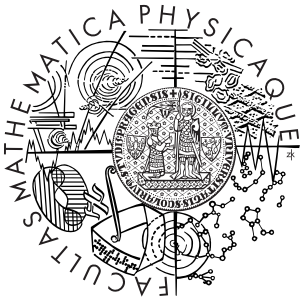
Univerzita Karlova v Praze
Matematicko-fyzikální fakulta

BAKALÁŘSKÁ PRÁCE



Kateřina Štíchová

Rozšíření těles a řešení algebraických rovnic

Katedra algebry Matematicko - fyzikální fakulty
Univerzity Karlovy v Praze

Vedoucí bakalářské práce: Mgr. Pavel Růžička, Ph.D
Studijní program: Matematika
Studijní obor: Matematické metody informační bezpečnosti

2008

Děkuji Mgr. Pavlu Růžičkovi, PhD., za vedení mé práce a za jeho cenné připomínky.

Prohlašuji, že jsem svou bakalářskou práci napsala samostatně a výhradně s použitím citovaných pramenů. Souhlasím se zapůjčováním práce a jejím zveřejňováním.

V Praze dne 23. 5. 2008 Kateřina Štíchová

Obsah

1 Úvod **5**

2 Teorie algebraických rovnic Cardanovy vzorce **8**
2.1 Rovnice druhého stupně 8
2.2 Rovnice třetího stupně 9
2.3 Rovnice čtvrtého stupně 14

3 Teorie těles **16**
3.1 Základní pojmy 16
3.2 Typy rozšíření těles a radikálová rozšíření 18

4 Grupy **20**
4.1 Teorie grup 20
4.2 Základní věta Galoisovy teorie 23

5 Aplikace Galoisovy teorie **35**
5.1 Řešitelnost polynomů v radikálech 35

Literatura **40**

Název práce: Rozšíření těles a řešení algebraických rovnic
Autor: Kateřina Štíchová
Katedra (ústav): Katedra algebry Matematicko-fyzikální fakulty v Praze
Vedoucí bakalářské práce: Mgr. Pavel Růžička, Ph.D, Katedra algebry
e-mail vedoucího: Pavel.Ruzicka@mff.cuni.cz

Abstrakt: V předložené práci se věnujeme řešení algebraických rovnic druhého až pátého stupně a Galoisově teorii. V první části je popsán způsob řešení algebraických rovnic, speciálně Cardanovy vzorce. Dále je uvedena teorie těles, která je stavebním prvkem pro následující kapitolu vlastní Galoisovy teorie, jež je jádrem této práce. Poslední kapitola se zabývá aplikací Galoisovy teorie, konkrétně neřešitelností rovnice pátého stupně v radikálech.

V Úvodu, pro Aplikace a příklady a jsme vycházeli hlavně ze zdroje [7]. Ve 2. kapitole jsme se inspirovali [3] a [6], v Teorii těles jsme použili [2]. Dále 4. kapitola byla napsána pomocí [1], [4] a [8] a pro obecné poznatky z algebry nám posloužil zdroj [5].

Klíčová slova: algebraická rovnice, rozšíření těles, Galoisova grupa, řešitelnost polynomů v radikálech

Title: Field extensions and solution of algebraic equations
Author: Katerina Stichova
Department: Department of Algebra
Supervisor: Mgr. Pavel Ruzicka, Ph.D
Supervisor's e-mail address: Pavel.Ruzicka@mff.cuni.cz

Abstract: In the present work we study solution of general algebraic equations of second to fifth degree and Galois theory. In the first chapter we describe possibilities of solution of algebraic equations, especially Cardano´s formulas. Next there is mentioned field theory, which is the basis of Galois theory, the main topic of this work. The last chapter describes one application of Galois theory, especially insolvability of algebraic equation of fifth degree in radicals.

In the Introduction, Applications and examples we borrowed from source [7]. We were mainly based on sources [3] and [6] in the second Chapter, in the Field theory we used [2]. The fourth Chapter was written with sources [1], [4] and [8] and for general knowledge of algebra we used [5].

Keywords: algebraic equation, field extension, Galois group, solvability of polynomials in radicals

Kapitola 1

Úvod

Až do poloviny 19. století bylo řešení algebraických rovnic základní otázkou klasické algebry.

Kořeny rovnice prvního a druhého stupně uměli nalézt již starověcí Egypťané. Ale až v 16. století se italským matematikům podařilo získat vzorce pro řešení rovnic třetího a čtvrtého stupně. Nejprve kolem roku 1500 *Scipione del Ferro* objevil řešení rovnic třetího stupně, které dále zobecnil *Nicolo z Brescii*, známý pod jménem *Tartaglia*. Zanedlouho poté vyřešil rovnici čtvrtého stupně *Ludovico Ferrari*. Vzorec pro řešení rovnice třetího stupně byl publikován *Gerolamem Cardanem*. I když byl Tartaglia v Cardanově práci *Artis magnae sive de regulis algebraicus liber unus* vydané v roce 1545 označen jako objevitel těchto vzorců, jsou tyto formule známy pod jménem Cardanovy vzorce.

Roku 1824 dokázal norský matematik *Abel (Niels Henrik)*, že rovnice vyššího než čtvrtého stupně, zapsané v obecném tvaru, tj. pomocí koeficientů, nemohou být řešeny v radikálech, tj. pomocí čtyř aritmetických operací - sčítání, odčítání, násobení a dělení - a pomocí odmocnin.

Jednou z nejzajímavějších partií matematiky, která se zabývá řešením algebraických rovnic, je Galoisova teorie. Její kořeny sahají až do starověkého Babylonu kolem r. 1600 před Kristem. Některé hliněné tabulky se zachovaly až do dnešních dob a díky nim se můžeme dovědět, jak široké spektrum výpočtů dokázali starověcí Babyloňané zvládnout - určením daní počínaje až po stanovení dráhy planety Jupiter. K tomuto historickému pohledu lze připočíst i klasické rébusy matematiky, které lze pomocí Galoisovy teorie řešit: kvadraturu kruhu, zdvojení krychle, trisekci úhlu, konstrukci pravidelného sedmnáctiúhelníku, neřešitelnost rovnice pátého stupně. Neobyčejnou různorodost této teorie pak dokreslují samotný život jejího tvůrce, zneuznaného génia a zavrženého vědce, Evarista Galoise.

Evariste Galois se narodil 25. října 1811 ve městě Bourg-la-Reine, nedaleko Paříže. Do dvanácti let se Evariste vzdělával v rodině, roku 1823 vstoupil na lyceum Ludvíka Velikého, které mu mělo poskytnout humanitní vzdělání. První dva roky Evariste v lyceu prospíval a obdržel první cenu v latině. Po sporu s učiteli byl však potrestán propadnutím. Tento nespravedlivý trest se stal pro Galoise velmi významným: útěkem z nudy se stává studium matematiky.

Legendrovy *Základy geometrie*, klasická, mnohokrát vydaná učebnice, je prvním matematickým textem, s kterým se Galois setká. Následují práce Josepha Louise Lagrangea o matematické analýze. Ve věku patnácti let čte materiály určené pouze profesionálním matematikům a s překvapivou lehkostí je zvládá. Čte spisy Eulera, Gausse, Jacobiho. A je pevně rozhodnut vstoupit do centra matematiky Francie té doby - na Polytechnickou školu.

Galois však doplácí na neuspořádaný a nesystematický způsob svého studia, na který ho upozorňovali jeho učitelé. Bez adekvátní přípravy předstupuje před examinátora a propadá.

Roku 1828 se Galois zapisuje do speciálního matematického kurzu. Jeho učitel Richard byl prvním, kdo rozpoznal jeho schopnosti a velmi s ním soucítil. Byl toho názoru, že člověk jeho kvalit by měl být přijat na Polytechniku bez přijímacího řízení. Následující rok mu Richard pomohl publikovat jeho první práci *Důkaz jedné věty o periodických spojitých zlomcích*, která však upadla v zapomnění. Své fundamentální poznatky o řešitelnosti algebraických rovnic formuloval v materiálu, který ve formě rukopisu poslal francouzské Akademii věd. Arbitrem byl Augustin Louise Cauchy, který už publikoval práci o chování funkcí při permutaci proměnných, což je hlavní téma Galoisovy teorie. Další osud rukopisu, obsahujícího nejgeniálnější matematické ideje století, je opředen tajemstvím, faktem však zůstává, že rukopis nebyl v původní ani opravené verzi na půdě Akademie prezentován.

Roku 1829 se Galois opět účastnil přijímacího řízení na Polytechniku - byla to jeho poslední šance. Traduje se (Bell, 1965; Dupuy, 1896), že ztratil nervy a hodil hadr na mazání tabule po zkoušejících, ale podle Bertranda (1899) je tento příběh fabulace. Jisté je, že Evariste u přijímacího řízení opět neuspěl. Galois tedy vstupuje na Echole Normale, která není tak prestižní jako Polytechnika. Za veřejnou kritiku vedení školy je posléze ze školy vyloučen. Má zakázáno nejen navštěvovat přednášky, ale je také zbaven prostředků k životu. V lednu 1831 se pokouší otevřít kurz pokročilé algebry, sestávající z nových teorií, které nebyly dosud publikovány. 17.1.1831 předkládá třetí verzi své

práce *Podmínky řešitelnosti rovnic pomocí radikálů*. Galois se nedočkal na tuto svoji práci ani po opakovaném dotazu žádného ohlasu. Až 4. července se dozvídá, jaký osud měla jeho práce předložená Akademii. Posudek nezněl pozitivně, Akademie nerozuměla a zavrhla jeho práci: "Vynaložili jsme veškeré úsilí, abychom pochopili důkazy pana Galoise. Jeho tvrzení je nedostatečně jasné, nedostatečně rozvinuté, abychom posoudili, nakolik je přesné. Nejsme schopni dát jakýkoliv posudek o jeho práci."

14. července, v den dobytí Bastily, byl Galois za údajnou politickou provokaci uvězněn. Epidemie cholery způsobila, že byl roku 1832 přemístěn do nemocnice a pak podmínečně propuštěn. V tomto čase své svobody také prožil první (a zároveň i poslední) milostnou zkušenost se slečnou Stephanií du Motel. Nedlouho poté byl Galois vyzván na souboj. 29. května, v předvečer souboje, píše Galois dopis svému příteli Augustu Chevalierovi, v kterém načrtává své matematické objevy. Zde nastiňuje vztah mezi grupami a polynomiálními rovnicemi, konstatuje, že rovnice je řešitelná pomocí radikálů, pokud její grupa je řešitelná. Ale zmiňuje i mnoho dalších myšlenek o eliptických funkcích a jiné své matematické ideje.

Evariste Galois zemřel 31. května 1832. Jeho dopis Chevalierovi končil těmito slovy: "Požádej Jacobiho nebo Gausse, aby sdělili svůj názor (na moje práce), ne kvůli pravdě, ale kvůli důležitosti těchto teorémů. Doufám, že v budoucnu se najdou lidé, kteří získají užitek z rozluštění tohoto chaosu…".

Čeho Galois dosáhl? Ve svých pracech Galois dokázal, jak určit, zda lze rovnice řešit v radikálech, nebo ne. Jeho objevy představovaly významný okamžik v pětitisícileté historii klasické algebry, pro kterou bylo hlavním cílem hledání řešení rovnic. Hlavním pojmem teorie Galoise byl pojem grupy. Jeho práce byly natolik složité, že vynikající francouzští matematikové zkoumali následujících 25 let jeho práce a přiznávali, že ničemu nerozuměli. Význam prací Galoise, které se vztahují k algebře a představují šedesát stran, je ohromný. Ale ideje a metody Galoise mají podstatný vliv na rozvoj nejen algebry, ale celé matematiky.

Kapitola 2

Teorie algebraických rovnic Cardanovy vzorce

V této kapitole se budeme věnovat výpočtu kořenů algebraických rovnic druhého až čtvrtého stupně.

2.1 Rovnice druhého stupně

Hledáme kořeny kvadratického polynomu

$$f(x) = x^2 + bx + c. \tag{2.1}$$

Použitím substituce

$$x = y - \frac{1}{2}b \tag{2.2}$$

přepíšeme $f(x)$ v proměnné x na polynom $g(y)$ v proměnné y, ve kterém se nevyskytuje term s y, jako

$$g(y) = y^2 + c - \frac{1}{4}b^2. \tag{2.3}$$

Platí, že číslo α je kořen polynomu $g(y)$ právě tehdy, když $\left(\alpha - \frac{1}{2}b\right)$ je kořen polynomu $f(x)$. Vidíme, že kořeny polynomu $g(y)$ jsou

$$\pm\frac{1}{2}\sqrt{b^2 - 4ac}, \tag{2.4}$$

a z toho plyne, že kořeny $f(x)$ jsou

$$\frac{1}{2}\left(-b \pm \sqrt{b^2 - 4ac}\right). \tag{2.5}$$

Číslo $D = b^2 - 4ac$ se nazývá *diskriminant*. Platí-li, že $D > 0$, pak má kvadratická rovnice *dva reálné kořeny*. Pokud máme $D < 0$, má kvadratická rovnice *dva komplexní kořeny*. V případě, že $D = 0$, máme *jeden dvojnásobný reálný kořen*

$$y_{1,2} = -\frac{1}{2}b. \tag{2.6}$$

Abychom získali kořeny původní rovnice (2.1), již nám stačí dosadit za y do substituce (2.2).

2.2 Rovnice třetího stupně

Nyní budeme řešit polynom třetího stupně, tedy rovnici

$$f(x) = x^3 + ax^2 + bx + c = 0. \tag{2.7}$$

Substitucí

$$x = y - \frac{1}{3}a \tag{2.8}$$

převedeme polynom z (2.7) na tvar

$$g(y) = y^3 + qy + r, \tag{2.9}$$

kde q, r jsou polynomy v a, b, c. Po dosazení získáme

$$g(y) = \left(y - \frac{1}{3}a\right)^3 + a\left(y - \frac{1}{3}a\right)^2 + b\left(y - \frac{1}{3}a\right) + c, \tag{2.10}$$

odkud úpravou dostaneme

$$g(y) = y^3 + \left(b - \frac{1}{3}a^2\right)y + \left(\frac{2}{27}a^3 - \frac{1}{3}a + c\right), \tag{2.11}$$

a tedy platí

$$q = b - \frac{1}{3}a^2 \tag{2.12}$$

$$r = \frac{2}{27}a^3 - \frac{1}{3}a + c. \tag{2.13}$$

Podobně jako v případě rovnice druhého stupně je α kořen $g(y)$ právě tehdy, když $\left(\alpha - \frac{1}{3}a\right)$ je kořen $f(x)$.

