbf{T}$-*izomorfismus*, pokud $\varphi(t) = t$ pro každé $t \in T$.

Všimněte si, že $\mathbf{T}$-izomorfismus je lineárním zobrazením vektorových prostorů $\mathbf{S_T} \to \mathbf{U_T}$: obě definice vyžadují $\varphi(a + b) = \varphi(a) + \varphi(b)$ pro všechna $a, b \in S$ a pro skalární násobení platí $\varphi(t \cdot a) = \varphi(t) \cdot \varphi(a) = t \cdot \varphi(a)$ pro všechna $t \in T$, $a \in S$. Opačná implikace samozřejmě neplatí: je řada lineárních zobrazení, které nezachovávají násobení.

Definice. Buď $\mathbf{T} \leq \mathbf{S}$ rozšíření těles. $\mathbf{T}$-izomorfismy $\mathbf{S} \to \mathbf{S}$ se nazývají $\mathbf{T}$-*automorfismy*. Je snadné nahlédnout, že jsou uzavřeny na skládání a invertování, a tedy tvoří podgrupu symetrické grupy na množině S. Tato grupa se nazývá *Galoisova grupa rozšíření* $\mathbf{T} \leq \mathbf{S}$ a značí se $\mathbf{Gal}(\mathbf{S}/\mathbf{T})$.

---

22. května 2019.

Příklad. Spočteme grupu $\mathbf{Gal}(\mathbb{C}/\mathbb{R})$. Báze vektorového prostoru $\mathbb{C}_\mathbb{R}$ je $1, i$. Uvažujme $\mathbb{R}$-automorfismus φ. Nutně $\varphi(1) = 1$, neboť $1 \in \mathbb{R}$. Dále $\varphi(i)^2 = \varphi(i^2) = \varphi(-1) = -1$, a tedy $\varphi(i) \in \{i, -i\}$. Protože $\varphi(a+bi) = a+b\varphi(i)$, dostáváme přesně dvě možnosti: $\varphi = id$ a $\varphi = {}^-$, komplexní sdružení. Obě zobrazení jsou okruhovými homomorfismy, a tedy

$$\mathrm{Gal}(\mathbb{C}/\mathbb{R}) = \{id, {}^-\}, \qquad \mathbf{Gal}(\mathbb{C}/\mathbb{R}) \simeq \mathbb{Z}_2.$$

Příklad. Obecně je výpočet Galoisových grup obtížný a výsledek předem nejasný. Například, platí, ale není snadné dokázat, že $\mathbf{Gal}(\mathbb{R}/\mathbb{Q})$ je jednoprvková, zatímco $\mathbf{Gal}(\mathbb{C}/\mathbb{Q})$ je nekonečná.

V dalším textu se soustředíme na případ $\mathbf{S} = \mathbf{T}(a_1, \ldots, a_n)$, kde $a_1, \ldots, a_n$ jsou algebraické prvky nad $\mathbf{T}$. Základním pozorováním je, že $\mathbf{T}$-automorfismy jsou určeny hodnotami na prvcích $a_1, \ldots, a_n$. Buď φ nějaký $\mathbf{T}$-automorfismus a označme $\varphi(a_i) = u_i$. Obecný prvek $s \in S$ můžeme vyjádřit jako součet

$$s = \sum c_{i_1,\ldots,i_n} a_1^{i_1} \cdots a_n^{i_n}$$

pro nějaká $c_{i_1,\ldots,i_n} \in T$ a jeho obraz pak bude

$$\varphi(s) = \sum \varphi(c_{i_1,\ldots,i_n})\varphi(a_1)^{i_1} \cdots \varphi(a_n)^{i_n} = \sum c_{i_1,\ldots,i_n} u_1^{i_1} \cdots u_n^{i_n}.$$

Ovšem pozor, ne každá volba hodnot u_i dává $\mathbf{T}$-automorfismus. Jak jsme viděli na příkladě výše, pro $\mathbf{S} = \mathbb{Q}(i)$ jsou jediné možnosti $\varphi(i) \in \{\pm i\}$. Obecný princip formuluje následující tvrzení.

Tvrzení 1.1. *Buď $\mathbf{T} \leq \mathbf{S}$ rozšíření těles, $f \in T[x]$ a $A \subseteq S$ množina všech kořenů polynomu f v $S \setminus T$. Pro každé $\varphi \in \mathrm{Gal}(\mathbf{S}/\mathbf{T})$ je $\varphi|_A$ permutací množiny A.*

Důkaz. Označme $f = \sum c_i x^i$ a uvažujme jeho kořen $a \in S$. Pak $\varphi(a)$ je také kořenem f, protože

$$f(\varphi(a)) = \sum c_i \varphi(a)^i = \sum \varphi(c_i)\varphi(a)^i = \varphi\left(\sum c_i a^i\right) = \varphi(f(a)) = \varphi(0) = 0,$$

kde druhá rovnost využívá faktu, že $\varphi|_T$ je identita. Přitom kořeny, které leží v T, se musí zobrazit na sebe, a z prostosti φ plyne, že se na ně nezobrazí žádný kořen z $S \setminus T$. Čili $\varphi|_A$ zobrazuje A do A, je prosté, množina A je konečná, takže musí být permutací. □

Příklad. Spočteme grupu $\mathbf{Gal}(\mathbb{Q}(\sqrt{s})/\mathbb{Q})$, kde s není čtvercem. Buď φ nějaký $\mathbb{Q}$-automorfismus. Prvek $\sqrt{s}$ je kořenem polynomu $f = x^2 - s$ a podle Tvrzení 1.1 se musí zobrazit na některý z kořenů f v $\mathbb{Q}(\sqrt{s})$. Ty jsou pouze dva, čili $\varphi(\sqrt{s}) \in \{\pm\sqrt{s}\}$ a dostáváme zobrazení $\varphi(a + b\sqrt{s}) = a \pm b\sqrt{s}$. Snadno ověříme, že jde o $\mathbb{Q}$-automorfismy, a tedy

$$\mathbf{Gal}(\mathbb{Q}(\sqrt{s})/\mathbb{Q}) \simeq \mathbb{Z}_2.$$

Příklad. Spočteme grupu $\mathbf{Gal}(\mathbb{Q}(\sqrt[3]{s})/\mathbb{Q})$, kde $\sqrt[3]{s} \notin \mathbb{Q}$. Buď φ nějaký $\mathbb{Q}$-automorfismus. Prvek $\sqrt[3]{s}$ je kořenem polynomu $f = x^3 - s$ a podle Tvrzení 1.1 se musí zobrazit na některý z kořenů f v $\mathbb{Q}(\sqrt[3]{s})$. Ale v tomto tělese f žádný jiný kořen nemá (oba zbylé kořeny v $\mathbb{C}$ jsou imaginární), čili máme pouze jeden $\mathbf{T}$-automorfismus, identitu. Galoisova grupa je jednoprvková.

1.2. **Izomorfismy kořenových a rozkladových nadtěles.**

Pro Galoisovu teorii jsou stěžejní Galoisovy grupy rozkladových nadtěles. V této podsekci doplníme teorii rozkladových nadtěles, která je nutná k jejich výpočtu.

Buď $\mathbf{T}$ těleso a f polynom z $\mathbf{T}[x]$ stupně ≥ 1. Připomeňme, že

- *kořenovým nadtělesem* pro f nad $\mathbf{T}$ rozumíme minimální rozšíření, ve kterém má polynom f kořen (tj. rozšíření $\mathbf{S}$, kde existuje $a \in S$ takové, že $\mathbf{S} = \mathbf{T}(a)$ a $f(a) = 0$);
- *rozkladovým nadtělesem* rozumíme minimální rozšíření, kde se rozkládá na lineární činitele (tj. rozšíření $\mathbf{S}$, kde existují $a_1, \ldots, a_n \in S$ taková, že $\mathbf{S} = \mathbf{T}(a_1, \ldots, a_n)$ a $f \parallel (x - a_1) \cdot \ldots \cdot (x - a_n)$).

