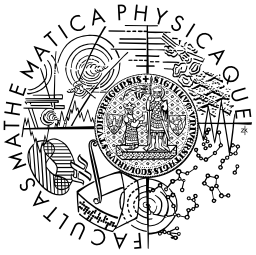

MATEMATICKO-FYZIKÁLNÍ FAKULTA
Univerzita Karlova

BAKALÁŘSKÁ PRÁCE

Žaneta Lipertová

Nejednoznačné rozklady v číselných tělesech

Katedra algebry

Vedoucí bakalářské práce: doc. Mgr. Vítězslav Kala, Ph.D.

Studijní program: Obecná matematika

Studijní obor: Obecná matematika

Praha 2024

Prohlašuji, že jsem tuto bakalářskou práci vypracovala samostatně a výhradně s použitím citovaných pramenů, literatury a dalších odborných zdrojů. Tato práce nebyla využita k získání jiného nebo stejného titulu.

Beru na vědomí, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., autorského zákona v platném znění, zejména skutečnost, že Univerzita Karlova má právo na uzavření licenční smlouvy o užití této práce jako školního díla podle §60 odst. 1 autorského zákona.

V ..... dne ....

Podpis autora

Ráda bych poděkovala mému vedoucímu doc. Mgr. Vítězslavu Kalovi, Ph.D., za cenné rady, trpělivost, ochotu a čas mně věnovaný při psaní této bakalářské práce. Také bych ráda poděkovala Jáchymu Miervovi za pomoc při mém počátečním souboji s LaTeXem.

Název práce: Nejednoznačné rozklady v číselných tělesech

Autor: Žaneta Lipertová

Katedra: Katedra algebry

Vedoucí bakalářské práce: doc. Mgr. Vítězslav Kala, Ph.D., Katedra algebry

Abstrakt: Hlavním cílem práce je zkoumat ireducibilní rozklady v oborech celistvých prvků číselných těles. Ke zkoumání těchto rozkladů je velmi nápomocný jednoznačný rozklad ideálů na prvoideály. Ireducibilní rozklady nějakého prvku x totiž jistým způsobem korespondují s rozkladem na prvoideály hlavního ideálu generovaného tímto prvkem x. Také je definováno třídové číslo a podrobněji se práce zabývá obory s třídovým číslem 2 a 3. V oborech s těmito třídovými čísly práce charakterizuje podobu ireducibilních prvků a zabývá se ireducibilními rozklady, které nejsou jednoznačné. Je dokázána Carlitzova věta, která dává úplnou charakterizaci oborů s třídovým číslem nejvýše 2. Poté práce rozšiřuje některé charakterizační vlastnosti i pro obory s třídovým číslem 3. Nakonec je ukázána cesta k nalezení všech ireducibilních rozkladů čísla 126 v oboru celistvých prvků $\mathbb{Z}\left[\frac{1+\sqrt{-23}}{2}\right]$.

Klíčová slova: číselný okruh; prvoideál; třídové číslo; ireducibilní rozklad

Title: Non-unique factorization in number fields

Author: Žaneta Lipertová

Department: Department of Algebra

Supervisor: doc. Mgr. Vítězslav Kala, Ph.D., Department of Algebra

Abstract: The thesis is studying irreducible factorization in rings of integers of an algebraic number fields. To study factorization, the unique factorization of ideals into prime ideals is extremely useful. The irreducible factorization of an element x in a way corresponds with factorization of principal ideal, generated by x, into prime ideals. The class number is defined and the thesis is focusing on rings with class numbers 2 and 3. In rings with those class numbers the thesis characterizes irreducible elements and irreducible factorization, which is not unique. The Carlitz theorem, which fully characterizes rings with class number at most 2, is proved. Then the thesis extends some characteristic properties for rings with class number 3. At the end there is demonstrated searching for all irreducible factorizations of the number 126 in algebraic number ring $\mathbb{Z}\left[\frac{1+\sqrt{-23}}{2}\right]$.

Keywords: algebraic number ring; prime ideal; class number; irreducible factorization

Obsah

Úvod

Základní věta aritmetiky, jejíž název zní důležitě, tvrdí, že přirozená čísla mají jednoznačný součin na prvočísla. Celá čísla potom mají jednoznačný součin na „prvočísla“ až na pořadí a asociovanost, tj. vynásobení -1. To, že tyto rozklady jsou jednoznačné, není vůbec samozřejmé a ne ve všech okruzích to platí. Tato zásadní vlastnost rozkladů se využívá především v teorii čísel při řešení diofantických rovnic, je proto užitečné rozklady zkoumat. Když už nemůžeme dostat rozklad jednoznačný, je dobré se zajímat o to, jak moc nejednoznačný vůbec může být, či pokud vůbec existuje (což také není samozřejmé a neplatí to obecně, tím se však zabývat nebudeme). V různých okruzích jich může být různý počet či mohou nabývat různých délek.

