STŘEDOŠKOLSKÁ ODBORNÁ ČINNOST

Obor č. 1: Matematika a statistika

Užití dekompoziční grupy k důkazu zákona kvadratické reciprocity

Tomáš Perutka
Jihomoravský kraj

Brno 2018

STŘEDOŠKOLSKÁ ODBORNÁ ČINNOST

Obor č. 1: Matematika a statistika

Užití dekompoziční grupy k důkazu zákona kvadratické reciprocity

Using decomposition group to prove the quadratic reciprocity law

Autor: Tomáš Perutka
Škola: Gymnázium Brno, třída Kapitána Jaroše, p. o.
Kraj: Jihomoravský
Konzultant: prof. RNDr. Radan Kučera, DSc.

Prohlášení

Prohlašuji, že jsem svou práci SOČ vypracoval samostatně a použil jsem pouze prameny a literaturu uvedené v seznamu bibliografických záznamů. Prohlašuji, že tištěná verze a elektronická verze soutěžní práce SOČ jsou shodné. Nemám závažný důvod proti zpřístupňování této práce v souladu se zákonem č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) v platném znění.

V Brně dne: ..... Podpis: .....

Poděkování

Na tomto místě bych chtěl velice poděkovat prof. RNDr. Radanovi Kučerovi, DSc. za mimořádnou ochotu a vstřícnost při vedení mé práce a též za cenné rady a připomínky.

Abstrakt

Hlavním cílem této práce je aplikovat algebraickou teorii čísel na teorii kvadratických zbytků. Konkrétněji: zaprvé, vysvětlit čtenáři se základními znalostmi abstraktní a lineární algebry důkaz kvadratické reciprocity, který využívá kvadratické reciprocity a je uveden v jednom z mých zdrojů. A zadruhé, pokusit se sám využitím dekompozičních grup dokázat další tvrzení o kvadratických zbytcích.

Klíčová slova

kvadratický zbytek; Legendreův symbol; zákon kvadratické reciprocity; dekompoziční grupa; Frobeniův automorfismus

Abstract

The main goal of this thesis is to applicate algebraic number theory onto quadratic residues theory. More concretely: at first, to explain proof of the quadratic reciprocity law in which decomposition groups are used – and which is described in one of my sources – to a reader who was introduced to abstract and linear algebra. And at second, to try to use decomposition groups to prove more theorems about quadratic residues by myself.

Key words

quadratic residue; Legendre symbol; quadratic reciprocity law; decomposition group; Frobenius automorphism

Obsah

Úvod

Hlavním cílem této práce je pomocí algebraické teorie čísel využitím dekompozičních grup dokázat zákon kvadratické reciprocity a aplikovat tuto teorii na další tvrzení o kvadratických zbytcích. Aby čtenář mohl celému textu bez potíží rozumět, měl by mít znalosti algebry přibližně v rozsahu [3] a také ovládat základy linární algebry. Nicméně obtížnější algebraické pojmy, které jsou v textu využívány, jsou povětšinou zopakovány.

První kapitola pojednává o kvadraticky zbytcích a snad z ní plyne dostatečná motivace pro to, dozvědět se o tomto objektu více. V druhé kapitole se pak seznamujeme s pojmy týkajícími se rozšíření těles. V třetí kapitole je pak zavedena Galoisova teorie konečných rozšíření – text by měl být přístupný i čtenáři, který doposud neměl možnost se s tímto tématem seznámit. Hlavní výsledky jsou odvozovány a vysvětlovány především na příkladech.

Ve čtvrté kapitole popisujeme základní výsledky algebraické teorie čísel. Většina tvrzení je uvedena bez důkazu a jejich platnost je demonstrována na několika příkladech; v této části textu je cílem především stručně čtenáře seznámit s důležitými pojmy a tvrzeními, které budou potřeba dále – zevrubnější zavedení algebraické teorie čísel je možno nalézt např. v [1] (čtvrtá a pátá kapitola této práce vychází především z druhé, třetí a čtvrté kapitoly citované publikace) nebo v [6] (lze doporučit, pokud čtenář preferuje česky psaný text).

Výsledky předchozích kapitol jsou propojeny v kapitole páté, která se zabývá algebraickou teorií čísel v Galoisových rozšířeních. Zde se seznamujeme s klíčovými pojmy jako dekompoziční grupa a Frobeniův automorfismus. Teoretické poznatky pak aplikujeme v kapitole šesté, kde se nejprve zabýváme rozkládáním prvočísel v kvadratických a kruhových tělesech a posléze teorií kvadratických zbytků. Pomocí teorie v textu vybudované dokážeme nejen zákon kvadratické reciprocity, ale i další tvrzení, jako např. multiplikativitu Legendreova symbolu, Eulerovo kritérium nebo podmínky řešitelnosti rovnice $x^2 + y^2 = p$ pro liché prvočíslo p a celá čísla x, y.

Kapitola 1

Kvadratické zbytky

Teorie kvadratických zbytků patří k důležitým částem elementární teorie čísel. Mezi autory prvních poznatků o kvadratických zbytcích patřili mnozí významní matematici 17. a 18. století, mezi nimi například Pierre de Fermat a Leonhard Euler. Uceleně se jim začal věnovat až Carl Friedrich Gauss ve svém slavném díle *Disquisitiones Arithmeticae*. Povězme si tedy nyní, co to kvadratické zbytky vlastně jsou.

Definice 1.0.1. *O celém čísle a nesoudělném s přirozeným číslem m řekneme, že je kvadratický zbytek modulo m, pokud existuje nějaké $c \in \mathbb{Z}$ takové, že $a \equiv c^2 \pmod{m}$. Pokud žádné takové c neexistuje, říkáme, že a je kvadratický nezbytek modulo m.*

Je poměrně jednoduché určit všechny kvadratické zbytky modulo p, kde p je liché prvočíslo. Zkusme určit všechny kvadratické zbytky modulo třináct. Zbytkové třídy si zapíšeme jako $\pm[1]_{13}, \pm[2]_{13}, \pm[3]_{13}, \pm[4]_{13}, \pm[5]_{13}, \pm[6]_{13}$. Neuvažujeme třídu obsahující nulu, leží v ní totiž násobky třinácti, které podle definice kvadratickými zbytky být nemohou. Všechny tyto třídy umocníme na druhou modulo 13: $(\pm1)^2 \equiv 1$, $(\pm2)^2 \equiv 4$, $(\pm3)^2 \equiv 9$, $(\pm4)^2 \equiv 3$, $(\pm5)^2 \equiv 12$, $(\pm6)^2 \equiv 10$. Tedy celé číslo a je kvadratický zbytek modulo 13 právě tehdy, když $a \equiv 1, 3, 4, 9, 10, 12 \pmod{13}$.

Předchozí úvahu lze zobecnit pro libovolné liché prvočíslo. Všechny třídy obsahující kvadratické zbytky modulo p jsou tedy tvaru $[1^2]_p, [2^2]_p, ..., [(\frac{p-1}{2})^2]_p$. Můžeme jednoduše ukázat, že se opravdu jedná o $\frac{p-1}{2}$ různých tříd: kdyby totiž pro dvě celá čísla m, n, $0 < m < n \leq \frac{p-1}{2}$, platilo $m^2 \equiv n^2 \pmod{p}$, dostali bychom $0 \equiv m^2 - n^2 \equiv (m+n)(m-n) \pmod{p}$, a tedy p dělí součin $(m+n)(m-n)$. Pokud ale prvočíslo dělí součin, musí dělit alespoň jednoho z činitelů, tedy p dělí $m+n$ nebo $m-n$, což je ve sporu s tím, jak jsme volili čísla m, n. Poznamenejme ještě, že jelikož pro každé liché prvočíslo p máme právě $\frac{p-1}{2}$ kvadratických zbytků, zbývá nám tedy nutně rovněž $\frac{p-1}{2}$ kvadratických nezbytků. U předchozího příkladu $p = 13$ vidíme, že celé číslo a je kvadratický nezbytek, právě když $a \equiv 2, 5, 6, 7, 8, 11 \pmod{13}$.

Je užitečné tyto poznatky shrnout do následující věty:

Věta 1.0.2. *Nechť p je prvočíslo. Pak existuje právě $\frac{p-1}{2}$ tříd obsahujících kvadratické zbytky modulo p a stejný počet tříd obsahujících kvadratické nezbytky.*

Tato věta má zajímavý důsledek:

Věta 1.0.3. *Nechť $K = \{[a^2]_p | a \in \mathbb{Z}, a \neq 0\}$ je množina všech zbytkových tříd obsahujících kvadratické zbytky modulo p. Pak K tvoří $\frac{p-1}{2}$-prvkovou podgrupu grupy $(\mathbb{Z}/p\mathbb{Z})^*$.*

Důkaz. Ukázali jsme již, že K je $\frac{p-1}{2}$-prvková podmnožina množiny $(\mathbb{Z}/p\mathbb{Z})^*$. Zbývá tedy ukázat, že se jedná o grupu. Uvažujme libovolná nenulová celá čísla a, b. Jistě $[1]_p = [1^2]_p \in K$ a také $[a^2]_p \cdot [b^2]_p = [(ab)^2]_p \in K$. Nakonec uvažujme třídu $[a^2]_p^{-1}$ a ukažme, že leží v K. Označme c nějaké celé číslo splňující $[c]_p = [a]_p^{-1}$ (jistě je c nenulové). Pak $[a^2]_p^{-1} = ([a]_p^{-1})^2 = [c]_p^2 = [c^2]_p \in K$, což jsme chtěli. K je tedy opravdu grupa a tvrzení je dokázáno.

□

Abychom s kvadratickými zbytky mohli pracovat, je potřeba zavést si jisté značení zvané Legendreův symbol.

Definice 1.0.4. *Nechť $a \in \mathbb{Z}$ a p je liché prvočíslo. Pak Legendreův symbol $(\frac{a}{p})$ je definován následovně:*

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{pokud je } a \text{ kvadratický zbytek modulo } p, \\ 0 & \text{pokud } p \text{ dělí } a, \\ -1 & \text{pokud je } a \text{ kvadratický nezbytek modulo } p. \end{cases}$$

Je třeba si všimnout, že pokud $m \equiv n \pmod{p}$, tak $\left(\frac{m}{p}\right) = \left(\frac{n}{p}\right)$, tedy všechna čísla z dané zbytkové třídy mají týž Legendreův symbol. Jinými slovy tento symbol můžeme chápat jako jakési zobrazení z množiny $\mathbb{Z}/p\mathbb{Z}$ do množiny $\{-1, 0, 1\}$.

Zatím však nemáme potřebné nástroje na to, abychom s Legendreovým symbolem mohli počítat. Zamysleme se třeba nad následujícím příkladem:

Příklad 1.0.1. Určete, pro která lichá prvočísla p existuje celé číslo m takové, že $p|(m^2+10)$.

Zkoumanou podmínku můžeme vyjádřit v ekvivalentním tvaru $m^2 \equiv -10 \pmod{p}$, což je totéž jako $\left(\frac{-10}{p}\right) = 1$. Zajímá nás tedy, pro která p je tato podmínka splněna. Abychom ale tento a další příklady mohli řešit, musíme se seznámit se zákonem kvadratické reciprocity.

Zákon kvadratické reciprocity se skládá z jednoho hlavního tvrzení a několika doplňujících poznatků (v angličtině jsou známy jako *suplementary laws* nebo *additional laws*). Uvedeme toto tvrzení v té nejplnější podobě, ve které je možno jej v publikacích nalézt, tedy hlavní zákon a dva doplňující.

Věta 1.0.5. *Nechť p, q jsou různá lichá prvočísla. Potom*

$$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right) \cdot (-1)^{\frac{(p-1)(q-1)}{4}}.$$

Dále navíc platí:

1. $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$,

2. $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$.

Vzhledem k důležitosti těchto tvrzení uvedeme ještě ekvivalentní formu, jíž je možné toto tvrzení vyjádřit – a to pomocí kongruencí:

Věta 1.0.6. *Nechť p, q jsou různá lichá prvočísla. Potom*

$$\left(\frac{p}{q}\right) = \begin{cases} \left(\frac{q}{p}\right) & \text{pokud } p \equiv 1 \text{ nebo } q \equiv 1 \pmod 4, \\ -\left(\frac{q}{p}\right) & \text{pokud } p \equiv q \equiv 3 \pmod 4. \end{cases}$$

Dále navíc platí:

1. $\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{pokud } p \equiv 1 \pmod 4, \\ -1 & \text{pokud } p \equiv 3 \pmod 4, \end{cases}$

2. $\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{pokud } p \equiv \pm 1 \pmod 8, \\ -1 & \text{pokud } p \equiv \pm 3 \pmod 8. \end{cases}$

Doplňující zákony lze dokázat prostředky elementární teorie čísel; co se týče hlavního tvrzení, je dnes známo několik důkazů, od těch využívajících poměrně elementární prostředky až po některé velmi pokročilé. Mezi ty spíše elementární patří důkaz pomocí Gaussova lemmatu nebo Gaussovy sumy (s nimi je možno se seznámit např. v [4]) – to není náhodou, tento slavný matematik si kvadratické reciprocity i důkazů, jež objevil, velice považoval, zákon dokonce nazýval *Theorema Aurum*, tedy zlatá věta. Jeho motivací navíc bylo tuto zákonitost zobecnit (což se však povedlo až později).

V šesté kapitole uvedeme jeden z oněch pokročilejších důkazů zákona kvadratické reciprocity – využijeme při něm poznatky z algebraické teorie čísel v Galoisových rozšířeních.

Než se vrátíme k příkladu 1.0.1, uveďme ještě jedno důležité tvrzení potřebné pro počítání s Legendreovými symboly, a to je jeho multiplikativita:

Věta 1.0.7. *Pro libovolná celá čísla a, b a liché prvočíslo p platí:*

$$\left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right).$$

Důkaz této věty uvedeme také až ke konci práce.

Nyní ale zpět ke kvadratickým zbytkům. S pomocí obou tvrzení výše s nimi můžeme velmi dobře pracovat. Podívejme se na příklad 1.0.1, tedy pro která lichá prvočísla p platí $\left(\frac{-10}{p}\right) = 1$. Při výpočtu použijeme všechna čtyři výše zmíněná tvrzení:

$$\left(\frac{-10}{p}\right) = \left(\frac{-1}{p}\right) \cdot \left(\frac{2}{p}\right) \cdot \left(\frac{5}{p}\right) = (-1)^{\frac{p-1}{2}} \cdot (-1)^{\frac{p^2-1}{8}} \cdot \left(\frac{p}{5}\right) \cdot (-1)^{\frac{(p-1)(5-1)}{4}}.$$

Nyní upravíme jednotlivé části vzniklého součinu. Nejprve

$$(-1)^{\frac{(p-1)(5-1)}{4}} = (-1)^{\frac{(p-1)\cdot 4}{4}} = (-1)^{p-1}$$

a jelikož p je liché, tak $(-1)^{p-1} = 1$. Dále:

$$(-1)^{\frac{p-1}{2}} \cdot (-1)^{\frac{p^2-1}{8}} = (-1)^{\frac{p-1}{2}+\frac{p^2-1}{8}}.$$

Exponent upravíme:

$$\frac{p-1}{2} + \frac{p^2-1}{8} = \frac{p^2+4p-5}{8} = \frac{(p-1)(p+5)}{8}.$$

Celkem tedy $\left(\frac{-10}{p}\right) = 1$, právě když $(-1)^{\frac{(p-1)(p+5)}{8}} \cdot \left(\frac{p}{5}\right) = 1$. To nastane v případě, kdy jsou buď oba činitelé rovni jedné, nebo minus jedné.

Abychom zjistili možné hodnoty prvního činitele, můžeme uvažovat následovně: $p+5$ i $p-1$ jsou sudá čísla, avšak jejich rozdíl je 6, tudíž čtyřmi je dělitelné právě jedno z nich. Tedy pokud je $p+5$ nebo $p-1$ dělitelné osmi, jejich součin je dělitelný šestnácti, po vydělení osmi dostaneme sudé číslo a $(-1)^{\frac{(p-1)(p+5)}{8}} = 1$. Pokud ani $p+5$, ani $p-1$ není dělitelné osmi, je celý výraz $(-1)^{\frac{(p-1)(p+5)}{8}}$ roven číslu -1. A podmínka, že $p+5$ nebo $p-1$ je dělitelné osmi, zjevně nastane, právě když $p \equiv 1, 3 \pmod 8$.

Abychom zjistili možné hodnoty druhého činitele, je nutno zjistit, jaký dává p zbytek po dělení pěti. To můžeme spolu s předchozím zanést do tabulky:

$p \mod 8$	$(-1)^{\frac{(p-1)(p+5)}{8}}$	$p \mod 5$	$\left(\frac{p}{5}\right)$
1	1	1	1
3	1	2	-1
5	-1	3	-1
7	-1	4	1

Teď již stačí dát získané poznatky dohromady. Případ $(-1)^{\frac{(p-1)(p+5)}{8}} = \left(\frac{p}{5}\right) = 1$ nastane, právě když $p \equiv 1, 3, \pmod 8$ a zároveň $p \equiv 1, 4 \pmod 5$. Podle čínské zbytkové věty můžeme obě kongruence sjednotit modulo 40, tedy $p \equiv 1, 9, 11, 19 \pmod{40}$. Případ $(-1)^{\frac{(p-1)(p+5)}{8}} = \left(\frac{p}{5}\right) = -1$ nastane, právě když $p \equiv 5, 7 \pmod 8$ a zároveň $p \equiv 2, 3 \pmod 5$, tedy podle čínské zbytkové věty $p \equiv 7, 13, 23, 37 \pmod{40}$. Celkem tedy liché prvočíslo p dělí výraz m^2+10 pro nějaké celé číslo m, právě když $p \equiv 1, 7, 9, 11, 13, 19, 23, 37 \pmod{40}$. Můžeme uvést několik příkladů: $41|(20^2+10)$, $53|(19^2+10)$, $157|(33^2+10)$.

Uvědomme si, že řešit tento příklad bez kvadratických zbytků by bylo velmi náročné, zatímco s nimi byl příklad sice poněkud pracný, ale principiálně poměrně jednoduchý. Dále si můžeme všimnout, že spolu s ním jsme dokázali například, že diofantická rovnice $17y = x^2 + 10$, $x, y \in \mathbb{Z}$ nemá řešení.

Doufejme, že to vše čtenáře přesvědčilo o tom, že kvadratické zbytky a zákon kvadratické reciprocity jsou velice silné nástroje. Dále je lze využít např. v kryptografii, ale překvapivě i v teorii grafů nebo akustice. Další jejich významné využití je v řešení problému, která lichá prvočísla p lze pro dané přirozené n vyjádřit ve tvaru $x^2 + ny^2$, $x, y \in \mathbb{Z}$ (metodám řešení tohoto problému je věnována kniha [8]). Má tedy smysl zákon kvadratické reciprocity dokazovat. Abychom se k tomuto důkazu dostali, je však třeba nejprve se hlouběji seznámit s pojmem rozšíření těles.

Kapitola 2

Rozšíření těles

Tělesa patří k jednomu ze základních objektů studovaných v algebře, potažmo v algebraické teorii čísel. Nás bude především zajímat situace, kdy budeme mít více do sebe vnořených těles – pak je možno mluvit o rozšíření.

Definice 2.0.1. *Nechť $(K, +, \cdot), (L, +, \cdot)$ jsou tělesa. Pokud $K \subseteq L$, říkáme, že těleso L je rozšířením tělesa K.*

Můžeme hned uvést mnoho příkladů. Libovolné těleso K je rozšířením sebe samého. Těleso komplexních čísel je rozšířením tělesa reálných čísel, to je rozšířením tělesa racionálních čísel. Těleso $\mathbb{Q}(\sqrt{n})$ je pro každé přirozené n rozšířením tělesa racionálních čísel. Těleso $\mathbb{R}(x, y)$ racionálních funkcí dvou proměnných nad reálnými čísly (tedy $\mathbb{R}(x, y) = \{\frac{f}{g} | f, g \in \mathbb{R}[x, y], g \neq 0\}$) je rozšířením tělesa $\mathbb{R}(x)$.

Poznámka 2.0.1. V dalším textu budeme používat následující značení: pro těleso K symbolem $K(a_1, ..., a_n)$ míníme těleso generované množinou $K \cup \{a_1, ..., a_n\}$; tedy předpokládáme-li existenci tělesa F takového, že $K \subseteq F$ a $a_1, ..., a_n \in F$, tělesem generovaným množinou $K \cup \{a_1, ..., a_n\}$ myslíme nejmenší podtěleso tělesa F tuto množinu obsahující. V případě okruhů používáme obdobné značení – je-li R okruh, značíme okruh generovaný množinou $R \cap \{a_1, ..., a_n\}$ jako $R[a_1, ..., a_n]$. Tedy např. $\mathbb{Q}(\sqrt{2})$ nejmenší podtěleso reálných čísel obsahující racionální čísla a odmocninu ze dvou a $\mathbb{Z}[i]$ je nejmenší podokruh komplexních čísel obsahující celá čísla a imaginární jednotku i.

Ideál daného okruhu R generovaný množinou $\{a_1, ..., a_n\}$ (tedy průnik všech ideálů okruhu R obsahujících tuto množinu) pak značíme jednoduše jako $(a_1, ..., a_n)$.

Důležitou vlastností rozšíření těles je, že to „větší“ tvoří vektorový prostor nad tím „menším“:

Věta 2.0.2. *Nechť $K \subseteq L$ je rozšíření těles. Pak platí, že L tvoří vektorový prostor nad tělesem K.*

Důkaz. Abychom tvrzení dokázali, stačí si ověřit axiomy vektorového prostoru. L bude tvořit vektorový prostor nad K, právě když se nám podaří nalézt nějakou operaci zadanou

jako $+ : L \times L \to L$, s níž L tvoří komutativní grupu, a operaci $\cdot : K \times L \to L$, která pro libovolná $a, b \in K$ a $\mathbf{u}, \mathbf{v} \in L$ splňuje následující čtyři podmínky:

1. $a \cdot (b \cdot \mathbf{v}) = (ab) \cdot \mathbf{v}$,
2. $1 \cdot \mathbf{v} = \mathbf{v}$ (kde 1 je neutrální prvek vůči násobení v tělese K),
3. $a \cdot (\mathbf{u} + \mathbf{v}) = a \cdot \mathbf{u} + a \cdot \mathbf{v}$,
4. $(a + b) \cdot \mathbf{v} = a \cdot \mathbf{v} + b \cdot \mathbf{v}$.

Avšak je snadno vidět, že pokud si zvolíme za operaci + klasické sčítání v tělese L a za operaci $\cdot$ zúžení klasického násobení v L na $K \times L$, všechny tyto podmínky jsou splněny.

□

Máme-li definován vektorový prostor, můžeme hovořit i o jeho dimenzi:

Definice 2.0.3. *Nechť $K \subseteq L$ je rozšíření těles. Pak dimenzi L jako vektorového prostoru nad K nazýváme stupeň rozšíření L nad K a značíme tento stupeň jako $[L : K]$. Je-li dimenze nekonečná, píšeme $[L : K] = \infty$.*

Například $[\mathbb{C} : \mathbb{R}] = 2$, jelikož báze $\mathbb{C}$ nad $\mathbb{R}$ je množina $\{1, i\}$, která je dvojprvková. Dále $[\mathbb{R} : \mathbb{Q}] = \infty$, $[K : K] = 1$.

V situacích, kdy máme více do sebe vnořených těles, se stupně rozšíření chovají velice sympatickým způsobem, jak nám říká věta o násobení stupňů:

Věta 2.0.4. *Nechť $K \subseteq M$, $M \subseteq L$ jsou rozšíření těles. Pak pro stupně těchto rozšíření platí*

$$[L : K] = [L : M] \cdot [M : K],$$

přičemž využíváme konvence $n \cdot \infty = n = \infty \cdot n$ pro všechna přirozená n.

Důkaz. Pokud je $[L : M]$ nebo $[M : K]$ rovno nekonečnu, můžeme snadno nahlédnout, že i $[L : K]$ bude rovno nekonečnu. Nechť tedy $[L : M] = n, [M : K] = m$. Zvolme nějakou bázi $\alpha_1, ..., \alpha_n$ L nad M a bázi $\beta_1, ..., \beta_m$ M nad K. Pak lze přímým výpočtem (který je ale poněkud zdlouhavý, proto ho zde vynecháme) ukázat, že $\alpha_i\beta_j$ $(1 \leq i \leq n, 1 \leq j \leq m)$ je bází L nad K, tedy vskutku $[L : K] = mn$.

□

Důležitý pojem týkající se rozšíření těles je *kompozitum*.

Definice 2.0.5. *Nechť $K \subseteq M$, $K \subseteq N$ jsou rozšíření těles, navíc M i N jsou podtělesa nějakého tělesa L. Pak nejmenší podtěleso tělesa L, které obsahuje M i N, nazýváme kompozitum těles M a N a značíme ho MN.*

Poznámka 2.0.2. Lze ukázat, že $[MN : K] \leq [M : K] \cdot [N : K]$. Rovnost v této nerovnosti nastává, právě když je báze vektorového prostoru M nad K lineárně nezávislá nad N.

Jsou-li navíc M a N rozšíření tělesa K konečného stupně a prvky $\alpha_1, ..., \alpha_m$ (resp. $\beta_1, ..., \beta_n$) tvoří bázi vektorového prostoru M (resp. N) nad K, lze ukázat, že součiny $\alpha_i\beta_j$, $1 \leq i \leq m$, $l \leq j \leq n$, generují vektorový prostor MN nad K.

Např. kompozitum těles $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{3})$ je těleso $\mathbb{Q}(\sqrt{2},\sqrt{3})$, což vidíme z definice: $\mathbb{Q}(\sqrt{2})$ je nejmenší těleso obsahující $\mathbb{Q}$ a $\sqrt{2}$, $\mathbb{Q}(\sqrt{3})$ je nejmenší těleso obsahující $\mathbb{Q}$ a $\sqrt{3}$; $\mathbb{Q}(\sqrt{2},\sqrt{3})$ je nejmenší těleso obsahující $\mathbb{Q}$, $\sqrt{2}$ a $\sqrt{3}$, tedy kompozitum předchozích dvou.

Zatím o rozšířeních nemluvíme explicitně – hovoříme sice o tělese $\mathbb{Q}(\sqrt{2})$, ale ne o tom, z jakých prvků se skládá. Situace se nám osvětlí, seznámíme-li se s konceptem minimálního polynomu. Díky němu zjistíme, v jakém vztahu jsou prvky „většího“ tělesa k „menšímu“.

Poznámka 2.0.3. Než přijde řeč na okruhy polynomů jedné proměnné nad tělesem, připomeňme, že v těchto okruzích můžeme dělit se zbytkem a používat Bezoutovu rovnost. To proto, že se jedná o příklad tzv. *Euklidovského okruhu* – to je obor integrity R, na němž existuje funkce $f : R \setminus \{0\} \to \mathbb{N}$ splňující 1) pro všechna $a, b \in R, b \neq 0$ existují $q, r \in R$ tak, že $a = bq + r$ a buď $r = 0$, nebo $f(r) < f(b)$, 2) $f(a) \leq f(ab)$ pro libovolná nenulová a, b z R. V takovémto okruhu mj. vždy můžeme dělit se zbytkem a používat Bezoutovu rovnost.

Nechť $K \subseteq L$ je rozšíření těles a $f \in K[x]$, tedy $f(x) = a_n x^n + \cdots + a_1 x + a_0, a_0, ..., a_n \in K$, $a_n \neq 0$ (připomeňme, že číslu n říkáme *stupeň polynomu* f a značíme ho $\deg f$). Pak pro libovolné $\alpha \in L$ je $f(\alpha) = a_n\alpha^n + \cdots + a_1\alpha + a_0$ prvkem tělesa L. Připomeňme, že *kořenem polynomu* f nazýváme libovolné a takové, že $f(a) = 0$.

Definice 2.0.6. *Nechť $K \subseteq L$ je rozšíření těles, $\alpha \in L$. Řekneme, že α je algebraický nad K, pokud existuje polynom $f \in K[x], f \neq 0$ takový, že α je jeho kořenem. Pokud žádný takový polynom neexistuje, říkáme, že α je transcendentní nad K.*

Můžeme uvést mnoho příkladů algebraických prvků. Každý prvek a libovolného tělesa K je algebraický nad K, protože je kořenem polynomu $x - a$. Imaginární jednotka i je algebraická nad $\mathbb{R}$, protože je kořenem polynomu x^2+1. Pro libovolné celé číslo n a přirozené číslo m je m-tá odmocnina z n algebraická nad $\mathbb{Q}$, protože je kořenem polynomu $x^m - n$.

S transcendentními čísly je to o něco náročnější. Je totiž nesrovnatelně jednodušší dokázat, že číslo je nad nějakým tělesem K algebraické – tedy najít polynom $f \in K$, jehož by bylo kořenem – než ukázat, že je nad K transcendentní, tedy dokázat, že žádný takový polynom neexistuje. Matematikům trvalo dlouhý čas ukázat, že čísla π a e jsou transcendentní nad $\mathbb{R}$. Můžeme ale uvést snazší příklad: $y \in \mathbb{R}(x, y)$ je transcendentní nad $\mathbb{R}(x)$.

Nechť je prvek $\alpha \in L$ algebraický nad K – existuje tedy polynom $f \in K[x]$ takový, že α je jeho kořenem. Takových polynomů je však určitě více – například polynom $2f$ nebo f^2. Budeme nyní definovat polynom s vlastností $f(\alpha) = 0$, který je v jistém smyslu nejmenší, a uvidíme, že má některé důležité vlastnosti.

Věta 2.0.7. *Nechť $K \subseteq L$ je rozšíření těles, $\alpha \in L$ je algebraický nad K. Pak platí, že α je kořenem právě jednoho normovaného ireducibilního polynomu $f \in K[x]$. Navíc platí:*

1. *pro libovolný polynom $h \in K[x]$ platí $h(\alpha) = 0$, právě když $f|h$,*
2. *$K(\alpha) = K[\alpha]$,*

3. $1, \alpha, \alpha^2, ..., \alpha^{n-1}$ *je bází vektorového prostoru* $K(\alpha)$ *nad* K*, kde* $n = \deg f$*,*

4. $[K(\alpha) : K] = n$*.*

Důkaz. Nejprve si uvědomme, že α je jistě v $K[x]$ kořenem alespoň jednoho normovaného ireducibilního polynomu. Víme totiž, že je kořenem nějakého polynomu $p \in K[x]$, proto musí být kořenem nějakého z ireducibilních dělitelů polynomu p. Rozložíme-li totiž p na součin ireducibilních polynomů jako $p = f_1 \cdots f_r$, dostaneme $0 = p(\alpha) = f_1(\alpha) \cdots f_r(\alpha)$, tedy $f_i(\alpha) = 0$ pro vhodné i a α je kořenem ireducibilního polynomuf_i. Ten sice nemusí být normovaný, ale je-li jeho vedoucí koeficient roven m, tak je α jistě také kořenem ireducibilního polynomu $m^{-1}f_i$, jenž už normovaný je.

Předpokládejme nyní, že α je kořenem více než jednoho normovaného ireducibilního polynomu, označme je f a g. Pak podle Bezoutovy rovnosti platí $af + bg = 1$ pro nějaké $a, b \in K[x]$. Pak ale $1 = a(\alpha)f(\alpha) + b(\alpha)g(\alpha) = 0$, což je spor. Tedy α je opravdu kořenem právě jednoho normovanéhu ireducibilního polynomu $f \in K[x]$.

Nechť je nyní $h \in K[x]$ libovolný polynom, jehož je α kořenem. Jelikož je okruh polynomů jedné proměnné nad tělesem okruh s jednoznačným rozkladem, můžeme psát $h = mp_1 \cdots p_k$, kde $m \in K[x]$ a $p_i \in K[x]$ jsou nějaké normované ireducibilní polynomy. Potom je jistě α kořenem nějakého z těchto polynomů, řekněme p_1. Protože však jediný normovaný ireducibilní polynom, jehož je α kořenem, je f, tak $p_1 = f$ a tedy $f|h$. Naopak také pokud $f|h$, tak zjevně $h(\alpha) = 0$. Dokázali jsme tedy tvrzení 1.

