GALOISOVA TEORIE

DAVID STANOVSKÝ

Předběžná varianta!!! Obsahuje aktualizaci obsahu kapitoly o kořenových rozšířeních a novou kapitolu o Galoisově teorii. Četl jsem to po sobě jenom jednou, takže text určitě obsahuje chyby a nejasná místa. Budu vděčný, když mě na ně upozorníte (stanovsk karlin.mff.cuni.cz).

1. Kořenová rozšíření

1.1. Kořenová a rozkladová nadtělesa.

Cílem tohoto odstavce je dokázat, že pro každý polynom $f \in T[x]$ existuje nejmenší rozšíření $\mathbf{S} \geq \mathbf{T}$, kde se f rozkládá na lineární činitele (tj. polynomy stupně 1). Intuitivně je věc jasná: je-li $\mathbf{T} \leq \mathbb{C}$, pak stačí vzít $\mathbf{S} = \mathbf{T}(a_1, \ldots, a_n)$, kde $a_1, \ldots, a_n$ jsou komplexní kořeny polynomu f. Problémy jsou dva: jednak jsme nedokázali, že se f nad komplexními čísly skutečně rozkládá (tento fakt se nazývá základní věta algebry a není zas tak snadné ho dokázat), ale, a to zejména, ne každé těleso je podtělesem $\mathbb{C}$.

Definice. Buď $\mathbf{T} \leq \mathbf{S}$ rozšíření těles a $f \in T[x]$. Řekneme, že $\mathbf{S}$ je

(1) *kořenové nadtěleso* polynomu f nad $\mathbf{T}$, pokud má polynom f v tělese $\mathbf{S}$ kořen a a navíc $\mathbf{S} = \mathbf{T}(a)$.
(2) *rozkladové nadtěleso* polynomu f nad $\mathbf{T}$, pokud se polynom f rozkládá v $\mathbf{S}[x]$ na lineární činitele, tj. $f \parallel (x-a_1)\cdot\ldots\cdot(x-a_n)$ pro nějaká $a_1, \ldots, a_n \in S$, a navíc $\mathbf{S} = \mathbf{T}(a_1, \ldots, a_n)$.

Příklad. Příklady kořenových a rozkladových nadtěles (uvedena jsou všechna, která jsou obsažena v tělese $\mathbb{C}$):

f	kořenová nadtělesa f nad $\mathbb{Q}$	rozkladové nadtěleso f nad $\mathbb{Q}$
x^2+1	$\mathbb{Q}(i)$	$\mathbb{Q}(i)$
x^2-1	$\mathbb{Q}$	$\mathbb{Q}$
x^3-1	$\mathbb{Q},\ \mathbb{Q}(e^{2\pi i/3})$	$\mathbb{Q}(e^{2\pi i/3})$
x^4-1	$\mathbb{Q},\ \mathbb{Q}(i)$	$\mathbb{Q}(i)$
x^3-2	$\mathbb{Q}(\sqrt[3]{2}),\ \mathbb{Q}(\sqrt[3]{2}\cdot e^{2\pi i/3})$	$\mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{2}\cdot e^{2\pi i/3})$

Obecně, kořenové nadtěleso polynomu $x^n - 1$ nad tělesem $\mathbb{Q}$ je každé $\mathbb{Q}(e^{2k\pi i/n})$, kde $k = 0, \ldots, n-1$, ale není jasné, která z těchto těles jsou totožná. Rozkladové nadtěleso dostaneme volbou $k = 1$. Z teorie cyklotomických polynomů plyne, že stupeň tohoto rozkladového nadtělesa je $\varphi(n)$, kde φ značí Eulerovu funkci.

Dokážeme, že pro každý polynom stupně aspoň 1 existuje kořenové i rozkladové nadtěleso, a navíc, že rozkladové nadtěleso je určeno jednoznačně až na izomorfismus. Klíčovým krokem je kontrukce rozšíření, kde má daný polynom aspoň *nějaký* kořen. Dále pak stačí postupovat indukcí.

Lemma 1.1. *Buď $\mathbf{T}$ těleso a $f \in T[x]$ stupně ≥ 1. Pak existuje kořenové nadtěleso polynomu f nad $\mathbf{T}$.*

Důkaz. Buď g nějaký ireducibilní dělitel polynomu f. Hlavní ideál $I = gT[x]$ je maximální ideál v oboru $\mathbf{T}[x]$, a tedy faktorokruh $\mathbf{S} = \mathbf{T}[x]/(g)$ je podle Věty **??** těleso. Uvažujme homomorfismus

$$\psi : \mathbf{T} \to \mathbf{S}, \qquad a \mapsto [a].$$

Ten je podle Tvrzení **??**(3) prostý, protože prvky tělesa $\mathbf{T}$ (jakožto konstantní polynomy) nejsou v ideálu I. Můžeme tedy ztotožnit těleso $\mathbf{T}$ s $\mathbf{Im}(\psi)$ (formálně vzato, jsou izomorfní) a budeme uvažovat, že $\mathbf{T} \leq \mathbf{S}$. (Podobným způsobem jsme se vypořádali s vnořením daného oboru do jeho podílového tělesa, kde ztotožňujeme prvek a a zlomek $\frac{a}{1}$.) Dosadíme-li do polynomu $g = \sum_{i=0}^{n} a_i x^i$ prvek $b = [x] \in S$, dostaneme

$$g(b) = \sum_{i=0}^{n} a_i [x]^i = [\sum_{i=0}^{n} a_i x^i] = [g] = [0],$$

neboť $g \in I$. Prvek b je tedy kořenem polynomu g, čili také polynomu f, v tělese $\mathbf{S}$. Přitom $\mathbf{S} = \mathbf{T}(b)$, protože už okruh $\mathbf{T}[x]$ je generován množinou $T \cup \{x\}$. □

Příklad. Uvažujme těleso $\mathbb{Q}$ a polynom $x^2 + 1$. Kořenovým nadtělesem je jistě těleso $\mathbb{Q}(i) \leq \mathbb{C}$. Důkaz Lemmatu 1.1 nabízí jinou, abstraktní konstrukci kořenového nadtělesa: protože je polynom $x^2 + 1$ ireducibilní, je jím faktorokruh $\mathbb{Q}[x]/(x^2 + 1)$. Je snadné ukázat, že obě nadtělesa jsou izomorfní: uvažujme homomorfismus

$$\varphi : \mathbb{Q}[x] \to \mathbb{Q}(i), \quad f \mapsto f(i).$$

Jak jsme rozebrali v Sekci **??**, jádrem tohoto homomorfismu je ideál $(x^2 + 1)\mathbb{Q}[x]$, takže podle 1. věty o izomorfismu platí $\mathbb{Q}[x]/(x^2 + 1) \simeq \mathbb{Q}(i)$.

Věta 1.2. *Buď $\mathbf{T}$ těleso a $f \in T[x]$ stupně ≥ 1. Pak existuje rozkladové nadtěleso polynomu f nad $\mathbf{T}$.*

Důkaz. Budeme postupovat indukcí podle stupně polynomu f. Je-li f stupně 1, pak $\mathbf{S} = \mathbf{T}$. V opačném případě uvažujme kořenové nadtěleso $\mathbf{T}(a) \geq \mathbf{T}$ polynomu f a polynom $g \in T(a)[x]$ takový že $f = g \cdot (x - a)$. Pak $\deg g < \deg f$, tedy podle indukčního předpokladu existuje jeho rozkladové nadtěleso $\mathbf{S} = \mathbf{T}(a, b_1, \ldots, b_m)$ nad $\mathbf{T}(a)$. Protože se polynom g rozkládá v $\mathbf{S}[x]$ na lineární činitele, rozkládá se tam i $f = g \cdot (x - a)$. □

Buď $\mathbf{T} \leq \mathbf{S}$, $\mathbf{T} \leq \mathbf{U}$ rozšíření těles. Zobrazení $\varphi : \mathbf{S} \to \mathbf{U}$ se nazývá $\mathbf{T}$-*izomorfismus*, pokud je to tělesový izomorfismus splňující $\varphi(a) = a$ pro každé $a \in T$. Důležitou vlastností rozkladových nadtěles je jejich jednoznačnost až na $\mathbf{T}$-izomorfismus. Prvním krokem je dokázat jednoznačnost kořenových nadtěles pro ireducibilní polynomy.