Hlavní trik spočívá ve vyjádření kořenu α polynomu $g(y)$ jako součtu β a γ, tj.

$$\alpha = \beta + \gamma, \tag{2.14}$$

kde β, γ jsou čísla splňující podmínku

$$\beta\gamma = -\frac{q}{3}, \tag{2.15}$$

jejíž význam bude zřejmý z následujících výpočtů. Po umocnění na třetí plyne z (2.14), že

$$\alpha^3 = (\beta + \gamma)^3 = \beta^3 + \gamma^3 + 3\beta\gamma(\beta + \gamma) = \beta^3 + \gamma^3 + 3\alpha\beta\gamma. \tag{2.16}$$

Dosazením α do polynomu $g(x)$ získáme

$$g(\alpha) = \alpha^3 + q\alpha + r = (\beta + \gamma)^3 + q(\beta + \gamma) + r = \beta^3 + \gamma^3 + (3\beta\gamma + q)\alpha + r, \tag{2.17}$$

odkud

$$g(\alpha) = \beta^3 + \gamma^3 + (3\beta\gamma + q)\alpha + r = 0, \tag{2.18}$$

protože α je kořen $g(y)$. Díky podmínce

$$\beta\gamma = -\frac{q}{3} \tag{2.19}$$

plyne z předchozí rovnosti, že

$$\beta^3 + \gamma^3 = -r \tag{2.20}$$

Umocněním obou stran rovnosti (2.19) na třetí dostaneme

$$\beta^3\gamma^3 = -\frac{q^3}{27}, \tag{2.21}$$

odkud

$$\gamma^3 = -\frac{q^3}{27\beta^3}. \tag{2.22}$$

Dosazením do (2.20) máme

$$\beta^3 - \frac{q^3}{27\beta^3} = -r, \tag{2.23}$$

odkud plyne, že

$$\beta^6 + r\beta^3 - \frac{q^3}{27} = 0. \tag{2.24}$$

Dostáváme tak kvadratickou rovnici v proměnné β^3, jejímž řešením získáme

$$\beta^3 = \frac{1}{2}\left(-r \pm \sqrt{r^2 + \frac{4q^3}{27}}\right) \tag{2.25}$$

a snadno již z (2.21)

$$\gamma^3 = \frac{1}{2}\left(-r \mp \sqrt{r^2 + \frac{4q^3}{27}}\right). \tag{2.26}$$

Číslo

$$r^2 + \frac{4q^3}{27} = \left(\frac{r}{2}\right)^2 + \left(\frac{q}{3}\right)^3 \tag{2.27}$$

nazýváme *diskriminant rovnice třetího stupně.*

Buď

$$\omega = e^{\frac{2\pi i}{3}} = cos\frac{2\pi}{3} + isin\frac{2\pi}{3} \tag{2.28}$$

primitivní třetí odmocnina z jedné. Je-li β nějaké řešení rovnice (2.25), dostaneme všechna řešení (2.25) postupným násobením β mocninami ω. Všechna řešení rovnice (2.25) jsou tedy β, $\omega\beta$, $\omega^2\beta$. Podobně vyhovuje-li γ rovnici (2.26), jsou γ, $\omega\gamma$, $\omega^2\gamma$ všechna řešení této rovnice. Splňují-li navíc β, γ podmínku (2.19), můžeme zbylá řešení spárovat tak, že

$$-\frac{q}{3} = \beta\gamma = (\omega\beta)(\omega^2\gamma) = (\omega^2\beta)(\omega\gamma). \tag{2.29}$$

Kořeny polynomu $g(y)$ nyní z (2.14) spočítáme jako

$$\alpha_1 = \beta + \gamma \tag{2.30}$$
$$\alpha_2 = \omega\beta + \omega^2\gamma \tag{2.31}$$
$$\alpha_3 = \omega^2\beta + \omega\gamma. \tag{2.32}$$

Nakonec dosadíme za y zpět do substituce (2.8) a získáme tak kořeny původní rovnice (2.7).

Nyní rozeznáváme dva případy podle typu kořenů: Je-li diskriminant rovnice (2.9)

$$D = \left(\frac{r}{2}\right)^2 + \left(\frac{q}{3}\right)^3 \geq 0, \tag{2.33}$$

β a γ jsou reálná čísla, proto se při výpočtu kořenu α jako součtu třetích odmocnin čísel β a γ pod těmito odmocninami vyskytne také reálné číslo. V tomto případě má rovnice (2.9) *jedno reálné a dvě komplexní řešení*, přičemž dvě komplexní řešení jsou čísla komplexně sdružená. Pokud naopak platí

$$D = \left(\frac{r}{2}\right)^2 + \left(\frac{q}{3}\right)^3 < 0, \tag{2.34}$$

nachází se pod druhou odmocninou ve vzorci (2.25) a (2.26) komplexní číslo, a tedy i β a $\gamma \in \mathbb{C}$, (β a γ jsou čísla komplexně sdružená), proto musíme počítat třetí odmocninu z komplexního čísla. Nyní má rovnice (2.9) *tři reálná řešení.* Tento druhý případ speciálně nazývá *casus irreducibilis.*

Nyní si v souvislosti s řešením rovnic uvedeme obecnou definici diskriminantu.

Definice 2.2.1 Buď $f \in T[x]$ polynom stupně n a buďte $\alpha_1, \alpha_2, \ldots \alpha_n$ jeho kořeny v rozkladovém tělese S. Označme

$$\delta = \prod_{i<j} (\alpha_i - \alpha_j). \tag{2.35}$$

Potom *diskriminant* $\Delta(f)$ *polynomu* f je

$$\Delta(f) = \delta^2. \tag{2.36}$$

Uvažujme polynom třetího stupně $f(x) = x^3 - ax^2 + bx - c \in T[x]$, pro nějž platí $a = 0$, a buďte $\alpha_1, \alpha_2, \alpha_3$ jeho kořeny v rozkladovém tělese S. Protože f je monický, platí

$$f(x) = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3), \tag{2.37}$$

z čehož po roznásobení plyne, že

$$\begin{aligned} a &= \alpha_1 + \alpha_2 + \alpha_3, & (2.38)\\ b &= \alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3, & (2.39)\\ c &= \alpha_1\alpha_2\alpha_3. & (2.40) \end{aligned}$$

Protože $a = 0$, z rovnosti (2.38) pro kořen α_3 platí vztah $\alpha_3 = -(\alpha_1 + \alpha_2)$, jehož dosazením do (2.39) a (2.40) dostaneme

$$\begin{aligned} b &= -(\alpha_1^2 + \alpha_1\alpha_2 + \alpha_2^2), & (2.41)\\ c &= -(\alpha_1^2\alpha_2 + \alpha_1\alpha_2^2). & (2.42) \end{aligned}$$

Pro diskriminant $\Delta(f)$ podle předchozí definice platí

$$\Delta(f) = [(\alpha_1 - \alpha_2)(\alpha_1 - \alpha_3)(\alpha_2 - \alpha_3)]^2 = (\alpha_1 - \alpha_2)^2(\alpha_1 - \alpha_3)^2(\alpha_2 - \alpha_3)^2. \tag{2.43}$$

Dále platí $(\alpha_1 - \alpha_2)^2 = \alpha_1^2 - 2\alpha_1\alpha_2 + \alpha_2^2$, a protože podle (2.41) máme $-b = \alpha_1^2 + \alpha_1\alpha_2 + \alpha_2^2$, platí, že

$$(\alpha_1 - \alpha_2)^2 = -b - 3\alpha_1\alpha_2. \tag{2.44}$$

Podobně po vyjádření $\alpha_2 = -\alpha_1 - \alpha_3$ z (2.38) pro $a = 0$ dostaneme rovnost

$$(\alpha_1 - \alpha_3)^2 = -b - 3\alpha_1\alpha_3, \tag{2.45}$$

a protože $\alpha_1 = -\alpha_2 - \alpha_3$, platí také

$$(\alpha_2 - \alpha_3)^2 = -b - 3\alpha_2\alpha_3. \tag{2.46}$$

Spojením podmínek (2.44), (2.45) a (2.46) z (2.43) dostáváme, že

$$\Delta(f) = -[(b + 3\alpha_1\alpha_2)(b + 3\alpha_1\alpha_3)(b + 3\alpha_2\alpha_3)], \tag{2.47}$$

což po roznásobení dává

$$(-b)^3 - Ab^2 - Bb - C, \tag{2.48}$$

kde

$$\begin{aligned} A &= 3(\alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3) = 3b, && (2.49)\\ B &= 9(\alpha_1\alpha_2\alpha_3)(\alpha_1 + \alpha_2 + \alpha_3) = 9ca = 0, && (2.50)\\ C &= 27(\alpha_1\alpha_2\alpha_3)^2 = 27c^2 && (2.51) \end{aligned}$$

podle (2.38), (2.39) a (2.40). Tedy

$$\Delta(f) = -4b^3 - 27c^2 = -(4b^3 + 27c^2). \tag{2.52}$$

Protože jsme v původní rovnici $f(x)$ uvažovali $a = 0$, odpovídá tato rovnice s koeficienty $1, 0, b, c$ rovnici (2.9). Cardanova definice diskriminantu (2.27) tedy odpovídá násobku výrazu $\Delta(f)$ zápornou konstantou.

Nyní se ještě podíváme na souvislost znaménka diskriminantu $\Delta(f)$ s tvarem kořenů. Uvažujme nejprve, že $f(x) = x^3 - ax^2 + bx - c \in T[x]$ má tři reálné kořeny α_1, α_2, $\alpha_3 \in \mathbb{R}$. Podle Definice 2.2.1 platí

$$\Delta(f) = (\alpha_1 - \alpha_2)^2(\alpha_1 - \alpha_3)^2(\alpha_2 - \alpha_3)^2, \tag{2.53}$$

z čehož je vidět, že výraz $\Delta(f)$ je součin tří druhých mocnin rozdílu reálných čísel, tedy jistě platí $\Delta(f) \geq 0$. Pokud má polynom f naopak jeden reálný kořen $\alpha_1 = \alpha$ a dva komplexně sdružené kořeny $\alpha_2 = \beta = \beta_1 + i\beta_2$, $\alpha_3 = \bar{\beta} = \beta_1 - i\beta_2$, kde β_1, $\beta_2 \in \mathbb{R}$ a $\beta_2 \neq 0$, potom

$$\Delta(f) = [(\alpha-\beta)(\alpha-\bar{\beta})(\beta-\bar{\beta})]^2 = [(\alpha-(\beta_1+i\beta_2))(\alpha-(\beta_1-i\beta_2))(\beta_1+i\beta_2-(\beta_1-i\beta_2))]^2, \tag{2.54}$$

což po úpravě dává

$$\Delta(f) = [(\alpha - \beta_1)^2 - i^2\beta_2^2]^2(2i\beta_2)^2 = [(\alpha - \beta_1)^2 + \beta_2^2]^2(4i^2\beta_2^2), \tag{2.55}$$

odkud je vidět, že zatímco první činitel je vždy kladný, druhý je vždy záporný, neboť obsahuje dvě kladná reálná čísla násobená $i^2 = -1$. Tedy v tomto případě platí $\Delta(f) < 0$.

2.3 Rovnice čtvrtého stupně

Je dán polynom čtvrtého stupně

$$f(x) = x^4 + ax^3 + bx^2 + cx + d. \tag{2.56}$$

Pomocí substituce

$$x = y - \frac{1}{4}a \tag{2.57}$$

získáme polynom $g(y)$, který neobsahuje term s y^3,

$$g(y) = y^4 + qy^2 + ry + s, \tag{2.58}$$

kde q, r, s jsou polynomy v a, b, c, d. Navíc stejně jako u předchozích případů rovnic nižších stupňů je α kořen $g(y)$ právě tehdy, když $(x - \frac{1}{4}\alpha)$ je kořen $f(x)$. Získáme

$$g(y) = y^4 + \left(b - \frac{3}{8}a^2\right)y^2 + \left(\frac{1}{8}a^3 - \frac{1}{2}ab + c\right)y + \left(-\frac{3}{256}a^4 + \frac{1}{16}a^2b - \frac{1}{4}ac + d\right), \tag{2.59}$$

tedy

$$q = b - \frac{3}{8}a^2 \tag{2.60}$$

$$r = \frac{1}{8}a^3 - \frac{1}{2}ab + c \tag{2.61}$$

$$s = -\frac{3}{256}a^4 + \frac{1}{16}a^2b - \frac{1}{4}ac + d. \tag{2.62}$$

Nyní $g(y)$ rozložíme na polynomy druhého stupně. Snadno nahlédneme, že koeficient u y ve druhém faktoru musí být $-k$, protože polynom $g(y)$ neobsahuje term s y^3.

$$y^4 + qy^2 + ry + s = (y^2 + ky + l)(y^2 - ky + m) \tag{2.63}$$

$$= y^4 + (-k^2 + l + m)y^2 + (km - kl)y + lm. \tag{2.64}$$

Pokud najdeme k, l a m, potom kořeny $g(y)$ mohou být nalezeny pomocí kvadratické rovnice. Porovnáním koeficientů q, r a s s vyjádřenými čísly k, l a m získáme podmínky pro k, l, m:

$$q = -k^2 + l + m \tag{2.65}$$

$$r = km - kl, \quad \left(m - l = \frac{r}{k}\right) \tag{2.66}$$

$$s = lm. \tag{2.67}$$

Sečtením prvních dvou rovnic získáme

$$2m = q + k^2 + \frac{r}{k}, \tag{2.68}$$

tedy

$$m = \frac{1}{2}\left(q + k^2 + \frac{r}{k}\right), \tag{2.69}$$

a dopočteme l,

$$l = \frac{1}{2}\left(q + k^2 - \frac{r}{k}\right). \tag{2.70}$$

Nyní, když máme l a m, snadno spočítáme

$$s = lm = \frac{1}{4}\left(q + k^2 + \frac{r}{k}\right)(q + k^2 - \frac{r}{k}). \tag{2.71}$$

Dále

$$4sk^2 = k^2q^2 + 2qk^4 + k^6 - r^2, \tag{2.72}$$

tedy získáme rovnici v proměnné k^2 tvaru

$$k^6 + 2qk^4 + (q^2 - 4s)k^2 - r^2 = 0, \tag{2.73}$$

která se použitím substituce

$$t = k^2 \tag{2.74}$$

převede na kubickou rovnici

$$t^3 + 2qt^2 + (q^2 - 4s)t - r^2 = 0 \tag{2.75}$$

v proměnné t. Nyní stačí výpočet kořenů této rovnice převést případ řešení rovnice třetího stupně.