Věta ze zimního semestru prokazuje existenci těchto rozšíření.

Příklad. Díky základní větě algebry víme, že kořenové i rozkladové nadtěleso polynomu f nad tělesem $\mathbb{Q}$ lze nalézt uvnitř tělesa $\mathbb{C}$: kořenovým bude libovolné $\mathbb{Q}(a)$, kde a je nějaký komplexní kořen f, a rozkladovým bude $\mathbb{Q}(a_1, \ldots, a_m)$, kde $a_1, \ldots, a_m$ jsou všechny komplexní kořeny f.

- Uvažujme polynom $x^2 + 1$. Jediným kořenovým nadtělesem obsaženým v $\mathbb{C}$ je těleso $\mathbb{Q}(i) = \mathbb{Q}(-i)$, které obsahuje oba kořeny $\pm i$, a tedy je i nadtělesem rozkladovým.
- Uvažujme polynom $x^3 - 1$. Tento polynom má dvě různá kořenová nadtělesa v $\mathbb{C}$, a to $\mathbb{Q} = \mathbb{Q}(1)$ a $\mathbb{Q}(e^{2\pi i/3}) = \mathbb{Q}(e^{4\pi i/3})$. Tato tělesa jistě nejsou $\mathbb{Q}$-izomorfní. To větší je rozkladové, neboť obsahuje všechny tři kořeny.
- Uvažujme polynom $x^3 - 2$. Tento polynom má dvě různá kořenová nadtělesa, $\mathbb{Q}(\sqrt[3]{2})$ a $\mathbb{Q}(\sqrt[3]{2} \cdot e^{2\pi i/3})$ (to druhé obsahuje oba imaginární kořeny). Ač to není vidět na první pohled, tato tělesa jsou $\mathbb{Q}$-izomorfní. Rozkladovým nadtělesem pak bude těleso $\mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{2} \cdot e^{2\pi i/3}) = \mathbb{Q}(\sqrt[3]{2}, e^{2\pi i/3})$.

Rozložitelné polynomy typicky nemají izomorfní kořenová nadtělesa: mimo jiné proto, že ireducibilní dělitelé různých stupňů vynucují různý stupeň příslušných kořenových nadtěles. Na druhou stranu, možná trochu překvapivě, pro ireducibilní polynomy jsou všechna kořenová nadtělesa izomorfní. Pro rozkladová nadtělesa máme izomorfismus také, tentokrát již bez předpokladu ireducibility.

Věta 1.2. *Buď $\mathbf{T}$ těleso a $f \in T[x]$ stupně ≥ 1.*

(1) *Je-li f ireducibilní, pak každá dvě kořenová nadtělesa pro f nad $\mathbf{T}$ jsou $\mathbf{T}$-izomorfní.*
(2) *Každá dvě rozkladová nadtělesa pro f nad $\mathbf{T}$ jsou $\mathbf{T}$-izomorfní.*

V dalším výkladu (konkrétně k výpočtu Galoisových grup a jednoznačnosti algebraického uzávěru) budeme potřebovat silnější tvrzení o rozšiřování částečných izomorfismů mezi kořenovými a rozkladovými nadtělesy. Věta 1.2 tak bude speciálním případem Lemmat 1.3 a 1.4. K jejich formulaci je potřeba následující značení a pozorování.

Buď $\mathbf{T} \leq \mathbf{T}_1$, $\mathbf{T} \leq \mathbf{T}_2$ rozšíření těles a $\varphi : \mathbf{T}_1 \to \mathbf{T}_2$ $\mathbf{T}$-izomorfismus. Zobrazení φ lze rozšířit na $\mathbf{T}$-izomorfismus oborů polynomů nad těmito tělesy (budeme jej opět značit φ):

$$\varphi : \mathbf{T}_1[x] \to \mathbf{T}_2[x], \qquad \sum a_i x^i \mapsto \sum \varphi(a_i) x^i.$$

Označme $f = \sum a_i x^i$, $g = \sum b_i x^i$. Koeficienty součtu $f + g$ jsou $a_i + b_i$, koeficienty součtu $\varphi(f) + \varphi(g)$ jsou $\varphi(a_i) + \varphi(b_i) = \varphi(a_i + b_i)$ a vidíme, že $\varphi(f + g) = \varphi(f) +$

$\varphi(g)$. Koeficienty součinu fg jsou $\sum_{i+j=k} a_i b_j$, koeficienty součinu $\varphi(f)\varphi(g)$ jsou $\sum_{i+j=k} \varphi(a_i)\varphi(b_j) = \varphi(\sum_{i+j=k} a_i b_j)$ a vidíme, že $\varphi(fg) = \varphi(f)\varphi(g)$. Bijektivita zobrazení je zřejmá. Okamžitým důsledkem součinové vlastnosti je, že

- $f \mid g$ v $\mathbf{T}_1[x]$ právě tehdy, když $\varphi(f) \mid \varphi(g)$ v $\mathbf{T}_2[x]$;
- polynom f je ireducibilní v $\mathbf{T}_1[x]$ právě tehdy, když $\varphi(f)$ je ireducibilní v $\mathbf{T}_2[x]$.

Lemma 1.3. *Buď $\mathbf{T} \leq \mathbf{T}_1$, $\mathbf{T} \leq \mathbf{T}_2$ rozšíření těles a $\varphi : \mathbf{T}_1 \to \mathbf{T}_2$ $\mathbf{T}$-izomorfismus. Buď $f \in T_1[x]$ ireducibilní polynom, $\mathbf{T}_1(a)$ kořenové nadtěleso pro f nad $\mathbf{T}_1$ a $\mathbf{T}_2(b)$ kořenové nadtěleso pro $\varphi(f)$ nad $\mathbf{T}_2$. Pak existuje $\mathbf{T}$-izomorfismus $\psi : \mathbf{T}_1(a) \to \mathbf{T}_2(b)$ takový, že $\psi(a) = b$ a $\psi|_{T_1} = \varphi$.*

Důkaz. Podle Tvrzení **??** je $T_1(a) = T_1[a] = \{g(a) : \ g \in T_1[x]\}$ a $T_2(b) = T_2[b] = \{g(b) : \ g \in T_2[x]\}$. Uvažujme tedy zobrazení

$$\psi : T_1(a) \to T_2(b), \qquad g(a) \mapsto g(b).$$

Předně je třeba dokázat, že to je dobře definované zobrazení. Označme $\tilde{a} = \varphi(a)$. Uvědomte si, že $f = m_{a,\mathbf{T}_1}$, protože f je ireducibilní polynom a a je jeho kořen, a zrovna tak $\varphi(f) = m_{\tilde{a},\mathbf{T}_2}$, protože $\varphi(f)$ je ireducibilní polynom a $\tilde{a}$ je jeho kořen. Čili

$$g(a) = h(a) \ \Leftrightarrow \ (g-h)(a) = 0 \ \Leftrightarrow \ f \mid g - h$$

a analogicky

$$\varphi(g)(\tilde{a}) = \varphi(h)(\tilde{a}) \ \Leftrightarrow \ \varphi(g-h)(\tilde{a}) = 0 \ \Leftrightarrow \ \varphi(f) \mid \varphi(g-h).$$