Lemma 1.3. *Buď $\mathbf{T}$ těleso, $f \in T[x]$ ireducibilní polynom a $\mathbf{S}_1, \mathbf{S}_2$ kořenová nadtělesa polynomu f nad $\mathbf{T}$. Pak existuje $\mathbf{T}$-izomorfismus $\mathbf{S}_1 \to \mathbf{S}_2$.*

Důkaz. Uvažujme dvě kořenová nadtělesa $\mathbf{T} \leq \mathbf{T}(a)$ a $\mathbf{T} \leq \mathbf{T}(b)$. Podle Tvrzení **??** a **??** je $T(a) = \{g(a) : g \in T[x]\}$ a $T(b) = \{g(b) : g \in T[x]\}$. Uvažujme tedy zobrazení

$$\varphi : T(a) \to T(b), \qquad g(a) \mapsto g(b).$$

Přesněji řečeno, je třeba dokázat, že to je skutečně zobrazení. Je důležité si uvědomit, že $f = m_{a,\mathbf{T}} = m_{b,\mathbf{T}}$, protože f je ireducibilní polynom a a i b jsou jeho kořeny. Proto, podle definice minimálního polynomu,

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

Čili φ je skutečně zobrazení, a navíc prosté. Protože očividně zachovává všechny operace a přitom nehýbe s prvky $\mathbf{T}$ (které odpovídají konstantním polynomům g), je to $\mathbf{T}$-izomorfismus $\mathbf{T}(a) \to \mathbf{T}(b)$. □

K důkazu jednoznačnosti rozkladových nadtěles se hodí o něco obecnější princip, který využijeme také v sekcích o algebraickém uzávěru a o Galoisových grupách.

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. Uvažujme polynomy $f = \sum a_i x^i \in T_1[x]$, $\varphi(f) = \sum \varphi(a_i) x^i \in T_2[x]$ 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 opět postupovat indukcí podle stupně polynomu f. Je-li $\deg f = 1$, pak je $\mathbf{S}_1 = \mathbf{T}_1$ a $\mathbf{S}_2 = \mathbf{T}_2$ jediná volba. V opačném případě 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 $\mathbf{S}_2$. Podobně jako v Lemmatu 1.3 uvažujme zobrazení

$$\psi : \mathbf{T}_1(a) \to \mathbf{T}_2(b), \qquad h(a) \mapsto \varphi(h)(b).$$

Analogicky dokážeme, že jde o $\mathbf{T}$-izomorfismus, je třeba si všimnout, že $m_{a,\mathbf{T}_1} = g$, zatímco $m_{b,\mathbf{T}_2} = \varphi(g)$. Navíc $\psi|_{T_1} = \varphi$, neboť v tomto případě jde o zúžení na polynomy g, které jsou stupně 0. Nyní použijeme indukční předpoklad. Označme $h \in T_1(a)[x]$ polynom splňující $f = (x - a) \cdot h$, tedy také $\psi(f) = (x - b) \cdot \psi(h)$ protože $\psi(a) = b$. Dále označme $\mathbf{S}_1$ a $\mathbf{S}_2$ rozkladová nadtělesa těchto polynomů nad tělesy $\mathbf{T}_1(a)$ a $\mathbf{T}_2(b)$. Protože $\deg h < \deg f$, podle indukčního předpokladu existuje $\mathbf{T}$-izomorfismus $\rho : \mathbf{S}_1 \to \mathbf{S}_2$ takový, že $\rho|_{T_1(a)} = \psi$, a tedy $\rho|_{T_1} = \varphi$. □

Věta 1.5. *Buď $\mathbf{T}$ těleso a $f \in T[x]$ stupně ≥ 1. Pak každá dvě rozkladová nadtělesa polynomu f nad $\mathbf{T}$ jsou $\mathbf{T}$-izomorfní.*

Důkaz. Plyne z předchozího lemmatu dosazením $\mathbf{T}_1 = \mathbf{T}_2 = \mathbf{T}$ a $\varphi = id$. □

1.2. **Algebraický uzávěr.**

Definice. Těleso $\mathbf{T}$ se nazývá *algebraicky uzavřené*, jestliže má každý polynom z $\mathbf{T}[x]$ stupně ≥ 1 v tělese $\mathbf{T}$ kořen.

V algebraicky uzavřeném tělese se každý polynom rozkládá na lineární činitele, což můžeme snadno dokázat indukcí podle $\deg f$: pro polynomy stupně 1 je tvrzení triviální; pro vyšší stupně využijeme existenci nějakého kořene a, vydělíme f polynomem $x - a$, čímž získáme polynom menšího stupně a ten rozložíme pomocí indukčního předpokladu.

Příklad. Těleso $\mathbb{C}$ je algebraicky uzavřené. Tomuto tvrzení se říká *základní věta algebry* a její důkaz lze nejsnáze provést pomocí komplexní analýzy. Ač se její platnost dlouho tušila, poprvé byla se všemi detaily dokázána Gaussem až kolem roku 1800. (Název věty je z dnešního pohledu poněkud zavádějící a pochází z počátku 19. století, kdy se algebra zabývala především kořeny polynomů.)

Poznámka. Žádné konečné těleso nemůže být algebraicky uzavřené. Označíme-li $a_1, \ldots, a_n$ jeho prvky, pak polynom $(x - a_1) \cdot \ldots \cdot (x - a_n) + 1$ nemá v tomto tělese kořen.

Definice. Řekneme, že $\mathbf{S} \geq \mathbf{T}$ je *algebraický uzávěr* tělesa $\mathbf{T}$, pokud je $\mathbf{S}$ algebraicky uzavřené těleso a zároveň je algebraickým rozšířením tělesa $\mathbf{T}$.

Příklady.

- Algebraický uzávěr tělesa $\mathbb{R}$ je těleso $\mathbb{C}$; je to rozšíření stupně 2, tedy algebraické.
- Algebraický uzávěr tělesa $\mathbb{Q}$ není těleso $\mathbb{C}$, neboť nejde o algebraické rozšíření. Algebraický uzávěr $\mathbb{Q}$ popisuje následující tvrzení.

Věta 1.6. *Buď $\mathbf{S}$ rozšíření tělesa $\mathbf{T}$. Pak*

(1) *množina*

$$U = \{a \in S : \ a \text{ je algebraický prvek nad } \mathbf{T}\}$$

tvoří podtěleso tělesa $\mathbf{S}$;

(2) *je-li těleso $\mathbf{S}$ algebraicky uzavřené, pak $\mathbf{U}$ je algebraický uzávěr tělesa $\mathbf{T}$.*

Důkaz. (1) Nechť $a, b \in U$ a uvažujme těleso $\mathbf{T}(a, b)$. Protože jsou a, b algebraické prvky nad $\mathbf{T}$, jde o rozšíření konečného stupně (Věta **??**), a tudíž o rozšíření algebraické (Tvrzení **??**). Čili $T(a, b) \subseteq U$ a speciálně tedy U obsahuje prvky $a + b$, $a \cdot b$, $-a$ i a^{-1} (pro $a \neq 0$). Tedy U tvoří podtěleso.