Tato bakalářská práce pojednává o nejednoznačných rozkladech na ireducibilní prvky v číselných tělesech a jejich okruzích celistvých prvků. Je to téma z algebraické teorie čísel, je tedy řešeno pomocí abstraktní algebry a klíčovou roli hraje ideál a jeho rozklad na prvoideály (základní věta teorie ideálů 3).

Následuje krátký přehled obsahu celé práce.

V kapitole 1 jsou uvedeny základní definice nutné k pochopení celé práce. V první sekci 1.1 je většina známých definic pouze připomenuta. V druhé sekci 1.2 je uvedena definice normy prvku a ideálu a základní vlastnosti těchto norem. Poslední sekce 1.3 zavádí pojmy týkající se oborů a ireducibilních rozkladů v nich. Jsou to atomický, pologaussovský a gaussovský obor (definice 10), které jsou důležité ve třetí kapitole 3.

Kapitola 2 je zakončena klíčovou definicí třídového čísla 18. Tomu předchází zavedení lomených ideálů v sekci 2.1 a dokázání některých jejich vlastností. Většina vlastností je převzata z [4], některé důkazy jsou však vlastním přínosem. V sekci 2.2 o třídovém čísle je poté uvedena dokonce druhá definice třídového čísla a je podán vlastní důkaz známého tvrzení o tom, že jsou ekvivalentní (věta 21).

Kapitola 3 se zabývá jak charakteristikou samotných okruhů s třídovým číslem 2 a 3 (Carlitzova věta 29 pro třídové číslo 2, jíž je věnována sekce 3.2), tak charakteristikou ireducibilních prvků a rozkladů v číselných okruzích s třídovým číslem 2 (sekce 3.1) a 3 (sekce 3.3). Většina tvrzení i důkazů z prvních dvou sekcí je převzata z [2]. V tomto článku se však vůbec neřeší případ třídového čísla 3. Největším vlastním přínosem je zobecnění těchto tvrzení pro případy s třídovým číslem 3 (důsledek 30, tvrzení 31) v sekci Třídové číslo 3 (3.3). Dalším vlastním přínosem je také kombinatorické počítání počtu ireducibilních rozkladů prvků za předpokladu, že v rozkladu hlavního ideálu jsou všechny nehlavní prvoideály různé. Toto je opět spočteno pro případy třídového čísla 2 i 3 (tvrzení 27 a 32).

Poslední kapitola 4 ukazuje aplikaci předchozích výsledků. Zabývá se konkrétními rozklady hlavních ideálů na prvoideály a tvorbou ireducibilních rozkladů v číselném okruhu $\mathbb{Z}\left[\frac{1+\sqrt{-23}}{2}\right]$. Po prvních třech sekcích, kde se postupně budují potřebné znalosti, je kapitola zakončena spočtením všech ireducibilních rozkladů čísla 126 v tomto okruhu (tvrzení 42). Protože je teorie poněkud složitější a nestačí pouze tvrzení uvedená v této práci, využívá proto několik pomocných vět z [5].

1. Základní definice

V první kapitole si zopakujeme klíčové definice a vztahy nezbytné k porozumění celé práce.

1.1 Připomenutí

Vůbec klíčovým pojmem k celé práci je pojem ideálu, proto připomeneme jeho definici. Ať R značí komutativní okruh. V celé práci budeme uvažovat pouze komutativní okruhy. Pak *ideál* je čtveřice $(I, +, -, 0)$, značí se obvykle pouze I, která je uzavřená na sčítání. Splňuje navíc podmínku, že pro všechna $r \in R, x \in I : rx = xr \in I$. Množinu všech nenulových ideálů v R značíme $\mathcal{I}(R)$.