Uvažujme nyní zobrazení $\varphi : K[x] \to K[\alpha]$, které libovolnému polynomu $g(x)$ přiřadí jeho hodnotu $g(\alpha)$. Toto zobrazení je jistě homomorfismus, navíc surjektivní, tedy $K[\alpha] \cong$ $\cong K[x]/\ker\varphi$. Jádrem homomorfismu φ je však množina polynomů h takových, že $h(\alpha) = 0$, což jsou právě ty polynomy, jejichž dělitelem je náš polynom f. Tedy $\ker\varphi = (f)$, což je prvoideál (protože je f ireducibilní), a tudíž i maximální ideál (jelikož se pohybujeme v okruhu s jednoznačným rozkladem). Proto $K[x]/(f)$ je těleso (faktorizujeme podle maximálního ideálu) a tedy i $K[\alpha]$ je těleso. Jelikož je to nejmenší okruh obsahující K i α, je to tedy i nejmenší těleso obsahující tyto prvky, tedy přímo $K(\alpha)$. Dokázali jsme tedy tvrzení 2.

Abychom dokázali tvrzení 3 a 4, uvědomme si, že každý polynom $h \in K[x]$ je tvaru $af + r$, kde $a, r \in K[x]$ a $\deg r < n$. Pak tedy

$$\begin{aligned} K(\alpha) = K[\alpha] = \{h(\alpha)|h \in K[x]\} = \{a(\alpha)f(\alpha) + r(\alpha)\} = \{r(\alpha)|r \in K[x], \deg r < n\} = \\ = \{a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1}|a_0, ..., a_{n-1} \in K\}. \end{aligned}$$

Prvky $1, \alpha, \alpha^2, ..., \alpha^{n-1}$ tedy generují vektorový prostor $K(\alpha)$ nad K. Abychom ukázali, že tyto prvky tvoří bázi, zbývá ukázat, že jsou lineárně nezávislé nad K. To provedeme sporem: jsou-li lineárně závislé, dostáváme rovnost

$$c_0 + c_1\alpha + \cdots + c_{n-1}\alpha^{n-1} = 0,$$

tedy α je kořenem polynomu

$$h(x) = c_{n-1}\alpha^{n-1} + \cdots + c_1\alpha + c_0 \in K[x].$$

Z tvrzení jedna tedy $f|h$, což nelze, jelikož $\deg h < \deg f$.

Prvky $1, \alpha, \alpha^2, ..., \alpha^{n-1}$ tedy opravdu tvoří bázi vektorového prostoru $K(\alpha)$ nad K a z toho plyne $[K(\alpha) : K] = n$.

□

Definice 2.0.8. *Polynom f z předchozí věty nazýváme minimální polynom prvku α nad tělesem K.*

Důkaz je poněkud pracný, ale představuje krásné využití základních kamenů teorie okruhů – především hlavní věty o faktorokruzích a tvrzení, že okruh polynomů jedné proměnné nad libovolným tělesem je Euklidovský (a tedy s jednoznačným rozkladem).

Abychom ukázali, kolik nového nám tato věta přináší, zamysleme se nad následujícím příkladem:

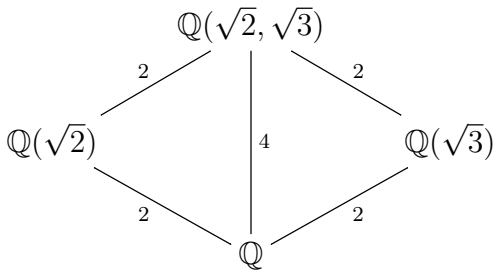
Příklad 2.0.1. Určete explicitně prvky těles $M = \mathbb{Q}(\sqrt{2})$, $N = \mathbb{Q}(\sqrt{3})$, $L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Navíc určete stupně rozšíření $[L : M], [L : N], [M : \mathbb{Q}], [N : \mathbb{Q}], [L : \mathbb{Q}]$.

Díky větě o minimálním polynomu si s příkladem hravě poradíme. Polynom $x^2 - 2$ je normovaný a ireducibilní polynom nad $\mathbb{Q}$ a jeho kořenem je $\sqrt{2}$, tudíž je to minimální polynom prvku $\sqrt{2}$ nad $\mathbb{Q}$. Proto $M = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$ a $[M : \mathbb{Q}] = 2$. Obdobně $N = \{a + b\sqrt{3} \mid a, b \in \mathbb{Q}\}$ a $[N : \mathbb{Q}] = 2$, tentokrát použijeme polynom $x^2 - 3$.

Nyní si všimněme, že $x^2 - 2$ je rovněž minimálním polynomem prvku $\sqrt{2}$ nad N. Jistě je normovaný a je také ireducibilní v $N[x]$ – kdyby nebyl, mohli bychom ho v $N[x]$ rozložit na součin lineárních činitelů a jeho kořeny by tedy ležely v N, ale $\sqrt{2}$ ani $-\sqrt{2}$ v $N = \mathbb{Q}(\sqrt{3})$ zjevně neleží (kdyby ano, musela by nějaká racionální čísla a, b splňovat rovnost $\sqrt{2} = a + b\sqrt{3}$, po umocnění na druhou bychom tedy dostali, že $\sqrt{3}$ je racionální číslo, což je spor). Proto $[L : N] = [N(\sqrt{2}) : N] = 2$ a tedy $[L : \mathbb{Q}] = [L : N] \cdot [N : \mathbb{Q}] = 4$ (podle věty o násobení stupňů), obdobně bychom ukázali i $[L : M] = [M(\sqrt{3}) : M] = 2$.

Zbývá nám zjistit, jakého tvaru jsou prvky tělesa L. Jelikož $L = N(\sqrt{2})$, můžeme psát

$$\begin{aligned} L &= \{\alpha + \beta\sqrt{2} \mid \alpha, \beta \in N\} \\ &= \{(k + l\sqrt{3}) + (m + n\sqrt{3})\sqrt{2} \mid k, l, m, n \in \mathbb{Q}\} \\ &= \{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{2}\sqrt{3} \mid a, b, c, d \in \mathbb{Q}\}. \end{aligned}$$



Nyní je třeba zavést několik pojmů týkajících se rozšíření:

Definice 2.0.9. *Nechť $K \subseteq L$ je rozšíření těles. Řekneme, že toto rozšíření je:*

- *konečné, pokud $[L : K] \in \mathbb{N}$,*
- *jednoduché, pokud $L = K(\alpha)$ pro nějaký prvek α algebraický nad K,*
- *algebraické, pokud je každý prvek L algebraický nad K.*

Jistě je každé jednoduché rozšíření konečné, jelikož jeho stupeň je roven stupni nějakého polynomu, což je přirozené číslo. Dále platí:

Věta 2.0.10. *Každé konečné rozšíření je algebraické.*

Důkaz. Nechť $K \subseteq L$ je libovolné konečné rozšíření. Označme $n = [L : K]$. Pak pro libovolný prvek $\alpha \in L$ jsou prvky $1, \alpha, ..., \alpha^n$ lineárně závislé nad K, tedy existují prvky $a_0, ..., a_n \in K$, ne všechny rovny nule, pro něž platí $a_n\alpha^n + \cdots + a_1\alpha + a_0 = 0$. Pak je α kořenem polynomu $f(x) = a_nx^n + \cdots + a_1x + a_0 \in K[x]$ a je tedy algebraický nad K. □

Všimněme si, že důkaz věty o minimálním polynomu mimo jiné říká, že jakékoli jednoduché rozšíření $K(\alpha)$ můžeme popsat také jako faktorokruh $K[x]/(f)$, kde f je minimální polynom α nad K. Až na izomorfismy tak tedy můžeme popsat veškerá jednoduchá rozšíření.

Podívejme se, co dostaneme v případě, kdy těleso K budou reálná čísla a α bude imaginární jednotka i. Jistě minimální polynom i nad $\mathbb{R}$ je polynom $x^2 + 1$ – je normovaný a ireducibilní nad $\mathbb{R}$. Těleso komplexních čísel je vlastně těleso $\mathbb{R}(i)$, tudíž dostáváme $\mathbb{C} \cong \cong \mathbb{R}[x]/(x^2 + 1)$.

Další významnou skupinou rozšíření těles jsou rozkladová tělesa.

Věta 2.0.11. *Nechť K je těleso, $f \in K[x]$ je nekonstantní polynom. Pak vždy existuje těleso L, které je rozšířením tělesa K a v němž se f rozkládá na součin lineárních činitelů.*

Tuto větu lze dokázat matematickou indukcí vůči stupni polynomu f.

Definice 2.0.12. *Nechť K je těleso, $f \in K[x]$ je nekonstantní polynom. Zvolme rozšíření L tělesa K, v němž se f rozkládá na součin lineárních činitelů, tedy*

$$f = m \cdot (x - \alpha_1) \cdots (x - \alpha_n),$$

kde $m \in K, \alpha_1, ..., \alpha_n \in L$. Pak těleso $K(\alpha_1, ..., \alpha_n)$ nazýváme rozkladovým tělesem polynomu $f \in K[x]$.

Rozkladové těleso je tedy nejmenší podtěleso tělesa L, v němž se polynom f rozkládá na součin lineárních činitelů. Lze ukázat, že rozkladové těleso je vždy určeno jednoznačně až na izomorfismus, avšak není to úplně snadné, proto to v textu dokazovat nebudeme.

Například pro libovolný polynom nad racionálními čísly je podle základní věty algebry jeho rozkladové těleso nějaké podtěleso komplexních čísel. Rozkladové těleso polynomu $x^2 - 2$ je těleso $\mathbb{Q}(\sqrt{2})$.

Příklad 2.0.2. Najděte rozkladové těleso polynomu $x^3 - 2 \in \mathbb{Q}[x]$.

Daný polynom můžeme nad komplexními čísly rozložit do tvaru

$$x^3 - 2 = (x - \sqrt[3]{2})(x - \omega\sqrt[3]{2})(x - \omega^2\sqrt[3]{2}),$$

kde $\omega = \frac{-1+i\sqrt{3}}{2}$ je primitvní třetí odmocnina z jedné. Rozkladové těleso polynomu $x^3 - 2$ je tedy tvaru $\mathbb{Q}(\sqrt[3]{2}, \omega\sqrt[3]{2}, \omega^2\sqrt[3]{2})$.

Ukážeme, že tento zápis můžeme dále upravit na elegantnější tvar $\mathbb{Q}(\sqrt[3]{2}, \omega)$. Jistě $\mathbb{Q}(\sqrt[3]{2}, \omega\sqrt[3]{2}, \omega^2\sqrt[3]{2}) \subseteq \mathbb{Q}(\sqrt[3]{2}, \omega)$. Ale jelikož zjevně

$$\sqrt[3]{2} \in \mathbb{Q}(\sqrt[3]{2}, \omega\sqrt[3]{2}, \omega^2\sqrt[3]{2})$$

a rovněž

$$\omega = \frac{1}{2} \cdot (\sqrt[3]{2})^2 \cdot \omega\sqrt[3]{2} \in \mathbb{Q}(\sqrt[3]{2}, \omega\sqrt[3]{2}, \omega^2\sqrt[3]{2}),$$

tak i $\mathbb{Q}(\sqrt[3]{2}, \omega) \subseteq \mathbb{Q}(\sqrt[3]{2}, \omega\sqrt[3]{2}, \omega^2\sqrt[3]{2})$ (jakožto nejmenší podtěleso komplexních čísel obsahující tyto prvky). Dostáváme tedy rovnost obou těles.

Abychom ukázali, že rozkladové těleso je pojem velmi užitečný, poznamenejme, že každé konečné těleso je izomorfní s rozkladovým tělesem polynomu $x^{p^n} - x \in (\mathbb{Z}/p\mathbb{Z})[x]$ pro vhodné prvočíslo p a přirozené číslo n.

Rozkladové těleso je možné definovat nejen pro jeden polynom, ale také pro libovolnou množinu polynomů nad daným tělesem K – je to nejmenší těleso obsahující K, v němž se všechny polynomy dané množiny rozkládají na součin lineárních činitelů. Lze ukázat (ale je to poměrně pracné), že takové těleso také vždy existuje a je určeno jednoznačně až na izomorfismy. Můžeme tedy dokonce sestrojit rozkladové těleso celé množiny $K[x]$:

Definice 2.0.13. *Nechť K je těleso. Algebraickým uzávěrem tělesa K nazýváme nejmenší těleso L takové, že $K \subseteq L$ a každý polynom z $K[x]$ se v L rozkládá na součin lineárních činitelů.*

Dobře známý příklad algebraického uzávěru je těleso komplexních čísel, které podle základní věty algebry tvoří algebraický uzávěr tělesa reálných čísel.

Dalším aspektem rozšíření těles je grupa automorfismů daného rozšíření. Její hlubší studium nás zavede až ke Galoisově teorii, o které budeme hovořit v následující kapitole.

Kapitola 3

Galoisova teorie

Galoisova teorie byla původně vytvořena k určení řešitelnosti polynomiálních rovnic, časem se z ní však stal silný nástroj v mnoha odvětvích matematiky souvisejících s algebrou. Abychom ji mohli zavést, je nejdříve potřeba připomenout a definovat některé pojmy.

Definice 3.0.1. *Nechť K je těleso, U jeho algebraický uzávěr, $f \in K[x]$ nekonstantní polynom. Říkáme, že polynom f je separabilní, pokud v U nemá násobné kořeny (jinak řečeno, pokud* $\mathrm{nsd}(f, f') = 1$*, kde f' je derivace polynomu f).*

Snadno lze ukázat následující věta:

Věta 3.0.2. *Každý ireducibilní polynom nad tělesem charakteristiky 0 je separabilní.*

Speciálně tedy každý ireducibilní polynom nad tělesem K, kde $\mathbb{Q} \subseteq K \subseteq \mathbb{C}$, je separabilní, protože všechna takováto K mají charakteristiku 0.

K separabilnímu polynomu se váže pojem separabilní rozšíření:

Definice 3.0.3. *Nechť $K \subseteq L$ je algebraické rozšíření těles. Pak říkáme, že toto rozšíření je separabilní, pokud je pro libovolné $\alpha \in L$ minimální polynom α nad K separabilní.*

Vidíme, že každé algebraické rozšíření $K \subseteq L$, kde $\mathbb{Q} \subseteq K \subseteq L \subseteq \mathbb{C}$, je separabilní, protože minimální polynom libovolného prvku $\alpha \in L$ nad K je ireducibilní polynom nad tělesem charakteristiky 0, a tedy je separabilní.

Další pojem, který je nutno zavést, je normální rozšíření:

Definice 3.0.4. *Nechť $K \subseteq L$ je algebraické rozšíření těles. Říkáme, že toto rozšíření je normální, pokud pro každý prvek $\alpha \in L$ platí, že v L leží všechny kořeny minimálního polynomu α nad K.*

Normální rozšíření je tedy např. $\mathbb{Q} \subseteq \mathbb{Q}(i)$, jelikož v $\mathbb{Q}(i)$ je s každým prvkem $a + bi, a, b \in \mathbb{Q}, b \neq 0$ obsažen i prvek $a - bi$, což je druhý kořen minimálního polynomu $a + bi$ nad $\mathbb{Q}$. Naproti tomu rozšíření $\mathbb{Q}(\sqrt[3]{2})$ normální není, protože obsahuje pouze jeden kořen polynomu $x^3 - 2$, tedy minimálního polynomu prvku $\sqrt[3]{2}$ nad $\mathbb{Q}$ (druhé dva kořeny jsou imaginární a těleso $\mathbb{Q}(\sqrt[3]{2})$ se skládá pouze z reálných čísel).

Galoisova teorie popisuje svou hlavní větou vlastnosti tzv. Galoisových rozšíření, což jsou právě konečná separabilní normální rozšíření. My se budeme zabývat pouze rozšířeními tělesa racionálních čísel, pro která je předpoklad separability splněn vždy (s obecnějším přístupem je možno se setkat např. v [5]). Budou nás tedy převážně zajímat tělesa K a L taková, že $\mathbb{Q} \subseteq K \subseteq L \subseteq \mathbb{C}$ a $K \subseteq L$ je konečné – tedy i algebraické – rozšíření.

Než se dostaneme k samotné Galoisově teorii, je potřeba se věnovat automorfismům daného rozšíření. Dále se seznámíme s hlavní větou Galoisovy teorie a jejími důsledky. Nakonec se podíváme na aplikace Galoisovy teorie v případě kruhových těles, což budeme potřebovat v šesté kapitole.

3.1 Automorfismy a vnoření

Budeme se nyní zabývat automorfismy daného rozšíření těles. Připomeňme nejprve, co to automorfismus je:

Definice 3.1.1. *Nechť K je těleso. Zobrazení $\varphi : K \to K$ nazýváme automorfismus tělesa K, pokud je to bijektivní homomorfismus.*

Můžeme tedy říci, že automorfismus je izomorfismus tělesa s ním samotným. Množina všech automorfismů tělesa K s operací skládání je jistě grupa: to hned vidíme, uvědomíme-li si, že na automorfismus můžeme nahlížet jako na permutaci prvků K, která je zároveň homomorfismem okruhů. Tuto grupu značíme $\mathrm{Aut}(K)$.

Nežli definujeme grupu automorfismů dané rozšíření, zaveďme následující názvosloví:

Definice 3.1.2. *Nechť M, N, X jsou množiny, $M \subseteq N$. Nechť $\varphi : M \to X$, $f : N \to X$ jsou zobrazení a pro všechna $m \in M$ platí $f(m) = \varphi(m)$. Pak říkáme, že zobrazení φ je zúžení (neboli restrikce) zobrazení f na množinu M (značíme $\varphi = f\big|_M$).*

Definice 3.1.3. *Nechť L, L' jsou libovolná tělesa, K jejich společné podtěleso, $\varphi : L \to L'$ je homomorfismus. Pokud pro všechna $a \in K$ platí $\varphi(a) = a$, říkáme, že φ fixuje těleso K.*

Tedy například zobrazení $\tau : \mathbb{C} \to \mathbb{C}$ zadané pro libovolná $a, b \in \mathbb{R}$ předpisem $\tau(a+bi) = a - bi$ fixuje těleso reálných čísel.

Definice 3.1.4. *Nechť $K \subseteq L$ je rozšíření těles. Pak libovolný automorfismus tělesa L, který fixuje těleso K, nazýváme automorfismem rozšíření $K \subseteq L$. Množinu takovýchto automorfismů značíme* $\mathrm{Aut}(L/K)$.

Množina $\mathrm{Aut}(L/K)$ je tedy podmnožinou $\mathrm{Aut}(K)$. Přidáme-li k oběma množinám operaci skládání, vidíme, že $\mathrm{Aut}(L/K)$ je dokonce podgrupa grupy $\mathrm{Aut}(K)$.

Abychom grupu $\mathrm{Aut}(L/K)$ mohli studovat, zaměříme se na obecnější objekt, jímž je vnoření. Budeme-li v následujícím mluvit o tělesech K a L, budeme tím vždy myslet tělesa taková, že $K \subseteq L$ je konečné rozšíření a navíc $\mathbb{Q} \subseteq K \subseteq L \subseteq \mathbb{C}$. Jiná tělesa budeme značit jinými písmeny.

Nejprve připomeňme definici vnoření:

Definice 3.1.5. *Nechť R, S jsou okruhy. Pak homomorfismus $\sigma : R \to S$ nazýváme vnoření R do S, pokud je injektivní.*

Je důležité si uvědomit, že na libovolné vnoření můžeme nahlížet také jako na izomorfismus $R \to \sigma(R)$, kde $\sigma(R) = \{\sigma(a)|a \in R\} \subseteq S$. Navíc si všimněme, že pokud jsou R, S tělesa, tak je každý homomorfismus mezi nimi vnoření: je-li $\varphi : R \to S$ homomorfismus, pak $\ker \varphi$ je ideál tělesa R, tedy buď $\ker \varphi = \{0\}$ a φ je tedy injektivní, nebo $\ker \varphi = R$, ale v tom případě $\varphi(1) = 0$, což je ve sporu s tím, že φ je homomorfismus okruhů.

Uvědomme si, že každý automorfismus je zároveň vnoření. Automorfismus je totiž bijektivní homomorfismus, je to tedy také injektivní homomorfismus, a tudíž vnoření. Označíme-li si $\mathcal{V}(L)$ množinu všech vnoření tělesa L do komplexních čísel a $\mathcal{V}(L/K)$ množinu všech vnoření L do $\mathbb{C}$ fixujících K (pozor, už to spolu se skládáním nemusí být grupy, protože obecně vnoření nemůžeme skládat), platí inkluze $\mathrm{Aut}(L) \subseteq \mathcal{V}(L)$, $\mathrm{Aut}(L/K) \subseteq \mathcal{V}(L/K)$.

Budeme se nyní zabývat počtem vnoření L do komplexních čísel a jejich vztahem k vnořením tělesa K do $\mathbb{C}$.

Věta 3.1.6. *Nechť $K \subseteq L$ je algebraické rozšíření těles, $\sigma : L \to \mathbb{C}$ je vnoření, které fixuje těleso K. Pak pro libovolné $\alpha \in L$ platí, že $\sigma(\alpha)$ je kořenem minimálního polynomu prvku α nad K.*

Důkaz. Nechť $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ je minimální polynom prvku α nad K. Pak tedy platí $\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 = 0$. Potom ale

$$\begin{aligned} f(\sigma(\alpha)) &= (\sigma(\alpha))^n + a_{n-1}(\sigma(\alpha))^{n-1} + \cdots + a_1\sigma(\alpha) + a_0 \\ &= (\sigma(\alpha))^n + \sigma(a_{n-1})(\sigma(\alpha))^{n-1} + \cdots + \sigma(a_1)\sigma(\alpha) + \sigma(a_0) \\ &= \sigma(\alpha^n) + \sigma(a_{n-1}\alpha^{n-1}) + \cdots + \sigma(a_1\alpha) + \sigma(a_0) \\ &= \sigma(\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0) \\ &= \sigma(0) \\ &= 0. \end{aligned}$$

Tedy $\sigma(\alpha)$ je kořen polynomu f.

□

Tato věta bude mít mnoho důsledků. Na následujícím příkladu si ukážeme, jak celá situace vypadá; bude sice náročný, ale pomůže nám pochopit, co se v rozšířeních s vnořeními a automorfismy děje. Než se do něj pustíme, vyslovíme následující lemma, které zjednoduší některé úvahy:

Lemma 3.1.7. *Nechť $K \subseteq K(\alpha)$ je rozšíření těles, α je algebraický nad K, $[K(\alpha) : K] = n$. Pak pokud pro nějaké $\sigma_1, \sigma_2 \in \mathcal{V}(K(\alpha)/K)$ platí $\sigma_1(\alpha) = \sigma_2(\alpha)$, tak $\sigma_1 = \sigma_2$. Jinými slovy, každý prvek množiny $\mathcal{V}(K(\alpha)/K)$ je jednoznačně zadán tím, na co zobrazí prvek α.*

Důkaz. Předpokládejme, že nějaké takové σ_1, σ_2 existují. Jelikož podle věty 2.0.7

$$K(\alpha) = \{a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} | a_0, ..., a_{n-1} \in K\},$$

tak dostáváme pro každý prvek γ tělesa $K(\alpha)$

$$\begin{aligned}\sigma_1(\gamma) &= \sigma_1(a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1}) \\ &= a_0 + a_1\sigma_1(\alpha) + \cdots + a_{n-1}(\sigma_1(\alpha))^{n-1} \\ &= a_0 + a_1\sigma_2(\alpha) + \cdots + a_{n-1}(\sigma_2(\alpha))^{n-1} \\ &= \sigma_2(\gamma).\end{aligned}$$

To jsme chtěli a důkaz je hotov.

□

Příklad 3.1.1. Určete grupy automorfismů a množiny vnoření v situaci, kdy jsou dána tělesa $\mathbb{Q}(\sqrt[3]{2}), \mathbb{Q}(\omega)$ a jejich kompozitum $\mathbb{Q}(\omega, \sqrt[3]{2})$, kde $\omega = \frac{-1+i\sqrt{3}}{2}$ je primitivní třetí odmocnina z jedné.

Zkoumejme nejprve těleso $\mathbb{Q}(\sqrt[3]{2})$ a hledejme prvky množiny $\mathcal{V}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})$, tedy všechna vnoření tělesa $\mathbb{Q}(\sqrt[3]{2})$ do komplexních čísel, která fixují racionální čísla. Víme, že každé takovéto zobrazení musí prvku $\sqrt[3]{2}$ přiřadit některý z kořenů minimálního polynomu tohoto prvku nad $\mathbb{Q}$, jímž, jak víme, je polynom $f(x) = x^3 - 2$.

Nechť β je nějaký kořen polynomu f. Podle lemmatu 3.1.7 existuje nejvýše jedno vnoření $\sigma \in \mathcal{V}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})$ takové, že $\sigma(\sqrt[3]{2}) = \beta$. Máme tedy tři potenciální prvky množiny $\mathcal{V}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})$:

$$\begin{aligned}&\sigma_1(a + b\sqrt[3]{2} + c\sqrt[3]{2}^2) = a + b\sqrt[3]{2} + c\sqrt[3]{2}^2, \\ &\sigma_2(a + b\sqrt[3]{2} + c\sqrt[3]{2}^2) = a + b\omega\sqrt[3]{2} + c\omega^2\sqrt[3]{2}^2, \\ &\sigma_3(a + b\sqrt[3]{2} + c\sqrt[3]{2}^2) = a + b\omega^2\sqrt[3]{2} + c(\omega^2\sqrt[3]{2})^2 = a + b\omega^2\sqrt[3]{2} + c\omega\sqrt[3]{2}^2.\end{aligned}$$

Poznamenejme, že σ_1 je sice formálně zobrazení $\mathbb{Q}(\sqrt[3]{2}) \to \mathbb{C}$, ale můžeme ho ztotožnit s identitou tělesa $\mathbb{Q}(\sqrt[3]{2})$, protože pro všechna $\alpha \in \mathbb{Q}(\sqrt[3]{2})$ platí $\sigma_1(\alpha) = \mathrm{id}(\alpha)$. Podobně budeme ztotožňovat i některá další zobrazení, která se liší pouze takto formálně.

Lze si přímým výpočtem ověřit, že $\sigma_1, \sigma_2, \sigma_3$ jsou opravdu homomorfismy $\mathbb{Q}(\sqrt[3]{2}) \to \mathbb{C}$ a zjevně jsou injektivní. Množina $\mathcal{V}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})$ má tedy právě tři prvky, což, jak si můžeme všimnout, je také stupeň rozšíření $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[3]{2})$. Také vidíme, že obrazy těchto vnoření jsou ve tvaru $\sigma_1(\mathbb{Q}(\sqrt[3]{2})) = \mathbb{Q}(\sqrt[3]{2})$, $\sigma_2(\mathbb{Q}(\sqrt[3]{2})) = \mathbb{Q}(\omega\sqrt[3]{2})$, $\sigma_3(\mathbb{Q}(\sqrt[3]{2})) = \mathbb{Q}(\omega^2\sqrt[3]{2})$; tedy pouze jedno z nich je zároveň automorfismus. Dostáváme tedy $\mathrm{Aut}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}) = \{\mathrm{id}\}$.

V případě tělesa $\mathbb{Q}(\omega)$ lze postupovat obdobným způsobem. Minimální polynom prvku ω nad $\mathbb{Q}$ je polynom $g(x) = x^2 + x + 1$. Máme tedy nejvýše dvě vnoření $\tau_1, \tau_2 \in \mathcal{V}(\mathbb{Q}(\omega)/\mathbb{Q})$. Jistě $\tau_1 = \mathrm{id}$. Kandidát na druhý prvek zobrazí číslo ω na druhý kořen polynomu $q(x)$, což je ω^2, jak můžeme vidět např. z Viètových vztahů (protože $\omega \cdot \omega^2 = 1$, $\omega + \omega^2 = 1$). Dostáváme tedy zobrazení $\tau_2 : a + b\omega \mapsto a + b\omega^2$. Opět lze výpočtem ukázat, že τ_2 je homomorfismus. Navíc $\tau_2(\mathbb{Q}(\omega)) = \mathbb{Q}(\omega^2) = \mathbb{Q}(\omega)$ (rovnost plyne z toho, že $\omega = (\omega^2)^2 \in \mathbb{Q}(\omega^2)$). Tudíž je τ_2 nejen vnoření, ale dokonce automorfismus. Dostáváme tedy $\mathrm{Aut}(\mathbb{Q}(\omega)/\mathbb{Q}) = \mathcal{V}(\mathbb{Q}(\omega)/\mathbb{Q})$. Obě množiny navíc opět mají tolik prvků, kolik je stupeň daného rozšíření.

Nyní se podívejme, co se stane v kompozitu obou těles – uvědomme si, že je to těleso tvaru $\mathbb{Q}(\omega, \sqrt[3]{2}) = \{a+b\sqrt[3]{2}+c\sqrt[3]{2}^2+d\omega+e\omega\sqrt[3]{2}+f\omega\sqrt[3]{2}^2 | a,b,c,d,e,f \in \mathbb{Q}\}$ a $[\mathbb{Q}(\omega, \sqrt[3]{2}) : \mathbb{Q}] = 6$. To plyne např. z toho, že báze vektorového prostoru $\mathbb{Q}(\sqrt[3]{2})$ nad $\mathbb{Q}$, tj. množina $\{1, \sqrt[3]{2}, \sqrt[3]{2}^2\}$, je linárně nezávislá nad $\mathbb{Q}(\omega)$ (můžeme tedy zohlednit poznámku 2.0.2).

Úvahou analogickou k té, jíž jsme dokázali lemma 3.1.7, můžeme ukázat, že libovolné vnoření $\psi \in \mathcal{V}(\mathbb{Q}(\omega, \sqrt[3]{2})/\mathbb{Q})$ je jednoznačně určeno tím, kam zobrazí prvky $\sqrt[3]{2}$ a ω. Navíc libovolná restrikce tohoto vnoření je jistě také vnoření (injektivní homomorfismus nemůže přestat být injektivním homomorfismem jen proto, že mu zmenšíme definiční obor). Tedy $\psi\big|_{\mathbb{Q}(\sqrt[3]{2})} \in \mathcal{V}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})$ a $\psi\big|_{\mathbb{Q}(\omega)} \in \mathcal{V}(\mathbb{Q}(\omega)/\mathbb{Q})$. Máme tedy $3 \cdot 2 = 6$ možností, jak zvolit ψ, a proto $|\mathcal{V}(\mathbb{Q}(\omega, \sqrt[3]{2})/\mathbb{Q})| \leq 6$. Ukážeme, že platí rovnost.

Zvažme zobrazení $\sigma : \mathbb{Q}(\omega, \sqrt[3]{2}) \to \mathbb{C}$, které fixuje $\mathbb{Q}(\omega)$ a prvek $\sqrt[3]{2}$ zobrazí na $\omega\sqrt[3]{2}$. Přímým (ale zdlouhavým) výpočtem si můžeme ověřit, že se jedná nejen o vnoření, ale dokonce o automorfismus! Navíc je to v grupě $\mathrm{Aut}(\mathbb{Q}(\omega, \sqrt[3]{2})/\mathbb{Q})$ prvek řádu 3, protože $\sigma^2(\sqrt[3]{2}) = \omega^2\sqrt[3]{2}, \sigma^2(\omega) = \omega \Rightarrow \sigma^2 \neq \mathrm{id}$ a $\sigma^3(\sqrt[3]{2}) = \omega^3\sqrt[3]{2} = \sqrt[3]{2}, \sigma^3(\omega) = \omega \Rightarrow \sigma^3 = \mathrm{id}$. Tedy $3 \big| |\mathrm{Aut}(\mathbb{Q}(\omega, \sqrt[3]{2})/\mathbb{Q})|$.

Dále uvažujme zobrazení $\tau : \mathbb{Q}(\omega, \sqrt[3]{2}) \to \mathbb{C}$, které fixuje $\mathbb{Q}(\sqrt[3]{2})$ a prvek ω zobrazí na ω^2. Opět si můžeme ověřit, že je to automorfismus, tentokrát řádu 2, jelikož $\tau^2(\sqrt[3]{2}) = \sqrt[3]{2}, \tau^2(\omega) = \omega^4 = \omega$. Tedy $2 \big| |\mathrm{Aut}(\mathbb{Q}(\omega, \sqrt[3]{2})/\mathbb{Q})|$.

Dohromady tedy 6 dělí počet prvků grupy automorfismů rozšíření $\mathbb{Q} \subseteq \mathbb{Q}(\omega, \sqrt[3]{2})$. Spolu s předchozím pak $6 \leq |\mathrm{Aut}(\mathbb{Q}(\omega, \sqrt[3]{2})/\mathbb{Q})| \leq |\mathcal{V}(\mathbb{Q}(\omega, \sqrt[3]{2})/\mathbb{Q})| \leq 6$.