(2) Evidentně je $\mathbf{U}$ algebraické rozšíření tělesa $\mathbf{T}$. Je algebraicky uzavřené? Uvažujme libovolný polynom

$$f = \sum_{i=0}^{n} a_i x^i \in U[x].$$

Tento polynom má jistě kořen $b \in S$, protože těleso $\mathbf{S}$ je algebraicky uzavřené. Přitom prvek b je algebraický nad tělesem $\mathbf{T}(a_0, \ldots, a_n)$, protože ve skutečnosti je $f \in T(a_0, \ldots, a_n)[x]$. Z Tvrzení **??** tak plyne, že stupeň $[\mathbf{T}(a_0, \ldots, a_n, b) : : \mathbf{T}(a_0, \ldots, a_n)]$ je konečný. Přitom stupeň $[\mathbf{T}(a_0, \ldots, a_n) : \mathbf{T}]$ je také konečný, neboť $a_0, \ldots, a_n$ jsou algebraické nad $\mathbf{T}$, a tak podle Tvrzení **??** je stupeň

$$[\mathbf{T}(a_0, \ldots, a_n, b) : \mathbf{T}] = [\mathbf{T}(a_0, \ldots, a_n, b) : \mathbf{T}(a_0, \ldots, a_n)] \cdot [\mathbf{T}(a_0, \ldots, a_n) : \mathbf{T}]$$

také konečný. Tedy podle Tvrzení **??** je prvek b algebraický nad $\mathbf{T}$, čili kořen b polynomu f leží v $\mathbf{U}$. □

Tedy algebraický uzávěr tělesa $\mathbb{Q}$ sestává právě z těch komplexních čísel, která jsou algebraická nad $\mathbb{Q}$. Speciálně, algebraický uzávěr $\mathbb{Q}$ je spočetný, zatímco množina $\mathbb{C}$ je nespočetná. (Obecněji, algebraický uzávěr nekonečného tělesa má stejnou velikost jako dané těleso. Argument je analogický důkazu, že algebraických čísel nad $\mathbb{Q}$ je jen spočetně mnoho, viz Sekce **??**.)

Věta 1.7. *Ke každému tělesu $\mathbf{T}$ existuje algebraický uzávěr. Každé dva algebraické uzávěry tělesa $\mathbf{T}$ jsou $\mathbf{T}$-izomorfní.*

Lemma 1.8. *Buď $\mathbf{R}$ okruh a $A \subseteq R$. Pak existuje maximální ideál v $\mathbf{R}$ obsahující množinu A.*

Důkaz. Buď $\mathcal{I}$ množina všech vlastních ideálů obsahujících podmnožinu A, uspořádaná inkluzí. Množina $\mathcal{I}$ je neprázdná, obsahuje například ideál generovaný množinou A. Každý řetězec v $(\mathcal{I}, \subseteq)$ má horní mez, konkrétně sjednocení těchto ideálů (důkáže se podobně jako Tvrzení **??**). Podle Zornova lemmatu **??** tedy existuje maximální prvek v $(\mathcal{I}, \subseteq)$. □

Lemma 1.9. *Ke každému tělesu* $\mathbf{T}$ *existuje rozšíření* $\mathbf{S} \geq \mathbf{T}$ *takové, že každý polynom z* $\mathbf{T}[x]$ *má v* $\mathbf{S}$ *kořen.*

Důkaz. Důkaz je analogický konstrukci kořenového nadtělesa daného polynomu; budeme konstruovat něco jako „kořenové nadtěleso pro všechny polynomy zároveň". Buď tedy X množina proměnných taková, že každému ireducibilnímu polynomu z $\mathbf{T}[x]$ stupně aspoň 1 odpovídá jedna proměnná; formálně, položme

$$X = \{x_f : f \in T[x], \deg f \geq 1\}.$$

Uvažujme nyní okruh $\mathbf{T}[X]$ (polynomy konečně mnoha proměnných vybíraných z X). Podle Lemmatu 1.8 existuje maximální ideál $\mathbf{I}$ obsahující všechny polynomy $f(x_f)$, $f \in T[x]$, $\deg f \geq 1$ (zde za proměnnou x v polynomu f substituujeme proměnnou x_f). Faktorokruh $\mathbf{S} = \mathbf{T}[X]/\mathbf{I}$ je podle Věty **??** těleso a podobně jako v důkazu Lemmatu 1.1 se dokáže, že do něj lze vnořit těleso $\mathbf{T}$ (vnoření $t \mapsto [t]$) a že každý polynom $f \in T[x]$ má v $\mathbf{S}$ kořen, konkrétně $[x_f]$. □

Důkaz Věty 1.7. Nejprve dokážeme existenci. Uvažujme řetězec nadtěles $\mathbf{T} = \mathbf{S}_0 \leq \mathbf{S}_1 \leq \mathbf{S}_2 \leq \ldots$, kde $\mathbf{S}_{i+1}$ vznikne z $\mathbf{S}_i$ konstrukcí z Lemmatu 1.9. Položme $\mathbf{S} := \bigcup_{i=0}^{\infty} \mathbf{S}_i$. Toto je také těleso. Přitom je algebraicky uzavřené, neboť každý polynom $f \in S[x]$ má jen konečně mnoho koeficientů, tedy $f \in S_i[x]$ pro nějaké (dostatečně velké) i, a tedy f má kořen v $\mathbf{S}_{i+1}$, čili také v $\mathbf{S}$. Algebraický uzávěr získáme aplikací Věty 1.6.

Uvažujme nyní dva algebraické uzávěry $\mathbf{S}_1, \mathbf{S}_2$ tělesa $\mathbf{T}$. Pokud $\mathbf{S}_1 \leq \mathbf{S}_2$, pak podle Věty 1.6 těleso $\mathbf{S}_1$ sestává ze všech prvků tělesa $\mathbf{S}_2$, které jsou algebraické nad $\mathbf{T}$. Protože $\mathbf{S}_2$ je z definice algebraické rozšíření tělesa $\mathbf{T}$, musí být $\mathbf{S}_1 = \mathbf{S}_2$. Nyní uvažujme obecnou situaci $\mathbf{T} \leq \mathbf{S}_1$, $\mathbf{T} \leq \mathbf{S}_2$. Uvažujme množinu

$$\mathcal{M} = \{\varphi : \mathbf{U}_1 \to \mathbf{U}_2 \ \mathbf{T}\text{-izomorfismus} : \mathbf{T} \leq \mathbf{U}_1 \leq \mathbf{S}_1, \mathbf{T} \leq \mathbf{U}_2 \leq \mathbf{S}_2\}$$

uspořádanou inkluzí, tj. $\varphi \leq \psi$ právě tehdy, když definiční obor φ je podmnožinou definičního oboru ψ a $\varphi(x) = \psi(x)$ pro všechna x z definičního oboru zobrazení φ. Množina $\mathcal{M}$ je neprázdná, obsahuje např. identické zobrazení na $\mathbf{T}$. Sjednocením řetězce zobrazení $\varphi_i \in \mathcal{M}$ dostaneme opět zobrazení z $\mathcal{M}$ (ověřte jako cvičení!). Podle Zornova lemmatu **??** tedy existuje maximální prvek v $(\mathcal{M}, \subseteq)$, označme jej $\varphi : \mathbf{U}_1 \to \mathbf{U}_2$. Dokážeme, že toto maximální zobrazení φ je $\mathbf{T}$-izomorfismus $\mathbf{S}_1 \to \mathbf{S}_2$.

Nejprve uvažujme případ, že $\mathbf{U}_1 \neq \mathbf{S}_1$. Pak $\mathbf{U}_1$ není algebraicky uzavřené těleso (jinak bychom měli dva do sebe vnořené algebraické uzávěry, což jsme vyvrátili výše), tedy existuje polynom $f = \sum a_i x^i \in U_1[x]$, který nemá v $\mathbf{U}_1$ kořen. Buď $\mathbf{V}_1$ rozkladové nadtěleso polynomu f nad $\mathbf{U}_1$ a buď $\mathbf{V}_2$ rozkladové nadtěleso polynomu $\varphi(f) = \sum \varphi(a_i) x^i \in U_2[x]$ nad $\mathbf{U}_2$. Podle Lemmatu 1.4 existuje $\mathbf{T}$-izomorfismus $\psi : \mathbf{V}_1 \to \mathbf{V}_2$ takový, že $\psi|_{\mathbf{U}_1} = \varphi$, čímž dostáváme spor s maximalitou zobrazení φ.