Pro dvě množiny $I, J \subset R$ definujeme jejich součin jako

$$IJ = \left\{ \sum_{i=1}^{n} a_i b_i \;\middle|\; a_i \in I, b_i \in J, n \in \mathbb{N} \right\}.$$

Dále si připomeneme, že *hlavní ideál* v okruhu R je ideál generovaný jedním prvkem, to jest ideál tvaru $xR, x \in R$. Budeme jej značit (x). Řekneme, že R je *obor hlavních ideálů*, pokud v R nejsou jiné než hlavní ideály. *Prvoideálem* nazveme ideál P okruhu R, který není nulový ani roven celému R, a splňuje následující podmínku:

$$\forall I, J \subset R : I \cdot J \subset P \implies I \subset P \text{ nebo } J \subset P.$$

Mějme podokruh W okruhu R, tedy W je podmnožina R, která je uzavřená na sčítání i násobení a obsahuje nulový prvek. Řekneme, že $r \in R$ je *algebraický*, pokud existuje libovolný polynom $f(x) \in W[x]$ takový, že $f(r) = 0$. Prvek $r \in R$ nazveme *celistvý* nad W, pokud je to kořen nějakého *monického polynomu* v $W[x]$. To jest pokud existuje polynom $g(x) \in W[x]$ s vedoucím koeficientem 1, splňující $g(r) = 0$. *Minimálním polynomem* algebraického prvku $r \in R$ nad W rozumíme nerozložitelný monický polynom $m_{r,W}$ z $W[x]$, jehož kořenem je r.

Nechť r je prvek okruhu R. Řekneme, že r je *invertibilní*, pokud v okruhu existuje jeho inverzní prvek. Množinu všech invertibilních prvků okruhu R budeme značit $R^\times$. O dvou prvcích $a, b \in R$ řekneme, že jsou *asociované*, pokud existuje invertibilní prvek $u \in R^\times$ takový, že platí $au = b$. Prvek r je *ireducibilní*, pokud není invertibilní a nelze zapsat jako součin dvou neinvertibilních prvků. *Ireducibilní rozklad* r je rozklad r na součin ireducibilních prvků.

Dále se bude hodit připomenout pojem rozšíření těles. Mějme těleso T. Potom jeho *rozšíření* definujeme jako těleso $U \supset T$ takové, že T je podtělesem U, tedy že je uzavřené na všechny operace v tělese. *Stupeň* tohoto rozšíření je dimenze U jakožto vektorového prostoru nad T. Rozšíření nazveme *konečné*, je-li stupeň rozšíření konečný.

Nacházíme se v pozici, kdy už můžeme definovat další klíčový pojem, a to číselný obor. Těleso K nazveme *číselným tělesem*, pokud je to rozšíření $\mathbb{Q}$ konečného stupně. Potom množinu všech prvků K, jež jsou celistvé nad $\mathbb{Z}$, nazveme *číselným oborem* a budeme jej značit $\mathcal{O}_K$. Po celý zbytek práce budeme $\mathcal{O}_K$ rozumět právě takto definovaný číselný obor a K bude vždy značit číselné těleso.

Přestože je $\mathcal{O}_K$ obor, je konvence o něm mluvit jako o (algebraickém) číselném okruhu, nebo okruhu celistvých prvků, proto se toho v práci budeme držet a nadále budeme $\mathcal{O}_K$ nazývat *číselným okruhem*. V následujícím tvrzení si ukážeme vztah mezi K a $\mathcal{O}_K$.

Tvrzení 1. *Pro všechna $\mu \in K$ existuje $\nu \in \mathcal{O}_K$ a $n \in \mathbb{N}$ takové, že $\mu = \frac{\nu}{n}$.*

Důkaz. Vezměme $\mu \in K$ a označme jeho minimální polynom $m_\mu(x) = \sum_{i=1}^{m} a_i x^i$, kde $m \in \mathbb{N}$. Platí $m_\mu(x) \in \mathbb{Q}[x]$. Bez újmy na obecnosti předpokládejme, že $a_m > 0$ (pro nulový polynom rovnost zřejmě platí, stačí položit $\nu = 0$). Označme l nejmenší společný násobek jmenovatelů koeficientů polynomu $m_\mu(x)$. Poté platí $l \cdot m_\mu(x) \in \mathbb{Z}[x]$, tento polynom je navíc primitivní, to jest největší společný dělitel všech koeficientů je roven jedné. Vynásobením l-násobku $m_\mu(\mu)$ prvkem $(l \cdot a_m)^{m-1}$ dostaneme rovnost

$$(la_m\mu)^m + (la_m)^{m-1} la_{m-1}\mu^{m-1} + \cdots + (la_m)^{m-1} la_0 = 0.$$

Nyní stačí položit $n = l \cdot a_m$. Platí $n \in \mathbb{N}$ a $m_{n\mu}(n\mu) = 0$. Minimální polynom $m_{n\mu}(x) \in \mathbb{Z}[x]$ je navíc monický, jelikož vedoucí koeficient je 1. Dostáváme, že $n\mu$ je v $\mathcal{O}_K$, tudíž existuje nějaké $\nu \in \mathcal{O}_K$ takové, že platí $n\mu = \nu$. □

Důsledek 2. *K je podílové těleso $\mathcal{O}_K$.*

Následující tvrzení je jedna ze základních vět teorie ideálů, nebudeme ji však dokazovat.

