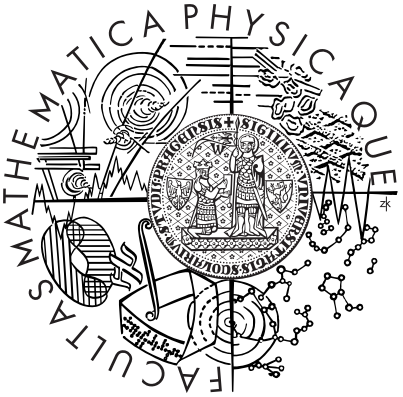
Univerzita Karlova v Praze
Matematicko-fyzikální fakulta

# BAKALÁŘSKÁ PRÁCE




David Kubečka

## Cyklotomická tělesa

Katedra algebry

Vedoucí bakalářské práce: Mgr. Pavel Příhoda, Ph.D.

Studijní program: Matematika, obecná matematika

2009

Rád bych poděkoval vedoucímu své práce Mgr. Pavlu Příhodovi, Ph.D. za trpělivost při vysvětlování látky a za spoustu inspirujících poznámek.

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

V Praze dne 27. května 2009 David Kubečka

# Obsah

Název práce: Cyklotomická tělesa
Autor: David Kubečka
Katedra (ústav): Katedra algebry
Vedoucí bakalářské práce: Mgr. Pavel Příhoda, Ph.D.
e-mail vedoucího: Pavel.Prihoda@mff.cuni.cz

Abstrakt: Tématem této práce jsou cyklotomická tělesa a jejich aplikace. V úvodních kapitolách se zmíní některé obecné výsledky teorie číselných těles a ty se pak aplikují na speciální případ cyklotomických těles. První hlavní část práce je věnována základním vlastnostem cyklotomických těles. Je zde ukázáno, jak vypadá jejich celistvá báze a její diskriminant. Pomocí dosažených výsledků se dokážou speciální případy Kronecker-Weberovy věty a Dirichletovy věty o prvočíslech v aritmetických posloupnostech. Následuje relativně samostatná kapitola pojednávající o konstrukci pravidelných $n$-úhelníků pravítkem a kružítkem. Zbytek práce se zabývá Kummerovým přístupem k Velké Fermatově větě. V rozsahu nezbytně nutném jsou vyloženy Dedekindovy obory, které se využijí v poslední kapitole. V ní je podrobně dokázána Velká Fermatova věta pro regulární prvočísla.

Klíčová slova: cyklotomická tělesa, Dedekindovy obory, algebraická teorie čísel, Velká Fermatova věta pro regulární prvočísla

Title: Cyclotomic Fields
Author: David Kubečka
Department: Department of Algebra
Supervisor: Mgr. Pavel Příhoda, Ph.D.
Supervisor's e-mail address: Pavel.Prihoda@mff.cuni.cz

Abstract: The main theme of this thesis is the theory of cyclotomic fields and its applications. The general results of the theory of number fields are mentioned in the introductory chapters and then applicated to the special case of cyclotomic fields. In the first main part of the thesis basic properties of the cyclotomic fields are studied. This part describes their integral basis and shows how to calculate its discriminant. Due to these results it is possible to prove certain special cases of theorem of Kronecker and Weber and also of Dirichlet's theorem of primes in arithmetic progressions. Then follows relatively independent chapter which deals with the construction of regular $n$-gons using only ruler and compass. The rest of this thesis is devoted to the Kummer's approach to Fermat's Last Theorem. Dedekind domains are introduced and their basic properties are shown with respect to the purpose of the last chapter where a detailed proof of Fermat's last Theorem for regular primes is given.

Keywords: Cyclotomic Fields, Dedekind Domains, Algebraic Number Theory, Fermat's Last Theorem for Regular Primes

# Kapitola 1

# Motivace

Kolem roku 1637 vyslovil francouzský matematik Pierre de Fermat tvrzení, že rovnice

$$x^n + y^n = z^n, \qquad n \in \mathbb{N}, \quad x, y, z \in \mathbb{Z} \setminus \{0\} \tag{1.1}$$

nemá pro $n \geq 3$ řešení. Všechny generace matematiků se od té doby pokoušely dokázat toto tvrzení, známé u nás jako *Velká Fermatova věta*. Ačkoliv úspěchy v tomto směru byly většinou jen částečné, při pokusech o důkaz byly často vyvinuty mocné matematické nástroje, které potom našly uplatnění i v jiných, zdánlivě s Velkou Fermatovou větou nesouvisejících, oblastech matematiky. Takovým nástrojem jsou i cyklotomická tělesa, která stála dokonce u zrodu celé nové matematické disciplíny zvané algebraická teorie čísel. Než však přistoupíme k vybudování teorie cyklotomických těles a dokázání některých fundamentálních výsledků, vyřešíme jednu s naším problémem přímo související diofantickou rovnici. Nadále budeme nazývat rovnici (1.1) *Fermatovou rovnicí n-tého stupně*. Budou nás zajímat její netriviální řešení, tj. $xyz \neq 0$.

Řešení Fermatovy rovnice druhého stupně byla známa už ve starověku. Protože jakákoliv trojice $x, y, z$ kladných celých čísel splňující tuto rovnici udává podle Pythagorovy věty délky stran pravoúhlého trojúhelníka, nazývá se tato trojice i příslušná rovnice pythagorejskou. Pokud navíc kromě kladnosti předpokládáme i $\mathrm{NSD}(x, y, z) = 1$ a $x$ je sudé, nazývá se trojice $(x, y, z)$ *základní pythagorejskou trojicí*. Ukážeme, že k nalezení všech řešení pythagorejské rovnice stačí najít všechny základní pythagorejské trojice.

Předpoklad o kladnosti a nesoudělnosti $x, y, z$ je zřejmý. Kdyby $z$ bylo sudé, musely by $x$ i $y$ být liché (jinak by nebylo $\mathrm{NSD}(x, y, z) = 1$). Potom $x^2 + y^2 \equiv 2 \pmod 4$, ale $z^2 \equiv 0 \pmod 4$. Tedy $z$ je liché a $x$ a $y$ mají různou paritu. Díky symetrii $x$ a $y$ můžeme bez újmy na obecnosti požadovat sudost $x$.

Hledejme nyní všechny základní trojice. Nejprve přepíšeme pythagorejskou rovnici do ekvivalentního tvaru

$$x^2 = z^2 - y^2 = (z - y)(z + y).$$

Nyní můžeme vyjádřit

$$x = 2u, \quad z - y = 2v, \quad z + y = 2w,$$

a $u^2 = vw$, přičemž $v$ a $w$ mají různou paritu a $\mathrm{NSD}(v, w) = 1$ vzhledem k nesoudělnosti $y$ a $z$. Díky jednoznačnosti prvočíselného rozkladu je $v = a^2$, $w = b^2$ a $u = ab$. Navíc čísla $a$ a $b$ musí být nesoudělná, jinak by nebyla nesoudělná ani $v$ a $w$. Máme tedy

$$x = 2ab, \quad y = \frac{2w - 2v}{2} = b^2 - a^2, \quad z = \frac{2w + 2v}{2} = b^2 + a^2.$$

Dosazením ověříme, že čísla tohoto tvaru skutečně splňují řešenou rovnici. Dostáváme tedy

**Tvrzení 1.1.** *Trojice $(x, y, z)$ je základní pythagorejskou trojicí, právě když*

$$\begin{aligned} x &= 2ab, \\ y &= b^2 - a^2, \\ z &= b^2 + a^2 \end{aligned}$$

*pro nějaká $a, b \in \mathbb{Z}$ splňující: $b > a > 0$, $a, b$ mají různou paritu a $\mathrm{NSD}(a, b) = 1$.*

Nyní se pokusíme dokázat, že Fermatova rovnice stupně 4 nemá netriviální řešení. Toto je jediný případ, jenž dokázal už sám Fermat. Ačkoliv je důkaz elementární, poprvé se v něm objevuje metoda tzv. *nekonečného sestupu*, kterou v jisté podobě využijeme ve všech důkazech dalších speciálních případů Fermatovy věty. Proto ji formulujeme obecně. Předpokládejme, že $x_1, y_1, z_1$ je (netriviální) řešení nějaké diofantické rovnice. Pokud budeme umět najít takové řešení $x_2, y_2, z_2$ téže rovnice, že $0 < |z_2| < |z_1|$, dosáhneme sporu. Tento postup bychom totiž mohli opakovat do nekonečna, čímž bychom dostali nekonečnou ostře klesající posloupnost přirozených čísel. Nemožné.

**Tvrzení 1.2.** *Rovnice*

$$x^4 + y^4 = z^2 \tag{1.2}$$

*nemá netriviální celočíselné řešení. Speciálně nemá netriviální řešení ani Fermatova rovnice stupně* 4.

*Důkaz:* Nejprve dokážeme druhou část tvrzení za předpokladu platnosti první. Kdyby nějaká nenulová čísla $x, y, z$ splňovala rovnici (1.1) pro $n = 4$, pak by čísla $x, y, z^2$ splňovala rovnici (1.2) – spor.

Nechť nyní netriviální trojice $(x, y, z)$ vyhovuje rovnici (1.2). Budeme chtít najít netriviální trojici $(e, f, g)$ tak, aby vyhovovala téže rovnici a zároveň $|g| < |z|$. Protože trojice $(x^2, y^2, z)$ splňuje pythagorejskou rovnici, můžeme bez újmy na

obecnosti předpokládat, že je to základní pythagorejská trojice. Podle tvrzení 1.1 existují nesoudělná celá čísla $a, b$ tak, že

$$x^2 = 2ab,\ y^2 = b^2 - a^2,\ z = b^2 + a^2,$$

$b > a > 0$ a $a, b$ mají různou paritu. Potom však $y^2 + a^2 = b^2$ a vzhledem k nesoudělnosti $a, b, y$ a lichosti $y$ je $(a, y, b)$ znovu základní pythagorejskou trojicí. Opětovným použitím tvrzení 1.1 dostáváme nesoudělná celá čísla $c, d$ různé parity taková, že $c > d > 0$ a

$$a = 2cd,\ y = c^2 - d^2,\ b = c^2 + d^2.$$

Dosaďme nyní za $x$:

$$x^2 = 2ab = 4cd(c^2 + d^2).$$

Rádi bychom teď usoudili, že $c, d$ i $c^2 + d^2$ musí být druhé mocniny. To poplyne z jednoznačného rozkladu celých čísel na prvočísla, pokud dokážeme, že $c, d, c^2 + d^2$ jsou po dvou nesoudělná.

Díky nesoudělnosti $c, d$ stačí ověřit nesoudělnost $c$ a $c^2 + d^2$ (stejně pak pro $d, c^2 + d^2$). Kdyby ale nějaké prvočíslo $p$ dělilo jak $c$, tak $c^2 + d^2$, dělilo by $d^2$ a tedy i $d$ – spor.

Z výše zmíněné vlastnosti celých čísel tak usuzujeme, že pro nějaká kladná $e, f, g$ je

$$c = e^2,\ d = f^2,\ c^2 + d^2 = g^2.$$

Potom platí $e^4 + f^4 = g^2$, neboli trojice $(e, f, g)$ je netriviálním řešením rovnice (1.2). Porovnejme $z$ a $g$:

$$|z| = z = a^2 + b^2 = 4c^2d^2 + \left(c^2 + d^2\right)^2 > g^4 > g > 0.$$

Tímto jsme metodou nekonečného sestupu dovedli ke sporu existenci netriviálního řešení rovnice (1.2). ✠

Nyní učiníme snadné pozorování. Nechť $n \geq m \geq 3$ a nechť čísla $x, y, z$ splňují Fermatovu rovnici stupně $n$. Pokud $m$ dělí $n$, $n = md$, tak čísla $x^d, y^d, z^d$ splňují Fermatovu rovnici stupně $m$. Jinak řečeno – není-li rovnice stupně $m$ řešitelná, není řešitelná ani žádná rovnice stupně, který je násobkem $m$. Protože všechna celá čísla větší než 2 jsou buď násobkem 4 nebo nějakého lichého prvočísla, zbývá vzhledem k předchozímu tvrzení dokázat Velkou Fermatovu větu jen pro liché prvočíselné exponenty.

Vraťme se ještě na chvíli k důkazům dvou předchozích tvrzení. Protože jsme dosud nevybudovali žádnou pokročilejší teorii, zvolili jsme důkazy elementární, které může pochopit i středoškolák. Existují však i jiné přístupy, které, ač složitější a vyžadující hlubší matematické znalosti, jsou v jistém smyslu přirozenější. Ukazují totiž, jakým směrem se máme vydat, abychom mohli mít naději, že Velkou Fermatovu větu dokážeme naráz pro více než jeden exponent.

Prvním takovým ukazatelem je obor takzvaných *Gaussových celých čísel* $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$, kde $i = \sqrt{-1}$. Je to tedy jistá podmnožina komplexních čísel, která obsahuje kořen nad celými čísly ireducibilního polynomu $x^2 + 1$. Geometricky představují Gaussova celá čísla mřížové body v pravoúhlé mříži s buňkami o velikosti strany 1. Je dobře známo, že $\mathbb{Z}[i]$ tvoří Euklidův a tedy i Gaussův obor. Vlastnosti jednoznačných rozkladů na prvočísla se dá v důkazu předcházejících tvrzení využít podobně, jako jsme to učinili my.

Toto už je zárodek metody, kterou při dokazování Velké Fermatovy věty použil Ernst Eduard Kummer (1810–1890). S většími či menšími odbočkami budeme v této práci směřovat právě k jeho výsledku, který byl ve své době bezesporu největším pokrokem na důkazu věty od jejího vyslovení Fermatem.

# Kapitola 2

# Číselná tělesa

V této přípravné kapitole připomeneme některé klíčové pojmy potřebné v dalších kapitolách. U čtenáře předpokládáme základní orientaci v oblasti, a proto tvrzení uvádíme bez důkazů. Pro elementární definice i důkazy uvedených tvrzení odkazujeme na [1].

## 2.1 Základní pojmy

*Číselným tělesem* rozumíme podtěleso komplexních čísel, které je zároveň (algebraickým) rozšířením konečného stupně tělesa $\mathbb{Q}$ racionálních čísel. Protože každé algebraické rozšíření $\mathbb{Q}$ (obecně každé algebraické rozšíření perfektního tělesa) je separabilní, jsou číselná tělesa tvaru $K = \mathbb{Q}(t)$, kde $t \in \mathbb{C}$ je nějaký algebraický prvek nad $\mathbb{Q}$. Stupeň $n$ rozšíření $K|\mathbb{Q}$ (někdy mluvíme prostě o stupni $K$) je pak roven stupni minimálního polynomu $f \in \mathbb{Q}[X]$ prvku $t$. Za bázi $K|\mathbb{Q}$ můžeme zvolit $\{1, t, \ldots, t^{n-1}\}$. Všechny netriviální homomorfismy z $K$ do $\mathbb{C}$ jsou pak jednoznačně určeny obrazy prvků této báze. Protože obrazem jednotkového prvku je zase jednotkový prvek, vidíme, že každý takový homorfismus je již $\mathbb{Q}$–homomorfismem. Naopak každý $\mathbb{Q}$–homomorfismus je již určen obrazem prvku $t$. Tento obraz musí nutně být kořenem polynomu $f$. Obecně nazýváme algebraické prvky $x, x' \in \mathbb{C}$ *vzájemně konjugované*, pokud mají stejný minimální polynom nad $\mathbb{Q}$. Občas budeme krátce říkat, že $x'$ je konjugací $x$.

Připomeneme nyní základní fakta o Galoisových rozšířeních $\mathbb{Q}$ (tj. normálních a konečných). Nechť $G = \mathrm{Gal}(K|\mathbb{Q})$ je Galoisova grupa Galoisova rozšíření $K|\mathbb{Q}$, tj. grupa všech automorfismů tělesa $K$. $K$ *Abelovým* (resp. *cyklickým*) rozšířením, pokud je G Abelova, resp. cyklická. *Základní věta Galoisovy teorie* říká, že každá podgrupa $G'$ grupy $G$ je Galoisovou grupou (jednoznačně určeného) podtělesa $K' \leq K$, které sestává z pevných bodů všech automorfismů $\sigma \in G'$. Naopak každé podtěleso $K'$ je pevnými body grupy $G' = \mathrm{Gal}(K|K')$. Navíc normální podgrupy $G$ odpovídají podtělesům $K$, která jsou normálními rozšířeními $\mathbb{Q}$. V takovém případě platí $\mathrm{Gal}(K'|\mathbb{Q}) \cong G/G'$. Pokud je rozšíření $K|\mathbb{Q}$ Abelovo, je

tedy každé podtěleso $K$ normálním (Galoisovým) rozšířením $\mathbb{Q}$.

Nechť $K$ je stále Galoisovo rozšíření a $L$ je další (ne nutně Galoisovo, ale konečné) rozšíření $\mathbb{Q}$. Pak je $KL$ Galoisovým rozšířením $L$ a $K$ Galoisovým rozšířením $K \cap L$, přičemž symbolem $KL$ značíme nejmenší podtěleso $\mathbb{C}$ obsahující $K$ i $L$. Navíc platí $[KL : L] = [K : K \cap L]$ a $\mathrm{Gal}(KL|L) \cong \mathrm{Gal}(K|K \cap L)$.

Věnujme se teď pojmům stopa, norma a diskriminant. Protože tyto pojmy budou v dalším textu hrát podstatnou roli, budeme podrobněji komentovat odvození některých základních vztahů.

Nechť $K = \mathbb{Q}(t)$ je číselné těleso stupně $n$, chápané jako vektorový prostor nad $\mathbb{Q}$. Zvolme $x \in K$ a definujme lineární zobrazení $\theta_x \colon K \to K$ vztahem $\theta_x(z) = xz$ pro každé $z \in K$. Označme $M(\theta_x) = (a_{ij})_{i,j=1}^n$ jeho matici vzhledem k nějaké bázi $\{b_1, \ldots, b_n\}$ vektorového prostoru $K$, tj.

$$\theta_x(b_j) = \sum_{i=1}^{n} a_{ij} b_i, \quad j = 1, \ldots, n. \quad (a_{ij} \in \mathbb{Q})$$

Nyní definujeme *stopu* prvku $x$ jako $\mathrm{Tr}_K(x) = \mathrm{Tr}(M(\theta_x))$ a *normu* prvku $x$ jako $\mathrm{N}_K(x) = \det(M(\theta_x))$. Z lineární algebry víme, že stopa ani determinant matice lineárního zobrazení nezávisejí na volbě báze, takže právě zavedené pojmy jsou dobře definované. Pokud nebude hrozit nedorozumění, budeme stopu a normu prvku $x$ značit prostě $\mathrm{Tr}(x)$ a $\mathrm{N}(x)$.

Nechť $x$ má minimální polynom $g = X^r + a_{r-1}X^{r-1} + \cdots + a_0$, $s = n/r$ značí dimenzi $K$ nad $\mathbb{Q}(x)$, $\{x_1 = x, x_2, \ldots, x_r\}$ je množina všech kořenů $g$ a $\{\sigma_1, \ldots, \sigma_n\}$ je množina všech homomorfismů z $K$ do $\mathbb{C}$. Pak platí

$$\mathrm{Tr}(x) = -sa_{r-1} = s\sum_{i=1}^{r} x_i = \sum_{j=1}^{n} \sigma_j(x), \tag{2.1}$$

$$\mathrm{N}(x) = (-1)^n a_0^s = \prod_{i=1}^{r} {x_i}^s = \prod_{j=1}^{n} \sigma_j(x). \tag{2.2}$$

Z těchto vztahů dostáváme okamžitě pro $x, y \in K$ a $b \in \mathbb{Q}$

$$\begin{aligned} \mathrm{Tr}(x+y) &= \mathrm{Tr}(x) + \mathrm{Tr}(y), \\ \mathrm{Tr}(bx) &= b\,\mathrm{Tr}(x), \\ \mathrm{N}(xy) &= \mathrm{N}(x)\,\mathrm{N}(y), \end{aligned} \tag{2.3}$$

neboli stopa (resp. norma) je homomorfismem aditivní (resp. multiplikativní) grupy tělesa $K$. Navíc pro $x \in \mathbb{Q}$ máme $\mathrm{Tr}(x) = nx$ a $\mathrm{N}(x) = x^n$.

Dostáváme se teď k pojmu diskriminantu, který bude, jak uvidíme později, jedním z invariantů číselných těles.

Stále předpokládejme, že $K|\mathbb{Q}$ je rozšíření stupně $n$. Nechť $(x_1, \ldots, x_n)$ je nějaká $n$-tice prvků z $K$. Její *diskriminant* definujeme jako

$$\mathrm{discr}_K(x_1, \ldots, x_n) = \det(\mathrm{Tr}_K(x_i x_j))_{i,j=1}^n.$$

Označme jako $A$ matici, která má na místě $(i,j)$ prvek $\sigma_i(x_j)$, kde $\{\sigma_1,\ldots,\sigma_n\}$ je množina všech homomorfismů z $K$ do $\mathbb{C}$. Zřejmě platí $A\cdot A^T = (\mathrm{Tr}(x_ix_j))_{i,j}$ a z věty o násobení determinantů dostáváme

$$\mathrm{discr}_K(x_1,\ldots,x_n) = [\det(A)]^2. \tag{2.4}$$

Nechť nyní $\mathcal{B} = \{x_1,\ldots,x_n\}$ tvoří bázi vekotorového prostoru $K$ a vyjádřeme jednotlivé složky vektoru $(y_1,\ldots,y_n)\in K^n$ vzhledem k $\mathcal{B}$, tj. $y_j = \sum_{i=1}^n c_{ij}x_i,\ j = 1,\ldots,n$ ($c_{ij}\in\mathbb{Q}$). Pak platí

$$\mathrm{discr}(y_1,\ldots,y_n) = [\det(c_{ij})]^2\cdot\mathrm{discr}(x_1,\ldots,x_n). \tag{2.5}$$

Uvažme nyní speciální bázi $\{1,t,\ldots,t^{n-1}\}$ tělesa $K=\mathbb{Q}(t)$ a označme $t_1 = t, t_2,\ldots,t_n$ všechny prvky konjugované s $t$ (tedy všechny komplexní kořeny jeho minimálního polynomu). S využitím (2.4) a znalosti Vandermondova determinantu máme

$$\mathrm{discr}(1,t,\ldots,t^{n-1}) = \prod_{1\le i<j\le n}(t_i-t_j)^2 = (-1)^{\frac{n(n-1)}{2}}\prod_{i\neq j}(t_i-t_j). \tag{2.6}$$

Protože jsou $t_1 = t, t_2,\ldots,t_n$ po dvou různé ($K$ je separabilní rozšíření), je poslední diskriminant nenulový a díky (2.5) vidíme, že $\mathrm{discr}(y_1,\ldots,y_n)=0$, právě když jsou $y_1,\ldots,y_n$ lineárně závislé.

Na závěr této sekce zavedeme ještě jeden pojem, který se nám bude později hodit i v obecnějším kontextu. Ať $T$ je těleso charakteristiky 0 a ať $T\le\mathbb{C}$. *Diskriminant* monického polynomu $f\in T[X]$ s (ne nutně různými) kořeny $x_1,\ldots,x_n\in\mathbb{C}$ definujeme vztahem

$$\mathrm{discr}(f) = \prod_{1\le i<j\le n}(x_i-x_j)^2. \tag{2.7}$$

Alternativně jej můžeme spočítat ze vzorce

$$\mathrm{discr}(f) = (-1)^{\frac{n(n-1)}{2}}\prod_{j=1}^n f'(x_j), \tag{2.8}$$

kde $f'$ značí derivaci $f$. Souvislost diskriminantu polynomu s diskriminantem prvku (definice pro obecná rozšíření je stejná) je následující: Ať $K=T(y)$ je rozšíření stupně $r$ a $g\in T[X]$ je minimální polynom prvku $y$. Pak $\mathrm{discr}(g) = \mathrm{discr}(1,y,\ldots,y^{r-1})$, jak napovídá vztah (2.6).

## 2.2 Celistvé prvky číselných těles

Vztah mezi celistvými prvky a příslušnými tělesy odpovídá vztahu mezi celými a racionálními čísly, resp. je jeho zobecněním. V této sekci definujeme základní pojmy a uvedeme tvrzení v rozsahu nezbytně nutném pro budování teorie v dalších

kapitolách. U čtenáře předpokládáme zběžnou znalost látky, a tak budeme tvrzení uvádět většinou bez důkazů.