Dokázali jsme, že maximální zobrazení v $(\mathcal{M}, \subseteq)$ má za definiční obor $\mathbf{U}_1 = \mathbf{S}_1$. Tedy obor hodnot, $\mathbf{U}_2$, je také algebraicky uzavřený. Podle výše uvedeného pozorování musí nutně platit $\mathbf{U}_2 = \mathbf{S}_2$. □

2. Galoisovy grupy a neřešitelnost polynomů stupně ≥ 5

2.1. **Galoisovy grupy.**

Definice. Buď $\mathbf{T} \leq \mathbf{S}$ rozšíření těles. Připomeňme, že $\mathbf{T}$-*automorfismy* tělesa $\mathbf{S}$ jsou právě ty izomorfismy $\varphi : \mathbf{S} \to \mathbf{S}$ splňující $\varphi(x) = x$ pro každé $x \in T$. Všechny $\mathbf{T}$-automorfismy tělesa $\mathbf{S}$ tvoří podgrupu symetrické grupy na množině S, tato grupa se nazývá *Galoisova grupa* rozšíření $\mathbf{T} \leq \mathbf{S}$ a značí se $\mathbf{Gal}(\mathbf{S}/\mathbf{T})$.

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 za použití základních aritmetických operací $+, -, \cdot, /$ a n-tých odmocnin. První „důkaz" podal 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 odahlil o 10 let později Évariste Galois. Jeho metoda navíc umožňuje dokázat silnější tvrzení, totiž že pro každé $n \geq 5$ existuje polynom stupně n, jehož kořeny nelze vyjádřit vzorcem (tj. nejen že neexistuje vzorec, který by fungoval pro všechny polynomy zároveň, ale pro některé polynomy neexistuje ani jednorázové vyjádření kořenů pomocí uvedených operací). Nazývejme takové polynomy *neřešitelné v radikálech*, formální definici uvedeme v Sekci 2.3. Galoisův důkaz je založen na následujícím kritériu, pomocí kterého je dokonce možné zjistit, zda je daný polynom řešitelný v radikálech.

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

Pojem řešitelné grupy vysvětlíme v Sekci 2.2. Zatím se spokojme s informací, že grupy $\mathbf{S}_n$, $n \geq 5$, řešitelné nejsou. K důkazu silnější verze Abel-Ruffiniho věty tak stačí najít polynomy stupně n, jejichž Galoisova grupa je izomorfní grupě $\mathbf{S}_n$. Z toho důvodu v tomto textu ukážeme pouze jednu implikaci v Galoisově větě, totiž že řešitelné polynomy mají řešitelnou Galoisovu grupu. Opačná implikace je složitější a k důkazu Abel-Ruffiniho věty není potřeba.

Poznamenejme, že předpoklad charakteristiky 0 je zbytečně silný. Co ve skutečnosti potřebujeme, je fakt, že ireducibilní polynomy nemají vícenásobné kořeny (této vlastnosti se říká *separabilita*), což pro tělesa charakteristiky 0 plyne z Věty **??**: vícenásobné kořeny polynomu f by způsobily, že $\mathrm{NSD}(f, f') \neq 1$. Detaily přenecháme obsažnějším učebnicím.

Kapitolu začneme zkoumáním základních vlastností Galoisových grup, které nám umožní tyto grupy pro některé jednoduché polynomy spočítat. Zcela základním pozorováním je, že $\mathbf{T}$-automorfismy zachovávají kořeny všech polynomů, tj. obraz kořene polynomu f je opět kořenem f. Protože jde o automorfimy, toto zobrazení indukuje permutaci na množině všech kořenů daného polynomu.

Lemma 2.2. *Buď $\mathbf{T} \leq \mathbf{S}$ rozšíření těles, $f \in T[x]$ a A množina všech kořenů polynomu f v $\mathbf{S}$. Pak pro každé $\varphi \in \mathrm{Gal}(\mathbf{S}/\mathbf{T})$ je $\varphi|_A$ permutací množiny A.*

Důkaz. Označme polynom $f = \sum a_i x^i \in T[x]$ a uvažujme jeho kořen $u \in S$. Pak $\varphi(u)$ je také kořenem f, protože

$$f(\varphi(u)) = \sum a_i \varphi(u)^i = \sum \varphi(a_i)\varphi(u)^i = \varphi\left(\sum a_i u^i\right) = \varphi(f(u)) = \varphi(0) = 0,$$

kde druhá rovnost využívá faktu, že $\varphi|_T$ je identita, a třetí rovnost plyne z faktu, že φ je homomorfismus. Tedy φ je zobrazení na množině A všech kořenů f v S. Z definice Galopisovy grupy je to prosté zobrazení, a protože je množina A konečná, je to permutace na A. □

Připomeňme fakt, že homomorfismus je jednoznačně určen svými hodnotami na generátorech. Speciálně, pokud $\mathbf{S} = \mathbf{T}(a_1, \dots, a_n)$, pak každý $\mathbf{T}$-homomorfismus $\varphi : \mathbf{S} \to \mathbf{S}$ je určen hodnotami $\varphi(a_1), \dots, \varphi(a_n)$: obecný prvek $u \in S$ lze zapsat jako $u = f(a_1, \dots, a_n)$ pro nějaký polynom $f \in T[x_1, \dots, x_n]$, tedy $u = \sum c_{i_1,\dots,i_n} a_1^{i_1} \dots a_n^{i_n}$ pro nějaké koeficienty $c_{i_1,\dots,i_n} \in T$, a tedy

$$\begin{aligned}\varphi(u) = \varphi(\sum c_{i_1,\dots,i_n} a_1^{i_1} \dots a_n^{i_n}) &= \sum \varphi(c_{i_1,\dots,i_n}) \varphi(a_1)^{i_1} \dots \varphi(a_n)^{i_n} \\ &= \sum c_{i_1,\dots,i_n} \varphi(a_1)^{i_1} \dots \varphi(a_n)^{i_n},\end{aligned}$$

využívajíce faktu, že φ je $\mathbf{T}$-homomorfismus. Na druhou stranu, ne každá sada hodnot na generátorech dává homorfismus: např. neexistuje $\mathbb{R}$-homomorfismus $\varphi : \mathbb{C} \to \mathbb{C}$ splňující $\varphi(i) = 2i$, protože $\varphi(i^2) = \varphi(-1) = -1$, avšak $\varphi(i)^2 = (2i)^2 = -4$.

Příklad. Spočteme prvky grupy $\mathbf{Gal}(\mathbb{C}/\mathbb{R})$. Každý $\mathbb{R}$-automorfismus φ tělesa $\mathbb{C}$ je určen hodnotou $\varphi(i)$. Přitom podle Lemmatu 2.2 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. Grupa $\mathbf{Gal}(\mathbb{C}/\mathbb{R})$ je tedy dvouprvková, izomorfní grupě $\mathbb{Z}_2$.

Příklady. Analogicky lze odvodit následující:

- $\mathbf{Gal}(\mathbb{Q}(\sqrt{2}) : \mathbb{Q}) \simeq \mathbb{Z}_2$, protože prvky této grupy musejí zachovávat kořeny polynomu $x^2 - 2$, netriviálním $\mathbb{Q}$-automorfismem je zobrazení $a + b\sqrt{2} \mapsto a - b\sqrt{2}$.
- $|\mathbf{Gal}(\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q})| = 1$, protože prvky této grupy musejí zachovávat kořeny polynomu $x^3 - 2$, avšak tento polynom má v $\mathbb{Q}(\sqrt[3]{2})$ jediný kořen $\sqrt[3]{2}$.

Výpočty Galoisových grup jsou obecně komplikované. Např. platí, ale není úplně snadné dokázat, že $|\mathbf{Gal}(\mathbb{R}/\mathbb{Q})| = 1$, zatímco $\mathbf{Gal}(\mathbb{C}/\mathbb{Q})$ je nekonečná. Galoisovy grupy mají zajímavější vlastnosti, pokud jde o rozkladové rozšíření. Následující tvrzení umožňují určit Galoisovy grupy rozkladových nadtěles některých jednodušších polynomů.