Věta 3 (Základní věta teorie ideálů, [2, str. 2])**.** *Nechť I je ideál v $\mathcal{O}_K$. Potom existuje jeho jednoznačný rozklad (až na pořadí) na součin ne nutně různých prvoideálů $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_n \in \mathcal{I}(\mathcal{O}_K), n \in \mathbb{N}$.*

Základní věta teorie ideálů nám říká, že na ideály v $\mathcal{I}(\mathcal{O}_K)$ můžeme nahlížet podobně jako na prvky v $\mathcal{O}_K$. Můžeme uvažovat jejich rozklady na prvoideály, podobně jako v okruhu hledáme ireducibilní rozklady prvků, navíc ale máme zaručenou jednoznačnost tohoto rozkladu, což v obecných okruzích není samozřejmostí.

Na závěr si uvedeme následující tvrzení, abychom znali nějaké příklady číselných okruhů. Tvrzení nebudeme dokazovat, je známé a dá se najít například v [5, věta 4.3]. Předem ještě připomeňme, že celé číslo z nazveme *nečtvercové*, pokud není rovno 0, 1, a zároveň není dělitelné druhou mocninou žádného přirozeného čísla větší než 1.

Tvrzení 4. *Nechť $D \in \mathbb{Z}$, D je nečtvercové a $K = \mathbb{Q}\left[\sqrt{D}\right]$. Potom K je číselné těleso a jeho číselný okruh má následující tvar:*

$$\mathcal{O}_K = \begin{cases} \mathbb{Z}\left[\sqrt{D}\right] = \left\{a + b\sqrt{D} \;\middle|\; a, b \in \mathbb{Z}\right\}, & \text{pokud } D \equiv 2, 3 \pmod 4; \\ \mathbb{Z}\left[\frac{1+\sqrt{D}}{2}\right] = \left\{a + b\frac{1+\sqrt{D}}{2} \;\middle|\; a, b \in \mathbb{Z}\right\}, & \text{pokud } D \equiv 1 \pmod 4. \end{cases}$$

1.2 Norma

Definice 5. Nechť K je číselné těleso. Potom zobrazení $\sigma\colon K \hookrightarrow \mathbb{C}$ nazveme vnořením (anglicky embedding) K do $\mathbb{C}$, pokud platí následující:

1. $\forall a, b \in K\colon \sigma(a+b) = \sigma(a) + \sigma(b);\ \sigma(ab) = \sigma(a)\sigma(b)$;
2. σ je prosté.

Tedy σ je prostý okruhový homomorfismus.

Definice 6. Nechť K je číselné těleso a $x \in K$. Definujeme normu prvku x jako

$$\mathcal{N}_{K/\mathbb{Q}}(x) = \prod \sigma_i(x),$$

kde násobíme přes všechna různá vnoření σ_i K do $\mathbb{C}$.

Poznámka. Pokud bude jasné, nad jakým číselným tělesem K pracujeme, budeme někdy místo $\mathcal{N}_{K/\mathbb{Q}}(x)$ psát pouze $\mathcal{N}(x)$.

Shrňme si některé vlastnosti normy do následujícího lemmatu.

Lemma 7 (Vlastnosti normy)**.** *Nechť K je číselné těleso. Potom o normě platí následující:*

1. *norma je multiplikativní, tj. pro $a, b \in K$ platí*

$$\mathcal{N}_{K/\mathbb{Q}}(ab) = \mathcal{N}_{K/\mathbb{Q}}(a) \cdot \mathcal{N}_{K/\mathbb{Q}}(b);$$

2. *$\forall x \in K\colon \mathcal{N}_{K/\mathbb{Q}}(x) \in \mathbb{Q}$;*
3. *je-li $x \in \mathcal{O}_K$, pak dokonce $\mathcal{N}_{K/\mathbb{Q}}(x) \in \mathbb{Z}$.*

Důkaz. 1. Plyne přímo z definice normy.