Ekvivalence obou tvrzení na pravé straně plyne z pozorování výše. Dokázali jsme, že φ je dobře definované zobrazení a navíc prosté. Očividně jde o bijekci a je snadné ověřit, že jde o okruhový homomorfismus: pro každé $g, h \in T_1[x]$ platí $\psi(g(a) + h(a)) = \psi((g+h)(a)) = \varphi(g+h)(b) = \varphi(g)(b) + \varphi(h)(b) = \psi(g(a)) + \psi(h(a))$ a analogicky pro násobení. Prvky tělesa $\mathbf{T}_1$ odpovídají volbě konstantního polynomu c, pro takový polynom platí $\psi(c) = \psi(c(a)) = \varphi(c)(b) = \varphi(c)$, čili $\psi|_{\mathbf{T}_1} = \varphi$. Volbou $g = x$ ověříme, že $\varphi(a) = b$. □

Lemma 1.4. *Buď $\mathbf{T} \leq \mathbf{T}_1$, $\mathbf{T} \leq \mathbf{T}_2$ rozšíření těles a $\varphi : \mathbf{T}_1 \to \mathbf{T}_2$ $\mathbf{T}$-izomorfismus. Buď $f \in T_1[x]$ polynom stupně ≥ 1 a označme $\mathbf{S}_1$ rozkladové nadtěleso polynomu f nad $\mathbf{T}_1$ a $\mathbf{S}_2$ rozkladové nadtěleso polynomu $\varphi(f)$ nad $\mathbf{T}_2$. Pak existuje $\mathbf{T}$-izomorfismus $\psi : \mathbf{S}_1 \to \mathbf{S}_2$ takový, že $\psi|_{T_1} = \varphi$.*

Důkaz. Budeme postupovat indukcí podle stupně polynomu f. Je-li $\deg f = 1$, pak $\mathbf{S}_1 = \mathbf{T}_1$, $\mathbf{S}_2 = \mathbf{T}_2$ a $\psi = \varphi$. V indukčním kroku uvažujme ireducibilní dělitel g polynomu f a jeho kořen a v $\mathbf{S}_1$. Pak $\varphi(g)$ je ireducibilní dělitel polynomu $\varphi(f)$ a uvažujme jeho kořen b v $\mathbf{S}_2$. Podle Lemmatu 1.3 existuje zobrazení $\psi : \mathbf{T}_1(a) \to \mathbf{T}_2(b)$ takové, že $\psi(a) = b$ a $\psi|_{T_1} = \varphi$. Napišme $f = (x-a)\cdot h$ pro nějaký $h \in T_1[x]$, čili také $\psi(f) = (x-b)\cdot\psi(h)$. Pak $\mathbf{S}_1$ je rozkladové nadtěleso polynomu h nad $\mathbf{T}_1(a)$ a $\mathbf{S}_2$ je rozkladové nadtěleso polynomu $\psi(h)$ nad $\mathbf{T}_2(b)$. Protože $\deg h < \deg f$, podle indukčního předpokladu existuje $\mathbf{T}$-izomorfismus $\rho : \mathbf{S}_1 \to \mathbf{S}_2$ takový, že $\rho|_{T_1(a)} = \psi$, čili také $\rho|_{T_1} = \varphi$. □

Volbou $\mathbf{T}_1 = \mathbf{T}_2 = \mathbf{T}$ a $\varphi = id$ v obou lemmatech dostaneme důkaz Věty 1.2.

1.3. **Galoisova grupa polynomu.**

Definice. Buď f polynom z $\mathbf{T}[x]$ stupně ≥ 1. *Galoisovou grupou polynomu* f nad tělesem $\mathbf{T}$, značíme $\mathbf{Gal}(f/\mathbf{T})$, rozumíme jakoukoliv grupu $\mathbf{Gal}(\mathbf{S}/\mathbf{T})$, kde $\mathbf{S}$ je rozkladové nadtěleso polynomu f nad $\mathbf{T}$.

Dává tento pojem smysl, když je rozkladové nadtěleso určeno jednoznačně pouze *až na izomorfismus*? Uvažujme $\mathbf{T}$-izomorfismus $\psi : \mathbf{S}_1 \to \mathbf{S}_2$ dvou rozkladových nadtěles pro f. Je snadné ověřit (proveďte jako cvičení!), že

$$\mathbf{Gal}(\mathbf{S}_1/\mathbf{T}) \to \mathbf{Gal}(\mathbf{S}_2/\mathbf{T}), \qquad \varphi \mapsto \psi \circ \varphi \circ \psi^{-1}$$

je izomorfismem příslušných Galoisových grup. Čili Galoisova grupa polynomu jsou určena *až na izomorfismus*.

Příklad. V příkladech v sekci 1.1 jsme ukázali, že $\mathbf{Gal}(x^2 - s/\mathbb{Q}) \simeq \mathbb{Z}_2$. Ale pozor, $\mathbf{Gal}(x^3 - 2/\mathbb{Q})$ není jednoprvková grupa, neboť $\mathbb{Q}(\sqrt[3]{2})$ není rozkladové nadtěleso polynomu $x^3 - 2$.

Následující tvrzení umožňují určit Galoisovy grupy některých jednodušších polynomů.

Tvrzení 1.5. *Buď* $\mathbf{T}$ *těleso,* f *polynom z* $\mathbf{T}[x]$ *stupně* ≥ 1 *a* $\mathbf{S}$ *jeho rozkladové nadtěleso. Pak*

(1) $\mathbf{Gal}(\mathbf{S}/\mathbf{T})$ *se vnořuje do symetrické grupy* $\mathbf{S}_m$*, kde* m *je počet různých kořenů polynomu* f *v* $S \setminus T$*;*
(2) *je-li* f *ireducibilní, pak pro každé dva kořeny* $a, b \in S$ *existuje* $\varphi \in \mathrm{Gal}(\mathbf{S}/\mathbf{T})$ *takový, že* $\varphi(a) = b$*;*
(3) *pro každé rozšíření* $\mathbf{T} \leq \mathbf{S} \leq \mathbf{U}$ *takové, že* $\mathbf{U}$ *je také rozkladovým nadtělesem nějakého polynomu nad* $\mathbf{T}$*, platí* $\mathbf{Gal}(\mathbf{U}/\mathbf{S}) \trianglelefteq \mathbf{Gal}(\mathbf{U}/\mathbf{T})$ *a*

$$\mathbf{Gal}(\mathbf{U}/\mathbf{T}) \,/\, \mathbf{Gal}(\mathbf{U}/\mathbf{S}) \simeq \mathbf{Gal}(\mathbf{S}/\mathbf{T}).$$

Důkaz. (1) Označme $A = \{a_1, \ldots, a_m\}$ množinu kořenů polynomu f v $S \setminus T$. Tvrzení 1.1 říká, že pro každé $\varphi \in \mathrm{Gal}(\mathbf{S}/\mathbf{T})$ je $\varphi|_A$ permutace na A, čili zobrazení

$$\mathbf{Gal}(\mathbf{S}/\mathbf{T}) \to \mathbf{S}_A, \qquad \varphi \mapsto \varphi|_A$$

je dobře definovaný homomorfismus. Dokážeme, že je prostý. Protože je $\mathbf{S}$ rozkladové pro f, platí $\mathbf{S} = \mathbf{T}(a_1, \ldots, a_m)$. Čili každé $\varphi \in \mathrm{Gal}(\mathbf{S}/\mathbf{T})$ je jednoznačně určené svými hodnotami na prvcích $a_1, \ldots, a_m$, a tedy také svojí restrikcí $\varphi|_A$.

(2) Podle Lemmatu 1.3 existuje $\mathbf{T}$-izomorfismus kořenových nadtěles $\psi : \mathbf{T}(a) \to \mathbf{T}(b)$ takový, že $\psi(a) = b$. Ten se podle Lemmatu 1.4 rozšiřuje do $\mathbf{T}$-izomorfismu $\rho : \mathbf{S} \to \mathbf{S}$ takového, že $\rho|_{T(a)} = \psi$, speciálně tedy $\rho(a) = b$.