Tvrzení 2.3. *Buď $\mathbf{S}$ rozkladové nadtěleso polynomu $f \in T[x]$ nad tělesem $\mathbf{T}$. Pak*

(1) *$\mathbf{Gal}(\mathbf{S}/\mathbf{T})$ se vnořuje do symetrické grupy $\mathbf{S}_n$, kde n je počet různých kořenů polynomu f;*
(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 $A = \{a_1, \dots, a_n\}$ množinu kořenů polynomu f v tělese $\mathbf{S}$. Protože je $\mathbf{S}$ rozkladové pro f, platí $\mathbf{S} = \mathbf{T}(a_1, \dots, a_n)$. Uvažujme libovolné $\varphi \in \mathrm{Gal}(\mathbf{S}/\mathbf{T})$. Tvrzení 2.2 říká, že $\varphi|_A$ je permutace na A. Přitom φ je jednoznačně určené svými hodnotami na generátorech $a_1, \dots, a_n$, tedy φ je jednoznačně 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) Protože je f ireducibilní, Lemma 1.3 říká, že kořenová nadtělesa $\mathbf{T}(a), \mathbf{T}(b)$ jsou $\mathbf{T}$-izomorfní, přičemž $\mathbf{T}$-izomorfismem je zobrazení definované předpisem $\varphi(h(a)) = h(b)$ pro každé $h \in T[x]$. Speciálně (pro $h = x$) vidíme, že $\varphi(a) = b$. Nyní stačí použít Lemma 1.4 pro $\mathbf{S}_1 = \mathbf{S}_2 = \mathbf{S}$ a získáme $\psi \in \mathrm{Gal}(\mathbf{S}/\mathbf{T})$ takový, že $\psi|_{\mathbf{T}(a)} = \varphi$, tedy speciálně $\psi(a) = b$.

(3) Pro $\varphi \in \mathrm{Gal}(\mathbf{U}/\mathbf{T})$ definujeme zobrazení $\Phi(\varphi) = \varphi|_S$. Dokážeme, že jde 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 ihned 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 Tvrzení 2.2 zobrazení φ permutuje kořeny polynomu f, které generují těleso $\mathbf{S}$, a tedy $\varphi(S) = S$, čili zobrazení $\varphi|_S$ je $\mathbf{T}$-automorfismem tělesa $\mathbf{S}$. Restrikce na podmnožinu zřejmě 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 $\psi \in \mathrm{Gal}(\mathbf{S}/\mathbf{T})$, pak podle Lemmatu 1.4 existuje $\mathbf{T}$-automorfismus φ tělesa $\mathbf{U}$ takový, že $\varphi|_S = \psi$, tedy $\mathbf{Im}(\Phi) = \mathbf{Gal}(\mathbf{S}/\mathbf{T})$. □

Na dvou příkladech ilustrujeme použití Tvrzení 2.3 k výpočtu Galoisových grup.

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 $m_{\sqrt{2}+\sqrt{3},\mathbb{Q}} = x^4 - 10x^2 + 1$. 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 $\varphi \in \mathbf{Gal}(\mathbf{S}/\mathbb{Q})$ je určen hodnotou na tomto generátoru. Podle Lemmatu 2.2 se kořeny zobrazují na kořeny, tedy $|\mathbf{Gal}(\mathbf{S}/\mathbb{Q})| \leq 4$. Podle (2) je každá hodnota na generátoru přípustná, 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 2.2 na polynomy $x^2 - 2$ a $x^2 - 3$ dostaneme, že $\varphi(\sqrt{2}) = u\sqrt{2}$ 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 $\mathbf{Gal}(\mathbf{S}/\mathbb{Q}) \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$.

Příklad. Spočteme grupu

$$\mathbf{Gal}(\mathbf{S}/\mathbb{Q}), \text{ kde } \mathbf{S} = \mathbb{Q}(\sqrt[3]{2}, e^{2\pi i/3}).$$

Je snadné nahlédnout, že $\mathbf{S}$ je rozkladové nadtěleso polynomu $x^3 - 2$. Kolik má jeho Galoisova grupa prvků? Jednoduchá úvaha jako v předchozím příkladě nepomůže, protože těleso $\mathbf{S}$ je dáno dvěma generátory (podle Věty **??** lze toto těleso generovat jedním prvkem, ale ten nebude kořenem tohoto polynomu a navíc není jasné, jak jej najít). Uvažujme mezitěleso $\mathbb{Q}(e^{2\pi i/3})$. Jde o rozkladové nadtěleso polynomu $x^3 - 1 = (x - 1)(x^2 - x + 1)$. Z toho plyne

$$|\mathbf{Gal}(\mathbb{Q}(e^{2\pi i/3})/\mathbb{Q})| = 2,$$

protože automorfismy musí permutovat kořeny polynomu $x^2 - x + 1$. Dále se podíváme na prvky grupy $\mathbf{Gal}(\mathbf{S}/\mathbb{Q}(e^{2\pi i/3}))$. Pro takový $\mathbb{Q}(e^{2\pi i/3})$-automorfismus φ musí platit $\varphi(e^{2\pi i/3}) = e^{2\pi i/3}$ a dále $\varphi(\sqrt[3]{2})$ se musí zobrazit na nějaký kořen polynomu $x^3 - 2$, přičemž podle (2) je každá volba přípustná. Vidíme, že

$$|\mathbf{Gal}(\mathbf{S}/\mathbb{Q}(e^{2\pi i/3})| = 3.$$

Podle (3) platí

$$\mathbf{Gal}(\mathbf{S}/\mathbb{Q})/\mathbf{Gal}(\mathbf{S}/\mathbb{Q}(e^{2\pi i/3})) \simeq \mathbf{Gal}(\mathbb{Q}(e^{2\pi i/3})/\mathbb{Q}),$$

tedy $|\mathbf{Gal}(\mathbf{S}/\mathbb{Q})| = |\mathbf{Gal}(\mathbf{S}/\mathbb{Q}(e^{2\pi i/3}))| \cdot |\mathbf{Gal}(\mathbb{Q}(e^{2\pi i/3})/\mathbb{Q})| = 3 \cdot 2 = 6$ (velikost faktorgrupy je podíl velikosti grupy a velikosti příslušné normální podgrupy, viz Lagrangeova věta). Podle (1) se grupa $\mathbf{Gal}(\mathbf{S}/\mathbb{Q})$ vnořuje do grupy $\mathbf{S}_3$, tedy nemůže být izomorfní grupě $\mathbb{Z}_6$, tedy $\mathbf{Gal}(\mathbf{S}/\mathbb{Q}) \simeq \mathbf{S}_3$.

Stěžejním krokem k důkazu Galoisovy věty je následující vlastnost polynomů, jejichž kořeny definují n-té odmocniny. Grupa $\mathbf{G}$ se nazývá *metabelovská*, pokud existuje $\mathbf{N} \trianglelefteq \mathbf{G}$ taková, že obě grupy $\mathbf{N}$, $\mathbf{G}/\mathbf{N}$ jsou abelovské. Jde o speciální typ řešitelných grup, viz Sekce 2.2.

Tvrzení 2.4. *Buď $\mathbf{T}$ těleso charakteristiky 0.*

(1) *Buď $\mathbf{S}$ rozkladové nadtěleso polynomu $x^n - 1$ nad $\mathbf{T}$. Pak $\mathbf{Gal}(\mathbf{S}/\mathbf{T})$ je abelovská grupa.*
(2) *Buď $\mathbf{S}$ rozkladové nadtěleso polynomu $x^n - a$ nad $\mathbf{T}$, kde $a \in T$. Pak $\mathbf{Gal}(\mathbf{S}/\mathbf{T})$ je metabelovská grupa.*

Důkaz. (1) Dokážeme, že $\mathbf{Gal}(\mathbf{S}/\mathbf{T})$ je izomorfní nějaké podgrupě grupy $\mathbb{Z}_n^*$, tedy jde o abelovskou grupu. Vzhledem k charakteristice 0 můžeme předpokládat

$$\mathbb{Q} \leq \mathbf{T} \leq \mathbf{S} = \mathbf{T}(e^{2\pi i/n}) \leq \mathbb{C}.$$

Každý automorfismus $\varphi \in \mathrm{Gal}(\mathbf{S}/\mathbf{T})$ permutuje kořeny polynomu $x^n - 1$, tedy splňuje $\varphi(e^{2\pi i/n}) = e^{2k\pi i/n}$ pro nějaké $k \in \{0, \ldots, n-1\}$. Přitom nutně $\mathrm{NSD}(k, n) = 1$, protože φ permutuje také kořeny všech polynomů $x^m - 1$, tedy prvky, které mají v grupě $\mathbb{C}^*$ řád dělící m, se musí zobrazit na prvky řádu, který dělí m; čili prvky řádu přesně n se musí zobrazit na prvky řádu přesně n, což jsou právě čísla $e^{2k\pi i/n}$ kde $\mathrm{NSD}(k, n) = 1$. Vidíme, že zobrazení, 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 k.