To nám dává $\mathrm{Aut}(\mathbb{Q}(\omega, \sqrt[3]{2})/\mathbb{Q}) = \mathcal{V}(\mathbb{Q}(\omega, \sqrt[3]{2})/\mathbb{Q}) = \langle \sigma, \tau \rangle$, $|\mathrm{Aut}(\mathbb{Q}(\omega, \sqrt[3]{2})/\mathbb{Q})| = 6 = [\mathbb{Q}(\omega, \sqrt[3]{2}) : \mathbb{Q}]$. Co o této grupě můžeme říci? Všimněme si, že každý její prvek nějak permutuje tříprvkovou množinu $\{\sqrt[3]{2}, \omega\sqrt[3]{2}, \omega^2\sqrt[3]{2}\}$ (jedná se o kořeny polynomu $x^3 - 2$). Můžeme se tedy na σ dívat jako na trojcyklus a na τ jako na transpozici a dostáváme $\mathrm{Aut}(\mathbb{Q}(\omega, \sqrt[3]{2})/\mathbb{Q}) \cong \mathbb{S}_3$. Podle vědomostí o této grupě můžeme psát

$$\mathrm{Aut}(\mathbb{Q}(\omega, \sqrt[3]{2})/\mathbb{Q}) = \{\mathrm{id}, \sigma, \sigma^2, \tau, \sigma\tau, \sigma^2\tau\}$$

a můžeme sestavit mulitplikativní tabulku této grupy:

	id	σ	σ^2	τ	$\sigma\tau$	$\sigma^2\tau$
id	id	σ	σ^2	τ	$\sigma\tau$	$\sigma^2\tau$
σ	σ	σ^2	id	$\sigma^2\tau$	τ	$\sigma\tau$
σ^2	σ^2	id	σ	$\sigma\tau$	$\sigma^2\tau$	τ
τ	τ	$\sigma\tau$	$\sigma^2\tau$	id	σ	σ^2
$\sigma\tau$	$\sigma\tau$	$\sigma^2\tau$	τ	σ^2	id	σ
$\sigma^2\tau$	$\sigma^2\tau$	τ	$\sigma\tau$	σ	σ^2	id

Na tomto příkladě jsme vypozorovali několik zajímavých faktů, jež by bylo možné zobecnit. Především si nyní položme následující otázky: platí vždy $|\mathcal{V}(L/K)| = [L : K]$? A obecněji, rozšiřuje se každé vnoření $K \to \mathbb{C}$ na právě $[L : K]$ vnoření $L \to \mathbb{C}$?

Abychom na tyto otázky mohli odpovědět, uveďme nejprve bez důkazu následující větu:

Věta 3.1.8. *Nechť F, F' jsou tělesa, $\psi : F \to F'$ je jejich izomorfismus, $p \in F[x]$ je ireducibilní polynom. Nechť $\Psi : F[x] \to F'[x]$ je izomorfismus indukovaný izomorfismem ψ na koeficientech, tedy*

$$\Psi(a_n x^n + \cdots + a_1 x + a_0) = \psi(a_n)x^n + \cdots + \psi(a_1)x + \psi(a_0)$$

pro libovolné $a_n, ..., a_0 \in F$. Označme $p' = \Psi(p)$. Nechť α je kořenem polynomu p v algebraickém uzávěru tělesa F, β je kořenem p' v algebraickém uzávěru tělesa F'; existují tedy tělesa $F(\alpha), F'(\beta)$. Pak existuje – a to jediný – izomorfismus $\varphi : F(\alpha) \to F'(\beta)$ splňující $\varphi(a) = \psi(a)$ pro všechna $a \in F$ a navíc $\varphi(\alpha) = \beta$.

Ve speciálním případě, kdy $F = F' = K$, $\psi = \mathrm{id}$ a p je minimální polynom α nad K, dostáváme jako důsledek lemma 3.1.7.

Na větu 3.1.8 se můžeme podívat ještě poněkud jinou optikou: pokud F, F' jsou podtělesa komplexních čísel, můžeme se na izomorfismus ψ dívat jako na vnoření F do komplexních čísel, tedy prvek množiny $\mathcal{V}(F)$. Také izomorfismy $\varphi : F(\alpha) \to F'(\beta)$ pak můžeme pokládat za vnoření $F(\alpha) \to \mathbb{C}$. Potom tedy dostáváme následující důsledek:

Důsledek 3.1.9. *Nechť $L = K(\alpha)$. Pak se každé vnoření tělesa K do komplexních čísel rozšiřuje na $[L : K]$ vnoření L do komplexních čísel.*

Důkaz. Z textu výše je zřejmé, že každé vnoření $K \to \mathbb{C}$ se rozšiřuje na tolik vnoření $L \to \mathbb{C}$, kolik je kořenů polynomu $p' = \Psi(p)$. Vzhledem k tomu, jak je tento polynom definován, má právě tolik kořenů, kolik jich má polynom p. To je ale minimální polynom α nad K, má tedy právě $[K(\alpha) : K] = [L : K]$ kořenů.

□

Dostáváme tedy kladnou odpověď naše otázky ve speciálním případě $L = K(\alpha)$. Uvědomme si navíc, že každé vnoření $L \to \mathbb{C}$ je rozšířením nějakého vnoření $K \to \mathbb{C}$. Platí tedy $|\mathcal{V}(K(\alpha))| = [K(\alpha) : K] \cdot |\mathcal{V}(K)|$.

Nyní tuto situaci zobecníme. K tomu nám poslouží důsledek 3.1.9 s pomocí matematické indukce.

Věta 3.1.10. *Nechť $K \subseteq L$ je konečné rozšíření, $\mathbb{Q} \subseteq K \subseteq L \subseteq \mathbb{C}$. Pak se každé vnoření tělesa K do komplexních čísel rozšiřuje na právě $[L : K]$ vnoření tělesa L do komplexních čísel.*

Důkaz. Budeme postupovat matematickou indukcí podle stupně rozšíření $K \subseteq L$. Pokud $[L : K] = 1$, tak $L = K$ a tvrzení je zřejmé. Předpokládejme tedy nyní, že $[L : K] = n, n > 1$ a že pro všechna tělesa M, $K \subseteq M \subseteq L$, $[L : M] < [L : K]$, tvrzení platí, tedy každý prvek $\mathcal{V}(M)$ se rozšiřuje na $[L : M]$ prvků množiny $\mathcal{V}(L)$.

Zvolme si libovolný prvek $\alpha \in L \setminus K$. Pak jistě $K \subseteq K(\alpha) \subseteq L$, $[L : K(\alpha)] < [L : K]$, tedy z indukčního předpokladu platí, že každý prvek $\mathcal{V}(K(\alpha))$ se rozšiřuje na $[L : K(\alpha)]$ prvků $\mathcal{V}(L)$.

Z důsledku 3.1.9 však víme, že každý prvek $\mathcal{V}(K)$ se rozšiřuje na $[K(\alpha) : K]$ prvků $\mathcal{V}(K(\alpha))$. Ve spojení s předchozím tedy dostáváme, že každý prvek $\mathcal{V}(K)$ se rozšiřuje na $[L : K(\alpha)][K(\alpha) : K] = [L : K]$ prvků $\mathcal{V}(L)$. To jsme ale chtěli dokázat.

□

Dostáváme tedy kladnou odpověď na naše otázky, speciálně:

Důsledek 3.1.11. *Existuje právě $[L : K]$ vnoření tělesa L do komplexních čísel, která fixují těleso K.*

Zobecnili jsme tedy pozorování z příkladu 3.1.1. Jelikož každý automorfismus je vnoření, okamžitě dostáváme následující omezení:

Věta 3.1.12. *Nechť $K \subseteq L$ je konečné rozšíření, $\mathbb{Q} \subseteq K \subseteq L \subseteq \mathbb{Q}$. Pak $|\operatorname{Aut}(K/L)| \leq [L : K]$.*

Nabízí se otázka, kdy v této nerovnosti nastane rovnost. Aby se vnoření $\sigma \in \mathcal{V}(L/K)$ stalo automorfismem, musí v L ležet obrazy všech prvků z L – pro libovolný prvek $\alpha \in L$ je ale $\sigma(\alpha)$ jedním z kořenů minimálního polynomu α nad K. Aby tedy bylo σ prvkem grupy $\operatorname{Aut}(L/K)$, musí L s každým svým prvkem obsahovat také všechny kořeny minimálního polynomu tohoto prvku nad K. To je ale přesně definice normálního rozšíření!

Zde již však hovoříme o Galoisových rozšířeních:

Definice 3.1.13. *Nechť $K \subseteq L$ je konečné algebraické rozšíření, $\mathbb{Q} \subseteq K \subseteq L \subseteq \mathbb{C}$. Pak říkáme, že toto rozšíření je Galoisovo, pokud $\mathcal{V}(L/K) = \operatorname{Aut}(L/K)$ neboli $|\operatorname{Aut}(L/K)| = [L : K]$. Grupu $\operatorname{Aut}(L/K)$ pak nazýváme Galoisovou grupou rošíření $K \subseteq L$ a značíme ji $\operatorname{Gal}(L/K)$.*

Výše jsme již mohli vidět několik příkladů: rozšíření $\mathbb{Q} \subseteq \mathbb{Q}(\omega, \sqrt[3]{2})$, $\mathbb{Q} \subseteq \mathbb{Q}(\omega)$ jsou Galoisova, zatímco rozšíření $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[3]{2})$ není.

Ukázali jsme si, že v případě konečného rozšíření $K \subseteq L$, $\mathbb{Q} \subseteq K \subseteq L \subseteq \mathbb{C}$, je normálnost tohoto rozšíření nutná podmínka k tomu, aby bylo Galoisovo. V obecném případě je nutno požadovat ještě separabilitu daného rozšíření, která je v námi diskutovaném případě automatická. Obecně platí následující věta:

Věta 3.1.14. *Nechť $K \subseteq L$ je konečné (tedy i algebraické) rozšíření těles. Pak následující podmínky jsou ekvivalentní:*

1. *$K \subseteq L$ je Galoisovo (tedy $|\operatorname{Aut}(L/K)| = [L : K]$),*
2. *L je rozkladové těleso nějakého separabilního polynomu $f \in K[x]$,*
3. *$K \subseteq L$ je separabilní a normální.*

V další části se zaměříme na hlavní větu Galoisovy teorie, která dává do souvislosti mezitělesa rozšíření s podgrupami Galoisovy grupy.

3.2 Hlavní věta Galoisovy teorie

Uvažujme libovolné rozšíření těles $K \subseteq L$. Pak tělesa M taková, že $K \subseteq M \subseteq L$, nazýváme *mezitělesa* rozšíření $K \subseteq L$. V případě rozšíření $\mathbb{Q} \subseteq \mathbb{Q}(\omega, \sqrt[3]{2})$ jsme objevili např. mezitělesa $\mathbb{Q}(\sqrt[3]{2}), \mathbb{Q}(\omega)$ (a očividná mezitělesa $\mathbb{Q}, \mathbb{Q}(\omega, \sqrt[3]{2})$), ale také $\mathbb{Q}(\omega\sqrt[3]{2}), \mathbb{Q}(\omega^2\sqrt[3]{2})$. Nevíme však, existují-li další, popř. jakého jsou tvaru. Uvidíme, že v případě Galoisových rozšíření dokážeme elegantně popsat všechna mezitělesa daného rozšíření.

Uvažujme nyní konečné rozšíření $K \subseteq L$, ne nutně Galoisovo. Nechť M je libovolné mezitěleso. Pak můžeme uvažovat grupu $\mathrm{Aut}(L/M)$, která je jistě podgrupa grupy $\mathrm{Aut}(L/K)$ – pokud nějaký automorfismus fixuje M, tak tím spíše fixuje $K \subseteq M$.

Mezitělesům tedy můžeme přiřadit některé podgrupy grupy automorfismů. Je tomu však i naopak. Je-li H podgrupa grupy $\mathrm{Aut}(L/K)$, můžeme jí přiřadit tzv. *fixní podtěleso* $\mathrm{Fix}(H) = \{a \in L | \forall \varphi \in H : \varphi(a) = a\}$. Příklad může být opět rozšíření $\mathbb{Q} \subseteq \mathbb{Q}(\omega, \sqrt[3]{2})$ a podgrupa $H = \{\mathrm{id}, \tau\}$, kde τ je stejné jako v příkladu 3.1.1– zřejmě $\mathrm{Fix}(H) = \mathbb{Q}(\sqrt[3]{2})$. Otázkou samozřejmě je, jestli je každé mezitěleso fixním podtělesem nějaké grupy.

První důležitý poznatek ohledně fixních podtěles v Galoisových rozšířeních je následující ekvivalence:

Věta 3.2.1. *Nechť $K \subseteq L$ je algebraické rozšíření těles. Pak je Galoisovo, právě když* $\mathrm{Fix}(\mathrm{Gal}(L/K)) = K$.

V rozšířeních, která nejsou Galoisova, by se mohlo stát, že by těleso $\mathrm{Fix}(\mathrm{Aut}(L/K))$ bylo mezitěleso větší než K.

Poznámka 3.2.1. Připomeňme, že je-li M podmnožina nosné množiny nějaké grupy G, zápisem $\langle M \rangle$ značíme podgrupu grupy G generovanou množinou M (tedy průnik všech podgrup grupy G obsahujících M).

Uveďme nyní hlavní větu (konečné) Galoisovy teorie. Ta nám říká, že podgrupy Galoisovy grupy a mezitělesa si jednoznačně odpovídají:

Věta 3.2.2. *Nechť $K \subseteq L$ je konečné Galoisovo rozšíření, $G = \mathrm{Gal}(L/K)$. Označme $\mathcal{H} = \{H | H$ je podgrupa $G\}$, $\mathcal{M} = \{M | M$ je těleso, $K \subseteq M \subseteq L\}$. Pak dvojice zobrazení $H \mapsto \mathrm{Fix}(H)$, $M \mapsto Aut(L/M)$ jsou navzájem inverzní bijekce mezi $\mathcal{H}$ a $\mathcal{M}$ (tzn.* $\mathrm{Fix}(\mathrm{Aut}(L/M)) = M$, $\mathrm{Aut}(L/\mathrm{Fix}(H)) = H$*). Navíc platí:*

1. *Je-li $M_1 = \mathrm{Fix}(H_1), M_2 = \mathrm{Fix}(H_2)$ pro libovolné $H_1, H_2 \in \mathcal{H}$, pak:*
   - *(a)* $M_1 \subseteq M_2 \Leftrightarrow H_2 \subseteq H_1$,
   - *(b)* $M_1 M_2 = \mathrm{Fix}(H_1 \cap H_2)$,
   - *(c)* $M_1 \cap M_2 = \mathrm{Fix}(\langle H_1 \cup H_2 \rangle)$;
2. *je-li $M = \mathrm{Fix}(H)$, pak:*

(a) $[L : M] = |H|, [M : K] = |G/H|$,

(b) $M \subseteq L$ *je vždy Galoisovo,* $\mathrm{Gal}(L/M) = H$,

(c) $K \subseteq M$ *je Galoisovo, právě když je* H *normální podgrupa* G*; v tom případě* $\mathrm{Gal}(M/K) \cong G/H$ *(izomorfismus je dán restrikcí).*

Zamysleme se nad tím, co nám tato věta vlastně říká. Zásadní informací je, že podgrupy a mezitělesa si jednoznačně odpovídají; to však není všechno. Tvrzení 1 nám sděluje, jakým způsobem si přesně tyto objekty odpovídají – v kostce to můžeme popsat jako „čím větší podgrupa, tím menší mezitěleso," což není překvapivé vzhledem k $\mathrm{Fix}(\mathrm{Gal}(L/K)) = K$, $\mathrm{Fix}(\{\mathrm{id}\}) = L$. Tvrzení 2 nám pak říká více o vztahu tělesa M k tělesům L a K.

Nebudeme se dopodrobna zabývat důkazem této věty, jelikož většina myšlenek pro další text není příliš přínosná; nicméně lze říci, že důkaz tvrzení 1 a toho, že mezi $\mathcal{H}$ a $\mathcal{M}$ jsou navzájem inverzní bijekce, využívá převážně věty 3.1.14 a 3.2.1 a není příliš náročný.

Ukážeme si ale důkaz tvrzení 2, protože ho budeme dále potřebovat (a také je poměrně zajímavý). Důkazy tvrzení (a) a (b) jsou poměrně jednoduché. Předpokládejme platnost předchozích skutečností z hlavní věty Galoisovy teorie. Nejprve ukážeme (b): jelikož $K \subseteq L$ je Galoisovo, tak je L rozkladové těleso nějakého separabilního polynomu $f \in K[x]$. Ale jelikož $K \subseteq M$, tak také $f \in M[x]$ a L je zároveň rozkladové těleso polynomu z $M[x]$ – tedy $M \subseteq L$ je Galoisovo. Pak tedy $\mathrm{Gal}(L/M) = \mathrm{Aut}(L/M) = \mathrm{Aut}(L/\mathrm{Fix}(H)) = H$. Z toho hned plyne (a): $[L : M] = |\mathrm{Gal}(L/M)| = |H|$ a z Lagrangeovy věty $[M : K] = \frac{[L:K]}{[L:M]} = \frac{|G|}{|H|} = |G/H|$.

Nyní k tvrzení (c). Zavedeme zobrazení $\mathrm{res}_M : \mathcal{V}(L/K) \to \mathcal{V}(M/K)$ zadané jako $\mathrm{res}_M(\sigma) = \sigma\big|_M$, tedy každému vnoření přiřadí jeho restrikci na M. Toto zobrazení je korektní, jelikož restrikcí injektivního homomorfismu vskutku dostaneme opět injektivní homomorfismus. Navíc je to podle věty 3.1.10 surjekce.

Jelikož $K \subseteq L$ je Galoisovo, tak $\mathcal{V}(L/K) = G$. Ukážeme, že jádro zobrazení res_M je přesně množina H. Jistě $\mathrm{res}_M(H) = \{\mathrm{id}_M\}$, jelikož $H = \mathrm{Aut}(L/M)$. A protože se id_M podle věty 3.1.10 rozšiřuje na právě $[L : M] = |H|$ prvků množiny $\mathcal{V}(L/K)$, tak jsme podle $2(a)$ hotovi a H je opravdu jádro.

Uvažujme nyní třídy rozkladu G/H. Pokud dva automorfismy σ, τ leží v jedné třídě, tak ze základů teorie grup platí $\tau = \sigma\psi$ pro vhodné $\psi \in H$. Pak ale pro všechna $a \in M$ platí $\tau(a) = (\sigma\psi)(a) = \sigma(\psi(a)) = \sigma(\mathrm{id}_M(a)) = \sigma(a)$, jelikož $\psi\big|_M = \mathrm{id}_M$. Tedy všech $|H|$ prvků dané třídy rozkladu se zužuje na stejný prvek množiny $\mathcal{V}(M/K)$. Naopak ale podle věty 3.1.10 platí, že se každé $\sigma \in \mathcal{V}(M/K)$ rozšiřuje na $|H|$ prvků množiny $\mathcal{V}(L/K) = G$. Dohromady to znamená, že třídy rozkladu G/H a prvky množiny $\mathcal{V}(M/K)$ si jednoznačně odpovídají.

Z toho ale už dostáváme tvrzení (c) následujícím způsobem:

$$\begin{aligned} K \subseteq M \text{ je Galoisovo} &\Leftrightarrow \mathcal{V}(M/K) = \mathrm{Gal}(M/K) \\ &\Leftrightarrow \mathrm{res}_M \text{ je homomorfismus grup} \\ &\Leftrightarrow H = \ker(\mathrm{res}_M) \text{ je normální podgrupa.} \end{aligned}$$

Navíc pokud je H normální, tak zjevně $G/H \cong \mathrm{Gal}(M/K)$.

Poznámka 3.2.2. Pro Galoisovu teorii nekonečných rozšíření platí podobná věta, jako je věta 3.2.2. Zde si však mezitělesa neodpovídají se všemi podgrupami Galoisovy grupy, ale jen s některými. Aby se zjistilo, s kterými, je nutné zavést na Galoisově grupě jistou topologii (tzv. Krullova topologie), kterou se z Galoisovy grupy vytvoří tzv. *topologická grupa* (to znamená, že grupová operace a operace braní inverzního prvku jsou spojitá zobrazení). Pak mezitělesa odpovídají právě těm podgrupám Galoisovy grupy, které jsou v této topologii uzavřené.

Dostat se k hlavní větě Galoisovy teorie bylo vskutku náročné, ale přináší to své ovoce. Aplikací této věty je nepřeberné množství, mezi významné výsledky získané s pomocí Galoisovy teorie jsou například kritéria řešitelnosti polynomiálních rovnic a nebo konstruovatelnosti mnohoúhelníků – významné jsou také aplikace v algebraické teorii čísel, k nimž se dostaneme v další kapitole. Nyní však uveďme některé příklady.

Příklad 3.2.1. Nechť m, n jsou libovolná různá celá čísla taková, že $m, n \notin \{0, 1\}$ a žádné z nich není dělitelné druhou mocninou žádného prvočísla. Popište rozšíření $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{m}, \sqrt{n})$.

Uvědomme si nejdříve, že toto rozšíření je Galoisovo – je to rozkladové těleso separabilního polynomu $(x^2-m)(x^2-n)$. Abychom popsali toto rozšíření, zaměříme se nejprve na tělesa $\mathbb{Q}(\sqrt{m}), \mathbb{Q}(\sqrt{n})$; jistě je $\mathbb{Q}(\sqrt{m}, \sqrt{n})$ kompozitum těchto těles (z definice, viz příklad 2.0.1).

Rozšíření $\mathbb{Q}(\sqrt{m})$ je Galoisovo, jelikož je to rozkladové těleso separabilního polynomu $x^2 - m$. Tedy $\mathrm{Gal}(\mathbb{Q}(\sqrt{m})/\mathbb{Q})$ je dvouprvková, obsahuje tedy identitu a prvek řádu dva. Jelikož automorfismus zobrazuje prvky na kořeny jejich minimálního polynomu, označíme-li onen prvek řádu dva jako σ_m, dostáváme $\sigma_m(\sqrt{m}) = -\sqrt{m}$ a tedy $\sigma_m(a+b\sqrt{m}) = a-b\sqrt{m}$ pro všechna $a, b \in \mathbb{Q}$. Tedy $\mathrm{Gal}(\mathbb{Q}(\sqrt{m})/\mathbb{Q}) = \{\mathrm{id}, \sigma_m\} \cong \mathbb{Z}/2\mathbb{Z}$. Jelikož jediné podgrupy této grupy jsou celá grupa a triviální grupa, tak jediná mezitělesa rozšíření $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{m})$ jsou tato dvě tělesa.

Analogickou situaci máme v případě $\mathbb{Q}(\sqrt{n})$, tentokrát prvek řádu 2 v Galoisově grupě označíme jako σ_n.

Nyní se podívejme na jejich kompozitum – tím je těleso

$$\mathbb{Q}(\sqrt{m}, \sqrt{n}) = \{a + b\sqrt{m} + c\sqrt{n} + d\sqrt{m}\sqrt{n} \mid a, b, c, d \in \mathbb{Q}\}.$$

To můžeme dokázat analogicky jako v příkladu 2.0.1, který byl vlastně jen speciálním případem této situace (jde tedy opět o to, že polynom $x^2 - m$ je ireducibilní nad $\mathbb{Q}(\sqrt{n})$ a naopak). Obdobně tedy dostáváme $[\mathbb{Q}(\sqrt{m}, \sqrt{n}) : \mathbb{Q}] = 4$.

Rozšíříme-li na toto těleso automorfismy σ_m, σ_n předpisem $\sigma_m : \sqrt{m} \mapsto -\sqrt{m}$, $\sqrt{n} \mapsto \sqrt{n}$, přesněji

$$\sigma_m(a + b\sqrt{m} + c\sqrt{n} + d\sqrt{m}\sqrt{n}) = a - b\sqrt{m} + c\sqrt{n} - d\sqrt{m}\sqrt{n}$$

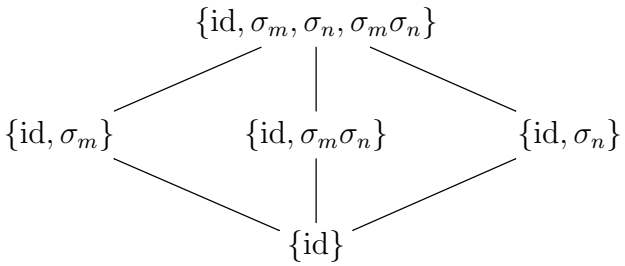
a obdobně pro σ_n, vidíme, že jsou to opět automorfismy. Navíc si uvědomme, že $\sigma_m\sigma_n = \sigma_n\sigma_m$. To si můžeme ověřit přímým výpočtem:

$$\begin{aligned}(\sigma_m\sigma_n)(a+b\sqrt{m}+c\sqrt{n}+d\sqrt{m}\sqrt{n}) &= \sigma_m(\sigma_n(a+b\sqrt{m}+c\sqrt{n}+d\sqrt{m}\sqrt{n}))\\ &= \sigma_m(a+b\sqrt{m}-c\sqrt{n}-d\sqrt{m}\sqrt{n})\\ &= a-b\sqrt{m}-c\sqrt{n}+d\sqrt{m}\sqrt{n}\\ &= \sigma_n(a-b\sqrt{m}+c\sqrt{n}-d\sqrt{m}\sqrt{n})\\ &= \sigma_n(\sigma_m(a+b\sqrt{m}+c\sqrt{n}+d\sqrt{m}\sqrt{n}))\\ &= (\sigma_n\sigma_m)(a+b\sqrt{m}+c\sqrt{n}+d\sqrt{m}\sqrt{n}).\end{aligned}$$

Protože Galoisova grupa rozšíření $\mathbb{Q}\subseteq\mathbb{Q}(\sqrt{m},\sqrt{n})$ je čtyřprvková, dostáváme

$$\mathrm{Gal}(\mathbb{Q}(\sqrt{m},\sqrt{n})/\,\mathbb{Q}) = \langle\sigma_m,\sigma_n\rangle = \{\mathrm{id},\sigma_m,\sigma_n,\sigma_m\sigma_n\} \cong (\mathbb{Z}\,/2\,\mathbb{Z})\times(\mathbb{Z}\,/2\,\mathbb{Z}).$$

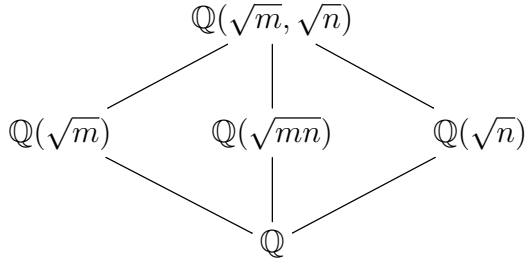
Podgrupy této grupy můžeme vidět na diagramu níže:



Podívejme se na svaz mezitěles. Jistě $\mathrm{Fix}(\{\mathrm{id}\,\sigma_m,\sigma_n,\sigma_m\sigma_n\}) = \mathbb{Q}$ a také $\mathrm{Fix}(\{\mathrm{id}\}) = \mathbb{Q}(\sqrt{m},\sqrt{n})$. Dále rovněž $\mathrm{Fix}(\{\mathrm{id},\sigma_m\}) = \mathbb{Q}(\sqrt{n})$, $\mathrm{Fix}(\{\mathrm{id},\sigma_n\}) = \mathbb{Q}(\sqrt{m})$. Jak ale popsat těleso $\mathrm{Fix}(\{\mathrm{id},\sigma_m\sigma_n\})$? Výše jsme ukázali, že $(\sigma_m\sigma_n)(a+b\sqrt{m}+c\sqrt{n}+d\sqrt{m}\sqrt{n}) = a-b\sqrt{m}-c\sqrt{n}+d\sqrt{m}\sqrt{n}$. Tedy

$$\begin{aligned}\mathrm{Fix}(\{\mathrm{id},\sigma_m\sigma_n\}) &= \{\alpha\in\mathbb{Q}(\sqrt{m},\sqrt{n}) \mid \sigma_m\sigma_n(\alpha)=\alpha\}\\ &= \{(a+b\sqrt{m}+c\sqrt{n}+d\sqrt{m}\sqrt{n} \mid b=c=0, a,d\in\mathbb{Q}\}\\ &= \{a+d\sqrt{mn} \mid a,d\in\mathbb{Q}\}\\ &= \mathbb{Q}(\sqrt{mn}).\end{aligned}$$

Jiná mezitělesa již nejsou. Můžeme je vidět na diagramu níže:



Poznámka 3.2.3. Je-li dáno m, n stejně jako v předchozím příkladu, nazýváme tělesa tvaru $\mathbb{Q}(\sqrt{m})$ jako *kvadratická* a tělesa tvaru $\mathbb{Q}(\sqrt{m}, \sqrt{n})$ jako *bikvadratická*.

Dalším významným příkladem jsou konečná tělesa. Sice jsme Galoisovu teorii odvozovali pouze pro podtělesa komplexních čísel, ve větě 3.1.14 jsme si ale řekli podmínky pro libovolné rozšíření. A lze ukázat, že každé konečné těleso je rozkladovým tělesem separabilního polynomu $x^{p^n} - x \in (\mathbb{Z}/p\mathbb{Z})[x]$ pro nějaké prvočíslo p. Nemáme prostor zde toto tvrzení dokázat, nicméně dokážeme alespoň, že je polynom $x^{p^n} - x$ separabilní: pokud by existoval nějaký jeho dvojnásobný kořen $\alpha \in \mathbb{Z}/p\mathbb{Z}$, byl by to i kořen derivace tohoto polynomu $(x^{p^n} - x)' = [p^n]_p x^{p^n - 1} - [1]_p = [-1]_p$. Takovýto polynom ale žádné kořeny nemá, spor.

Jelikož p i n můžeme volit libovolně, tak z vlastností rozkladového tělesa popsaných v druhé kapitole plyne následující:

Věta 3.2.3. *Pro libovolné prvočíslo p a přirozené číslo n existuje (až na izomorfismy) právě jedno konečné těleso o p^n prvcích; budeme ho značit $\mathbf{F}_{p^n}$. Navíc $\mathbb{Z}/p\mathbb{Z} \subseteq \mathbf{F}_{p^n}$ je Galoisovo rozšíření stupně n.*

Galoisova grupa tohoto rozšíření je až překvapivě dobře popsána:

Věta 3.2.4. *Grupa* $\mathrm{Gal}(\mathbf{F}_{p^n}/(\mathbb{Z}/p\mathbb{Z}))$ *je cyklická. Jejím generátorem je prvek ϕ s vlastností $\phi(a) = a^p$ pro všechna $a \in \mathbf{F}_{p^n}$. Tento prvek nazýváme Frobeniův automorfismus.*

Toto důležité tvrzení budeme v budoucnu potřebovat. Nemáme prostor je dokázat, poznamenejme ale, že podrobnější seznámení s konečnými tělesy je možno nalézt např. v [2] a že je to velice zajímavé téma.

3.3 Aplikace Galoisovy teorie na kruhová tělesa

Nejdříve musíme připomenout pojem n-tá odmocnina z jedné.

Definice 3.3.1. *O komplexním čísle ζ řekneme, že je n-tá odmocnina z jedné, pokud je to některý z kořenů polynomu $x^n - 1$. V případě, že ζ není k-tá odmocnina z jedné pro žádné přirozené k menší než n, říkáme, že ζ je primitivní n-tá odmocnina z jedné.*

Označme $\mathcal{M}_n$ množinu n-tých odmocnin z jedné. Pak např. $\mathcal{M}_2 = \{-1, 1\}$, přičemž -1 je primitivní druhá odmocnina z jedné; $\mathcal{M}_4 = \{1, -1, i, -i\}$ (kde i je imaginární jednotka) a z toho $i, -i$ jsou primitivní čtvrté odmocniny z jedné.