Kapitola 3

Teorie těles

3.1 Základní pojmy

V této kapitole podáme přehled základních vlastností rozšíření těles, které budeme používat v dalším textu.

Definice 3.1.1 *Rozšíření těles* S/T je dvojice těles T, S taková, že T je podtěleso S. V tomto případě také říkáme, že S je rozšíření tělesa T.

Uvědomme si, že S lze chápat jako vektorový prostor nad tělesem T.

Definice 3.1.2 Dimenzi tohoto vektorového prostoru budeme nazývat *stupeň rozšíření* S *tělesa* T a značit $[S : T]$.

Definice 3.1.3 Prvek $\alpha \in S$ nazýváme *algebraický prvek nad* T, pokud je kořenem nějakého polynomu $p \in T[x]$. V opačném případě říkáme, že α je *transcendentní prvek nad* T.

Definice 3.1.4 Je-li $\alpha \in S$ algebraický prvek nad T, potom *minimální polynom prvku* α *nad* T je monický polynom $m_\alpha \in T[x]$ nejmenšího možného stupně, jehož je α kořenem. Prvek α je kořenem polynomu p právě tehdy, když je tento polynom dělitelný m_α.

Definice 3.1.5 Buď S/T rozšíření těles a $\alpha \in S$. Potom $T[\alpha]$ značí *nejmenší okruh tělesa* T *obsahující prvek* α. Podobně $T(\alpha)$ značí *nejmenší nadtěleso tělesa* T *obsahující prvek* α. Okruh $T[\alpha]$ je tělesem a tedy roven $T(\alpha)$, právě když je α algebraický prvek nad T.

Jsou-li prvky $\alpha_1, \ldots, \alpha_n \in S$, je $T[\alpha_1, \ldots, \alpha_n]$ *nejmenší okruh tělesa* T, *který obsahuje* $\alpha_1, \ldots, \alpha_n$, a podobně $T(\alpha_1, \ldots, \alpha_n)$ značí *nejmenší nadtěleso tělesa* T obsahující prvky $\alpha_1, \ldots, \alpha_n$. Říkáme, že těleso $T(\alpha_1, \ldots, \alpha_n)$ *je generované prvky* $\alpha_1, \ldots, \alpha_n$. Dále uvažujme polynom $p \in T[x]$ a $\alpha \in S$ jeho kořen. Těleso $T(\alpha)$ zadefinované výše

nazýváme *kořenové nadtěleso polynomu* p. Podobně $T(\alpha_1, \ldots, \alpha_n)$ se nazývá *rozkladové nadtěleso polynomu* p, kde $\alpha_1, \ldots, \alpha_n$ jsou kořeny p.

Poznámka 3.1.6 *Rozkladové těleso polynomu p je nejmenší nadtěleso, ve kterém se p rozkládá na součin lineárních faktorů.*

Dále si uvedeme souvislost teorie těles s ideály okruhů: Jednoduchý komutativní okruh je těleso a tedy faktor R/I komutativního okruhu R podle ideálu I je tělesem, právě když je ideál I maximální. Toto jednoduché pozorování má zásadní význam pro konstrukci kořenového nadtělesa ireducibilního polynomu.

Poznámka 3.1.7 *Uvažujme polynom $p \in T[x]$. Je-li p polynom stupně většího než 0, řekněme n, je $T[x]/p = \{q \in T[x],\ st\ q\ < st\ p\}$, tedy faktorové třídy $T[x]/p$ jsou jednoznačně reprezentovány polynomy stupně menšího než je stupeň polynomu p. Přitom množina $\{1, x, \ldots, x^{n-1}\}$ tvoří bázi vektorového prostoru $T[x]/p$ nad T. Tedy faktorový okruh $T[x]/p$ je vektorový prostor nad tělesem T dimenze $st\ p$, tedy $dim_T T[x]/p = st\ p$.*

Poznámka 3.1.8 *Uvažujme polynomy $p,\ \bar{p} \in T[x]$. Uvědomme si, že pro ideály $pT[x]$ a $\bar{p}T[x]$ platí $pT[x] \subseteq \bar{p}T[x]$ právě tehdy, když $\bar{p}|p$. V uspořádání inkluzí tedy maximálním ideálům odpovídají ireducibilní polynomy.*

Lemma 3.1.9 *Platí, že pokud je polynom $p \in T[x]$ ireducibilní, je $T[x]/p$ těleso.*

Důkaz. Podle Poznámky 3.1.8 se snadno nahlédne, že ideál $pT[x]$ je maximální, tedy $T[x]/p$ je těleso. □

Věta 3.1.10 (O jednoznačnosti jednoduchého algebraického rozšíření) *Buď T těleso, $p \in T[x]$ ireducibilní polynom nad T, S/T libovolné rozšíření tělesa T obsahující nějaký kořen α polynomu p. Potom je $T(\alpha)$ izomorfní s jednoduchým algebraickým rozšířením T určeným polynomem p, tj. s $T[x]/p$.*

Důkaz. Provádí se v základním kurzu algebry. □

Definice 3.1.11 Buď $p \in T[x]$ polynom. Označme $T[x]/p$ množinu všech polynomů stupně menšího než stupeň p s operací sčítání a násobení polynomů modulo p, tedy $T[x]/p = \{q \in T[x] \mid st\, q < st\, p\}$. Podle předchozí věty platí, že $T[x]/p \cong T(\alpha)$, kde α je nějaký kořen polynomu p. V tomto případě budeme $T(\alpha) = \{q(\alpha) \mid st\, q < st\, p\}$ *nazývat kořenové rozšíření tělesa T* určené kořenem α polynomu $p \in T[x]$.

Lemma 3.1.12 *Mějme rozšíření těles S/T. Prvek $\alpha \in S$ je algebraický nad T právě tehdy, když je stupeň rozšíření $[T(\alpha) : T]$ konečný a je roven stupni minimálního polynomu m_α nad T.*

Důkaz. Buď $[T(\alpha) : T] = n$. Vezměme posloupnost prvků $1, \alpha, \alpha^2, \ldots, \alpha^n$ tělesa $T(\alpha)$. Protože $dim_T T(\alpha) = n$, jsou prvky $1, \alpha, \alpha^2, \ldots, \alpha^n$ lineárně závislé. Existují proto ne vesměs nulové prvky $a_0, a_1, \ldots, a_n \in T$ tak, že $a_0 1 + a_1\alpha + \ldots + a_n\alpha^n = 0$. Z toho plyne, že α je kořen polynomu $f(x) = a_0 + a_1 x + \ldots + a_n x^n \in T[x]$, a proto je prvek α algebraický nad T.

Předpokládejme naopak, že α je algebraický prvek nad T. Potom $g(\alpha) = 0$ pro nějaký polynom $g(x) = b_0 + b_1 x + \ldots + b_n x^n \in T[x]$. Mezi všemi takovými polynomy vezmeme monický polynom minimálního stupně (minimální polynom prvku α). Nechť je to polynom $m_\alpha(x) = c_0 + c_1 x + \ldots + c_{n-1}x^{n-1} + x^n$. Libovolný polynom $g \in T[x]$, jehož kořenem je α, vydělíme polynomem m_α se zbytkem. Tedy $g = m_\alpha k + r$, kde buď $r = 0$ nebo $st\ r < st\ m_\alpha$. Po dosazení α dostaneme $0 = g(\alpha) = m_\alpha(\alpha)k(\alpha) + r(\alpha) = r(\alpha)$. Vzhledem k volbě m_α platí $r = 0$, tedy $m_\alpha | g$.

Chceme ukázat, že minimální polynom m_α je ireducibilní v $T[x]$. Kdyby platilo $m_\alpha(x) = a(x)b(x)$, kde $st\ a$, $st\ b < st\ m_\alpha$, dosazením α za x bychom dostali $0 = m_\alpha(\alpha) = a(\alpha)b(\alpha)$, tedy buď $a(\alpha) = 0$ nebo $b(\alpha) = 0$. V obou případech by to byl spor s volbou m_α.

Podle Věty 3.1.10 je $T(\alpha) \cong T[x]/m_\alpha \supseteq T$. Toto rozšíření tělesa T má podle Poznámky 3.1.7. stupeň n. □

Důsledek 3.1.13 *Pokud je polynom $p \in T[x]$ ireducibilní nad T, potom $[T[x]/p : T[x]] = st\ p$.*

Důkaz. Tvrzení plyne přímo z důkazu Lemma 3.1.12. □

Lemma 3.1.14 *Buď $\alpha \in S$ algebraický nad T. Potom je $T[\alpha]$ těleso.*

Důkaz. Stačí ukázat, že polynom m_α je ireducibilní, což jsme provedli v důkazu Lemma 3.1.12. □

3.2 Typy rozšíření těles a radikálová rozšíření

V dalším textu se omezíme na tělesa charakteristiky 0.

Definice 3.2.1 Řekneme, že rozšíření těles S/T je *algebraické*, pokud je každý prvek tělesa S algebraický nad T. Těleso S nazveme *algebraicky uzavřené*, pokud neexistuje žádné algebraické rozšíření $\bar{S}/S$ takové, že $S \neq \bar{S}$.

Definice 3.2.2 Je-li rozšíření S/T algebraické a těleso S algebraicky uzavřené, pak S nazýváme *algebraický uzávěr tělesa T*.

Věta 3.2.3 *Každé těleso má algebraický uzávěr a ten je až na izomorfismus určen jednoznačně.*

Důkaz. Tvrzení se dokazuje na základním kursu algebry. □

Lemma 3.2.4 *Pokud je S algebraicky uzavřené těleso, pak se každý polynom z $S[x]$ rozkládá v $S[x]$ na součin lineárních faktorů.*

Důkaz. Tvrzení je snadné. □

Definice 3.2.5 Konečné rozšíření těles S/T nazýváme *normální* (nebo také *rozkladové*), pokud každý polynom $p \in T[x]$, který má kořen v S, se v S rozkládá na součin lineárních faktorů.

Definice 3.2.6 Rozšíření těles U/T nazveme *čistě radikálové*, pokud existují tělesa $K_0 = T \subseteq K_1 \subseteq \ldots \subseteq K_r = U$ tak, že pro každé $i = 1, \ldots, r-1$ existuje prvočíslo p_i a $\beta_i \in K_{i+1}$ splňující $K_{i+1} = K_i(\beta_i)$, kde $\gamma_i = \beta_i^{p_i} \in K_i$. Prvek β_i potom nazýváme *p_i-tý radikál nad K_i*.

Definice 3.2.7 Rozšíření těles S/T je *radikálové*, existuje-li čistě radikálové rozšíření U/T tak, že $T \subseteq S \subseteq U$.

Definice 3.2.8 Uvažujme $p \in T[x]$ polynom, jehož rozkladové těleso je S nad T. Potom řekneme, že *p je řešitelný pomocí radikálů*, pokud je S radikálové.

Poznámka 3.2.9 Polynom $p \in T[x]$ je pak řešitelný pomocí radikálů, pokud jeho rozkladové těleso leží v radikálovém rozšíření.

Kapitola 4

Grupy

4.1 Teorie grup

I zde si nejprve připomeneme několik základních pojmů z teorie grup, které využijeme později.

Definice 4.1.1 Podgrupu K grupy G se nazveme *normální*, pokud pro všechna $k \in K$ a všechna $g \in G$ platí

$$g^{-1}kg \in K. \tag{4.1}$$

Definice 4.1.2 Řekneme, že konečná grupa G je *řešitelná*, pokud existuje posloupnost podgrup

$$G = G_0 \supseteq G_1 \supseteq \ldots \supseteq G_t = \{1\}, \tag{4.2}$$

kde G_{i+1} je normální podgrupa grupy G_i pro všechna $i = 0, \ldots, t-1$, a faktorová grupa G_i/G_{i+1} je komutativní pro všechna $i = 0, \ldots, t-1$. Posloupnost (4.2) nazýváme *kompoziční řada grupy* G.

Definice 4.1.3 Grupa G se nazývá *jednoduchá*, pokud její jediné normální podgrupy jsou G a $\{1\}$.

Pro podgrupy G, H grupy K položme $GH = \{gh \mid g \in G,\ h \in H\}$. Obecně není součin GH uzavřen na násobení, je-li však alespoň jedna z grup G, H normální podgrupou K, je GH podgrupa K. V tomto případě platí:

Věta 4.1.4 (3. věta o izomorfismu grup)
Buď G grupa, H její podgrupa a N její normální podgrupa. Potom součin HN je nejmenší podgrupa G obsahující H i N a $H/(H \cap N) \cong HN/N$.

Důkaz. Důkaz této věty najdeme například v [8] na straně 10, Věta 1.51. □

Věta 4.1.5 *Každá podgrupa řešitelné grupy je řešitelná.*

Důkaz. Buď G řešitelná grupa s kompoziční řadou (4.2). Dále buď H podgrupa G a položme $H_i = H \cap G_i$. Podle Věty 4.1.4 je $G_iH_{i-1}/G_i \cong H_{i-1}/H_i$, kde G_iH_{i-1}/G_i je podgrupa komutativní grupy G_{i-1}/G_i. Odtud je vidět, že je faktorgrupa H_{i-1}/H_i komutativní a tedy $H = H_0 \supseteq H_1 \supseteq \ldots \supseteq H_t = \{1\}$ je kompoziční řada H. Proto je grupa H řešitelná. □

Věta 4.1.6 *Faktorová grupa řešitelné grupy je řešitelná.*

Důkaz. Buď G řešitelná grupa s kompoziční řadou (4.2) a buď $f : G \to H$ surjektivní homomorfismus. Položme $H_i = f(G_i)$. Snadno nahlédneme, že faktorgrupa H_{i-1}/H_i je obrazem G_{i-1}/G_i, a tedy grupy H_i tvoří kompoziční řadu grupy H a H je řešitelná. □

Definice 4.1.7 Buď G grupa. Říkáme, že prvky $a, b \in G$ jsou konjugované v G, pokud existuje $c \in G$ tak, že $a = c^{-1}bc$.