(2) Označme b kořen polynomu $x^n - a$ v $\mathbf{S}$. Pak $be^{2k\pi i/n}$, $k = 0, \ldots, n-1$, jsou právě všechny kořeny polynomu $x^n - a$ v $\mathbf{S}$. Vidíme, že $\mathbf{S} = \mathbf{T}(b, e^{2\pi i/n})$, máme tedy řadu rozšíření

$$\mathbf{T} \leq \mathbf{T}(e^{2\pi i/n}) \leq \mathbf{S} = \mathbf{T}(b, e^{2\pi i/n}).$$

Prostřední těleso $\mathbf{T}(e^{2\pi i/n})$ je rozkladové pro polynom $x^n - 1$, můžeme tedy aplikovat Tvrzení 2.3(3), které říká, že

$$\mathbf{Gal}(\mathbf{S}/\mathbf{T}) \,/\, \mathbf{Gal}(\mathbf{S}/\mathbf{T}(e^{2\pi i/n})) \simeq \mathbf{Gal}(\mathbf{T}(e^{2\pi i/n})/\mathbf{T}).$$

Jak vypadá grupa $\mathbf{Gal}(\mathbf{S}/\mathbf{T}(e^{2\pi i/n}))$? Každý prvek φ je určen hodnotou na generátoru b. Ten se musí zobrazit na jeden z kořenů polynomu $x^n - a$, tedy $\varphi(b) = be^{2k\pi i/n}$ pro nějaké k. Vidíme, že skládání automorfismů odpovídá sčítání těchto koeficientů, tedy zobrazení $\mathbf{Gal}(\mathbf{S}/\mathbf{T}(e^{2\pi i/n})) \to \mathbb{Z}_n$, které automorfismu φ přiřadí toto

k, je prostým homomorfismem do cyklické grupy $\mathbb{Z}_n$. Dokázali jsme, že podgrupa $\mathbf{N} = \mathbf{Gal}(\mathbf{S}/\mathbf{T}(e^{2\pi i/n}))$ je cyklická, tudíž abelovská, a díky části (1) je faktorgrupa $\mathbf{Gal}(\mathbf{S}/\mathbf{T})/\mathbf{N}$ také abelovská. Takže grupa $\mathbf{Gal}(\mathbf{S}/\mathbf{T})$ je metabelovská. □

Poznamenejme, že důkaz tohoto tvrzení je jediné místo, kde potřebujeme předpoklad charakteristiky 0. Pro tělesa kladné charakteristiky toto tvrzení neplatí.

Na závěr uvedeme jednu důležitou vlastnost, která se dokazuje podobným trikem jako Tvrzení 2.3.

Tvrzení 2.5. *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 $\mathbf{S}$. Podobně jako v Tvrzení 2.3(2) rozšíříme $\mathbf{T}$-izomorfismus $\mathbf{T}(a) \simeq \mathbf{T}(b)$ na prvek $\varphi \in \mathrm{Gal}(\mathbf{U}/\mathbf{T})$ splňující $\varphi(a) = b$ (nemůžeme přímo použít bod (2), protože polynom fg není ireducibilní). Nyní si uvědomíme, že φ permutuje kořeny polynomu f, které generují těleso $\mathbf{S}$, a tedy $\varphi(S) \subseteq S$. Speciálně dostáváme, že $b = \varphi(a) \in S$. □

2.2. Řešitelnost grup.

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

Vidíme, že grupa je

- řešitelná stupně 1 právě tehdy, když je abelovská;
- řešitelná stupně 2 právě tehdy, když je metabelovská.

Příklady.

- Grupa $\mathbf{S}_3$ je řešitelná stupně 2, jak prokazuje řada podgrup $\{1\} \leq \mathbf{A}_3 \leq \mathbf{S}_3$. Vidíme, že obě faktorgrupy $\mathbf{A}_3/\{1\} = \mathbf{A}_3 \simeq \mathbb{Z}_3$ a $\mathbf{S}_3/\mathbf{A}_3 \simeq \mathbb{Z}_2$ jsou abelovské.
- Obecněji, dihedrální grupy $\mathbf{D}_{2n}$ jsou řešitelné stupně 2, jak prokazuje řada podgrup $\{1\} \leq \mathbf{N} \leq \mathbf{D}_{2n}$, kde $\mathbf{N}$ sestává ze všech otočení. Vidíme, že obě faktorgrupy $\mathbf{N}/\{1\} = \mathbf{N} \simeq \mathbb{Z}_n$ a $\mathbf{D}_{2n}/\mathbf{N} \simeq \mathbb{Z}_2$ jsou abelovské.
- Grupa $\mathbf{S}_4$ je řešitelná stupně 3, jak prokazuje řada podgrup $\{1\} \leq \mathbf{K} \leq \mathbf{A}_4 \leq \mathbf{S}_4$, kde $\mathbf{K} = \langle (1\ 2)(3\ 4), (1\ 3)(2\ 4) \rangle$ je Kleinova podgrupa. Vidíme, že $\mathbf{K} \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$, $|\mathbf{A}_3/\mathbf{K}| = 12/4 = 3$ a $\mathbf{S}_4/\mathbf{A}_4 \simeq \mathbb{Z}_2$, tedy všechny faktorgrupy jsou abelovské.

Příklad. Grupa $\mathbf{S}_5$ není řešitelná. Stačí dokázat, že jediná vlastní podgrupa této grupy je $\mathbf{A}_5$, tedy že jediná možná řada je $\{1\} \leq \mathbf{A}_5 \leq \mathbf{S}_5$, avšak $\mathbf{A}_5$ není abelovská. Důkaz lze provést rozborem případů podle typu permutací. Uvažujme normální podgrupu $\{1\} \neq \mathbf{N} \trianglelefteq \mathbf{S}_5$.

(1) Pokud $\mathbf{N}$ obsahuje transpozici, pak obsahuje všechny transpozice, protože $\mathbf{N}$ je uzavřená na konjugaci, a tedy $\mathbf{N} = \mathbf{S}_5$, neboť transpozice generují celou grupu $\mathbf{S}_5$.

(2) Pokud $\mathbf{N}$ obsahuje trojcyklus, pak obsahuje všechny trojcykly, a tedy $\mathbf{A}_5 \leq \mathbf{N}$, neboť trojcykly generují celou grupu $\mathbf{A}_5$. Z Lagrangeovy věty plyne, že $\mathbf{N} = \mathbf{A}_5$ nebo $\mathbf{N} = \mathbf{S}_5$.
(3) Pokud $\mathbf{N}$ obsahuje permutaci složenou ze dvou disjunktních transpozic, pak obsahuje všechny takové a složení $(1\ 2)(3\ 4) \circ (1\ 2)(3\ 5) = (3\ 5\ 4)$ převádí problém na bod (2).
(4) Pokud $\mathbf{N}$ obsahuje permutaci složenou z trojcyklu a dvojcyklu, pak obsahuje všechny takové a složení $((1\ 2\ 3)(4\ 5))^2 = (1\ 3\ 2)$ převádí problém na bod (2).
(5) Pokud $\mathbf{N}$ obsahuje čtyřcyklus, pak obsahuje všechny takové a složení $(1\ 2\ 3\ 4) \circ (1\ 2\ 4\ 3) = (1\ 3\ 2)$ převádí problém na bod (2).
(6) Pokud $\mathbf{N}$ obsahuje pěticyklus, pak obsahuje všechny takové a složení $(1\ 2\ 3\ 4\ 5) \circ (1\ 2\ 3\ 4\ 5) = (1\ 3)(2\ 4)$ převádí problém na bod (3).