Připomeňme si zápis komplexního čísla v exponenciálním a goniometrickém tvaru. Definujme číslo ζ_n jako $\zeta_n = e^{\frac{2\pi i}{n}} = \cos(\frac{2\pi}{n}) + i\sin(\frac{2\pi}{n})$. Jistě $\zeta_n \in \mathcal{M}_n$, jelikož $\zeta_n^n = e^{2\pi i} = 1$. Navíc pro každé $k \in \mathbb{N}$, $1 \leq k \leq n$, jistě platí $\zeta^k \in \mathcal{M}_n$. Zřejmě také pro každé $i, j \in \{1, 2, ...n\}$, $i \neq j$, platí $\zeta_n^i \neq \zeta_n^j$. Z toho plynou dva poznatky: zaprvé, pro každé $n \in \mathbb{N}$ existuje alespoň jedna primitivní n-tá odmocnina z jedné, a to ζ_n; zadruhé $\mathcal{M}_n = \{\zeta_n, \zeta_n^2, ..., \zeta_n^n\}$.

O primitivních n-tých odmocninách můžeme říct následující:

Lemma 3.3.2. *Nechť $k \in \mathbb{Z}$, $1 \leq k < n$. Prvek ζ_n^k je primitivní n-tá odmocnina z jedné, právě když* $\mathrm{nsd}(k,n) = 1$.

Důkaz. Pokud $\mathrm{nsd}(k,n) = d > 1$, tak $\frac{k}{n} = \frac{q}{p}$, kde $p = \frac{n}{d} < n$, $q = \frac{k}{d} < k$ jsou nesoudělná celá čísla. Potom $(\zeta_n^k)^p = e^{\frac{2\pi i}{n} \cdot kp} = e^{2\pi i \cdot q} = 1^q = 1$, tedy ζ_n^k je p-tá odmocnina z jedné. Jelikož $p < n$, tak ζ_n^k není primitivní n-tá odmocnina z jedné.

Pokud $\mathrm{nsd}(k,n) = 1$, tak pro každé $a \in \mathbb{Z}$, $1 \leq a < n$ dostáváme $(\zeta_n^k)^a = e^{\frac{2\pi i}{n} \cdot ka}$. Uvědomme si, že se tento výraz rovná jedné, právě když $\frac{ak}{n} \in \mathbb{Z}$; to je zřejmé. Ale jelikož $\mathrm{nsd}(k,n) = 1$ a $a < n$, ζ_n^k pro žádné $a < n$ není a-tá odmocnina z jedné. Z definice je to tedy primitivní n-tá odmocnina z jedné.

□

Máme tedy právě $\varphi(n)$ primitivních n-tých odmocnin z jedné, kde φ je Eulerova funkce.

Není těžké ukázat následující větu:

Věta 3.3.3. *Množina $\mathcal{M}_n$ tvoří pro každé n spolu s operací násobení grupu. Tato grupa je dokonce cyklická a jejím generátorem je libovolná primitivní n-tá odmocnina z jedné.*

Důkaz. Nejprve je třeba ukázat, že násobení je operace na množině $\mathcal{M}_n$. Nechť $\alpha, \beta \in \mathcal{M}_n$. Pak $(\alpha \cdot \beta)^n - 1 = \alpha^n \cdot \beta^n - 1 = 1 \cdot 1 - 1 = 0$, tj. pro libovolné prvky $\mathcal{M}_n$ leží v této množině i jejich součin, což jsme chtěli dokázat.

Asociativita operace násobení je zřejmá, v množině leží i neutrální prvek, jímž je prvek 1. Navíc pro libovolné komplexní číslo ζ platí $1 = (\zeta \cdot \zeta^{-1})^n = \zeta^n \cdot (\zeta^{-1})^n$, tedy pokud $\zeta \in \mathcal{M}_n$, tak v této množině leží i inverzní prvek k ζ. Tím jsme dokázali, že $(\mathcal{M}_n, \cdot)$ je grupa.

Nyní ukážeme, že $\mathcal{M}_n$ s násobením je dokonce cyklická. Jelikož $|\mathcal{M}_n| = 1$, chceme nalézt prvek řádu n. Tím je ale z definice libovolná primitivní n-tá odmocnina z jedné. Důkaz je tedy hotov, jestliže pro každé n alespoň jedna primitivní n-tá odmocnina existuje. Výše jsme ale ukázali, že ano, totiž číslo ζ_n.

□

V případě $n = 4$ máme $\zeta_4 = i$ a vskutku vidíme $i^1 = 1, i^2 = -1, i^3 = -i, i^4 = 1$, stejně tak $(-i)^1 = -i, (-i)^2 = -1, (-i)^3 = i, (-i)^4 = 1$.

Nyní můžeme definovat n-té kruhové těleso.

Definice 3.3.4. *Nechť $n \in \mathbb{N}$, $\zeta_n = e^{\frac{2\pi i}{n}}$ je primitivní n-tá odmocnina z jedné. Pak tělesu $\mathbb{Q}(\zeta_n)$ říkáme n-té kruhové těleso.*

Hovoříme-li tedy o kruhovém tělese, je řeč o nějakém jednoduchém rozšíření racionálních čísel. Můžeme uvést některé příklady: první i druhé kruhové těleso je rovno $\mathbb{Q}$, čtvrté kruhové těleso je $\mathbb{Q}(i)$, osmé kruhové těleso je tvaru $\mathbb{Q}(\frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}) = \mathbb{Q}(i, \sqrt{2})$.

Jednoduše lze ukázat důležité tvrzení:

Věta 3.3.5. *Rozšíření $\mathbb{Q} \subseteq \mathbb{Q}(\zeta_n)$ je Galoisovo.*

Důkaz. Jelikož $\zeta_n \in \mathbb{Q}(\zeta_n)$, tak podle věty 3.3.3 $\mathcal{M}_n \in \mathbb{Q}(\zeta_n)$. Polynom $x^n - 1$ se tedy v $\mathbb{Q}(\zeta_n)$ rozkládá na součin lineárních činitelů a jelikož $\mathbb{Q}(\zeta_n)$ je nejmenší těleso obsahující $\mathbb{Q}$ a ζ_n, je to rozkladové těleso tohoto polynomu. Jelikož se jedná o separabilní polynom, tvrzení je dokázáno.

□

Předchozí větu jsme dokázali, aniž bychom explicitně znali minimální polynom $f(x)$ prvku ζ_n nad $\mathbb{Q}$. Lze však ukázat, že $f(x)$ je ve skutečnosti tzv. *n-tý kruhový polynom*, jenž je tvaru

$$\Phi_n(x) = \prod_{\substack{1 \leq k < n \\ \mathrm{nsd}(n,k)=1}} (x - \zeta_n^k).$$

Vidíme, že je to polynom stupně $\varphi(n)$, kde φ je Eulerova funkce, tedy dostáváme $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)$. Je možné ukázat, že n-tý kruhový polynom má vždy nejen racionální, ale dokonce i celočíselné koeficienty, což se bude hodit v další kapitole.

Další užitečná informace je, že kruhová tělesa jsou až na jeden případ navzájem různá. Obecně lze ukázat, že pro dvě různá přirozená čísla $m < n$ jsou tělesa $\mathbb{Q}(\zeta_m)$ a $\mathbb{Q}(\zeta_n)$ stejná, právě když je m liché a $n = 2m$. Příkladem mohou být tělesa $\mathbb{Q}(\zeta_3)$ a $\mathbb{Q}(\zeta_6)$. Jelikož $\zeta_3 = \cos(\frac{2\pi}{3}) + i\sin(\frac{2\pi}{3}) = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$, dostáváme $\mathbb{Q}(\zeta_3) = \mathbb{Q}(i\sqrt{3})$. Stejně tak ale jelikož $\zeta_6 = \frac{1}{2} + i\frac{\sqrt{3}}{2}$, tak $\mathbb{Q}(\zeta_6) = \mathbb{Q}(i\sqrt{3}) = \mathbb{Q}(\zeta_3)$.

Kruhová tělesa jsou velmi významným objektem s rozsáhlou teorií i mnoha aplikacemi, na něž v této práci bohužel není mnoho místa (mnohem, mnohem více je možno se dozvědět ve [7]). Přesto je na místě zmínit alespoň pár zajímavostí. Věta Kroneckera a Webera říká, že pro každé konečné abelovské rozšíření $\mathbb{Q} \subseteq K$ – tzn. je to konečné Galoisovo rozšíření s komutativní Galoisovou grupou – je K podtěleso některého kruhového tělesa. Jedná se o velmi hluboký výsledek algebraické teorie čísel. Kruhová tělesa tělesa hrají také významnou roli v důkazech dvou známých tvrzení. Prvním z nich je Velká Fermatova věta, která říká, že pro přirozená n větší než 2 rovnice $x^n + y^n = z^n$ nemá celočíselná řešení. Větu je možno díky kruhovým tělesům dokázat pro velkou skupinu prvočísel, bohužel nekonečně mnoho dalších prvočísel odolávalo celkem takřka 350 let. Druhým z nich je Catalanova domněnka, která říká, že jediné celočíselné řešení rovnice $x^a - y^b = 1$ pro $a, b > 1, x, y > 0$ je tvaru $3^2 - 2^3 = 1$. Kompletní důkaz tohoto tvrzení z roku 2002 používá některé hluboké výsledky teorie kruhových těles.

Nám však bude z teorie kruhových těles stačit pouze několik informací, a to především popis Galoisovy grupy $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$. Víme, že prvky této grupy jsou automorfismy tělesa $\mathbb{Q}(\zeta_n)$ fixující $\mathbb{Q}$, a tedy každý z nich zobrazí ζ_n na některý z kořenů minimálního polynomu prvku ζ_n nad tělesem $\mathbb{Q}$. Tím je Φ_n a jeho kořeny jsou tvaru ζ_n^k pro $k \in \mathbb{N}$, $1 \leq k \leq n$, $\mathrm{nsd}(n,k) = 1$. Pro všechna taková k označme σ_k automorfismus takový, že $\sigma_k(\zeta_n) = \zeta_n^k$.

Za těchto předpokladů můžeme vyslovit následující větu:

Věta 3.3.6. *Nechť $\mathbb{Q}(\zeta_n)$ je n-té kruhové těleso. Pak*

$$\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^*,$$

tedy Galoisova grupa rozšíření $\mathbb{Q} \subseteq \mathbb{Q}(\zeta_n)$ je izomorfní s multiplikativní grupou jednotek okruhu $\mathbb{Z}/n\mathbb{Z}$. Izomorfismus $\phi : (\mathbb{Z}/n\mathbb{Z})^* \to \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ je dán předpisem $[k]_n \mapsto \sigma_k$ pro všechna $k \in \mathbb{N}$, $1 \leq k \leq n$, $\mathrm{nsd}(n,k) = 1$.

Důkaz. Jelikož prvky množiny $(\mathbb{Z}/n\mathbb{Z})^*$ jsou právě zbytkové třídy modulo n tvaru $[k]_n$ pro všechna $k \in \mathbb{N}$, $1 \leq k \leq n$, $\mathrm{nsd}(n,k) = 1$, je $[k]_n \mapsto \sigma_k$ bijekce. Zbývá ukázat, že je to homomorfismus. Platí $\phi([a]_n) \circ \phi([b]_n) = \sigma_a \circ \sigma_b$ ($\circ$ značí operaci skládání automorfismů). Ale $(\sigma_a \circ \sigma_b)(\zeta_n) = \sigma_a(\sigma_b(\zeta_n)) = \sigma_a(\zeta_n^b) = (\sigma_a(\zeta_n))^b = (\zeta_n^a)^b = \zeta_n^{ab} = \sigma_{ab}(\zeta_n)$, tedy $\sigma_a \circ \sigma_b = \sigma_{ab}$. Z toho dostáváme $\phi([a]_n) \circ \phi([b]_n) = \phi([ab]_n)$, tedy ϕ je opravdu homomorfismus a důkaz je hotov.

□

Galoisovu grupu rozšíření $\mathbb{Q} \subseteq \mathbb{Q}(\zeta_n)$ tedy můžeme popsat pomocí objektu, který je nám dobře známý. Tedy například $\mathrm{Gal}(\mathbb{Q}(\zeta_8)/\mathbb{Q})$ je izomorfní s grupou $(\mathbb{Z}/8\mathbb{Z})^*$. Ta se skládá ze tří prvků řádu dva a neutrálního prvku, je tedy izomorfní s grupou $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. To odpovídá poznatku, že $\mathbb{Q}(\zeta_8)$ je vlastně bikvadratické těleso $\mathbb{Q}(i, \sqrt{2})$.

Poznámka 3.3.1. Zajímavá situace nastává, pokud uvažujeme těleso $\mathbb{Q}(\zeta_p)$, kde p je liché prvočíslo. Dostáváme totiž $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \cong (\mathbb{Z}/p\mathbb{Z})^*$, což je cyklická grupa řádu $p-1$. Pomocí teorie grup umíme popsat veškeré její podgrupy: pro každé kladné d, které dělí $p-1$, máme právě jednu podgrupu H_d indexu d (tj. $|(\mathbb{Z}/p\mathbb{Z})^*/H_d| = d$). Navíc $H_{d_1} \subseteq H_{d_2}$, právě když $d_1 \mid d_2$. Vzhledem k hlavní větě Galoisovy teorie tedy vidíme, že mezitělesa rozšíření $\mathbb{Q} \subseteq \mathbb{Q}(\zeta_p)$ jsou tvaru $F_d = \mathrm{Fix}(H_d)$ (např. $F_1 = \mathbb{Q}, F_{p-1} = \mathbb{Q}(\zeta_p)$) a navíc $F_{d_1} \subseteq F_{d_2}$, právě když $d_1 \mid d_2$.

Jelikož $p-1$ je sudé, jedno z mezitěles rozšíření $\mathbb{Q} \subseteq \mathbb{Q}(\zeta_p)$ je kvadratické těleso. Následující věta říká, jakého je tvaru:

Věta 3.3.7. *Nechť p je liché prvočíslo. Pak p-té kruhové těleso obsahuje kvadratické těleso $\mathbb{Q}(\sqrt{p^*})$ kde $p^* = (-1)^{\frac{p-1}{2}}$.*

Toto tvrzení, které se nám podaří dokázat v části 6.2, bude hrát významnou roli v důkazu zákona kvadratické reciprocity.

V této kapitole jsme se seznámili s Galoisovou teorií, od jejího vybudování přes hlavní větu až po některé aplikace; nakonec jsme si ukázali některé vlastnosti kruhových těles. Galoisovu teorii budeme potřebovat v další kapitole, abychom ji aplikovali na prvoideály jistých algebraických rozšíření racionálních čísel a zavedli pojem dekompoziční grupa – což není nic jiného než podgrupa Galoisovy grupy. Kruhová tělesa a dekompoziční grupu nakonec využijeme k důkazu zákona kvadratické reciprocity.

Kapitola 4

Algebraická teorie čísel

Když v roce 1637 slavný matematik Pierre de Fermat uveřejnil svoji domněnku, že rovnice $x^n + y^n = z^n, x, y, z, n \in \mathbb{N}$ nemá řešení, nevěděl, že tím nastoluje budoucím generacím matematiků problém, který budou řešit přes 350 let. Snaha dokázat Fermatovu domněnku, dnes známou pod názvem Velká Fermatova věta, položila základ celého nového odvětví matematiky – algebraické teorie čísel. Tato oblast je v dnešní době velice rozvinutá a má mnoho zajímavých aplikací – dnes především v kryptografii.

V následujícím textu se seznámíme se základy algebraické teorie čísel a po jejich vybudování se budeme dále zabývat rozkladem ideálů v číselných tělesech. Na naše výsledky pak budeme aplikovat Galoisovu teorii.

4.1 Číselná tělesa a množina $\mathcal{O}_K$

Jak podle názvu nepřekvapí, algebraická teorie čísel pracuje převážně s algebraickými čísly, a to nad tělesem racionálních čísel. Proto pokud nebude řečeno jinak, v následujícím textu bude pod pojmem algebraické číslo myšleno číslo algebraické nad $\mathbb{Q}$.

Tělesa algebraických čísel, jež nás budou zajímat, nazýváme *číselná tělesa*:

Definice 4.1.1. *Nechť K je konečné (a tedy i algebraické) rozšíření racionálních čísel. Pak říkáme, že K je číselné těleso.*

Nyní nás bude zajímat jistá podmnožina algebraických čísel, které říkáme *celá algebraická čísla*:

Definice 4.1.2. *Nechť $\alpha \in \mathbb{C}$. Řekneme, že α je celé algebraické číslo, pokud je kořenem nějakého normovaného polynomu s celočíselnými koeficienty.*

Příkladem celých algebraických čísel mohou být například čísla tvaru $\sqrt{m}$ pro všechna $m \in \mathbb{Z}$, dále například číslo $\zeta_n = e^{\frac{2\pi i}{n}}$ definované v předchozí kapitole (je vždy kořenem normovaného polynomu $x^n - 1 \in \mathbb{Z}[x]$). Obecně je určitě každé celé algebraické číslo zároveň algebraické. Naopak to ale být nemusí, jak si ukážeme na následujícím příkladě:

Příklad 4.1.1. Ukažte, že číslo $\frac{\sqrt{3}}{2}$ je algebraické, ale není celé algebraické.

Jedná se o algebraické číslo, jelikož je kořenem polynomu $x^2 - \frac{3}{4}$. Ukážeme sporem, že celé algebraické číslo to není. Předpokládejme tedy, že ano, tedy existuje polynom

$$f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0; a_0, ..., a_{n-1} \in \mathbb{Z}$$

takový, že $f(\frac{3}{4}) = 0$. Platí tedy $(\frac{\sqrt{3}}{2})^n + a_{n-1}(\frac{\sqrt{3}}{2})^{n-1} + \cdots + a_1(\frac{\sqrt{3}}{2}) + a_0 = 0$. Vynásobíme rovnost číslem 2^n, abychom na levé straně dostali celočíselné koeficienty:

$$(\sqrt{3})^n + 2a_{n-1}(\sqrt{3})^{n-1} + \cdots + 2^{n-1}a_1(\sqrt{3}) + 2^n a_0 = 0.$$

Tím dostáváme rovnost (pokud položíme $a_n = 1$) $A + B\sqrt{3} = 0$, kde

$$A = \sum_{\substack{i=0 \\ i \text{ je sudé}}}^{n} (\sqrt{3})^i a_i 2^{n-i} \in \mathbb{Z},$$

$$B = \sum_{\substack{i=0 \\ i \text{ je liché}}}^{n} (\sqrt{3})^{i-1} a_i 2^{n-i} \in \mathbb{Z}\,.$$

Jelikož prvky $1, \sqrt{3}$ jsou lineárně nezávislé nad $\mathbb{Q}$, dostáváme $A = B = 0$. Nyní si vybereme jedno z čísel A, B podle parity n a demonstrujeme spor. Pokud je n sudé, tak z $2 \mid 0 = A$ dostáváme $2|(\sqrt{3})^n a_n 2^{n-n} = 3^{\frac{n}{2}}$ (jelikož ostatní sčítance jsou sudé), což je spor. V případě, kdy je n liché, dostaneme obdobně spor na základě rovnosti $B = 0$.

U algebraických čísel jsme ukázali, že jsou nejen kořenem nějakého polynomu z $\mathbb{Q}[x]$, ale vždy i nějakého normovaného a ireducibilního polynomu nad $\mathbb{Q}$ (tím je minimální polynom). I u celých algebraických čísel lze ukázat, že jsou vždy kořenem nějakého normovaného ireducibilního polynomu s celočíselnými koeficienty, tj. že jejich minimální polynom vždy leží v $\mathbb{Z}[x]$. Plyne to okamžitě z následujícího lemmatu:

Lemma 4.1.3. *Nechť $h \in \mathbb{Z}[x], f, g \in \mathbb{Q}[x]$ jsou normované polynomy a $h = fg$. Pak mají f i g celočíselné koeficienty.*

Důkaz. Označme m (resp. n) nejmenší přirozené číslo takové, že mf (resp. ng) má celočíselné koeficienty. To znamená, že neexistuje prvočíslo, které by dělilo všechny koeficienty polynomu mf nebo ng. Ukážeme sporem, že $m = n = 1$.

Předpokládejme, že to neplatí, tj. existuje prvočíslo p, které dělí mn. Jelikož $mnh = mf \cdot ng$ je rovnost polynomů v $\mathbb{Z}[x]$ a p dělí levou stranu, dostáváme $p|mf \cdot ng$ v okruhu $\mathbb{Z}[x]$.

Ukážeme, že v $\mathbb{Z}[x]$ platí totéž, co v $\mathbb{Z}$, tedy pokud prvočíslo dělí součin prvků ze $\mathbb{Z}[x]$, dělí alespoň jednoho z činitelů. Předpokládejme, že tomu tak není, tj. existují dva polynomy $h, k \in \mathbb{Z}[x]$ takové, že $p|hk$, ale p nedělí ani h, ani k. Oba polynomy tedy mají koeficienty, které nejsou dělitelné p; zvolme koeficient a (resp. b) polynomu h (resp. k),

který je ze všech toto splňujících koeficientů polynomu h (resp. k) u nejmenší mocniny x; řekněme a je koeficient u x^u a b je koeficient u x^v. Pak je koeficient polynomu hk u x^{u+v} roven součtu hk s několika násobky p, což je číslo, které není dělitelné p. To je spor s tím, že $p|hk$.

Potom tedy jelikož $p|mf \cdot ng$, tak $p|mf$ nebo $p|ng$ v $\mathbb{Z}[x]$. Pak tedy p dělí všechny koeficienty alespoň jednoho z těchto dvou polynomů, což je spor. Dostáváme tedy kýžené $f, g \in \mathbb{Z}[x]$.

□

Např. číslo ζ_n je kořenem normovaného ireducibilního polynomu $\Phi_n(x)$, o němž jsme si řekli, že celočíselné koeficienty má.

Jistě je každé celé algebraické číslo algebraické, ale naopak (jak jsme viděli výše) to neplatí. Platí ale, že pro každé algebraické číslo existuje nějaký jeho celočíselný násobek, který již celý algebraický je:

Věta 4.1.4. *Nechť $\alpha \in \mathbb{C}$ je algebraické číslo. Pak existuje přirozené číslo m takové, že $m\alpha$ je celé algebraické číslo.*

Důkaz. Označme $f(x)$ minimální polynom α nad $\mathbb{Q}$. Jeho koeficienty jsou racionální, můžeme tedy psát

$$f(x) = x^n + \frac{a_{n-1}}{b_{n-1}}x^{n-1} + \cdots + \frac{a_1}{b_1}x + \frac{a_0}{b_0}, a_0, ..., a_{n-1} \in \mathbb{Z}, b_0, ..., b_{n-1} \in \mathbb{N},$$

kde $\mathrm{nsd}(a_i, b_i) = 1$ pro všechna $i \in \{0, 1, ..., n-1\}$.

Uvažujme nyní číslo m, které je nejmenším společným násobkem čísel $b_0, b_1, ..., b_{n-1}$. Vynásobíme-li rovnost

$$\alpha^n + \frac{a_{n-1}}{b_{n-1}}\alpha^{n-1} + \cdots + \frac{a_1}{b_1}\alpha + \frac{a_0}{b_0} = 0$$

číslem m^n, dostaneme

$$(m\alpha)^n + \frac{ma_{n-1}}{b_{n-1}}(m\alpha)^{n-1} + \cdots + \frac{m^{n-1}a_1}{b_1}(m\alpha) + \frac{m^n a_0}{b_0} = 0.$$

Tedy číslo $m\alpha$ je kořenem polynomu

$$x^n + \frac{ma_{n-1}}{b_{n-1}}x^{n-1} + \cdots + \frac{m^{n-1}a_1}{b_1}x + \frac{m^n a_0}{b_0},$$

který je normovaný a má celočíselné koeficienty, protože $b_i|m$ pro všechna $i \in \{0, 1, ..., n-1\}$. Proto je $m\alpha$ celé algebraické číslo.

□

Příkladem může být opět číslo $\frac{\sqrt{3}}{2}$ – viděli jsme, že není celé algebraické, ale vynásobíme-li ho dvojkou, dostaneme číslo $\sqrt{3}$, které celé algebraické je (protože je kořenem polynomu $x^2 - 3$).

Uvažujme těleso $\mathbb{Q}$; jistě je to číselné těleso. Uvažujme množinu C všech celých algebraických čísel v tomto tělese. Minimální polynom libovolného čísla $r \in \mathbb{Q}$ nad $\mathbb{Q}$ je tvaru $x - r$. Jelikož celé algebraické číslo je vždy kořenem nějakého normovaného ireducibilního polynomu s celočíselnými koeficienty, platí, že $r \in C \Leftrightarrow x - r \in \mathbb{Z}[x] \Leftrightarrow r \in \mathbb{Z}$, tedy množina všech celých algebraických čísel tělesa $\mathbb{Q}$ je rovna množině celých čísel. Tvoří tedy okruh.

Předchozí poznatek lze zobecnit na libovolné číselné těleso:

Věta 4.1.5. *Nechť K je číselné těleso. Pak množina celých algebraických čísel tělesa K tvoří spolu s operacemi sčítání a násobení okruh.*

Poznámka 4.1.1. Okruh celých algebraických čísel v tělese K značíme $\mathcal{O}_K$.

Platí navíc následující:

Věta 4.1.6. *Nechť K je číselné těleso. Pak K je podílové těleso okruhu $\mathcal{O}_K$, jinak řečeno:*

$$K = \left\{ \frac{\alpha}{\beta} \mid \alpha, \beta \in \mathcal{O}_K, \beta \neq 0 \right\}.$$

Platnost této věty si můžeme snadno ověřit na příkladu $K = \mathbb{Q}$.

Máme-li dáno nějaké číselné těleso K, většinou není snadné určit, jakého tvaru je množina $\mathcal{O}_K$. Ukážeme si, jak $\mathcal{O}_K$ vypadá v případech, kdy je K kvadratické nebo kruhové těleso, protože s těmito okruhy budeme pracovat nejvíce.

Věta 4.1.7. *Nechť $K = \mathbb{Q}(\sqrt{m})$, kde $m \neq 0, 1$ je celé číslo, které není dělitelné druhou mocninou žádného prvočísla. Potom platí*

$$\mathcal{O}_K = \begin{cases} \mathbb{Z}[\sqrt{m}] = \{a + b\sqrt{m} | a, b \in \mathbb{Z}\} \ \textit{pokud} \ m \equiv 2, 3 \pmod 4, \\ \\ \mathbb{Z}[\frac{1+\sqrt{m}}{2}] = \{\frac{a+b\sqrt{m}}{2} | a, b \in \mathbb{Z}, a \equiv b \pmod 2\} \ \textit{pokud} \ m \equiv 1 \pmod 4. \end{cases}$$

Důkaz předchozí věty není obtížný, ale početně je poměrně zdlouhavý. Důkaz následující věty je již náročnější:

Věta 4.1.8. *Nechť $K = \mathbb{Q}(\zeta_m)$ je m-té kruhové těleso. Potom platí*

$$\mathcal{O}_K = \mathbb{Z}[\zeta_m] = \{a_0 + a_1 \zeta_m + \cdots + a_{\varphi(m)-1} \zeta_m^{\varphi(m)-1} | a_0, a_1, ..., a_{\varphi(m)-1} \in \mathbb{Z}\},$$

kde φ je Eulerova funkce.

To, že se všechny tyto okruhy dají vyjádřit pomocí celých čísel, není náhoda. Obecně lze ukázat následující:

Věta 4.1.9. *Nechť K je číselné těleso, $[K : \mathbb{Q}] = n$. Pak existují prvky $\beta_1, ..., \beta_n \in K$ takové, že $\mathcal{O}_K = \{a_1\beta_1 + \cdots + a_n\beta_n | a_1, ..., a_n \in \mathbb{Z}\}$.*

Definice 4.1.10. *Prvky $\beta_1, ..., \beta_n$ z předchozí věty nazýváme celočíselná báze okruhu $\mathcal{O}_K$.*

Celočíselné báze okruhů z věty 4.1.7 a věty 4.1.8 jsou tedy například $(1, \sqrt{m})$, $(1, \frac{1+\sqrt{m}}{2})$, $(1, \zeta_n, ..., \zeta_n^{\varphi(n)-1})$. Všimněme si, že celočíselná báze okruhu $\mathcal{O}_K$ je vždy zároveň i báze vektorového prostoru K nad $\mathbb{Q}$.

Důležitý pojem vztahující se k číselným tělesům je diskriminant.

Definice 4.1.11. *Nechť K je číselné těleso, $[K/\mathbb{Q}] = n$, $\sigma_1, ..., \sigma_n \in \mathcal{V}(K/\mathbb{Q})$ jsou všechna jeho vnoření do komplexních čísel (každé takovéto vnoření fixuje $\mathbb{Q}$). Pak diskriminant libovolné n-tice $\alpha_1, ..., \alpha_n \in K$ je definován jako $d(\alpha_1, ..., \alpha_n) = (\det(A))^2$, kde*

$$A = (\sigma_i(\alpha_j)) = \begin{pmatrix} \sigma_1(\alpha_1) & \sigma_2(\alpha_1) & \cdots & \sigma_n(\alpha_1) \\ \sigma_1(\alpha_2) & \sigma_2(\alpha_2) & \cdots & \sigma_n(\alpha_2) \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_1(\alpha_n) & \sigma_2(\alpha_n) & \cdots & \sigma_n(\alpha_n) \end{pmatrix}.$$

Diskriminant má mnoho pozoruhodných vlastností. Je roven nule, právě když se daná n-tice skládá s lineárně závislých prvků. Je to vždy racionální číslo a pokud se daná n-tice skládá z celých algebraických čísel, je to dokonce vždy celé číslo. Navíc se ukazuje, že diskriminant může sloužit jako jakýsi invariant okruhu $\mathcal{O}_K$:

Věta 4.1.12. *Nechť K je číselné těleso, $\beta_1, ..., \beta_n$ a $\gamma_1, ..., \gamma_n$ jsou různé celočíselné báze okruhu $\mathcal{O}_K$. Pak $d(\beta_1, ..., \beta_n) = d(\gamma_1, ..., \gamma_n)$.*

Definice 4.1.13. *Nechť K, je číselné těleso. Pak diskriminantem okruhu $\mathcal{O}_K$ – píšeme $d(\mathcal{O}_K)$ – nazveme diskriminant libovolné jeho celočíselné báze.*

Nechť $K = \mathbb{Q}(i)$. Spočítejme diskriminant okruhu $\mathcal{O}_K = \mathbb{Z}[i]$. Celočíselná báze je např. $(1, i)$ a jistě $\mathcal{V}(\mathbb{Q}(i)/\mathbb{Q}) = \{\mathrm{id}, \tau\}$, kde $\tau : a + bi \mapsto a - bi$. Dostáváme tedy

$$d(\mathbb{Z}[i]) = d(1, i) = \begin{vmatrix} \mathrm{id}(1) & \tau(1) \\ \mathrm{id}(i) & \tau(i) \end{vmatrix}^2 = \begin{vmatrix} 1 & 1 \\ i & -i \end{vmatrix}^2 = (1 \cdot (-i) - 1 \cdot i)^2 = (-2i)^2 = -4.$$

Předchozí úvahu můžeme zobecnit na případ $K = \mathbb{Q}(\sqrt{m})$, $m \in \mathbb{Z}$ není dělitelné druhou mocninou žádného prvočísla. Jistě vždy $\mathcal{V}(K/\mathbb{Q}) = \{\mathrm{id}, \sigma\}$, kde $\sigma : a + b\sqrt{m} \mapsto a - b\sqrt{m}$. Pokud $m \equiv 2, 3 \pmod 4$, tak máme celočíselnou bázi $(1, \sqrt{m})$ a dostaneme

$$d(\mathcal{O}_K) = d(1, \sqrt{m}) = \begin{vmatrix} 1 & 1 \\ \sqrt{m} & -\sqrt{m} \end{vmatrix}^2 = (1 \cdot (-\sqrt{m}) - 1 \cdot \sqrt{m})^2 = (-2\sqrt{m})^2 = 4m.$$

Pokud $m \equiv 1 \pmod 4$, máme celočíselnou bázi $(1, \frac{1+\sqrt{m}}{2})$ a obdobně dostáváme $d(\mathcal{O}_K) = m$.

V případě kruhových těles je výpočet diskriminantu komplikovanější, lze však ukázat, že je-li K m-té kruhové těleso, tak $d(\mathcal{O}_K)$ dělí číslo $m^{\varphi(m)}$.

