GALOISOVA TEORIE

DAVID STANOVSKÝ

1. 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 1.1. *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 1.2. *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.*

2. Izomorfismy tělesových rozšíření

2.1. Kořenová a rozkladová nadtělesa: jednoznačnost.

Buď $\mathbf{T}$ těleso a $f \in T[x]$ 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 $f(a) = 0$), a *rozkladovým nadtělesem* rozumíme minimální rozšíření, kde se rozkládá na lineární činitele (tj. rozšíření $\mathbf{S}$, kde existují $a_1, \dots, a_n \in S$ taková, že $\mathbf{S} = \mathbf{T}(a_1, \dots, a_n)$ a $f \parallel (x-a_1)\cdot\ldots\cdot(x-a_n)$).

V sekci **??** jsme si ukázali existenci těchto rozšíření. Vzpomeňte, že nejsou určena jednoznačně: například pro polynom x^3-2 nad $\mathbb{Q}$ lze vzít kořenová nadtělesa $\mathbb{Q}(\sqrt[3]{2})$ nebo $\mathbb{Q}(\sqrt[3]{2}\cdot e^{2\pi i/3}) = \mathbb{Q}(\sqrt[3]{2}\cdot e^{4\pi i/3})$ (obě jsou číselná tělesa, jedno reálné, druhé imaginární), ale také třeba $\mathbb{Q}[\alpha]/(\alpha^3 - 2)$, které není podtělesem $\mathbb{C}$. Tato tělesa jsou různá, ale přesto jsou $\mathbb{Q}$-izomorfní. Uvidíme, že postačující podmínkou pro izomorfismus je ireducibilita daného polynomu. (Neireducibilní polynomy typicky nemají izomorfní kořenová nadtělesa, např. pokud se f rozkládá na součin dvou polynomů g, h různého stupně, pak jejich kořenová nadtělesa mají různý stupeň, a tedy nemohou být izomorfní.)

Pro rozkladová nadtělesa máme izomorfismus také, tentokrát již bez předpokladu ireducibility.

---

29. května 2018.

Věta 2.1. *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 podrobnější tvrzení o existenci izomorfismů mezi kořenovými a rozkladovými nadtělesy s jistými vlastnostmi. Věta 2.1 bude speciálním případem těchto lemmat. K jejich formulaci bude 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 2.2. *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 **??** a **??** 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 2.3. *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 $f \in T_1[x]$ 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 $\mathbf{T}$-izormorfismus $\psi : \mathbf{S}_1 \to \mathbf{S}_2$ 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 2.2 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 2.1.

2.2. **Galoisova grupa polynomu.**

Buď $\mathbf{T} \leq \mathbf{S}$ rozšíření těles. Všechny $\mathbf{T}$-automorfismy tělesa $\mathbf{S}$ (tj. $\mathbf{T}$-izomorfismy $\mathbf{S} \to \mathbf{S}$) tvoří podgrupu symetrické grupy na množině S (Tvrzení **??**), která se nazývá *Galoisova grupa rozšíření* $\mathbf{T} \leq \mathbf{S}$ a značí se $\mathbf{Gal}(\mathbf{S}/\mathbf{T})$.

Buď f polynom z $\mathbf{T}[x]$ stupně ≥ 1. *Galoisovou grupou polynomu* f, značíme $\mathbf{Gal}(f/\mathbf{T})$, rozumíme grupu $\mathbf{Gal}(\mathbf{S}/\mathbf{T})$, kde $\mathbf{S}$ je rozkladové nadtěleso polynomu f nad $\mathbf{T}$. Dává tento pojem smysl, když rozkladové nadtěleso není určeno jednoznačně? Uvažujme $\mathbf{T}$-izomorfismus $\psi : \mathbf{S}_1 \to \mathbf{S}_2$ dvou rozkladových nadtěles pro f. Pak

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

je izomorfismus příslušných Galoisových grup (dokažte jako cvičení!). Čili Galoisovy grupy polynomu jsou určeny *až na izomorfismus*.