(3) Podobně jako v části (1), Tvrzení 1.1 říká, že každé $\varphi \in \mathrm{Gal}(\mathbf{U}/\mathbf{T})$ permutuje kořeny polynomu f v $\mathbf{U}$, ovšem tyto kořeny generují těleso $\mathbf{S}$, takže $\varphi(S) = S$ a restrikce $\varphi|_S$ je $\mathbf{T}$-automorfismem tělesa $\mathbf{S}$. Čili zobrazení

$$\Phi : \mathbf{Gal}(\mathbf{U}/\mathbf{T}) \to \mathbf{Gal}(\mathbf{S}/\mathbf{T}), \qquad \varphi \mapsto \varphi|_S$$

je dobře definovaný homomorfismus. Dokážeme, že jeho jádrem je $\mathbf{Gal}(\mathbf{U}/\mathbf{S})$ a obrazem celé $\mathbf{Gal}(\mathbf{S}/\mathbf{T})$. Dokazované tvrzení pak plyne z faktu, že jádro je normální podgrupou, a z 1. věty o izomorfismu.

Jádro $\mathbf{Ker}(\Phi)$ obsahuje právě ty automorfismy φ, pro které $\varphi|_S$ je identita, tedy právě všechny $\mathbf{S}$-automorfismy tělesa $\mathbf{U}$, tedy $\mathbf{Ker}(\Phi) = \mathbf{Gal}(\mathbf{U}/\mathbf{S})$. Co se týče obrazu, je-li dáno $\psi \in \mathrm{Gal}(\mathbf{S}/\mathbf{T})$, čili $\mathbf{T}$-izomorfismus $\mathbf{S} \to \mathbf{S}$, podle Lemmatu

1.4 existuje $\mathbf{T}$-automorfismus φ tělesa $\mathbf{U}$ takový, že $\varphi|_S = \psi$, a tedy $\mathbf{Im}(\Phi) = \mathbf{Gal}(\mathbf{S}/\mathbf{T})$. □

Na třech příkladech ilustrujeme použití Tvrzení 1.5 k výpočtu Galoisových grup.

Příklad. Je-li f ireducibilní polynom stupně 2 nad tělesem $\mathbf{T}$, pak $\mathbf{Gal}(f/\mathbf{T}) \simeq \mathbb{Z}_2$. Podle bodu (1) je tato grupa nejvýše dvouprvková, podle bodu (2) musí mít alespoň dva prvky.

Stejnou úvahu můžeme vztáhnout i na ireducibilní polynomy stupně 3: podle bodu (1) se $\mathbf{Gal}(f/\mathbf{T})$ vnořuje do $\mathbf{S}_3$, podle bodu (2) musí obsahovat aspoň tři prvky. Čili jsou pouze dvě možnosti: $\mathbf{Gal}(f/\mathbf{T})$ je izomorfní buď celé grupě $\mathbf{S}_3$, nebo její tříprvkové cyklické podgrupě, čili $\mathbb{Z}_3$. Oba případy jsou možné.

Příklad. Spočteme, že

$$\mathbf{Gal}(x^3 - 2/\mathbb{Q}) \simeq \mathbf{S}_3 \quad \text{a} \quad \mathbf{Gal}(x^3 - 2/\mathbb{Q}(e^{2\pi i/3})) \simeq \mathbb{Z}_3.$$

Označme $\mathbf{U} = \mathbb{Q}(\sqrt[3]{2}, e^{2\pi i/3})$ rozkladové nadtěleso polynomu $x^3 - 2$ a $\mathbf{S} = \mathbb{Q}(e^{2\pi i/3})$ rozkladové nadtěleso polynomu $x^3 - 1 = (x-1)(x^2+x+1)$ nad $\mathbb{Q}$. Z předchozího příkladu plyne, že $\mathbf{Gal}(x^2 + x + 1/\mathbb{Q}) = \mathbf{Gal}(\mathbf{S}/\mathbb{Q})$ je dvouprvková grupa. Nyní se podíváme na grupu $\mathbf{Gal}(x^3 - 2/\mathbf{S}) = \mathbf{Gal}(\mathbf{U}/\mathbf{S})$. Prvek $e^{2\pi i/3}$ je pevným bodem, $\sqrt[3]{2}$ se zobrazuje na jeden ze tří kořenů polynomu $x^3 - 2$, čili grupa může obsahovat nejvýše tři prvky. Podle bodu (2) musí mít alespoň tři prvky, čili je izomorfní $\mathbb{Z}_3$. Podle bodu (3) pak platí $\mathbf{Gal}(\mathbf{U}/\mathbb{Q})/\mathbf{Gal}(\mathbf{U}/\mathbf{S}) \simeq \mathbf{Gal}(\mathbf{S}/\mathbb{Q})$, tedy

$$|\mathbf{Gal}(\mathbf{U}/\mathbb{Q})| = |\mathbf{Gal}(\mathbf{U}/\mathbf{S})| \cdot |\mathbf{Gal}(\mathbf{S}/\mathbb{Q})| = 3 \cdot 2 = 6,$$

čili díky (1) je $\mathbf{Gal}(\mathbf{S}/\mathbb{Q}) \simeq \mathbf{S}_3$.

Příklad. Spočteme grupu

$$\mathbf{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}).$$

V sekci **??** jsme ukázali, že

$$\mathbf{S} = \mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$$

a že $m = m_{\sqrt{2}+\sqrt{3},\mathbb{Q}} = x^4 - 10x^2 + 1$. Tento polynom má 4 kořeny, $\pm\sqrt{2} \pm \sqrt{3}$, tedy těleso $\mathbf{S}$ je jeho rozkladovým nadtělesem. Těleso $\mathbf{S}$ má jediný generátor $\sqrt{2} + \sqrt{3}$, každý prvek $\mathbf{Gal}(\mathbf{S}/\mathbb{Q})$ jej zobrazuje na jeden ze čtyř kořenů polynomu m, přičemž bod (2) zajišťuje, že všechny čtyři možnosti dají automorfismus. Tedy $|\mathbf{Gal}(\mathbf{S}/\mathbb{Q})| = 4$.

Zbývá určit, jak prvky $\mathbf{Gal}(\mathbf{S}/\mathbb{Q})$ vypadají a zda je $\mathbf{Gal}(\mathbf{S}/\mathbb{Q})$ izomorfní grupě $\mathbb{Z}_4$, anebo grupě $\mathbb{Z}_2 \times \mathbb{Z}_2$. Aplikací Tvrzení 1.1 na polynomy $x^2 - 2$ a $x^2 - 3$ dostaneme, že každý $\varphi \in \mathrm{Gal}(\mathbf{S}/\mathbb{Q})$ splňuje $\varphi(\sqrt{2}) = u\sqrt{2}$ a $\varphi(\sqrt{3}) = v\sqrt{3}$ pro nějaká $u, v \in \{1, -1\}$. Čili

$$\varphi(a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}) = a + ub\sqrt{2} + vc\sqrt{3} + uvd\sqrt{6}$$

a snadno ověříme, že $\varphi^2 = id$ pro všechny volby u, v. Tedy $\mathbf{Gal}(\mathbf{S}/\mathbb{Q}) \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$.

Všimněte si, že ve všech příkladech vyšel stupeň rozkladového nadtělesa stejně, jako řád Galoisovy grupy. Formálně, je-li $\mathbf{S}$ rozkladovým nadtělesem polynomu f nad $\mathbf{T}$, pak $[\mathbf{S} : \mathbf{T}] = |\mathbf{Gal}(\mathbf{S}/\mathbf{T})|$. To není náhoda, nýbrž pravidlo (pro tělesa charakteristiky 0). Jeho důkaz je nicméně již mimo možnosti tohoto textu, viz např. [**?**].