Nyní si pro potřeby důkazu následující věty uvedeme toto pomocné tvrzení:

Lemma 4.1.8 *Buď $n \geq 5$. Potom jsou cykly délky 3 v $\mathbb{A}_n$ konjugované.*

Důkaz. Buď H normální podgrupa grupy $\mathbb{A}_n$ a buď $\alpha = (ijk) \in H$. Uvažujme trojcykl $\beta = (\bar{i}\bar{j}\bar{k})$. Chceme ukázat, že $\beta \in H$. Protože v $\mathbb{S}_n$ jsou permutace stejného typu konjugované, existuje $\gamma \in \mathbb{S}_n$ tak, že

$$\alpha = \gamma^{-1}\beta\gamma. \tag{4.3}$$

Je-li $\gamma \in \mathbb{A}_n$, jsou α, β konjugované v $\mathbb{A}_n$. Předpokládejme naopak, že γ je lichá permutace. Protože $n \geq 5$, existují m, l různá od $\bar{i}, \bar{j}, \bar{k}$. Potom $\bar{\gamma} = \gamma.(ml)$ je sudá permutace a $\bar{\gamma}^{-1}\alpha\bar{\gamma} = (ml)\gamma^{-1}\alpha\gamma(ml) = \beta$. □

Věta 4.1.9 *Alternující grupa všech sudých permutací n-tého stupně $\mathbb{A}_n$ je jednoduchá pro $n \geq 5$.*

Důkaz. Nechť $n \geq 5$. Nejprve ukážeme, že cykly (ijk) délky 3 generují grupu $\mathbb{A}_n$. Protože cykly délky 3 (trojcykly) jsou sudými permutacemi, lze je rozložit na sudý počet transpozic. Každou sudou permutaci lze navíc napsat jako součin trojcyklů, protože

$$(ij).(ik) = (ijk), \tag{4.4}$$

obsahují-li transpozice stejný prvek, a

$$(ij).(kl) = (ijk).(ikl), \tag{4.5}$$

obsahují-li transpozice různé prvky.

Nyní ukážeme, že každá normální podgrupa H grupy $\mathbb{A}_n$ obsahuje nějaký trojcyklus. Buď H normální podgrupa $\mathbb{A}_n$. Pokud H obsahuje nějaký trojcyklus, pak vzhledem k tomu, že trojcykly jsou v $\mathbb{A}_n$ konjugované, obsahuje všechny trojcykly. Protože je možné rozložit každou sudou permutaci v součin trojcyklů, je $H = \mathbb{A}_n$.

V posledním kroku dokážeme, že každá normální podgrupa H, $H \neq (1)$, obsahuje alespoň jeden trojcyklus. V H zvolíme neidentickou permutaci α takovou, aby zobrazovala co nejvíce prvků na sebe. Ukážeme, že α musí být trojcyklus. Pokud α není trojcyklus, vypadá takto:

1. Rozklad α na cykly obsahuje alespoň jeden trojcyklus délky alespoň 3:

$$\alpha = (ijk...)... \tag{4.6}$$

Protože α je sudá permutace, nemůže být cyklem délky 4, a tedy přehazuje nejméně další dva prvky l, m, různé od i, j, k.

2. Rozklad α obsahuje alespoň dvě nezávislé transpozice:

$$\alpha = (ij)(kl)... \tag{4.7}$$

Protože uvažujeme $n \geq 5$, existuje symbol m, různý od i, j, k, l. Položme $\beta = (klm) \in \mathbb{A}_n$. Pak $\beta^{-1}\alpha\beta \in H$, tedy

$$\gamma = \beta^{-1}\alpha\beta\alpha^{-1} \in H. \tag{4.8}$$

Všimneme si, že γ není identická permutace, protože v prvním případě $\beta^{-1}\alpha\beta$ zobrazuje prvek j na l a ne na k, jak je zobrazen pomocí α. V druhém případě α zobrazuje l na k, zatímco permutace $\beta^{-1}\alpha\beta$ zobrazuje l na m.

Dále γ v prvním bodě na sebe zobrazuje všechny symboly, které na sebe zobrazuje α, protože všechny tyto symboly jsou různé od k, l, m. Ve druhém případě na sebe γ zobrazuje všechny symboly stejné jako permutace α, kromě symbolu m. V prvním případě na sebe γ zobrazuje navíc prvek i, ve druhém prvky i a j.

Tedy v obou případech na sebe permutace γ zobrazuje více prvků než α a zároveň γ není identická permutace. To je spor s volbou permutace α, z čehož plyne, že α musí být trojcyklus. □

V dalším využijeme to, že pro $n \geq 5$ není grupa $\mathbb{A}_n$ (a tedy ani $\mathbb{S}_n$) řešitelná, což je triviální důsledek Věty 4.1.9. Tento fakt plyne i z následujícího jednoduchého tvrzení: (viz [1], str. 71, Věta 4).

Tvrzení 4.1.10 *Buď N podgrupa symetrické grupy $\mathbb{S}_n$, $n \geq 5$. Označme M normální podgrupu N. Pokud N obsahuje každý trojcyklus a N/M je komutativní, potom M obsahuje každý trojcyklus.*

Důkaz. Buď $f : N \to N/M$ homomorfismus a buďte $x = (ijk)$, $y = (krs)$ dva trojcykly z N. Označme $\bar{x}$ obraz x v N/M pro všechna $x \in N$. Protože je grupa

N/M komutativní, je $f(x^{-1}y^{-1}xy) = \bar{x}^{-1}\bar{y}^{-1}\bar{x}\bar{y} = 1$ pro každé $x, y \in M$. Protože $x^{-1}y^{-1}xy = (kji).(srk).(ijk).(krs) = (kjs)$, pro libovolné k, j, s, máme $(kjs) \in M$. □

Důsledek 4.1.11 $\mathbb{A}_n$ není řešitelná pro $n \geq 5$.

Důkaz. Pokud by existovala posloupnost zaručující řešitelnost, protože $\mathbb{A}_n$ obsahuje každý trojcyklus, potom by každý trojcyklus obsahovala každá následující grupa v kompoziční řadě a posloupnost by nekončila jedničkou. □

Protože je podle Věty 4.1.5 podgrupa řešitelné grupy řešitelná, dostáváme z předcházejícího tvrzení:

Důsledek 4.1.12 $\mathbb{S}_n$ není řešitelná pro $n \geq 5$. □

4.2 Základní věta Galoisovy teorie

Definice 4.2.1 Buď T libovolné těleso. Množina všech automorfismů $\mathbb{A}ut(T)$ tělesa T tvoří zřejmě vzhledem k operaci skládání zobrazení grupu. Tato grupa se nazývá *grupa automorfismů tělesa* T. Je-li T podtěleso tělesa S, pak označme $\mathbb{A}ut_T(S)$ množinu všech automorfismů tělesa S, které jsou na T identické, tj. $\mathbb{A}ut_T(S) = \{\sigma : S \to S \,|\, \sigma(\alpha) = \alpha \text{ pro všechna } \alpha \in T\}$. Snadno nahlédneme, že $\mathbb{A}ut_T(S)$ je podgrupa $\mathbb{A}ut(S)$. Tuto podgrupu budeme nazývat *grupa T-automorfismů tělesa S.*

Poznámka 4.2.2 Je-li σ automorfismus tělesa S, který je identický na T, říkáme, že σ je T-automorfismus tělesa S. Naopak v tomto případě řekneme, že T je fixní těleso automorfismu σ.

Definice 4.2.3 Buď S/T rozšíření těles. Potom grupu $\mathbb{A}ut_T(S)$ definovanou výše nazýváme *Galoisova grupa rozšíření* S/T a značíme $Gal(S/T)$. Dále buď $p \in T[x]$ polynom bez vícenásobných kořenů a S jeho rozkladové těleso. Grupa $Gal(S/T)$ je potom *Galoisova grupa polynomu* p.

Protože každý T-automorfismus tělesa S je jednoznačně určen obrazy kořenů polynomu p a tyto kořeny se T-automorfismy vzájemně permutují, je možné se dívat na grupu $Gal(S/T)$ jako na podgrupu symetrické grupy $\mathbb{S}_n$, kde n je stupeň polynomu p.

Nyní si zformulujeme několik tvrzení, která později využijeme v důkazu hlavní věty.

Nechť S, $\hat{S}$ jsou dvě tělesa. Buď $\Sigma = \{\sigma_1, \sigma_2, \ldots, \sigma_n\}$ množina homomorfismů z S do $\hat{S}$. Každý prvek $s \in S$ takový, že $\sigma_1(s) = \sigma_2(s) = \ldots = \sigma_n(s)$, nazýváme *fixní bod tělesa S vzhledem k Σ*. Snadno nahlédneme, že množina fixních bodů S tvoří podtěleso tělesa S. Toto podtěleso nazýváme *fixní těleso množiny* Σ. Pro naše potřeby ho označíme $Fix(S, \Sigma)$, tedy $Fix(S, \Sigma) = \{s \in S \,|\, \sigma_1(s) = \sigma_2(s) = \ldots = \sigma_n(s)\}$.

Nyní si zde uvedeme ještě jednu definici, která, jak později ukážeme, odpovídá normálnímu rozšíření konečného stupně (viz Definice 3.2.5).

Definice 4.2.4 Rozšíření těles S/T nazýváme *Galoisovo*, pokud je T fixní těleso grupy $Gal(S/T)$, tedy grupy všech T-automorfismů tělesa S, a $[S : T]$ je konečný.

Definice 4.2.5 Buďte S, $\hat{S}$ dvě tělesa a buď $\Sigma = \{\sigma_1, \ldots, \sigma_n\}$ množina vzájemně různých homomorfismů z S do $\hat{S}$. Řekneme, že $\sigma_1, \ldots, \sigma_n$ jsou *lineárně závislé*, pokud existují prvky $\alpha_1, \ldots, \alpha_n \in \hat{S}$, alespoň jeden z nich nenulový, takové, že platí $\alpha_1\sigma_1(x) + \alpha_2\sigma_2(x) + \ldots + \alpha_n\sigma_n(x) = 0$ pro všechna $x \in S$. Řekneme, že $\sigma_1, \ldots, \sigma_n$ jsou *lineárně nezávislé*, pokud nejsou lineárně závislé.

Věta 4.2.6 *Buďte S, $\hat{S}$ dvě tělesa a buď $\Sigma = \{\sigma_1, \ldots, \sigma_n\}$ množina vzájemně různých homomorfismů z S do $\hat{S}$.* Potom *$\sigma_1, \ldots, \sigma_n$ jsou lineárně nezávislé.*

Důkaz. Toto tvrzení uvedeme bez důkazu. Ten najdeme např. v [1] na straně 34, Věta 12 a její Důsledek. □

Věta 4.2.7 *Nechť $\Sigma = \{\sigma_1, \sigma_2, \ldots, \sigma_n\}$ je množina n různých homomorfismů tělesa S do tělesa $\hat{S}$. Označme $T = Fix(S, \Sigma)$. Potom je $[S : T] \geq n$.*

Důkaz. Pro spor předpokládejme, že $[S : T] = r < n$. Buď $\beta_1, \beta_2, \ldots, \beta_r$ báze S jako vektorového prostoru nad T. Protože v soustavě

$$\begin{aligned}
&\sigma_1(\beta_1)x_1 + \sigma_2(\beta_1)x_2 + \ldots + \sigma_n(\beta_1)x_n = 0\\
&\sigma_1(\beta_2)x_1 + \sigma_2(\beta_2)x_2 + \ldots + \sigma_n(\beta_2)x_n = 0\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\
&\sigma_1(\beta_r)x_1 + \sigma_2(\beta_r)x_2 + \ldots + \sigma_n(\beta_r)x_n = 0
\end{aligned}$$

je více neznámých než rovnic, existuje netriviální řešení $\alpha_1, \alpha_2, \ldots, \alpha_n$. Pro každý prvek $x \in S$ můžeme najít $a_1, a_2, \ldots, a_r \in T$ tak, že $x = a_1\beta_1 + a_2\beta_2 + \ldots + a_r\beta_r$. První rovnici vynásobíme $\sigma_1(a_1)$, druhou $\sigma_1(a_2)$, atd. Protože $a_i \in T$ pro $i = 1, 2 \ldots, n$, máme $\sigma_1(a_i) = \sigma_j(a_i) = a_i$ a platí také $\sigma_j(a_i)\sigma_j(\beta_i) = \sigma_j(a_i\beta_i)$. Dostáváme

$$\begin{aligned}
&\sigma_1(a_1\beta_1)x_1 + \sigma_2(a_1\beta_1)x_2 + \ldots + \sigma_n(a_1\beta_1)x_n = 0\\
&\sigma_1(a_2\beta_2)x_1 + \sigma_2(a_2\beta_2)x_2 + \ldots + \sigma_n(a_2\beta_2)x_n = 0\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\
&\sigma_1(a_r\beta_r)x_1 + \sigma_2(a_r\beta_r)x_2 + \ldots + \sigma_n(a_r\beta_r)x_n = 0.
\end{aligned}$$

Sečtením těchto rovic a použitím $\sigma_i(a_1\beta_1) + \sigma_i(a_2\beta_2) + \ldots + \sigma_i(a_r\beta_r) = \sigma_i(a_1\beta_1 + a_2\beta_2 + \ldots + a_r\beta_r) = \sigma_i(x)$ dostaneme

$$\sigma_1(x)\alpha_1 + \sigma_2(x)\alpha_2 \ldots + \sigma_n(x)\alpha_n = 0. \tag{4.9}$$

Toto však znamená, že $\sigma_1, \sigma_2, \ldots, \sigma_n$ jsou lineárně závislé, což je ve sporu s Větou 4.2.6. □

Důsledek 4.2.8 *Buď $\Sigma = \{\sigma_1, \sigma_2, \ldots, \sigma_n\}$ množina různých automorfismů tělesa S a $T = Fix(S, \Sigma)$. Potom $[S : T] \geq n$.*

Důkaz. Plyne z předchozího tvrzení. □

Přestože Důsledek 4.2.8 nelze zobecnit, existuje případ, ve kterém se vždy vyskytuje rovnost. Tento případ nastane právě tehdy, když množina automorfismů Σ tělesa S tvoří *grupu*. Pro nás bude podstatná jedna z implikací předchozí ekvivalence, kterou si nyní ukážeme.