Všechny tyto poznatky můžeme shrnout do následující věty:

Věta 4.1.14. *Informace o některých okruzích celých algebraických čísel a jejich diskriminantech můžeme shrnout do následující tabulky:*

K	$\mathcal{O}_K$	$d(\mathcal{O}_K)$
$\mathbb{Q}$	$\mathbb{Z}$	1
$\mathbb{Q}(\sqrt{m}), m \equiv 2,3 \pmod 4$	$\mathbb{Z}[\sqrt{m}]$	$4m$
$\mathbb{Q}(\sqrt{m}), m \equiv 1 \pmod 4$	$\mathbb{Z}[\frac{1+\sqrt{m}}{2}]$	m
$\mathbb{Q}(\zeta_m)$	$\mathbb{Z}[\zeta_m]$	$d, d \mid m^{\varphi(m)}$

Diskriminant je velmi silný nástroj při dokazování tvrzení z elementární algebraické teorie čísel. V práci ho budeme dále potřebovat, až budeme studovat větvení prvoidálů v rozšířeních číselných těles.

Na závěr této části uvedeme jedno tvrzení, které se může jevit jako poněkud překvapivé:

Věta 4.1.15. *Nechť K je číselné těleso. Pak $K = \mathbb{Q}(\alpha)$ pro vhodné $\alpha \in K$.*

Každé číselné těleso je tedy ve skutečnosti jednoduché rozšíření racionálních čísel! Důkaz tohoto tvrzení využívá matematické indukce a některých vlastností minimálního polynomu. Příkladem může být nám již známá rovnost $\mathbb{Q}(i, \sqrt{2}) = \mathbb{Q}(\zeta_8) = \mathbb{Q}(\frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2})$.

Nyní se přesuneme k dalšímu významnému aspektu okruhu $\mathcal{O}_K$, a to k vlastnostem jeho ideálů.

4.2 Ideály $\mathcal{O}_K$ a nejednoznačnost rozkladu

V této části se seznámíme se dvěma důležitými pojmy, jimiž jsou těleso zbytků a Dedekindův okruh.

Nechť $\mathcal{P}$ je vlastní prvoideál okruhu $\mathcal{P}$. Víme, že $\mathcal{P} = p\mathbb{Z}$ pro nějaké prvočíslo p. Z elementární teorie čísel víme, že $\mathbb{Z}/\mathcal{P} = \mathbb{Z}/p\mathbb{Z}$ je konečný faktorokruh; dokonce těleso, jelikož vlastní prvoideály jsou v okruhu $\mathbb{Z}$ také maximálními ideály. Skutečnost, že dva prvky $a, b \in \mathbb{Z}$ leží ve stejné třídě tohoto faktorokruhu, tedy že $a - b \in p\mathbb{Z}$, pak značíme $a \equiv b \pmod p$.

Tyto poznatky lze zobecnit na libovolný okruh $\mathcal{O}_K$ celých algebraických čísel číselného tělesa K. Je-li $\mathcal{P}$ libovolný vlastní ideál $\mathcal{O}_K$, pak lze ukázat, že faktorokruh $\mathcal{O}_K/\mathcal{P}$ je konečný (dále uvidíme, že je to opět dokonce těleso). Leží-li dva prvky $a, b \in \mathcal{O}_K$ ve stejné třídě v tomto faktorokruhu, pak píšeme $a \equiv b \pmod{\mathcal{P}}$.

Za těchto podmínek můžeme zformulovat následující definici:

Definice 4.2.1. *Nechť K je číselné těleso, $\mathcal{P}$ je vlastní prvoideál okruhu $\mathcal{O}_K$. Pak faktorokruh $\mathcal{O}_K / \mathcal{P}$ nazýváme těleso zbytků.*

Jde opravdu o těleso; sice aby $\mathcal{O}_K / \mathcal{P}$ bylo těleso, musí být prvoideál $\mathcal{P}$ maximální, o něco níže však uvidíme, že tomu tak v okruhu $\mathcal{O}_K$ vždy je.

Nyní se přesuňme k nejednoznačnosti rozkladu. Připomeňme, že v libovolném komutativním okruhu R můžeme zavést koncept dělitelnosti: $a \in R$ dělí $b \in R$ (značíme $a|b$), pokud existuje $k \in R$ takové, že $b = ak$. Prvkům $a, b \in R$ říkáme, že jsou asociované, pokud $a|b$ a zároveň $b|a$. Je-li R obor integrity, je předchozí definice ekvivalentní s tím, že $a = ub$, kde u je nějaká jednotka okruhu R (např. v $\mathbb{Z}$ jsou prvky m a $-m$ asociované, v $\mathbb{Z}[i]$ jsou asociované prvky $z, -z, iz, -iz$).

Důležitý pojem související s dělitelností je okruh s jednoznačným rozkladem. Připomeňme, že se jedná o obor integrity, v němž lze každý prvek, který není nula nebo jednotka, skoro jednoznačně rozložit na součin ireducibilních prvků (a je ireducibilní, pokud to není nula nebo jednotka a jeho jediní dělitelé jsou jednotky a prvky asociované s a). Slovy „skoro jednoznačně“ je míněno to, že počet činitelů je vždy stejný a při jejich zápisu dvou různých rozkladů ve vhodném pořadí je k-tý činitel prvního asociovaný s k-tým činitelem druhého (pro každé možné k).

$\mathcal{O}_K$ však vždy okruhem s jednoznačným rozkladem být nemusí. Někdy tomu tak je – např. u celých čísel nebo u kruhových těles $\mathbb{Q}(\zeta_p)$, kde p je prvočíslo menší nebo rovno dvaceti třem. Bohužel v nekonečně mnoha případech tomu tak není. Příkladem může být např. okruh $\mathcal{O}_{\mathbb{Q}(\sqrt{-5})} = \mathbb{Z}[\sqrt{-5}]$: platí $6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$, což jsou dva rozklady na neasociované ireducibilní prvky okruhu $\mathbb{Z}[\sqrt{-5}]$.

Abychom se mohli zabývat rozkladem na prvoideály, definujme nejprve součet a součin ideálů:

Definice 4.2.2. *Nechť $\mathcal{I}, \mathcal{J}$ jsou ideály komutativního okruhu R. Pak definujeme jejich součet a součin následovně:*

$$\mathcal{I} + \mathcal{J} = \{a + b | a \in \mathcal{I}, b \in \mathcal{J}\},$$

$$\mathcal{I} \cdot \mathcal{J} = \left\{ \sum_{i=1}^{n} a_i b_i | n \in \mathbb{N}, a_i \in \mathcal{I}, b_i \in \mathcal{J} \right\},$$

tj. součin ideálů je množina všech konečných součtů, kde jednotlivými sčítanci jsou součiny prvku jednoho ideálu s prvkem druhého ideálu.

Všimněme si hned, že $\mathcal{I} + \mathcal{J}$ i $\mathcal{I} \cdot \mathcal{J}$ jsou také ideály okruhu R Součin ideálů $\mathcal{I}$ a $\mathcal{J}$ je nejmenší ideál obsahující všechny součiny prvků z $\mathcal{I}$ s prvky z $\mathcal{J}$.

Vzhledem k tomu, že sčítání a násobení ideálů je velmi důležité, zdržíme se u něj formou několika příkladů.

Příklad 4.2.1. Spočítejte součet $\mathcal{I}$ a součin $\mathcal{J}$ ideálů (2) a (3) okruhu $\mathbb{Z}$.

Jelikož $\mathcal{I} = (2) + (3) = \{a + b | a \in (2), b \in (3)\}$, dostáváme $1 = -2 + 3 \in \mathcal{I}$, tedy $\mathcal{I} = \mathbb{Z}$. Spočítejme součin těchto ideálů:

$$\mathcal{J} = (2)\cdot(3) = \left\{ \sum_{i=1}^{n} a_i b_i | n \in \mathbb{N}, a_i \in (2), b_i \in (3) \right\} = \left\{ \sum_{i=1}^{n} 2a_i' \cdot 3b_i' | n \in \mathbb{N}, a_i', b_i' \in \mathbb{Z} \right\} = (6).$$

Příklad 4.2.2. Nechť R je komutativní obor integrity, který je dokonce euklidovský, $\mathbb{Z} \subseteq R$, $a, b, c, d \in R$, $m, n \in \mathbb{Z}$. Dokažte následující:

1. $(a) \cdot (b) = (ab)$,
2. $(a) = (b) \Leftrightarrow a = ub$, kde u je nějaká jednotka okruhu R,
3. $(m) + (n) = (d)$, kde $d = \mathrm{nsd}(m, n)$,
4. $(a, b) \cdot (c, d) = (ac, ad, bc, bd)$, kde $(a, b) = aR + bR$ je ideál generovaný prvky a a b.

První část dokážeme zobecněním výpočtu v předchozím příkladu:

$$(a) \cdot (b) = \left\{ \sum_{i=1}^{n} a_i b_i | n \in \mathbb{N}, a_i \in (a), b_i \in (b) \right\} = \left\{ \sum_{i=1}^{n} aa_i' \cdot bb_i' | n \in \mathbb{N}, a_i', b_i' \in \mathbb{Z} \right\} = (ab).$$

Důkaz druhé části využívá vlastnosti asociovaných prvků. Jelikož $a \in (b)$, tak $a = bk$ pro nějaké $k \in R$, tedy $b|a$. Zároveň ale jelikož $b \in (a)$, tak $a|b$. Takováto situace nastává, právě když jsou prvky a a b asociované, tj. $a = ub$ pro nějakou jednotku u (jelikož se pohybujeme v oboru integrity). Naopak, pokud $a = ub$, tak je rovnost $(a) = (b)$ zřejmá.

Třetí část dokážeme pomocí Bezoutovy rovnosti (tu můžeme použít, jelikož se pohybujeme v euklidovském okruhu). Podle ní jelikož $d = \mathrm{nsd}(m, n)$, tak existují celá čísla u, v taková, že $um+vn = d$. Jelikož $\mathbb{Z} \in R$, tak $um \in (m)$ a $vn \in (n)$, tj. $d = um+vn \in (m)+(n)$ a proto $(d) \subseteq (m)+(n)$. Navíc jelikož $d|m$ a $d|n$, tak každý prvek ideálu $(m)+(n)$ je násobkem čísla d, tedy $(m) + (n) \subseteq (d)$. Proto $(m) + (n) = (d)$.

Čtvrtá část plyne přímo z definice součinu:

$$\begin{aligned}
(a, b) \cdot (c, d) &= \{ak + bl | k, l \in R\} \cdot \{ck' + dl' | k', l' \in R\} \\
&= \{\textstyle\sum_{i=1}^{n} (ak_i + bl_i)(ck_i' + dl_i') | k_i, l_i, k_i', l_i' \in R\} \\
&= \{\textstyle\sum_{i=1}^{n} (ack_ik_i' + adk_il_i' + bcl_ik_i' + bdl_il_i' | k_i, l_i, k_i', l_i' \in R\} \\
&= \{ac \textstyle\sum_{i=1}^{n} k_ik_i' + ad \sum_{i=1}^{n} k_il_i' + bc \sum_{i=1}^{n} l_ik_i' + bd \sum_{i=1}^{n} l_il_i' | k_i, l_i, k_i', l_i' \in R\} \\
&= \{acK + adL + bcK' + bdL' | K, L, K', L' \in R\} \\
&= (ac, ad, bc, bd).
\end{aligned}$$

Všimněme si, že násobení ideálů je komutativní a asociativní. Navíc zde existuje neutrální prvek – tím je sám okruh R, protože přímo z definice ideálu vidíme, že $\mathcal{I} \cdot R = R \cdot \mathcal{I} = \mathcal{I}$.

Vzápětí uvidíme, proč je pro nás násobení ideálů tak důležité. Sice totiž $\mathcal{O}_K$ vždy nemusí být okruh s jednoznačným rozkladem, ale vždy je to tzv. *Dedekindův okruh*, tzn. vyhovuje následující definici:

Definice 4.2.3. *Nechť R je obor integrity. Říkáme, že R je Dedekindův okruh, pokud splňuje následující tři podmínky:*

1. *každý ideál okruhu R je konečně generovaný,*
2. *každý vlastní prvoideál okruhu R je zároveň maximální ideál,*
3. *R je celouzavřený ve svém podílovém tělese K.*

Poslední podmínka říká, že pokud je libovolný prvek $\alpha \in K$ kořenem normovaného polynomu z $R[x]$, tak $\alpha \in R$. Ilustrovat to můžeme příkladem $K = \mathbb{Q}, R = \mathbb{Z}$: pokud je $a \in \mathbb{Q}$ kořenem normovaného polynomu v $\mathbb{Z}[x]$, je to celé algebraické číslo, tj. $a \in \mathbb{Z}$.

Zavedli jsme násobení ideálů, můžeme tedy zavést i dělitelnost ideálů. Tedy $\mathcal{I} \mid \mathcal{J}$, pokud existuje ideál $\mathcal{A}$ takový, že $\mathcal{J} = \mathcal{A}\mathcal{I}$. O dělitelnosti ideálů v Dedekindových okruzích platí následující věta:

Věta 4.2.4. *Nechť $\mathcal{I}, \mathcal{J}$ jsou ideály komutativního okruhu. Pak $\mathcal{I} \mid \mathcal{J}$, právě když $\mathcal{J} \subseteq \mathcal{I}$.*

Důkaz. Dokážeme pouze implikaci „⇒“, jelikož důkaz druhé implikace je poměrně náročný. Předpokládejme tedy, že $\mathcal{I} \mid \mathcal{J}$, tedy z definice existuje ideál $\mathcal{A}$ takový, že $\mathcal{J} = \mathcal{A}\mathcal{I}$.

Uvažujme libovolný prvek $\xi \in \mathcal{J}$. Jelikož $\xi \in \mathcal{A}\mathcal{I}$, tak platí $\xi = \sum_{i=1}^{n} a_i\gamma_i$, kde $a_i \in \mathcal{A}$ a $\gamma_i \in \mathcal{I}$. Ale z definice ideálu $a_i\gamma_i \in \mathcal{I}$ a pak i $\xi = \sum_{i=1}^{n} a_i\gamma_i \in \mathcal{I}$. Tedy $\mathcal{J} \subseteq \mathcal{I}$.

□

Velmi podstatná je pro nás následující věta:

Věta 4.2.5. *Nechť K je číselné těleso. Pak $\mathcal{O}_K$ je Dedekindův okruh.*

Díky tomuto faktu jsme zaprvé obhájili korektnost definice 4.2.1 a zadruhé je zachráněna jednoznačnost rozkladu, jelikož platí následující věta:

Věta 4.2.6. *Nechť R je Dedekindův okruh, $\mathcal{I}$ je libovolný vlastní ideál okruhu R. Pak můžeme $\mathcal{I}$ rozložit na součin prvoideálů, tedy*

$$\mathcal{I} = \mathcal{P}_1^{e_1} \cdot \ \cdots \ \cdot \mathcal{P}_n^{e_n},$$

kde $\mathcal{P}_i$ jsou navzájem různé prvoideály okruhu R a $e_1, ..., e_n \in \mathbb{N}$. Tento rozklad je navíc až na pořadí činitelů jednoznačný.

Nemůžeme tedy vždy jednoznačně rozložit čísla na součin ireducibilních prvků, ale v každém Dedekindově okruhu můžeme jednoznačně rozložit ideály na součin prvoideálů.

Příklad 4.2.3. Ukázali jsme si, že šestku nemůžeme v okruhu $\mathcal{O}_{\mathbb{Q}(\sqrt{-5})} = \mathbb{Z}[\sqrt{-5}]$ jednoznačně rozložit, jelikož $6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$. Pomocí ideálů si však s nejednoznačností snadno poradíme, provedeme totiž rozklad všech činitelů na prvoideály, který je následující:

$$(2) = (2, 1 + \sqrt{-5})^2,$$

$$(3) = (3, 1-\sqrt{-5}) \cdot (3, 1+\sqrt{-5}),$$
$$(1+\sqrt{-5}) = (2, 1+\sqrt{-5}) \cdot (3, 1+\sqrt{-5}),$$
$$(1-\sqrt{-5}) = (2, 1+\sqrt{-5}) \cdot (3, 1-\sqrt{-5}).$$

Tedy $(6) = (2)\cdot(3) = (2, 1+\sqrt{-5})^2 \cdot (3, 1-\sqrt{-5}) \cdot (3, 1+\sqrt{-5}) = (1+\sqrt{-5}) \cdot (1-\sqrt{-5})$.

Nebudeme se nyní zabývat tím, proč jsou prvoideály právě takové; to uvidíme v příští části. Ověřme si ale, že rovnosti výše platí a že se jedná opravdu o prvoideály. Nebudeme se však zabývat všemi případy, protože postupy jsou analogické.

Ověřme platnost rovnosti $(3) = (3, 1-\sqrt{-5}) \cdot (3, 1+\sqrt{-5})$. Počítejme (využíváme část 4 příkladu 4.2.2):

$$\begin{aligned}(3, 1-\sqrt{-5}) \cdot (3, 1+\sqrt{-5}) &= (3 \cdot 3, 3(1+\sqrt{-5}), 3(1-\sqrt{-5}), (1+\sqrt{-5})(1-\sqrt{-5})) \\ &= (9, 3(1+\sqrt{-5}), 3(1-\sqrt{-5}), 6) \\ &= (3).\end{aligned}$$

Ukažme, že $(2, 1+\sqrt{-5})$ je prvoideál. Uvažujme zobrazení $f : \mathbb{Z}[\sqrt{-5}] \to \mathbb{Z}/2\mathbb{Z}$ dané takto: $f(a+b\sqrt{-5}) = [a-b]_2$ pro všechna $a, b \in \mathbb{Z}$. Ukažme, že je to homomorfismus. Jistě $f(1) = [1]_2$. Dále $f(a+b\sqrt{-5}) + f(a'+b'\sqrt{-5}) = [a-b]_2 + [a'-b']_2 = [(a+a')-(b+b')]_2 = f((a+b\sqrt{-5}) + (a'+b'\sqrt{-5}))$. A nakonec $f(a+b\sqrt{-5}) \cdot f(a'+b'\sqrt{-5}) = [a-b]_2 \cdot [a'-b']_2 = [aa'+bb'-ab'-a'b]_2 = [(aa'-5bb')-(ab'+a'b)]_2 = f((a+b\sqrt{-5}) \cdot (a'+b'\sqrt{-5}))$.

Zobrazení f je tedy vskutku homomorfismus. Uvažujme nad jeho jádrem: $\alpha = a + b\sqrt{-5} \in \ker f \Leftrightarrow [a-b]_2 = [0]_2 \Leftrightarrow a = 2k+b$ pro nějaké $k \in \mathbb{Z}$. Potom $\alpha = 2k+b(1+\sqrt{-5}) \in (2, 1+\sqrt{-5})$, tj. $\ker f \subseteq (2, 1+\sqrt{-5})$. Na druhou stranu $f(2) = f(1+\sqrt{-5}) = [0]_2$, tedy ideál $\ker f$ obsahuje prvky 2 a $1+\sqrt{-5}$. Jelikož $(2, 1+\sqrt{-5})$ je nejmenší ideál obsahující tyto dva prvky, dostáváme $(2, 1+\sqrt{-5}) \subseteq \ker f$ a dohromady s předchozím dostáváme rovnost obou ideálů. Tudíž $\mathbb{Z}[\sqrt{-5}]/(2, 1+\sqrt{-5}) \cong \mathbb{Z}/2\mathbb{Z}$ je těleso a ideál $(2, 1+\sqrt{-5})$ je maximální – v Dedekindově okruhu tudíž i nenulový prvoideál.

V této části jsme se dozvěděli o důležitých vlastnostech okruhu $\mathcal{O}_K$. Situace se však stane ještě mnohem zajímavější, pokud nebudeme uvažovat pouze jedno číselné těleso, ale hned dvě, jedno do druhého vnořené. Kolik zajímavých poznatků nám to přinese, uvidíme v následujícím textu.

4.3 Rozkládání prvočísel v $\mathcal{O}_K$

Představme si následující situaci: je dáno rozšíření těles $K \subseteq L$, kde K, L jsou číselná tělesa. Nechť $\mathcal{P}$ je nějaký prvoideál okruhu $\mathcal{O}_K$. Pak jistě

$$\mathcal{P}\mathcal{O}_L = \left\{ \sum_{i=1}^{n} a_i b_i | n \in \mathbb{N}, a_i \in \mathcal{P}, b_i \in \mathcal{O}_L \right\}$$

je ideál okruhu $\mathcal{O}_L$, můžeme ho tedy rozložit na součin prvoideálů okruhu $\mathcal{O}_L$: $\mathcal{P}\mathcal{O}_L = \mathfrak{p}_1^{e_1} \cdot \cdots \cdot \mathfrak{p}_r^{e_r}$.

Studiem této situace je možno se dobrat k mnoha zajímavým výsledkům. Budovat však následující teorii v plné obecnosti je nad rámec tohoto textu, proto se omezíme na speciální případ $K = \mathbb{Q}$. Všechna tvrzení, která dále uvedeme, ale mohou být zobecněna – někdy bez jakýchkoli problémů, někdy s obtížemi.

Budeme tedy rozebírat situaci $\mathbb{Q} \subseteq K$, kde K je libovolné číselné těleso. Uvědomme si, že nenulové prvoideály okruhu $\mathcal{O}_{\mathbb{Q}} = \mathbb{Z}$ jsou tvaru $p\,\mathbb{Z}$, kde p je prvočíslo (tedy $p\,\mathbb{Z} \cdot \mathcal{O}_K = p\,\mathcal{O}_K$).

V dalším textu bude vždy K značit číselné těleso a budeme-li mluvit o prvoideálech, budeme tím vždy myslet vlastní prvoideály.

Následující věta nám ukazuje některé souvislosti mezi prvoideály $\mathbb{Z}$ a $\mathcal{O}_K$:

Věta 4.3.1. *Nechť $\mathcal{P}$ je prvoideál okruhu $\mathcal{O}_K$, p je prvočíslo. Pak jsou následující podmínky ekvivalentní:*

1. $\mathcal{P} \mid p\,\mathcal{O}_K$,
2. $p\,\mathcal{O}_K \subseteq \mathcal{P}$,
3. $p\,\mathbb{Z} \subseteq \mathcal{P}$,
4. $p \in \mathcal{P}$
5. $\mathcal{P} \cap \mathbb{Z} = p\,\mathbb{Z}$.

Důkaz. Věta 4.2.4 říká přímo (1) $\Leftrightarrow$ (2). (2) $\Rightarrow$ (3) $\Rightarrow$ (4) je zřejmé: pokud $p\,\mathcal{O}_K \subseteq \mathcal{P}$, tak $p \in p\,\mathbb{Z} \subseteq p\,\mathcal{O}_K \subseteq \mathcal{P}$. Jistě také (3) $\Leftrightarrow$ (4). Ukažme (3) $\Rightarrow$ (2): pokud $p\,\mathbb{Z} \subseteq \mathcal{P}$, tak také $p \in \mathcal{P}$. Jelikož $\mathcal{P}$ je ideál okruhu $\mathcal{O}_K$, tak pro každé $\alpha \in \mathcal{O}_K$ platí $p\alpha \in \mathcal{P}$. To ale znamená $p\,\mathcal{O}_K \subseteq \mathcal{P}$, což jsme chtěli.

Ukázali jsme již (1) $\Leftrightarrow$ (2) $\Leftrightarrow$ (3) $\Leftrightarrow$ (4), zbývá tedy ukázat (4) $\Leftrightarrow$ (5). (5) $\Rightarrow$ (4) je zřejmé. Abychom ukázali (4) $\Rightarrow$ (5), vzpomeňme si z definice Dedekindova okruhu, že $p\,\mathbb{Z}$ jakožto prvoideál je také maximální ideál okruhu $\mathbb{Z}$. Pokud $p\,\mathbb{Z} \subseteq \mathcal{P}$, tak $p\,\mathbb{Z} \subseteq \mathcal{P} \cap \mathbb{Z} \subseteq \mathbb{Z}$ (přičemž $\mathcal{P} \cap \mathbb{Z}$ je jistě ideál okruhu $\mathbb{Z}$), tedy z maximality $p\,\mathbb{Z}$ buď $\mathcal{P} \cap \mathbb{Z} = p\,\mathbb{Z}$ nebo $\mathcal{P} \cap \mathbb{Z} = \mathbb{Z}$. Pokud by platila druhá možnost, znamenalo by to $1 \in \mathcal{P} \cap \mathbb{Z} \subseteq \mathcal{P}$, tedy ideál $\mathcal{P}$ by obsahoval jednotku okruhu $\mathbb{Z}$, která je zároveň jednotkou okruhu $\mathcal{O}_K$, platilo by tedy $\mathcal{P} = \mathcal{O}_K$, což je spor. Platí tedy $\mathcal{P} \cap \mathbb{Z} = p\,\mathbb{Z}$ a tvrzení je dokázáno.

□

Ohledně dělitelnosti navíc platí následující věta:

Věta 4.3.2. *Pro každé $p \in \mathbb{Z}$ je ideál $p\,\mathcal{O}_K$ je obsažen v alespoň jednom prvoideálu okruhu $\mathcal{O}_K$. Každý vlastní prvoideál okruhu $\mathcal{O}_K$ obsahuje právě jedno prvočíslo.*

Důkaz. Z předchozího víme, že $p\,\mathcal{O}_K$ je obsažen v těch prvoideálech, které ho dělí, tj. vystupují v jeho rozkladu na součin prvoideálů; jistě vždy alespoň jeden takový ideál existuje. Navíc jsme se dozvěděli, že je-li $\mathcal{P}$ libovolný nenulový prvoideál okruhu $\mathcal{O}_K$, je $\mathcal{O}_K \,/\, \mathcal{P}$ konečné těleso. Jako takové má prvočíselnou charakteristiku; označíme-li si tuto

charakteristiku jako p, vidíme, že $p \in \mathcal{P}$, tedy alespoň jedno prvočíslo v $\mathcal{P}$ leží. Nakonec předpokládejme, že v $\mathcal{P}$ leží jiné prvočíslo q. Potom ale díky Bezoutově rovnosti v $\mathcal{P}$ leží i největší společný dělitel p a q, jímž je 1, tj. $\mathcal{P} = \mathcal{O}_K$, což je spor s tím, že $\mathcal{P}$ je vlastní ideál. V $\mathcal{P}$ tedy leží právě jedno prvočíslo.

□

Definujme nyní dva pojmy klíčové pro další teorii. Těmi jsou index větvení a stupeň inercie.

Definice 4.3.3. *Nechť $\mathcal{P}$ je ideál okruhu $\mathcal{O}_K$, p je prvočíslo, $\mathcal{P} \mid p\,\mathcal{O}_K$. Nechť e je největší přirozené číslo k takové, že $\mathcal{P}^k \,|p\,\mathcal{O}_K$. Pak číslu e říkáme index větvení $\mathcal{P}$ nad p a značíme ho $e(\mathcal{P}\,|p)$.*

Koncept indexu větvení je jasný: je- li $p\,\mathcal{O}_K = \mathcal{P}_1^{e_1} \cdot \ \cdots \ \cdot \mathcal{P}_r^{e_r}$ rozklad ideálu $p\,\mathcal{O}_K$ na prvoideály, tak $e(\mathcal{P}_i\,|p) = e_i$.

Definujme nyní stupeň inercie. Nechť $\mathcal{P}$ je ideál okruhu $\mathcal{O}_K$, p je prvočíslo, $\mathcal{P}\,|p\,\mathcal{O}_K$. Pak existuje homomorfismus $f : \mathbb{Z} \to \mathcal{O}_K\,/\,\mathcal{P}$, který vznikne jako složení inkluze $\mathbb{Z} \to \mathcal{O}_K$ a projekce na faktorokruh $\mathcal{O}_K \to \mathcal{O}_K\,/\,\mathcal{P}$. Pak $\ker f = \{a \in \mathbb{Z}\,|a \in \mathcal{P}\} = \mathbb{Z} \cap \mathcal{P} = p\,\mathbb{Z}$. Z hlavní věty o faktorokruzích tedy dostáváme injektivní homomorfismus $\mathbb{Z}\,/p\,\mathbb{Z} \to \mathcal{O}_K\,/\,\mathcal{P}$ – tedy vnoření. Konečné těleso $\mathbb{Z}\,/p\,\mathbb{Z}$ je tedy izomorfní s nějakým podtělesem konečného tělesa $\mathcal{O}_K\,/\,\mathcal{P}$. Pomineme-li tento izomorfismus (izomorfní struktury v algebře není příliš nutné rozlišovat), můžeme uvažovat $\mathbb{Z}\,/p\,\mathbb{Z} \subseteq \mathcal{O}_K\,/\,\mathcal{P}$ jako rozšíření těles. Stupeň inercie pak definujeme jako stupeň tohoto rozšíření:

Definice 4.3.4. *Nechť $\mathcal{P}$ je ideál okruhu $\mathcal{O}_K$, p je prvočíslo, $\mathcal{P} \mid p\,\mathcal{O}_K$. Pak přirozené číslo $[\mathcal{O}_K\,/\,\mathcal{P} : \mathbb{Z}\,/p\,\mathbb{Z}]$ nazýváme stupeň inercie $\mathcal{P}$ nad p a značíme ho $f(\mathcal{P}\,|p)$.*

Všimněme si, že jelikož hovoříme o konečných tělesech, tak platí $|\,\mathcal{O}_K\,/\,\mathcal{P}\,| = p^{f(\mathcal{P}\,|p)}$.

Význam těchto pojmů nám ukáže následující věta:

Věta 4.3.5. *Nechť $[K : \mathbb{Q}] = n$. Nechť p je prvočíslo, $p\,\mathcal{O}_K = \mathcal{P}_1^{e_1} \cdot \ \cdots \ \cdot \mathcal{P}_r^{e_r}$ je rozklad ideálu $p\,\mathcal{O}_K$ na prvoideály okruhu $\mathcal{O}_K$. Pak platí*

$$\sum_{i=1}^{r} e(\mathcal{P}_i\,|p) f(\mathcal{P}_i\,|p) = n.$$

Platnost této důležité věty si ověříme na konkrétních příkladech. Jelikož zatím nevíme, jak obecně rozkládat na prvoideály, musíme se vystačit z příklady v kvadratických tělesech, kde je situace celkem jednoduchá.

Vzpomeňme si na příklad 4.2.3. V něm jsme si řekli, že v okruhu $O_{\mathbb{Q}(\sqrt{-5})} = \mathbb{Z}[\sqrt{-5}]$ platí $2\,\mathbb{Z}[\sqrt{-5}] = (2, 1 + \sqrt{-5})^2$ a $3\,\mathbb{Z}[\sqrt{-5}] = (3, 1 + \sqrt{-5}) \cdot (3, 1 - \sqrt{-5})$. V prvním případě tedy $e((2, 1 + \sqrt{-5})|2) = 2$ a $f((2, 1 + \sqrt{-5})|2) = 1$, jelikož jsme ukázali, že $\mathbb{Z}[\sqrt{-5}]/(2, 1 + \sqrt{-5}) \cong \mathbb{Z}\,/2\,\mathbb{Z}$. Jelikož $[\mathbb{Q}(\sqrt{-5}) : \mathbb{Q}] = 2$, věta 4.3.5 v tomto případě opravdu platí.

V druhém případě pak můžeme analogicky jako předtím ukázat $\mathbb{Z}[\sqrt{-5}]/(3, 1\pm\sqrt{-5}) \cong$ $\cong \mathbb{Z}/3\,\mathbb{Z}$ (jedná se o jádro homomorfismu $a+b\sqrt{-5} \mapsto [a\mp b]_3$), tedy $f((3, 1\pm\sqrt{-5})|3) = 1$; navíc očividně $e((3, 1 \pm \sqrt{-5})|3) = 1$. Tedy $2 = 1 \cdot 1 + 1 \cdot 1$ a věta 4.3.5 opět platí.

Větu 4.3.5 můžeme však využít i jiným způsobem, jak nám ukáže následující příklad:

Příklad 4.3.1. Ukažte, že $13\,\mathbb{Z}[\sqrt{3}] = (4 + \sqrt{3}) \cdot (4 - \sqrt{3})$ je rozklad prvočísla 13 na prvoideály okruhu $\mathcal{O}_{\mathbb{Q}(\sqrt{3})} = \mathbb{Z}[\sqrt{3}]$.