Ve zbytku sekce se budeme věnovat dvěma speciálním případům. Za prvé, ukážeme, že rozkladová nadtělesa polynomů definujících n-té odmocniny mají řešitelné Galoisovy grupy; tento fakt je stěžejní v důkazu části Galoisovy věty (Věta 2.1), která říká, že polynomy, jejichž kořeny lze vyjádřit vzorcem, mají řešitelné Galoisovy grupy. Za druhé, ukážeme si polynom, jehož Galoisova grupa není řešitelná, a o němž tedy Galoisova věta říká, že jeho kořeny vzorcem vyjádřit nejdou.

Připomeňme značení $\zeta_n = e^{2\pi i/n}$.

Lemma 1.6. *Buď $0 \neq a \in \mathbb{Q}$. Rozkladovým nadtělesem polynomu $f = x^n - a$ nad tělesem $\mathbb{Q}$ je těleso $\mathbb{Q}(\zeta_n, b)$, kde b je libovolný komplexní kořen polynomu f.*

Důkaz. Komplexní kořeny polynomu f jsou právě čísla $b \cdot \zeta_n^k$, $k = 0, \ldots, n-1$: dosazením snadno ověříme, že každé z těchto čísel je kořenem, a víc kořenů být nemůže. Rozkladové nadtěleso tedy obsahuje jak prvek b (volbou $k = 0$), tak prvek ζ_n (součin $b^{-1} \cdot (b \cdot \zeta_n)$). Přitom každý kořen je součinem těchto dvou čísel, takže rozkladové nadtěleso můžeme napsat jako $\mathbb{Q}(\zeta_n, b)$. □

Tvrzení 1.7. *Buď $\mathbb{Q} \leq \mathbf{T} \leq \mathbb{C}$ těleso, $n \in \mathbb{N}$, $a \in T$. Pak*

(1) $\mathbf{Gal}(x^n - 1/\mathbf{T})$ *je abelovská grupa,*
(2) $\mathbf{Gal}(x^n - a/\mathbf{T}(\zeta_n))$ *je abelovská grupa,*
(3) $\mathbf{Gal}(x^n - a/\mathbf{T})$ *je metabelovská grupa.*

Důkaz. Označme $\mathbf{S} = \mathbf{T}(\zeta_n)$ a $\mathbf{U} = \mathbf{T}(\zeta_n, b)$, kde b je nějaký komplexní kořen polynomu $x^n - a$.

(1) Dokážeme, že $\mathbf{Gal}(x^n - 1/\mathbf{T})$ je izomorfní nějaké podgrupě grupy $\mathbb{Z}_n^*$, tedy jde o abelovskou grupu. Každý automorfismus $\varphi \in \mathrm{Gal}(\mathbf{S}/\mathbf{T})$ permutuje kořeny polynomu $x^n - 1$, čili $\varphi(\zeta_n) = \zeta_n^k$ pro nějaké $k \in \{0, \ldots, n-1\}$. Zároveň také permutuje kořeny všech polynomů $x^m - 1$, $m \mid n$, tedy zobrazení φ zachovává řády prvků v grupě $\mathbf{S}^*$, takže $\mathrm{ord}(\zeta_n^k) = n$, což nastane právě tehdy, když $\mathrm{NSD}(k, n) = 1$ (Tvrzení **??**). Vidíme, že zobrazení $\mathbf{Gal}(\mathbf{S}/\mathbf{T}) \to \mathbb{Z}_n^*$, které automorfismu φ přiřadí toto k, je prostý homomorfismus: prostý díky tomu, že φ je jednoznačně určeno hodnotou na generátoru, a homomorfismus díky tomu, že skládání automorfismů odpovídá násobení příslušných exponentů: je-li $\varphi(\zeta_n) = \zeta_n^k$ a $\psi(\zeta_n) = \zeta_n^l$, pak $\varphi(\psi(\zeta_n)) = (\zeta_n^l)^k = \zeta_n^{kl}$.

(2) Dokážeme, že $\mathbf{Gal}(x^n - a/\mathbf{S})$ je izomorfní nějaké podgrupě grupy $\mathbb{Z}_n$, tedy jde o abelovskou grupu. Kořeny polynomu $x^n - a$ v $\mathbf{S}$ jsou právě čísla tvaru $b \cdot \zeta_n^k$, $k = 0, \ldots, n-1$. Každý automorfismus $\varphi \in \mathrm{Gal}(\mathbf{U}/\mathbf{S})$ fixuje prvek ζ_n a zobrazuje $b \mapsto b \cdot \zeta_n^k$ pro nějaké k. Vidíme, že zobrazení $\mathbf{Gal}(\mathbf{U}/\mathbf{S}) \to \mathbb{Z}_n$, které automorfismu φ přiřadí toto k, je prostý homomorfismus: prostý díky tomu, že φ je jednoznačně určeno hodnotou na generátoru, a homomorfismus díky tomu, že skládání automorfismů odpovídá sčítání příslušných exponentů: je-li $\varphi(b) = b \cdot \zeta_n^k$ a $\psi(b) = b \cdot \zeta_n^l$, pak $\varphi(\psi(b)) = (b \cdot \zeta_n^l) \cdot \zeta_n^k = b \cdot \zeta_n^{k+l}$.

(3) Uvažujme rozšíření $\mathbf{T} \leq \mathbf{S} \leq \mathbf{U}$. Obě větší tělesa jsou rozkladová, můžeme tedy aplikovat Tvrzení 1.5(3), které říká, že $\{id\} \leq \mathbf{Gal}(\mathbf{U}/\mathbf{S}) \trianglelefteq \mathbf{Gal}(\mathbf{U}/\mathbf{T})$. Přitom grupa $\mathbf{Gal}(\mathbf{U}/\mathbf{S})$ je abelovská podle bodu (2), grupa $\mathbf{Gal}(\mathbf{U}/\mathbf{T}) \,/\, \mathbf{Gal}(\mathbf{U}/\mathbf{S}) \simeq \mathbf{Gal}(\mathbf{S}/\mathbf{T})$ je abelovská podle bodu (1), čili grupa $\mathbf{Gal}(\mathbf{U}/\mathbf{T})$ je metabelovská. □

Přestože většina polynomů stupně ≥ 5 nemá řešitelnou Galoisovu grupu, není úplně snadné nějaké konkrétní ukázat. Asi nejjednodušší rodinu příkladů popisuje následující tvrzení.

Tvrzení 1.8. *Buď p prvočíslo a $f \in \mathbb{Q}[x]$ ireducibilní polynom stupně p, který má $p-2$ reálných a 2 imaginární kořeny. Pak* $\mathbf{Gal}(f/\mathbb{Q}) \simeq \mathbf{S}_p$.

Důkaz. Buď $\mathbf{U}$ rozkladové nadtěleso polynomu f nad $\mathbb{Q}$. Podle Tvrzení 1.5(1) se grupa $\mathbf{G} = \mathbf{Gal}(\mathbf{U}/\mathbb{Q})$ vnořuje do grupy $\mathbf{S}_p$, dívejme se na její prvky jako na permutace na kořenech polynomu f. Dokážeme, že $\mathbf{G}$ obsahuje aspoň jednu transpozici a aspoň jeden p-cyklus. Pak stačí využít pozorování, že libovolná transpozice a libovolný p-cyklus generují celou grupu $\mathbf{S}_p$ (viz cvičení v sekci **??**).

Komplexní sdružení je netriviálním $\mathbb{Q}$-automorfismem tělesa $\mathbf{U}$. Přitom $p-2$ kořenů fixuje a 2 prohazuje, jde tedy o transpozici na kořenech.