Příklad.

- $\mathbf{Gal}(\mathbb{R}/\mathbb{Q}) = \{id\}$,
- $\mathbf{Gal}(\mathbb{C}/\mathbb{R}) = \mathbf{Gal}(x^2+1/\mathbb{R}) = \{id, {}^-\}$, kde ${}^-$ je komplexní sdružení,
- $\mathbf{Gal}(\mathbb{C}/\mathbb{Q})$ je nekonečná.

Spočítat prvky Galoisovy grupy daného rozšíření jsou obecně komplikované, snadné není ani ověřit tvrzení z předchozího příkladu. Ve zbytku sekce si ukážeme, jak počítat Galoisovy grupy rozkladových nadtěles a spočítáme několik příkladů, včetně $\mathbf{Gal}(\mathbb{C}/\mathbb{R})$.

Zcela základním pozorováním je, že $\mathbf{T}$-automorfismy tělesa $\mathbf{S} = \mathbf{T}(a_1, \ldots, a_n)$ jsou určeny obrazem na prvcích $a_1, \ldots, a_n$. Buď φ nějaký $\mathbf{T}$-automorfismus a označme $\varphi(a_i) = u_i$. Jsou-li prvky $a_1, \ldots, a_n$ algebraické nad $\mathbf{T}$, obecný prvek $s \in S$ můžeme vyjádřit jako (konečný) 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

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

Ovšem pozor, daná volba hodnot u_i nemusí být přípustná pro žádný $\mathbf{T}$-automorfismus! Např. pro $\mathbf{T} = \mathbb{Q}$ a $\mathbf{S} = \mathbb{Q}(i)$ musí platit $\varphi(i)^2 = \varphi(i^2) = \varphi(-1) = -1$, čili jediné přípustné hodnoty jsou $\pm i$. Obecný princip formuluje následující lemma.

Lemma 2.4. *Buď* $\mathbf{T} \leq \mathbf{S}$ *rozšíření těles,* $f \in T[x]$ *a* A *množina všech kořenů polynomu* f *v* $\mathbf{S}$*. 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. Tedy $\varphi(A) \subseteq A$. Protože je φ izomorfismus, je $\varphi|_A$ prosté zobrazení, a protože je množina A konečná, je to permutace na A. □

Příklad. Spočteme prvky grupy $\mathbf{Gal}(\mathbb{Q}(i)/\mathbb{Q})$. Každý $\mathbb{Q}$-automorfismus φ tělesa $\mathbb{Q}(i)$ je určen hodnotou $\varphi(i)$. Přitom podle Lemmatu 2.4 permutuje φ kořeny polynomu x^2+1, tedy $\varphi(i) = i$ nebo $\varphi(i) = -i$. První volba vede na zobrazení $\varphi(a+bi) = \varphi(a)+\varphi(b)\varphi(i) = a+bi$, tedy jde o identické zobrazení. Druhá volba vede na zobrazení $\varphi(a+bi) = a-bi$, tedy jde o operaci komplexního sdružení, což je jistě homomorfismus. Čili $\mathbf{Gal}(\mathbb{Q}(i)/\mathbb{Q}) = \{id, {}^-\}$ je dvouprvková grupa. Protože je $\mathbb{Q}(i)$ rozkladové nadtěleso polynomu x^2+1 nad $\mathbb{Q}$, můžeme psát $\mathbf{Gal}(x^2+1/\mathbb{Q}) \simeq \mathbb{Z}_2$.

Stejný argument projde i pro rozšíření $\mathbb{R} \leq \mathbb{C} = \mathbb{R}(i)$ a velmi podobně lze spočítat, že $\mathbf{Gal}(\mathbb{Q}(\sqrt{s}) : \mathbb{Q}) = \{id, \varphi\}$, kde $\varphi(a + b\sqrt{s}) = a - b\sqrt{s}$.