2. Lze najít v [7, Corollary 1, str. 15].
3. Lze najít v [7, Corollary 2, str. 16]. □

Specificky se podíváme, pro pozdější využití, jak norma vypadá, pokud je rozšíření K kvadratické, to jest stupně 2. Kvadratické rozšíření je tvaru $K = \mathbb{Q}\left[\sqrt{D}\right]$, kde D je nečtvercové číslo, kladné či záporné. Potom existují pouze 2 různá vnoření. Všechny prvky K jsou tvaru $a + b\sqrt{D}, a, b \in \mathbb{Q}$, tudíž vnoření je popsáno pouze tím, kam se zobrazí $\sqrt{D}$. Jednotka se musí vždy poslat na jednotku. Máme pouze dvě možnosti, kam $\sqrt{D}$ zobrazit, aby stále šlo o vnoření, a to jsou možnosti $\sqrt{D} \mapsto \sqrt{D}$ a $\sqrt{D} \mapsto -\sqrt{D}$. Mějme libovolný prvek $a+b\sqrt{D} \in \mathbb{Q}\left[\sqrt{D}\right]$, jeho norma je tvaru:

$$\mathcal{N}_{\mathbb{Q}[\sqrt{D}]/\mathbb{Q}}\left(a + b\sqrt{D}\right) = \left(a + b\sqrt{D}\right)\left(a - b\sqrt{D}\right) = a^2 - Db^2.$$

Lemma 8 ([5, tvrzení 4.4])**.** *Nechť $\mathcal{O}_K$ je okruh celistvých prvků. Potom $\varepsilon \in \mathcal{O}_K^\times \iff \mathcal{N}(\varepsilon) = \pm 1$.*

Důkaz. $\Rightarrow$ Je-li ε invertibilní, pak existuje $\iota \in \mathcal{O}_K^\times$ splňující $\varepsilon\iota = 1$. Pro normy platí $\mathcal{N}(\varepsilon\iota) = \mathcal{N}(1) = 1$. Protože je pro prvky $\mathcal{O}_K$ norma celé číslo, je nutně $\mathcal{N}(\varepsilon) = \pm 1$.

$\Leftarrow$ Z předpokladů platí $\mathcal{N}(\varepsilon) = \prod \sigma_i(\varepsilon) = \pm 1$, kde násobíme přes všechna různá vnoření σ_i z K do $\mathbb{C}$. Označme si triviální vnoření, které zachovává všechny prvky, jako σ_1 a pišme:

$$\mathcal{N}(\varepsilon) = \sigma_1(\varepsilon) \prod_{i \neq 1} \sigma_i(\varepsilon),$$

tj. triviální vnoření ze součinu vynechme. Poté platí

$$\sigma_1(\varepsilon) \prod_{i \neq 1} \sigma_i(\varepsilon) = \varepsilon \prod_{i \neq 1} \sigma_i(\varepsilon) = \pm 1.$$

Označme $P = \prod_{i \neq 1} \sigma_i(\varepsilon)$ a přepišme rovnost $\varepsilon P = \pm 1$ jako $P = \pm \varepsilon^{-1}$. Chceme ukázat, že P je prvkem $\mathcal{O}_K$. Protože je K těleso a $\varepsilon \in K$, je také $P \in K$. Dokážeme, že každé $\sigma_i(\varepsilon)$ je celistvé nad $\mathbb{Z}$, načež bude i P celistvé. Ať $i \neq 1$ dáno, ukážeme, že $\sigma_i(\varepsilon)$ je kořenem monického polynomu $m_{\varepsilon,\mathbb{Z}}$. Pišme $m_{\varepsilon,\mathbb{Z}} = \sum_{j=1}^{n} a_j x^j, n \in \mathbb{N}$. Díky tomu, že je vnoření okruhový homomorfismus, který nutně zachovává jednotku, platí:

$$\sum_{j=1}^{n} a_j \varepsilon^j = 0 \iff \sigma_i\left(\sum_{j=1}^{n} a_j \varepsilon^j\right) = \sigma_i(0) \iff$$
$$\iff \sum_{j=1}^{n} \sigma_i(a_j)\sigma_i(\varepsilon^j) = 0 \iff \sum_{j=1}^{n} a_j \sigma_i(\varepsilon^j) = 0.$$