Začneme pojmem celistvého prvku. Ten se dá definovat obecně pro okruhy takto. Ať $S$ je okruh (komutativní s jednotkovým prvkem) a $R$ jeho podokruh. Prvek $x \in S$ nazveme *celistvým* nad $R$, pokud existuje nenulový monický polynom z $R[X]$, jehož je $x$ kořenem. O $S$ pak řekneme, že je *celistvý* nad $R$, pokud je každý prvek z $S$ celistvým nad $R$. Pokud každý prvek z $S$, celistvý nad $R$, již patří do $R$, nazveme $R$ *celistvě uzavřeným* v $S$. Pokud je $R$ obor integrity, řekneme o něm, že je *celistvě uzavřený*, pokud je celistvě uzavřený ve svém podílovém tělese ve smyslu předchozí definice.

**Lemma 2.1.** *Ať $R'$ značí množinu všech prvků z $S$, které jsou celistvé nad $R$. Pak $R'$ tvoří podokruh $S$ a $R'$ je celistvé nad $R$ a celistvě uzavřené v $S$.*

Okruh $R'$ z předchozího lemmatu nazveme *celistvým uzávěrem* $R$ v $S$. Dříve než přejdeme z obecné řeči okruhů do konkrétního případu číselných těles, učiníme ještě dvě pozorování, která se nám budou dříve či později hodit.

**Lemma 2.2.** *Ať $S$ je obor integrity, $I$ jeho nenulový ideál a $R$ podobor $S$.*

(1) *Pokud je $R$ Gaussův, pak je už celistvě uzavřený.*

(2) *Pokud je $S$ celistvý nad $R$, tak $R \cap I \neq \{0\}$.*

Nás bude teď zajímat situace, kdy $R = \mathbb{Z}$. Podle předchozího lemmatu je tedy obor $\mathbb{Z}$ celistvě uzavřený ve svém podílovém tělese $\mathbb{Q}$. Celistvým prvkům nad $\mathbb{Z}$ budeme říkat *algebraická celá čísla*.

Nechť $K$ je nějaké číselné těleso a označme jako $\mathbb{Z}_K$ množinu včech algebraických celých čísel z $K$. Podle lemmatu 2.1 je tedy $\mathbb{Z}_K$ celistvým uzávěrem $\mathbb{Z}$ v $K$. Výše naznačená analogie vztahu $\mathbb{Z}$ ke $\mathbb{Q}$ a $\mathbb{Z}_K$ ke $K$ je obsahem následujícího

**Tvrzení 2.3.** *Každý prvek z $K$ se dá napsat ve tvaru $b/d$, kde $b \in \mathbb{Z}_K$ a $d \in \mathbb{Z} \subseteq \mathbb{Z}_K$, $d \neq 0$. Speciálně $K$ je isomorfní podílovému tělesu oboru $\mathbb{Z}_K$.*

Přímo z definice $\mathbb{Z}_K$ plyne, že $\mathbb{Z}_K \cap \mathbb{Q} = \mathbb{Z}$. Uveďme teď další důležité vlastnosti algebraických celých čísel.

**Tvrzení 2.4.** *Nechť $x \in \mathbb{Z}_K$ má minimální polynom $f \in \mathbb{Q}[X]$. Potom včechny koeficienty $f$ leží v $\mathbb{Z}$ (neboli $f \in \mathbb{Z}[X]$). Zároveň všechny prvky konjugované s $x$ (tj. všechny kořeny $f$) jsou celistvé nad $\mathbb{Z}$.*

Ze vztahů (2.1), (2.2) z předchozí sekce vidíme, že norma i stopa prvku se dají odvodit z koeficientů jeho minimálního polynomu. Pokud tedy $x \in \mathbb{Z}_K$, máme podle předchozího tvrzení i $\mathrm{Tr}_K(x), \mathrm{N}_K(x) \in \mathbb{Z}$.

Při zkoumání vztahů dělitelnosti v okruzích „ignorujeme“ invertibilní prvky. V celých číslech jsou takové prvky jenom dva, jmenovitě $\pm 1$. Následující tvrzení podává základní charakterizaci invertibilních prvků v okruzích algebraických celých čísel.

**Tvrzení 2.5.** *Ať $K$ je číselné těleso a $x \in \mathbb{Z}_K$. Pak $x$ je invertibilní $\Leftrightarrow \mathrm{N}_K(x) = \pm 1$.*

Díky znalosti podoby invertibilních prvků a díky multiplikavitě normy je možné dokázat

**Tvrzení 2.6.** *Nechť $x \in \mathbb{Z}_K$, $x \neq 0$ a $x$ není invertibilní. Pak $x$ se dá napsat jako součin ireducibilních prvků ze $\mathbb{Z}_K$ (tj. prvků bez vlastního dělitele).*

Nyní se dostáváme ke klíčovému tvrzení této sekce.

**Tvrzení 2.7.** *Ať $K$ je číselné těleso stupně $n$ nad $\mathbb{Q}$. Pak okruh algebraických celých čísel $\mathbb{Z}_K$ je volnou Abelovou grupou hodnosti $n$. To znamená, že existují prvky $b_1, \ldots, b_n \in \mathbb{Z}_K$ takové, že každý prvek ze $\mathbb{Z}_K$ lze jednoznačně zapsat ve tvaru $b_1 z_1 + \cdots + b_n z_n$, kde $z_i \in \mathbb{Z}$.*

Ačkoliv toto tvrzení nevypadá složitě, jeho dosti dlouhý důkaz vyžaduje celkem úpornou práci s moduly. My jej nicméně v další kapitole dokážeme pro speciální třídu číselných těles.

Tvrzení 2.7 nás opravňuje definovat jeden důležitý pojem: Každou bázi volné Abelovy grupy $\mathbb{Z}_K$ nazýváme *celistvou bází* číselného tělesa $K$. Protože celistvá báze má $n = [K : \mathbb{Q}]$ prvků, je zároveň i bází $K$ chápaného jako vektorový prostor nad $\mathbb{Q}$. V následujícím tvrzení objasníme výše naznačenou roli diskrimantu jako základního invariantu číselných těles.

**Tvrzení 2.8.** *Nechť $\{b_1, \ldots, b_n\}$ je celistvá báze číselného tělesa $K$ stupně $n$ a $b'_1, \ldots, b'_n \in \mathbb{Z}_K$. Potom*

$$\mathrm{discr}_K(b_1, \ldots, b_n) = \mathrm{discr}_K(b'_1, \ldots, b'_n),$$

*právě když $\{b'_1, \ldots, b'_n\}$ je celistvou bází $K$.*

*Důkaz:* Protože $\{b_1, \ldots, b_n\}$ je celistvá báze, můžeme pro $j = 1, \ldots, n$ psát $b'_j = \sum_{i=1}^{n} z_{ij} b_i$, kde $z_{ij} \in \mathbb{Z}$. Podle vztahu (2.5) z předchozí sekce tak máme

$$\mathrm{discr}_K(b'_1, \ldots, b'_n) = [\det(z_{ij})]^2 \cdot \mathrm{discr}_K(b_1, \ldots, b_n).$$

Protože je matice $(z_{ij})_{i,j}$ celočíselná, je invertibilní, právě když je její determinant roven $\pm 1$. Ovšem invertibilita této matice znamená právě to, že $\{b'_1, \ldots, b'_n\}$ je celistvá báze. ✠

Ačkoliv celistvá báze číselného tělesa není určena jednoznačně, je jednoznačně určen její diskriminant. Proto má smysl zavádět pojem *diskriminant číselného tělesa* jako diskriminant jeho libovolné celistvé báze. Budeme jej značit $\delta_K$.

# Kapitola 3

# Cyklotomická tělesa

## 3.1 Odmocniny z jedné a cyklotomické polynomy

V této kapitole vybudujeme základy teorie cyklotomických těles. Dokážeme pro ně některá tvrzení, která platí obecně pro číselná tělesa. Začneme pojmem odmocnina z jedné.

Prvek $\zeta \in \mathbb{C}$ nazveme *$n$-tou odmocninou z jedné*, pokud splňuje $\zeta^n = 1$. Víme, že potom je $\zeta$ tvaru $e^{2k\pi i/n}$ pro nějaké $k = 1, \ldots, n$ a tedy $|\zeta| = 1$. Snadno se ověří, že všechny $n$-té odmocniny z jedné tvoří multiplikativní cyklickou grupu. Generátory této grupy (prvky řádu $n$) nazýváme *primitivní $n$-té odmocniny z jedné*. Pokud $\zeta_n$ je generátor, tak všechny ostatní generátory jsou tvaru $\zeta_n^k$, $\mathrm{NSD}(k, n) = (k, n) = 1$. Máme tedy $\varphi(n)$ primitivních $n$-tých odmocnin z jedné ($\varphi$ značí, jak je obvyklé, Eulerovu funkci).

Nechť $\zeta_n$ je primitivní $n$-tá odmocnina z jedné. Polynom

$$\Phi_n(X) = \prod_{\substack{1 \le k < n \\ (k,n)=1}} (X - \zeta_n^k)$$

nazýváme *$n$-tým cyklotomickým polynomem*. Kořeny tohoto polynomu jsou právě všechny primitivní $n$-té odmocniny z jedné. Podle předchozího je tedy $\Phi_n$ stupně $\varphi(n)$.

**Lemma 3.1.** $X^n - 1 = \prod_{d|n} \Phi_d(X)$.

*Důkaz:* Stupeň polynomu na pravé straně je roven $\sum_{d|n} \varphi(d) = n$. Protože $X^n - 1$ nemá násobné kořeny, stačí dokázat, že kořeny obou polynomů se shodují. Kořeny každého polynomu $\Phi_d$ jsou právě všechny primitivní $d$-té odmocniny z jedné. Kořeny $X^n - 1$ jsou všechny $n$-té odmocniny z jedné. Každá $n$-tá odmocnina z jedné je však primitivní $d$-tou odmocninou z jedné pro nějaké $d$, $d|n$, a naopak. ✠

Podívejme se na několik prvních cyklotomických polynomů:

$$\Phi_1(X) = X - 1, \quad \Phi_2(X) = X + 1, \quad \Phi_3(X) = X^2 + X + 1$$
$$\Phi_4(X) = X^2 + 1, \quad \Phi_5(X) = X^4 + X^3 + X^2 + X + 1.$$

Jejich tvar je motivací k následujícímu lemmatu, které by bylo sice možno časem dokázat aplikací výsledků z předchozí kapitoly, ale my jej nyní dokážeme přímo.

**Tvrzení 3.2.** $\Phi_n(X) \in \mathbb{Z}[X]$.

*Důkaz:* Indukcí podle $n$. Případ $n = 1$ je jasný. Předpokládejme, že tvrzení platí pro všechna $m < n$. Podle předchozího lemmatu je

$$X^n - 1 = \Phi_n(X) \prod_{\substack{d|n \\ d<n}} \Phi_d(X).$$

Z indukčního předpokladu víme, že produkt v předchozí rovnosti je celočíselným polynomem. Navíc je monický, takže jím můžeme vydělit polynom na levé straně a výsledný podíl, který je roven $\Phi_n$, zůstane polynomem v $\mathbb{Z}[X]$. ✠

K důkazu následujícího tvrzení budeme potřebovat tzv. Gaussovo lemma, které říká, že primitivní (speciálně monický) polynom ze $\mathbb{Z}[X]$ je ireducibilní nad $\mathbb{Z}$, právě když je ireducibilní nad $\mathbb{Q}$.

**Tvrzení 3.3.** *Polynom $\Phi_n$ je ireducibilní nad $\mathbb{Q}$.*

*Důkaz:* Podle Gaussova lemmatu stačí dokázat ireducibilitu v $\mathbb{Z}[X]$. Nechť tedy $\Phi_n(X) = f(X)g(X)$, kde $f(X), g(X) \in \mathbb{Z}[X]$, přičemž $f(X)$ je minimální polynom prvku $\zeta_n$. Zvolme prvočíslo $p$ nesoudělé s $n$. Pak $\zeta_n^p$ je opět primitivní $n$-tá odmocnina z jedné a tedy $\Phi_n(\zeta_n^p) = 0$. Nechť $f(\zeta_n^p) \neq 0$, tedy $g(\zeta_n^p) = 0$. Protože $g(x^p) \equiv g(x)^p \pmod{p}$, mají $f(X)$ i $g(X)$, chápané jako polynomy v $\mathbb{F}_p[X]$, společný kořen v $\overline{\mathbb{F}_p}$ (algebraický uzávěr $\mathbb{F}_p$). Protože $\Phi_n(X) | X^n - 1$, má $X^n - 1 \in \mathbb{F}_p[X]$ vícenásobný kořen v $\overline{\mathbb{F}_p}$, což není možné, jelikož $(X^n - 1)' = nX^{n-1}$ a $\mathrm{NSD}(p, n) = 1$.

Je tedy $f(\zeta_n^p) = 0$ pro každé prvočíslo nesoudělné s $n$ a tím pádem i pro každé $k$ nesoudělné s $n$, $1 \leq k < n$. Protože $\zeta_n^k \neq \zeta_n^j$ pro $k \not\equiv j \pmod{n}$, je $\deg(f) \geq \varphi(n) = \deg(\Phi_n)$. Polynomy $\Phi_n$ a $f$ se tedy rovnají a vzhledem k ireducibilitě $f$ je ireducibilní i $\Phi_n$. ✠

Zkoumejme nyní blíže koeficienty cyklotomických polynomů.

**Tvrzení 3.4.** *Pro každé $n \geq 2$ je polynom $\Phi_n$ reciproký, tj. pokud $\Phi_n(X) = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_0$, platí $a_i = a_{n-i}$ pro všechna $i = 0, \ldots, n$. Speciálně konstatní člen je roven 1.*

*Důkaz:* Pro $n = 2$ tvrzení jistě platí, protože $\Phi_2(X) = X + 1$. Nechť tedy $n > 2$.

Reciprokost $\Phi_n$ se dá ještě jinak vyjádřit vztahem $\Phi_n(X) = X^{\varphi(n)}\Phi_n(X^{-1})$. Podle definice je

$$\Phi_n(X) = \prod_{\substack{1\le k<n\\(k,n)=1}} (X - \zeta_n^k) \qquad \text{a}$$

$$X^{\varphi(n)}\Phi_n(X^{-1}) = X^{\varphi(n)} \prod_{\substack{1\le k<n\\(k,n)=1}} (X^{-1} - \zeta_n^k) = \prod_{\substack{1\le k<n\\(k,n)=1}} (1 - X\zeta_n^{-k}),$$

kde $\zeta_n$ je nějaká primitivní $n$-tá odmocnina z jedné a v poslední rovnosti jsme využili toho, že primitivní $n$-té odmocniny jsou uzavřené na operaci inverzního prvku.

Vynásobme nyní poslední výraz prvkem $\prod_{\substack{1\le k<n\\(k,n)=1}} \zeta_n^k = \zeta_n^s$, kde $s = \sum_{\substack{1\le k<n\\(k,n)=1}} k$. Protože platí $(k, n) = 1 \Leftrightarrow (n - k, n) = 1$ a pro $n$ sudé není $(n, n/2) = 1$, je

$$s = \sum_{\substack{1\le k<n/2\\(k,n)=1}} (k + (n - k)) \equiv 0 \pmod{n},$$

a proto $\zeta_n^s = 1$. Dostáváme tedy

$$\prod_{\substack{1\le k<n\\(k,n)=1}} (1 - X\zeta_n^{-k}) = \zeta_n^s \prod_{\substack{1\le k<n\\(k,n)=1}} (1 - X\zeta_n^{-k}) = \prod_{\substack{1\le k<n\\(k,n)=1}} (\zeta_n^k - X) = \prod_{\substack{1\le k<n\\(k,n)=1}} (X - \zeta_n^k),$$

protože mezi sebou násobíme $\varphi(n)$ členů a to je pro $n > 2$ sudé číslo.

Speciální případ platí, protože $\Phi_n$ má vedoucí koeficient roven 1. ✠

Ukážeme si teď první aplikaci cyklotomických polynomů. Dokážeme jeden důležitý speciální případ slavné Dirichletovy věty, která říká, že pokud $\mathrm{NSD}(a, n) = 1$, pak v aritmetické posloupnosti $a, a + n, a + 2n, \ldots$ existuje nekonečně mnoho prvočísel.

**Tvrzení 3.5.** *Pro každé $n \in \mathbb{N}$ existuje nekonečně mnoho prvočísel $p$, takových že $p \equiv 1 \pmod{n}$.*

*Důkaz:* Přebíráme z [5, Theorem 4.16]. Tvrzení pro $n \le 2$ neříká nic jiného, než že existuje nekonečně mnoho prvočísel, což již před naším letopočtem dokázal Eukleidés. Předpokládejme tedy, že $n > 2$.

Budeme dokazovat, že pro každé takové $n$ existuje aspoň jedno prvočíslo kongruentní s 1 modulo $n$. Kdyby potom pro nějaké $n_0$ pouze konečně mnoho prvočísel, řekněme $p_1, \ldots, p_t$, bylo kongruentních s 1 modulo $n_0$, jistě by existovalo prvočíslo $p$ takové, že

$$p \equiv 1 \pmod{n_0 p_1 \ldots p_t}.$$

Přitom by bylo $p \equiv 1 \pmod{n_0}$ a zřejmě $p \neq p_i$, $i = 1, \ldots, t$, což je spor.

Nejprve dokážeme, že pro všechna $n > 2$ je $|\Phi_n(n)| > 1$ a tedy $\Phi_n(n)$ je dělitelné aspoň jedním prvočíslem. Protože ale platí pro $k \in \mathbb{N}$ nerovnosti $|n - \zeta_n^k| \geq |n| - |\zeta_n^k| = n - 1 > 1$, je

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

K dokončení důkazu nyní bude stačit, když ukážeme, že pro $n > 2$ je každý prvočíselný dělitel $\Phi_n(n)$ kongruentní s 1 modulo $n$. Zvolme tedy $p$ prvočíselného dělitele $\Phi_n(n)$. Z úvah výše víme, že takové $p$ existuje. Protože $\Phi_n(X)|X^n - 1$ je i $\Phi_n(n)|n^n - 1$ a tedy $p|n^n - 1$, neboli podle Lagrangeovy věty řád $t$ prvku $n$ v grupě $\mathbb{Z}_p^*$ dělí $n$. Pokud dokážeme, že $t = n$, bude podle téže věty $n|p - 1$ a tedy $p \equiv 1 \pmod{n}$.

Pro spor předpokládejme, že $t < n$. Potom $\Phi_n(X)$ podle lemmatu 3.1 nedělí $X^t - 1$, a proto je polynom $(X^n - 1)/(X^t - 1)$ dělitelný $\Phi_n(X)$. Dosazením $n$ za $X$ dostáváme $p|(n^n - 1)/(n^t - 1)$. Na druhou stranu spočítáme, že

$$\frac{n^n - 1}{n^t - 1} = \frac{(n^t)^{\frac{n}{t}} - 1}{n^t - 1} = (n^t)^{\frac{n}{t}-1} + (n^t)^{\frac{n}{t}-2} + \cdots + n^t + 1.$$

Díky $n^t \equiv 1 \pmod{p}$ dostáváme

$$\frac{n^n - 1}{n^t - 1} \equiv \underbrace{1 + \cdots + 1}_{\frac{n}{t} \text{ jedniček}} = \frac{n}{t} \pmod{p}.$$

Protože $p$ dělí levou stranu poslední kongruence, musí dělit i pravou a tedy $p|n$. Z $p|n^n - 1$ ale dostáváme $p \nmid n$, což je spor. Platí tedy $t = n$ a $p \equiv 1 \pmod{n}$, jak se mělo dokázat. ✠

## 3.2 Základní vlastnosti cyklotomických těles

Nechť $\zeta_n = e^{2\pi i/n}$. Těleso $\mathbb{Q}(\zeta_n)$ nazveme *$n$-tým cyklotomickým tělesem*. Pokud bude $n$ z kontextu zřejmé, budeme občas prostě psát $\zeta$ a $\mathbb{Q}(\zeta)$.

Z předchozí sekce víme, že minimálním polynomem prvku $\zeta = \zeta_n$ je polynom $\Phi_n \in \mathbb{Z}[X]$, a tedy stupeň rozšíření $[\mathbb{Q}(\zeta) : \mathbb{Q}]$ je roven $\varphi(n)$. Bází $\mathbb{Q}(\zeta)$ nad $\mathbb{Q}$ je pak například

$$\{1, \zeta, \zeta^2, \ldots, \zeta^{\varphi(n)-1}\}.$$

Protože všechny kořeny $\Phi_n$ jsou tvaru $\zeta^k$, kde $\mathrm{NSD}(k, n) = 1$, a tedy leží v $\mathbb{Q}(\zeta)$, je $\mathbb{Q}(\zeta)$ rozkladovým rozšířením polynomu $\Phi_n$. Zároveň jsou všechny kořeny tohoto polynomu jednoduché, a tak je $\mathbb{Q}(\zeta)$ i normálním (Galoisovým) rozšířením tělesa $\mathbb{Q}$. Podívejme se na jeho Galoisovu grupu.

**Tvrzení 3.6.** *Galoisova grupa* $\mathrm{Gal}(\mathbb{Q}(\zeta)|\mathbb{Q})$ *je isomorfní multiplikativní grupě* $\mathbb{Z}_n^*$. *Speciálně je* $\mathrm{Gal}(\mathbb{Q}(\zeta)|\mathbb{Q})$ *Abelovou grupou.*

*Důkaz:* Hledaným isomorfismem bude zobrazení $\psi$, které prvku $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta)|\mathbb{Q})$, $\sigma(\zeta) = \zeta^k$, přiřadí prvek $k \in \mathbb{Z}_n^*$. Vzhledem k úvahám prováděným výše je $\psi$ dobře definované a prosté. Protože se jedná o zobrazení mezi dvěma konečnými množinami stejné velikosti $\varphi(n)$, je i na. Zbývá rutinně ověřit, že to je homomorfismus.

Nechť $\sigma_1, \sigma_2 \in \mathrm{Gal}(\mathbb{Q}(\zeta)|\mathbb{Q})$. Můžeme psát $\sigma_i(\zeta) = \zeta^{\psi(\sigma_i)}$, $i = 1, 2$. Potom

$$\zeta^{\psi(\sigma_1\sigma_2)} = \sigma_1\sigma_2(\zeta) = \sigma_1(\sigma_2(\zeta)) = \sigma_1\left(\zeta^{\psi(\sigma_2)}\right).$$

Protože je $\sigma_1$ homomorfismus, máme

$$\sigma_1\left(\zeta^{\psi(\sigma_2)}\right) = (\sigma_1(\zeta))^{\psi(\sigma_2)} = \left(\zeta^{\psi(\sigma_1)}\right)^{\psi(\sigma_2)} = \zeta^{\psi(\sigma_1)\psi(\sigma_2)},$$

a tedy $\psi(\sigma_1\sigma_2) = \psi(\sigma_1)\psi(\sigma_2)$. ✠

Pro následující sérii tvrzení budeme potřebovat některé základní vlastnosti Eulerovy funkce. Shrneme je do lemmatu, které nebudeme dokazovat.

**Lemma 3.7.** *Nechť* $m, n$ *jsou přirozená čísla a* $d = \mathrm{NSD}(m, n)$, $f = \mathrm{nsn}(m, n)$. *Potom platí:*

(1) $\varphi(n)\varphi(m) = \varphi(d)\varphi(f)$.

(2) *Ať* $m|n$. *Pak* $\varphi(n) = \varphi(m)$, *právě když* $m = n$ *nebo* $m$ *je liché a* $n = 2m$.

**Tvrzení 3.8.** *Nechť* $m, n, d$ *a* $f$ *jsou jako v předchozím lemmatu. Potom je* $\mathbb{Q}(\zeta_n)\mathbb{Q}(\zeta_m) = \mathbb{Q}(\zeta_f)$ *a* $\mathbb{Q}(\zeta_n) \cap \mathbb{Q}(\zeta_m) = \mathbb{Q}(\zeta_d)$.

*Důkaz:* Pro přehlednost budeme místo $\mathbb{Q}(\zeta_n)$ psát krátce $\mathbb{Q}_n$.