Uvažujme působení grupy $\mathbf{G}$ na množině kořenů polynomu f. Podle Tvrzení 1.5(2) jde o tranzitivní působení, má tedy jednu orbitu velikosti p. Avšak velikost orbity dělí řád působící grupy, čili $p \mid |G|$. Podle Cauchyho věty obsahuje grupa $\mathbf{G}$ prvek řádu p, což může být pouze p-cyklus. □

Příklad. Příkladem polynomu, který splňuje předpoklady Tvrzení 1.8, je třeba $f = x^5 - 4x + 2$. Tento polynom je ireducibilní podle Eisensteinova kritéria a počet reálných kořenů snadno zjistíme pomocí diferenciálního kalkulu: $f' = 5x^4 - 4$, tato rovnice má dvě reálná řešení, tedy příslušná reálná funkce f má jedno lokální maximum a jedno lokální minimum, přičemž snadno dopočítáme, že maximum je kladné a minimum záporné. Protože jsou polynomiální funkce spojité, f musí mít právě tři reálné kořeny.

2. (Ne)řešitelnost polynomů v radikálech

Definice. Buď $\mathbf{T} \leq \mathbf{U}$ rozšíření těles a $a \in U$. Řekneme, že prvek a je *vyjádřitelný v radikálech* nad tělesem $\mathbf{T}$, pokud existuje řada rozšíření $\mathbf{T} = \mathbf{T}_0 \leq \mathbf{T}_1 \leq \ldots \leq \mathbf{T}_k$ taková, že $a \in T_k$ a každé $\mathbf{T}_i$ je rozkladovým nadtělesem nějakého polynomu $x^{n_i} - a_i \in T_{i-1}[x]$ nad tělesem $\mathbf{T}_{i-1}$.

Neformálně, prvek je vyjádřitelný v radikálech nad $\mathbf{T}$, pokud jej lze zapsat za pomoci prvků tělesa $\mathbf{T}$, operací $+, -, \cdot, /$ a n-tých odmocnin. Např. prvek

$$\frac{\sqrt{\sqrt[3]{2}+1}}{i+1}$$

je vyjádřitelný nad $\mathbb{Q}$, neboť je prvkem rozšíření $\mathbb{Q} \leq \mathbf{T}_1 \leq \mathbf{T}_2 \leq \mathbf{T}_3$, kde postupně použijeme polynomy $x^3 - 2 \in \mathbb{Q}[x]$, $x^2 - (\sqrt[3]{2}+1) \in T_1[x]$ a $x^2 + 1 \in T_2[x]$.

Definice. Buď $\mathbf{T}$ těleso a f polynom z $\mathbf{T}[x]$. Řekneme, že polynom f je *řešitelný v radikálech* nad tělesem $\mathbf{T}$, pokud je každý kořen polynomu f vyjádřitelný v radikálech nad $\mathbf{T}$. Jinými slovy, pokud existuje řada rozšíření $\mathbf{T} = \mathbf{T}_0 \leq \mathbf{T}_1 \leq \ldots \leq \mathbf{T}_k$ taková, že každé $\mathbf{T}_i$ je rozkladovým nadtělesem nějakého polynomu $x^{n_i} - a_i \in T_{i-1}[x]$ nad tělesem $\mathbf{T}_{i-1}$, a rozkladové nadtěleso polynomu f je obsaženo v $\mathbf{T}_k$.

Nyní můžeme zformulovat slavnou Galoisovu větu.

Věta 2.1 (Galoisova věta)**.** *Buď $\mathbf{T}$ těleso charakteristiky 0 a f polynom z $\mathbf{T}[x]$ stupně ≥ 1. Polynom f je řešitelný v radikálech právě tehdy, když je grupa* $\mathbf{Gal}(f/\mathbf{T})$ *řešitelná.*

Podle Tvrzení 1.5 se Galoisova grupa polynomu stupně n vnořuje do grupy $\mathbf{S}_n$. Existence vzorců na řešení polynomiálních rovnic stupně n se tak dostává do přímé souvislosti s řešitelností grupy $\mathbf{S}_n$.

Důsledek 2.2.
- *Všechny polynomy stupně ≤ 4 jsou řešitelné v radikálech.*
- (Abel-Ruffiniho věta) *Existují racionální polynomy stupně 5 a více, které nejsou řešitelné v radikálech nad tělesem $\mathbb{Q}$.*

Důkaz. (1) Buď f polynom stupně n. Podle Tvrzení 1.5(1) je $\mathbf{Gal}(f/\mathbf{T})$ podgrupou grupy $\mathbf{S}_n$. V sekci jsme ukázali, že grupy $\mathbf{S}_n$, $n \leq 4$, i jejich podgrupy (Tvrzení 0.1(1)) jsou řešitelné. Z Galoisovy věty tedy plyne, že polynomy stupně ≤ 4 jsou řešitelné v radikálech.

(2) Grupy $\mathbf{S}_n$, $n \geq 5$, nejsou řešitelné. Podle Tvrzení 1.8 existuje polynom stupně 5, jehož Galoisova grupa je $\mathbf{S}_5$. □

Nyní dokážeme část Galoisovy věty, která říká, že polynomy řešitelné v radikálech mají řešitelnou Galoisovu grupu. Idea důkazu je následující: pro řešitelný polynom f vezmeme rozšíření

$$\mathbb{Q} = \mathbf{T}_0 \leq \mathbf{T}_1 \leq \ldots \leq \mathbf{T}_k$$

taková, že $\mathbf{T}_i$ je rozkladové nadtěleso nějakého polynomu $x^{n_i} - a_i \in T_{i-1}[x]$ nad tělesem $\mathbf{T}_{i-1}$, a rozkladové nadtěleso polynomu f je obsaženo v $\mathbf{T}_k$. Za jistých okolností bude takové řadě odpovídat řada normálních podgrup

$$\mathbf{Gal}(\mathbf{T}_k/\mathbb{Q}) = \mathbf{Gal}(\mathbf{T}_k/\mathbf{T}_0) \geq \mathbf{Gal}(\mathbf{T}_k/\mathbf{T}_1) \geq \ldots \geq \mathbf{Gal}(\mathbf{T}_k/\mathbf{T}_k) = \{id\},$$

přičemž faktorgrupy $\mathbf{Gal}(\mathbf{T}_k/\mathbf{T}_i) \,/\, \mathbf{Gal}(\mathbf{T}_k/\mathbf{T}_{i+1})$ budou izomorfní $\mathbf{Gal}(x^{n_i} - a_i/\mathbf{T}_i)$, a tedy řešitelné podle Tvrzení 1.7. Potom Důsledek 0.2 zaručí, že celá grupa $\mathbf{Gal}(\mathbf{T}_k/\mathbb{Q})$ je řešitelná a pomocí Tvrzení 1.5(3) se ukáže řešitelnost i pro Galoisovu grupu rozkladového nadtělesa polynomu f, které je obsaženo v $\mathbf{T}_k$.

Aby tento postup fungoval, tělesa $\mathbf{T}_1, \ldots, \mathbf{T}_k$ by musela být rozkladová pro nějaké polynomy nad $\mathbf{T}$. To obecně pravda není, v důkazu tedy budeme konstruovat posloupnost o trochu větších těles, která tuto vlastnost mají a přitom Galoisova grupa největšího tělesa zůstává řešitelná.