Pro všechna i je tedy $\sigma_i(\varepsilon)$ celistvý prvek nad $\mathbb{Z}$, tedy jak jsme chtěli, je $P \in \mathcal{O}_K$ a prvek ε je invertibilní s inverzním prvkem $\pm P$. □

Pojem normy prvku se dá převést na normu ideálu. Obecná definice normy ideálu se dá zadefinovat snáze a konkrétněji pro číselné okruhy $\mathcal{O}_K$ takové, že K je kvadratické rozšíření. Normu ideálu budeme potřebovat v poslední kapitole, ale bude nám stačit pouze pro kvadratická rozšíření. Víc ji potřebovat nebudeme, proto ji zadefinujeme pouze takto konkrétně.

Definice 9. Nechť $K = \mathbb{Q}\left[\sqrt{D}\right]$, kde D je nečtvercové. Označme

$$I^* = \left\{a - b\sqrt{D} \;\middle|\; a + b\sqrt{D} \in I, a, b \in \mathbb{Q}\right\}.$$

Definujeme normu ideálu $I \in \mathcal{I}(\mathcal{O}_K)$ jako celé číslo $\mathcal{N}_{K/\mathbb{Q}}(I)$ takové, že $II^* = \left(\mathcal{N}_{K/\mathbb{Q}}(I)\right)$.

Norma ideálu je dobře definovaná dle [5, tvrzení 4.5 a 4.11].

Poznámka. Stejně jako u normy prvku, pokud bude jasné, nad jakým tělesem K pracujeme, budeme někdy místo $\mathcal{N}_{K/\mathbb{Q}}(I)$ psát pouze $\mathcal{N}(I)$.

Pozorování. Norma ideálu je multiplikativní, tj. pro ideály I, J v $\mathcal{O}_K$ platí: $\mathcal{N}_{K/\mathbb{Q}}(IJ) = \mathcal{N}_{K/\mathbb{Q}}(I) \cdot \mathcal{N}_{K/\mathbb{Q}}(J)$.

Důkaz.

$$\mathcal{N}(IJ) = IJ(IJ)^* = IJI^*J^* = II^*JJ^* = \mathcal{N}(I) \cdot \mathcal{N}(J),$$

kde využíváme komutativitu okruhu $\mathcal{O}_K$. □

1.3 Gaussovské a pologaussovské obory

V této sekci si zavedeme pojmy atomického, pologaussovského a gaussovského oboru. Všechny obory souvisejí s rozkladem neinvertibilních prvků na ireducibilní rozklad a platí mezi nimi jisté inkluze.

Definice 10. Obor R nazveme *atomickým*, pokud v něm pro každý neinvertibilní nenulový prvek existuje jeho rozklad na ireducibilní činitele. Řekneme, že R je *pologaussovský*, pokud je atomický, a navíc kdykoli pro ireducibilní prvky $\upsilon_1, \ldots, \upsilon_n, \omega_1, \ldots, \omega_m \in R$ platí $\upsilon_1 \cdots \upsilon_n = \omega_1 \ldots \omega_m$, pak $m = n$, kde $m, n \in \mathbb{N}$. R je *gaussovský*, pokud v něm pro každý neinvertibilní nenulový prvek existuje jeho **jednoznačný** ireducibilní rozklad (až na asociovanost a pořadí činitelů).

Poznámka. V angličtině tyto obory nazýváme poněkud příznačnějšími pojmy, které více popisují jejich podstatu, a to po řadě atomic domain, half-factorial domain (HFD), unique factorization domain (UFD).

Pozorování. Platí následující vztahy: obor R je gaussovský $\Rightarrow$ R je pologaussovský $\Rightarrow$ R je atomický.

Příklad. Jeden z nejznámějších oborů, jenž není gaussovský, je obor $\mathbb{Z}\left[\sqrt{-5}\right]$ a následující rozklad: $6 = 2 \cdot 3 = (1 - \sqrt{-5})(1 + \sqrt{-5})$.

Uvedeme příklad toho, jak zkonstruovat obor, který je pologaussovský, ale není gaussovský. Jako výsledek pak obdržíme dva obory, které budou pologaussovské. Budeme vycházet z [3, Example 3].

Příklad. Mějme libovolné těleso T a jeho podtěleso S. Definujeme $R = S + xT[x]$. Z [1, Theorem 2.9] dostáváme, že ireducibilní prvky v R jsou právě jednoho z následujících dvou tvarů:

1. tx, kde $t \in T$;
2. $s(1+xf(x))$, kde $s \in S, f(x) \in T[x]$ a navíc $1+xf(x)$ je v $T[x]$ ireducibilní.