Věta 4.2.9 *Buď S těleso a $\Sigma = \{\sigma_1, \sigma_2, \ldots, \sigma_n\}$ grupa automorfismů tělesa S. Označme $T = Fix(S, \Sigma)$. Potom $[S : T] = n$.*

Důkaz. Pokud $\sigma_1, \sigma_2, \ldots, \sigma_n$ tvoří grupu, musí být mezi nimi identické zobrazení I. Bez újmy na obecnosti položme $\sigma_1 = I$. Fixní těleso $T = Fix(S, \Sigma)$ potom tvoří takové prvky $s \in S$, pro které platí $\sigma_i(s) = s$ pro všechna $i = 1, 2 \ldots n$. Podle Věty 4.2.7 platí, že $[S : T] \geq n$, a pro spor předpokládejme, že $[S : T] > n$. Existuje tedy $n + 1$ prvků $\alpha_1, \alpha_2, \ldots, \alpha_{n+1} \in S$, které jsou v T lineárně nezávislé. Protože v následující soustavě rovnic je počet neznámých větší než počet rovnic, existuje v S netriviální řešení soustavy

$$
\begin{aligned}
&x_1\sigma_1(\alpha_1) + x_2\sigma_1(\alpha_2) + \ldots + x_{n+1}\sigma_1(\alpha_{n+1}) = 0\\
&x_1\sigma_2(\alpha_1) + x_2\sigma_2(\alpha_2) + \ldots + x_{n+1}\sigma_2(\alpha_{n+1}) = 0\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\
&x_1\sigma_n(\alpha_1) + x_2\sigma_n(\alpha_2) + \ldots + x_{n+1}\sigma_n(\alpha_{n+1}) = 0.
\end{aligned}
$$

Řešení nemůže ležet v T, jinak by byly prvky $\alpha_1, \ldots, \alpha_{n+1}$ v první rovnici lineárně závislé, protože σ_1 je identita.

Mezi všemi netriviálními řešeními $x_1, x_2, \ldots, x_{n+1}$ soustavy vybereme jedno s největším počtem nulových prvků. Nechť je to řešení $a_1, a_2, \ldots, a_r, 0, 0, \ldots, 0$ při vhodném uspořádání neznámých, kde prvních r prvků je nenulových. Navíc platí $r \neq 1$, protože z $a_1\sigma_1(\alpha_1) = 0$ plyne $a_1 = 0$, neboť $\sigma_1(\alpha_1) = \alpha_1 \neq 0$. Můžeme předpokládat $a_r = 1$, neboť vynásobením daného řešení prvkem ${a_r}^{-1}$ získáme nové řešení, kde r-tý prvek je roven 1. Proto platí

$$a_1\sigma_i(\alpha_1) + a_2\sigma_i(\alpha_2) + \ldots + a_{r-1}\sigma_i(\alpha_{r-1}) + \sigma_i(\alpha_r) = 0 \tag{4.10}$$

pro všechna $i = 1, 2, \ldots, n$.

Protože $a_1, a_2, \ldots, a_{r-1}$ nemohou všechny patřit do T, mějme např. $a_1 \in S$, ale $a_1 \notin T = Fix(S, \Sigma)$. Proto existuje automorfismus σ_k takový, že $\sigma_k(a_1) \neq a_1$. Protože automorfismy $\sigma_1, \sigma_2, \ldots, \sigma_n$ tvoří grupu, $\sigma_k\sigma_1, \sigma_k\sigma_2, \ldots \sigma_k\sigma_n$ je permutace $\sigma_1, \sigma_2, \ldots, \sigma_n$.

Aplikací σ_k na soustavu rovnic (4.10) dostaneme

$$\sigma_k(a_1)\sigma_k\sigma_j(\alpha_1) + \sigma_k(a_2)\sigma_k\sigma_j(\alpha_2) + \ldots + \sigma_k(a_{r-1})\sigma_k\sigma_j(\alpha_{r-1}) + \sigma_k\sigma_j(\alpha_r) = 0 \tag{4.11}$$

pro $j = 1, 2, \ldots, n$, takže položením $\sigma_k\sigma_j = \sigma_i$ dostaneme

$$\sigma_k(a_1)\sigma_i(\alpha_1) + \sigma_k(a_2)\sigma_i(\alpha_2) + \ldots + \sigma_k(a_{r-1})\sigma_i(\alpha_{r-1}) + \sigma_i(\alpha_r) = 0 \tag{4.12}$$

a odečtením (4.12) od (4.10) máme

$$[a_1 - \sigma_k(a_1)]\sigma_i(\alpha_1) + \ldots + [a_{r-1} - \sigma_k(a_{r-1})]\sigma_i(\alpha_{r-1}) = 0, \tag{4.13}$$

což je netriviální řešení s méně než r nenulovými prvky, což je spor s volbou r v řešení soustavy z úvodu důkazu. □

Důsledek 4.2.10 *Buď S těleso a Σ podgrupa grupy automorfismů tělesa S. Potom $\Sigma = Gal(S/Fix(S,\Sigma))$.*

Důkaz. Položme $T = Fix(S,\Sigma)$. Určitě platí $\Sigma \subseteq Gal(S/T)$. Protože podle Věty 4.2.9 je $|\Sigma| = [S:T]$, platí rovnost. □

Důsledek 4.2.11 *Neexistují dvě různé konečné podgrupy Σ, Γ grupy $\mathbb{A}ut(S)$ takové, že $Fix(S,\Sigma) = T = Fix(S,\Gamma)$.*

Důkaz. Podle předchozího důsledku platí $\Sigma = Gal(S/T) = \Gamma$. □

Nechť je nyní $\sigma : T \to \hat{T}$ homomorfismus těles. Pro polynom $p(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1(x) + a_0$ z $T[x]$ označme $p^\sigma(x) = \sigma(a_n)x^n + \sigma(a_{n-1})x^{n-1} + \ldots + \sigma(a_1)x + \sigma(a_0)$ polynom z $\hat{T}[x]$.

Věta 4.2.12 *Buď $\sigma : T \to \hat{T}$ izomorfismus těles a $p \in T[x]$ ireducibilní polynom. Je-li α kořen p a $\hat{\alpha}$ kořen p^σ, potom existuje rozšíření $\hat{\sigma} : T(\alpha) \to \hat{T}(\hat{\alpha})$ izomorfismu σ takové, že $\sigma(\alpha) = \hat{\alpha}$.*

Důkaz. Najdeme např. v [1] na straně 30, Věta 8. □

Následující tvrzení plyne z jednoznačnosti algebraického uzávěru.

Věta 4.2.13 *Buď $\sigma : T \to \hat{T}$ izomorfismus a buď $p \in T[x]$ polynom korespondující s $\hat{p} \in \hat{T}[x]$ vzhledem k σ. Uvažujme S rozkladové těleso polynomu p a $\hat{S}$ rozkladové těleso polynomu $\hat{p}$. Potom izomorfismus σ může být rozšířen na izomorfismus rozkladových nadtěles $\hat{\sigma} : S \to \hat{S}$.*

Věta 4.2.14 *Buď $p \in T[x]$ polynom bez vícenásobných kořenů. Pokud je S rozkladové těleso polynomu p, potom je S Galoisovo rozšíření tělesa T, tj. T je fixní těleso grupy $Gal(S/T)$.*

Důkaz. Pokud všechny kořeny polynomu p leží v T, potom $S = T$ a pouze identický automorfismus fixuje T. V tomto případě věta platí.

Nechť platí, že p má v $S \setminus T$ k kořenů, kde $k > 1$, a předpokládejme, že pro každou dvojici těles S, T takovou, že p má v S méně než k kořenů, tvrzení platí.

Buď $p = p_1.p_2.\ldots.p_r$ rozklad polynomu p na ireducibilní faktory. Můžeme předpokládat, že jeden z těchto faktorů je stupně většího než 1, jinak by se p rozkládal v T. Buď tedy $s > 1$ stupeň p_1 a α_1 kořen tohoto faktoru. Protože p_1 je ireducibilní v T, platí $[T(\alpha_1) : T] = st\ p_1 = s$. Pokud dále uvažujeme $T(\alpha_1)$ jako nové "základní" těleso,

platí, že méně než k kořenů p leží v $S \setminus T(\alpha_1)$. Pokud $p \in T(\alpha_1)[x]$ a S je rozkladové těleso p nad $T(\alpha_1)$, potom podle indukčního předpokladu platí, že S je Galoisovo rozšíření $T(\alpha_1)$. Proto každý prvek z $S \setminus T(\alpha_1)$ je neidenticky zobrazován alespoň jedním automorfismem tělesa S, který fixuje $T(\alpha_1)$.

Protože p je bez vícenásobných kořenů, kořeny $\alpha_1, \alpha_2, \ldots, \alpha_s$ polynomu p_1 jsou různé prvky tělesa S. Podle Věty 4.2.12 existují izomorfismy $\sigma_i : T(\alpha_1) \to T(\alpha_i)$, $i = 1, 2 \ldots, s$, které jsou identické na T, a platí $\sigma_i(\alpha_1) = \alpha_i$. S je rozkladové těleso polynomu $p \in T(\alpha_1)$ a také rozkladové těleso $p \in T(\alpha_i)$. Proto izomorfismus σ_i, vzhledem ke kterému koresponduje polynom $p \in T(\alpha_1)$ s tím samým polynomem $p \in T(\alpha_i)$, může být podle Věty 4.2.13 rozšířen na izomorfismus $\hat{\sigma}_i : S \to S$, tedy na automorfismus tělesa S. Tedy $\hat{\sigma_1}$, $\hat{\sigma_2}, \ldots$ $\hat{\sigma_s}$ jsou T-automorfismy tělesa S, tj. $\hat{\sigma}_i \in Gal(S/T)$ pro všechna $i = 1, 2, \ldots, s$, a platí $\hat{\sigma_1}(\alpha_1) = \alpha_1, \hat{\sigma_2}(\alpha_1) = \alpha_2, \ldots, \hat{\sigma_s}(\alpha_1) = \alpha_s$.

Buď nyní θ prvek tělesa S splňující $\hat{\sigma_1}(\theta) = \hat{\sigma_2}(\theta) = \ldots = \hat{\sigma_s}(\theta) = \theta$. Musí platit, že $\theta \in T(\alpha_1)$, protože pokud by $\theta \in S \setminus T(\alpha_1)$, alespoň jeden automorfismus $\hat{\sigma}_i$ by prvek θ zobrazoval neidenticky. Proto je θ tvaru

$$\theta = a_0 + a_1\alpha_1 + a_2\alpha_1^2 + \ldots + a_{s-1}\alpha_1^{s-1}, \tag{4.14}$$

kde $a_i \in T$. Pokud aplikujeme $\hat{\sigma}_i$ na (4.14), z rovnosti $\hat{\sigma}_i(\theta) = \theta$ pro každé $i = 1, 2, \ldots, s$, dostáváme

$$\theta = a_0 + a_1\alpha_i + a_2\alpha_i^2 + \ldots + a_{s-1}\alpha_i^{s-1}. \tag{4.15}$$

Polynom

$$a_{s-1}x^{s-1} + a_{s-2}x^{s-2} + \ldots + a_1x + (a_0 - \theta) \tag{4.16}$$

má proto s různých kořenů $\alpha_1, \alpha_2, \ldots \alpha_s$, což je více než jeho stupeň. Proto všechny koeficienty musí být nulové, včetně $a_0 - \theta$. Platí tedy $\theta \in T$. □

Věta 4.2.15 Základní věta Galoisovy teorie

Buď $p \in T[x]$ polynom bez vícenásobných kořenů, S jeho rozkladové těleso a $Gal(S/T)$ Galoisova grupa polynomu p. Potom platí:

1. Každé mezitěleso M, $T \subseteq M \subseteq S$, je fixní těleso podgrupy $Gal(S/M)$ grupy $Gal(S/T)$ a různé podgrupy mají různá fixní tělesa. (Říkáme, že M koresponduje s $Gal(S/M)$.)

2. Pro každé mezitěleso M platí, že $[M : T] = i(Gal(S/M))$, kde $i(Gal(S/M))$ je index grupy $Gal(S/M)$ v grupě $Gal(S/T)$, a $[S : M] = |Gal(S/M)|$.

3. Mezitěleso M je Galoisovo rozšíření tělesa T právě tehdy, když podgrupa $Gal(S/M)$ je normální podgrupa grupy $Gal(S/T)$. V tomto případě platí, že grupa $Gal(M/T) \cong Gal(S/T)/Gal(S/M)$.

Důkaz. Protože $T \subseteq M$, je jistě $p \in M[x]$ a S je jeho rozkladové těleso. Proto je S podle Věty 4.2.14 Galoisovo rozšíření M, takže M je fixní těleso podgrupy $Gal(S/M)$ grupy $Gal(S/T)$, která se skládá z M-automorfismů tělesa S. Z Důsledku 4.2.11 potom plyne, že různé podgrupy grupy $Gal(S/T)$ mají různá fixní tělesa. Tím jsme ukázali 1.

Buď M nějaké mezitěleso. Protože M je fixní těleso podgrupy $Gal(S/M)$ grupy $Gal(S/T)$, z Věty 4.2.9 plyne, že $[S : M] = |Gal(S/M)|$. Dále podle Lagrangeovy věty platí, že $|Gal(S/T)| = |Gal(S/M)|.i(Gal(S/M))$, kde $i(Gal(S/M))$ je index podgrupy $Gal(S/M)$ v grupě $Gal(S/T)$, tedy počet rozkladových tříd $Gal(S/T)$ podle $Gal(S/M)$. Protože platí rovnost $[S : T] = |Gal(S/T)|$ a také $[S : T] = [S : M].[M : T]$, dostáváme, že $[M : T] = i(Gal(S/M))$, čímž jsme dokázali druhou část věty.

K důkazu poslední části věty použijeme následujících dvou tvrzení. Buď M mezitěleso, $T \subseteq M \subseteq S$.