Stěžejní vlastností řešitelných grup je následující charakterizace, která umožňuje problém řešitelnosti dané grupy převést na problém řešitelnosti dvou menších podgrup.

Lemma 2.6. *Buď $\mathbf{G}$ grupa. Pak $\mathbf{G}$ je řešitelná právě tehdy když existuje $\mathbf{N} \trianglelefteq \mathbf{G}$ taková, že obě grupy $\mathbf{N}$, $\mathbf{G}/\mathbf{N}$ jsou řešitelné.*

Důkaz. V TÉTO VERZI NEBUDE, viz libovolná učebnice teorie grup □

Příklad. Grupy $\mathbf{S}_n$, $n \geq 5$, nejsou řešitelné, protože obsahují podgrupu $\mathbf{S}_5$, o které jsme již ukázali, že není řešitelná.

Důsledkem lemmatu je následující kritérium řešitelnosti, které zeslabuje podmínky na normální podgrupy z definice řešitelnosti.

Důsledek 2.7. *Buď $\mathbf{G}$ grupa a předpokládejme, že existuje číslo k a normální podgrupy $\mathbf{N}_0, \ldots, \mathbf{N}_k \trianglelefteq \mathbf{G}$ takové, že $\{1\} = \mathbf{N}_0 \leq \mathbf{N}_1 \leq \ldots \leq \mathbf{N}_k = \mathbf{G}$ a každá faktorgrupa $\mathbf{N}_i/\mathbf{N}_{i-1}$, $i = 1, \ldots, k$, je řešitelná. Pak $\mathbf{G}$ je řešitelná.*

Důkaz. Snadno indukcí podle k. □

2.3. Řešitelnost polynomů v radikálech.

Definice. Buď $\mathbf{T} \leq \mathbf{S}$ rozšíření těles a $a \in S$. Řekneme, že prvek a je *vyjádřitelný v radikálech* nad tělesem $\mathbf{T}$, pokud existují rozšíření $\mathbf{T} = \mathbf{S}_0 \leq \mathbf{S}_1 \leq \ldots \leq \mathbf{S}_k$ taková, že $\mathbf{S}_{i+1}$ je rozkladové nadtěleso nějakého polynomu $x^{n_i} - a_i \in S_i[x]$ nad tělesem $\mathbf{S}_i$, a $a \in S_k$.

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 $\mathbb{Q} \leq \mathbf{S}_1 \leq \mathbf{S}_2 \leq \mathbf{S}_3$, kde postupně použijeme polynomy $x^3 - 2 \in \mathbb{Q}[x]$, $x^2 - (\sqrt[3]{2}+1) \in S_1[x]$ a $x^2 + 1 \in S_2[x]$.

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 rovnice $f = 0$ vyjádřitelný v radikálech nad $\mathbf{T}$. Jinými slovy, pokud existují rozšíření $\mathbf{T} = \mathbf{S}_0 \leq \mathbf{S}_1 \leq \ldots \leq \mathbf{S}_k$ taková, že $\mathbf{S}_{i+1}$ je rozkladové nadtěleso nějakého polynomu $x^{n_i} - a_i \in S_i[x]$ nad tělesem $\mathbf{S}_i$, a rozkladové nadtěleso polynomu f je obsaženo v $\mathbf{S}_k$.

Rozebereme si případ polynomů stupně 2 a 3. Pro kořeny kvadratického polynomu $x^2 + bx + c \in \mathbb{Q}[x]$ máme vzorec

$$\frac{-b \pm \sqrt{b^2 - 4c}}{2},$$

tedy kořeny leží v nadtělese $\mathbb{Q}(\sqrt{b^2 - 4c})$, které je rozkladovým nadtělesem polynomu $x^2 - (b^2 - 4c)$. Stačí tedy jediné rozšíření tělesa $\mathbb{Q}$. Pro kořen a kubického polynomu $x^3 + bx + c \in \mathbb{Q}[x]$ máme vzorec

$$a = \sqrt[3]{\frac{-c + \sqrt{D}}{2}} - \sqrt[3]{\frac{c + \sqrt{D}}{2}},$$

kde $D = c^2 + \frac{4}{27}b^3$, takže potřebujeme aspoň dvě rozšíření: nejprve o prvek $\sqrt{D}$, a pak o příslušnou třetí odmocninu. Formálně, $\mathbb{Q} \leq \mathbf{S}_1 \leq \mathbf{S}_2$, kde $\mathbf{S}_1$ je rozkladové nadtěleso polynomu $x^2 - D$ a $\mathbf{S}_2$ je rozkladové nadtěleso polynomu $x^3 - (-c + \sqrt{D})$. Není těžké dokázat, že těleso $\mathbf{S}_2$ obsahuje i druhý sčítanec ze vzorce, tedy $a \in S_2$, a že se daný polynom v $\mathbf{S}_2$ dokonce rozkladá. Podobně by bylo možné rozebrat i výpočet kořenů polynomů stupně 4.

Uvedená diskuse souvisí s řešitelností grup $\mathbf{S}_2, \mathbf{S}_3, \mathbf{S}_4$. Všimněte si, že $\mathbf{S}_2$ je abelovská dvouprvková a k řešení rovnice stačilo jedno rozšíření stupně 2. Grupa $\mathbf{S}_3$ je metabelovská, velikosti faktorgrup jsou postupně $3 = |\mathbf{A}_3/\{1\}|$ a $2 = |\mathbf{S}_3/\mathbf{A}_3|$, přitom k vyjádření kořene byla potřeba rozšíření stupně 2 a 3. Podobné pozorování lze učinit i pro stupeň 4. To není náhoda, nýbrž zákonitost, která plyne z pokročilejší Galoisovy teorie (tak daleko se nedostaneme). Naopak neexistence vzorce na řešení polynomů stupně 5 a více plyne z neřešitelnosti grup $\mathbf{S}_n$, $n \geq 5$, jak si nyní ukážeme.

V této chvíli máme k dispozici všechny pojmy potřebné k důkazu stěžejní implikace Galoisovy věty 2.1. Její důkaz je založen na Tvrzení 2.4. Definice vyjádřitelnosti v radikálech používá řetězec rozšíření $\mathbf{S}_0 \leq \mathbf{S}_1 \leq \ldots \leq \mathbf{S}_k$, kde každé $\mathbf{S}_{i+1}$ je rozkladovým nadtělesem nějakého polynomu typu $x^n - a$, kde a je prvkem $\mathbf{S}_i$. Tvrzení 2.4 říká, že Galoisova grupa takového rozšíření je řešitelná. Nabízí se použít vlastnost (3) z Tvrzení 2.3, dostat řadu normálních podgrup, jejíž faktorgrupy jsou řešitelné a použít kritérium řešitelnosti z Důsledku 2.7. Problém je v tom, že Tvrzení 2.3 lze použít pouze na tělesa, jež jsou rozkladová nad bázovým tělesem $\mathbf{T}$. Situaci lze řešit pomocí následujícího technického lemmatu.

Lemma 2.8. *Buď $\mathbf{T}$ těleso charakteristiky 0 a $\mathbf{T} \leq \mathbf{S} \leq \mathbf{U}$ rozšíření těles taková, že $\mathbf{S}$ je rozkladové naděleso 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 naděleso 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 použít Tvrzení 2.4.