Příklad. Všimněte si, že $\mathbf{Gal}(\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}) = \{id\}$, protože $\sqrt[3]{2}$ je jediným kořenem polynomu $x^3 - 2$ v tomto tělese.

Ovšem $\mathbf{Gal}(x^3 - 2/\mathbb{Q})$ je netriviální grupa: je potřeba se podívat na rozkladové nadtěleso $\mathbb{Q}(\sqrt[3]{2}, e^{2\pi i/3})$. Vidíme, že první generátor má tři možné obrazy (tři různé kořeny $x^3 - 2$), zatímco druhý prvek pouze dva možné obrazy (dva různé kořeny polynomu $x^2 + x + 1$), čili Galoisova grupa má nejvýše šest prvků. Složitější je dokázat, že skutečně šest $\mathbb{Q}$-automorfismů tohoto tělesa existuje a že tvoří grupu izomorfní grupě $\mathbf{S}_3$, což uvidíme později na základě Tvrzení 2.5.

Následující tvrzení umožňují určit Galoisovy grupy některých jednodušších polynomů.

Tvrzení 2.5. *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 tělese $\mathbf{S}$, které nejsou v $\mathbf{T}$. Protože je $\mathbf{S}$ rozkladové pro f, platí $\mathbf{S} = \mathbf{T}(a_1, \ldots, a_m)$. Uvažujme libovolné $\varphi \in \mathrm{Gal}(\mathbf{S}/\mathbf{T})$. Lemma 2.4 říká, že $\varphi|_A$ je permutace na A (ostatní kořeny musí fixovat). Přitom φ je jednoznačně určené svými hodnotami na prvcích $a_1, \ldots, a_m$, tedy je určené svojí restrikcí $\varphi|_A$. Z toho plyne, že zobrazení

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

je prosté, a je snadné nahlédnout, že to je homomorfismus.

(2) Podle Lemmatu 2.2 existuje $\mathbf{T}$-isomorfismus kořenových nadtěles $\psi : \mathbf{T}(a) \to \mathbf{T}(b)$ takový, že $\psi(a) = b$. Ten se podle Lemmatu 2.3 rozšiřuje do $\mathbf{T}$-isomorfismu $\rho : \mathbf{S} \to \mathbf{S}$ takového, že $\rho|_{T(a)} = \psi$, speciálně tedy $\rho(a) = b$.

(3) Pro $\varphi \in \mathrm{Gal}(\mathbf{U}/\mathbf{T})$ definujeme zobrazení $\Phi(\varphi) = \varphi|_S$. Dokážeme, že Φ je o homomorfismus $\mathbf{Gal}(\mathbf{U}/\mathbf{T}) \to \mathbf{Gal}(\mathbf{S}/\mathbf{T})$, jehož 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.

Nejprve musíme ověřit, že $\varphi|_S$ je vždy prvkem grupy $\mathbf{Gal}(\mathbf{S}/\mathbf{T})$. Podle Lemmatu 2.4 zobrazení φ permutuje kořeny polynomu f. Ty ovšem generují těleso $\mathbf{S}$, a tedy $\varphi(S) = S$, čili zobrazení $\varphi|_S$ je $\mathbf{T}$-automorfismem tělesa $\mathbf{S}$. Restrikce na podmnožinu zachovává skládání, takže zobrazení Φ je homomorfismem $\mathbf{Gal}(\mathbf{U}/\mathbf{T}) \to \mathbf{Gal}(\mathbf{S}/\mathbf{T})$. Spočteme jeho jádro a obraz.

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 $\mathbf{T}$-isomorfismus $\mathbf{S} \to \mathbf{S}$, podle Lemmatu 2.3 existuje $\mathbf{T}$-automorfismus φ tělesa $\mathbf{U}$ takový, že $\varphi|_S = \psi$, tedy $\mathbf{Im}(\Phi) = \mathbf{Gal}(\mathbf{S}/\mathbf{T})$. □

Na třech příkladech ilustrujeme použití Tvrzení 2.5 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 2.5(1) je tato grupa nejvýše dvouprvková, podle 2.5(2) musí mít alespoň dva prvky.