Tvrzení 1: *Počet různých T-homomorfismů M do S je roven počtu rozkladových tříd $Gal(S/T)$ podle $Gal(S/M)$, tedy $i(Gal(S/M))$.*

Důkaz. Nejprve ověříme, že dva homomorfismy σ, $\tau \in Gal(S/T)$ se shodují na M, právě když patří do stejné rozkladové třídy podle $Gal(S/M)$. Jsou-li $\sigma\sigma_1$, $\sigma\sigma_2$ dva prvky rozkladové třídy $\sigma Gal(S/M) = \{\sigma\sigma_i \,|\, \sigma_i \in Gal(S/M)\}$, kde $\sigma \in Gal(S/T)$ a σ_1, $\sigma_2 \in Gal(S/M)$, pak pro všechna $m \in M$ platí $\sigma\sigma_1(m) = \sigma(m) = \sigma\sigma_2(m)$. Nyní ukážeme, že prvky různých rozkladových tříd podle $Gal(S/M)$ dávají různé T-homomorfismy M do S. Nechť naopak platí $\sigma(m) = \tau(m)$ pro všechna $m \in M$. Potom $\tau^{-1}\sigma(m) = m$, proto je $\tau^{-1}\sigma \in Gal(S/M)$ a tedy σ a τ jsou z téže rozkladové třídy podle $Gal(S/M)$. Protože lze každý T-homomorfismus M do tělesa S rozšířit na prvek $Gal(S/T)$, je počet různých T-homomorfismů M do S roven počtu rozkladových tříd $Gal(S/T)$ podle $Gal(S/M)$. □

Tvrzení 2: *Těleso M je Galoisovo rozšíření T právě tehdy, když je počet různých T-automorfismů tělesa M roven $[M : T]$.*

Důkaz. Pokud je M Galoisovo rozšíření T, počet různých automorfismů tělesa M identických na T je podle Vět 4.2.9 a 4.2.14 roven $[M : T]$. Buď naopak počet různých T-automorfismů tělesa M roven $[M : T] = k$. Označme jejich množinu $\Sigma = \{\sigma_1, \sigma_2, \ldots, \sigma_k\}$. Označíme-li dále $\hat{T}$ fixní těleso těchto automorfismů, tedy $\hat{T} = Fix(M, \Sigma) = \{m \in M \,|\, \sigma_1(m) = \sigma_2(m) = \ldots = \sigma_k(m) = m\}$, platí $T \subset \hat{T} \subset M$ a podle Věty 4.2.9 je $[M : \hat{T}] = |\Sigma| = [M : T]$. Dále z rovnosti $[M : T] = [M : \hat{T}].[\hat{T} : T]$ plyne, že $[\hat{T} : T] = 1$, čili $T = \hat{T}$. Proto je M Galoisovo rozšíření tělesa T. □

Těleso M je Galoisovo rozšíření T právě tehdy, když každý T-homomorfismus M do S je automorfismus tělesa M. Protože podle bodu 2. máme $i(Gal(S/M)) = [M : T]$, spojením obou předchozích tvrzení dostáváme, že takovýchto homomorfismů a T-automorfismů M je stejný počet. Snadno nahlédneme, že $Gal(S/\sigma(M))$ je právě grupa $\sigma Gal(S/M)\sigma^{-1}$ pro každé $\sigma \in Gal(S/T)$. Odtud je již zřejmé, že $\sigma(M) = M$ pro každé $\sigma \in Gal(S/T)$ právě tehdy, když $\sigma Gal(S/M)\sigma^{-1} = Gal(S/M)$ pro každé $\sigma \in Gal(S/T)$, což nastane právě tehdy, když je $Gal(S/M)$ normální podgrupou $Gal(S/T)$. Těleso M je tedy Galoisovo rozšíření T právě tehdy, když je grupa $Gal(S/M)$ normální podgrupa grupy $Gal(S/T)$.

Jak jsme ukázali, každý T-homomorfismus tělesa M odpovídá některé rozkladové třídě podle podgrupy $Gal(S/M)$. Pokud je M Galoisovo rozšíření tělesa T, tyto homomorfismy jsou automorfismy M, ale v tomto případě jsou rozkladové třídy prvky faktorové grupy $Gal(S/T)/Gal(S/M)$. Proto T-automorfismy tělesa M jednoznačně

odpovídají prvkům faktorgrupy $Gal(S/T)/Gal(S/M)$. Protože násobení v grupě $Gal(S/T)/Gal(S/M)$ je určeno skládáním zobrazení, je tímto vztahem určen izomorfismus mezi $Gal(S/T)/Gal(S/M)$ a grupou $Gal(M/T)$. Tímto je důkaz věty dokončen. □

Nyní si zde uvedeme větu ukazující souvislost diskriminantu a Galoisovy grupy polynomu, která doplňuje kapitolu 2.2. Připomeňme, že diskriminant polynomu p je podle Definice 2.2.1 výraz $\Delta(p) = \delta^2$, kde $\delta = \prod_{i<j}(\alpha_i - \alpha_j)$ a α_k jsou kořeny p v jeho rozkladovém tělese.

Dále poznamenejme, že prvek β nazýváme *perfektní čtverec v* T, pokud pro $\beta^2 \in T$ platí také $\beta \in T$.

Věta 4.2.16 *Buď $p \in T[x]$ polynom, S jeho rozkladové těleso a předpokládejme, že $\mathrm{char}\, T \neq 2$. Potom*

1. $\Delta(p) \in T$,

2. $\Delta(p) = 0$ právě tehdy, když p má vícenásobný kořen,

3. $\Delta(p)$ je perfektní čtverec v T, právě když Galoisova grupa $Gal(S/T) \subset \mathbb{A}_n$.

Důkaz. Buď $\sigma \in \mathbb{S}_n$ permutace na kořenech α_i polynomu p. Snadno se nahlédne, že pokud permutaci σ aplikujeme na δ, obrazem je δ, pokud je σ sudá permutace, a $-\delta$, pokud je σ lichá. Proto $\delta \in \hat{A}$, kde $\hat{A}$ je fixní těleso grupy $\mathbb{A}_n$. Dále platí, že $\delta^2 = \Delta(p)$ je fixován každou permutací z $\sigma \in \mathbb{S}_n$, tedy $\Delta(p) \in T$.

Druhá část věty plyne přímo z definice diskriminantu $\Delta(p)$.

Buď $Gal(S/T)$ Galoisova grupa polynomu p, která je podgrupou $\mathbb{S}_n$. Pokud je $\Delta(p) = \delta^2$ perfektní čtverec v T, potom $\delta \in T$, tedy $Gal(S/T)$ fixuje δ. Pro σ lichou permutaci máme $\sigma(\delta) = -\delta$, a protože $\mathrm{char}\, T \neq 2$, platí $\delta \neq -\delta$. Proto $Gal(S/T)$ obsahuje pouze sudé permutace, tedy $Gal(S/T) \subset \mathbb{A}_n$. Naopak, pokud $Gal(S/T) \subset \mathbb{A}_n$ a platí $\delta^2 \in T$, potom také $\delta \in \hat{G}$, kde $\hat{G} = T$ je fixní těleso $Gal(S/T)$. Proto je $\Delta(p)$ perfektní čtverec v T. □

Důsledek 4.2.17 *Buď $p(x) = x^3 - ax^2 + bx - c \in \mathbb{Q}[x]$ ireducibilní polynom nad $\mathbb{Q}$. Potom pro Galoisovu grupu tohoto polynomu $Gal(S/T)$ platí, že $Gal(S/T) = \mathbb{A}_3$, právě když je $\Delta(p)$ perfektní čtverec v $\mathbb{Q}$, a $Gal(S/T) = \mathbb{S}_3$ jinak.* □

V závěru kapitoly 2.2 jsme určili, že pokud má polynom p tři reálné kořeny, potom $\Delta(p) = \delta^2 \geq 0$. Tehdy jsme viděli, že $\Delta(p) = \delta^2 \in \mathbb{R}$, ale také $\delta \in \mathbb{R}$, tedy $\delta^2 = \Delta(p)$ je perfektní čtverec v $\mathbb{R}$. Pokud měl p naopak jeden reálný a dva komplexně sdružené kořeny, potom $\Delta(p) < 0$, a platilo $\Delta(p) = \delta^2 \in \mathbb{R}$, ale $\delta \notin \mathbb{R}$, tedy $\Delta(p)$ v tomto případě není perfektní čtverec v $\mathbb{R}$.

Tedy podle předchozího důsledku platí, že pokud má p tři reálné kořeny, potom $Gal(S/T) = \mathbb{A}_3$, zatímco pro jeden reálný a dva komplexní kořeny polynomu p platí $Gal(S/T) = \mathbb{S}_3$.

Na závěr této kapitoly si uvedeme jeden ilustrační příklad, kde určíme Galoisovu grupu daného polynomu a podíváme se, jak vypadají její normální podgrupy a fixní tělesa příslušná těmto podgrupám - tedy jak funguje Galoisova korespondence.

Buď $p(x) = x^4 - 2 \in \mathbb{Q}[x]$ polynom a buď S jeho rozkladové těleso takové, že $S \subseteq \mathbb{C}$. Nyní rozložíme $p(x)$ jako

$$p(x) = (x - \alpha)(x + \alpha)(x - i\alpha)(x + i\alpha), \tag{4.17}$$

kde $\alpha = \sqrt[4]{2}$ je kladné reálné číslo. Proto $S = \mathbb{Q}(\alpha, i)$.

Protože S je rokladové těleso polynomu p, rozšíření $S/\mathbb{Q}$ je podle Věty 4.2.14 Galoisovo. Dále pracujeme v $\mathbb{C}$, takže je toto rozšíření také separabilní, tedy polynom p nemá vícenásobné kořeny.

Nyní určíme stupeň $[S : \mathbb{Q}]$ tohoto rozšíření. Jistě platí

$$[S : \mathbb{Q}] = [S : \mathbb{Q}(\alpha)].[\mathbb{Q}(\alpha) : \mathbb{Q}]. \tag{4.18}$$

Minimální polynom prvku i nad nad $\mathbb{Q}(\alpha)$ je $x^2 + 1$ (je ireducibilní nad $\mathbb{R}$, protože i je kořenem tohoto polynomu, ale $i \notin \mathbb{R} \supseteq \mathbb{Q}(\alpha)$). Proto $[\mathbb{Q}(\alpha, i) : \mathbb{Q}(\alpha)] = 2$.

Dále je $\alpha = \sqrt[4]{2}$ kořen polynomu $p(x) = x^4 - 2$ nad $\mathbb{Q}$, který je podle Eisensteinova kritéria 5.1.12 ireducibilní. Proto je p minimální polynom prvku α nad $\mathbb{Q}$, a tedy $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$. Máme tedy $[S : \mathbb{Q}] = 8$.

V dalším kroku určíme prvky Galoisovy grupy $Gal(S/\mathbb{Q})$ rozšíření $S/\mathbb{Q}$. Protože $\mathbb{Q} \subseteq \mathbb{Q}(i) \subseteq S = \mathbb{Q}(\alpha, i)$, $p(x) = x^4 - 2$ je ireducibilní v $\mathbb{Q}(i)$ a kořeny polynomu p v S jsou α a $i\alpha$, existuje $\mathbb{Q}(i)$-automorfismus σ tělesa S takový, že

$$\sigma(i) = i \qquad \sigma(\alpha) = i\alpha. \tag{4.19}$$

Podobně platí $\mathbb{Q} \subseteq \mathbb{Q}(\alpha) \subseteq S$, polynom $x^2 + 1$ je ireducibilní v $\mathbb{Q}(\alpha)$ a kořeny tohoto polynomu v S jsou i a $-i$, proto existuje $\mathbb{Q}(\alpha)$-automorfismus τ tělesa S takový, že

$$\tau(\alpha) = \alpha \qquad \tau(i) = -i. \tag{4.20}$$

Protože $[S : \mathbb{Q}] = 8$, složením těchto automorfismů získáme osm různých $\mathbb{Q}$-automorfismů tělesa S, které vypadají následovně:

Automorfismus	**Obraz prvku** α	**Obraz prvku** i
1	α	i
σ	$i\alpha$	i
σ^2	$-\alpha$	i
σ^3	$-i\alpha$	i
τ	α	$-i$
$\sigma\tau$	$i\alpha$	$-i$
$\sigma^2\tau$	$-\alpha$	$-i$
$\sigma^3\tau$	$-i\alpha$	$-i$

Navíc platí $\sigma^4 = 1 = \tau^2$, $\tau\sigma = \sigma^3\tau$, $\tau\sigma^2 = \sigma^2\tau$ a $\tau\sigma^3 = \sigma\tau$, tedy kombinace uvedené v tabulce jsou právě všechny $\mathbb{Q}$-automorfismy tělesa S.

Vidíme, že libovolný $\mathbb{Q}$-automorfismus tělesa S zobrazuje prvek i na nějaký kořen polynomu $x^2 + 1$, tedy $i \to \pm i$; podobně je prvek α zobrazován na prvky α, $i\alpha$, $-\alpha$ nebo $-i\alpha$, tedy vždy na nějaký kořen polynomu $p(x) = x^4 - 2$.

Galoisova grupa $Gal(S/\mathbb{Q})$ tedy vypadá následovně:

$$Gal(S/\mathbb{Q}) = \{1, \sigma, \sigma^2, \sigma^3, \tau, \sigma\tau, \sigma^2\tau, \sigma^3\tau\} = \langle \sigma, \tau : \sigma^4 = \tau^2 = 1, \tau\sigma = \sigma^3\tau \rangle, \qquad (4.21)$$

což je dihedrální grupa $\mathbb{D}_8$, tedy grupa všech vzájemně jednoznačných zobrazení čtverce na sebe.

Nyní najdeme podgrupy grupy $Gal(S/\mathbb{Q})$. Označíme-li $\mathbb{Z}_n$ cyklickou grupu řádu n, podgrupy $Gal(S/\mathbb{Q})$ vypadají takto:

Řádu 8:	$Gal(S/\mathbb{Q})$	$Gal(S/\mathbb{Q}) \cong \mathbb{D}_8$
Řádu 4:	$U = \{1, \sigma, \sigma^2, \sigma^3\}$	$U \cong \mathbb{Z}_4$
	$V = \{1, \sigma^2, \tau, \sigma^2\tau\}$	$V \cong \mathbb{Z}_2 \times \mathbb{Z}_2$
	$W = \{1, \sigma^2, \sigma\tau, \sigma^3\tau\}$	$W \cong \mathbb{Z}_2 \times \mathbb{Z}_2$
Řádu 2:	$A = \{1, \sigma^2\}$	$A \cong \mathbb{Z}_2$
	$B = \{1, \tau\}$	$B \cong \mathbb{Z}_2$
	$C = \{1, \sigma\tau\}$	$C \cong \mathbb{Z}_2$
	$D = \{1, \sigma^2\tau\}$	$D \cong \mathbb{Z}_2$
	$E = \{1, \sigma^3\tau\}$	$E \cong \mathbb{Z}_2$
Řádu 1:	$I = \{1\}$	$I \cong 1$

Vzhledem ke Galoisově korespondenci získáme mezitělesa M_i, $\mathbb{Q} \subseteq M_i \subseteq S = \mathbb{Q}(\alpha, i)$, tedy fixní tělesa podgrup grupy $Gal(S/\mathbb{Q})$.