Protože největší společný dělitel $m$ a $n$ je roven $mn/f$, existují celá čísla $a, b$ taková, že $am + bn = mn/f$, neboli $a/n + b/m = 1/f$. Dostáváme tak vztah

$$\zeta_n^a\zeta_m^b = \left(e^{2\pi i/n}\right)^a \left(e^{2\pi i/m}\right)^b = e^{2\pi i/f} = \zeta_f,$$

a proto $\mathbb{Q}_f \subseteq \mathbb{Q}_n\mathbb{Q}_m$. Na druhou stranu máme $n|f$ i $m|f$, takže zřejmě $\mathbb{Q}_n \subseteq \mathbb{Q}_f$ i $\mathbb{Q}_m \subseteq \mathbb{Q}_f$ a z definice součinu těles je i $\mathbb{Q}_n\mathbb{Q}_m \subseteq \mathbb{Q}_f$. Celkem jsme tedy dokázali $\mathbb{Q}_n\mathbb{Q}_m = \mathbb{Q}_f$.

Dokažme teď druhou rovnost. Základní tvrzení o vztahu součinu a průniku dvou těles nám spolu s položkou (1) předchozího lemmatu říká, že

$$[\mathbb{Q}_n : (\mathbb{Q}_n \cap \mathbb{Q}_m)] = [\mathbb{Q}_n\mathbb{Q}_m : \mathbb{Q}_m] = [\mathbb{Q}_f : \mathbb{Q}_m] = \varphi(f)/\varphi(m) = \varphi(n)/\varphi(d).$$

Z této rovnosti a vztahu $[\mathbb{Q}_n : \mathbb{Q}] = [\mathbb{Q}_n : (\mathbb{Q}_n \cap \mathbb{Q}_m)]\,[(\mathbb{Q}_n \cap \mathbb{Q}_m) : \mathbb{Q}]$ dostáváme ihned $[(\mathbb{Q}_n \cap \mathbb{Q}_m) : \mathbb{Q}] = \varphi(d) = [\mathbb{Q}_d : \mathbb{Q}]$. K dokončení důkazu si nyní stačí uvědomit, že díky $d|n, m$ zřejmě platí $\mathbb{Q}_d \subseteq \mathbb{Q}_n, \mathbb{Q}_m$ a tedy i $\mathbb{Q}_d \subseteq \mathbb{Q}_n \cap \mathbb{Q}_m$. ✠

**Tvrzení 3.9.** *Nechť $m \leq n$. Pak $\mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_m)$, právě když $m = n$ nebo $m$ je liché a $n = 2m$.*

*Důkaz:* ($\Leftarrow$) Pokud $m$ je liché a $n = 2m$, tak podle lemmatu 3.7(2) je $\varphi(n) = \varphi(m)$. Tedy $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = [\mathbb{Q}(\zeta_m) : \mathbb{Q}]$. Protože $m|n$, máme $\mathbb{Q}(\zeta_m) \subseteq \mathbb{Q}(\zeta_n)$. Tím je první část tvrzení dokázána.

($\Rightarrow$) Víme, že $\varphi(n) = \varphi(m)$, ale z toho bohužel tvrzení neplyne. Protipříkladem je např. $\varphi(3) = \varphi(4) = 2$.

Označme tedy $d = \mathrm{NSD}(m, n)$, $f = \mathrm{nsn}(m, n)$. Podle předchozího tvrzení máme $\mathbb{Q}(\zeta_d) = \mathbb{Q}(\zeta_f) = \mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_m)$. Dedukujeme, že $\varphi(d) = \varphi(f)$, ale navíc teď máme i $d|f$, takže můžeme použít lemma 3.7(2). Pokud platí $m < n$, je $d$ vlastním dělitelem $f$, a tedy $f = 2d$ a $d$ je navíc liché. Počítejme:

$$2d = f = \frac{mn}{d} \quad \Longrightarrow \quad 2 = \frac{m}{d} \cdot \frac{n}{d}.$$

Protože pracujeme s přirozenými čísly a $m < n$, musí být $m = d$. Tedy $m$ je liché a $n = 2m$, jak se mělo dokázat. ✠

**Tvrzení 3.10.** *$\mathbb{Q}(\zeta_m) \subseteq \mathbb{Q}(\zeta_n) \Leftrightarrow m|n$ nebo $m = 2u$ pro nějaké liché $u$ takové, že $u|n$.*

*Důkaz:* ($\Leftarrow$) Případ $m|n$ je jasný. Pokud $m = 2u$, plyne z předchozího tvrzení $\mathbb{Q}(\zeta_m) = \mathbb{Q}(\zeta_u) \subseteq \mathbb{Q}(\zeta_n)$.

($\Rightarrow$) Z předpokládané inkluze plyne $\mathbb{Q}(\zeta_m) = \mathbb{Q}(\zeta_n) \cap \mathbb{Q}(\zeta_m) = \mathbb{Q}(\zeta_d)$, kde $d$ je jako vždy největší společný dělitel $m$ a $n$. Opět z předchozího tvrzení tedy máme buď $d = m$, a tedy $m|n$, nebo $m = 2d$ a $d$ je liché. ✠

## 3.3 Kronecker-Weberova věta

Opět dokážeme speciální případ jedné věty, týkající se tentokrát už přímo cyklotomických těles. Nejprve si všimneme některých důsledků tvrzení 3.6 a základní věty Galoisovy teorie.

Nechť $\mathbb{Q}(\zeta_n)$ je cyklotomické těleso. Potom je grupa $\mathrm{Gal}(\mathbb{Q}(\zeta_n)|\mathbb{Q})$ komutativní a každá její podgrupa je normální. Každé podgrupě $H$ tedy odpovídá podtěleso $K \leq \mathbb{Q}(\zeta_n)$, které je normálním rozšířením $\mathbb{Q}$. Protože je tato korespondence jednoznačná, dokázali jsme tímto opačnou implikaci následující věty.

**Věta 3.11** (Kronecker,Weber)**.** *Ať $K$ je konečné rozšíření $\mathbb{Q}$. Pak $K$ je Abelovo (tj. normální s komutativní Galoisovou grupou), právě když $K \subseteq \mathbb{Q}(\zeta_n)$ pro nějaké $n \in \mathbb{N}$.*

Přímou implikaci dokážeme pro *kvadratická rozšíření* racionálních čísel, tj. pro rozšíření stupně 2, která jsou jistě Abelova. K tomu budeme potřebovat následující dvě lemmata, z nichž první vyslovíme obecně, protože jej využijeme i později.

**Lemma 3.12.** *Ať $K$ je kvadratické rozšíření tělesa $T$ charakteristiky 0. Pak existuje $d \in T$ takové, že $K = T(\sqrt{d})$. Pokud navíc $T = \mathbb{Q}$, můžeme volit $d$ jako* bezčtvercové *celé číslo (tj. $p^2 \nmid d$ pro žádné prvočíslo $p$).*

*Důkaz:* Protože $K$ je rozšíření konečného stupně, existuje $x \in K$ takové, že $K = T(x)$. Nechť minimální polynom prvku $x$ je $f(X) = X^2 + bX + c \in T[X]$. Snadno se ověří, že jeho druhým kořenem je $-b-x$. Spočítejme nyní diskriminant $f$ podle vztahu (2.7):

$$d_1 = \operatorname{discr}(f) = (x - (-b - x))^2 = (b + 2x)^2 = b^2 + 4(bx + x^2) = b^2 - 4c.$$

Protože $K$ je rozšíření stupně 2, neleží $\sqrt{d_1}$ v $T$ ($\operatorname{discr}(f)$ nápadně připomíná vzorec známý ze střední školy). Máme tedy $K = T(\sqrt{d_1})$. V případě $T = \mathbb{Q}$ leží podle tvrzení 2.4 koeficienty minimálního polynomu v $\mathbb{Z}$, takže i $d_1 \in \mathbb{Z}$. Pokud $d$ vznikne odstraněním sudých mocnin všech prvočísel, vyskytujících se v rozkladu $d_1$, bude $d$ bezčtvercové a jistě $K = \mathbb{Q}(\sqrt{d})$. ✠

**Lemma 3.13.** *Nechť $g(X) = X^n - 1$. Potom $\operatorname{discr}(g) = n^n(-1)^{\frac{(n-1)(3n-2)}{2}}$ a $\sqrt{\operatorname{discr}(g)} \in \mathbb{Q}(\zeta_n)$.*

*Důkaz:* K výpočtu diskriminantu tentokrát využijeme vzorec (2.8). Derivace $g(X)$ je $nX^{n-1}$. Označme ještě pro jednoduchost kořeny $g$ jako $x_1, \ldots, x_n$. Zřejmě $(-1)^n \prod_{j=1}^n x_j = \prod_{j=1}^n (-x_j) = -1$.

$$\begin{aligned}\operatorname{discr}(g) &= (-1)^{\frac{n(n-1)}{2}} \prod_{j=1}^{n} \left(n x_j^{n-1}\right) = (-1)^{\frac{n(n-1)}{2}} n^n \left(\prod_{j=1}^{n} x_j\right)^{n-1} \\ &= (-1)^{\frac{n(n-1)}{2}} n^n (-1)^{(n-1)^2} = n^n (-1)^{\frac{(n-1)(3n-2)}{2}}.\end{aligned}$$

Dokažme teď část o odmocnině. Protože kořeny $g$ jsou právě všechny $n$-té odmocniny z jedné, leží všechny v $\mathbb{Q}(\zeta_n)$. Pak jistě leží v $\mathbb{Q}(\zeta_n)$ i prvek

$$w = \prod_{1 \le i < j \le n} (\zeta_n^i - \zeta_n^j).$$

Z definice diskriminantu je přesně $w = \sqrt{\operatorname{discr}(g)}$. ✠

Nyní již můžeme dokázat, že každé kvadratické rozšíření $K$ tělesa $\mathbb{Q}$ leží v nějakém cyklotomickém tělese. Podle lemmatu 3.12 je $K = \mathbb{Q}(\sqrt{d})$ pro nějaké celé číslo $d = \pm 2^e p_1 \cdots p_r$, kde $e$ je 0 nebo 1 a $p_i$ jsou po dvou různá lichá prvočísla. Potom jistě $K \subseteq \mathbb{Q}(\sqrt{-1}, \sqrt{2}, \sqrt{p_1}, \ldots, \sqrt{p_r})$. Přitom $\sqrt{-1} = \zeta_4 = i$ a $\sqrt{2}$ se dá za pomoci $\zeta_8^2 = \zeta_4$ vyjádřit takto:

$$\left(\zeta_8 + \zeta_8^{-1}\right)^2 = \zeta_4 + \zeta_4^{-1} + 2 = i + (-i) + 2 = 2.$$

Máme tedy $\mathbb{Q}(\sqrt{-1},\sqrt{2}) \subseteq \mathbb{Q}(\zeta_8)$ a zbývá se vypořádat s lichými prvočísly. Proti nim použijeme lemma 3.13.

Diskriminant polynomu $X^p - 1$ můžeme pro liché prvočíslo $p$ napsat jako $p^p(-1)^{(p-1)(3p-2)/2} = p(-1)^{(p-1)/2}(p^{(p-1)/2})^2$ a jeho odmocnina leží v $\mathbb{Q}(\zeta_p)$. Celkem tedy máme

$$\mathbb{Q}(\zeta_p) \supseteq \mathbb{Q}\left(\sqrt{\operatorname{discr}(X^p-1)}\right) = \\ = \mathbb{Q}\left(\sqrt{p(-1)^{\frac{p-1}{2}}}\right) = \begin{cases} \mathbb{Q}(\sqrt{p}) & \text{pokud } p \equiv 1 \pmod 4, \\ \mathbb{Q}(\sqrt{-p}) & \text{pokud } p \equiv 3 \pmod 4. \end{cases}$$

Zkombinujeme dosavadní výsledky dohromady a dostaneme

$$K = \mathbb{Q}(\sqrt{d}) \subseteq \mathbb{Q}(\sqrt{-1},\sqrt{2},\sqrt{p_1},\ldots,\sqrt{p_r}) \subseteq \mathbb{Q}(\zeta_8,\zeta_{p_1},\ldots,\zeta_{p_r}) \subseteq \mathbb{Q}(\zeta_m),$$

kde $m = 8p_1\cdots p_r$. ✠

*Poznámka.* Ať $p$ je liché prvočíslo. Galoisova grupa tělesa $\mathbb{Q}(\zeta_p)$ je isomorfní $\mathbb{Z}_p^*$ a je tedy cyklická. Proto obsahuje právě jednu podgrupu indexu 2 a tedy $\mathbb{Q}(\zeta_p)$ obsahuje právě jedno kvadratické rozšíření $\mathbb{Q}$. Z předchozího důkazu plyne, že to je buď $\mathbb{Q}(\sqrt{p})$, nebo $\mathbb{Q}(\sqrt{-p})$ podle toho, jestli je $p \equiv 1$ nebo $3 \pmod 4$.

Podívejme se na závěr této sekce na reálná podtělesa $\mathbb{Q}(\zeta_n)$, jmenovitě na to největší vzhledem k inkluzi.

**Tvrzení 3.14.** *Ať $\alpha_n$ značí $\zeta_n + \zeta_n^{-1}$. Potom $\mathbb{Q}(\alpha_n) = \mathbb{Q}(\zeta_n) \cap \mathbb{R}$.*

*Důkaz:* $\zeta_n + \zeta_n^{-1} = 2\cos(2\pi/n)$, takže jistě $\mathbb{Q}(\alpha_n) \subseteq \mathbb{Q}(\zeta_n) \cap \mathbb{R}$. Zároveň máme $[\mathbb{Q}(\zeta_n) : (\mathbb{Q}(\zeta_n) \cap \mathbb{R})] = 2$ a díky $\zeta_n^2 - \alpha\zeta_n + 1 = 0$ je určitě $[\mathbb{Q}(\zeta_n) : \mathbb{Q}(\alpha)] \leq 2$, takže platí i $\mathbb{Q}(\alpha_n) \supseteq \mathbb{Q}(\zeta_n) \cap \mathbb{R}$. ✠

## 3.4 Celistvé prvky a diskriminant

V následujících dvou sekcích se budeme věnovat $p$-tým cyklotomickým tělesům $\mathbb{Q}(\zeta_p)$, kde $\zeta_p$ je primitivní $p$-tá odmocnina z jedné a $p$ liché prvočíslo. Minimálním polynomem prvku $\zeta_p$ je

$$\Phi_p(X) = \prod_{i=1}^{p-1}(X - \zeta_p^i) = X^{p-1} + X^{p-2} + \cdots + X + 1. \tag{3.1}$$

Stupeň $\mathbb{Q}(\zeta_p)$ nad $\mathbb{Q}$ je tedy $p-1$ a jeho prvky jsou tvaru $a_0 + a_1\zeta_p + \cdots + a_{p-2}\zeta_p^{p-2}$, $a_i \in \mathbb{Q}$. Pišme nadále místo $\zeta_p$ prostě $\zeta$ a značme $A$ okruh algebraických celých čísel tělesa $\mathbb{Q}(\zeta)$. Zřejmě je $\zeta \in A$. Následující lemma se nám bude často hodit.

**Lemma 3.15.**

(1) *Prvky* $1-\zeta, 1-\zeta^2, \ldots, 1-\zeta^{p-1}$ *jsou navzájem asociované v* $A$.

(2) $\mathrm{N}(1-\zeta) = \prod_{i=1}^{p-1}(1-\zeta^i) = \Phi_p(1) = p = \varepsilon(1-\zeta)^{p-1}$, *kde* $\varepsilon$ *je invertibilní prvek v* $A$.

(3) $1-\zeta$ *je ireducibilní a* $A(1-\zeta)\cap\mathbb{Z} = \mathbb{Z}p$.

*Důkaz:* (1) Zvolme $i, j \in \{1, \ldots, p-1\}$. Protože $\mathbb{Z}_p^*$ je cyklická grupa, existuje $k$ takové, že $j \equiv ik \pmod p$. Protože $\zeta$ je $p$-tá odmocnina z jedné, dostáváme

$$\frac{1-\zeta^j}{1-\zeta^i} = \frac{1-\zeta^{ik}}{1-\zeta^i} = 1+\zeta^i+\cdots+\zeta^{(k-1)i} \in A.$$

Podobně i $(1-\zeta^i)/(1-\zeta^j) \in A$ a tedy $1-\zeta^i \parallel 1-\zeta^j$.

(2) Podle vzorce (2.2) máme

$$\mathrm{N}(1-\zeta) = \prod_{i=1}^{p-1}\sigma_i(1-\zeta) = \prod_{i=1}^{p-1}(1-\zeta^i),$$

kde $\sigma_1, \ldots, \sigma_{p-1}$ jsou prvky Galoisovy grupy tělesa $\mathbb{Q}(\zeta)$. Druhá a třetí rovnost plynou přímo z definice a čtvrtou rovnost dostaneme aplikací předchozí části důkazu.

(3) Kdyby nějaké $\alpha \in A$ bylo vlastním dělitelem $1-\zeta$, musela by i norma $\mathrm{N}(\alpha)$ být vlastním dělitelem $\mathrm{N}(1-\zeta) = p$. Protože $\mathrm{N}(\alpha)$ je podle tvrzení 2.4 prvkem $\mathbb{Z}$, dostáváme spor.

Vzhledem k tomu, že $A(1-\zeta)$ díky části (2) obsahuje $p$ a neobsahuje 1, je $A(1-\zeta)\cap\mathbb{Z} = \mathbb{Z}p$. ✠

Naše další snažení bude směřovat k popisu prvků okruhu $A$. Obecný výsledek z předchozí kapitoly říká, že $A$ je volná Abelova grupa hodnosti stejné, jako je dimenze tělesa, tedy $p-1$. My tento fakt nyní dokážeme explicitně (důkaz přebíráme z [9, sekce 5.5]. Protože $A$ obsahuje $\mathbb{Z}$ a $\zeta$ je prvkem $A$, zřejmě je $\mathbb{Z}[\zeta] = \{z_0 + z_1\zeta + \cdots + z_{p-2}\zeta^{p-2} \mid z_i \in \mathbb{Z}\} \subseteq A$. Je dobré, že platí i opačná inkluze:

**Tvrzení 3.16.** $A = \mathbb{Z}[\zeta]$, *neboli* $A$ *je volná Abelova grupa s bází* $\{1, \zeta, \ldots, \zeta^{p-2}\}$.

*Důkaz:* Zvolme $x \in A$, $x = a_0 + a_1\zeta + \cdots + a_{p-2}\zeta^{p-2}$, kde $a_i \in \mathbb{Q}$. Dokažme indukcí, že všechna $a_i$ ve skutečnosti leží v $\mathbb{Z}$.

Odečteme-li od $x$ prvek $x\zeta = a_0\zeta + a_1\zeta^2 + \cdots + a_{p-2}\zeta^{p-1}$, dostáváme

$$x(1-\zeta) = a_0(1-\zeta) + a_1(\zeta-\zeta^2) + \cdots + a_{p-2}(\zeta^{p-2}-\zeta^{p-1}).$$

Protože prvky $\zeta, \ldots, \zeta^{p-1}$ jsou navzájem konjugované (jsou to kořeny polynomu (3.1)), mají všechny stejnou stopu rovnou $\mathrm{Tr}(\zeta) = \sum_{i=1}^{p-1}\zeta^i = -1$. S využitím vztahů (2.3) tak máme

$$\begin{aligned}\mathrm{Tr}(x(1-\zeta)) &= \mathrm{Tr}(a_0(1-\zeta)) + \cdots + \mathrm{Tr}(a_{p-2}(\zeta^{p-2}-\zeta^{p-1}))\\ &= a_0\cdot\mathrm{Tr}(1-\zeta) = a_0[(p-1)-(-1)] = a_0p.\end{aligned}$$

Nechť $x_1 = x, x_2, \ldots, x_{p-1}$ jsou konjugace prvku $x$. Podle tvrzení 2.4 víme, že leží v $A$. S využitím této znalosti a části (1) předchozího lemmatu spočítejme stopu ještě jiným způsobem, tentokrát podle vztahu (2.1):

$$\begin{aligned}\mathrm{Tr}(x(1-\zeta)) &= x_1(1-\zeta) + x_2(1-\zeta^2) + \cdots + x_{p-1}(1-\zeta^{p-1}) \\ &= x'(1-\zeta) \in A(1-\zeta).\end{aligned}$$

Ale $\mathrm{Tr}(x(1-\zeta))$ patří do $\mathbb{Z}$, a tak podle části (3) téhož lemmatu dostáváme $\mathrm{Tr}(x(1-\zeta)) = a_0 p \in \mathbb{Z}p$, neboli $a_0 \in \mathbb{Z}$.

Předpokládejme nyní, že $a_{j-1}$ leží v $\mathbb{Z}$, a dokažme to samé o $a_j$. Násobme $x$ tentokrát $\zeta^{p-j}$: $x\zeta^{p-j} = a_0\zeta^{p-j} + \cdots + a_{j-1}\zeta^{p-1} + a_j + a_{j+1}\zeta + \cdots + a_{p-2}\zeta^{p-j-2}$. Vyjádříme-li $\zeta^{p-1}$ podle (3.1) v nižších mocninách $\zeta$, dostaneme po vhodné substituci zápis

$$x\zeta^{p-j} = (a_j - a_{j-1}) + a'_1\zeta + a'_2\zeta + \cdots + a'_{p-2}\zeta^{p-2}.$$

Protože $x\zeta^{p-j} \in A$, analogickým postupem jako v první části důkazu dostaneme $a_j - a_{j-1} \in \mathbb{Z}$ a díky indukčnímu předpokladu tak máme i $a_j \in \mathbb{Z}$. Tím je důkaz hotov. ✠

V druhé části této sekce spočteme diskriminant $\delta_{\mathbb{Q}(\zeta)}$ tělesa $\mathbb{Q}(\zeta)$, tj. diskriminant jeho celistvé báze $\{1, \zeta, \ldots, \zeta^{p-2}\}$.

**Tvrzení 3.17.** $\delta_{\mathbb{Q}(\zeta)} = (-1)^{(p-1)/2} p^{p-2}$.

*Důkaz:* Diskriminant budeme počítat podle definičního vzorce $\mathrm{discr}(1, \zeta, \ldots, \zeta^{p-2}) = \det(\mathrm{Tr}(\zeta^{i+j})_{i,j=0}^{p-2})$. V důkazu předchozího tvrzení jsme spočetli $\mathrm{Tr}(1) = p-1$ a $\mathrm{Tr}(\zeta) = \cdots = \mathrm{Tr}(\zeta^{p-1}) = -1$. Máme tedy

$$\mathrm{discr}(1, \zeta, \ldots, \zeta^{p-2}) = \begin{vmatrix} p-1 & -1 & -1 & -1 & \ldots & -1 \\ -1 & -1 & -1 & -1 & \ldots & -1 \\ -1 & -1 & -1 & -1 & \ldots & p-1 \\ \vdots & \vdots & \vdots & \vdots & \iddots & \vdots \\ -1 & -1 & -1 & p-1 & \ldots & -1 \\ -1 & -1 & p-1 & -1 & \ldots & -1 \end{vmatrix}.$$

Tento determinant $D$ budeme upravovat takto:

(1) Odečteme první řádek od všech ostatních řádků.
(2) Rozvineme determinant podle druhého řádku.
(3) Nový determinant rozvineme podle prvního sloupce.

$$D \overset{(1)}{=} \overbrace{\begin{vmatrix} p-1 & -1 & -1 & \dots & -1 \\ -p & 0 & 0 & \dots & 0 \\ -p & 0 & 0 & \dots & p \\ \vdots & \vdots & \vdots & \iddots & \vdots \\ -p & 0 & p & \dots & 0 \end{vmatrix}}^{p-1} \overset{(2)}{=} -p(-1)^3 \cdot \overbrace{\begin{vmatrix} -1 & -1 & \dots & -1 \\ 0 & 0 & \dots & p \\ \vdots & \vdots & \iddots & \vdots \\ 0 & p & \dots & 0 \end{vmatrix}}^{p-2}$$

$$\overset{(3)}{=} -p(-1)^2 \cdot \overbrace{\begin{vmatrix} 0 & \dots & 0 & p \\ 0 & \dots & p & 0 \\ \vdots & \iddots & \vdots & \vdots \\ p & \dots & 0 & 0 \end{vmatrix}}^{p-3} = -p(-1)^{(p-3)/2}p^{p-3} = (-1)^{(p-1)/2}p^{p-2}.$$

✠

*Poznámka.* Pro každé cyklotomické těleso $\mathbb{Q}(\zeta_m)$ platí, že jeho okruh algebraických celých čísel je $\mathbb{Z}[\zeta_m]$. Stejně tak se dají podobnou metodou odvodit i příslušné diskriminanty. Důkazy nejsou obtížné, pouze trochu zdlouhavé. Navíc tyto výsledky nebudeme nikde potřebovat, a tak čtenáře pouze odkážeme na [9, sekce 16.2].