Lemma 2.3. *Buď $\mathbf{S}$ rozkladové nadtěleso nějakého polynomu nad tělesem $\mathbf{T}$ a buď g ireducibilní polynom v $\mathbf{T}[x]$. Pokud má polynom g v tělese $\mathbf{S}$ nějaký kořen, pak se v $\mathbf{S}[x]$ rozkládá na lineární činitele.*

Důkaz. Označme f polynom, pro nějž je $\mathbf{S}$ rozkladovým nadtělesem, a uvažujme rozkladové nadtěleso $\mathbf{U}$ pro polynom fg nad $\mathbf{T}$. Označme a kořen polynomu g v tělese $\mathbf{S}$ a uvažujme jakýkoliv jiný kořen b tohoto polynomu v $\mathbf{U}$. Chceme dokázat, že b leží v $\mathbf{S}$. Podle Lemmatu 1.3 existuje $\mathbf{T}$-izomorfismus $\mathbf{T}(a) \to \mathbf{T}(b)$ zobrazující $a \mapsto b$, a ten se podle Lemmatu 1.4 rozšiřuje do $\mathbf{T}$-izomorfismu $\varphi : \mathbf{U} \to \mathbf{U}$, tj. prvku $\mathbf{Gal}(\mathbf{U}/\mathbf{T})$, který splňuje $\varphi(a) = b$. Podle Tvrzení 1.1 zobrazení φ permutuje kořeny polynomu f, ty generují těleso $\mathbf{S}$, a tedy $\varphi(S) \subseteq S$. Speciálně dostáváme, že $b = \varphi(a) \in S$. □

Lemma 2.4. *Buď $\mathbf{T}$ těleso charakteristiky 0 a $\mathbf{T} \leq \mathbf{S} \leq \mathbf{U}$ rozšíření těles taková, že $\mathbf{S}$ je rozkladové nadtěleso nějakého polynomu nad $\mathbf{T}$ a $\mathbf{U}$ je rozkladové nadtěleso polynomu $x^n - a \in S[x]$ nad $\mathbf{S}$. Pak existuje rozšíření $\mathbf{U} \leq \mathbf{V}$ takové, že $\mathbf{V}$ je rozkladové nadtěleso nějakého polynomu nad $\mathbf{T}$ a $\mathbf{Gal}(\mathbf{V}/\mathbf{S})$ je řešitelná grupa.*

Poznamenejme, že kdyby bylo samo $\mathbf{U}$ rozkladovým nadtělesem nějakého polynomu nad $\mathbf{T}$, pak bychom mohli volit $\mathbf{V} = \mathbf{U}$ a řešitelnost by zajistilo Tvrzení 1.7.

Důkaz. Bez újmy na obecnosti můžeme předpokládat, že $\mathbf{U} \leq \mathbb{C}$ (rozkladová nadtělesa jsou izomorfní a jedno lze najít v $\mathbb{C}$). Označme f polynom, pro nějž je $\mathbf{S}$ rozkladovým nadtělesem. Definujeme polynom

$$g = m_{a,\mathbf{T}}(x^n) \in T[x]$$

(do minimálního polynomu $m_{a,\mathbf{T}}$ dosadíme mocninu proměnné x) a uvažujme rozkladové nadtěleso $\mathbf{V} \leq \mathbb{C}$ polynomu $fg \in T[x]$ nad tělesem $\mathbf{T}$.

Nejprve si všimneme, že $\mathbf{U} \leq \mathbf{V}$: v oboru $\mathbf{S}[x]$ platí $x - a \mid m_{a,\mathbf{T}}$, tedy také $x^n - a \mid m_{a,\mathbf{T}}(x^n) = g$, takže se polynom $x^n - a$ rozkládá ve $\mathbf{V}[x]$ na lineární činitele. Dokážeme, že $\mathbf{Gal}(\mathbf{V}/\mathbf{S})$ je řešitelná grupa.

Polynom $m_{a,\mathbf{T}}$ je ireducibilní, má kořen v tělese $\mathbf{S}$, a tedy se tam podle Lemmatu 2.3 rozkládá na lineární činitele. Označme tento rozklad $m_{a,\mathbf{T}} = (x-a_1)\cdots(x-a_m)$. Pak

$$g = m_{a,\mathbf{T}}(x^n) = (x^n - a_1)\cdots(x^n - a_m).$$

Definujeme sekvenci

$$\mathbf{S} = \mathbf{S}_0 \leq \mathbf{S}_1 \leq \ldots \leq \mathbf{S}_{m-1} \leq \mathbf{S}_m = \mathbf{V},$$

kde $\mathbf{S}_i$ je rozkladovým nadtělesem polynomu $x^n - a_i$ nad $\mathbf{S}_{i-1}$, čili také rozkladovým nadtělesem polynomu $(x^n-a_1)\cdots(x^n-a_i)$ nad $\mathbf{S}$, pro každé $i = 1, \ldots, m$. Uvažujme řadu podgrup

$$\mathbf{Gal}(\mathbf{V}/\mathbf{S}) = \mathbf{Gal}(\mathbf{V}/\mathbf{S}_0) \geq \mathbf{Gal}(\mathbf{V}/\mathbf{S}_1) \geq \ldots \geq \mathbf{Gal}(\mathbf{V}/\mathbf{S}_m) = \{id\}.$$

Protože jsou všechna mezitělesa $\mathbf{S}_i$ rozkladová nad $\mathbf{S}$, můžeme aplikovat Tvrzení 1.5(3). Aplikací na rozšíření $\mathbf{S} \leq \mathbf{S}_i \leq \mathbf{V}$ vidíme, že $\mathbf{Gal}(\mathbf{V}/\mathbf{S}_i) \trianglelefteq \mathbf{Gal}(\mathbf{V}/\mathbf{S})$. Aplikací na rozšíření $\mathbf{S} \leq \mathbf{S}_{i-1} \leq \mathbf{S}_i$ vidíme, že

$$\mathbf{Gal}(\mathbf{V}/\mathbf{S}_i) \,/\, \mathbf{Gal}(\mathbf{V}/\mathbf{S}_{i+1}) \simeq \mathbf{Gal}(\mathbf{S}_{i+1}/\mathbf{S}_i),$$

přičemž tyto faktorgrupy jsou řešitelné podle Tvrzení 1.7, protože $\mathbf{S}_i$ je rozkladovým nadtělesem polynomu $x^n - a_i$ nad tělesem $\mathbf{S}_{i-1}$. Důsledek 0.2 zaručí, že celá grupa $\mathbf{Gal}(\mathbf{V}/\mathbf{S})$ je řešitelná. □

Důkaz Galoisovy věty 2.1, část ($\Rightarrow$).

Buď f polynom řešitelný v radikálech a uvažujme řadu rozšíření prokazující tento fakt, tj. mějme $\mathbf{T} = \mathbf{T}_0 \leq \mathbf{T}_1 \leq \ldots \leq \mathbf{T}_k$ taková, že $\mathbf{T}_i$ je rozkladové nadtěleso nějakého polynomu $x^{n_i} - a_i \in T_{i-1}[x]$ nad tělesem $\mathbf{T}_{i-1}$ a rozkladové nadtěleso $\mathbf{W}$ polynomu f nad $\mathbf{T}$ je obsaženo v tělese $\mathbf{T}_k$. Dokážeme, že grupa $\mathbf{Gal}(f/\mathbf{T}) = \mathbf{Gal}(\mathbf{W}/\mathbf{T})$ je řešitelná.

Postavíme řadu rozšíření

$$\mathbf{T} = \mathbf{U}_0 = \mathbf{V}_0 \leq \mathbf{U}_1 \leq \mathbf{V}_1 \leq \ldots \leq \mathbf{U}_k \leq \mathbf{V}_k$$

tak, že pro $i = 1, \ldots, m$ vezmeme $\mathbf{U}_i$ rozkladové nadtěleso polynomu $x^{n_i} - a_i$ nad tělesem $\mathbf{V}_{i-1}$ a vezmeme $\mathbf{V}_i$ jako těleso $\mathbf{V}$ z Lemmatu 2.4 aplikovaného na rozšíření $\mathbf{T} \leq \mathbf{V}_{i-1} \leq \mathbf{U}_i$. Čili každé $\mathbf{V}_i$ je rozkladové nadtěleso nad $\mathbf{T}$ a grupa $\mathbf{Gal}(\mathbf{V}_i/\mathbf{V}_{i-1})$ je řešitelná.