Nyní popíšeme prvky těchto mezitěles. Snadno určíme tři podtělesa tělesa S stupně 2 nad $\mathbb{Q}$, konkrétně $\hat{U} = \mathbb{Q}(i)$, $\hat{V} = \mathbb{Q}(\alpha^2) = \mathbb{Q}(\sqrt{2})$ a $\hat{W} = \mathbb{Q}(i\alpha^2) = \mathbb{Q}(i\sqrt{2})$. Tato tělesa jsou po řadě fixní tělesa příslušná grupám U, V a W. Nyní se podívejme na ostatní fixní tělesa. Nejprve popíšeme prvky $\hat{A}$. Libovolný prvek $x \in S = \mathbb{Q}(\alpha, i)$ může být jednoznačně napsán ve tvaru

$$x = a_0 + a_1\alpha + a_2\alpha^2 + a_3\alpha^3 + a_4 i + a_5 i\alpha + a_6 i\alpha^2 + a_7 i\alpha^3, \qquad (4.22)$$

kde $a_i \in \mathbb{Q}$. Protože $A = \{1, \sigma^2\}$, máme

$$\sigma^2(x) = a_0 - a_1\alpha + a_2\alpha^2 - a_3\alpha^3 + a_4 i - a_5 i\alpha + a_6 i\alpha^2 - a_7 i\alpha^3. \qquad (4.23)$$

Prvek x je fixován automorfismem σ^2 (a tedy celou grupou A) právě tehdy, když

$a_0 = a_0$, $a_1 = -a_1$, $a_2 = a_2$, $a_3 = -a_3$, $a_4 = a_4$, $a_5 = -a_5$, $a_6 = a_6$, $a_7 = -a_7$.

Tedy $\sigma^2(x) = x$ právě když prvky a_0, a_2, a_4 a a_6 jsou libovolné a $a_1 = a_3 = a_5 = a_7 = 0$. Máme tedy

$$x = a_0 + a_2\alpha^2 + a_4 i + a_6 i\alpha^2, \tag{4.24}$$

proto $\hat{A} = \mathbb{Q}(i, \alpha^2) = \mathbb{Q}(i, \sqrt{2})$.

Dále zkusme určit $\hat{B}$. Protože podle předchozího může být $x \in S$ napsán jako (4.22) a $B = \{1, \tau\}$, dostaneme

$$\tau(x) = a_0 + a_1\alpha + a_2\alpha^2 + a_3\alpha^3 - a_4 i - a_5 i\alpha - a_6 i\alpha^2 - a_7 i\alpha^3. \tag{4.25}$$

Platí $\tau(x) = x$, právě když

$a_0 = a_0$, $a_1 = a_1$, $a_2 = a_2$, $a_3 = a_3$, $a_4 = -a_4$, $a_5 = -a_5$, $a_6 = -a_6$, $a_7 = -a_7$.

Tedy prvky a_0, a_1, a_2 a a_3 jsou libovolné a $a_4 = a_5 = a_6 = a_7 = 0$. Proto

$$x = a_0 + a_1\alpha + a_2\alpha^2 + a_3\alpha^3 \tag{4.26}$$

a $\hat{B} = \mathbb{Q}(\alpha)$.

Pro těleso $\hat{C}$ máme $C = \{1, \sigma\tau\}$. Zde opět

$$x = a_0 + a_1\alpha + a_2\alpha^2 + a_3\alpha^3 + a_4 i + a_5 i\alpha + a_6 i\alpha^2 + a_7 i\alpha^3 \tag{4.27}$$

a

$$\sigma\tau(x) = a_0 + a_5\alpha - a_2\alpha^2 - a_7\alpha^3 - a_4 i + a_1 i\alpha + a_6 i\alpha^2 - a_3 i\alpha^3. \tag{4.28}$$

Vidíme tedy, že prvek x je fixován automorfismem $\sigma\tau$, právě když

$a_0 = a_0$, $a_1 = a_5$, $a_2 = -a_2$, $a_3 = -a_7$, $a_4 = -a_4$, $a_5 = a_1$, $a_6 = a_6$, $a_7 = -a_3$.

Tedy prvky a_0 a a_6 můžeme zvolit libovolně, zatímco $a_2 = 0 = a_4$, $a_5 = a_1$ a $a_7 = -a_3$. Tedy

$$x = a_0 + a_1(1+i)\alpha + a_6 i\alpha^2 + a_3(1-i)\alpha^3 = a_0 + a_1[(1+i)\alpha] + \frac{a_6}{2}[(1+i)\alpha]^2 - \frac{a_3}{2}[(1+i)\alpha]^3, \tag{4.29}$$

z čehož plyne, že $\hat{C} = \mathbb{Q}((1+i)\alpha)$.

Dále máme $D = \{1, \sigma^2\tau\}$, tedy

$$\sigma^2\tau(x) = a_0 - a_1\alpha + a_2\alpha^2 - a_3\alpha^3 - a_4 i + a_5 i\alpha - a_6 i\alpha^2 + a_7 i\alpha^3, \tag{4.30}$$

tedy a_0, a_2, a_5 a a_7 jsou libovolná a $a_1 = a_3 = a_4 = a_6 = 0$. Proto

$$x = a_0 + a_2\alpha^2 + a_5 i\alpha + a_7 i\alpha^3 \tag{4.31}$$

a $\hat{D} = \mathbb{Q}(i\alpha)$.

Konečně grupa $E = \{1, \sigma^3\tau\}$. Protože opět

$$x = a_0 + a_1\alpha + a_2\alpha^2 + a_3\alpha^3 + a_4 i + a_5 i\alpha + a_6 i\alpha^2 + a_7 i\alpha^3 \tag{4.32}$$

a tedy

$$\sigma^3\tau(x) = a_0 - a_5\alpha - a_2\alpha^2 + a_7\alpha^3 - a_4 i - a_1 i\alpha + a_6 i\alpha^2 + a_3 i\alpha^3, \tag{4.33}$$

vidíme, že $x = \sigma\tau(x)$, právě když

$a_0 = a_0$, $a_1 = -a_5$, $a_2 = -a_2$, $a_3 = a_7$, $a_4 = -a_4$, $a_5 = -a_1$, $a_6 = a_6$, $a_7 = a_3$.

Proto prvky a_0 a a_6 můžeme zvolit libovolně, zatímco $a_2 = a_4 = 0$, $a_5 = -a_1$ a $a_7 = a_3$. Tedy

$$x = a_0 + a_1(1-i)\alpha + a_6 i\alpha^2 + a_3(1+i)\alpha^3 = a_0 + a_1[(1-i)\alpha] - \frac{a_6}{2}[(1-i)\alpha]^2 - \frac{a_3}{2}[(1-i)\alpha]^3 \tag{4.34}$$

a máme $\hat{E} = \mathbb{Q}((1-i)\alpha)$.

Normální podgrupy grupy $Gal(S/\mathbb{Q})$ jsou $Gal(S/\mathbb{Q})$, U, V, W, A, I. Proto jsou podle Základní věty Galoisovy teorie fixní tělesa $\hat{G} = \mathbb{Q}$, $\hat{U}$, $\hat{V}$, $\hat{W}$, $\hat{A}$ a $\hat{I} = S$ jediná normální rozšíření tělesa $\mathbb{Q}$, která jsou podtělesem S.

Snadno se nahlédne, že tato tělesa jsou po řadě rozkladová tělesa polynomů x, x^2+1, x^2-2, x^2+2, x^4-x^2-2 a x^4-2 nad $\mathbb{Q}$, proto jsou to normální rozšíření tělesa $\mathbb{Q}$.

Na druhé straně např. $\hat{B}/\mathbb{Q}$ není normální rozšíření, protože polynom $p(x) = x^4 - 2$ má v $\hat{B} = \mathbb{Q}(\alpha)$ kořen, ale nerozkládá se tam. Rozšíření $\hat{C}/\mathbb{Q}$ také není normální, protože kořen α je sice obsažen v $\hat{C} = \mathbb{Q}((1+i)\alpha)$, ale $\hat{C}$ není rozkladové těleso tohoto polynomu. Proto podobně tělesa $\hat{D}$ a $\hat{E}$ nejsou normální rozšíření $\mathbb{Q}$.

Dále podle Základní věty Galoisovy teorie platí, že $Gal(\hat{A}/\mathbb{Q}) \cong Gal(S/\mathbb{Q})/A$. Předpokládáme, že platí $Gal(S/\mathbb{Q})/A \cong \mathbb{Z}_2 \times \mathbb{Z}_2$. Nyní se podíváme, jak Galoisova grupa $Gal(\hat{A}/\mathbb{Q})$ vypadá. Protože $\hat{A} = \mathbb{Q}(i, \sqrt{2})$, existují čtyři automorfismy tělesa $\hat{A}$ identické na $\mathbb{Q}$:

Automorfismus	**Obraz prvku** i	**Obraz prvku** $\sqrt{2}$
1	i	$\sqrt{2}$
β	i	$-\sqrt{2}$
γ	$-i$	$\sqrt{2}$
$\beta\gamma$	$-i$	$-\sqrt{2}$

Protože $\beta^2 = \gamma^2 = 1$ a $\beta\gamma = \gamma\beta$, kombinace uvedené v tabulce jsou již všechny $\mathbb{Q}$-automorfismy tělesa $\hat{A}$. Tedy

$$Gal(\hat{A}/\mathbb{Q}) = \{1, \beta, \gamma, \beta\gamma\} \cong \mathbb{Z}_2 \times \mathbb{Z}_2. \tag{4.35}$$

Dále určíme Galoisovu grupu $Gal(\hat{U}/\mathbb{Q})$ rozšíření $\hat{U}/\mathbb{Q}$, pro kterou platí $Gal(\hat{U}/\mathbb{Q}) \cong Gal(S/\mathbb{Q})/U$. Protože $\hat{U} = \mathbb{Q}(i)$ je rozkladové těleso polynomu $x^2 + 1 \in \mathbb{Q}[x]$ a tento polynom je minimální polynom prvku $i \notin \mathbb{R} \supseteq Q(i)$, platí $[\hat{U} : \mathbb{Q}] = 2$. Proto existují dva $\mathbb{Q}$-automorfismy tělesa $\hat{U}$:

Automorfismus	**Obraz prvku** i
1	i
δ	$-i$

Tedy $Gal(\hat{U}/\mathbb{Q}) = \{1, \delta\}$.

Dále máme $\hat{V} = \mathbb{Q}(\alpha^2) = \mathbb{Q}(\sqrt{2})$ rozkladové těleso polynomu $x^2 - 2 \in \mathbb{Q}[x]$, jehož kořeny ve $\hat{V}$ jsou $\pm\sqrt{2}$. Platí, že $[\hat{V} : \mathbb{Q}] = 2$. Proto máme dva automorfismy, které zobrazují kořeny tohoto polynomu na nějaký jiný kořen:

Automorfismus	**Obraz prvku** $\sqrt{2}$
1	$\sqrt{2}$
ϵ	$-\sqrt{2}$

Tedy $Gal(\hat{V}/\mathbb{Q}) = \{1, \epsilon\}$.

Podobně platí $\hat{W} = \mathbb{Q}(i\alpha^2) = \mathbb{Q}(i\sqrt{2})$ je rozkladové těleso $x^2 + 2 \in \mathbb{Q}[x]$, jehož kořeny ve $\hat{W}$ jsou $\pm i\sqrt{2}$. Platí, že $[\hat{W} : \mathbb{Q}] = 2$. Proto nám i zde vycházejí dva $\mathbb{Q}$-automorfismy $\hat{W}$:

Automorfismus	**Obraz prvku** $i\sqrt{2}$
1	$i\sqrt{2}$
ω	$-i\sqrt{2}$

Tedy $Gal(\hat{W}/\mathbb{Q}) = \{1, \omega\}$.

Kapitola 5

Aplikace Galoisovy teorie

Cílem této kapitoly je najít rovnici pátého stupně, která není řešitelná pomocí radikálů.

5.1 Řešitelnost polynomů v radikálech

Nejprve si zde uvedeme několik pomocných tvrzení, která nám pomohou dokázat hlavní větu této kapitoly.

Lemma 5.1.1 *Buď U/T rozšíření těles, kde $U = T(\beta)$ pro β splňující $\beta^p = \gamma \in T$ pro nějaké prvočíslo p. Označme δ, $\delta \neq 1$, kořen polynomu $x^p - 1$ (p-tá primitivní odmocnina z 1). Potom je rozšíření $T(\beta, \delta)/T$ normální čistě radikálové.*

Důkaz. Podle definice zaručuje posloupnost $T \subseteq T(\delta) \subseteq T(\delta, \beta)$, že rozšíření $T(\beta, \delta)/T$ je čistě radikálové. Vzhledem k tomu, že p je prvočíslo, jsou kořeny polynomu $x^p - 1$ mocniny δ. Kořeny polynomu $x^p - \gamma$ potom dostaneme jako násobky β kořeny polynomu $x^p - 1$. Odtud je vidět, že se v $T(\beta, \delta)$ oba polynomy $x^p - 1$ a $x^p - \gamma$ rozkládají, proto je rozšíření $T(\beta, \delta)/T$ také normální. □

Poznámka 5.1.2 Jak bude patrné z důkazu Lemmatu 5.1.7, je těleso $T(\beta, \delta)$ rozkladovým nadtělesem polynomu $x^p - \gamma$.

Indukcí snadno ukážeme následující tvrzení:

Lemma 5.1.3 *Buď U/T čistě radikálové rozšíření, kde $U = (\beta_1, \ldots, \beta_n)$ a β_i je kořenem polynomu $x^{p_i} - \gamma_i$ pro $\gamma_i \in T(\beta_1, \ldots, \beta_{i-1})$ pro $i = 1, \ldots, n$ a p_i je prvočíslo. Pro $i = 1, \ldots, n$ buď δ_i, $\delta_i \neq 1$, kořen polynomu $x^{p_i} - 1$. Potom je rozšíření V/T, kde $V = (\beta_1, \ldots, \beta_n, \delta_1, \ldots \delta_n)$, čistě radikálové a normální.* □

Důsledek 5.1.4 *Buď U radikálové rozšíření tělesa T. Potom je normální uzávěr V rozšíření U/T také radikálové rozšíření.*

Důkaz. Podle definice je U obsaženo v nějakém čistě radikálovém rozšíření U' tělesa T. Podle Lemmatu 5.1.3 je U' obsaženo v normálním čistě radikálovém rozšíření V'. Protože je V' normální, platí $T \subseteq V \subseteq V'$, a tedy V je podle definice radikálové. □

Lemma 5.1.5 *Buď U rozkladové těleso polynomu $q(x) = x^p - 1 \in T[x]$, kde p je prvočíslo. Potom je $Gal(U/T)$ komutativní a dokonce cyklická.*

Důkaz. Protože derivace polynomu q je $q'(x) = px^{p-1}$, jejímž kořenem je pouze 0, nemá q v U vícenásobné kořeny. Snadno se nahlédne, že kořeny q tvoří cyklickou grupu řádu p. Buď ξ generátor této grupy. Potom $U = T(\xi)$ a libovolný T-automorfismus permutuje kořeny q, splňuje tedy

$$\sigma_i(\xi) = \xi^i \tag{5.1}$$

a touto podmínkou je jednoznačně určen. Potom ale platí $\sigma_i\sigma_j(\xi) = \sigma_i(\xi^j) = \xi^{ij} = \sigma_{ij}(\xi)$, a tedy $Gal(U/T)$ je cyklická. □

Lemma 5.1.6 *Buď U rozkladové těleso polynomu $s(x) = x^n - 1 \in T[x]$. Dále buď $\gamma \in U$ a V rozkladové těleso polynomu $t(x) = x^n - \gamma \in U[x]$. Potom je $Gal(V/U)$ komutativní.*

Důkaz. Buď α nějaký kořen polynomu t. Protože se polynom $s(x) = x^n - 1$ v U rozkládá, kořeny polynomu t jsou tvaru $\delta\alpha$, kde δ je kořen polynomu s v U. Protože $V = U(\alpha)$, libovolný U-automorfismus tělesa V je tvořen obrazy prvku α. Jsou-li σ, τ dva U-automorfismy V takové, že

$$\sigma(\alpha) = \delta\alpha \qquad \tau(\alpha) = \eta\alpha, \tag{5.2}$$

kde δ, $\eta \in U$, potom platí $\sigma\tau(\alpha) = \eta\delta\alpha = \delta\eta\alpha = \tau\sigma(\alpha)$, a tedy $Gal(V/U)$ je komutativní. □

Lemma 5.1.7 *Buď U/T normální čistě radikálové rozšíření. Potom je $Gal(U/T)$ řešitelná.*

Důkaz. U/T je čistě radikálové, proto $U = T(\beta_1, \ldots, \beta_n)$, kde $\beta_i^{p_i} \in T(\beta_1, \ldots, \beta_{i-1})$ pro každé $i \geq 1$. Můžeme předpokládat, že p_i je prvočíslo pro každé $i = 1, \ldots, n$.