Stejnou úvahu můžeme vztáhnout i na ireducibilní polynomy stupně 3: podle 2.5(1) se $\mathbf{Gal}(f/\mathbf{T})$ vnořuje do $\mathbf{S}_3$, podle 2.5(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 $\mathbb{Q}$. Úvaha pro polynomy stupně 2 říká, 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 $e^{2\pi i/3}$ se fixuje, $\sqrt[3]{2}$ se zobrazuje na jeden ze tří kořenů polynomu $x^3 - 2$, čili grupa může obsahovat nejvýše tři prvky. Podle 2.5(2) musí mít alespoň tři prvky, čili je izomorfní $\mathbb{Z}_3$. Podle 2.5(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 2.5(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

2.5(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 $\mathbb{Z}_4$ nebo grupě $\mathbb{Z}_2 \times \mathbb{Z}_2$. Aplikací Lemmatu 2.4 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 $u, v \in \{1, -1\}$, a tedy

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

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

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 stěžejním v důkazu části Galoisovy věty (Věta 3.1), která říká, že polynomy, jejichž kořeny lze vyjádřit vzorcem (který specifikujeme v sekci 3), mají řešitelné Galoisovy grupy. Za druhé, ukážeme si polynom, jehož Galoisova grupa není řešitelná.

Tvrzení 2.6. *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) $\mathbf{Gal}(x^n - a/\mathbf{T}(e^{2\pi i/n}))$ *je abelovská grupa,*
(3) $\mathbf{Gal}(x^n - a/\mathbf{T})$ *je metabelovská grupa.*

Důkaz. Označme $\zeta_n = e^{2\pi i/n}$, $\mathbf{S} = \mathbf{T}(\zeta_n)$ 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. Vzhledem k charakteristice 0 můžeme předpokládat, že rozkladovým nadtělesem polynomu $x^n - 1$ je $\mathbf{S} = \mathbf{T}(\zeta_n)$. 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. Vzhledem k charakteristice 0 můžeme předpokládat, že rozkladovým nadtělesem polynomu $x^n - a$ je $\mathbf{U} = \mathbf{T}(\zeta_n, b)$. 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 2.5(3), které říká, že $\{id\} \leq \mathbf{Gal}(\mathbf{U}/\mathbf{S}) \trianglelefteq \mathbf{Gal}(\mathbf{U}/\mathbf{T})$, a 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 předvést. Asi nejjednodušší rodinu příkladů popisuje následující tvrzení.

Tvrzení 2.7. *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 2.5(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 (viz cvičení v sekci **??**), že libovolná transpozice a libovolný p-cyklus generují celou grupu $\mathbf{S}_p$.

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 2.5(2) jde o tranzitivní působení, má tedy jednu orbitu velikosti p. Avšak velikost orbity dělí řád působící grupy (Tvrzení **??**), čili $p \mid |G|$. Podle Cauchyho věty (Věta **??**) obsahuje grupa $\mathbf{G}$ prvek řádu p, což může být pouze p-cyklus. □

Příklad. Příkladem polynomu, který splňuje předpoklady Tvrzení 2.7, 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 polynomiální funkce jsou spojité, musí existovat právě tři reálné kořeny.

3. (Ne)řešitelnost polynomů v radikálech

3.1. Vyjádřitelnost v radikálech.

Cílem této kapitoly je ukázat tzv. *Abel-Ruffiniho větu*, která říká, že pro $n \geq 5$ neexistuje vzorec, který by vyjadřoval kořeny polynomů stupně n pomocí jeho koeficientů za použití základních aritmetických operací $+, -, \cdot, /$ a n-tých odmocnin. První argument předvedl v roce 1799 Paolo Ruffini, ten však byl neúplný. Na základě Ruffiniho myšlenek pak Niels Henrik Abel našel v roce 1823 kompletní důkaz. My půjdeme jinou, přímější cestou, kterou odhalil o 10 let později Évariste Galois. Jeho metoda navíc umožňuje dokázat kritérium, které popisuje ty polynomy, jejichž kořeny nelze vyjádřit vzorcem. Čili nejen že neexistuje vzorec, který by fungoval pro všechny polynomy daného stupně zároveň, ale pro některé polynomy neexistuje ani jednorázové vyjádření kořenů.