Jistě podle příkladu 4.2.2 platí $(4 + \sqrt{3}) \cdot (4 - \sqrt{3}) = ((4 + \sqrt{3}) \cdot (4 - \sqrt{3})) = (13) = 13\,\mathbb{Z}[\sqrt{3}]$. Jedná se navíc o různé ideály, jelikož jsou generované neasociovanými prvky (jak si můžeme snadno ověřit). Otázkou však je, jestli jsou $(4\pm\sqrt{3})$ prvoideály. Předpokládejme, že alespoň jeden ne, tedy že $(4 + \sqrt{3}) = \prod_{i=1}^{k} \mathcal{P}_i^{e_i}$, $(4 - \sqrt{3}) = \prod_{i=k+1}^{r} \mathcal{P}_i^{e_i}$, kde $r > 2$. Pak podle věty 4.3.5 platí $2 = [\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] = \sum_{i=1}^{r} e(\mathcal{P}_i\,|p) f(\mathcal{P}_i\,|p) \geq \sum_{i=1}^{r} 1 = r > 2$, spor. Tím je příklad vyřešen.

Nyní zavedeme nové názvosloví:

Definice 4.3.6. *Nechť $[K : \mathbb{Q}] = n$. Nechť p je prvočíslo, $p\,\mathcal{O}_K = \mathcal{P}_1^{e_1} \cdot \cdots \cdot \mathcal{P}_r^{e_r}$ je rozklad ideálu $p\,\mathcal{O}_K$ na prvoideály okruhu $\mathcal{O}_K$. Potom říkáme, že*

- *p se větví v K, pokud pro alespoň jedno i platí $e_i > 1$,*
- *p se totálně větví v K, pokud $r = 1$ a $e_1 = n$,*
- *p se nevětví v K, pokud pro všechna i platí $e_i = 1$,*
- *p se zcela rozkládá v K, pokud $r = n$ (a tedy $e_i = f(\mathcal{P}_i\,|p) = 1$ pro všechna i).*

Např. 2 se větví (dokonce totálně) v $\mathbb{Q}(\sqrt{-5})$ (viz příklad 4.2.3), 13 se zcela rozkládá v $\mathbb{Q}(\sqrt{3})$ (viz příklad 4.3.1).

Větvení prvočísel není příliš častý jev, jak říká následující věta:

Věta 4.3.7. *Nechť K je číselné těleso, $p \in \mathbb{Z}$ je prvočíslo. Pak se p větví v K, právě když $p|d(\mathcal{O}_K)$.*

Jednoduchým důsledkem tedy je, že se v libovolném tělese větví pouze konečně mnoho prvočísel.

O rozkladu prvočísel na prvoideály již víme mnohé. Můžeme ale zajít dále a určit přesnou podobu ideálů $\mathcal{P}_i$.

Vyslovme nejprve následující lemma:

Lemma 4.3.8. *Nechť K je číselné těleso. Pak existuje $\gamma \in \mathcal{O}_K$ takové, že $K = \mathbb{Q}(\gamma)$.*

Důkaz. Podle věty 4.1.15 existuje $\alpha \in K$ takové, že $K = \mathbb{Q}(\alpha)$. Podle věty 4.1.4 navíc existuje $m \in \mathbb{N}$ takové, že $m\alpha \in \mathcal{O}_K$. Označme $\gamma = m\alpha$. Jistě $\mathbb{Q}(\gamma) \subseteq \mathbb{Q}(\alpha)$, ale také $\mathbb{Q}(\alpha) \subseteq \mathbb{Q}(\gamma)$, jelikož $\alpha = \frac{1}{m} \cdot \gamma$, $\frac{1}{m} \in \mathbb{Q}$. Dohromady tedy $K = \mathbb{Q}(\alpha) = \mathbb{Q}(\gamma)$, $\gamma \in \mathcal{O}_K$. □

Zvolme nyní nějaké $\gamma \in \mathcal{O}_K$ tak, aby $K = \mathbb{Q}(\gamma)$. Jistě je $(\mathbb{Z}[\gamma], +)$ podgrupa grupy $(\mathcal{O}_K, +)$. Lze ukázat, že $|\,\mathcal{O}_K \,/\, \mathbb{Z}[\gamma]|$ je konečné číslo; označme ho r. Věta, kterou vyslovíme, bude platit pro všechny prvoideály okruhu $p\,\mathbb{Z}$ až ty, kde p dělí r. Výjimku z věty tedy bude tvořit konečně mnoho prvoideálů.

Dále definujme homomorfismus $\mathbb{Z}[x] \to (\mathbb{Z}\,/p\,\mathbb{Z})[x]$, který polynomu $h = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$ přiřadí polynom $\bar{h} = [a_n]_p x^n + \cdots + [a_1]_p x + [a_0]_p \in (\mathbb{Z}\,/p\,\mathbb{Z})[x]$.

Nechť $g(x)$ je minimální polynom prvku γ nad $\mathbb{Q}$. Jelikož γ je celé algebraické číslo, tak $g(x) \in \mathbb{Z}[x]$. Tedy $\bar{g} \in (\mathbb{Z}\,/p\,\mathbb{Z})[x]$ a jelikož okruh polynomů nad tělesem je okruh s jednoznačným rozkladem, můžeme psát $\bar{g} = \bar{g_1}^{e_1} \cdot \,\cdots\, \cdot \bar{g_r}^{e_r}$, kde $\bar{g_1}, ..., \bar{g_r}$ jsou normované ireducibilní polynomy nad $\mathbb{Z}\,/p\,\mathbb{Z}$. Ekvivalentně můžeme psát $g \equiv {g_1}^{e_1} \cdot \,\cdots\, \cdot {g_r}^{e_r} \pmod p$ (kde g_i jsou normované ireducibilní polynomy v $\mathbb{Z}[x]$).

Za těchto předpokladů můžeme vyslovit následující větu:

Věta 4.3.9. *Předpokládejme všechno jako výše, navíc předpokládejme, že p nedělí číslo $|\,\mathcal{O}_K \,/\, \mathbb{Z}[\gamma]|$. Pak rozklad ideálu $p\,\mathcal{O}_K$ na prvoideály je následujícího tvaru:*

$$p\,\mathcal{O}_K = \mathcal{P}_1^{e_1} \cdot \,\cdots\, \cdot \mathcal{P}_r^{e_r},$$

kde $\mathcal{P}_i = (p, g_i(\gamma)) = p\,\mathcal{O}_K + g_i(\gamma)\,\mathcal{O}_K$. Navíc stupeň inercie $f(\mathcal{P}_i\,|p)$ je roven stupni polynomu $g_i(x)$.

Uvědomme si, jak je tato věta silná: pomocí ní snadno dostáváme to, co jsme v příkladech 4.2.3 a 4.3.1 pracně dokazovali. Jelikož $|\,\mathcal{O}_{\mathbb{Q}(\sqrt{3})} \,/\, \mathbb{Z}[\sqrt{3}]| = |\,\mathcal{O}_{\mathbb{Q}(\sqrt{-5})} \,/\, \mathbb{Z}[\sqrt{-5}]| = 1$, můžeme větu použít pro každé prvočíslo. Jelikož $x^2 + 5 \equiv x^2 + 1 \equiv (x+1)^2 \pmod 2$, tak $2\,\mathbb{Z}[\sqrt{-5}] = (2, 1 + \sqrt{-5})^2$. Jelikož $x^2 + 5 \equiv x^2 - 1 \equiv (x-1)(x+1) \pmod 3$, tak $3\,\mathbb{Z}[\sqrt{-5}] = (3, 1-\sqrt{-5}) \cdot (3, 1+\sqrt{-5})$. A do třetice jelikož $x^2 - 3 \equiv x^2 - 16 \equiv (x+4)(x-4) \pmod{13}$, tak $13\,\mathbb{Z}[\sqrt{3}] = (13, 4+\sqrt{3}) \cdot (13, 4-\sqrt{3}) = ((4+\sqrt{3})(4-\sqrt{3}), 4+\sqrt{3}) \cdot ((4-\sqrt{3})(4+\sqrt{3}), 4-\sqrt{3}) = (4+\sqrt{3}) \cdot (4-\sqrt{3})$.

V další kapitole uvidíme, co se bude dít, pokud je $\mathbb{Q} \subseteq K$ Galoisovo.

Kapitola 5

Rozkládání prvočísel v Galoisových rozšířeních

V předchozí kapitole jsme se seznámili se základy algebraické teorie čísel a s tím, jak se prvočísla rozkládájí na prvoideály okruhu $\mathcal{O}_K$. Rozšíření $\mathbb{Q} \subseteq K$ vždy nemusí být Galoisovo, např. $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[3]{2})$, ale v mnoha případech tomu tak je.

V následující kapitole si ukážeme, jak obecná situace vypadá v Galoisových rozšířeních. Víme, že v těchto rozšířeních je situace v mnoha ohledech přehlednější – máme dobře popsaná mezitělesa, automorfismy atd. Uvidíme, že i nyní se nám situace v Galoisových rozšířeních zjednoduší. To nám ale umožní zavést nové pojmy.

Jedním z důvodů, proč je následující text vyčleněn jako samostatná kapitola, je ten, že se od předchozího bude lišit následujícím: v předchozí kapitole obvykle nebyl prostor tvrzení dokazovat, maximálně jsme si je mohli ověřit na příkladech. Nyní již máme velkou zásobu teorie, a proto následující situaci můžeme studovat více do hloubky a častěji uvádět i důkazy jednotlivých tvrzení.

Poznamenejme ještě, že i tuto situaci lze zobecnit na Galoisova rozšíření číselných těles K, L. Dohodněme se také, že v následujícím textu bude vždy K značit nějaké číselné těleso, které je Galoisovým rošířením tělesa racionálních čísel a grupu $\mathrm{Gal}(K/\mathbb{Q})$ budeme značit jako G.

5.1 Působení Galoisovy grupy na ideály $\mathcal{O}_K$

Nejdříve ukažme, že automorfismy rozšíření $\mathbb{Q} \subseteq K$ zobrazí okruh $\mathcal{O}_K$ sám na sebe:

Věta 5.1.1. *Nechť σ je libovolný prvek grupy G. Pak $\sigma(\mathcal{O}_K) = \mathcal{O}_K$ a pokud $\mathcal{I}$ je ideál $\mathcal{O}_K$, tak i $\sigma(\mathcal{I}) = \{\sigma(\alpha) | \alpha \in \mathcal{I}\}$ je ideál $\mathcal{O}_K$.*

Důkaz. Zvolme libovolné $\alpha \in \mathcal{O}_K$. Minimální polynom f prvku α nad $\mathbb{Q}$ má celočíselné koeficienty, jelikož α je celé algebraické číslo. Z kapitoly 2 víme, že pro libovolné $\sigma \in G$ je $\sigma(\alpha)$ některý kořen polynomu f. Je to tedy také celé algebraické číslo, proto $\sigma(\mathcal{O}_K) = \{\sigma(\alpha) | \alpha \in$

$\mathcal{O}_K\} \subseteq \mathcal{O}_K$. Pak ale také $\sigma^{-1}(\mathcal{O}_K) \subseteq \mathcal{O}_K$, po aplikaci σ dostáváme inkluzi $\mathcal{O}_K \subseteq \sigma(\mathcal{O}_K)$. Dohromady tedy $\sigma(\mathcal{O}_K) = \mathcal{O}_K$.

Podle předchozího tedy pro libovolný ideál $\mathcal{I}$ okruhu $\mathcal{O}_K$ platí $\sigma(\mathcal{I}) \subseteq \mathcal{O}_K$. S pomocí faktu, že je σ automorfismus, si můžeme snadno ověřit, že $\sigma(\mathcal{I})$ je ideál okruhu $\mathcal{O}_K$. Jistě je to neprázdná množina. Dále pro libovolná $\alpha, \beta \in \mathcal{I}$ platí $\sigma(\alpha)+\sigma(\beta) = \sigma(\alpha+\beta) \in \sigma(\mathcal{I})$ (jelikož $\alpha + \beta \in \mathcal{I}$). Nakonec pro libovolné $r \in \mathcal{O}_K$ označme $r' = \sigma^{-1}(r)$ (už víme, že $r' \in \mathcal{O}_K$). Potom $r\sigma(\alpha) = \sigma(r')\sigma(\alpha) = \sigma(r'\alpha) \in \sigma(\mathcal{I})$ pro libovolné $\alpha \in \mathcal{I}$ (jelikož $r'\alpha \in \mathcal{I}$). □

Zajímavé je především působení Galoisovy grupy na prvoideály okruhu $\mathcal{O}_K$, které dělí ideál $p\,\mathcal{O}_K$ pro nějaké prvočíslo p. Permutuje je následujícím způsobem:

Věta 5.1.2. *Nechť p je prvočíslo, $\mathcal{P}$ je prvoideál $\mathcal{O}_K$, $\mathcal{P} \,|\, p\,\mathcal{O}_K$. Pak pro všechny $\sigma \in G$ platí $\sigma(\mathcal{P}) | p\,\mathcal{O}_K$ a navíc pro libovolný prvoideál $\mathcal{P}' \subseteq \mathcal{O}_K$, $\mathcal{P}' \,|\, p\,\mathcal{O}_K$ existuje $\sigma \in G$ tak, že $\sigma(\mathcal{P}) = \mathcal{P}'$.*

Poznámka 5.1.1. Věta nám vlastně říká toto: je-li $p\,\mathcal{O}_K = \mathcal{P}_1^{e_1} \cdot \,\cdots\, \cdot \mathcal{P}_r^{e_r}$ rozklad ideálu $p\,\mathcal{O}_K$ na prvoideály okruhu $\mathcal{O}_K$, pak pro každé $i \in \mathbb{Z}, 1 \leq i \leq r$ platí $\{\sigma(\mathcal{P}_i) | \sigma \in G\} = \\ = \{\mathcal{P}_1, ..., \mathcal{P}_r\}$.

Toto působení si můžeme ověřit na předchozích příkladech: v 4.3.1 jsme měli $13 = \\ = (4-\sqrt{3})(4+\sqrt{3})$, přičemž $\mathrm{Gal}(\mathbb{Q}(\sqrt{3})/\,\mathbb{Q}) = \{\mathrm{id}, \sigma\}$, $\sigma : \sqrt{3} \mapsto -\sqrt{3}$. A vskutku, vidíme $\mathrm{id}((4+\sqrt{3})) = (4+\sqrt{3})$, $\sigma((4+\sqrt{3})) = (4-\sqrt{3})$.

Tím dostáváme následující:

Věta 5.1.3. *Nechť $\mathbb{Q} \subseteq K$ je Galoisovo, p je prvočíslo, $p\,\mathcal{O}_K = \mathcal{P}_1^{e_1} \cdot \,\cdots\, \cdot \mathcal{P}_r^{e_r}$ je rozklad ideálu $p\,\mathcal{O}_K$ na prvoideály. Pak $e_1 = e_2 = \cdots = e_r$ a $f_1 = f_2 = \cdots = f_r$ (kde $e_i = e(\mathcal{P}_i\,|p)$ je index větvení a $f_i = f(\mathcal{P}_i\,|p)$ je stupeň inercie).*

Důkaz. Nejdříve si uvědomme, že pro libovolné $\sigma \in \mathrm{Gal}(K/\,\mathbb{Q})$ platí $\sigma(p\,\mathcal{O}_K) = p\,\mathcal{O}_K$; to proto, že $\sigma(p) = p$ (prvky Galoisovy grupy fixují celé $\mathbb{Q}$) a $\sigma(\mathcal{O}_K) = \mathcal{O}_K$ (z věty 5.1.1).

Proto tudíž, budeme-li uvažovat rozklad ideálu $p\,\mathcal{O}_K$ na prvoideály, platí pro každé $\sigma \in \mathrm{Gal}(K/\,\mathbb{Q})$ následující:

$$\mathcal{P}_1^{e_1} \cdot \,\cdots\, \cdot \mathcal{P}_r^{e_r} = p\,\mathcal{O}_K = \sigma(p\,\mathcal{O}_K) = \sigma(\mathcal{P}_1^{e_1} \cdot \,\cdots\, \cdot \mathcal{P}_r^{e_r}) = \sigma(\mathcal{P}_1)^{e_1} \cdot \,\cdots\, \cdot \sigma(\mathcal{P}_r)^{e_r}.$$

Chceme nyní ukázat, že $e_1 = e_2 = \cdots = e_r$. Předpokládejme, že tomu tak není, např. $e_1 \neq e_2$. Podle věty 5.1.2 existuje $\sigma \in G$ takové, že $\sigma(\mathcal{P}_1) = \mathcal{P}_2$. Pak podle rovnosti výše platí $e(\mathcal{P}_2\,|p) = e(\sigma(\mathcal{P}_1)|p) = e_1$. Z definice ale $e(\mathcal{P}_2\,|p) = e_2$, tedy $e_1 = e_2$, spor.

Nyní ukažme $f_1 = f_2 = \cdots = f_r$. Zvolme libovolně dva ideály $\mathcal{P}, \mathcal{P}' \in \{\mathcal{P}_1, ..., \mathcal{P}_r\}$. Podle věty 5.1.2 existuje $\sigma \in G$ takové, že $\sigma(\mathcal{P}) = \mathcal{P}'$. Uvažujme nyní zobrazení $\varphi : \mathcal{O}_K\,/\,\mathcal{P} \to \mathcal{O}_K\,/\,\mathcal{P}'$ definované pomocí σ jako $\varphi(a+\mathcal{P}) = \sigma(a) + \mathcal{P}'$ pro všechna $a \in \mathcal{O}_K$. Vzhledem k tomu, jak jsme volili σ, je φ korektně definované zobrazení. Ukážeme, že je to izomorfismus. Jistě je φ surjekce, protože σ je surjekce. Ukažme, že je to i injekce.

Předpokládejme $\varphi(a+\mathcal{P}) = \varphi(b+\mathcal{P})$ a chceme ukázat rovnost těchto tříd, tedy $a-b \in \mathcal{P}$. Jelikož $\varphi(a+\mathcal{P}) = \sigma(a)+\mathcal{P}'$, $\varphi(b+\mathcal{P}) = \sigma(b)+\mathcal{P}'$, dostáváme $\varphi(a+\mathcal{P}) = \varphi(b+\mathcal{P}) \Leftrightarrow \sigma(a)+\mathcal{P}' = \sigma(b)+\mathcal{P}' \Leftrightarrow \sigma(a)-\sigma(b) \in \mathcal{P}' = \sigma(\mathcal{P}) \Leftrightarrow a-b \in \mathcal{P}$, což jsme chtěli. Tedy $\mathcal{O}_K \,/\, \mathcal{P} \cong \mathcal{O}_K \,/\, \mathcal{P}' \Rightarrow |\,\mathcal{O}_K \,/\, \mathcal{P}\,| = |\,\mathcal{O}_K \,/\, \mathcal{P}'\,| \Rightarrow p^{f(\mathcal{P}\,|p)} = p^{f(\mathcal{P}'\,|p)} \Rightarrow f(\mathcal{P}\,|p) = f(\mathcal{P}'\,|p)$, což jsme chtěli dokázat.

□

Poznámka 5.1.2. Z předchozí věty plyne, že stupeň inercie i index větvení závisí v Galoisových rozšířeních pouze na tělese K a prvočísle p. Proto budeme dále používat zjednodušující názvosloví, kde index větvení p v K budeme značit $e(K,p)$ a stupeň inercie obdobně $f(K,p)$.

Aplikací věty 5.1.3 dostáváme důležitý výsledek:

Důsledek 5.1.4. *Nechť $\mathbb{Q} \subseteq K$ je Galoisovo rozšíření $[K:\mathbb{Q}] = n$, p je prvočíslo. Označíme-li $e = e(K,p)$, $f = f(K,p)$ a r je rovno počtu prvoideálů dělících $p\,\mathcal{O}_K$, dostaneme*

$$ref = n.$$

5.2 Dekompoziční a inerční grupa

V předchozí části jsme viděli, jak působí Galoisova grupa rozšíření $\mathbb{Q} \subseteq K$, kde K je číselné těleso, na prvoideály $\mathcal{P}$ okruhu $\mathcal{O}_K$ které dělí daný ideál $p\,\mathcal{O}_K$, p je prvočíslo. Tento fenomén nyní budeme studovat více do hloubky.

Jistě existuje alespoň jedno $\sigma \in G$ takové, že $\sigma(\mathcal{P}) = \mathcal{P}$ (určitě to splňuje identita). Pak také $\sigma^{-1}(\mathcal{P}) = \sigma^{-1}(\sigma(\mathcal{P})) = \mathcal{P}$. Navíc pokud platí $\sigma(\mathcal{P}) = \mathcal{P}, \sigma'(\mathcal{P}) = \mathcal{P}$, dostaneme $(\sigma\sigma')(\mathcal{P}) = \sigma(\sigma'(\mathcal{P})) = \sigma(\mathcal{P}) = \mathcal{P}$; obdobně $(\sigma'\sigma)(\mathcal{P}) = \mathcal{P}$. Prvky Galoisovy grupy permutující $\mathcal{P}$ tedy tvoří grupu!

S těmito poznatky můžeme uvést následující definici:

Definice 5.2.1. *Nechť p je prvočíslo, $\mathcal{P}$ je prvoideál $\mathcal{O}_K$, $\mathcal{P}\,|p\,\mathcal{O}_K$. Pak definujeme dekompoziční grupu prvoideálu $\mathcal{P}$ jako*

$$D(\mathcal{P}\,|p) = \{\sigma \in G | \sigma(\mathcal{P}) = \mathcal{P}\}.$$

Například pokud $D(\mathcal{P}\,|p) = G$, tak $p\,\mathcal{O}_K = \mathcal{P}^e, e \geq 1$. To proto, že ideály, které dělí $p\,\mathcal{O}_K$, jsou podle věty 5.1.2, obrazy jednotlivých automorfismů z G, a tedy pokud $D(\mathcal{P}\,|p) = G$, tak všechny tyto obrazy jsou rovny $\mathcal{P}$.

Příklad 5.2.1. Označme $K = \mathbb{Q}(i, \sqrt{m})$. Platí $G = \mathrm{Gal}(K/\,\mathbb{Q}) = \{\mathrm{id}, \sigma, \tau, \tau\sigma\}$, kde jako obvykle $\tau : i \mapsto -i, \sqrt{m} \mapsto \sqrt{m}$, $\sigma : \sqrt{m} \mapsto -\sqrt{m}, i \mapsto i$. Pak ukažte, že pokud $D(\mathcal{P}\,|p) = \{\mathrm{id}, \sigma\}$ a p je prvočíslo, které se nevětví v K, tak $p\,\mathcal{O}_K = \mathcal{P}\,\mathcal{Q}$ a $\mathcal{Q}$ se skládá z prvků komplexně sdružených s prvky $\mathcal{P}$.

Z věty 5.1.2 víme, že prvoideály dělící $p\,\mathcal{O}_K$ jsou rovny obrazům $\mathcal{P}$ ve všech možných automorfismech grupy G. Jelikož $D(\mathcal{P}\,|p) = \{\mathrm{id}, \sigma\}$, tak $\mathrm{id}(\mathcal{P}) = \sigma(\mathcal{P}) = \mathcal{P}$. Dále $\tau(\mathcal{P}) = \mathcal{Q}$, kde $\mathcal{Q}$ je nějaký jiný prvoideál dělící $p\,\mathcal{O}_K$. A nakonec $(\tau\sigma)(\mathcal{P}) = \tau(\sigma(\mathcal{P})) = \tau(\mathcal{P}) = \mathcal{Q}$. Tedy jediné dva ideály, které dělí $p\,\mathcal{O}_K$, jsou $\mathcal{P}$ a $\mathcal{Q}$ a jelikož se p nevětví, tak $p\,\mathcal{O}_K = \mathcal{P}\,\mathcal{Q}$. Navíc jelikož $\mathcal{Q} = \tau(\mathcal{P})$ a τ je restrikcí komplexní konjugovanosti, tak se $\mathcal{Q}$ skládá z prvků komplexně sdružených s prvky $\mathcal{P}$. Tím je příklad vyřešen.

Poznámka 5.2.1. Na předchozím případě jsme si mohli všimnout, že prvoideály dělící p odpovídaly třídám rozkladu $G/D(\mathcal{P}\,|p) = \{\{\mathrm{id}, \sigma\}, \{\tau, \tau\sigma\}\}$. Již brzy se nám toto pozorování podaří zobecnit.

Kromě dekompoziční grupy můžeme definovat ještě jednu důležitou podgrupu grupy G:

Definice 5.2.2. *Nechť p je prvočíslo, $\mathcal{P}$ je prvoideál $\mathcal{O}_K$, $\mathcal{P}\,|p\,\mathcal{O}_K$. Pak definujeme inerční grupu prvoideálu $\mathcal{P}$ jako*

$$E(\mathcal{P}\,|p) = \{\sigma \in G | \forall \alpha \in \mathcal{O}_K : \sigma(\alpha) \equiv \alpha \pmod{\mathcal{P}}\}.$$

Mezi oběma grupami panuje následující vztah:

Věta 5.2.3. *Označme $D = D(\mathcal{P}\,|p), E = E(\mathcal{P}\,|p)$. Pak je E normální podgrupa grupy D.*

Důkaz. Vyberme libovolné $\sigma \in E$. Pak pro všechny $\alpha \in \mathcal{P}$ platí $\sigma(\alpha) \equiv \alpha \equiv 0 \pmod{\mathcal{P}}$, tedy $\sigma(\alpha) \in \mathcal{P}$ a $\sigma(\mathcal{P}) \subseteq \mathcal{P}$. Jelikož $\sigma(\mathcal{P})$ i $\mathcal{P}$ jsou prvoideály v Dedekindově okruhu, jsou zároveň maximální a dostáváme rovnost $\sigma(\mathcal{P}) = \mathcal{P}$. Proto $\sigma \in D$ a E je podgrupa grupy D.

Nyní ukažme, že E je dokonce normální podgrupa D. Zvolme libovolně $\delta \in D$, $\sigma \in E$. Zvolme libovolné $\alpha \in \mathcal{O}_K$. Jelikož $\sigma \in E$, platí $\sigma(\delta^{-1}(\alpha)) \equiv \delta^{-1}(\alpha) \pmod{\mathcal{P}}$. Pak tedy $(\delta\sigma\delta^{-1})(\alpha) = \delta(\sigma(\delta^{-1}(\alpha))) \equiv \delta(\delta^{-1}(\alpha)) = \alpha \pmod{\delta(\mathcal{P})}$. Ale jelikož $\delta \in D$, tak $\delta(\mathcal{P}) = \mathcal{P}$ a tudíž $\delta\sigma\delta^{-1} \in E$. Tudíž je E opravdu normální.

□

V důkazu věty 5.1.3 jsme mimo jiné ukázali, že každý automorfismus $\sigma \in G$ indukuje izomorfismus $\mathcal{O}_K\,/\,\mathcal{P} \to \mathcal{O}_K\,/\sigma(\mathcal{P})$ (kde $\mathcal{P}$ je nějaký prvoideál okruhu $\mathcal{O}_K$). To ale znamená, že každý prvek σ dekompoziční grupy indukuje automorfismus φ tělesa $\mathcal{O}_K\,/\,\mathcal{P}$ ve smyslu $\varphi(\alpha + \mathcal{P}) = \sigma(\alpha) + \mathcal{P}$.

Víme, že pokud $\mathcal{P}\,|p\,\mathcal{O}_K$, tak $\mathbb{Z}\,/p\,\mathbb{Z} \subseteq \mathcal{O}_K\,/\,\mathcal{P}$ (kde $\mathbb{Z}\,/p\,\mathbb{Z}$ ztotožňujeme s jeho vnořením do $\mathcal{O}_K\,/\,\mathcal{P}$) je rozšíření konečných těles, tedy je Galoisovo. Je-li φ automorfismus tělesa $\mathcal{O}_K\,/\,\mathcal{P}$ indukovaný prvkem dekompoziční grupy, pak φ fixuje těleso $\mathbb{Z}\,/p\,\mathbb{Z}$ (prvky dekompoziční grupy jsou zároveň prvky grupy $\mathrm{Gal}(K/\,\mathbb{Q})$, tedy fixují $\mathbb{Q}$ a tím spíše $\mathbb{Z}$, proto φ fixuje $\mathbb{Z}\,/p\,\mathbb{Z}$), tedy $\varphi \in \mathrm{Gal}((\mathcal{O}_K\,/\,\mathcal{P})/(\mathbb{Z}\,/p\,\mathbb{Z}))$. Označíme-li $\tilde{G} = \mathrm{Gal}((\mathcal{O}_K\,/\,\mathcal{P})/(\mathbb{Z}\,/p\,\mathbb{Z}))$, dostáváme tedy zobrazení $\Phi : D \to \tilde{G}$. Toto zobrazení je dokonce homomorfismus (jak si můžeme snadno ověřit).

To jsou sice zajímavé poznatky, ale můžeme zajít ještě dál: zkoumejme jádro homomorfismu Φ. Zvolme libovolné $\sigma \in D$ a označme $\varphi = \Phi(\sigma)$; pak platí: $\sigma \in \ker\Phi \Leftrightarrow \varphi = \mathrm{id} \Leftrightarrow$

$\Leftrightarrow \forall \alpha \in \mathcal{O}_K : \varphi(\alpha + \mathcal{P}) = \alpha + \mathcal{P} \Leftrightarrow \forall \alpha \in \mathcal{O}_K : \sigma(\alpha) + \mathcal{P} = \alpha + \mathcal{P} \Leftrightarrow \forall \alpha \in \mathcal{O}_K : \sigma(\alpha) \equiv \alpha \pmod{\mathcal{P}} \Leftrightarrow \sigma \in E$. Tedy $\ker \Phi = E$ a podle hlavní věty o faktorgrupách dostáváme injektivní homomorfismus grup $D/E \to \tilde{G}$.

Je možné ukázat ještě více, a to že Φ je surjekce, tedy každý prvek $\tilde{G}$ je indukován prvkem dekompoziční grupy. Z toho plyne následující:

Věta 5.2.4. *Nechť $D = D(\mathcal{P}\,|p)$, $E = E(\mathcal{P}\,|p)$, $\tilde{G} = \mathrm{Gal}((\mathcal{O}_K\,/\,\mathcal{P})/(\mathbb{Z}\,/p\,\mathbb{Z}))$, $f = f(\mathcal{P}\,|p)$. Pak $D/E \cong \tilde{G}$ a tedy $\frac{|D|}{|E|} = f$.*

Poznámka 5.2.2. Pokud budeme mít pevně zvoleno prvočíslo p a prvoideál $\mathcal{P}$ dělící ideál $p\,\mathcal{O}_K$, budeme dále používat zjednodušené názvosloví $D = D(\mathcal{P}\,|p)$, $E = E(\mathcal{P}\,|p)$, $\tilde{G} = \mathrm{Gal}((\mathcal{O}_K\,/\,\mathcal{P})/(\mathbb{Z}\,/p\,\mathbb{Z}))$, $f = f(\mathcal{P}\,|p)$, $e = e(\mathcal{P}\,|p)$, r je počet prvoideálů dělících $p\,\mathcal{O}_K$.

Z předchozích poznatků odvodíme následující větu:

Věta 5.2.5. *Nechť $D, E, \tilde{G}, f, e, r$ je jako obvykle, $n = [K : \mathbb{Q}]$. Pak platí $r = |G/D|$, $|D| = ef$ a $|E| = e$.*

Důkaz. Nejprve ukážeme $r = |G/D|$. Zvolme dva různé automorfismy $\sigma, \tau \in G$, které leží v stejné třídě rozkladu G/D. Ze základů teorie grup pak $\tau^{-1}\sigma \in D$, tedy $(\tau^{-1}\sigma)(\mathcal{P}) = \mathcal{P}$. Potom $\tau(\mathcal{P}) = \tau((\tau^{-1}\sigma)(\mathcal{P})) = \sigma(\mathcal{P})$. Tedy třídy rozkladu G/D a prvoideály dělící $p\,\mathcal{O}_K$ si jednoznačně odpovídají a platí $|G/D| = r$, což jsme chtěli dokázat (tím zobecňujeme příklad 5.2.1, jak nám říká poznámka 5.2.1).

Další tvrzení z věty plynou z právě dokázaného a z věty 5.2.4. Jelikož $r = |G/D| = \frac{|G|}{|D|}$, tak $|D| = \frac{|G|}{r} = \frac{n}{r} = \frac{ref}{r} = ef$. A protože $\frac{|D|}{|E|} = f$, tak $|E| = e$.