## 3.5 Invertibilní prvky

Popis invertibilních prvků (jednotek) v okruhu algebraických celých čísel cyklotomického tělesa pro nás bude velmi důležitý v kapitole 7. Jako základní výsledek jej však uvedeme už teď.

Budeme se pohybovat ve fixním tělese $\mathbb{Q}(\zeta_p) = \mathbb{Q}(\zeta)$, $p$ liché prvočíslo, s okruhem celistvých prvků $A$. Jednotky v $A$ zřejmě tvoří multiplikativní grupu. Budeme ji značit $U_{\mathbb{Q}(\zeta)} = U$. Označme ještě $W_{\mathbb{Q}(\zeta)} = W$ grupu všech odmocnin z jedné v $\mathbb{Q}(\zeta)$. Zřejmě $W \subseteq A$. Budou nás přirozeně zajímat jak velikosti $U$ a $W$, tak vztahy mezi nimi. Některé snadné výsledky obsahuje následující

**Lemma 3.18.**

(1) $W = \{1, \zeta, \zeta^2, \dots, \zeta^{p-1}, -1, -\zeta, -\zeta^2, \dots, -\zeta^{p-1}\}$.

(2) *$W$ je cyklickou podgrupou $U$.*

(3) *Ať $x^{(1)} = x, x^{(2)}, \dots, x^{(p-1)}$ jsou prvky konjugované s $x \in A$ a ať $|x^{(i)}| = 1$ pro $1 \leq i \leq p-1$, přičemž $|\cdot|$ značí absolutní hodnotu komplexního čísla. Pak $x$ je odmocnina z jedné.*

*Důkaz:* (1) Všechny uvedené prvky $W$ jistě obsahuje. Jsou to totiž $2p$-té odmocniny z jedné. Kdyby ve $W$ byla ještě nějaká primitivní $m$-tá odmocnina z jedné,

$m \nmid 2p$, pak by bylo $\mathbb{Q}(\zeta_m) \subseteq \mathbb{Q}(\zeta_p)$. Podle tvrzení 3.10 však $\mathbb{Q}(\zeta_p)$ obsahuje jen cyklotomická tělesa $\mathbb{Q}(\zeta_1) = \mathbb{Q}(\zeta_2) = \mathbb{Q}$ a $\mathbb{Q}(\zeta_{2p}) = \mathbb{Q}(\zeta_p)$.

(2) Je-li $\pm\zeta^k \in W$, tak je i $\pm\zeta^{-k} = \pm\zeta^{p-k} \in W$. Tedy $W$ je podgrupou $U$. Její cykličnost plyne z toho, že $-\zeta$ má řád $2p$.

(3) Nejprve ukážeme, že prvků $x$ splňujících předpoklady je jen konečně mnoho. Nechť $f(X) = \prod_{i=1}^{p-1}(X - x^{(i)}) = a_0 + a_1X + \cdots + a_kX^{p-1}$ je takzvaný charakteristický polynom prvku $x$. Je vidět, že $f \in \mathbb{Z}[X]$ (je to mocnina minimálního polynomu $x$). Jeho koeficienty jsou až na znaménko elementární symetrické polynomy v proměnných $x^{(1)}, \ldots, x^{(p-1)}$, tj.

$$a_k = \sum_{i_1<i_2<\cdots<i_k} x^{(i_1)}x^{(i_2)}\cdots x^{(i_k)}, \qquad k = 0, 1, \ldots, p-1.$$

Absolutní hodnota všech sčítanců je rovna 1, takže $|a_k| \leq \binom{p-1}{k} \leq (p-1)!$ pro všechna $1 \leq k \leq p-1$. Tedy prvky s předpokládanou vlastností jsou kořeny polynomů z množiny $S = \{g \in \mathbb{Z}[X] \mid \deg(g) = p-1 \ a \ |\text{koeficient } g| \leq (p-1)!\}$. Ta je konečná, a proto je konečný i počet kořenů jejích polynomů.

Pokud prvky konjugované s $x$ jsou v absolutní hodnotě menší než jedna, jistě tuto vlastnost mají i konjugace prvků $x^2, x^3, \ldots$ Podle předchozího je tato množina konečná, a tak musí být $x^r = x^s$ pro nějaká $1 \leq r < s$. Jinak řečeno $x$ je $(s-r)$-tá odmocnina z jedné. ✠

Dostáváme se nyní k hlavnímu tvrzení sekce, které dokázal Kummer při práci na důkazu Velké Fermatovy věty. Citujeme z [9, str.176].

**Tvrzení 3.19.** *Každé $u \in U$ se dá napsat jako $\zeta^k v$, kde $v \in U \cap \mathbb{R}$.*

*Důkaz:* Nechť $\overline{u}$ značí číslo komplexně sdružené k $u$. Pak $\overline{u}$ je zřejmě také jednotka ($uv = 1 \Rightarrow \overline{u} \cdot \overline{v} = 1$). Položme $u' = u \cdot \overline{u}^{-1}$. Ukážeme, že $u'$ je odmocnina z jedné.

Zvolme $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta)|\mathbb{Q})$. Protože komplexní sdružování je automorfismem tělesa $\mathbb{Q}(\zeta)$ a $\mathrm{Gal}(\mathbb{Q}(\zeta)|\mathbb{Q})$ je Abelova grupa, platí $\sigma(\overline{u}) = \overline{\sigma(u)}$. Počítejme:

$$|\sigma(u \cdot \overline{u}^{-1})| = |\sigma(u) \cdot \sigma(\overline{u})^{-1}| = |\sigma(u)| \cdot |\overline{\sigma(u)}|^{-1} = 1.$$

Při značení položky (3) předchozího lemmatu tedy máme $|u'^{(i)}| = 1$ pro všechna $1 \leq i \leq p-1$, takže $u'$ je skutečně odmocnina z jedné. Podle (1) téhož lemmatu je $u' = \pm\zeta^h$ pro nějaké $h = 0, 1, \ldots, p-1$. Ukážeme, že musí být $u' = \zeta^h$.

Pokud $u$ je tvaru $z_0 + z_1\zeta + \cdots + z_{p-2}\zeta^{p-2}$, pak zřejmě $\overline{u} = z_0 + z_1\zeta^{-1} + \cdots + z_{p-2}\zeta^{-(p-2)}$. Počítejme modulo $p$:

$$u^p = \left(\sum_{i=0}^{p-2} z_i\zeta^i\right)^p \equiv \sum_{i=0}^{p-2} z_i^p \equiv \left(\sum_{i=0}^{p-2} z_i\zeta^{-i}\right)^p = \overline{u}^p \pmod{p}.$$

Kdyby bylo $u' = -\zeta^h$, tak $u = -\zeta^h\overline{u}$ a $u^p \equiv -\overline{u}^p \pmod{p}$. Potom $2u^p \equiv 0 \pmod{p}$, neboli $p|2u^p$. Protože $u^p$ je jednotka, musí být $p|2$, což není možné, a proto $u' = \zeta^h$.

Zvolme $k$ tak, aby $2k \equiv h \pmod{p}$. Potom díky $\zeta^{2k} = \zeta^h$ dostáváme

$$\frac{u}{\zeta^k} = \zeta^k \overline{u} = \frac{\overline{u}}{\zeta^{-k}} = \overline{\left(\frac{u}{\zeta^k}\right)}.$$

Položíme-li $v = u/\zeta^k$, máme $v \in U \cap \mathbb{R}$, $v$ je jednotka a $u = \zeta^k v$. ✠

**Důsledek.** *Označme $U^+$ grupu jednotek okruhu algebraických celých čísel tělesa $\mathbb{Q}(\zeta + \zeta^{-1})$. Pak $U = \langle\zeta\rangle \times U^+$, kde $\langle\zeta\rangle$ značí cyklickou grupu generovanou $\zeta$.*

*Důkaz:* Plyne z předchozího tvrzení a tvrzení 3.14. ✠

Podívejme se teď na jednu důležitou třídu jednotek z $U^+$. Podle lemmatu 3.15 z předchozí sekce je $1 - \zeta^s$ asociované s $1 - \zeta$ pro $1 \leq s \leq p - 1$ a tedy $u = (1 - \zeta^s)/(1 - \zeta)$ je jednotkou okruhu $A$. Zřejmě je $\overline{u} = (1 - \zeta^{-s})/(1 - \zeta^{-1})$, a proto podle poslední části předchozího důkazu existuje $k$ celé tak, že $(1-\zeta^s)/(1-\zeta) = \zeta^{2k}(1 - \zeta^{-s})/(1 - \zeta^{-1})$, neboli

$$\frac{1 - \zeta^s}{1 - \zeta} \cdot \frac{1 - \zeta^{-s}}{1 - \zeta^{-1}} = \left(\zeta^k \frac{1 - \zeta^{-s}}{1 - \zeta^{-1}}\right)^2.$$

Položíme-li

$$v_s = \sqrt{\frac{1 - \zeta^s}{1 - \zeta} \cdot \frac{1 - \zeta^{-s}}{1 - \zeta^{-1}}},$$

pak $v_s \in A$ a protože je výraz pod odmocninou invariatní vůči komplexnímu sdružování, je $v_s \in \mathbb{R}$. Celkem tedy máme $v_s \in U^+$. Prvky $v_s$ pro $s = 2, 3, \ldots, (p-1)/2$ nazýváme *kruhové jednotky*. Je vidět, že jsou po dvou různé a že nejsou ani 1, ani $-1$.

V této sekci jsme tedy ukázali, že každá jednotka okruhu algebraických celých čísel cyklotomického tělesa $\mathbb{Q}(\zeta_p)$ je součinem $p$-té odmocniny z jedné a reálné jednotky. S tímto si pro naše účely vystačíme. Následující tvrzení, které zde uvedeme alespoň bez důkazu, však dává strukturní výsledek pro všechna číselná tělesa. Uvažujme teď obecné rozšíření $K = \mathbb{Q}(t)$ stupně $n$ a nechť $t_1 = t, t_2, \ldots, t_n$ jsou kořeny minimálního polynomu $f$ prvku $t$. Víme, že ty ryze komplexní se vyskytují v párech. Označme $r_1$, resp. $2r_2$ počet reálných, resp. ryze komplexních kořenů polynomu $f$, tedy $r_1 + 2r_2 = n$. Nyní již můžeme zformulovat tzv. *Dirichletovu větu o jednotce*. Její důkaz nalezne čtenář v [9, sekce 10.4].

**Věta 3.20** (Dirichlet)**.** *Grupa jednotek $U_K$ okruhu celistvých prvků tělesa $K$ je tvaru*

$$U_K \cong W_K \times C_1 \times \cdots \times C_r,$$

*kde $W_K$ je konečná cyklická grupa všech odmocnin z jedné, $C_i$ jsou nekonečné cyklické multiplikativní grupy a $r = r_1 + r_2 - 1$.*

Číslo $r$ se nazývá *hodnost* grupy $U_K$.

# Kapitola 4

# Konstrukce pravidelných n-úhelníků

Tato kapitola slouží jako mírné odlehčení po předchozích teoretických částech. Čtenář by při její četbě měl nabrat dostatek energie ke strávení kapitol následujících, jejichž tématem již bude Velká Fermatova věta. Ačkoliv se zde o cyklotomických tělesech nedokazují žádné hluboké výsledky, je to partie matematiky natolik klasická, že si zaslouží být v této souvislosti uvedena.

## 4.1 Konstrukce pravítkem a kružítkem

Podíváme se na jeden velmi starý problém, kterým je konstrukce geometrických útvarů „ideálním“ pravítkem a kružítkem. Jak ale uvidíme, oba dva nástroje budou mít k dokonalosti daleko, protože značně omezíme funkce, které se jinak u běžných pravítek a kružítek využívají.

Tak především naše *ideální pravítko* má jen jednu hranu (zato nekonečnou), ale nemá žádné značky, které bychom mohli použít k měření vzdáleností. Pravítkem tedy můžeme narýsovat jen přímku procházející dvěma zadanými body. *Ideální kružítko* slouží k rýsování kružnice se zadaným středem a poloměrem. Díky jeho dokonalosti můžeme tímto kružítkem narýsovat kružnici o libovolně velkém (zadaném) poloměru. Na druhou stranu nemůže být přímo použito k přenášení vzdáleností. Toto velmi silné omezení se dá naštěstí povolenými prostředky snadno obejít, takže jej dále nebudeme uvažovat.

Už z dob antického Řecka pocházejí tyto tři slavné úlohy:

**Kvadratura kruhu** Pro daný poloměr $r$ sestroj stranu čtverce, který má stejný obsah jako kruh o poloměru $r$.

**Zdvojení krychle** K dané krychli s hranou $a$ sestroj hranu $b$, že krychle s hranou $b$ má dvojnásobný objem oproti krychli s hranou $a$.

**Trisekce úhlu** Daný úhel rozděl na tři stejně velké úhly.

Ekvivalentní vyslovení prvních dvou úloh v řeči moderní matematiky zní takto: Pro danou jednotkovou úsečku sestroj úsečku délky $\pi$, resp. $\sqrt[3]{2}$. Po 2000 let se matematici snažili tyto úlohy vyřešit, leč neúspěšně. Až teprve rozvoj algebry a zejména teorie číselných těles v 19. století jim dal do ruky nástroj vhodný k uchopení těchto problémů. My v této sekci jako vedlejší výsledek dostaneme řešení všech tří úloh. Naším hlavním cílem je však zkoumání jiného problému, jehož kořeny sahají také až do starověku.

Eukleidés (asi 300 př.n.l.) ve 4. knize svých *Základů* (řec. $\Sigma\tau o\iota\chi\epsilon\tilde{\iota}\alpha$) provedl konstrukci pravidelného čtyř-, pěti-, šesti- a patnáctiúhelníka. Od té doby zůstávalo stále otevřeným problémem, zda i pro jiná $n > 3$ lze sesrojit pravidelný $n$-úhelník. Až v roce 1796 dokázal teprve 19 letý Carl Friedrich Gauss, že je možné sestrojit pravidelný 17-úhelník. O pár let později potom podal postačující podmínku sestrojitelnosti pravidelných $n$-úhelníků pro libovolná $n$.

K rozhodnutí řešitelnosti nebo neřešitelnosti daného konstrukčního problému chceme využít teorii číselných těles. K tomu budeme potřebovat vhodně formalizovat proces konstruování geometrických útvarů. Konstrukce provádíme v rovině, kterou chápeme jako reálný eukleidovský prostor dimenze 2. Každý bod roviny potom ztotožňujeme s jeho souřadnicemi vzhledem k nějaké bázi. Na začátku konstrukčního procesu jsme obdařeni jen *počátečními body* $(0, 0)$ a $(1, 0)$. Bod roviny nazveme *sestrojitelným*, pokud jej můžeme sestrojit opakováním některých z níže uvedených konstrukcí:

1. Veď přímku dvěma již sestrojenými body.
2. Narýsuj kružnici se středem v již sestrojeném bodě a poloměrem rovným vzdálenosti mezi dvěma již sestrojenými body.
3. K již sestrojeným bodům přidej další bod, který je:
   (a) průsečíkem dvou přímek nebo
   (b) průsečíkem přímky a kružnice nebo
   (c) průsečíkem dvou kružnic.

Předpokládejme, že jsme již sestrojili množinu bodů $\mathcal{P}_n = \{P_0 = (0, 0),\ P_1 = (1, 0),\ P_2, \ldots, P_n\}$ a označme $K$ nejmenší podtěleso $\mathbb{R}$, které obsahuje souřadnice všech $P_i$. Podívejme se nyní, jakým způsobem z těchto bodů můžeme sestrojit další bod $P_{n+1}$. Konstrukci rozlišíme podle případů uvedených v 3.:

(a) Přímka daná některými dvěma body z $\mathcal{P}_n$ má rovnici s koeficienty z $K$. Průsečík dvou takových přímek je řešením soustavy dvou lineárních rovnic o dvou neznámých s koeficienty v $K$, a tedy má souřadnice také v $K$.

(b) I kružnice sestrojená pomocí bodů z $\mathcal{P}_n$ má rovnici s koeficienty v $K$. V tomto případě je průsečík dán jako řešení soustavy lineární a kvadratické rovnice o dvou neznámých. Vyjádřením z lineární rovnice a dosazením do kvadratické dostaneme kvadratickou rovnici o jedné neznámé s nezáporným

diskriminantem $d$. Podle toho, zda $\sqrt{d}$ leží nebo neleží v $K$, má průsečík přímky a kružnice souřadnice buď v $K$, nebo v $K(\sqrt{d})$.

(c) Podobně jako v (b) se ukáže, že hledaný průsečík má opět souřadnice z $K$ nebo z $K(\sqrt{d})$.

Závěr: Nejmenší reálné podtěleso obsahující souřadnice bodů $P_{n+1} \cup \mathcal{P}_n$ je buď $K$ nebo $K(\sqrt{d})$.

Abychom mohli zapojit do hry cyklotomická tělesa (což kromě netriviálních případů nejsou podtělesa $\mathbb{R}$), zavedeme pojem sestrojitelné komplexní číslo. Tak tedy komplexní číslo $a+bi$ se nazývá *sestrojitelné*, pokud je sestrojitelný bod $(a, b)$ podle předešlé definice. Výše prováděné úvahy nyní zformulujeme pro sestrojitelná komplexní čísla jako

**Tvrzení 4.1.** *Pro každé sestrojitelné číslo $z \in \mathbb{C}$ existuje konečná posloupnost $K_0 = \mathbb{Q}, K_1, \ldots, K_t, K_{t+1}$ algebraických rozšíření tělesa $\mathbb{Q}$ taková, že $z$ patří do $K_{t+1}$, pro $j = 1, \ldots, t$ je $K_j = K_{j-1}(\sqrt{d_{j-1}})$, kde $d_{j-1} \in K_{j-1}$, $d_{j-1} \geq 0$, a konečně $K_{t+1} = K_t(i)$, kde $i = \sqrt{-1}$. Speciálně je $[K_{t+1} : \mathbb{Q}]$ rovno $2^k$ pro nějaké $k \geq 0$.*

*Důkaz:* Tvrzení je opravdu důsledkem předchozích úvah. Stačí si jen uvědomit, že $K_t$ již obsahuje reálnou i imaginární část $z$, a tedy $z$ patří do $K_t(i)$. Část o dimenzi plyne z toho, že $[M : L][L : K] = [M : K]$ pro každé rozšíření těles $K \leq L \leq M$ a $X^2 + 1 \in K_t[X]$ je minimálním polynomem $i$. ✠

*Poznámka.* Prvek $i$ samozřejmě můžeme přidat kdykoliv během rozšiřování. My jsme jej přidali až nakonec jen z toho důvodu, abychom mohli korektně navázat na předcházející názorné úvahy.

K tomu, abychom dokázali, že nějaké číslo $z$ není sestrojitelné, stačí podle předchozího tvrzení ukázat, že existuje rozšíření těles $L \geq K \geq \mathbb{Q}$ takové, že $L = K(z)$ a buď dimenze $L$ nad $K$ není konečná, nebo není mocnina dvojky. Na závěr sekce využijeme toto pozorování k důkazu neřešitelnosti kvadratury kruhu a zdvojení krychle.

Díky výsledkům z 19.století víme, že číslo $\pi$ je transcendentní, což dokazuje nemožnost kvadratury kruhu. Minimálním polynomem čísla $\sqrt[3]{2}$ nad $\mathbb{Q}$ je $X^3 - 2$, tj. $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$, takže ani zdvojení krychle není proveditelné jen za pomoci pravítka a kružítka.

## 4.2 Gaussova věta

V této sekci, která je inspirovaná [5, str.15–17], dokážeme nutnou a postačující podmínku k tomu, aby se pravidelný $n$-úhelník dal sestrojit pomocí pravítka a kružítka. Toto tvrzení zformuloval a jednu jeho část dokázal Gauss v knize Disquisitiones Arithmeticae z roku 1801. Druhou část dokázal Pierre Laurent Wantzel

v roce 1837. Ten také jako první předvedl nemožnost zdvojení krychle a trisekce úhlu.

Dříve než přistoupíme k hlavnímu tvrzení, dokážeme jedno pomocné lemma.

**Lemma 4.2.** *Označme $\mathcal{K}$ množinu všech sestrojitelných čísel. Pak $\mathcal{K}$ je podtěleso $\mathbb{C}$ uzavřené na odmocňování prvků.*

*Důkaz:* Ověříme axiomy tělesa. Z definice obsahuje $\mathcal{K}$ nulový prvek 0 i jednotkový prvek 1. Naznačíme, jak k daným bodům $A, B$ (budeme teď pro názornost opět ztotožňovat komplexní čísla s body roviny) sestrojit body $A+B$ a $A \cdot B$. Zároveň se vyhneme zřejmým triviálním případům, jako např. $A$ nebo $B$ je nula. Vřele čtenáři doporučujeme, aby si při důkazech kreslil.

Pro kterýkoliv bod $C$ budeme velikost úsečky $\overline{C0}$ značit prostě $|C|$.
*Součet:* Sestrojme kružnice $k_1(A, |B|)$ a $k_2(B, |A|)$. Hledaný bod $A + B$ je ten jejich průsečík, který neleží v polorovině určené přímkou $\overline{AB}$ a bodem 0 (případ $A, B, 0$ leží na jedné přímce je jasný).
*Součin:* Ať $B$ neleží na reálné přímce. Způsobem známým ze střední školy, využívajícím podobnosti trojúhelníků, sestrojíme úsečku délky $r = |A||B|$ a kružnici $k_3(0, r)$. Označme $A', B', 1'$ po řadě průsečíky kružnice $k_3$ s přímkami $\overline{A0}, \overline{B0}, \overline{10}$ (je zřejmé, který průsečík za dvou máme vybrat). Sestrojme kružnici $k_4(A', |1'B'|)$. Pokud leží bod $B$ v polorovině dané přímkou $\overline{10}$ a bodem $i = (0, 1)$ (je jasné, jak jej sestrojit), označíme jako $A \cdot B$ průsečík $k_4$ s $k_3$, který potkáme jako první, když půjdeme cestou po $k_3$ z bodu $A'$ proti směru hodinových ručiček. Analogicky naopak. Přitom máme na mysli ručičkové hodiny známé z běžných domácností. Světaznalý čtenář se totiž mohl setkat i s hodinami, kde jdou ručičky proti směru hodinových ručiček.

Konstrukce opačného prvku je zřejmá a inverzní prvek se sestrojí podobně jako součin. Uzavřenost na odmocniny plyne např. z Eukleidovy věty o výšce. ✠

Nyní již máme téměř vše připraveno, abychom dokázali hlavní tvrzení této kapitoly. Ještě však musíme definovat, co znamená tvrzení, že pravidelný $n$-úhelník je nebo není sestrojitelný. Umíme-li tento pravidelný útvar sestrojit, jistě umíme sestrojit i jeho základní úhel $2\pi/n$. Proto je přirozená následující definice.

Pravidelný $n$-úhelník nazveme *sestrojitelným*, pokud je sestrojitelné číslo $\zeta_n = e^{2\pi i/n}$.

**Věta 4.3** (Gauss: Disquisitiones Arithmeticae 1801)**.** *Pravidelný $n$-úhelník je pro $n > 2$ sestrojitelný, právě když je $n$ tvaru $2^s p_1 p_2 \cdots p_r$, kde $s, r \geq 0$ a $p_1, \ldots, p_r$ jsou po dvou různá lichá prvočísla tvaru $2^{l_r} + 1$ pro nějaká $l_r \geq 1$.*

*Důkaz:* Protože úloha rozpůlit i zdvojit úhel jde provést pravítkem a kružítkem, můžeme bez újmy na obecnosti předpokládat, že $n$ je liché.

($\Rightarrow$) Liché číslo $n$ je obecně tvaru $p_1^{a_1} \cdots p_r^{a_r}$, kde $a_i \geq 1$ a $p_1, \ldots, p_r$ jsou po dvou různá lichá prvočísla. Protože $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)$ a $\zeta_n$ je sestrojitelné, musí

být podle tvrzení 4.1 $\varphi(n) = 2^k$ pro nějaké $k \geq 0$. Platí

$$\varphi(n) = (p_1 - 1)p_1^{a_1-1} \cdots (p_r - 1)p_r^{a_r-1}.$$

Pokud má být $\varphi(n)$ mocnina dvojky, musí být nutně $p_1, \ldots, p_r$ tvaru $2^{l_r} + 1$ a $a_1 = \cdots = a_r = 1$, což je přesně tvrzení věty.