Zbytek důkazu je podobný jako v předchozím lemmatu. Z řady rozšíření $\mathbf{T} = \mathbf{V}_0 \leq \mathbf{V}_1 \leq \ldots \leq \mathbf{V}_k$ získáme řadu podgrup

$$\mathbf{Gal}(\mathbf{V}_k/\mathbf{T}) = \mathbf{Gal}(\mathbf{V}_k/\mathbf{V}_0) \geq \mathbf{Gal}(\mathbf{V}_k/\mathbf{V}_1) \geq \ldots \geq \mathbf{Gal}(\mathbf{V}_k/\mathbf{V}_k) = \{id\}.$$

Protože jde o rozkladová nadtělesa nad $\mathbf{T}$, můžeme aplikovat Tvrzení 1.5(3). Aplikací na rozšíření $\mathbf{T} \leq \mathbf{V}_i \leq \mathbf{V}_k$ vidíme, že $\mathbf{Gal}(\mathbf{V}/\mathbf{V}_i) \trianglelefteq \mathbf{Gal}(\mathbf{V}/\mathbf{T})$. Aplikací na rozšíření $\mathbf{T} \leq \mathbf{V}_{i-1} \leq \mathbf{V}_i$ vidíme, že

$$\mathbf{Gal}(\mathbf{V}_k/\mathbf{V}_i) \,/\, \mathbf{Gal}(\mathbf{V}_k/\mathbf{V}_{i+1}) \simeq \mathbf{Gal}(\mathbf{V}_{i+1}/\mathbf{V}_i),$$

což již víme, že jsou řešitelné grupy. Důsledek 0.2 zaručí, že celá grupa $\mathbf{Gal}(\mathbf{V}_k/\mathbf{T})$ je řešitelná.

Zbývá dokázat, že grupa $\mathbf{Gal}(\mathbf{W}/\mathbf{T})$ je také řešitelná. Znovu použijeme Tvrzení 1.5(3) na rozšíření $\mathbf{T} \leq \mathbf{W} \leq \mathbf{V}_k$ a vidíme, že

$$\mathbf{Gal}(\mathbf{W}/\mathbf{T}) \simeq \mathbf{Gal}(\mathbf{V}_k/\mathbf{T}) \,/\, \mathbf{Gal}(\mathbf{V}_k/\mathbf{W}).$$

Nyní stačí použít Tvrzení 0.1, které říká, že faktorgrupa řešitelné grupy $\mathbf{Gal}(\mathbf{V}_k/\mathbf{T})$ je také řešitelná. □

3. Cardanovy vzorce

VÍCE VIZ STARÁ SKRIPTA

Kubické rovnice. Budeme řešit rovnici

$$x^3 + bx + c = 0.$$

Všimněte si, že pro libovolné u, v platí

$$(u+v)^3 - 3uv(u+v) - (u^3 + v^3) = 0.$$

Řešení rovnice budeme hledat ve tvaru $x = u + v$, přičemž aby to sedělo, pro koeficienty dostáváme rovnosti

$$b = -3uv, \qquad c = -u^3 - v^3.$$

Nyní je snadné vyjádřit u, v pomocí koeficientů b, c: dosazením $v = -\frac{b}{3u}$ do druhé rovnosti dostáváme

$$u^6 + cu^3 - \frac{b^3}{27} = 0,$$

což je kvadratická rovnice s neznámou u^3. Označíme-li diskriminant $D = c^2 + \frac{4}{27}b^3$, řešením je $u^3 = \frac{-c \pm \sqrt{D}}{2}$. Ze dvou možností $\pm$ uvažujme například součet (druhá volba by přinesla ty samé tři kořeny, ale v jiném pořadí). Označíme-li ω libovolnou třetí odmocninu z $\frac{-c+\sqrt{D}}{2}$ a $\zeta = \zeta_3 = e^{2\pi i/3}$, máme pro u tři řešení,

$$u_k = \zeta^k \cdot \omega, \quad k = 0, 1, 2,$$

a k nim snadno dopočteme odpovídající hodnoty

$$v_k = -\frac{b}{3u_k} = \zeta^{-k} \cdot \frac{b}{3\omega}, \quad k = 0, 1, 2.$$

Řešením původní rovnice jsou pak všechny tři součty $u_k + v_k$.

Je-li zlomek $\frac{-c+\sqrt{D}}{2}$ reálný, je přirozené zvolit reálnou odmocninu $\omega = \sqrt[3]{\frac{-c+\sqrt{D}}{2}}$, upravíme zlomek $\frac{b}{3\omega} = \sqrt[3]{\frac{-c-\sqrt{D}}{2}}$ a dostaneme kořeny

$$x_k = \zeta^k \cdot \sqrt[3]{\frac{-c+\sqrt{D}}{2}} - \zeta^{-k} \cdot \sqrt[3]{\frac{c+\sqrt{D}}{2}}.$$

Vidíme, že se všechny tři kořeny $x_k = u_k + v_k$ nacházejí v tělese $\mathbb{Q}(\zeta, \omega)$, které dostaneme jako řadu dvou rozkladových rozšíření

$$\mathbb{Q} \leq \mathbb{Q}(\sqrt{D}) \leq \mathbb{Q}(\zeta, \omega),$$

první pro polynom $x^2 - D \in \mathbb{Q}[x]$, druhé pro polynom $x^3 - \frac{-c+\sqrt{D}}{2} \in \mathbb{Q}(\sqrt{D})[x]$. Rozkladové nadtěleso polynomu $x^3 + bx + c$ je jeho podtělesem.

Příklad. Vyřešíme rovnici

$$x^3 - 6x - 9 = 0.$$

Diskriminant je roven $D = 49$, čili $u^3 = \frac{9+7}{2} = 8$ a $v^3 = \frac{-9+7}{2} = -1$. Volbou $\omega = 2$ dostaneme kořeny

$$x_0 = u - v = 3, \quad x_1 = \zeta u - \zeta^2 v = \frac{-3 + \sqrt{3}i}{2}, \quad x_2 = \zeta^2 u - \zeta v = \frac{-3 - \sqrt{3}i}{2}.$$

Rozkladovým nadtělesem je $\mathbb{Q}(\zeta) = \mathbb{Q}(\sqrt{3}i)$ a v tomto případě je totožné s výše popsaným tělesem $\mathbb{Q}(\zeta, \omega)$.

Příklad. Vyřešíme rovnici

$$x^3 - 3x + 1 = 0.$$

Diskriminant je roven $D = -3$, čili $u^3 = \frac{-1+\sqrt{3}i}{2}$ a $v^3 = \frac{1+\sqrt{3}i}{2}$, z čehož snadno vyjádříme kořeny jako rozdíly třetích odmocnin z jistých imaginárních čísel. Přesto, jak se snadno přesvědčíme vyšetřením průběhu funkce, všechny tři kořeny jsou reálné. Čili rozkladové nadtěleso neobsahuje žádný z prvků $\sqrt{D}, \zeta, \omega$.

Případu, kdy jsou reálné kořeny vyjádřeny pomocí odmocnin z imaginárních čísel, se říká *casus irreducibilis*. Pro některé polynomy se tomuto popisu nelze vyhnout, tj. neexistuje zápis kořenů pomocí vzorce, který by používal pouze reálná čísla. Tento fakt přesvědčil tehdejší matematiky k přijetí komplexních čísel jako smysluplného číselného oboru.