□

Zamysleme se nad případem, kdy je $E = \{\mathrm{id}\}$ triviální. Pak $D \cong \tilde{G}$. Přitom $\tilde{G}$ je, jak víme z věty 3.2.4, cyklická grupa generovaná prvkem $\varphi \in \tilde{G}$, pro nějž platí $\varphi(\alpha + \mathcal{P}) = = (\alpha + \mathcal{P})^p$ pro všechna $\alpha \in \mathcal{O}_K$. Tedy D je generována prvkem $\phi = \Phi^{-1}(\varphi)$, pro nějž platí $\phi(\alpha) \equiv \alpha^p \pmod{\mathcal{P}}$. Tento prvek nazýváme *Frobeniův automorfismus* a značíme ho $\phi(\mathcal{P}\,|p)$. Je na místě dodat, že tímto názvem je často označován jak generátor dekompoziční grupy, tak generátor grupy automorfismů rozšíření konečných těles – to opět proto, že izomorfní struktury se v algebře často ztotožňují. Někdy jsou ještě tato zobrazení pojmově rozlišována jako globální a lokální Frobeniův automorfismus.

Frobeniův automorfismus je objekt velkého významu a bude pro nás důležitý v dalším textu. Nyní jej však ponecháme na chvíli stranou a dáme do souvislosti stupeň inercie a index větvení s dekompoziční a inerční grupou.

Nejprve si uvědomme, že jelikož jsou D i E podgrupy grupy $G = \mathrm{Gal}(K/\,\mathbb{Q})$, tak podle hlavní věty Galoisovy teorie existují tělesa $L_D = \mathrm{Fix}(D)$ a $L_E = \mathrm{Fix}(E)$ (nazýváme je jako dekompoziční a inerční těleso). Navíc jelikož $\{\mathrm{id}\} \subseteq E \subseteq D \subseteq G$, tak $\mathbb{Q} \subseteq L_D \subseteq L_E \subseteq K$. Tato tělesa mají mnoho důležitých vlastností, které můžeme shrnout do následující věty:

Věta 5.2.6. *Nechť $\mathbb{Q} \subseteq K$ je Galoisovo rozšíření, p je prvočíslo, $\mathcal{P}$ je prvoideál okruhu $\mathcal{O}_K$ takový, že $\mathcal{P} \,|p\, \mathcal{O}_K$. Nechť je D, E, r, e, f definováno pro zvolený prvoideál $\mathcal{P}$ jako obvykle. Pak platí $[K : L_E] = e$, $[L_E : L_D] = f$, $[L_D : \mathbb{Q}] = r$.*

Důkaz. Tvrzení plyne z předchozích vět a hlavní věty Galoisovy teorie: $[K : L_E] = |E| = e$, $[L_E : L_D] = |D/E| = f$, $[L_D : \mathbb{Q}] = |G/D| = r$. □

Dostáváme významný poznatek s velkým aplikačním potenciálem. Poznamenejme ale, že kdybychom předchozí teorii definovali v plné obecnosti, tedy pro rozšíření $K \subseteq L$ číselných těles, mohli bychom pozorovat ještě více, např. bychom zjistili některé vlastnosti prvoideálů okruhů $\mathcal{O}_{L_E}$ a $\mathcal{O}_{L_D}$.

V následující podkapitole si ukážeme, jak se situace zjednodušuje, pokud je $K \subseteq L$ nejen Galoisovo, ale dokonce abelovské rozšíření.

5.3 Dekompoziční grupa v abelovských rozšířeních

Ukážeme nejprve následující větu, která popisuje, jak spolu souvisí různé dekompoziční a inerční grupy příslušné danému prvočíslu:

Věta 5.3.1. *Nechť $\mathbb{Q} \subseteq K$ je Galoisovo rozšíření, p je prvočíslo, $\mathcal{P}, \mathcal{P}'$ jsou prvoideály okruhu $\mathcal{O}_K$, které dělí ideál $p\,\mathcal{O}_K$. Zvolme $\sigma \in G$ tak, že $\mathcal{P}' = \sigma(\mathcal{P})$. Pak platí*

$$D(\mathcal{P}' \,|p) = \sigma D(\mathcal{P} \,|p)\sigma^{-1},$$

$$E(\mathcal{P}' \,|p) = \sigma E(\mathcal{P} \,|p)\sigma^{-1}.$$

Důkaz. Nejprve dokažme část věty o dekompoziční grupě:

$$\begin{aligned}
\tau \in D(\mathcal{P}' \,|p) = D(\sigma(\mathcal{P})|p) &\Leftrightarrow \tau(\sigma(\mathcal{P})) = \sigma(\mathcal{P}) \\
&\Leftrightarrow \forall \alpha \in \mathcal{P} : \tau(\sigma(\alpha)) \in \sigma(\mathcal{P}) \\
&\Leftrightarrow \forall \alpha \in \mathcal{P} : \sigma^{-1}(\tau(\sigma(\alpha))) \in \sigma^{-1}(\sigma(\mathcal{P})) = \mathcal{P} \\
&\Leftrightarrow \forall \alpha \in \mathcal{P} : (\sigma^{-1}\tau\sigma)(\alpha) \in \mathcal{P} \\
&\Leftrightarrow (\sigma^{-1}\tau\sigma)(\mathcal{P}) = \mathcal{P} \\
&\Leftrightarrow \sigma^{-1}\tau\sigma \in D(\mathcal{P} \,|p).
\end{aligned}$$

Tedy $D(\mathcal{P}' \,|p) = \{\tau \in G | \sigma^{-1}\tau\sigma \in D(\mathcal{P} \,|p)\} = \sigma D(\mathcal{P} \,|p)\sigma^{-1}$.

Druhou část věty dokážeme obdobně, jen s trochu jiným argumentem:

$$\begin{aligned}
\tau \in E(\mathcal{P}' \,|p) = E(\sigma(\mathcal{P})|p) &\Leftrightarrow \forall \alpha \in \mathcal{O}_K : \tau(\sigma(\alpha)) \equiv \sigma(\alpha) \pmod{\sigma(\mathcal{P})} \\
&\Leftrightarrow \forall \alpha \in \mathcal{O}_K : \sigma^{-1}(\tau(\sigma(\alpha))) \equiv \sigma^{-1}(\sigma(\alpha)) = \alpha \pmod{\mathcal{P}} \\
&\Leftrightarrow \forall \alpha \in \mathcal{O}_K : (\sigma^{-1}\tau\sigma)(\alpha) \equiv (\alpha) \pmod{\mathcal{P}} \\
&\Leftrightarrow \sigma^{-1}\tau\sigma \in E(\mathcal{P} \,|p).
\end{aligned}$$

Tedy $E(\mathcal{P}' \,|p) = \{\tau \in G | \sigma^{-1}\tau\sigma \in E(\mathcal{P} \,|p)\} = \sigma E(\mathcal{P} \,|p)\sigma^{-1}$.

□

Z této věty plynou některé zajímavé poznatky:

Důsledek 5.3.2. *Nechť je dáno $p, \mathcal{P}, \mathcal{P}', \sigma$ jako výše, navíc předpokládejme, že se p nevětví v K. Pak $\phi(\mathcal{P}'\,|p) = \sigma\phi(\mathcal{P}\,|p)\sigma^{-1}$.*

Důkaz. Vzpomeňme si, že Frobeniovy automorfismy jsou jednoznačně určeny jistými kongruencemi: jsou to kongruence $\phi(\mathcal{P}\,|p)(\alpha) \equiv \alpha^p \pmod{\mathcal{P}}$, $\phi(\mathcal{P}'\,|p)(\alpha) \equiv \alpha^p \pmod{\mathcal{P}'}$ (pro všechna $\alpha \in \mathcal{O}_K$). Pak tedy pro všechna $\alpha \in \mathcal{O}_K$ platí

$$\phi(P|p)(\sigma^{-1}(\alpha)) \equiv (\sigma^{-1}(\alpha))^p = \sigma^{-1}(\alpha^p) \pmod{\mathcal{P}},$$

tedy

$$(\sigma\phi(P|p)\sigma^{-1})(\alpha) = \sigma(\phi(P|p)(\sigma^{-1}(\alpha))) \equiv \sigma(\sigma^{-1}(\alpha^p)) = \alpha^p \pmod{\sigma(\mathcal{P})}.$$

Jelikož $\sigma(\mathcal{P}) = \mathcal{P}'$, důkaz je hotov.

□

Důsledek 5.3.3. *Nechť G je komutativní, tzn. $\mathbb{Q} \subseteq K$ je abelovské. Nechť p je prvočíslo, $p\,\mathcal{O}_K = \mathcal{P}_1^e \cdot \,\cdots\, \cdot \mathcal{P}_r^e$ je rozklad ideálu $p\,\mathcal{O}_K$ na prvoideály. Pak $D(\mathcal{P}_1\,|p) = D(\mathcal{P}_2\,|p) = \cdots = D(\mathcal{P}_r\,|p)$, $E(\mathcal{P}_1\,|p) = E(\mathcal{P}_2\,|p) = \cdots = E(\mathcal{P}_r\,|p)$ a pokud je $E(\mathcal{P}_i\,|p)$ triviální, tak $\phi(\mathcal{P}_1\,|p) = \phi(\mathcal{P}_2\,|p) = \cdots = \phi(\mathcal{P}_r\,|p)$*

Důkaz je zřejmý; vidíme tedy, že pokud je rozšíření $\mathbb{Q} \subseteq K$ nejen Galoisovo, ale dokonce abelovské, záleží dekompoziční a inerční grupa i Frobeniův automorfismus pouze na prvočísle p.

Poznámka 5.3.1. Nechť p je prvočíslo. Je-li $\mathbb{Q} \subseteq K$ abelovské, budeme značit dekompoziční grupu příslušnou rozkladu prvočísla p v $\mathcal{O}_K$ jako $D(K,p)$, inerční grupu jako $E(K,p)$. Pokud je $E(K,p)$ triviální, Frobeniův automorfismus označíme $\phi(K,p)$.

Uvedeme nyní důležitou větu, která bude velmi užitečná nadále:

Věta 5.3.4. *Nechť $\mathbb{Q} \subseteq K$ je abelovské rozšíření, p je prvočíslo, M je libovolné mezitěleso rozšíření $\mathbb{Q} \subseteq K$. Označme $D = D(K,p), E = E(K,p)$. Pak:*

1. *p se zcela rozkládá v M, právě když $M \subseteq L_D$,*
2. *p se nevětví v M, právě když $M \subseteq L_E$.*

Po získání nových informací nyní shrňme do následující věty poznatky, které máme o větvení:

Věta 5.3.5. *Nechť $\mathbb{Q} \subseteq K$ je abelovské rozšíření, p je prvočíslo, $\mathcal{P}$ je prvoideál okruhu $\mathcal{O}_K$ takový, že $\mathcal{P}\,|p\,\mathcal{O}_K$, $E = E(\mathcal{P}\,|p)$. Pak jsou následující podmínky ekvivalentní:*

1. *p se větví v K,*

2. $p|d(\mathcal{O}_K)$,

3. $|E| > 1$,

4. $L_E \neq K$.

Předpokládejme nyní, že se dané prvočíslo p v K, nevětví a zaměřme se na Frobeniův automorfismus. Víme, že $\phi(\mathcal{P}\,|p)$ je zadán jako jediný automorfismus splňující $\phi(\mathcal{P}\,|p)(\alpha) \equiv \equiv \alpha^p \pmod{\mathcal{P}}$ pro všechna $\alpha \in \mathcal{O}_K$. Pokud je tedy $\mathbb{Q} \subseteq K$ abelovské, tak podle předchozí platí $\phi(K,p)(\alpha) \equiv \alpha^p \pmod{\mathcal{P}_i}$, kde $\mathcal{P}_i$ jsou všechny prvoideály okruhu $\mathcal{O}_K$, které dělí $p\,\mathcal{O}_K$. Pak tedy tato kongruence platí i modulo $\mathcal{I} = \bigcap_i \mathcal{P}_i$. To je však přímo ideál $p\,\mathcal{O}_K$, což můžeme ukázat následovně: jelikož $\mathcal{P}_i\,|p\,\mathcal{O}_K$ pro každé i, máme pro každé i také $p\,\mathcal{O}_K \subseteq \mathcal{P}_i$, tj. $p\,\mathcal{O}_K \subseteq \mathcal{I}$. Ale jelikož $\mathcal{I} \subseteq \mathcal{P}_i$ pro každé i, tak také $\mathcal{P}_i\,|\,\mathcal{I}$ a dohromady rovněž $p\,\mathcal{O}_K = \prod_i \mathcal{P}_i\,|\,\mathcal{I}$, tj. $\mathcal{I} \subseteq p\,\mathcal{O}_K$: celkem tedy $\mathcal{I} = p\,\mathcal{O}_K$.

Dostáváme tedy následující:

Věta 5.3.6. *Nechť $\mathbb{Q} \subseteq K$ je abelovské. Pak pro libovolné prvočíslo p, které se nevětví v K, a pro všechna $\alpha \in \mathcal{O}_K$ platí*

$$\phi(K,p)(\alpha) \equiv \alpha^p \pmod{p\,\mathcal{O}_K}.$$

Pokud je $\mathbb{Q} \subseteq K$ je abelovské, tak je i $\mathbb{Q} \subseteq M$ abelovské, kde M je libovolné mezitěleso rozšíření $\mathbb{Q} \subseteq K$. Ukážeme důležitou větu, jež bude hrát významnou roli v důkazu zákona kvadratické reciprocity:

Věta 5.3.7. *Nechť $\mathbb{Q} \subseteq K$ je abelovské, M je libovolné mezitěleso, p je libovolné prvočíslo, které se nevětví v K. Pak platí*

$$\phi(M,p) = \phi(K,p)\big|_M,$$

tedy $\phi(M,p)$ je roven restrikci $\phi(K,p)$ na M.

Důkaz. Z věty 5.3.6 víme, že pro všechna $\alpha \in \mathcal{O}_K$ platí $\phi(K,p)(\alpha) \equiv \alpha^p \pmod{p\,\mathcal{O}_K}$. Jelikož $\mathcal{O}_M \subseteq \mathcal{O}_K$, tak tato kongruence platí pro všechna $\alpha \in \mathcal{O}_M$; tedy z definice $\phi(K,p)(\alpha) - -\alpha^p \in p\,\mathcal{O}_K$. Pak tedy pro všechna $\alpha \in M$, platí $\phi(K,p)\big|_M(\alpha) - \alpha^p = \phi(K,p)(\alpha) - \alpha^p \in p\,\mathcal{O}_K \cap \mathcal{O}_M = p\,\mathcal{O}_M$, tj. $\phi(K,p)\big|_M(\alpha) \equiv \alpha^p \pmod{p\,\mathcal{O}_M}$. To je ale podmínka, již splňuje pouze automorfismus $\phi(M,p)$. Proto se oba automorfismy rovnají a tvrzení je dokázáno. □

Tato věta má následující důsledek:

Důsledek 5.3.8. *Nechť $\mathbb{Q} \subseteq K$ je abelovské rozšíření, M je libovolné mezitěleso tohoto rozšíření, $H = \mathrm{Gal}(K/M)$. Pak $\phi(K,p) \in H$, právě když $\phi(M,p) = \mathrm{id}_M$.*

Důkaz. Vzpomeňme si na důkaz části $2(c)$ hlavní věty Galoisovy teorie – v něm jsme ukázali, že všechny prvky grupy H se zužují na id_M. Také jsme ukázali, že id_M se rozšiřuje právě na prvky grupy H. Jelikož $\phi(M,p)$ je podle předchozí věty zúžením $\phi(K,p) \in H$ na M, tvrzení z toho okamžitě plyne.

□

Na závěr této kapitoly uvedeme jedno velmi hluboké tvrzení, které je důsledkem tzv. *class field theory*, která zkoumá číselná tělesa mnohem pokročilejšími metodami, než můžeme my v této práci.

Věta 5.3.9. *Nechť K je číselné těleso takové, že $\mathbb{Q} \subseteq K$ je abelovské rozšíření. Pak každý prvek grupy* $\mathrm{Gal}(K/\mathbb{Q})$ *je Frobeniovým automorfismem pro nekonečně mnoho prvočísel.*

V další kapitole uvidíme, že jedna významná věta o rozložení prvočísel – tzv. Dirichletova věta o prvočíslech v aritmetických posloupnostech – je pouhým důsledkem této velmi silné věty.

V této kapitole jsme se seznámili s algebraickou teorií čísel a získali jsme některé silné nástroje. V další kapitole budeme tuto teorii aplikovat na kvadratická a kruhová tělesa, abychom se dostali až ke kvadratickým zbytkům.

Kapitola 6

Aplikace algebraické teorie čísel na kvadratické zbytky

V prvních dvou částech této kapitoly podrobněji popíšeme situaci v kvadratických a kruhových tělesech. Ve třetí části pak dokážeme zákon kvadratické reciprocity a další tvrzení z teorie kvadratických zbytků.

6.1 Kvadratická tělesa

V následujícím textu bude m vždy značit celé číslo různé od jedné, které není dělitelné druhou mocninou žádného prvočísla.

Pro další text položme $K = \mathbb{Q}(\sqrt{m})$. Víme, že K je číselné těleso a $\mathbb{Q} \subseteq K$ je Galoisovo rozšíření stupně 2 s Galoisovou grupou $G \cong \mathbb{Z}/2\,\mathbb{Z}$. Teorie z předchozích kapitol nám dává následující lemma:

Lemma 6.1.1. *Nechť p je prvočíslo, $K = \mathbb{Q}(\sqrt{m})$. Pak platí právě jedno z následujcího:*

1. $p\,\mathcal{O}_K = \mathcal{P}^2$, $f(\mathcal{P}\,|p) = 1$,
2. $p\,\mathcal{O}_K = \mathcal{P}\mathcal{Q}$, $\mathcal{P} \neq \mathcal{Q}$, $f(\mathcal{P}\,|p) = f(\mathcal{Q}|p) = 1$,
3. $p\,\mathcal{O}_K = \mathcal{P}$, $f(\mathcal{P}\,|p) = 2$,

kde $\mathcal{P}, \mathcal{Q}$ jsou nějaké prvoideály okruhu $\mathcal{O}_K$. Navíc pro lichá prvočísla nastává možnost 1, právě když $p|m$.

Důkaz. Stačí aplikovat důsledek 5.1.4: jelikož $ref = 2$ (kde $e = e(K,p), f = f(K,p), r$ je počet prvoideálů dělících $p\,\mathcal{O}_K$), dostáváme pro možnosti $e = 2, r = 2, f = 2$ možnosti 1, 2, 3. Dodatek plyne z věty 5.3.5 a z toho, že $d(\mathcal{O}_K)$ je m nebo $4m$.

□

Uvědomme si, že v druhém případě se p zcela rozkládá v K.

Co se stane, když na prvoideály $\mathcal{O}_K$ dělící $p\,\mathcal{O}_K$ aplikujeme větu 4.3.9? Překvapivě se vrátíme ke kvadratickým zbytkům!

Nejdříve je však potřeba určit, pro která prvočísla můžeme větu 4.3.9 použít. Z věty 4.1.14 víme, že pokud $m \equiv 2,3 \pmod 4$, tak $\mathcal{O}_K = \mathbb{Z}[\sqrt{m}]$, tj. $|\,\mathcal{O}_K\,/\,\mathbb{Z}[\sqrt{m}]| = 1$. V případě $m \equiv 1 \pmod 4$ však $\mathcal{O}_K = \mathbb{Z}[\frac{1+\sqrt{m}}{2}]$. Ukážeme ale, že index $\mathbb{Z}[\sqrt{m}]$ v $\mathcal{O}_K$ je roven dvěma:

Lemma 6.1.2. *Nechť $m \equiv 1 \pmod 4$. Pak $|\,\mathcal{O}_K\,/\,\mathbb{Z}[\sqrt{m}]| = 2$.*

Důkaz. Uvědomme si, že v předchozím $\mathcal{O}_K$ i $\mathbb{Z}[\sqrt{m}]$ uvažujeme pouze jako aditivní grupy (podle předpokladů k větě 4.3.9). Uvažujme nyní homorfismus aditivních grup (pozor, nikoli okruhů!) $f : \mathcal{O}_K \to \mathbb{Z}\,/2\,\mathbb{Z}$ zadaný jako $f(a + b \cdot \frac{1+\sqrt{m}}{2}) = [b]_2$ pro libovolná celá čísla a, b. Zjevně se jedná o surjektivní homomorfismus a jeho jádro je (aditivní) grupa $\{a + 2k\frac{1+\sqrt{m}}{2} | a, k \in \mathbb{Z}\} = \mathbb{Z}[\sqrt{m}]$, tedy podle hlavní věty o faktorgrupách $\mathcal{O}_K\,/\,\mathbb{Z}[\sqrt{m}] \cong$ $\cong \mathbb{Z}\,/2\,\mathbb{Z}$ a tedy $|\,\mathcal{O}_K\,/\,\mathbb{Z}[\sqrt{m}]| = |\,\mathbb{Z}\,/2\,\mathbb{Z}\,| = 2$.

□

Pokud je tedy p liché prvočíslo, můžeme bez obav aplikovat větu 4.3.9 volbou $\alpha = \sqrt{m}$:

Věta 6.1.3. *Nechť $K = \mathbb{Q}(\sqrt{m})$, p je liché prvočíslo, p nedělí m. Pak následující podmínky jsou ekvivalentní:*

1. *p se zcela rozkládá v K,*
2. *m je kvadratický zbytek modulo p, tedy $\left(\frac{m}{p}\right) = 1$,*
3. *$p\,\mathcal{O}_K = (p, n - \sqrt{m})(p, n + \sqrt{m})$, kde $n^2 \equiv m \pmod p$.*

Dále $p\,\mathcal{O}_K$ je prvoideál $\mathcal{O}_K$, právě když $\left(\frac{m}{p}\right) = -1$. Navíc pokud p je liché prvočíslo, které dělí m, tak platí $p\,\mathcal{O}_K = (p, \sqrt{m})^2$.

Důkaz. Důkaz využívá větu 4.3.9 a lemma 6.1.1. Liché prvočíslo p se zcela rozkládá v K, právě když $p\,\mathcal{O}_K = \mathcal{P}\mathcal{Q}$, tedy podle věty 4.3.9 právě když $g \equiv g_1 g_2 \pmod p$, kde g je minimální polynom $\sqrt{m}$ nad $\mathbb{Q}$ a g_1, g_2 jsou normované ireducibilní polynomy. Jelikož $g(x) = x^2 - m$, dostáváme, že p se zcela rozkládá v K, právě když $x^2 - m \equiv (x + a)(x + b) \pmod p$ pro nějaká $a, b \in \mathbb{Z}$. To neznamená nic než že $x^2 - m$ má v $\mathbb{Z}\,/p\,\mathbb{Z}$ kořen, tedy existuje nějaké $n \in \mathbb{Z}$ takové, že $n^2 - m \equiv 0 \pmod p$, tedy $m \equiv n^2 \pmod p$. To ale znamená, že m je kvadratický zbytek modulo p.

Pak tedy $x^2 - m \equiv (x - n)(x + n) \pmod p$, tedy podle věty 4.3.9 $p\,\mathcal{O}_K = (p, \sqrt{m} - -n)(p, \sqrt{m} + n)$. Jelikož jistě $(p, \sqrt{m} \pm n) = (p, n \pm \sqrt{m})$, první část tvrzení je dokázána.

V případě $\left(\frac{m}{p}\right) = -1$ je polynom $x^2 - m$ ireducibilní, a tedy stupeň inercie příslušný prvočíslu p je roven dvěma. Tedy $p\,\mathcal{O}_K$ je opravdu prvoideál.

Pokud $p|m$, tak $x^2 - m \equiv x^2 \pmod p$ a tedy $p\,\mathcal{O}_K = (p, \sqrt{m})^2$. Tvrzení je tedy dokázáno.

□

Případ $p = 2$ vypadá následovně:

Věta 6.1.4. *Nechť $K = \mathbb{Q}(\sqrt{m})$. Potom se $2\,\mathcal{O}_K$ rozkládá na prvoideály okruhu $\mathcal{O}_K$ jako*

1. $(2, \sqrt{m})^2$ *pokud* $m \equiv 2 \pmod 4$,
2. $(2, 1 + \sqrt{m})^2$ *pokud* $m \equiv 3 \pmod 4$,
3. $(2, \frac{1-\sqrt{m}}{2})(2, \frac{1+\sqrt{m}}{2})$ *pokud* $m \equiv 1 \pmod 8$,
4. $2\,\mathcal{O}_K$, *tj. je prvoideál,* *pokud* $m \equiv 5 \pmod 8$.

Nebudeme se touto situací dopodrobna zabývat, jelikož to není pro další text užitečné. Poznamenejme jen, že zatímco v případech 1, 2 postupujeme podobně jako v předchozí větě, na případy 3 a 4 nemůžeme aplikovat větu 4.3.9, musíme si tedy poradit jinak: v případě 3 rovnost dokážeme obvyklým způsobem jako dvě inkluze. V případě 4 ukážeme, že pro libovolný prvoideál $\mathcal{P}$, který dělí $2\,\mathcal{O}_K$, platí $f(\mathcal{P}\,|2) = 2$. Ukážeme totiž, že $\mathcal{O}_K\,/\,\mathcal{P}$ není izomorfní se $\mathbb{Z}\,/2\,\mathbb{Z}$. A to tak, že vysvětlíme, že polynom $x^2 + x + \frac{1-m}{4}$ má v $\mathcal{O}_K\,/\,\mathcal{P}$ kořen, zatímco nad $\mathbb{Z}\,/2\,\mathbb{Z}$ je ireducibilní.

Nyní se podívejme, jak situace vypadá v tělesech kruhových.

6.2 Kruhová tělesa

V následujícím textu bude vždy n dané přirozené číslo a $\zeta_n = e^{\frac{2\pi i}{n}}$ bude primitivní n-tá odmocnina z jedné.

Nechť $K = \mathbb{Q}(\zeta_n)$. Víme již, že $\mathbb{Q} \subseteq K$ je Galoisovo a že $[K : \mathbb{Q}] = \varphi(n)$, kde φ je Eulerova funkce. Abychom zjistili, jak se prvoideál $p\,\mathcal{O}_K$ rozkládá, pišme $n = p^k m$, kde p není dělitelem přirozeného čísla m. Budeme sledovat, co se s prvočíslem p děje v tělesech $\mathbb{Q}(\zeta_{p^k})$ a $\mathbb{Q}(\zeta_m)$.

Lemma 6.2.1. *Za stejných předpokladů jako výše označme R okruh $\mathcal{O}_{\mathbb{Q}(\zeta_{p^k})} = \mathbb{Z}[\zeta_{p^k}]$. Pak $pR = (1 - \zeta_{p^k})^{\varphi(p^k)}$.*

Tedy p se v $\mathbb{Q}(\zeta_{p^k})$ totálně větví. Nebudeme se zdržovat důkazem tohoto tvrzení (lze ukázat pomocí věty 4.3.9 a kongruence $x^{p^k} - 1 \equiv (x-1)^{p^k} \pmod p$), protože nás bude především zajímat, co se děje v tělese $\mathbb{Q}(\zeta_m)$. Podstatné pro nás ale je, že z tohoto lemmatu plyne věta 3.3.7: z předchozího víme, že p se v $\mathbb{Q}(\zeta_p)$ totálně větví, tj. se větví i v kvadratickém podtělese K tělesa $\mathbb{Q}(\zeta_p)$. Jelikož $d(\mathbb{Z}[\zeta_p])$ je mocninou p, je p navíc jediné prvočíslo, které se v $\mathbb{Q}(\zeta_p)$ větví – je to tedy i jediné prvočíslo, které se větví v K, proto podle věty 5.3.5 nutně $d(\mathcal{O}_K) = p$. Z věty 4.1.14 můžeme snadno odvodit, že tato podmínka bude platit, právě když $K = \mathbb{Q}(\sqrt{p})$ a $p \equiv 1 \pmod 4$ nebo $K = \mathbb{Q}(\sqrt{-p})$ a $p \equiv 3 \pmod 4$. To můžeme shrnout do podmínky $K = \mathbb{Q}(\sqrt{p^*})$, kde $p^* = (-1)^{\frac{p-1}{2}} p$, což je přesně znění věty 3.3.7.

Přesuňme se nyní k tělesu $\mathbb{Q}(\zeta_m)$. Jelikož z věty 4.1.14 víme, že $d(\mathcal{O}_{\mathbb{Q}(\zeta_m)})$ dělí mocninu m, tak se p nevětví. Dekompoziční grupa $D(\mathbb{Q}(\zeta_m), p)$ je tedy cyklická; označme Frobeniův automorfismus, její generátor, jako ϕ. Připomeňme ještě, že

$$\mathrm{Gal}(\mathbb{Q}(\zeta_m)/\,\mathbb{Q}) = \{\sigma_k | 1 \leq k < m, \sigma_k(\zeta_m) = \zeta_m^k\}.$$

Za těchto předpokladů můžeme vyslovit následující větu:

Věta 6.2.2. *Předpokládejme všechno jako výše. Nechť ξ je celé číslo splňující $\xi \equiv p \pmod m$ takové, že $1 \leq \xi < m$. Pak $\phi_p = \sigma_\xi$.*

Důkaz. Frobeniův automorfismus je prvkem grupy $\mathrm{Gal}(\mathbb{Q}(\zeta_m)/\,\mathbb{Q})$, tedy musí být roven σ_k pro některé k. Které k to je, zjistíme tak, že jej aplikujeme na ζ_m. Z definice Frobeniova automorfismus dostáváme $\sigma_k(\zeta_m) = \zeta_m^k \equiv \zeta_m^p \pmod{p\,\mathbb{Z}[\zeta_m]}$, tedy p dělí $1-\zeta_m^{k-p}$ v okruhu $\mathbb{Z}[\zeta_m]$.

Ukažme sporem, že pak $m|k-p$. Kdyby ne, bylo by $\zeta_m^{k-p} \in \mathcal{M}_m \setminus \{1\}$ jedním z kořenů polynomu $f(x) = (x^m-1)/(x-1) = x^{m-1}+\cdots+x+1$. Jelikož $p|(1-\zeta_m^{k-p})$ a $(1-\zeta_m^{k-p})|f(1)$ (v okruhu $\mathbb{Z}[\zeta_m]$), platilo by $p|f(1)$, avšak $f(1) = m$, tedy dostáváme spor.

□

Vzpomeňme si, jak jsme definovali izomorfismus $\mathrm{Gal}(\mathbb{Q}(\zeta_m)/\,\mathbb{Q}) \to (\mathbb{Z}/m\,\mathbb{Z})^*$. Proto můžeme formulovat předchozí lemma i jinak: pokud p nedělí m, tak obraz Frobeniova automorfismu ϕ v izomorfismu výše je třída $[p]_m$.

Odbočme na chvíli a aplikujme na tento poznatek větu 5.3.9. Ta nám říká, že každý prvek Galoisovy grupy je Frobeniovým automorfismem pro nekonečně mnoho prvočísel. V případě kruhových těles to tedy znamená, že každá zbytková třída z $(\mathbb{Z}/m\,\mathbb{Z})^*$ je obrazem Frobeniova automorfismu pro nekonečně mnoho prvočísel, tedy každá tato třída podle předchozího lemmatu obsahuje nekonečně mnoho prvočísel. To je přesně znění Dirichletovy věty o prvočíslech v aritmetických posloupnostech. Jelikož sama tato věta je pokročilý výsledek, vidíme, jak silná věta 5.3.9 je.

Věta 6.2.2 má důležitý důsledek:

Důsledek 6.2.3. *Nechť $m \in \mathbb{Z}$, p je prvočíslo, p nedělí m. Nechť $f = f(\mathcal{P}_i\,|p)$ pro prvoideály $\mathcal{P}_i$ okruhu $\mathcal{O}_{\mathbb{Q}(\zeta_m)} = \mathbb{Z}[\zeta_m]$, které dělí $p\,\mathbb{Z}[\zeta_m]$. Pak f je rovno řádu prvočísla p modulo m.*

Důkaz. Ukázali jsme si, že Frobeniův automorfismus příslušný k p odpovídá zbytkové třídě $[p]_m$. Jelikož dekompoziční grupa je Frobeniovým automorfismem generovaná, tak $|D|$ je roven jeho řádu v Galoisově grupě, který je roven řádu $[p]_m$ v $(\mathbb{Z}/m\,\mathbb{Z})^*$. Jelikož $f = |D|$, důkaz je hotov.