($\Leftarrow$) Má-li $n$ prvočíselný rozklad, jaký se předpokládá ve větě, je $\varphi(n)$ podle výpočtu v první části důkazu tvaru $2^k$. Galoisova grupa $G$ tělesa $\mathbb{Q}(\zeta_n)$ je podle tvrzení 3.6 isomorfní Abelově grupě $\mathbb{Z}_n^*$, a tak podle tvrzení z teorie grup obsahuje řetězec podgrup

$$G = G_0 \supset G_1 \supset \ldots \supset G_{k-1} \supset G_k = \{\mathrm{Id}\},$$

kde index $|G_0 : G_1| = \cdots = |G_{k-1} : G_k| = 2$. Označíme-li $\mathcal{F}(G_i)$ těleso sestávající z pevných bodů všech automorfismů z $G_i$, dostaneme ze základní věty Galoisovy teorie řetězec těles

$$\mathbb{Q} = \mathcal{F}(G_0) \subset \mathcal{F}(G_1) \subset \ldots \subset \mathcal{F}(G_{k-1}) \subset \mathcal{F}(G_k) = \mathbb{Q}(\zeta_n),$$

přičemž $[\mathcal{F}(G_k) : \mathcal{F}(G_{k-1})] = \cdots = [\mathcal{F}(G_1) : \mathcal{F}(G_0)] = 2$. Podle lemmatu 3.12 je každé $\mathcal{F}(G_{i+1})$ tvaru $\mathcal{F}(G_i)(\sqrt{d_i})$, $d_i \in \mathcal{F}(G_i)$. Začali jsme tedy tělesem (sestrojitelných) racionálních čísel a postupně jsme přidávali odmocniny. Protože těleso $\mathcal{K}$ je podle lemmatu 4.2 uzavřené na odmocňování, je $\mathbb{Q}(\zeta_n) \subseteq \mathcal{K}$ a tedy i $\zeta_n \in \mathcal{K}$, což se mělo dokázat. ✠

Pro $n \leq 40$ jsou tedy pravidelné $n$-úhelníky sestrojitelné pouze pro $n = 3, 4, 5, 6, 8, 10, 12, 15, 16, 17, 20, 24, 30, 32, 34, 40,$ přičemž jen případy $n = 17, 34$ nebyly známy už Eukleidovi.

**Důsledek.** *Trisekce úhlu nelze provést pravítkem a kružítkem.*

*Důkaz:* Kdyby šla trisekce provést, dal by se setrojit pravidelný 9-úhelník – spor.✠

Ačkoliv již máme úplnou charakterizaci sestrojitelných pravidelných $n$-úhelníků, předchozí věta nedává žádný jasný návod, jak ty skutečně sestrojitelné zkonstruovat. Pokud ovšem již umíme setrojit pravidelný $p$-úhelník i pravidelný $q$-úhelník pro nějaká dvě různá prvočísla $p, q$, umíme sestrojit i pravidelný $pq$-úhelník. Protože jsou $p, q$ nesoudělná, existují totiž podle Bézoutovy rovnosti celá čísla $a, b$ taková, že $ap + bq = 1$. Pravidelný $pq$-úhelník pak sestrojíme podle

$$a\frac{2\pi}{q} + b\frac{2\pi}{p} = \frac{2\pi}{pq}.$$

Jak ale sestrojit pravidelný $p$-úhelník pro $p$ prvočíslo? Trojúhelník sestrojit jistě umíme. Horší to již bude s 5- a 17-úhelníkem (pětiúhelník možná někteří z nás sestrojovali na střední škole). Zřejmě platí, že $\zeta_p$ je sestrojitelné číslo, právě když

je sestrojitelný $\cos\left(\frac{2\pi}{p}\right)$. Gaussova věta jinými slovy říká, že pro $\zeta_p$ sestrojitelné se dá $\cos\left(\frac{2\pi}{p}\right)$ vyjádřit jako výraz skládající se z běžných operací a (případně do sebe vnořených) druhých odmocnin. Kdyby se nám toto vyjádření povedlo najít, měli bychom aspoň nějaké vodítko, jak $\cos\left(\frac{2\pi}{p}\right)$ sestrojit.

Je známo, že $\cos\left(\frac{2\pi}{3}\right) = -\frac{1}{2}$. Spočítáme teď $\cos\left(\frac{2\pi}{5}\right)$:

$$X^{-2}\Phi_5(X) = X^2 + X^1 + X + X^{-1} + X^{-2} = (X + 1/X)^2 + (X + 1/X) - 1,$$

neboli $\zeta_5 + \zeta_5^{-1} = 2\cos\left(\frac{2\pi}{5}\right)$ je kořenem polynomu $Z^2 + Z - 1$ a tedy

$$2\cos\left(\frac{2\pi}{5}\right) = \frac{\sqrt{5}-1}{2} \quad \Longrightarrow \quad \cos\left(\frac{2\pi}{5}\right) = \frac{\sqrt{5}-1}{4}.$$

Všimněme si, že $(\sqrt{5}-1)/2$ je tzv. *zlatý řez*, což jak známo je poměr, kterým dělí průsečík libovolných dvou úhlopříček v pravidelném pětiúhelníku každou z nich.

Při práci na důkazu sestrojitelnosti pravidelného 17-úhelníka se pak Gaussovi povedlo odvodit tento vzorec:

$$\begin{aligned}\cos\left(\frac{2\pi}{17}\right) = &-\frac{1}{16} + \frac{1}{16}\sqrt{17} + \frac{1}{16}\sqrt{34 - 2\sqrt{17}} + \\ &+ \frac{1}{8}\sqrt{17 + 3\sqrt{17} - \sqrt{34 - 2\sqrt{17}} - 2\sqrt{34 + 2\sqrt{17}}}.\end{aligned}$$

Až dosud jsme zatajovali zřejmý fakt, že k úplné charakterizaci pravidelných $n$-úhelníků potřebujeme vědět, která čísla tvaru $a = 2^k+1$ jsou prvočísly. Tvrdíme, že pokud $a$ je prvočíslo, pak nutně $k$ je mocnina dvojky.

Kdyby tomu tak totiž nebylo, existuje liché $l > 1$ takové, že $k = lm$. Pak

$$2^k + 1 = (2^m)^l - (-1)^l = (2^m - (-1))((2^m)^{l-1} - (2^m)^{l-2} + \cdots)$$

a tedy $2^m + 1$ je vlastním dělitelem $2^k + 1$ – spor.

Číslům tvaru $F_k = 2^{2^k} + 1$ se říká *Fermatova čísla*, protože je Fermat studoval a na základě toho, že $F_1, \ldots, F_4$ jsou prvočísla, vyslovil domněnku, že všechna čísla tohoto tvaru jsou prvočísly. Euler však ukázal, že $F_5$ je složené, a do dnešní doby se žádné jiné Fermatovo prvočíslo najít nepodařilo. Nutno ovšem říct, že vzhledem k exponenciální rychlosti, jakou roste počet cifer Fermatových čísel, je jen pro $5 \leq k \leq 32$ dokázáno, že je $F_k$ složené. Kompletní rozklad pak známe pouze u $F_5, \ldots, F_{11}$.

Tato domněnka se stala Fermatovým nejslavnějším omylem, na základě nějž někteří lidé pochybovali i o platnosti Velké Fermatovy věty, které se budeme věnovat ve zbytku této práce.

# Kapitola 5

# Gaussův důkaz

Následující tři kapitoly budou víceméně směřovat k důkazu speciálního případu Velké Fermatovy věty. Od doby jejího vyslovení Fermatem až po Kummerův slavný důkaz uběhlo přes dvě stě let. My nebudeme sledovat tuto dlouhou cestu od začátku, ačkoliv prvotní výsledky jsme zmínili už v úvodní kapitole. Přejdeme rovnou až ke Gaussovu důkazu neřešitelnosti Fermatovy rovnice třetího stupně. Před ním sice tento případ dokázal Euler, ale Gaussův přístup již předznamenává Kummerův, a proto se jím budeme v této práci zabývat.

Při hledání Pythagorejských trojic jsme použili vztah $z^2 - y^2 = (z-y)(z+y)$. Budeme se snažit o něco podobného i v případě $x^3 + y^3$. K tomu se nám budou hodit tzv. *Eisensteinova celá čísla*, což jsou celistvé prvky tělesa $\mathbb{Q}(\zeta_3) = \mathbb{Q}(\sqrt{-3})$. Z předchozích kapitol víme, že minimální polynom prvku $\zeta_3 = \zeta$ je $X^2 + X + 1$, Eisensteinova celá čísla tvoří okruh $\mathbb{Z}[\zeta] = \{a + b\zeta \mid a, b \in \mathbb{Z}\}$ a $\pm 1, \pm\zeta, \pm\zeta^2$ jsou všechny odmocniny z jedné v $\mathbb{Z}[\zeta]$ (přičemž $\zeta^2 = -1 - \zeta$). Klíčovou roli bude hrát prvek $\lambda = 1 - \zeta$. Podle lemmatu 3.15 je $\lambda$ ireducibilní v $\mathbb{Z}[\zeta]$ a $\lambda^2 \parallel 3$. Kdybychom pracovali v obyčejných celých číslech, snažili bychom se zredukováním rovnic modulo 3 obdržet spor s existencí netriviálního řešení Fermatovy rovnice. V oboru $\mathbb{Z}[\zeta]$ tuto roli převezme, jak uvidíme, právě prvek $\lambda$.

Důležité je také explicitně znát normu obecného prvku $\alpha = a + b\zeta$. Ta je podle definice rovna

$$\mathrm{N}(a + b\zeta) = (a + b\zeta)(a + b\zeta^2) = \alpha\overline{\alpha} = a^2 - ab + b^2. \tag{5.1}$$

Snadno se ověří, že norma v tomto případě nabývá pouze nezáporných (celočíselných) hodnot. Tyto poznatky nyní využijeme v důkazu následujícího lemmatu. Symbol $(\lambda)$ v něm znamená hlavní ideál $\mathbb{Z}[\zeta]\lambda$. Pokud nebude řečeno jinak, budeme od této chvíle značit prvky okruhu $\mathbb{Z}[\zeta]$ řeckými písmeny, zatímco obyčejná celá čísla latinkou. Symbol $(\lambda)$ znamená, jak je obvyklé, hlavní ideál $\mathbb{Z}[\zeta]\lambda$.

**Lemma 5.1.**

(1) *Všechny invertibilní prvky v $\mathbb{Z}[\zeta]$ jsou odmocninami z jedné.*

(2) $\mathbb{Z}[\zeta]$ *je Eukleidův obor.*

(3) *Těleso* $\mathbb{Z}[\zeta]/(\lambda)$ *má* 3 *prvky.*

*Důkaz:* (1) Vzhledem k tvrzení 2.5 stačí najít prvky s normou 1. Úpravou vzorce (5.1) se dostáváme k řešení rovnice

$$(2a-b)^2+3b^2=4.$$

Je ihned vidět, že $|b|\leq 1$. Ke každému ze tří možných $b$ vyjdou dvě různá $a$. Každý z těchto 6 prvků je pak nutně odmocninou z jedné.

(2) K zadaným prvkům $\alpha,\beta\in\mathbb{Z}[\zeta]$, $\beta\neq 0$, chceme najít $\gamma,\delta$ tak, že $\alpha=\gamma\beta+\delta$ a $\mathrm{N}(\delta)<\mathrm{N}(\beta)$. Protože $\beta\overline{\beta}\in\mathbb{Z}$, máme

$$\frac{\alpha}{\beta}=\frac{\alpha\overline{\beta}}{\beta\overline{\beta}}=s+t\zeta,\quad s,t\in\mathbb{Q}.$$

Najdeme celá čísla $m,n$ tak, aby $|m-s|\leq 1/2$ i $|n-t|\leq 1/2$, a položíme $\gamma=m+n\zeta$ a $\delta=\alpha-\gamma\beta$. Spočítáme normu:

$$\begin{aligned}\frac{\mathrm{N}(\delta)}{\mathrm{N}(\beta)}=\mathrm{N}\left(\frac{\delta}{\beta}\right)=\mathrm{N}\left(\frac{\alpha}{\beta}-\gamma\right)&=(s-m)^2-(s-m)(t-n)+(t-n)^2\\&\leq\frac{1}{4}+\frac{1}{4}+\frac{1}{4}<1.\end{aligned}$$

(3) Vyjádřeme každé $\alpha\in\mathbb{Z}[\zeta]$ jako $\gamma\lambda+\delta$. Protože $\mathrm{N}(\lambda)=3$, můžeme za reprezentanty tříd faktorokruhu $\mathbb{Z}[\zeta]/(\lambda)$ vzít prvky s normou menší než 3. Podobnou úpravou vzorce (5.1) jako výše zjistíme, že prvek s normou 2 v $\mathbb{Z}[\zeta]$ neexistuje. Prvky s normou 1 už známe. Jak se snadno ověří, platí $1\equiv\zeta\equiv\zeta^2 \pmod{\lambda}$ a $-1\equiv-\zeta\equiv-\zeta^2 \pmod{\lambda}$. Zároveň $1\not\equiv -1 \pmod{\lambda}$. Protože jediný prvek s nulovou normou je 0, dostáváme právě tři třídy reprezentované prvky $0,1,-1$, takže $\mathbb{Z}[\zeta]/(\lambda)\cong\mathbb{F}_3$. ✠

V blížícím se důkazu budeme často pracovat s prvky nedělitelnými $\lambda$. K tomu je vhodné znát jemnější chování těchto prvků.

**Lemma 5.2.** *Nechť* $\theta\in\mathbb{Z}[\zeta]$, $\lambda\nmid\theta$. *Pak* $\theta^3\equiv\pm 1 \pmod{\lambda^4}$.

*Důkaz:* Z předchozího lemmatu víme, že $\theta\equiv\pm 1 \pmod{\lambda}$. Položme $\mu=\pm\theta$ tak, aby $\mu\equiv 1 \pmod{\lambda}$, tedy $\mu=\rho\lambda+1$. S využitím vztahů (5.1) a $1-\zeta^2=(1-\zeta)(1+\zeta)=-\lambda\zeta^2$ dostáváme

$$\begin{aligned}\mu^3-1&=(\mu-1)(\mu-\zeta)(\mu-\zeta^2)=(\rho\lambda)(\rho\lambda+1-\zeta)(\rho\lambda+1-\zeta^2)\\&=\rho\lambda(\rho\lambda+\lambda)(\rho\lambda-\lambda\zeta^2)=\lambda^3\rho(\rho+1)(\rho-\zeta^2)\\&\equiv\lambda^3\rho(\rho+1)(\rho-1)\pmod{\lambda}.\end{aligned}$$

Opět podle předchozího lemmatu musí být jedno z čísel $\rho, \rho+1, \rho-1$ dělitelné $\lambda$, takže platí $\mu^3 - 1 \equiv 0 \pmod{\lambda^4}$. Zpětným dosazením $\theta$ za $\mu$ dostáváme požadovanou kongruenci $\theta^3 \equiv \pm 1 \pmod{\lambda^4}$. ✠

Nyní již přistoupíme ke Gaussovu důkazu neřešitelnosti Fermatovy rovnice 3. stupně, a to dokonce v Eisensteinových celých číslech. Citujeme jej z [2].

**Věta 5.3** (Gauss)**.** *Nechť $\alpha, \beta, \gamma \in \mathbb{Z}[\zeta]$. Pokud platí*

$$\alpha^3 + \beta^3 + \gamma^3 = 0, \tag{5.2}$$

*tak $\alpha\beta\gamma = 0$.*

*Důkaz:* V pokusech o důkaz Velké Fermatovy věty pro obecný exponent $p$ se často rozlišují případy $p \nmid \alpha\beta\gamma$ a $p|\alpha\beta\gamma$. Jak už jsme řekli, v našem případě tuto roli převezme $\lambda = 1 - \zeta$.

I. $\lambda \nmid \alpha\beta\gamma$

Podle předchozího lemmatu tedy platí

$$0 = \alpha^3 + \beta^3 + \gamma^3 \equiv \pm 1 \pm 1 \pm 1 \pmod{\lambda^4},$$

přičemž tento zápis znamená, že může nastat kterákoliv z osmi kombinací znamének. Výsledky jsou nicméně jen čtyři, a to $\pm 1$ nebo $\pm 3$. Případ $\pm 1$ je vyloučen, protože $\lambda^4$ není invertibilní. Jelikož $\lambda^2 \parallel 3$, není ani $\lambda^4 | \pm 3$. Je tedy nemožné, aby $\alpha^3 + \beta^3 + \gamma^3 = 0$ a zároveň $\lambda \nmid \alpha\beta\gamma$.

II. $\lambda | \alpha\beta\gamma$

Nechť $\alpha, \beta, \gamma$ jsou nenulová a přitom splňují (5.2). Z toho vyvodíme spor. Vzhledem k symetrii a homogenitě rovnice (5.2) můžeme bez újmy na obecnosti předpokládat, že $\lambda | \gamma$, $\lambda \nmid \alpha$, $\lambda \nmid \beta$ a $\mathrm{NSD}(\alpha, \beta) = 1$. Máme tedy $\alpha^3 + \beta^3 + \lambda^{3n}\delta^3 = 0$, kde $n \geq 1$ a $\lambda \nmid \delta$. Budeme chtít použít metodu nekonečného sestupu, tj. najít nenulová $\rho, \sigma$ a $\tau$ taková, že $\rho^3 + \sigma^3 + \lambda^{3(n-1)}\tau^3 = 0$, $\lambda$ nedělí $\rho, \sigma, \tau$ a $\mathrm{NSD}(\rho, \sigma) = 1$. Takto přímo se nám to ale bohužel nepovede. Příčina spočívá v tom, že v $\mathbb{Z}[\zeta]$ existují jednotky odlišné od $\pm 1$. Uvažujme proto obecnější rovnici

$$\alpha^3 + \beta^3 + \varepsilon\lambda^{3n}\delta^3 = 0, \tag{5.3}$$

kde $\varepsilon$ je jednotka okruhu $\mathbb{Z}[\zeta]$.

Nejprve znovu použijeme předchozí lemma a dostáváme $\pm 1 \pm 1 \equiv \pm\varepsilon\lambda^{3n} \pmod{\lambda^4}$. Levá strana je rovná buď 2 nebo 0. Protože ale $\lambda \nmid 2$ (stačí porovnat normy obou prvků), musí být nutně $\lambda^4 | \lambda^{3n}$ a tedy $n \geq 2$.

Přepišme rovnici (5.3) do tvaru

$$-\varepsilon\lambda^{3n}\delta^3 = \alpha^3 + \beta^3 = (\alpha + \beta)(\alpha + \beta\zeta)(\alpha + \beta\zeta^2),$$

kde druhá rovnost plyne ze vztahu (5.1). Pro zjednodušení zápisu budeme poslední tři činitele po řadě značit jako $A_1, A_2, A_3$. Prvek $\lambda$ dělí levou stranu rovnice, takže musí dělit i jednoho z nich. Protože $1 \equiv \zeta \equiv \zeta^2 \pmod{\lambda}$, dělí $\lambda$ všechny tři. Navíc $n \geq 2$, takže $\lambda^2$ dělí aspoň jedno $A_i$. Máme ale

$$\begin{aligned} A_1 - A_2 &= (1-\zeta)\beta = \lambda\beta, \\ A_1 - A_3 &= (1-\zeta^2)\beta = -\lambda\beta\zeta^2, \\ A_2 - A_3 &= (\zeta-\zeta^2)\beta = \lambda\beta\zeta. \end{aligned}$$

Protože $\lambda$ nedělí $\beta$, nedělí $\lambda^2$ levé strany předchozích rovností, a tak pouze jedno $A_i$ je násobkem $\lambda^2$. Případným nahrazením $\beta$ v rovnici (5.3) prvkem $\beta\zeta$ nebo $\beta\zeta^2$ můžeme (při zachování platnosti rovnice) docílit toho, že $\lambda^2 | A_1$. Dostáváme tedy

$$\begin{aligned} A_1 &= \lambda^{3n-2} B_1, \\ A_2 &= \lambda B_2, \\ A_3 &= \lambda B_3, \\ -\varepsilon\delta^3 &= B_1 B_2 B_3, \end{aligned}$$

přičemž $\lambda \nmid B_i$ (protože $\lambda \nmid \delta$).

Rádi bychom teď konstatovali, že $B_i$ musí být až na asociovanost třetí mocniny nějakých prvků ze $\mathbb{Z}[\zeta]$. K tomu potřebujeme, aby v našem oboru existoval jednoznačný rozklad na ireducibilní prvky a aby $B_1, B_2, B_3$ byly po dvou nesoudělné. První vlastnost plyne z lemmatu 5.1. Nesoudělnost ukážeme např. pro $B_1, B_2$. U ostatních dvojic se postupuje obdobně.

Kdyby nějaký ireducibilní prvek $\pi$ dělil $B_1$ i $B_2$, bylo by jistě

$$\pi | (A_1/\lambda - A_2/\lambda) = \beta$$

a zároveň

$$\pi | (A_1 + A_2/\lambda - A_1/\lambda) = A_1 - \beta = \alpha.$$

To ale není možné, jelikož jsme předpokládali nesoudělnost $\alpha$ a $\beta$.

Můžeme tedy psát

$$\begin{aligned} B_1 &= e_1 C_1^3, \\ B_2 &= e_2 C_2^3, \\ B_3 &= e_3 C_3^3, \end{aligned}$$

kde $e_i$ jsou jednotky v $\mathbb{Z}[\zeta]$ a $C_i$ po dvou nesoudělná a nedělitelná $\lambda$.

Ze vztahu $\zeta^2 + \zeta + 1 = 0$ nyní dostáváme

$$\zeta^2 A_3 + \zeta A_2 + A_1 = \alpha(\zeta^2 + \zeta + 1) + \beta(\zeta + \zeta^2 + 1) = 0,$$

takže po dosazení za $A_i$

$$\zeta^2 e_3 \lambda C_3^3 + \zeta e_2 \lambda C_2^3 + e_1 \lambda^{3n-2} C_1^3 = 0.$$

Tuto rovnici ještě vydělíme $\lambda$ a najdeme vhodné jednotky $e_4, e_5 \in \mathbb{Z}[\zeta]$ tak, aby platilo

$$C_3^3 + e_4 C_2^3 + e_5 \lambda^{3n-3} C_1^3 = 0. \tag{5.4}$$

Podívejme se na poslední rovnici modulo $\lambda^2$. Díky $n \geq 2$ dostaneme $C_3^3 + e_4 C_2^3 \equiv 0 \pmod{\lambda^2}$. Protože ale $\lambda$ nedělí $C_2$ ani $C_3$, je opět podle předchozího lemmatu

$$\pm 1 \pm e_4 \equiv 0 \pmod{\lambda^2}.$$

Zajímá nás teď, které z šesti jednotek v $\mathbb{Z}[\zeta]$ vyhovují při nějaké kombinaci znamének této kongruenci. Určitě to jsou 1 i $-1$ a tvrdíme, že $\pm\zeta$ ani $\pm\zeta^2$ uvažovaný vztah nesplňují.

$\mathrm{N}(1+\zeta) = 1$, a tedy $1+\zeta$ je jednotka. Pak ovšem nemůže být $\lambda^2 | 1+\zeta$. Neplatí ani $\lambda^2 | 1 - \zeta = \lambda$. Podobně pro $\pm\zeta^2$: $\lambda^2 \nmid 1 + \zeta^2 = -\zeta$ a $\lambda^2 \nmid 1 - \zeta^2 = \lambda(1+\zeta)$. Můžeme tedy rovnici (5.4) napsat jako

$$C_3^3 + (\pm C_2)^3 + e_5 \lambda^{3(n-1)} C_1^3 = 0.$$

Toto už je rovnice stejného typu jako (5.3), přičemž $\lambda$ nedělí $C_1, C_2, C_3$ a zároveň $\mathrm{NSD}(C_3, \pm C_2) = 1$. Dostáváme tedy nekonečný sestup, což vyvrací existenci netriviálního řešení rovnice (5.2). ✠

Již jsme naznačili, že tento Gaussův důkaz obsahuje některé ideje pozdějšího Kummerova důkazu. Které to jsou? Dopředu můžeme prozradit, že kostra důkazu zůstane nezměněna. Při zkoumání Fermatovy rovnice stupně $p$ využijeme vlastností okruhu algebraických celých čísel $p$-tého cyklotomického tělesa, v prvé řadě toho, že $\alpha^p + \beta^p = (\alpha+\beta)\,\mathrm{N}(\alpha+\beta\zeta)$. Bohužel ne všechny postupy jsou beze změny přenositelné.