Nejrpve si musíme ujasnit, co přesně znamená „vyjádřitelnost kořenů vzorcem“.

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 $\mathbf{T}_i$ je rozkladové nadtěleso nějakého polynomu $x^{n_i} - a_i \in T_{i-1}[x]$ nad tělesem $\mathbf{T}_{i-1}$, a $a \in T_k$.

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 $\mathbf{T}_i$ 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 $\mathbf{T}_k$.

Nyní můžeme zformulovat slavnou Galoisovu větu.

Věta 3.1 (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.*

Připomeňme Tvrzení 2.5(1): Galoisova grupa polynomu stupně n se vnořuje do grupy $\mathbf{S}_n$ (permutace kořenů). V sekci 1 jsme ukázali, že grupy $\mathbf{S}_2$, $\mathbf{S}_3$ a $\mathbf{S}_4$, i jejich podgrupy, jsou řešitelné. Z Galoisovy věty tedy plyne, že jejich kořeny lze vyjádřit pomocí vzorců. Tyto vzorce byly nalezeny již 16. století, říká se jim *Cardanovy vzorce* a ukážeme si je v další části. Naopak, grupa $\mathbf{S}_5$ řešitelná není a skutečně existuje polynom s takovou Galoisovou grupou (Tvrzení 2.7). Důsledkem je zmíněná Abel-Ruffiniho věta, totiž že existuje polynom stupně 5, který není řešitelný v radikálech.

Důsledek 3.2 (Abel-Ruffiniho věta)**.** *Existují racionální polynomy stupně 5 a více, které nejsou řešitelné v radikálech nad tělesem $\mathbb{Q}$.*

V těchto skriptech dokážeme pouze jednu implikaci Galoisovy věty, tu, ze které plyne neexistence vzorců. Opačná implikace je složitější a k důkazu Abel-Ruffiniho věty není potřeba. Mimo rozsah těchto skript jsou i další části Galoisovy teorie, zejména její hlavní věta o korespondenci mezi podtělesy daného rozkladového nadtělesa a podgrupami příslušné Galoisovy grupy. Také bychom měli zmínit, že předpoklad charakteristiky 0 je zbytečně silný, většina Galoisovy teorie platí i pro konečná tělesa a obecně všechna rozšíření, která jsou tzv. *separabilní*, tj. kde ireducibilní polynomy nemají vícenásobné kořeny.

3.2. Cardanovy vzorce.

VIZ SKRIPTA

3.3. Neřešitelnost polynomů stupně ≥ 5.

V této části 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 $\mathbf{Gal}(\mathbf{T}_k/\mathbf{T}_i) \,/\, \mathbf{Gal}(\mathbf{T}_k/\mathbf{T}_{i+1})$ jsou izomorfní $\mathbf{Gal}(x^{n_i} - a_i/\mathbf{T}_i)$, a tedy řešitelné podle Tvrzení 2.6. Potom Důsledek 1.2 zaručí, že celá grupa $\mathbf{Gal}(\mathbf{T}_k/\mathbb{Q})$

je řešitelná a pomocí Tvrzení 2.5(3) se ukáže řešitelnost i pro Galoisovu grupu rozkladového nadtělesa polynomu f, které je obsaženo v $\mathbf{T}_k$.

Aby tento postup fungoval, je třeba splnit řadu předpokladů. Zejména jde o to, abychom pracovali pouze s tělesy, která jsou rozkladová nad $\mathbb{Q}$, což tělesa $\mathbf{T}_1, \ldots, \mathbf{T}_k$ splňovat nemusí. Většina sekce je o vylepšení tohoto postupu tak, aby byl skutečně správně.