□

To, jak se rozkládá p v $\mathbb{Q}(\zeta_n)$ pro libovolné n, nyní poskládáme z předchozích dvou případů. Napíšeme $n = p^k m$, kde p nedělí m. Kvůli tomu, že jsme definice indexu větvení a stupně inercie vyslovili jen ve speciálním případě $\mathbb{Q} \subseteq K$, nemůžeme důkaz provést zcela

korektně, ale myšlenka je jednoduchá: z lemmatu 6.2.1 dostaneme $e \geq \varphi(p^k)$ a z věty 6.2.2 pak $fr \geq \varphi(m)$, dohromady $ref \geq \varphi(p^k)\,\varphi(m) = \varphi(n)$. Jelikož $ref = \varphi(n)$, nastává v této nerovnosti rovnost, právě když se nám známé e, f, r z předchozích případů nebude měnit. Dostaneme tedy:

Věta 6.2.4. *Je-li K n-té kruhové těleso, kde $n = p^k m$ a $p \nmid m$, dostáváme $e(K,p) = \varphi(p^k)$ a $f(K,p)$ je řád prvku p modulo m.*

6.3 Kvadratické zbytky

Účelem této části bude aplikovat předchozí teorii na kvadratické zbytky. Budeme používat především dvou výše dokázaných tvrzení: první z nich je, že $\left(\frac{m}{p}\right) = 1$, právě když se p zcela rozkládá v $\mathbb{Q}(\sqrt{m})$. Druhé pak, že Frobeniův automorfismus příslušný prvočíslu p v tělese $\mathbb{Q}(\zeta_n)$, $p \nmid n$ odpovídá zbytkové třídě $[p]_m$.

Proč právě kvadratická a kruhová tělesa? Dokažme nejprve jeden z vedlejší zákonů kvadratické reciprocity:

Věta 6.3.1. *Nechť p je liché prvočíslo. Pak $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$, neboli*

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{pokud } p \equiv 1 \pmod 4, \\ -1 & \text{pokud } p \equiv 3 \pmod 4. \end{cases}$$

Důkaz. Jelikož $p \nmid d(\mathbb{Z}[i]) = 4$, tak $E(\mathbb{Q}(i), p)$ je triviální a $D(\mathbb{Q}(i), p)$ je cyklická. Jistě je $\mathbb{Q}(i) = \mathbb{Q}(\sqrt{-1})$ kvadratické těleso. Proto podle věty 6.1.3 $\left(\frac{-1}{p}\right) = 1$, právě když se p zcela rozkládá v $\mathbb{Q}(i)$. V tom případě tedy $f(\mathbb{Q}(i), p) = 1$.

Také ovšem $\mathbb{Q}(i) = \mathbb{Q}(\zeta_4)$ je kruhové těleso. Tedy podle důsledku 6.2.3 $f(\mathbb{Q}(i), p) = 1$, právě když je řád prvku p modulo 4 roven jedné. To nastane, právě když $p \equiv 1 \pmod 4$. Tím je tvrzení dokázáno.

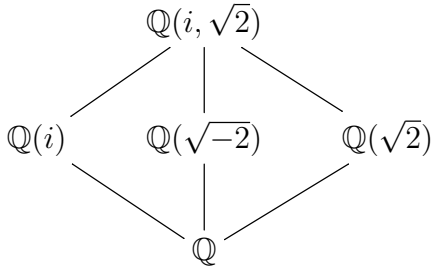
□

A další z nich:

Věta 6.3.2. *Nechť p je liché prvočíslo. Pak $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$, neboli*

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{pokud } p \equiv \pm 1 \pmod 8 \\ -1 & \text{pokud } p \equiv \pm 3 \pmod 8. \end{cases}$$

Důkaz. Uvažujme těleso $\mathbb{Q}(i, \sqrt{2}) = \mathbb{Q}(\zeta_8)$, tedy opět těleso kruhové a tentokrát ne kvadratické, ale bikvadratické. Jeho svaz podtěles můžeme vidět na diagramu níže.



Nyní využijeme Galoisovy teorie, a to tak, že popíšeme grupu $G = \mathrm{Gal}(\mathbb{Q}(i,\sqrt{2})/\mathbb{Q})$ dvojím způsobem. Zaprvé jako Galoisovu grupu bikvadratického tělesa: $G = \{\mathrm{id}, \sigma, \tau, \sigma\tau\}$, kde τ fixuje $\mathbb{Q}(\sqrt{2})$ a i zobrazí na $-i$, σ fixuje $\mathbb{Q}(i)$ a $\sqrt{2}$ zobrazí na $-\sqrt{2}$. Zadruhé jako Galoisovu grupu kruhového tělesa: $G = \{\sigma_1, \sigma_3, \sigma_5, \sigma_7\}$, kde $\sigma_k(\zeta_8) = \zeta_8^k$. Zjistíme, jak si tato dvě vyjádření odpovídají tím, že automorfismy z „bikvadratického“ vyjádření budeme aplikovat na $\zeta_8 = \frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}$. Nejdříve si ale napišme, jak příslušné mocniny vypadají:

- $\zeta_8^1 = \frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}$,
- $\zeta_8^3 = (\frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2})^3 = -\frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}$,
- $\zeta_8^5 = (\frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2})^5 = -\frac{\sqrt{2}}{2} - i\frac{\sqrt{2}}{2}$,
- $\zeta_8^7 = (\frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2})^7 = \frac{\sqrt{2}}{2} - i\frac{\sqrt{2}}{2}$.

Nyní aplikujme:

- $\mathrm{id}(\frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}) = \frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2} = \zeta_8^1 \Rightarrow \mathrm{id} = \sigma_1$,
- $\sigma(\frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}) = -\frac{\sqrt{2}}{2} - i\frac{\sqrt{2}}{2} = \zeta_8^5 \Rightarrow \sigma = \sigma_5$,
- $\tau(\frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}) = \frac{\sqrt{2}}{2} - i\frac{\sqrt{2}}{2} = \zeta_8^7 \Rightarrow \tau = \sigma_7$,
- $(\sigma\tau)(\frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}) = -\frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2} = \zeta_8^3 \Rightarrow \sigma\tau = \sigma_3$.

Pak už stačí jen projít všechny možnosti pro prvočíslo p:

- $p \equiv 1 \pmod 8 \Rightarrow \phi_p = \sigma_1 = \mathrm{id} \Rightarrow D = \{\mathrm{id}\} \Rightarrow L_D = \mathbb{Q}(i,\sqrt{2}) \Rightarrow p$ se v $\mathbb{Q}(\sqrt{2})$ zcela rozkládá $\Rightarrow \left(\frac{2}{p}\right) = 1$,
- $p \equiv 3 \pmod 8 \Rightarrow \phi_p = \sigma_3 = \sigma\tau \Rightarrow D = \langle\sigma\tau\rangle \Rightarrow L_D = \mathbb{Q}(i\sqrt{2}) \Rightarrow p$ se v $\mathbb{Q}(\sqrt{2})$ zcela nerozkládá $\Rightarrow \left(\frac{2}{p}\right) = -1$,
- $p \equiv 5 \pmod 8 \Rightarrow \phi_p = \sigma_5 = \sigma \Rightarrow D = \langle\sigma\rangle \Rightarrow L_D = \mathbb{Q}(i) \Rightarrow p$ se v $\mathbb{Q}(\sqrt{2})$ zcela nerozkládá $\Rightarrow \left(\frac{2}{p}\right) = -1$,
- $p \equiv 7 \pmod 8 \Rightarrow \phi_p = \sigma_7 = \tau \Rightarrow D = \langle\tau\rangle \Rightarrow L_D = \mathbb{Q}(\sqrt{2}) \Rightarrow p$ se v $\mathbb{Q}(\sqrt{2})$ zcela rozkládá $\Rightarrow \left(\frac{2}{p}\right) = 1$.

Tím je tvrzení dokázáno.

□

Vidíme, že se nám v předchozích důkazech dařilo dobře. To však nikoli proto, že by to snad byla jednoduchá tvrzení, ale kvůli nesmírné síle teorie, kterou jsme vybudovali dříve.

Klíčem k úspěchu bylo v obou tvrzeních využít poznatky o kvadratických a kruhových tělesech zároveň. Co však dělat, když je kruhové těleso, které potřebujeme, „větší“ než bikvadratické? Uvidíme, že to pro nás nebude obtíž a povede se nám dokázat i hlavní zákon kvadratické reciprocity.

Ukážeme dva důkazy. První z nich je uveden v [1]. Druhý z nich je méně technický a o něco abstraktnější.

Nejprve dokážeme, že se hlavní zákonem kvadratické reciprocity je ekvivalentní podobné tvrzení:

Věta 6.3.3. *Nechť p, q jsou různá lichá prvočísla. Hlavní zákon kvadratické reciprocity je ekvivalentní s rovností*

$$\left(\frac{p^*}{q}\right) = \left(\frac{q}{p}\right),$$

kde $p^* = (-1)^{\frac{p-1}{2}} p$.

Důkaz. Rozepíšme si danou rovnost podle toho, jaký zbytek dávají prvočísla p a q po dělení čtyřmi.

Pokud $p \equiv 1 \pmod 4$, tak $p^* = p$ a tedy $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$.

Pokud $p \equiv 3 \pmod 4$, tak $p^* = -p$ a tedy $\left(\frac{q}{p}\right) = \left(\frac{-p}{q}\right) = \left(\frac{-1}{q}\right) \cdot \left(\frac{p}{q}\right)$ (předpokládáme multiplikativitu Legendreova symbolu, ale není třeba se ničeho obávat, jelikož zanedlouho ji dokážeme). Pokud $q \equiv 1 \pmod 4$, tak $\left(\frac{-1}{q}\right) = 1$, pokud $q \equiv 3 \pmod 4$, tak $\left(\frac{-1}{q}\right) = -1$.

Dohromady tedy dostáváme

$$\left(\frac{p}{q}\right) = \begin{cases} \left(\frac{q}{p}\right) & \text{pokud } p \text{ nebo } q \equiv 1 \pmod 4, \\ -\left(\frac{q}{p}\right) & \text{pokud } p \equiv q \equiv 3 \pmod 4. \end{cases}$$

To je ale přesně znění hlavního zákona kvadratické reciprocity. Tím je tedy důkaz hotov.

□

Nyní se můžeme pustit do prvního důkazu. Připomeňme nejprve situaci z poznámky 3.3.1: pro prvočíslo p je $G = \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \cong (\mathbb{Z}/p\mathbb{Z})^*$ cyklická grupa řádu $p-1$ a mezitělesa rozšíření $\mathbb{Q} \subseteq \mathbb{Q}(\zeta_p)$ jsou fixována podgrupami H_d grupy G majícími v G index d, kde d jsou kladní dělitelé čísla $p-1$. Označíme nyní $F_d = \mathrm{Fix}(H_d)$; mj. platí $F_{d_1} \subseteq F_{d_2}$, právě když $d_1 | d_2$. Tedy např. $F_1 = \mathbb{Q}$ a především $F_2 = \mathbb{Q}(\sqrt{p^*})$, jak víme z věty 3.3.7.

Za těchto podmínek vyslovme následující lemma, které zobecňuje argument, jenž v důkazu použijeme:

Lemma 6.3.4. *Nechť p, q jsou dvě různá prvočísla, d je kladný dělitel čísla $p-1$, F_d mezitěleso rozšíření $\mathbb{Q} \subseteq \mathbb{Q}(\zeta_p)$ jako výše. Pak existuje $a \in \mathbb{Z}$ takové, že $q \equiv a^d \pmod p$, právě když se q zcela rozkládá v F_d.*

Důkaz. Uvědomme si, že existuje celé číslo a splňující $q \equiv a^d \pmod{p}$, právě když $q^{\frac{p-1}{d}} \equiv 1 \pmod{p}$, tedy právě když je řád prvku q modulo p dělitelem čísla $\frac{p-1}{d}$. Tím je ale $f = f(\mathbb{Q}(\zeta_p), q)$, tedy existuje celé číslo a splňující $q \equiv a^d \pmod{p}$, právě když $f|\frac{p-1}{d}$. Tato podmínka je ale ekvivalentní s $d|\frac{p-1}{f}$. Avšak jelikož $e = 1$, tak $ref = rf = p-1$ a $\frac{p-1}{f} = r$. Proto $q \equiv a^d \pmod{p} \Leftrightarrow d|r \Leftrightarrow F_d \subseteq F_r$. Ale F_r není nic jiného než dekompoziční těleso prvočísla q, jelikož je to jediné mezitěleso stupně r nad $\mathbb{Q}$ (využíváme poznatky z věty 5.2.6). Navíc $F_d \subseteq F_r$, (podle věty 5.3.4) právě když se q zcela rozkládá v F_d. Tím je tvrzení dokázáno.

□

Nyní se již dostaneme k hlavnímu zákonu kvadratické reciprocity:

Věta 6.3.5. *Nechť p, q jsou různá lichá prvočísla. Potom $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right) \cdot (-1)^{\frac{(p-1)(q-1)}{4}}$, neboli*

$$\left(\frac{p}{q}\right) = \begin{cases} \left(\frac{q}{p}\right) & \text{pokud } p \equiv 1 \text{ nebo } q \equiv 1 \pmod{4}; \\ -\left(\frac{q}{p}\right) & \text{pokud } p \equiv q \equiv 3 \pmod{4}. \end{cases}$$

Důkaz. Jelikož q je kvadratický zbytek modulo p, právě když existuje $a \in \mathbb{Z}$ takové, že $q \equiv a^2 \pmod{p}$, můžeme využít předchozí lemma pro $d = 2$ a a vidíme, že $\left(\frac{q}{p}\right) = 1$, právě když se q zcela rozkládá v F_2, což není podle věty 3.3.7 nic jiného než těleso $\mathbb{Q}(\sqrt{p^*})$. Avšak q se zcelá rozkládá v $\mathbb{Q}(\sqrt{p^*})$, právě když $\left(\frac{p^*}{q}\right) = 1$ Dostáváme tedy $\left(\frac{q}{p}\right) = 1 \Leftrightarrow \left(\frac{p^*}{q}\right) = 1$ a z toho hned $\left(\frac{q}{p}\right) = \left(\frac{p^*}{q}\right)$. To už však není nic jiného než znění zákona kvadratické reciprocity, jak jsme ukázali ve větě 6.3.3.

□

Nyní uvedeme ještě jeden důkaz kvadratické reciprocity, snad dokonce krásnější ve své jednoduchosti:

Důkaz. Stejně jako výše $\left(\frac{q}{p}\right) = 1$, právě když existuje a splňující $q \equiv a^2 \pmod{p}$. Označme nyní H podgrupu indexu 2 v $G = \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$. To je $\frac{p-1}{2}$-prvková podgrupa grupy G, tedy fixuje těleso $F_2 = \mathbb{Q}(\sqrt{p^*})$.

Uvažujme izomorfismus $G \cong (\mathbb{Z}/p\mathbb{Z})^*$. V něm podgrupa H odpovídá podgrupě čtverců, tj. grupě $K = \{[a^2]_p | a \in \mathbb{Z}, p \nmid a\}$ (to plyne z věty 1.0.3). Potom tedy $\left(\frac{q}{p}\right) = 1 \Leftrightarrow [q]_p \in K \Leftrightarrow$ $\Leftrightarrow \phi(\mathbb{Q}(\zeta_p), q) \in H$ (v poslední rovnosti jsme opět využili toho, že Frobeniův automorfismus příslušný q odpovídá třídě $[q]_p$).

Vzpomeňme si nyní na důsledek 5.3.8 věty 5.3.7. Podle něj $\phi(\mathbb{Q}(\zeta_p), q) \in H$, právě když $\phi(\mathrm{Fix}(H), p) = \phi(\mathbb{Q}(\sqrt{p^*}), q) = \mathrm{id}$. Tudíž $D(\mathbb{Q}(\sqrt{p^*}), q) = \{\mathrm{id}\}$. Přešli jsme tedy od dekompoziční grupy prvočísla q v kruhovém tělese k dekompoziční grupě prvočísla q v kvadratickém tělese. Označíme-li tuto novou dekompoziční grupu jako D, máme $L_D = \mathrm{Fix}(\{\mathrm{id}\}) = \mathbb{Q}(\sqrt{p^*})$, což nastane, právě když se q zcela rozkládá v $\mathbb{Q}(\sqrt{p^*})$. To je ekvivalentní s $\left(\frac{p^*}{q}\right) = 1$. Dohromady s předchozím tedy opět dostáváme $\left(\frac{q}{p}\right) = 1 \Leftrightarrow \left(\frac{p^*}{q}\right) = 1$ a z toho okamžitě plyne hlavní zákon kvadratické reciprocity.

□

Pro přehlednost stručně zopakujme argumenty, které jsme použili. V prvním důkaze (f značí stupeň inercie q v $\mathbb{Q}(\zeta_p)$ a r počet prvoideálů okruhu $\mathbb{Z}[\zeta_p]$ dělících $q\,\mathbb{Z}[\zeta_p]$):

$$\begin{aligned}\left(\frac{q}{p}\right) = 1 &\Leftrightarrow \exists a \in \mathbb{Z} : q \equiv a^2 \pmod{p} \\ &\Leftrightarrow q^{\frac{p-1}{2}} \equiv 1 \pmod{p} \\ &\Leftrightarrow \text{ řád } q \text{ modulo } p \text{ dělí } \frac{p-1}{2} \\ &\Leftrightarrow f(\mathbb{Q}(\zeta_p), q) \Big| \frac{p-1}{2} \\ &\Leftrightarrow 2 \Big| \frac{p-1}{f} = r \\ &\Leftrightarrow F_2 \subseteq F_r = L_{D(\mathbb{Q}(\zeta_p),q)} \\ &\Leftrightarrow q \text{ se zcela rozkládá v } F_2 = \mathbb{Q}(\sqrt{p^*}) \\ &\Leftrightarrow \left(\frac{p^*}{q}\right) = 1.\end{aligned}$$

V druhém pak (H opět značí podgrupu grupy $\mathrm{Gal}(\mathbb{Q}(\zeta_m)/\,\mathbb{Q})$ indexu 2):

$$\begin{aligned}\left(\frac{q}{p}\right) = 1 &\Leftrightarrow \exists a \in \mathbb{Z} : q \equiv a^2 \pmod{p} \\ &\Leftrightarrow [q]_p \in K = \{[a^2]_p | a \in \mathbb{Z}, p \nmid a\} \\ &\Leftrightarrow \phi(\mathbb{Q}(\zeta_p), q) \in H \cong K \\ &\Leftrightarrow \phi(\mathbb{Q}(\sqrt{p^*}), q) = \phi(\mathrm{Fix}(H), q) = \mathrm{id} \\ &\Leftrightarrow L_{D(\mathbb{Q}(\sqrt{p^*}),q)} = \mathbb{Q}(\sqrt{p^*}) \\ &\Leftrightarrow q \text{ se zcela rozkládá v } \mathbb{Q}(\sqrt{p^*}) \\ &\Leftrightarrow \left(\frac{p^*}{q}\right) = 1.\end{aligned}$$

Tím máme hotovo to hlavní, co jsme si v textu kladli za cíl: pomocí algebraické teorie čísel dokázat využitím dekompozičních grup zákon kvadratické reciprocity.

U toho se ale nezastavíme a aplikujeme tuto teorii na další tvrzení z teorie kvadratických zbytků. Začneme multiplikativitou Legendreova symbolu:

Věta 6.3.6. *Pro libovolná celá čísla a, b a liché prvočíslo p platí:* $\left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$.

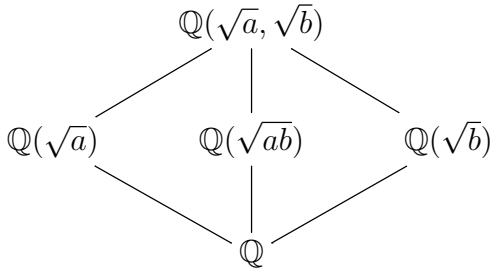
Důkaz. K důkazu této věty využijeme těleso $\mathbb{Q}(\sqrt{a}, \sqrt{b})$. Uvažujme nejprve $p|ab$. Pak $\left(\frac{a}{p}\right) = = 0$ nebo $\left(\frac{b}{p}\right) = 0$, ovšem také $\left(\frac{ab}{p}\right) = 0$, tudíž tvrzení platí. Předpokládejme tedy dále, že $p \nmid ab$, tj. p se nevětví v $\mathbb{Q}(\sqrt{a}, \sqrt{b})$.

Pokud je a nebo b druhá mocnina celého čísla, bez újmy na obecnosti můžeme předpokládat $a = k^2$, $k \in \mathbb{Z}$. Pak dostáváme $\left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right) = \left(\frac{k^2}{p}\right) \cdot \left(\frac{b}{p}\right) = \left(\frac{b}{p}\right)$. Dále můžeme jistě říct,

že $ab = k^2 b$ je kvadratický zbytek modulo p, právě když je b kvadratický zbytek modulo p, z čehož plyne $\left(\frac{ab}{p}\right) = \left(\frac{b}{p}\right)$, tvrzení tedy v tomto případě platí.

Pokud a ani b není druhá mocnina celého čísla, ale ab ano, je $\left(\frac{ab}{p}\right) = 1$. Jelikož můžeme psát $ab = k^2$ pro vhodné celé číslo k, dostáváme $ab \equiv k^2 \pmod{}$, z čehož plyne $\left(\frac{a}{p}\right) = 1$, právě když $\left(\frac{b}{p}\right) = 1$, tedy $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$ a $\left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right) = 1 = \left(\frac{ab}{p}\right)$. Tvrzení tedy platí i v tomto případě.

Nyní se konečně můžeme pustit do případu, kdy $p \nmid ab$ a ani a, ani b, ani ab není druhou mocninou celého čísla. Můžeme předpokládat, že $a, b \notin \{0, 1\}$ a ani a, ani b není dělitelné druhou mocninou žádného prvočísla (platilo-li by např. $a = q^2 k$ pro nějaké prvočíslo q a celé číslo k, z předchozího bychom dostali $\left(\frac{a}{p}\right) = \left(\frac{k}{p}\right)$). Potom je tedy $\mathbb{Q}(\sqrt{a}, \sqrt{b})$ bikvadratické těleso. Projdeme nyní jednotlivé případy podle toho, které z mezitěles rozšíření $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{a}, \sqrt{b})$ je dekompozičním tělesem vzhledem k dekompoziční grupě $D = D(\mathbb{Q}(\sqrt{a}, \sqrt{b}), p)$.



Jistě to není těleso $\mathbb{Q}$, protože pak by $D \cong (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$ nebyla cyklická, což by byl spor s tím, že p se nevětví. Pokud $L_D = \mathbb{Q}(\sqrt{a}, \sqrt{b})$, tak se p zcela rozkládá v $\mathbb{Q}(\sqrt{a}), \mathbb{Q}(\sqrt{b})$ i $\mathbb{Q}(\sqrt{ab})$. Proto $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right) = 1$, tvrzení tedy v tomto případě platí.

Pokud $L_D = \mathbb{Q}(\sqrt{a})$, tak se p zcela rozkládá pouze v $\mathbb{Q}(\sqrt{a})$, tedy $\left(\frac{a}{p}\right) = 1$ a také $\left(\frac{ab}{p}\right) = \left(\frac{b}{p}\right) = -1$. Tvrzení v tomto případě opět platí. V případě $L_D = \mathbb{Q}(\sqrt{b})$ můžme postupovat zcela analogicky.

Konečně pokud $L_D = \mathbb{Q}(\sqrt{ab})$, tak se p zcela rozkládá pouze v $\mathbb{Q}(\sqrt{ab})$, tedy $\left(\frac{ab}{p}\right) = 1$, $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right) = -1$. Tvrzení platí i nyní, platí tedy v všech možných situacích. Tím je důkaz hotov.

□

Nyní dokážeme ještě obecnější tvrzení, z nějž multiplikativita Legendreova symbolu přímo plyne, a tím je Eulerovo kritérium.

Věta 6.3.7. *Nechť $a \in \mathbb{Z}$, p je liché prvočíslo. Pak platí*

$$a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \pmod{p}.$$

Důkaz. Nejprve si uvědomme, že pokud $p|a$, tvrzení je zřejmé, protože na obou stranách kongruence figuruje nula. Předpokládejme tedy, že p nedělí a.

Důkaz lze vést mnoha způsoby, zřejmě nejjednodušší bude si vzpomenout na Dirichletovu větu o prvočíslech v aritmetických posloupnostech. Ta nám zaručuje existenci lichého prvočísla q, které leží s a ve stejné zbytkové třídě modulo p, tedy tvrzení, jež dokazujeme, je ekvivalentní s $q^{\frac{p-1}{2}} \equiv \left(\frac{q}{p}\right) \pmod p$ (druhý způsob, jak říci, že tvrzení stačí dokazovat pro lichá prvočísla, je zohlednit multiplikativitu Legendreova symbolu: víme, že obě strany dokazované kongruence jsou multiplikativní a a je součinem vhodných prvočísel).

Jistě ale $q^{p-1} \equiv 1 \pmod p$ (to je malá Fermatova věta). Proto $0 \equiv q^{p-1} - 1 = (q^{\frac{p-1}{2}} - 1)(q^{\frac{p-1}{2}} + 1)$, tudíž $q^{\frac{p-1}{2}} \equiv \pm 1 \pmod p$. V důkazu zákona kvadratické reciprocity jsme již ale viděli, že $q^{\frac{p-1}{2}} \equiv 1 \pmod p$, právě když $\left(\frac{q}{p}\right) = 1$. Tím je tvrzení dokázáno. □

Dále můžeme ukázat následující:

Věta 6.3.8. *Nechť a je celé číslo, které není čtverec. Pak existuje nekonečně mnoho prvočísel p, pro něž platí $\left(\frac{a}{p}\right) = 1$, a nekonečně mnoho prvočísel q, pro něž platí $\left(\frac{a}{q}\right) = -1$.*

Důkaz. Dokazovat toto tvrzení elementárními prostředky není úplně jednoduché. Pro nás to však jednoduché bude: tvrzení je přímým důsledkem věty 5.3.9. Uvědomme si, že napíšeme-li a ve tvaru $k^2 m$, kde m není dělitelné druhou mocninou žádného prvočísla (a z předpokladu to není ani 1 nebo 0), tak

$$\left(\frac{a}{p}\right) = \left(\frac{k^2 m}{p}\right) = \left(\frac{k}{p}\right)^2 \cdot \left(\frac{m}{p}\right) = \left(\frac{m}{p}\right)$$

pro všechna lichá prvočísla p (ve výpočtu jsme využili multiplikativitu Legendreova symbolu), tj. tvrzení stačí dokazovat pro m.

Podle věty 5.3.9 je každý prvek Galoisovy grupy $\mathrm{Gal}(\mathbb{Q}(\sqrt{m})/\mathbb{Q})$ Frobeniovým automorfismem pro nekonečně mnoho prvočísel. Existuje tedy nekonečně mnoho prvočísel p takových, že $\phi = \mathrm{id}$, tedy $D = \{\mathrm{id}\}, L_D = \mathbb{Q}(\sqrt{m}), \left(\frac{m}{p}\right) = 1$, a také nekonečně mnoho prvočísel q takových, že $\phi = \sigma$ ($\sigma : \sqrt{m} \mapsto -\sqrt{m}$), tedy $D = \langle \sigma \rangle, L_D = \mathbb{Q}, \left(\frac{m}{q}\right) = -1$. □

Tuto kapitolu zakončíme tvrzením, které aplikuje předchozí teorii na problém z oblasti diofantických rovnic:

Věta 6.3.9. *Nechť p je liché prvočíslo. Pak rovnice $x^2 + y^2 = p$ má celočíselná řešení, právě když $p \equiv 1 \pmod 4$.*

Důkaz. Na důkaz jednoho směru ekvivalence ani nepotřebujeme předchozí teorii. Předpokládejme, že $p = x^2 + y^2$ celočíselná řešení má, dejme tomu $x = a, y = b$. Pak mají a, b různou paritu, jelikož jinak bychom dostali $p \equiv 0 \pmod 2$, což je spor. Tedy jedno z nich je sudé, např. a, a druhé liché, např. b. Pak $p = a^2 + b^2 \equiv 0 + 1 = 1 \pmod 4$.

Na důkaz druhého směru již potřebujeme teorii, kterou jsme vybudovali. Předpokládejme $p \equiv 1 \pmod 4$. Pak $\left(\frac{-1}{p}\right) = 1$, tudíž se p zcela rozkládá v $\mathbb{Z}[i]$. Je ale známo, že $\mathbb{Z}[i]$ je okruh hlavních ideálů, proto můžeme psát $p\,\mathbb{Z}[i] = (p) = (a + bi) \cdot (c + di)$, $a, b, c, d \in \mathbb{Z}$.

Podle věty 5.1.2 jsou ideály dělící $p\,\mathbb{Z}[i]$ komplexně sdružené (Galoisova grupa rozšíření $\mathbb{Q} \subseteq \mathbb{Q}(i)$ se skládá z identity a z $\tau : a+bi \mapsto a-bi$). Můžeme tedy dokonce psát $(p) = (a+$ $+bi)\cdot(a-bi)$ pro nějaká celá čísla a, b. Pak z příkladu 4.2.2 $(p) = ((a+bi)(a-bi)) = (a^2+b^2)$ a $p = u(a^2 + b^2)$, kde u je nějaká jednotka okruhu $\mathbb{Z}[i]$. Je ale známo, že jednotky toho okruhu jsou $1, -1, i, -i$ a jelikož $u = \frac{p}{a^2+b^2}$ je kladné racionální číslo, tak $u = 1$ a rovnice $x^2 + y^2 = p$ má celočíselná řešení $x = a, y = b$.

□

Závěr

Díky dekompozičním grupám jsme získali mnoho informací o kvadratických zbytcích a dokázali zákon kvadratické reciprocity. Můžeme však ale definovat i reciprocitu vyšších řádů – např. kubickou reciprocitu, kde Legendreův symbol zobecňujeme na kubický mocninný symbol

$$\left(\frac{\alpha}{\pi}\right)_3 \equiv \alpha^{\frac{N(\pi)-1}{3}} \pmod{\pi}$$

pro $\alpha, \pi \in \mathbb{Z}[\zeta_3]$, kde π je libovolný prvočinitel tohoto okruhu a $N(\pi) = |\,\mathbb{Z}[\zeta_3]/\pi\,\mathbb{Z}[\zeta_3]|$. Zákon kubické reciprocity je pak překvapivě jednoduchého tvaru

$$\left(\frac{\theta}{\pi}\right)_3 = \left(\frac{\pi}{\theta}\right)_3,$$

kde π, θ jsou libovolní primární prvočinitelé (tzn. dávají zbytek dva po dělení třemi) splňující $N(\theta) \neq N(\pi)$.

Přirozenou otázkou je, jak zobecnit poznatky o Legendreově symbolu (který se obdobným způsobem jako v kubickém případě zobecňuje na tzv. *n-tý mocninný symbol*) a zákon kvadratické reciprocity? V případě kubické a bikvadratické reciprocity si matematici zvládli poradit zobecněním důkazu kvadratické reciprocity využívajícího Gaussovy sumy. Dále už však měli problém.

Ukázalo se, že správná cesta je ta, již jsme zvolili v této práci – pomocí algebraické teorie čísel. Ovšem na vyšší úrovni, než jaké jsme dosáhli my – jedná se o *class field theory*, kterou jsme již zmínili v souvislosti s větou 5.3.9. Jedním z jejích hlavních výsledků je tzv. *Artinův zákon reciprocity*. Jedním z jeho důsledků je právě *Zákon reciprocity n-tých mocninných symbolů* zobecňující kvadratickou reciprocitu. Zajímavé je, že jedním z objektů použitých k důkazům těchto vět je právě námi používaný Frobeniův automorfismus.

Literatura

[1] MARCUS, Daniel A.: *Number fields*. New York: Springer-Verlag, 1977.

[2] IRELAND, K. a M. ROSEN: *A Classical Introduction to Modern Number Theory*. New York: Springer-Verlag, 1999.

[3] ROSICKÝ, Jiří: *Algebra*. Brno: Masarykova univerzita, 2002.

[4] BENEŠ, Petr: *Zákony reciprocity*. Diplomová práce. Brno: Masarykova univerzita, 2010.

[5] DUMMIT, D. S. a R. M. FOOTE: *Abstract Algebra*. New York: Wiley, 2004.

[6] PUPÍK, Petr: *Užití grupy tříd ideálů při řešení některých diofantických rovnic*. Diplomová práce. Brno: Masarykova univerzita, 2009.

[7] WASHINGTON, Lawrence C.: *Introduction to Cyclotomic Fields*. New York: Springer-Verlag, 1997.

[8] COX, David A.: *Primes of the form* $x^2 + ny^2$: *Fermat, Class Field Theory, and Complex Multiplication*. New York: Wiley, 1989.