Zejména obecně neplatí, že by $\mathbb{Z}[\zeta_p]$ byl Gaussův obor. Přitom tato vlastnost byla úhelným kamenem našeho důkazu. Za nevyřčeného předpokladu gaussovskosti $\mathbb{Z}[\zeta_p]$ pro všechna prvočísla dokonce Gabriel Lamé v roce 1847 „dokázal“ Velkou Fermatovu větu v plné obecnosti. Přitom už roku 1844 ukázal Kummer, že $\mathbb{Z}[\zeta_{23}]$ není Gaussův. Tento výsledek Lamému nicméně nebyl znám. Kummer však nalezl způsob, jak nejednoznačnost rozkladu čísel z části napravit. Zavedl nová „ideální čísla“, která byla inspirací Richardu Dedekindovi k definici moderního pojmu ideál. Na jeho počest se obory integrity s jistými vlastnostmi nazývají Dedekindovy a my se jimi budeme zabývat v následující kapitole.

Dalším klíčovým faktem, který neplatí obecně, je existence pouze konečného množství invertibilních prvků. Podle Dirichletovy věty máme už pro případ $p = 5$ nekonečně mnoho jednotek. Tato skutečnost je důvodem, proč Gaussův důkaz nemůžeme použít jako šablonu ani pro další speciální případy, i kdyby v nich (jako třeba právě pro $p = 5$) existovaly jednoznačné rozklady na ireducibilní prvky. Vyrovnat se s tímto problémem bude velmi obtížné. Dokonce tak obtížné, že není v možnostech této práce sledovat důkaz Kummerovy věty o jednotkách v cyklotomických tělesech, která se využívá v závěrečné fázi jeho důkazu Velké Fermatovy věty.

# Kapitola 6

# Dedekindovy obory

Výsledky v této kapitole obsažené jsou pro nás jen odrazovým můstkem k důkazu Velké Fermatovy věty pro regulární prvočísla a nesouvisejí přímo s teorií cyklotomických těles. Proto budeme tvrzení uvádět až na výjimky bez důkazů, zato však s větší mírou obecnosti. Čtenář najde tuto partii i s důkazy podrobně zpracovanou v [9, kapitoly 7 a 8].

## 6.1 Proč je dobré mít ideály?

Začneme příkladem převzatým z [7]: Uvažujme těleso $\mathbb{Q}(\sqrt{-5})$ a označme $R$ množinu všech jeho prvků celistvých nad $\mathbb{Z}$. Dá se ukázat, že $R = \mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\}$. Podívejme se teď, jak se v tomto oboru rozkládá prvek 6. Zřejmě platí

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

Přitom prvky $2, 3, 1 \pm \sqrt{-5}$ jsou ireducibilní v $R$ a žádný prvek z dvojice $2, 3$ není asociovaný s žádným prvkem dvojice $1 + \sqrt{-5}, 1 - \sqrt{-5}$. V oboru $R$ tedy nemáme jednoznačný rozklad na ireducibilní činitele. Se stejným problémem se v případě cyklotomických těles potýkal Kummer. Zavedl však nová „ideální čísla“, s jejichž pomocí se mu nejednoznačnost rozkladů povedlo do jisté míry obejít. Jeho metoda se ukázala být přenositelná i do ostatních číselných těles, a proto ji budeme demonstrovat na výše zmíněném příkladě. Základní idea zde totiž vynikne lépe, než kdybychom pracovali s komplikovaným tělesem $\mathbb{Q}(\zeta_{23})$ (první cyklotomické těleso, jehož celistvé prvky netvoří Gaussův obor). Nebudeme ovšem blíže specifikovat Kummerova ideální čísla, nýbrž rovnou použijeme Dedekindův pojem ideál, který je jejich dnes používanou obdobou. U čtenáře předpokládáme dobrou obeznámenost s tímto pojmem. Připomeneme tak jen definici součtu a součinu ideálů: $I + J = \{a + b \mid a \in I, b \in J\}$, $IJ = \{\sum_{i=1}^{n} a_i b_i \mid a_i \in I, b_i \in J, n \in \mathbb{N}\}$. Přímo z definice se ověří, že platí $I(J + K) = IJ + IK$ a že $I + J$ i $IJ$ jsou také ideály.

Jako motivace k zavedení ideálů nám poslouží příklad, jehož autorem je Dirichlet. Uvažujme množinu $S = \{1, 5, 9, 13, \ldots\}$. Vidíme, že je uzavřena na násobení. Protože však $9 \cdot 49 = 21 \cdot 21$, není v $S$ jednoznačný rozklad na ireducibilní prvky. Tento nedostatek spočívá v tom, že chybí společné faktory čísel $9, 21$ a $49, 21$. Zavedeme proto ideální čísla $(9, 21) = \mathrm{NSD}(9, 21)$ a $(49, 21)$. Pomocí nich přepíšeme předchozí rovnost jako $(9, 21)^2(49, 21)^2 = (9, 21)(49, 21)(9, 21)(49, 21)$. Původní nejednoznačnost byla tedy způsobena jen odlišným spárováním činitelů $(49, 21)$ a $(9, 21)$ na různých stranách rovnice.

Analogicky teď budeme postupovat při odstraňování nejednoznačnosti rozkladu šestky v oboru $R$. Zavedeme ideály $P = (2, 1+\sqrt{-5}), Q = (3, 1+\sqrt{-5}), Q' = (3, 1-\sqrt{-5})$, kde $(a, b)$ značí ideál $Ra+Rb$. Roznásobením člen po členu dostáváme

$$\begin{aligned} P^2 &= (R2 + R(1 + \sqrt{-5}))^2 \\ &= R4 + R2(1 + \sqrt{-5}) + R2(1 + \sqrt{-5}) + R(-4 + 2\sqrt{-5}) \\ &= R2 \cdot (R2 + R(1 + \sqrt{-5}) + R(-2 + \sqrt{-5})) \\ &= (2)(2, 1 + \sqrt{-5}, -2 + \sqrt{-5}). \end{aligned}$$

Druhý ideál v posledním výrazu je roven $(1)$, protože $-2 + (1 + \sqrt{-5}) - (-2 + \sqrt{-5}) = 1$. Máme tedy $P^2 = (2)$ a podobně se ověří, že $QQ' = (3), PQ = (1 + \sqrt{-5}), PQ' = (1 - \sqrt{-5})$. Opět vidíme, že po zavedení ideálů má prvek 6 jednoznačný rozklad $(2, 1 + \sqrt{-5})^2(3, 1 + \sqrt{-5})(3, 1 - \sqrt{-5})$. Všimněme si ještě, že jsme explicitně nepotřebovali ideál $P' = (2, 1 - \sqrt{-5})$. Platí totiž $P = P'$, jak se snadno ověří.

Úvahy výše prováděné je nyní potřeba trochu upřesnit. Předně, pokud pracujeme s ideály, tak ve skutečnosti nerozkládáme prvek 6, ale hlavní ideál (6), který s ním ztotožňujeme. Za druhé musíme vyjasnit, jaké ideály by měly hrát roli již dále nerozložitelných prvků. Inspirujeme-li se celými čísly, dostaneme jako horké kandidáty prvoideály. Jak uvidíme v následující sekci, tato volba skutečně ponese své ovoce.

## 6.2 Základní vlastnosti Dedekindových oborů

Obor integrity $R$ nazveme *Dedekindovým oborem*, pokud každý jeho nenulový ideál lze až na pořadí jednoznačně vyjádřit jako součin prvoideálů. Jak brzy uvidíme, ideály Dedekindova oboru mají mnoho vlastností analogických s celými čísly.

Na libovolném okruhu můžeme zavést relaci dělitelnosti ideálů takto: $I$ dělí $J$, právě když existuje ideál $K$ takový, že $J = IK$. Potom $J$ je obsažen v $I$. V Dedekindových oborech platí i opačná implikace: $I|J \Leftrightarrow J \subseteq I$. V běžných okruzích se definují prvoideály podmínkou: $P \supseteq IJ \Rightarrow P \supseteq I$ nebo $P \supseteq J$. Dedekindovy obory umožňují díky předchozímu tuto ekvivalentní definici: $P$ je prvoideál, pokud platí ($P|IJ \Rightarrow P|I$ nebo $P|J$), což kopíruje definici prvočinitelů v $\mathbb{Z}$.

Uvažujme od této chvíle pevný Dedekindův obor $R$ a ukažme další analogie s celými čísly. Pro každý ideál $I$ oboru $R$ existuje pouze konečně mnoho ideálů, které dělí $I$ – to ovšem plyne přímo z definice. Dále můžeme stejným způsobem jako v $\mathbb{Z}$ definovat nejmenší společný násobek a největší společný dělitel ideálů $I$ a $J$. Potom platí: $\mathrm{nsn}(I,J) = I \cap J$, $\mathrm{NSD}(I,J) = I + J$. Díky této vlastnosti můžeme zformulovat *čínskou větu o zbytcích* pro Dedekindovy obory. O ideálech $I, J$ řekneme, že jsou *nesoudělné*, pokud $I + J = R$.

**Tvrzení 6.1.** *Nechť $P_1, \ldots, P_r$ jsou po dvou nesoudělné (tj. různé) prvoideály oboru $R$, $e_1, \ldots e_r$ přirozená čísla a $J = P_1^{e_1} \cdots P_r^{e_r}$. Pak*

$$R/J = \prod_{i=1}^{r} R/P_i^{e_i}.$$

Verze této věty pro obecný okruh $S$ a ideály $Q_1, \ldots, Q_r$ předpokládá $Q_i + Q_j = S$ a $J = Q_1 \cap \ldots \cap Q_r$, čemuž v oboru $R$ díky výše uvedeným vztahům přesně odpovídá nesoudělnost prvoideálů a fakt, že jejich nejmenší společný násobek je roven jejich součinu.

Podívejme se nyní, jaké je místo Dedekindových oborů mezi jinými obory speciálních vlastností, jmenovitě mezi obory hlavních ideálů a Gaussovými obory. Čtenář si jistě všiml nápadných podobností mezi vlastnostmi oborů hlavních ideálů a Dedekindových oborů. Není tedy překvapivé, že obor hlavních ideálů je i Dedekindovým oborem. Opačná implikace však neplatí. Na druhou stranu máme tuto ekvivalentní podmínku:

**Tvrzení 6.2.** *Dedekindův obor je oborem hlavních ideálů, právě když je Gaussovým oborem.*

Jak jsme již naznačili, obecně neplatí, že okruh celistvých prvků číselného tělesa je Gaussův. Dokážeme však, že vždy je alespoň Dedekindův. Za tím účelem uvedeme tvrzení, které se někdy užívá přímo jako definice Dedekindova oboru.

**Tvrzení 6.3.** *Obor $R$ je Dedekindův, právě když splňuje následující tři podmínky:*

(1) *$R$ je noetherovský.*

(2) *$R$ je celistvě uzavřený.*

(3) *Každý nenulový prvoideál oboru $R$ je maximální.*

Připomínáme, že noetherovskost oboru znamená konečnost každého ostře rostoucího řetězce ideálů, ekvivalentně konečnou generovanost každého ideálu. Dá se však dokonce ukázat, že každý ideál Dedekindova oboru je generován nejvýše dvěma prvky. Díky vlastnostem, které jsme zatím uvedli, můžeme ihned nahlédnout, že Dedekindův obor splňuje podmínku (3). Kdyby totiž pro nějaké $I \subset R$ bylo $P \subset I$, pak $I$ je vlastním dělitelem $P$, a tedy $P$ není prvoideál.

Zvolme nyní $K$ číselné těleso stupně $n$ s okruhem celistvých prvků $A$. Budeme ověřovat jednotlivé body předchozího tvrzení. Vlastnost (2) splňuje $A$ přímo z definice. K důkazu zbylých dvou budeme potřebovat jedno pomocné tvrzení.

**Lemma 6.4.** *Ať $I$ je nenulový ideál okruhu $A$. Pak $I$ má v $A$ konečný index.*

*Důkaz:* Z tvrzení 2.7 plyne, že $A$ je tvaru $\mathbb{Z}b_1 \oplus \cdots \oplus \mathbb{Z}b_n$. Lemma 2.2 nám poskytuje $a \in I \cap \mathbb{Z}, a \neq 0$. Zřejmě platí $Aa = \mathbb{Z}ab_1 \oplus \cdots \oplus \mathbb{Z}ab_n \subseteq I$. Index $Aa$ v $A$ je ale $a^n$. Lemma pak plyne z nerovnosti $|A/I| \leq |A/Aa|$. ✠

**Lemma 6.5.** *Každý nenulový prvoideál okruhu $A$ je maximální.*

*Důkaz:* Zvolme nenulový prvoideál $P$. Pak $A/P$ je obor integrity a podle předchozího lemmatu i konečný. To znamená, že $A/P$ už je těleso, neboli $P$ je maximální.✠

Abychom dokázali vlastnost (1), zavedeme pojem *norma ideálu $I$* jako $\mathrm{N}(I) = |A/I|$. Definice má smysl díky lemmatu 6.4. Vždy bude z kontextu jasné, zda operátor N značí normu prvku či normu ideálu, takže by nemělo docházet k nedorozumnění. Důvodem pro stejný název v obou případech je

**Tvrzení 6.6.** *Pro $0 \neq y \in A$ platí $\mathrm{N}(Ay) = |\mathrm{N}(y)|$.*

Uveďme alespoň pro zajímavost některé základní vlastnosti normy.

Pro prvoideály platí: $\mathrm{N}(P^e) = \mathrm{N}(P)^e$. Z tohoto faktu a z čínské věty o zbytcích je ihned vidět, že pro ideál $I = \prod_{i=1}^{r} P_i^{e_i}$ platí

$$\mathrm{N}(I) = \prod_{i=1}^{r} \mathrm{N}(P_i)^{e_i}. \tag{6.1}$$

Na okruhu $A$ lze také zavést Eulerovu funkci pro nenulové ideály, a to následovně: $\varphi(I) = |\{a + I \in A/I \mid Aa + I = A\}|$. Tato funkce je zobecněním celočíselné Eulerovy funkce a platí pro ní analogické vztahy. Např. $\varphi(IJ) = \varphi(I)\varphi(J)$ pro nesoudělné ideály $I, J$, nebo $\varphi(P) = \mathrm{N}(P) - 1$ pro prvoideál $P$. Dokonce platí i Eulerova věta: pokud $I$ je nenulový ideál a hlavní ideál generovaný prvkem $a \in A$ je nesoudělný s $I$, pak $a^{\varphi(I)} \equiv 1 \pmod{I}$.

My však směřujeme k důkazu noetherovskosti oboru $A$.

**Lemma 6.7.** *Nechť $I, J \subseteq A$ jsou ideály takové, že $I \subset J$. Pak $\mathrm{N}(I) > \mathrm{N}(J)$.*

*Důkaz:* Definujme zobrazení $f\colon A/I \to A/J$ předpisem $f(a + I) = a + J$. Zřejmě je zobrazení korektně definováno a je na. Zvolme $b \in J \setminus I$. Potom $b + I \neq 0$, ale $f(b + I) = b + J = 0$, takže $f$ není prosté. Máme tedy zobrazení mezi konečnými množinami, které je na a není prosté. Takže $|A/I| > |A/J|$. ✠

**Lemma 6.8.** *Okruh $A$ je noetherovský.*

*Důkaz:* Nechť $I_1 \subset I_2 \subset I_3 \cdots$ je nekonečná ostře rostoucí posloupnost ideálů. Podle předchozího lemmatu je $\mathrm{N}(I_1) > \mathrm{N}(I_2) > \mathrm{N}(I_3) > \cdots$. Norma je ale vždy

přirozené číslo, takže dostáváme spor. ✠

Dokázali jsme tedy, že obor $A$ celistvých prvků číselného tělesa $K$ je Dedekindovým oborem. Zároveň jsme v předchozí sekci viděli, že $A$ nemusí být obecně oborem hlavních ideálů. Když toto v případě cyklotomických těles zjistil Kummer, vymyslel způsob, jak měřit „vzdálenost“ $A$ od oboru hlavních ideálů. My jeho postup ukážeme opět obecně.

Podmnožinu $M \neq \{0\}$ tělesa $K$ navzveme *lomeným ideálem* okruhu $A$, pokud existuje nenulové $a \in A$ takové, že $Ma$ je ideál v $A$. Zřejmě každý nenulový ideál $I$ okruhu $A$ je také jeho lomeným ideálem. V takovém případě někdy o $I$ mluvíme jako o *celistvém* ideálu. Analogicky jako pro celistvé ideály definujeme i součin lomených ideálů. Protože $MA = M$ pro každý lomený ideál $M$, máme na množině všech lomených ideálů strukturu komutativního monoidu – budeme jej značit $\mathcal{J}_K$. Pro $M \in \mathcal{J}_K$ definujeme $M^{-1} = \{x \in K \mid Mx \subseteq A\}$. Důvodem k tomuto značení je to, že $M^{-1}M = A$ pro každý lomený ideál $M$. Zároveň $M^{-1}$ je také lomený ideál, takže $\mathcal{J}_K$ tvoří grupu.

**Tvrzení 6.9.** *Ať $M$ je lomený ideál okruhu $A$. Pak $M$ se dá jednoznačně vyjádřit jako $\prod_{i=1}^{r} P_i^{e_i}$, kde $r \geq 0$, $e_i$ jsou nenulová celá čísla a $P_i$ po dvou různé prvoideály. Navíc $M$ je celistvý ideál, právě když $e_i > 0$ pro $i = 1, \ldots, r$.*

Předchozí tvrzení jinými slovy říká, že $\mathcal{J}_K$ je volná Abelova grupa s bází tvořenou všemi prvoideály. Zřejmým způsobem tak můžeme mluvit o lomeném ideálu jako o podílu dvou celistvých ideálů.

Pro $x \in K^*$ nazveme množinu $Ax$ *hlavním lomeným ideálem* okruhu $A$. Připomínáme, že $K$ je podílovým tělesem $A$, takže $Ax$ je skutečně lomený ideál. Pro $a \in A$ nenulové platí $Aa^{-1} = (Aa)^{-1}$. Pokud tedy $x = b/c$, $b, c \in A$, máme $A(b/c) = Ab \cdot (Ac)^{-1}$, neboli hlavní lomené ideály jsou rovny podílům nenulových hlavních celistvých ideálů. Protože nenulové hlavní celistvé ideály tvoří podmonoid multiplikativního monoidu všech celistvých ideálů, tvoří hlavní lomené ideály podgrupu $\mathcal{J}_K$. Budeme ji značit $\mathcal{P}_K$. Můžeme tedy uvažovat *třídovou grupu* $C_K = \mathcal{J}_K/\mathcal{P}_K$. Jednotkovým prvkem této faktorgupy je třída obsahující nevlastní (celistvý) ideál $A$. Následující vlastnost grupy $\mathcal{C}_K$ je klíčová.

**Tvrzení 6.10.** *Grupa $\mathcal{C}_K$ je konečná.*

Počet prvků $\mathcal{C}_K$ značíme $h_K$ a říkáme mu *třídové číslo* tělesa $K$.

Ať $M$ je lomený ideál. Potom $Ma = M \cdot Aa$ je celistvý ideál pro nějaké $a \in A$. Každý lomený ideál je tedy roven podílu celistvého ideálu a hlavního celistvého ideálu. Proto platí

**Tvrzení 6.11.** *Každý lomený ideál je hlavní, tj. $h_K = 1$, právě když $A$ je obor hlavních ideálů.*

Nyní již máme připraveno vše potřebné pro následující kapitolu, která je vyvrcholením této práce.

# Kapitola 7

# Kummerův důkaz

## 7.1 Přípravné práce

V roce 1850 publikoval Kummer důkaz Velké Fermatovy věty pro prvočísla, která splňují následující dvě podmínky:

(i) Pokud $M^p$ je hlavní lomený ideál okruhu $\mathbb{Z}[\zeta_p]$, pak $M$ je také hlavní lomený ideál.
(ii) Nechť $\varepsilon$ je jednotka okruhu $\mathbb{Z}[\zeta_p]$. Pokud $\varepsilon \equiv m \pmod{p}$ pro nějaké $m \in \mathbb{Z}$, pak existuje jednotka $\varepsilon_1 \in \mathbb{Z}[\zeta_p]$ taková, že $\varepsilon = \varepsilon_1^p$.

Kummer později ukázal, že (i) ve skutečnosti implikuje (ii). Zároveň podal přesnou charakterizaci prvočísel, která splňují (i). My v této kapitole detailně provedeme Kummerův důkaz, kromě jednoho dokážeme i všechna pomocná lemmata. Historické podrobnosti týkající se Kummerova postupu a vůbec většiny moderní matematiky spjaté s Velkou Fermatovou větou najde čtenář v [8].

K tomu, abychom předvedli Kummerův důkaz, budeme ještě potřebovat několik lemmat. Tato platí obecně pro jakákoliv prvočísla. Zároveň obnovujeme značení použité většinou již dříve: $p$ je liché prvočíslo, $\zeta$ je primitivní $p$-tá odmocnina z jedné, $\lambda = 1 - \zeta$, $K = \mathbb{Q}(\zeta)$, $A = \mathbb{Z}[\zeta]$ a $U$ je grupa jednotek $A$. Pokud neřekneme jinak, bude opět řecké písmeno představovat prvek z $A$, zatímco latinské značí celé číslo.

První lemma obsahuje různorodé výsledky, které jsou většinou snadným důsledkem definic a tvrzení předchozích kapitol. Myslíme si ale, že je dobré je pro pohodlí čtenáře explicitně zformulovat.

**Lemma 7.1.**

(1) $A/A\lambda \cong \mathbb{F}_p$. *Speciálně* $A\lambda$ *je maximální ideál.*
(2) *Množina* $\mathcal{B} = \{1, \lambda, \lambda^2, \ldots, \lambda^{p-2}\}$ *tvoří celistvou bázi tělesa* $K$.
(3) *Ať* $\alpha \in A, a \in \mathbb{Z}, k \geq 1$. *Pokud* $\alpha \equiv a \pmod{\lambda^k}$, *pak* $\alpha^p \equiv a^p \pmod{\lambda^{p-1+k}}$.
(4) $\alpha^p + \beta^p = \prod_{i=0}^{p-1} \alpha + \zeta^i \beta = (\alpha + \beta)\,\mathrm{N}(\alpha + \zeta\beta)$.

(5) *Ať* $m \in \mathbb{Z}$. *Potom* $p|m \Leftrightarrow \lambda|m$.

*Důkaz:* (1) Dokážeme, že faktorokruh $A/A\lambda$ má $p$ prvků. Podobně jako v důkazu lemmatu 6.4 se ukáže, že index $Ap$ v $A$ je $p^{[K:\mathbb{Q}]} = p^{p-1}$. Lemma 3.15 nám říká, že $Ap = A\lambda^{p-1}$. Nyní stačí použít vztah (6.1): $p^{p-1} = |A/Ap| = \mathrm{N}(Ap) = \mathrm{N}(\lambda)^{p-1} = |A/A\lambda|^{p-1}$.

(2) Množina $\mathcal{B}$ je zřejmě bází tělesa $\mathbb{Q}(\lambda) = K$. Víme, že $\mathcal{Z} = \{1, \zeta, \ldots, \zeta^{p-2}\}$ je celistvou bází $K$. Vzhledem k tvrzení 2.8 stačí ukázat, že $\mathrm{discr}(\mathcal{B}) = \mathrm{discr}(\mathcal{Z})$. Prvky konjugované s $\lambda$ jsou zjevně $1-\zeta, 1-\zeta^2, \ldots, 1-\zeta^{p-1}$, takže ze vztahu (2.6) dostáváme

$$\mathrm{discr}(\mathcal{B}) = \prod_{1\le i<j\le p-1} \big(1-\zeta^i-(1-\zeta^j)\big)^2 = \prod_{1\le i<j\le p-1} (\zeta^j-\zeta^i)^2 = \mathrm{discr}(\mathcal{Z}).$$

(3) $\alpha \equiv a \pmod{\lambda^k}$ znamená, že $\alpha = a + \rho\lambda^k$. Pak $\alpha^p = \sum_{i=0}^{p} \binom{p}{i} a^i \rho^{p-i} \lambda^{k(p-i)}$. Přitom pro $1 \le i \le p-1$ je koeficient $\binom{p}{i}$ dělitelný $p \parallel \lambda^{p-1}$. Zároveň pro $1 \le i \le p-1$ máme $k(p-i)+p-1 \ge p-1+k$ a $k(p-0) \ge p-1+k$. Celkem tedy $\alpha^p \equiv \binom{p}{p} a^p \rho^0 \lambda^0 = a^p \pmod{\lambda^{p-1+k}}$.