Postupujme indukcí podle n. Pokud $n = 0$, tvrzení platí. Pokud $\beta_1 \in T$, potom $U = T(\beta_2, \ldots, \beta_n)$ a $Gal(U/T)$ je podle indukčního předpokladu řešitelná.

Nyní předpokládejme, že $\beta_1 \notin T$. Buď f minimální polynom prvku β_1 nad T. Protože je U/T normální, f se v U rozkládá, a protože $T \subseteq \mathbb{C}$, má f pouze jednoduché kořeny. Protože $\beta_1 \notin T$, je f stupně alespoň 2. Buď tedy $\alpha \neq \beta_1$ kořen f a položme $\varepsilon = \frac{\beta_1}{\alpha}$. Potom $\varepsilon^k = 1$ a $\varepsilon \neq 1$. Tedy ε je řádu k v multiplikativní grupě U^* tělesa U, tedy prvky $1, \varepsilon, \varepsilon^2, \ldots, \varepsilon^{k-1}$ jsou různé k-té odmocniny z jedné v U. Proto se polynom $g(x) = x^k - 1$ rozkládá v U.

Buď $K \subseteq U$ rozkladové těleso polynomu $g \in T[x]$, tedy $K = T(\varepsilon)$. Uvažujme posloupnost těles $T \subseteq K \subseteq K(\beta_1) \subseteq U$. Protože je rozšíření U/T konečné a normální, je konečné a normální také U/K. Protože se g nad K rozkládá a $\beta_1^k \in K$, z důkazu Lemma 5.1.6 plyne, že $K(\beta_1)$ je rozkladové těleso polynomu $x^k - \beta_1^k$ nad K. Proto je $K(\beta_1)/K$ normální a podle Lemma 5.1.6 je $Gal(K(\beta_1)/K)$ komutativní. Dále podle Základní věty Galoisovy teorie 4.2.15 bodu 3. platí

$$Gal(K(\beta_1)/K) \cong Gal(U/K)/Gal(U/K(\beta_1)). \tag{5.3}$$

Nyní je $U = K(\beta_1)(\beta_2, \ldots, \beta_n)$, takže $U/K(\beta_1)$ je normální radikálové, tedy podle indukčního předpokladu je $Gal(U/K(\beta_1))$ řešitelná. Proto je také $Gal(U/K)$ řešitelná.

Protože K je rozkladové těleso polynomu $g(x) = x^k - 1 \in T[x]$, rozšíření K/T je normální. Podle Lemma 5.1.5 je $Gal(K/T)$ komutativní. Pokud aplikujeme Základní větu 4.2.15 na rozšíření U/T, dostaneme

$$Gal(K/T) \cong Gal(U/T)/Gal(U/K). \tag{5.4}$$

Protože $Gal(U/K)$ je normální podgrupa $Gal(U/T)$, grupa $Gal(U/K)$ je řešitelná a faktorová grupa $Gal(U/T)/Gal(U/K)$ je izomorfní komutativní grupě $Gal(K/T)$ a je tedy také řešitelná, platí, že $Gal(U/T_0)$ je řešitelná, čímž je důkaz věty dokončen. □

Věta 5.1.8 *Buď U/T normální radikálové rozšíření. Potom je $Gal(U/T)$ řešitelná.*

Důkaz. Podle Důsledku 5.1.4 existuje normální čistě radikálové rozšíření V tělesa T obsahující U. Podle Lemmatu 5.1.7 je grupa $Gal(V/T)$ řešitelná. Protože rozšíření U/T je normální, je $Gal(V/U)$ normální podgrupa grupy $Gal(V/T)$ a platí

$$Gal(U/T) \cong Gal(V/T)/Gal(V/U). \tag{5.5}$$

$Gal(U/T)$ je tedy faktorovou grupou řešitelné grupy a je tedy řešitelná. □

Jak jsme uvedli v Definici 4.2.3, pokud uvažujeme polynom $p \in T[x]$ a S jeho rozkladové těleso, potom Galoisova grupa polynomu p je $Gal(S/T)$. Následující věta je tedy přeformulováním věty předchozí:

Věta 5.1.9 *Buď $p \in T[x]$ polynom a S jeho rozkladové těleso, ve kterém p nemá vícenásobné kořeny. Pokud je rovnice $p = 0$ řešitelná pomocí radikálů, je grupa $Gal(S/T)$ řešitelná.* □

Zde platí dokonce i ekvivalence, kterou ale nebudeme dokazovat.

Věta 5.1.10 *Buď $p \in T[x]$ polynom a S jeho rozkladové těleso, ve kterém p nemá vícenásobné kořeny. Rovnice $p = 0$ je řešitelná pomocí radikálů, právě když je grupa $Gal(S/T)$ řešitelná.* □

Lemma 5.1.11 *Buď $s \in \mathbb{Q}[x]$ polynom prvočíselného stupně p ireducibilní nad $\mathbb{Q}$, S jeho rozkladové těleso a předpokládejme, že s má právě dva kořeny v $\mathbb{C}\backslash\mathbb{R}$. Potom pro Galoisovu grupu polynomu s platí $Gal(S/\mathbb{Q}) \cong \mathbb{S}_p$.*

Důkaz. Jistě platí $S \subseteq \mathbb{C}$. Buď tedy $Gal(S/\mathbb{Q})$ Galoisova grupa polynomu s, jejíž prvky budeme chápat jako permutace na kořenech s. Tyto kořeny jsou jistě jednoduché, proto platí, že $Gal(S/\mathbb{Q})$ je izomorfní nějaké podgrupě grupy $\mathbb{S}_p$. Při konstrukci rozkladového tělesa polynomu s nejprve sestrojíme kořenové nadtěleso, které případně dále rozšiřujeme, dokud nepřidáme všechny kořeny polynomu s. Protože je stupeň s prvočíslo p, je stupeň rozšíření kořenovým nadtělesem také p a tedy platí, že $[S : \mathbb{Q}]$ je dělitelný prvočíslem p. Protože podle bodu 2. Základní věty 4.2.15 je $[S : \mathbb{Q}] = |Gal(S/\mathbb{Q})|$, číslo p dělí také řád grupy $Gal(S/\mathbb{Q})$. Dále z Lagrangeovy věty plyne, že řád prvku v

grupě dělí řád grupy, $Gal(S/\mathbb{Q})$ tedy obsahuje prvek řádu p. Protože ale jediné prvky grupy $\mathbb{S}_p$ řádu p jsou cykly délky p, musí $Gal(S/\mathbb{Q})$ obsahovat nějaký p-cyklus.

Označme jako ϕ zobrazení, které přiřadí komplexnímu číslu α číslo $\bar{\alpha}$ s ním komplexně sdružené. ϕ je $\mathbb{R}$-automorfismus $\mathbb{C}$, a tedy restrikce ϕ na S je $\mathbb{Q}$-automorfismus tohoto tělesa. To znamená, že $p-2$ reálných kořenů polynomu s zůstává na místě, zatímco dva komplexně sdružené kořeny se transponují. Proto musí $Gal(S/\mathbb{Q})$ obsahovat transpozici.

Bez újmy na obecnosti předpokládejme, že $Gal(S/\mathbb{Q})$ obsahuje transpozici (12) a p-cyklus $(12\dots p)$. Tvrdíme, že tyto dvě permutace generují celou grupu $\mathbb{S}_p$. Označme tedy $c = (12\dots p)$, $t = (12)$ a $Gal(S/\mathbb{Q})$ buď tedy generovaná cykly c a t. Potom $Gal(S/\mathbb{Q})$ obsahuje prvek $c^{-1}tc = (23)$, a dále také prvky $c^{-1}(23)c = (34)$, $c^{-1}(34)c = (45)$,..., a tedy $Gal(S/\mathbb{Q})$ obsahuje všechny transpozice $(m\,,\,m+1)$. Dále platí, že $Gal(S/\mathbb{Q})$ obsahuje $(12)(23)(12) = (13)$, $(13)(34)(13) = (14)$,..., $Gal(S/\mathbb{Q})$ proto obsahuje také všechny transpozice $(1m)$. $Gal(S/\mathbb{Q})$ dále obsahuje složení $(1m)(1r)(1m) = (mr)$. Protože je ale každý prvek grupy $\mathbb{S}_n$ součinem transpozic, platí, že $Gal(S/\mathbb{Q}) = \mathbb{S}_p$. □

Věta 5.1.12 (**Eisensteinovo kritérium ireducibility**)
Buď $f(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_1x + a_0$ polynom nad $\mathbb{Z}$. Předpokládejme, že existuje prvočíslo p takové, že

1. p dělí a_i pro všechna $i = 1, 2, \ldots, n-1$,

2. p^2 nedělí a_0.

Potom je polynom f ireducibilní nad $\mathbb{Q}$.

Důkaz. Důkaz této věty najdeme např. v [5] na straně 303, Věta 4.25.

Věta 5.1.13 *Buď $k > 1$ a p prvočíslo. Polynom $f(x) = x^5 - kpx + p \in \mathbb{Q}[x]$ není řešitelný pomocí radikálů.*

Důkaz. Podle Eisensteinova kritéria 5.1.12 platí, že f je ireducibilní nad $\mathbb{Q}$. Chceme dokázat, že f má právě tři jednoduché reálné kořeny, a tedy dva nereálné kořeny, které jsou komplexně sdružené. Protože 5 je prvočíslo, z Lemmatu 5.1.11 potom plyne, že $Gal(S/\mathbb{Q}) = \mathbb{S}_5$. Dále podle Důsledku 4.1.12 platí, že grupa $\mathbb{S}_5$ není řešitelná, a proto podle Věty 5.1.10 není rovnice $f = 0$ řešitelná pomocí radikálů.

Zbývá tedy dokázat, že f má právě tři reálné jednoduché kořeny. Spočteme derivaci $f'(x) = 5x^4 - kp$ a položíme ji rovnu 0. Vidíme, že dva stacionární body (nulové body derivace) jsou $\pm\sqrt[4]{\frac{kp}{5}}$. Nyní si spočítáme hodnoty derivace f' v bodě $\pm a = \pm\sqrt[4]{\frac{kp+1}{5}}$ a v 0. Máme tedy $f'(-a) = 1 > 0$, $f'(0) = -kp < 0$ a $f'(a) = f'(-a) = 1 > 0$. Protože derivace f' mění v těchto bodech znaménko, platí, že f má v bodech $\pm\sqrt[4]{\frac{kp}{5}}$ lokální extrémy. Dále máme $f(-\sqrt[4]{\frac{kp}{5}}) = \frac{4}{5}kp\sqrt[4]{\frac{kp}{5}} + p$, tedy v bodě $-\sqrt[4]{\frac{kp}{5}}$ nabývá f lokálního maxima, a $f(\sqrt[4]{\frac{kp}{5}}) = -\frac{4}{5}kp\sqrt[4]{\frac{kp}{5}} + p$, a proto v bodě $\sqrt[4]{\frac{kp}{5}}$ nabývá funkce f lokálního minima. Nyní si ještě spočtěme hodnoty funkce f v bodech 0 a 1. Protože platí $f(0) = p > 0$ a $f(1) = 1 - p(k-1) < 0$, existuje ξ, $0 < \xi < 1$, takové, že $f(\xi) = 0$.

Protože platí, že $\lim_{x\to-\infty} f(x) = -\infty$ a $f(0) > 0$, existuje $\varepsilon < 0$ takové, že $f(\varepsilon) = 0$. Dále platí $\lim_{x\to\infty} f(x) = \infty$ a $f(1) < 0$, existuje tedy také $\eta > 1$ splňující $f(\eta) = 0$. Polynom f má proto alespoň tři reálné kořeny. Vzhledem k tomu, že mezi každou dvojicí reálných kořenů je lokální extrém, má f naopak nejvýše tři reálné kořeny. Z toho plyne, že f má právě tři reálné kořeny, čímž je důkaz věty dokončen. □

Literatura

[1] Artin E.: *Galois Theory*, University of Notre Dame Press, 1944, 1998.

[2] Bashir R.: *Skripta Roberta Bashira*, http://www.karlin.mff.cuni.cz/∼bashir/, 1995.

[3] Koch H.: *Introduction to Classical Mathematics I*, Kluwer Academic Publishers, 1991.

[4] Kuroš A.G.: *Kapitoly z obecné algebry*, Academia, 1977.

[5] Procházka L.: *Algebra*, Academia, 1990.

[6] Rotman J. J.: *An Introduction to the Theory of Groups*, Springer/Verlag New York, Inc, fourth edition, 1995.

[7] Stewart I.: *Galois Theory (Third edition)*, Mathemarics Institute University of Warwick, 2004.

[8] Trlifaj J.: *Skripta Jana Trlifaje*, http://www.karlin.mff.cuni.cz/∼trlifaj/alg026-7.pdf.