Lemma 3.3. *Buď $\mathbf{S}$ rozkladové nadtěleso nějakého polynomu nad tělesem $\mathbf{T}$ a buď $g \in T[x]$ ireducibilní polynom. Pokud má polynom g v tělese $\mathbf{S}$ nějaký kořen, pak se nad tělesem $\mathbf{S}$ 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 2.2 existuje $\mathbf{T}$-izomorfismus $\mathbf{T}(a) \to \mathbf{T}(b)$ a ten se podle Lemmatu 2.3 rozšiřuje do $\mathbf{T}$-isomorfismu $\varphi : \mathbf{U} \to \mathbf{U}$, tj. prvku $\mathbf{Gal}(\mathbf{U}/\mathbf{T})$, který splňuje $\varphi(a) = b$. Podle Lemmatu 2.4 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 3.4. *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 2.6.

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 $\mathbf{T}$. Vidíme, že $\mathbf{U} \leq \mathbf{V}$, protože $x - a \mid m_{a,\mathbf{T}}$ v $\mathbf{S}[x]$, tedy $x^n - a \mid m_{a,\mathbf{T}}(x^n) = g$ v $\mathbf{S}[x]$, 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.

Označme $a_1, \ldots, a_m$ kořeny polynomu $m_{a,\mathbf{T}}$ ve svém rozkladovém nadtělese nad $\mathbf{S}$. Tento polynom je ireducibilní, jeho kořen a leží v $\mathbf{S}$, tedy podle Lemmatu 3.3 jsou všechny prvky $a_1, \ldots, a_m$ v $\mathbf{S}$. Čili $m_{a,\mathbf{T}} = (x - a_1) \cdots (x - a_m)$, a tak

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

v $\mathbf{S}[x]$. Definujeme sekcenci

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

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 $i = 1, \ldots, m$. Protože jsou všechna mezitělesa rozkladová nad $\mathbf{S}$, můžeme aplikovat Tvrzení 2.5(3). Uvažujme řadu normálních podgrup

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

Podle tvrzení aplikovaného na rozšíření $\mathbf{S} \leq \mathbf{S}_i \leq \mathbf{V}$ vidíme, že $\mathbf{Gal}(\mathbf{V}/\mathbf{S}_i) \trianglelefteq \mathbf{Gal}(\mathbf{V}/\mathbf{S})$. Podle tvrzení aplikovaného 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 2.6, protože $\mathbf{S}_i$ je rozkladovým nadtělesem polynomu $x^n - a_i$ nad tělesem $\mathbf{S}_{i-1}$. Důsledek 1.2 zaručí, že celá grupa $\mathbf{Gal}(\mathbf{V}/\mathbf{S})$ je řešitelná. □

Důkaz Galoisovy věty 3.1, 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 3.4 aplikovaného na $\mathbf{S} = \mathbf{V}_{i-1}$ a $\mathbf{U} = \mathbf{U}_i$. 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. Na řadu rozšíření $\mathbf{T} = \mathbf{V}_0 \leq \mathbf{V}_1 \leq \ldots \leq \mathbf{V}_k$ aplikujeme Tvrzení 2.5(3) a získáme řadu normálních podgrup

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

Podle tvrzení aplikovaného na rozšíření $\mathbf{T} \leq \mathbf{V}_i \leq \mathbf{V}_k$ vidíme, že $\mathbf{Gal}(\mathbf{V}/\mathbf{V}_i) \trianglelefteq \mathbf{Gal}(\mathbf{V}/\mathbf{T})$. Podle tvrzení aplikovaného 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 jsou řešitelné grupy. Důsledek 1.2 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 2.5(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 1.1, které říká, že faktorgrupa řešitelné grupy $\mathbf{Gal}(\mathbf{V}_k/\mathbf{T})$ je také řešitelná. □