Důkaz. Označme f polynom, pro který je těleso $\mathbf{S}$ rozkladové nad $\mathbf{T}$. 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 $\mathbf{V}$ 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 $m_{a,\mathbf{T}}$ v tělese $\mathbf{S}$. Tento polynom je ireducibilní, jeho kořen a leží v $\mathbf{S}$, tedy podle Tvrzení 2.5 jsou všechny prvky $a_1, \ldots, a_m$ v $\mathbf{S}$. Tedy $m_{a,\mathbf{T}} = (x-a_1)\cdots(x-a_m)$ a $g = (x^n-a_1)\cdots(x^n-a_m)$ v $\mathbf{S}[x]$. Označme

$$g_i = (x^n - a_1)\cdots(x^n - a_i) \in S[x]$$

a buď $\mathbf{U}_i$ rozkladovým nadtělesem polynomu g_i nad $\mathbf{S}$, pro každé $i = 0, \ldots, m$. Máme řadu rozšíření

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

všechna tělesa jsou rozkladová nad $\mathbf{S}$, tedy můžeme m-krát aplikovat Tvrzení 2.3(3) a dostáváme řadu normálních podgrup

$$\{id\} = \mathbf{N}_m \leq \mathbf{N}_{m-1} \leq \ldots \leq \mathbf{N}_1 \leq \mathbf{N}_0 = \mathbf{Gal}(\mathbf{V}/\mathbf{S}),$$

kde $\mathbf{N}_i = \mathbf{Gal}(\mathbf{V}/\mathbf{U}_i) \trianglelefteq \mathbf{Gal}(\mathbf{V}/\mathbf{S})$ pro všechna i. Navíc, opět díky Tvrzení 2.3(3),

$$\mathbf{N}_i/\mathbf{N}_{i-1} = \mathbf{Gal}(\mathbf{V}/\mathbf{U}_i) \,/\, \mathbf{Gal}(\mathbf{V}/\mathbf{U}_{i-1}) \simeq \mathbf{Gal}(\mathbf{U}_i/\mathbf{U}_{i-1}),$$

přičemž tyto faktorgrupy jsou řešitelné podle Tvrzení 2.4, protože $\mathbf{U}_i$ je rozkladovým nadtělesem polynomu $x^n - a_i$ nad tělesem $\mathbf{U}_{i-1}$. Důsledek 2.7 říká, že grupa $\mathbf{Gal}(\mathbf{V}/\mathbf{S})$ je řešitelná. □

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

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

Budeme stavět dvě řady rozšíření $\mathbf{T} = \mathbf{U}_0 \leq \mathbf{U}_1 \leq \ldots \leq \mathbf{U}_k$ a $\mathbf{T} = \mathbf{V}_0 \leq \mathbf{V}_1 \leq \ldots \leq \mathbf{V}_k$ splňující následující vlastnosti pro všechna $i = 1, \ldots, m$:

(1) $\mathbf{S}_i \leq \mathbf{U}_i \leq \mathbf{V}_i$,
(2) $\mathbf{V}_i$ je rozkladové nadtěleso nějakého polynomu nad $\mathbf{T}$,
(3) $\mathbf{Gal}(\mathbf{V}_i/\mathbf{V}_{i-1})$ je řešitelná grupa.

Definujme $\mathbf{U}_0 = \mathbf{V}_0 = \mathbf{S}_0 = \mathbf{T}$ a postupujme induktivně pro $i = 1, \ldots, m$. Buď $\mathbf{U}_i$ rozkladové nadtěleso polynomu $x^{n_i} - a_i$ nad tělesem $\mathbf{V}_{i-1}$. Nyní použijeme Lemma 2.8 na situaci $\mathbf{V}_{i-1} \leq \mathbf{U}_i$ a získáme rozšíření $\mathbf{U}_i \leq \mathbf{V}_i$ s vlastnostmi (2), (3). Vlastnost (1) je očividně splněna také.

Máme tedy řadu rozšíření $\mathbf{T} = \mathbf{V}_0 \leq \mathbf{V}_1 \leq \ldots \leq \mathbf{V}_k$, kde každé $\mathbf{V}_i$ je rozkladové nad $\mathbf{T}$, takže lze aplikovat Tvrzení 2.3(3) a získat řadu normálních podgrup

$$\{id\} = \mathbf{N}_m \leq \mathbf{N}_{m-1} \leq \ldots \leq \mathbf{N}_1 \leq \mathbf{N}_0 = \mathbf{Gal}(\mathbf{V}_k/\mathbf{T}),$$

kde $\mathbf{N}_i = \mathbf{Gal}(\mathbf{V}_k/\mathbf{V}_i) \trianglelefteq \mathbf{Gal}(\mathbf{V}_k/\mathbf{T})$ pro všechna i. Vlastnost (2) říká, že faktorgrupy

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

jsou řešitelné, a z Důsledku 2.7 vidíme, že grupa $\mathbf{Gal}(\mathbf{V}_k/\mathbf{T})$ je řešitelná.

Zbývá dokázat, že grupa $\mathbf{Gal}(\mathbf{W}/\mathbf{T})$ je také řešitelná. Z vlastnosti (1) plyne, že $\mathbf{T} \leq \mathbf{W} \leq \mathbf{V}_k$. Obě rozšíření jsou rozkladová nad $\mathbf{T}$, tedy opět můžeme použít Tvrzení 2.3(3) 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 Lemma 2.6, které říká, že faktorgrupa řešitelné grupy $\mathbf{Gal}(\mathbf{V}_k/\mathbf{T})$ je také řešitelná. □

K důkazu Abel-Ruffiniho věty zbývá najít polynomy, jejichž rozkladové nadtěleso nemá řešitelnou Galoisovu grupu. Takových polynomů je většina, přesto není úplně snadné nějaký příklad předvést. Asi nejjednodušší rodinu příkladů popisuje následující tvrzení.

Tvrzení 2.9. *Buď p prvočíslo a uvažujme ireducibilní polynom $f \in \mathbb{Q}[x]$ stupně p, který má $p-2$ reálných a 2 imaginární kořeny. Buď $\mathbf{S}$ rozkladové nadtěleso polynomu f nad $\mathbb{Q}$. Pak $\mathbf{Gal}(\mathbf{S}/\mathbb{Q}) \simeq \mathbf{S}_p$.*

Důkaz. Připomeňme, že grupa $\mathbf{Gal}(\mathbf{S}/\mathbb{Q})$ se vnořuje do grupy $\mathbf{S}_p$, přičemž její prvky jsou dány permutací na kořenech polynomu f. Nejprve si uvědomme, že komplexní sdružení je $\mathbb{Q}$-automorfismem tělesa $\mathbf{S}$, tedy obraz $\mathbf{Gal}(\mathbf{S}/\mathbb{Q})$ obsahuje transpozici. Věta **??** říká, že $|\mathbf{Gal}(\mathbf{S}/\mathbb{Q})| = [\mathbf{S} : \mathbb{Q}]$. Přitom $[\mathbf{S} : \mathbb{Q}]$ je dělitelné číslem p, tedy podle Cauchyho věty **??** obsahuje grupa $\mathbf{Gal}(\mathbf{S}/\mathbb{Q})$ prvek řádu p, tedy její obraz obsahuje p-cyklus. Nyní si stačí uvědomit, že libovolný p-cyklus a transpozice generuje celou grupu $\mathbf{S}_p$. □

Příkladem polynomu, který splňuje předchozí tvrzení, je třeba $f = x^5 - 4x + 2$. Tento polynom je ireducibilní podle Eisensteinova kritéria, počet reálných kořenů snadno zjistíme pomocí kalkulu: $f' = 5x^4 - 4$, tato rovnice má dvě reálná řešení, tedy příslušná reálná funkce f má jedno maximum a jedno minimum, přičemž snadno dopočítáme, že maximum je kladné a minimum záporné. Protože polynomiální funkce jsou spojité, musí existovat právě tři reálné kořeny. Galoisova grupa rozkladového nadtělesa polynomu f je tedy izomorfní grupě $\mathbf{S}_5$, která není řešitelná.

Důsledek 2.10 (Abel-Ruffiniho věta, silnější verze)**.** *Existují racionální polynomy stupně 5 a více, které nejsou řešitelné v radikálech nad tělesem $\mathbb{Q}$.*