Z tohoto plyne, že počet prvků v ireducibilním rozkladu nenulového neinvertibilního prvku $g(x) \in R$ je stejný jako počet prvků jeho ireducibilního rozkladu v $T[x]$. Protože je T těleso, je také triviálně gaussovské, neboť podmínka ireducibilních rozkladů je triviálně splněna. Vypůjčíme si tvrzení z [5, věta 1.18], které nám říká, že je-li obor V gaussovský, pak je také obor $V[x]$ gaussovský. Tedy $T[x]$ je gaussovský. Odsud již plyne, že všechny ireducibilní rozklady každého prvku mají stejnou délku. Ergo R je pologaussovský.

Abychom ukázali, že výsledný obor R opravdu nemusí být gaussovský, zvolme dva následující příklady pologaussovských oborů:

1. Položme $T = \mathbb{C}, S = \mathbb{R}$. Pak v $R = \mathbb{R} + x\mathbb{C}[x]$ platí $x^2 = x \cdot x = (ix)(-ix)$.
2. Položme $T = \mathbb{R}, S = \mathbb{Q}$. Pak v $R = \mathbb{Q} + x\mathbb{R}[x]$ platí $x^2 = x \cdot x = \left(\sqrt{37}x\right)\left(\frac{1}{\sqrt{37}}x\right)$.

Na závěr první kapitoly uvedeme následující tvrzení, bez něhož by celá práce postrádala smysl. Jelikož se v práci budeme zabývat rozklady v číselných okruzích, potřebujeme vědět, že vůbec existují, a tudíž dává smysl je studovat.

Tvrzení 11. *Algebraický číselný okruh $\mathcal{O}_K$ je atomický obor.*

Důkaz. Sporem ať $\mathcal{O}_K$ není atomický obor. Označme si

$$X = \{x \in \mathcal{O}_K \setminus \{0\} \mid x \text{ není invertibilní a nemá ireducibilní rozklad}\}.$$

Zvolme $x_0 \in X$ takové, že $|\mathcal{N}(x_0)|$ je nejmenší možná. Jelikož norma je vždy celé číslo (lemma o vlastnostech normy 7), platí $\forall x \in \mathcal{O}_K \colon |\mathcal{N}(x)| \in \mathbb{N} \cup \{0\}$, takže x_0 s nejmenší normou v absolutní hodnotě existuje. Nemusí být jednoznačné, ale to nepožadujeme, zvolíme ho libovolně. x_0 není ireducibilní (jinak by samo bylo vlastním ireducibilním rozkladem), pak z definice existují neinvertibilní $x_1, x_2 \in \mathcal{O}_K$ taková, že $x_0 = x_1 \cdot x_2$. Pokud by obě měla ireducibilní rozklad, pak x by také mělo ireducibilní rozklad, tvořený jejich součinem. Bez újmy na obecnosti ať x_1 nemá ireducibilní rozklad. Pak však $x_1 \in X$, a zároveň $1 < |\mathcal{N}(x_1)| < |\mathcal{N}(x_0)|$, což je spor s výběrem x jakožto prvku s nejmenší absolutní normou. □

2. Třídové číslo

2.1 Lomený ideál

V této sekci si zadefinujeme pojem lomený ideál, pomocí kterého později definujeme *třídové číslo*. Jednoduše řečeno si lze lomené ideály představovat jako ideály, které podělíme nějakým číslem. Pomocí lomených ideálů pak zadefinujeme inverzní ideály. Začneme definicí modulu, což je zobecnění ideálu.

Definice 12. Řekneme, že M je $\mathcal{O}_K$-modul nad komutativním okruhem $\mathcal{O}_K$, pokud $(M, +, -, 0)$ je abelovská grupa a existuje binární operace $\cdot : \mathcal{O}_K \times M \to M$ taková, že $\forall r, s \in \mathcal{O}_K, \forall m, n \in M$:

1. $(r + s)m = rm + sm$;
2. $r(m + n) = rm + rn$;
3. $(rs)m = r(sm)$;
4. $1_{\mathcal{O}_K} \cdot m = m$.

Poznámka. Místo $1_{\mathcal{O}_K}$ budeme psát pouze 1.