(4) Podle lemmatu 3.1 platí $X^p - 1 = \Phi_1(X)\Phi_p(X) = (X-1)\prod_{i=1}^{p-1}(X-\zeta^i)$. První rovnost odsud získáme dosazením $\alpha/-\beta$ za $X$ a vynásobením obou stran $(-\beta)^p$. Druhá rovnost plyne ze vztahu (2.2).

(5) Přímá implikace je jasná. Nechť tedy $\lambda|m$. Pak $m \in A\lambda \cap \mathbb{Z} = \mathbb{Z}p$ podle lemmatu 3.15(3). Tedy $p|m$. ✠

Nechť $\alpha \in A$ je takové, že $\lambda \nmid \alpha$. Podle předchozího lemmatu je $\alpha \equiv m + n\lambda \pmod{\lambda^2}$, přičemž $p \nmid m$. Číslo $\alpha$ nazveme *semiprimární*, pokud $n = 0$, tj. $\alpha \equiv m \pmod{\lambda^2}$. Semiprimární čísla se nám budou hodit v důkazu Kummerovy věty, a proto o nich dokážeme některá jednoduchá tvrzení.

**Lemma 7.2.**

(1) *Ať* $\alpha \equiv m + n\lambda \pmod{\lambda^2}$, *kde* $m, n \in \mathbb{Z}$ *a* $p \nmid m$. *Zvolme* $l \in \mathbb{Z}$ *tak, aby* $lm \equiv n \pmod{p}$. *Pak* $\zeta^l\alpha$ *je semiprimární.*

(2) *Pokud* $\alpha, \beta$ *jsou semiprimární, tak existuje* $l \in \mathbb{Z}$ *takové, že* $l\beta \equiv \alpha \pmod{\lambda^2}$.

*Důkaz:* (1)$\zeta^l = (1-\lambda)^l \equiv 1 - l\lambda \pmod{\lambda^2}$. Díky $lm \equiv n \pmod{p}$ a díky $p \parallel \lambda^{p-1}$ máme

$$\zeta^l\alpha \equiv (1-l\lambda)(m+n\lambda) \equiv m + (n-ml)\lambda \equiv m \pmod{\lambda^2},$$

takže $\zeta^l\alpha$ je semiprimární.

(2) Nechť $\alpha \equiv m \pmod{\lambda^2}, \beta \equiv n \pmod{\lambda^2}$, $p \nmid m, n$. Zvolme $l$ tak, aby $ln \equiv m \pmod{p}$. Potom $l\beta \equiv ln \equiv m \equiv \alpha \pmod{\lambda^2}$. ✠

V důkazu Kummerovy věty budeme stejně jako v případě $p = 3$ rozlišovat, kdy $\lambda|\gamma$ a kdy $\lambda \nmid \gamma$. Pro větší přehlednost důkazu provedeme některé delší výpočty v následujícím lemmatu. Čtenář v něm již může nalézt analogie s výše zmíněným případem. Připomínáme, že jsme v předchozí kapitole dokázali, že $A$ je Dedekindův obor.

**Lemma 7.3.** *Ať $\alpha\beta\gamma \neq 0$ a $\alpha^p + \beta^p + \gamma^p = 0$.*

(1) *Pokud $\lambda\nmid\gamma$, tak existují takové ideály $I, J_0, J_1, \ldots, J_{p-1}$ okruhu $A$, že $A\lambda\nmid J_k$ a $A(\alpha + \zeta^k\beta) = J_k^p I$, $k = 0, 1, \ldots, p-1$.*

(2) *Ať $\alpha^p + \beta^p = \varepsilon\delta^p\lambda^{mp}$, kde $\varepsilon \in U$, $m \geq 1$, $\lambda\nmid\alpha\beta\delta$. Pak $m \geq 2$.*

(3) *Ať $\gamma = \delta\lambda^m$, $m \geq 2$, $\lambda \nmid \alpha\beta\delta$ a $I' = \mathrm{NSD}(A\alpha, A\beta)$. Pak existuje index $j_0$, $0 \leq j_0 \leq p-1$, a ideály $J_0, \ldots, J_{p-1}$ takové, že $A\lambda\nmid J_k$ a*

$$A(\alpha + \zeta^{j_0}\beta) = (A\lambda)^{p(m-1)+1} I' J_{j_0}^p,$$
$$A(\alpha + \zeta^j\beta) = A\lambda \cdot I' J_j^p \qquad \text{pro } j \neq j_0.$$

*Důkaz:* (1) Podle lemmatu 7.1(4) máme

$$-\gamma^p = \alpha^p + \beta^p = \prod_{i=0}^{p-1} (\alpha + \zeta^i\beta).$$

Nejprve spočteme $\mathrm{NSD}(A(\alpha+\zeta^i\beta) \mid i = 0, 1, \ldots, p-1)$. Zvolme libovolně $j, k$, $0 \leq j < k \leq p-1$. Ukážeme, že pokud nějaký ideál $W$ je společným dělitelem $A(\alpha + \zeta^j\beta)$ a $A(\alpha + \zeta^k\beta)$, pak $W$ dělí $A(\alpha + \zeta^i\beta)$ pro všechna $i = 0, \ldots, p-1$.

$W|A(\alpha + \zeta^i\beta)$ znamená $\alpha + \zeta^i\beta \in W$. Platí

$$(\alpha + \zeta^j\beta) - (\alpha + \zeta^k\beta) = \zeta^j(1 - \zeta^{k-j})\beta \in W$$

a podobně

$$(\zeta^j\alpha + \zeta^{k+j}\beta) - (\zeta^k\alpha + \zeta^{k+j}\beta) = \zeta^j(1 - \zeta^{k-j})\alpha \in W.$$

Podle lemmatu 3.15 ale máme $1 - \zeta^{k-j} \parallel 1 - \zeta = \lambda$. Protože $\zeta$ je invertibilní, dostáváme $W|A\lambda \cdot A\beta$, $W|A\lambda \cdot A\alpha$.

$W$ však nedělí $A\lambda$. V opačném případě totiž (protože $A\lambda$ je prvoideál) $W = A\lambda$ dělí $\prod_{i=0}^{p-1} A(\alpha + \beta\zeta^i) = (A\gamma)^p$, což je proti našemu předpokladu. Máme tedy $W|A\alpha$, $W|A\beta$, neboli $\alpha, \beta \in W$. Potom jistě i $\alpha + \zeta^i\beta \in W$ pro každé $i = 0, \ldots, p-1$, neboli $W|A(\alpha + \zeta^i\beta)$.

Dokázali jsme, že $I = \mathrm{NSD}(A(\alpha + \zeta^j\beta), A(\alpha + \zeta^k\beta))$ je i největším společným dělitelem všech $A(\alpha+\zeta^i\beta)$. Proto jsou ideály $A(\alpha+\zeta^i\beta)\cdot I^{-1}$ po dvou nesoudělné a ze vztahu

$$\left(\frac{A\gamma}{I}\right)^p = \prod_{i=0}^{p-1} \frac{A(\alpha + \zeta^i\beta)}{I}$$

a jednoznačné faktorizace ideálů na prvoideály tak dostáváme

$$\frac{A(\alpha+\zeta^i\beta)}{I}=J_i^p$$

pro nějaké ideály $J_i$, $i=0,\dots,p-1$. Navíc $A\lambda$ nedělí žádné $J_i$, protože jinak by $A\lambda$ dělilo $A\gamma$.

(2) Vynásobíme-li $\alpha,\beta$ nějakou $p$-tou odmocninou z jedné, prvky takto obdržené budou opět vyhovovat uvažované rovnici. Protože $\lambda\nmid\alpha\beta$, můžeme podle lemmatu 7.2(1) bez újmy na obecnosti předpokládat, že $\alpha,\beta$ jsou semiprimární. Existují tedy $a,b$ taková, že $\alpha\equiv a \pmod{\lambda^2}$ a $\beta\equiv b \pmod{\lambda^2}$. Použitím lemmatu 7.1(3) dostáváme $\alpha^p\equiv a^p \pmod{\lambda^{p+1}}$ a $\beta^p\equiv b^p \pmod{\lambda^{p+1}}$.

Předpokládejme teď $m=1$. Potom $a^p+b^p=\alpha^p+\beta^p+\mu\lambda^{p+1}=\lambda^p(\varepsilon\delta^p+\mu\lambda)$. Díky $p\parallel\lambda^{p-1}$ tak vidíme, že $p|a^p+b^p$. Na druhou stranu ale $p^2\nmid a^p+b^p$ (protože $\lambda\nmid\delta$). Máme tedy $a^p+b^p=ps$, kde $p\nmid s$. Takže $a^p+b^p=\lambda^{p-1}s$ a podle lemmatu 7.1(5) $\lambda\nmid s$. To je ale spor, protože $\lambda^p|a^p+b^p$. Je tedy $m\geq 2$, jak se mělo dokázat.

(3) Postup je podobný jako v části (1). Proto některé kroky provedeme rychleji.

Platí

$$\delta^p\lambda^{mp}=\prod_{k=0}^{p-1}(\alpha+\beta\zeta^k),$$

takže $\lambda|\alpha+\zeta^j\beta$ pro nějaké $j$. Pro $k\neq j$ máme $\alpha+\zeta^k\beta=(\alpha+\zeta^j\beta)+\beta\zeta^j(\zeta^{k-j}-1)$, přičemž $\zeta^{k-j}-1\parallel\lambda$. $\lambda$ tedy dělí všechna $\alpha+\beta\zeta^k$. Protože $m\geq 2$, existuje index $j_0$, že $\lambda^2|\alpha+\zeta^{j_0}\beta$. Ukážeme, že $\lambda^2$ nedělí už žádná jiná $\alpha+\beta\zeta^k$.

Kdyby tomu tak nebylo, tak pro nějaké $k_0$, $k_0\neq j_0$, platí

$$\lambda^2|(\alpha+\zeta^{j_0}\beta)-(\alpha+\zeta^{k_0}\beta)=\zeta^{j_0}(1-\zeta^{k_0-j_0})\beta.$$

Potom ale $\lambda|\beta$, což je spor s předpokladem. Máme tedy $\lambda^{mp-(p-1)}|\alpha+\zeta^{j_0}\beta$.

Dále $\alpha,\beta\in I'$, takže $\alpha+\zeta^k\beta\in I'$ pro všechna $k=0,\dots,p-1$. Navíc $A\lambda\nmid I'$, protože $\lambda\nmid\alpha,\beta$.

Dohromady dostáváme

$$\begin{aligned}A(\alpha+\zeta^{j_0}\beta)&=(A\lambda)^{p(m-1)+1}I'J'_{j_0},\\ A(\alpha+\zeta^j\beta)&=A\lambda\cdot I'J'_j\qquad\text{pro } j\neq j_0,\end{aligned}$$

přičemž $A\lambda\nmid J'_k$ pro $k=0,\dots,p-1$. Zbývá ukázat, že ideály $J'_k$ jsou po dvou nesoudělné. Potom totiž ze vztahu

$$\left(\frac{A\delta}{I'}\right)^p=\prod_{k=0}^{p-1}J'_k$$

a z jednoznačné faktorizace dostaneme $J'_k=J_k^p$ pro nějaké ideály $J_0,\dots,J_{p-1}$ nedělitelné $A\lambda$.

Pro spor předpokládejme, že nějaký prvoideál $P$ dělí $J'_j$ i $J'_k$, $j < k$. Pak $P \neq A\lambda$, takže $A\lambda \cdot I'P$ dělí oba ideály $A(\alpha + \zeta^j\beta), A(\alpha + \zeta^k\beta)$. Stejným postupem jako výše se ukáže, že $I'P|A\beta$ a $I'P|A\alpha$. Pak ale $I'P|\,\mathrm{NSD}(A\alpha, A\beta) = I'$, což je nemožné. ✠

## 7.2 Velká Fermatova věta pro regulární prvočísla

Nejrpve popíšeme prvočísla, která splňují podmínky (i) a (ii) ze začátku předchozí sekce: liché prvočíslo $p$ nazveme *regulárním*, pokud $p$ nedělí řád grupy $\mathcal{C}_K$ tělesa $K = \mathbb{Q}(\zeta_p)$, neboli $p \nmid h_K$.

Formulujeme teď jedno snadné lemma, které ovšem implicitně obsahuje celou Kummerovu dlouholetou práci na důkazu Velké Fermatovy věty.

**Lemma 7.4.** *Následující dvě podmínky jsou ekvivalentní:*

(1) *$p$ je regulární.*

(2) *Pokud $M^p$ je hlavní lomený ideál okruhu $A = \mathbb{Z}[\zeta_p]$, pak $M$ je také hlavní lomený ideál.*

*Důkaz:* (1) → (2) Pokud $M$ není hlavní, tak jeho řád v grupě $\mathcal{C}_K$ je roven $p$. Tedy $p|h_K$ a $p$ není regulární.

(2) → (1) Nechť $p|h_K$. Protože $\mathcal{C}_K$ je konečná Abelova grupa, existuje v ní prvek řádu $p$, tj. takový lomený ideál $M$, který není hlavní, přičemž $M^p$ už hlavní je. ✠

Až do této chvíle nebylo příliš jasné, jakým způsobem se dají ideály využít v tvrzení, které pojednává pouze o vlastnostech čísel. Předchozí lemma nám však umožňuje tento postup:

Jak jsme viděli v kapitole 5, klíčovým krokem většiny potenciálních důkazů Velké Fermatovy věty je rozklad $\alpha^p + \beta^p$ na po dvou nesoudělné činitele a konstatování, že tyto činitele musí být $p$-tými mocninami. To je ovšem korektní argument jen za předpokladu gaussovskosti oboru, v němž pracujeme. Náš obor $A$ však tuto vlastnost obecně nemá, zato je Dedekindův. V tomto klíčovém kroku důkazu tedy na chvíli přejdeme z řeči čísel do řeči ideálů a díky jednoznačnosti rozkladů získáme faktory $N_i$, které jsou hlavními lomenými ideály a navíc $p$-tými mocninami nějakých lomených ideálů $M_i$. Za přepokladu regulárnosti $p$ pak konstatujeme, že $M_i$ jsou už také hlavní, a to nám umožní vrátit se zpátky k číslům. Poznamenejme, že většinu práce týkající se tohoto kroku jsme již provedli v posledním lemmatu předchozí sekce.

Druhým problémem, se kterým se musíme vyrovnat, jsou invertibilní prvky v $A$. Tento problém řeší *Kummerovo lemma o jednotkách*, které říká, že regulární prvočísla splňují podmínku (ii). Pro důkaz tohoto velmi obtížného lemmatu Kummer vyvinul tzv. $\lambda$-adické metody. Není v možnostech této práce Kummerovo

lemma dokázat. Vyžadovalo by to totiž vybudování takového množství teorie, že by se objem práce dvojnásobně zvětšil. Čtenáře tak aspoň odkazujeme na [9], kde kromě důkazu Kummerova lemmatu najde i veškerou s ním související teorii. Z kapitoly 19 této knihy také s drobnými změnami citujeme důkaz hlavní věty této práce.

**Věta 7.5** (Kummer 1850)**.** *Nechť $p$ je regulární prvočíslo a $\alpha, \beta, \gamma \in A$. Pokud $\alpha^p + \beta^p + \gamma^p = 0$, tak $\alpha\beta\gamma = 0$.*

*Důkaz:* Předpokládejme, že $\alpha, \beta, \gamma$ splňují Fermatovu rovnici stupně $p$ a $\alpha\beta\gamma \neq 0$. Z kapitoly 5 víme, že pak $p \geq 5$.

I. $\lambda \nmid \alpha\beta\gamma$

Nejprve použijeme lemma 7.1(4):

$$-\gamma^p = \alpha^p + \beta^p = \prod_{j=0}^{p-1} (\alpha + \zeta^j \beta).$$

Protože $\lambda \nmid \gamma$, je i $\lambda \nmid \alpha + \zeta^{p-1}\beta$. Podle lemmatu 7.2(1) tedy existuje $k$ takové, že $\zeta^k(\alpha + \zeta^{p-1}\beta)$ je semiprimární. Po vynásobení vhodnou $p$-tou odmocninou z jedné můžeme vzhledem k témuž lemmatu bez újmy na obecnosti předpokládat, že i $\alpha, \beta$ jsou semiprimární. Toto lemma, tentokrát část (2), nám poskytuje $a, b \in \mathbb{Z}$ taková, že

$$\begin{aligned} \alpha &\equiv a\zeta^k(\alpha + \zeta^{p-1}\beta) \pmod{\lambda^2}, \\ \beta &\equiv b\zeta^k(\alpha + \zeta^{p-1}\beta) \pmod{\lambda^2}. \end{aligned} \tag{7.1}$$

Tvrdíme, že $a + b \equiv 1 \pmod{p}$.

Ze vztahů (7.1) dostáváme

$$\alpha + \zeta^{p-1}\beta \equiv (a + \zeta^{p-1}b)\zeta^k(\alpha + \zeta^{p-1}\beta) \pmod{\lambda^2}.$$

Protože $\lambda \nmid \alpha + \zeta^{p-1}\beta$, je $1 \equiv (a + \zeta^{p-1}b)\zeta^k \pmod{\lambda^2}$. Již několikrát jsme ale viděli, že $\zeta^k \equiv \zeta^{p-1} \equiv 1 \pmod{\lambda}$, takže $1 \equiv a + b \pmod{\lambda}$. Lemma 7.1(5) nám pak dává $1 \equiv a + b \pmod{p}$.

Náš další postup spočívá v tom, že budeme postupně vylučovat všechny hodnoty, kterých by $b$ mohlo nabývat, a tím dostaneme kýžený spor. Zřejmě $b \not\equiv 0 \pmod{p}$, protože dosazením do (7.1) bychom dostali $\beta \equiv 0 \pmod{\lambda}$, o čemž předpokládáme, že nenastane. Nemůže být ani $b \equiv 1 \pmod{p}$. Pak totiž $a \equiv 0 \pmod{p}$ a $\alpha \equiv 0 \pmod{\lambda}$.

Za předpokladu $b \not\equiv 0, 1 \pmod{p}$ teď zbývají dva případy: $2b \equiv 1 \pmod{p}$ a $2b \not\equiv 1 \pmod{p}$. Níže dokážeme, že druhý případ nenastává, takže je už jen poslední možnost $2b \equiv 1 \pmod{p}$. Potom díky $a + b \equiv 1 \pmod{p}$ dostáváme $a \equiv b \pmod{p}$, a tedy $\alpha \equiv \beta \pmod{\lambda}$. Vzhledem k symetrii $\alpha, \beta, \gamma$ ve výchozí

rovnici bychom stejnými úvahami došli k závěru, že $\alpha \equiv \gamma \pmod{\lambda}$. Použitím lemmatu 7.1(1) a Malé Fermatovy věty tak dostáváme

$$0 = \alpha^p + \beta^p + \gamma^p \equiv \alpha + \beta + \gamma \equiv 3\alpha \pmod{\lambda}.$$

Protože, ale $p \neq 3$, musí být $\lambda | \alpha$, což je spor. Zbývá tedy vyloučit případ $2b \not\equiv 1 \pmod{p}$.

Podle lemmatu 7.3(1) je $A(\alpha+\zeta^j\beta) = J_j^p I$, přičemž $A\lambda \nmid J_j$. Potom pro všechna $j = 0, 1, \ldots, p-1$ platí

$$A\left(\frac{\alpha+\zeta^j\beta}{\alpha+\zeta^{p-1}\beta}\right) = \frac{A(\alpha+\zeta^j\beta)}{A(\alpha+\zeta^{p-1}\beta)} = \frac{J_j^p I}{J_{p-1}^p I} = \left(\frac{J_j}{J_{p-1}}\right)^p. \tag{7.2}$$

$(J_j/J_{p-1})^p$ je tedy hlavní lomený ideál, a tak podle lemmatu 7.4 je i $(J_j/J_{p-1})$ hlavním lomeným ideálem

$$\frac{J_j}{J_{p-1}} = A\left(\frac{\mu_j}{n_j}\right), \qquad \mu_j \in A, \quad 0 \neq n_j \in \mathbb{Z} \quad \text{(viz tvrzení 2.3)}.$$

Tato rovnost se dá ekvivalentně napsat jako

$$J_j \cdot An_j = J_{p-1} \cdot A\mu_j.$$

Protože $A\lambda \nmid J_j, J_{p-1}$, pro všechna $e > 0$ platí: $A\lambda^e | A\mu_j \Leftrightarrow A\lambda^e | An_j$. Po případném vydělení $\lambda^e$ tedy můžeme předpokládat $\lambda \nmid \mu_j, n_j$.

Tímto skončila naše exkurze do světa ideálů. Napišme teď rovnost (7.2) v číslech:

$$\frac{\alpha+\zeta^j\beta}{\alpha+\zeta^{p-1}\beta} = \omega_j\left(\frac{\mu_j}{n_j}\right)^p, \qquad \omega_j \in U.$$

Podle tvrzení 3.19 existují $\varepsilon_j \in U \cap \mathbb{R}$ a $c_j \in \mathbb{Z}$ taková, že $\zeta^{-k}\omega_j = \varepsilon_j\zeta^{c_j}$. Pak platí

$$n_j^p(\alpha+\zeta^j\beta) = \varepsilon_j\zeta^{c_j}\zeta^k(\alpha+\zeta^{p-1}\beta)\mu_j^p.$$

Položme

$$\alpha' = \frac{\alpha}{\zeta^k(\alpha+\zeta^{p-1}\beta)}, \qquad \beta' = \frac{\beta}{\zeta^k(\alpha+\zeta^{p-1}\beta)}.(\alpha', \beta' \in K)$$

Potom $n_j^p(\alpha'+\zeta^j\beta') = \varepsilon_j\zeta^{c_j}\mu_j^p \in A$. Podle lemmatu 7.1(2) existuje $m_j \in \mathbb{Z}$ takové, že $\mu_j \equiv m_j \pmod{\lambda}$. Podle části (3) téhož lemmatu je $\mu_j^p \equiv m_j^p \pmod{\lambda^p}$. Dostáváme tak

$$n_j^p(\alpha'+\zeta^j\beta') \equiv \varepsilon_j\zeta^{c_j}m_j^p \pmod{\lambda^p}.$$

Využijeme toho, že $\varepsilon_j \in \mathbb{R}$ a $\overline{\lambda} = 1 - \zeta^{-1} \parallel \lambda$, a aplikujeme na předchozí rovnici komplexní sdružování:

$$n_j^p(\overline{\alpha'}+\zeta^{-j}\overline{\beta'}) \equiv \varepsilon_j\zeta^{-c_j}m_j^p \pmod{\lambda^p}.$$

Tyto dvě rovnice teď spojíme dohromady

$$\zeta^{-c_j} n_j^p(\alpha' + \zeta^j \beta') \equiv \varepsilon_j m_j^p \equiv \zeta^{c_j} n_j^p(\overline{\alpha'} + \zeta^{-j}\overline{\beta'}) \pmod{\lambda^p}.$$

Protože $\lambda \nmid n_j$, můžeme s $n_j$ dělit:

$$\alpha' + \zeta^j \beta' \equiv \zeta^{2c_j}(\overline{\alpha'} + \zeta^{-j}\overline{\beta'}) \pmod{\lambda^p}. \tag{7.3}$$

Z definice $\alpha', \beta'$, ze vztahů (7.1) a z $\lambda \nmid \alpha + \zeta^{p-1}\beta$ plyne $\alpha' \equiv a \pmod{\lambda^2}, \beta' \equiv b \pmod{\lambda^2}$. Dosazením do (7.3) získáváme $a + \zeta^j b \equiv \zeta^{2c_j}(a + \zeta^{-j} b) \pmod{\lambda^2}$. Pro $l \in \mathbb{Z}$ ale máme $\zeta^l = (1-\lambda)^l \equiv 1 - l\lambda \pmod{\lambda^2}$, takže

$$a + b - jb\lambda \equiv (1 - 2c_j\lambda)(a + b + jb\lambda) \pmod{\lambda^2}.$$

Upravujme tento vztah pomocí výše dokázané kongruence $a + b \equiv 1 \pmod{p}$:

$$\begin{gathered} 2c_j\lambda \equiv 2jb\lambda \pmod{\lambda^2} \\ c_j \equiv jb \pmod{\lambda}. \end{gathered}$$

Obě strany poslední kongruence jsou celočíselné, takže

$$c_j \equiv jb \pmod{p} \qquad \text{pro všechna } j = 0, 1, \ldots, p-1. \tag{7.4}$$

Následuje lehce triková část důkazu, ve které již vyloučíme poslední možnost $b \not\equiv 0, 1 \pmod{p}$, $2b \not\equiv 1 \pmod{p}$, což bude spor.

Protože $p \geq 5$, můžeme s využitím (7.4) pro $j = 0, 1, 2, 3$ explicitně napsat rovnice (7.3):

$$\begin{array}{ccccccccc} \alpha' & + & \beta' & - & \overline{\alpha'} & - & \overline{\beta'} & = & \rho_0\lambda^p, \\ \alpha' & + & \zeta\beta' & - & \zeta^{2b}\overline{\alpha'} & - & \zeta^{2b-1}\overline{\beta'} & = & \rho_1\lambda^p, \\ \alpha' & + & \zeta^2\beta' & - & \zeta^{4b}\overline{\alpha'} & - & \zeta^{4b-2}\overline{\beta'} & = & \rho_2\lambda^p, \\ \alpha' & + & \zeta^3\beta' & - & \zeta^{6b}\overline{\alpha'} & - & \zeta^{6b-3}\overline{\beta'} & = & \rho_3\lambda^p. \end{array}$$

Koeficienty této soustavy lineárních rovnic s neznámými $\alpha', \beta', \overline{\alpha'}, \overline{\beta'}$ napíšeme do matice $M$. Několikanásobným rozvojem podle sloupců a řádků spočteme

$$\det(M) = (1-\zeta)(1-\zeta^{2b})(1-\zeta^{2b-1})(\zeta - \zeta^{2b})(\zeta - \zeta^{2b-1})(\zeta^{2b} - \zeta^{2b-1}).$$

Podle Cramerova pravidla máme

$$\alpha' = \frac{\det(M_1)}{\det(M)},$$

kde $M_1$ je matice vzniklá nahrazením prvního sloupce matice $M$ sloupcem

$$(\rho_0\lambda^p, \rho_1\lambda^p, \rho_2\lambda^p, \rho_3\lambda^p)^T,$$

a proto $\lambda^p | \det(M_1)$. Ale $\lambda \nmid \alpha'$, takže nutně $\lambda^p | \det(M)$. Protože předpokládáme $b \not\equiv 0, 1 \pmod p$, $2b \not\equiv 1 \pmod p$, jsou všechny faktory v $\det(M)$ asociovány s $\lambda$, a tedy $\det(M) \parallel \lambda^6$. Ovšem $\lambda^p | \lambda^6$ je nemožné pro $p \geq 7$. Zbývá tedy probrat případ $p = 5$.

Podle lemmatu 7.1(1) je $A/A\lambda \cong \mathbb{F}_5$. Protože $\lambda \nmid \alpha\beta\gamma$, máme $\alpha, \beta, \gamma \equiv \pm 1, \pm 2 \pmod \lambda$ a $\alpha^5, \beta^5, \gamma^5 \equiv \pm 1, \pm 32 \pmod{\lambda^5}$. Potom

$$0 = \alpha^5 + \beta^5 + \gamma^5 \equiv \pm 1, \pm 3, \pm 30, \pm 32, \pm 34, \pm 63, \pm 65, \pm 96 \pmod{\lambda^5}.$$

Protože $\lambda^5 \parallel 5\lambda$ a $\mathrm{N}(\lambda) = 5$, jsou tyto kongruence nesplnitelné.

II. $\lambda | \alpha\beta\gamma$

Předpokládejme bez újmy na obecnosti , že $\lambda | \gamma$, $\lambda \nmid \alpha$, $\lambda \nmid \beta$. Potom pro nějaké $\delta$, $\lambda \nmid \delta$, a $m \geq 1$ platí $\alpha^p + \beta^p = -\delta^p \lambda^{pm}$. Máme tedy vztah

$$\alpha^p + \beta^p = \varepsilon \delta^p \lambda^{pm}, \tag{7.5}$$

kde $\varepsilon \in U$. Protože $\lambda \nmid \alpha\beta\delta$, je podle lemmatu 7.3(2) $m \geq 2$. Stejně jako v případě $p = 3$ budeme chtít dosáhnout nekonečného sestupu vzhledem k $m$ a tím i sporu s existencí zadaných $\alpha, \beta, \gamma$.

Lemma 7.3(3) nám poskytuje jisté $j_0$. Nahrazením $\beta$ za $\zeta^{j_0}\beta$ a případnou změnou značení můžeme dosáhnout toho, že

$$\begin{aligned} A(\alpha + \beta) &= (A\lambda)^{p(m-1)+1} I' J_0^p, \\ A(\alpha + \zeta^j \beta) &= A\lambda \cdot I' J_j^p, \qquad j = 1, \ldots, p-1, \end{aligned}$$

přičemž $A\lambda \nmid J_0 J_1 \cdots J_{p-1}$. Potom je

$$A\left(\frac{\alpha + \zeta^j \beta}{\alpha + \beta}\right) = (A\lambda)^{-p(m-1)} \cdot \left(\frac{J_j}{J_0}\right)^p \quad \text{pro všechna } j = 1, \ldots, p-1. \tag{7.6}$$

Vidíme, že $(J_j/J_0)^p$ je hlavní lomený ideál. Protože $p$ je regulární, je i $J_j/J_0$ hlavní lomený ideál

$$\frac{J_j}{J_0} = A\left(\frac{\mu_j}{n_j}\right), \qquad \mu_j \in A, \quad 0 \neq n_j \in \mathbb{Z}, \quad \lambda \nmid \mu_j, n_j.$$

Existují tedy jednotky $\varepsilon_1, \varepsilon_2$ takové, že vztah (7.6) může být pro $j = 1, 2$ přepsán takto:

$$\begin{aligned} (\alpha + \zeta\beta)\lambda^{p(m-1)} &= \varepsilon_1(\alpha + \beta)\left(\frac{\mu_1}{n_1}\right)^p, \\ (\alpha + \zeta^2\beta)\lambda^{p(m-1)} &= \varepsilon_2(\alpha + \beta)\left(\frac{\mu_2}{n_2}\right)^p. \end{aligned}$$

Nyní odečteme druhou rovnici od $1+\zeta$-násobku první:

$$\zeta(\alpha+\beta)\lambda^{p(m-1)} = (\alpha+\beta)\left(\varepsilon_1(1+\zeta)\left(\frac{\mu_1}{n_1}\right)^p - \varepsilon_2\left(\frac{\mu_2}{n_2}\right)^p\right).$$

Tento vztah ještě upravíme na tvar

$$\frac{\zeta}{\varepsilon_1(1+\zeta)}\lambda^{p(m-1)}(n_1n_2)^p = (\mu_1n_2)^p - \frac{(\mu_2n_1)^p\varepsilon_2}{\varepsilon_1(1+\zeta)}.$$

Podle lemmatu 7.1(4) je $\mathrm{N}(1+\zeta) = (1+1)/(1+1) = 1$, takže $1+\zeta$ je invertibilní. Po substituci $\alpha' = \mu_1n_2$, $\beta' = \mu_2n_1$, $\delta' = n_1n_2$ nakonec dostáváme

$$(\alpha')^p + \varepsilon'(\beta')^p = \varepsilon''(\delta')^p\lambda^{p(m-1)}, \qquad \varepsilon', \varepsilon'' \in U.$$

Protože $m \geq 2$, $\lambda^p$ dělí $(\alpha')^p+\varepsilon'(\beta')^p$. Zároveň $\lambda \nmid \beta' = \mu_2n_1$, takže $A\lambda+A\beta' = A$ a pro nějaké $\kappa$ je $\kappa\beta' \equiv 1 \pmod{\lambda}$. Potom i $\kappa^p(\beta')^p \equiv 1 \pmod{\lambda^p}$, a proto $(\kappa\alpha')^p + \varepsilon' \equiv 0 \pmod{\lambda^p}$. Existuje tedy $\rho$ takové, že $\varepsilon' \equiv \rho^p \pmod{\lambda^p}$.

Dále podle lemmatu 7.1 je $\rho \equiv r \pmod{\lambda}$ pro nějaké $r \in \mathbb{Z}$ a $\varepsilon' \equiv \rho^p \equiv r^p \pmod{\lambda^p}$. Díky této kongruenci a regularitě $p$ jsou splněny předpoklady Kummerovy podmínky (ii), takže existuje $\varepsilon'_1 \in U$ takové, že $\varepsilon' = (\varepsilon'_1)^p$. Celkem tedy máme rovnici

$$(\alpha')^p + (\varepsilon'_1\beta')^p = \varepsilon''(\delta')^p\lambda^{p(m-1)},$$

která je stejného typu jako (7.5), ale s $m-1$ místo $m$. Tímto dostáváme požadovaný spor. ✠

## 7.3 Závěrečné poznámky

V souvislosti s Kummerovou větou je přirozené si položit otázky: Existují vůbec regulární prvočísla? Pokud ano, která to jsou? Je jich nekonečně mnoho? Nejsou všechna prvočísla už regulární?—Odpovědi na tyto otázky budou obsahem poslední části této práce. Teorie, která umožňuje zkoumat regularitu prvočísel, je však poměrně obtížná. Na této základní úrovni nám tak stejně jako v případě Kummerova lemmatu o jednotkách nezbývá, než uvádět tvrzení bez důkazů. Čtenáře opět odkazujeme na [9], kde kromě vyložené teorie najde i daleko víc výsledků týkajících se regulárních prvočísel.

Připomínáme, že prvočíslo $p$ je regulární, právě když nedělí řád $h_p$ třídové grupy $p$-tého cyklotomického tělesa $\mathbb{Q}(\zeta_p)$. Speciálně $p$ je regulární, pokud $h_p = 1$, neboli $\mathbb{Z}[\zeta_p]$ je obor hlavních ideálů. Podle tvrzení 6.2 tak Velká Fermatova věta platí pro všechny $\mathbb{Z}[\zeta_p]$, které jsou Gaussovými obory.

Prověřovat regularitu prvočísel se zdá být velmi jednoduché – stačí prostě spočítat $h_p$. Touto cestou se zpočátku vydal i Kummer. Jenže brzy bylo zřejmé, že s rostoucím $p$ se úměrně zvyšuje i obtížnost výpočtu $h_p$. Její příčinu se teď

pokusíme alespoň nastínit. K tomu potřebujeme znát ještě trochu teorie, která je sice mimo rámec této práce, na druhou stranu tak bude vidět, jakými cestami se dostává analýza do algebraické teorie čísel.

Do této chvíle jsme poznali dva základní invarianty číselných těles: diskriminant a třídové číslo. Dalším invariantem je tzv. regulátor. Tento pojem úzce souvisí s Dirichletovou větou o jednotce (viz veta 3.20, přebíráme i příslušné značení). Její verze pro cyklotomická tělesa jinými slovy říká, že existují jednotky nekonečného řádu $u_1, \dots, u_r$ takové, že každá jednotka $u$ okruhu $\mathbb{Z}[\zeta_p]$ se dá jednoznačně napsat jako $u = (-\zeta_p)^{e_0} u_1^{e_1} \cdots u_r^{e_r}$, kde $0 \leq e_0 < 2p$ a $e_1, \dots, e_r \in \mathbb{Z}$. Protože všechny konjugace $\zeta_p$ jsou ryze komplexní, je číslo $r$ (hodnost grupy jednotek) rovno $r_2 - 1 = (p-1)/2 - 1 = (p-3)/2$. Množina $\{u_1, \dots, u_r\}$ se nazývá *fundamentální systém jednotek* okruhu $\mathbb{Z}[\zeta_p]$.

Ať $\sigma_1, \dots, \sigma_{p-1}$ jsou prvky Galoisovy grupy tělesa $\mathbb{Q}(\zeta_p)$. Uspořádejme je tak, aby $\overline{\sigma_j(\zeta_p)} = \sigma_{r_2+j}(\zeta_p)$ pro $j = 1, 2, \dots, r_2 = (p-1)/2$. Pišme $\sigma_i(x) = x^{(i)}$ a uvažme matici

$$L = \begin{pmatrix} \log|u_1^{(1)}| & \log|u_1^{(2)}| & \cdots & \log|u_1^{(r)}| \\ \log|u_2^{(1)}| & \log|u_2^{(2)}| & \cdots & \log|u_2^{(r)}| \\ \vdots & \vdots & \ddots & \vdots \\ \log|u_r^{(1)}| & \log|u_r^{(2)}| & \cdots & \log|u_r^{(r)}| \end{pmatrix},$$

kde log značí přirozený logaritmus. Ačkoliv fundamentální systém jednotek není určen jednoznačně, dá se ukázat, že pokud pro jiný systém sestrojíme tímto způsobem matici $L_1$, bude vždy $|\det(L)| = |\det(L_1)|$. Číslo $R = |\det(L)|$ pak nazýváme *regulátor* tělesa $\mathbb{Q}(\zeta_p)$. K tomu, abychom jej spočetli, musíme nalézt nějaký fundamentální systém jednotek, což se obecně jeví jako krajně obtížný problém.

Souvislost regulátoru a třídového čísla nám objasní *Dedekindova zeta funkce*, kterou definujeme pro libovolné číselné těleso $K$ jako

$$\zeta_K(s) = \sum_{I \in \mathcal{I}} \frac{1}{\mathrm{N}(I)^s},$$

kde $\mathcal{I}$ značí množinu všech nenulových ideálů okruhu $\mathbb{Z}_K$. Řada na pravé straně konverguje absolutně a stejnoměrně na intervalu $[1+\delta, \infty)$ pro každé $\delta > 0$, takže $\zeta_K(s)$ je spojitou funkcí definovanou na $(1, \infty)$. Speciálně pokud $K = \mathbb{Q}$, je $\mathbb{Z}_K = \mathbb{Z}$ obor hlavních ideálů a podle tvrzení 6.6 máme $\mathrm{N}(\mathbb{Z}n) = |\mathrm{N}(n)| = n$ pro všechna $n \in \mathbb{Z}$. Pro racionální čísla tedy dostáváme

$$\zeta_{\mathbb{Q}}(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}.$$

Funkce $\zeta(s) = \zeta_{\mathbb{Q}}(s)$ se nazývá *Riemannova zeta funkce*.

A nyní již k slíbené souvislosti regulátoru a třídového čísla tělesa $K = \mathbb{Q}(\zeta_p)$. Platí

$$\lim_{s\to 1+}(s-1)\zeta_K(s) = h_p \cdot \frac{2^{(p-3)/2}\pi^{(p-1)/2}R}{p^{p/2}}.$$

Z tohoto vztahu bychom již teoreticky (a s pokročilejší teorií i prakticky) uměli spočítat součin $Rh_p$. Velmi zhruba řečeno tak obtížnost výpočtu $h_p$ spočívá právě v obtížnosti výpočtu regulátoru. Musíme se tedy vzdát myšlenky na přímý výpočet třídového čísla a raději se poohlédnout po jiných postupech.

Důležitým Kummerovým zjištěním v tomto směru bylo, že $h_p$ je dělitelné třídovým číslem $h_p^+$ tělesa $\mathbb{Q}(\zeta_p + \zeta_p^{-1}) = \mathbb{Q}(\zeta_p) \cap \mathbb{R}$. Kummer zároveň dokázal, že $h_p^+$ je rovno indexu $|U^+ : V|$, kde $U^+$ je grupa jednotek $\mathbb{Q}(\zeta_p + \zeta_p^{-1})$ a $V$ je volná Abelova grupa generovaná kruhovými jednotkami (viz kap. 3.5). Opět tedy vidíme, že invertibilní prvky hrají v cyklotomických tělesech důležitou roli.

Označme nyní $h_p^-$ podíl $h_p/h_p^+$. Kummer nakonec dospěl k tomuto překvapivému výsledku:

**Tvrzení 7.6.** *$p$ dělí $h_p \Leftrightarrow p$ dělí $h_p^-$.*

A tak začal zkoumat aritmetické vlastnosti čísla $h_p^-$. Aby bylo vidět, s jakými obtížemi se musel potýkat, uveďme pro zajímavost vzorec pro výpočet tohoto tzv. *přidruženého třídového čísla*:

$$h_p^- = |\gamma|/(2p)^{t-1},$$

kde

$$t = \frac{p-1}{2}, \quad \gamma = G(\eta)G(\eta^3)\cdots G(\eta^{p-2}), \quad G(X) = \sum_{j=0}^{p-2} g_j X^j, \quad g_j = g^j \bmod p,$$

a konečně $g$ je primitivní prvek grupy $\mathbb{Z}_p^*$ a $\eta$ primitivní $(p-1)$-tá odmocnina z jedné.

Kummer však dovedl z těchto vztahů dostat ještě jinou ekvivalentní podmínku regulárnosti, související tentokrát s tzv. Bernoulliovými čísly. Po Jakobu Bernoullim tato čísla znovu objevil Euler v souvislosti s následující formální mocninnou řadou:

$$\frac{e^X - 1}{X} = 1 + \frac{1}{2!}X + \frac{1}{3!}X^2 + \frac{1}{4!}X^3 + \cdots.$$

Protože konstatní člen je 1, má tato řada inverzi

$$\frac{X}{e^X - 1} = 1 + \frac{B_1}{1!}X + \frac{B_2}{2!}X^2 + \frac{B_3}{3!}X^3 + \cdots.$$

Číslům $B_i \in \mathbb{Q}$ říkáme *Bernoulliova čísla*. Dá se jednoduše ukázat, že $B_{2k+1} = 0$ pro $k \geq 1$. Stejně tak se dá dokázat spousta rekurentních formulí a jiných

vztahů, které Bernoulliova čísla splňují. Zmiňme alespoň jejich důležitou souvislost s Riemannovou zeta funkcí. Pro $k \geq 1$ platí

$$B_{2k} = (-1)^{k-1} \frac{2(2k)!}{(2\pi)^{2k}} \zeta(2k). \tag{7.7}$$

A nyní již ke Kummerovu hlavnímu výsledku. Pokud $a, b, c \in \mathbb{Z}$, $\mathrm{NSD}(b, c) = 1$, řekneme, že $a$ dělí $b/c$, jestliže $a|b$.

**Tvrzení 7.7.** *$p$ dělí $h_p^-$ (tj. $p$ není regulární), právě když $p$ dělí alespoň jedno z čísel $B_2, B_4, \ldots, B_{p-3}$.*

Ačkoliv čitatel Bernoulliových čísel roste celkem rychle, je tato podmínka již použitelná k ověřování regularity. Navíc platí: jmenovatel čísla $B_{2k}$ je součinem všech prvočísel takových, že $p - 1|2k$. Můžeme tedy k výpočtu využít i vztah (7.7). Nejprve za pomoci této metody a pro větší prvočísla pak použitím ještě mocnějších nástrojů došel Kummer po celoživotním počítání k těmto výsledkům:

$$p \leq 163 \text{ není regulární prvočíslo} \iff p = 37, 59, 67, 101, 103, 131, 149, 157.$$

Přehlednou Kummerovu tabulku rozkladů faktoru $h_p^-$ na prvočísla najde čtenář v [8, str.130–131]. Z ní je patrné, že pro $p \leq 163$ je $h_p^- = 1$, právě když $p \leq 19$. Navíc počínaje 23 až do 163 je růst $h_p$ monotónní. Tato fakta vedla matematiky ve 20. století k formulování hypotéz, které se nakonec ukázaly být pravdivé:

**Tvrzení 7.8.**

(1) *$h_p = 1$ (neboli $\mathbb{Z}[\zeta_p]$ je obor hlavních ideálů) $\Leftrightarrow p \leq 19$.*

(2) *Existuje $p_0$ takové, že funkce $h^-(p) = h_p^-$ je ryze rostoucí pro $p \geq p_0$.*

Poznamejme, že domněnka $p_0 = 19$ zatím nebyla potvrzena.

V této souvislosti zmiňme některé nedávné výsledky týkající se oborů $\mathbb{Z}[\zeta_m]$ pro libovolná $m$, přičemž nás budou zajímat ty, které jsou obory hlavních ideálů. Připomeňme, že podle tvrzení 3.9 stačí uvažovat $m \not\equiv 2 \pmod 4$. Montgomery a Masley v [6] ukázali, že $\mathbb{Z}[\zeta_m]$ je obor hlavních ideálů právě pro 30 konkrétních hodnot $m$. O desítce těchto oborů se už za Kummerových dob vědělo, že jsou Eukleidovy. Ve své práci [3] pak Harper dokázal (mimo jiné), že dokonce všech 30 už je Eukleidovými obory. Jak ukazuje následující věta, která s Harperovou prací přímo souvisí, toto vůbec není náhoda. Čtenáře odkazujeme na [4].

**Věta 7.9** (Harper, Murty 2004)**.** *Ať $K$ je Galoisovo rozšíření $\mathbb{Q}$ a ať hodnost $r$ grupy jednotek $U_K$ je větší než 3. Pak obor $\mathbb{Z}_K$ je Eukleidův, právě když je oborem hlavních ideálů.*

Na závěr se pokusme odpovědět na otázky, které jsme vyslovili na začátku sekce. Odkážeme-li se znovu na Kummerovu tabulku čísel $h_p^-$, můžeme konstatovat, že regulární stejně jako neregulární čísla existují. Zároveň se těch regulárních

jeví být poměrně víc. Za pomoci výpočetní techniky se ukazuje, že hustota regulárních prvočísel mezi všemi prvočísly je asi $0,61$. Přesto se ale dodnes neumí ani dokázat, že regulárních prvočísel je nekonečně mnoho, ani podat nějakou jejich explicitní charakterizaci. Na druhou stranu důkaz nekonečnosti množiny neregulárních prvočísel není nijak obtížný a plyne z vlastností Bernoulliových čísel. Kummer se po svém důkazu zabýval i neregulárními prvočísly a odvodil podmínky, za kterých Velká Fermatova věta platí i pro ně. Do dnešní doby se bohužel nikomu nepodařilo dojít Kummerovými postupy až k jejímu úplnému vyřešení, ačkoliv byla tato věta v roce 1995 jinými metodami dokázána Wilesem v plné obecnosti.

Zmínkou o důkazu Velké Fermatovy věty symbolicky končí naše exkurze do teorie číselných a zejména cyklotomických těles. Snažili jsme se předvést klasické výsledky 19. století, které, ač vyvinuty primárně pro řešení této nejslavnější matematické věty, přežily svou dobu a staly se základem algebraické teorie čísel. Jak je vidět z poslední sekce práce, cyklotomickými tělesy se matematici zabývají až do dnešních dob. Ačkoliv praktická užitečnost Velké Fermatovy věty je pravděpodobně malá a ačkoliv již byla dokázána, jistě by stálo za to ji Kummerovým postupem dokázat znovu. Její téměř 400 letá historie totiž ukazuje, že při jejím dokazování bylo vždy vyvinuto spoustu zajímavé a elegantní matematiky.

# Literatura


[1] Drápal A.: *Komutativní okruhy*, skripta (2006), dostupné na `http://www.karlin.mff.cuni.cz/~drapal/komalg.ps`

[2] Esmonde J., Murty M. Ram: *Problems in Algebraic Number Theory*, Springer-Verlag, New York, 1999, 17–19.

[3] Harper M.: $\mathbb{Z}[\sqrt{14}]$ *is Euclidean*, Canad. J. Math. **56** (2004), 55–70.

[4] Harper M., Murty M. Ram: *Euclidean rings of algebraic integers*, Canad. J. Math. **56** (2004), 71–76.

[5] Jensen Chr.U.: *Cyclotomic fields and applications*, skripta (2009), dostupné na `http://www.math.ku.dk/~olsson/manus/alg3-2009/ek4-2009.pdf`

[6] Masley J.M., Montgomery H.L.: *Cyclotomic fields with unique factorization*, J. Reine Angew. Math. **216/7** (1976), 248–256.

[7] Milne J.S.: *Algebraic Number Theory*, (2009), dostupné na `http://www.jmilne.org/math/CourseNotes/ANT.pdf`, 2–4.

[8] Ribenboim P.: *13 Lectures on Fermat's Last Theorem*, Springer-Verlag, New York, 1979.

[9] Ribenboim P.: *Classical Theory of Algebraic Numbers*, Springer-Verlag, New York, 2001.