Podobně jako máme podokruh, definujeme také *$\mathcal{O}_K$-podmodul*. Řekneme, že N je $\mathcal{O}_K$-podmodul $\mathcal{O}_K$-modulu M, pokud je N podmnožina M, která je uzavřená na sčítání a na operaci $\cdot$.

Pozorování. Zřejmě $\mathcal{O}_K$ je $\mathcal{O}_K$-modul.

Pozorování. Ideál je speciálním případem modulu. Ideál v $\mathcal{O}_K$ odpovídá $\mathcal{O}_K$-podmodulu $\mathcal{O}_K$, bereme-li ho jako modul nad sebou samým.

Definice 13. Lomený ideál v číselném tělese K je každý nenulový $\mathcal{O}_K$-podmodul I tělesa K, pro který existuje $d \in \mathcal{O}_K \setminus \{0\}$ splňující $dI \subset \mathcal{O}_K$. Toto d nazveme společným dělitelem I.

Poznámka. Explicitně můžeme definovat lomený ideál I jako podmnožinu K splňující následující podmínky:

1. I je uzavřené na sčítání a existenci opačných prvků (tedy obsahuje 0);
2. I je uzavřené na násobení prvky z $\mathcal{O}_K$;
3. $\exists d \in \mathcal{O}_K \setminus \{0\} : \ dI \subset \mathcal{O}_K$.

Pozor, v definici jsme se nezmínili nijak blíže o děliteli d. Tento dělitel určitě nemusí být jednoznačný, nemusí být ani minimální. Pro definici nám pouze stačí, že alespoň jeden takový existuje. Nic víc po něm nepožadujeme.

Poznámka. Ne vždy se lomený ideál definuje jako *nenulový* $\mathcal{O}_K$-modul, my si však touto definicí ušetříme možné pozdější komplikace.

Pozorování. Každý ideál je také lomený ideál. Stačí položit $d = 1$.

Lemma 14. *Nechť I, J jsou lomené ideály v K a $d, e \in \mathcal{O}_K \setminus \{0\}$ jsou jejich společní dělitelé. Potom platí následující:*

1. *dI je ideál v $\mathcal{O}_K$;*
2. *$dI \cdot eJ = (de)IJ$;*
3. *IJ je lomený ideál.*

Důkaz. 1. Potřebujeme ověřit 3 podmínky. Že je dI podmnožina $\mathcal{O}_K$, že je uzavřená na sčítání i vynásobení prvkem z $\mathcal{O}_K$. $dI \subset \mathcal{O}_K$ zřejmě platí. Pro ověření uzavřenosti na sčítání zvolme $x, y \in dI$, můžeme psát $x = di, y = dj$, kde $i, j \in I$. Pak dostáváme $x + y = di + dj = d(i + j) \in dI$. Pro ověření poslední podmínky zvolme $k \in \mathcal{O}_K$. Platí $x \cdot k = (di) \cdot k = d \cdot (ik)$, kde opět z definice lomeného ideálu $ik \in I$, proto $x \cdot k \in dI$.

2. Plyne snadno z definice:

$$dI \cdot eJ = \left\{ \sum_{i=1}^{n} da_i \cdot eb_i \;\middle|\; a_i \in I, b_i \in J, n \in \mathbb{N} \right\} =$$
$$= \left\{ de \sum_{i=1}^{n} a_i b_i \;\middle|\; a_i \in I, b_i \in J, n \in \mathbb{N} \right\} = deIJ.$$

3. Využijeme explicitní definici lomeného ideálu. Součin IJ je zřejmě uzavřen na sčítání a existenci opačných prvků (součin definován pomocí součtu). Je také uzavřen na násobení prvky z $\mathcal{O}_K$. Platí totiž pro libovolné $r \in \mathcal{O}_K$ a pro libovolný prvek $\sum_{i=1}^{n} a_i b_i \in IJ$, kde $n \in \mathbb{N}, a_i \in I, b_i \in J$ následující rovnost:

$$r \sum_{i=1}^{n} a_i b_i = \sum_{i=1}^{n} r a_i b_i = \sum_{i=1}^{n} c_i b_i \in IJ,$$

kde jsme označili $c_i = ra_i \; \forall i \in \{1, \ldots, n\}$. Z uzavřenosti I na vynásobení prvkem z $\mathcal{O}_K$ je pro všechna tato i $c_i \in I$. Dále z 1. víme, že $dI, eJ \subset \mathcal{O}_K$ jsou ideály, tudíž také $dIeJ \subset \mathcal{O}_K$ je ideál. Z 2. platí $dIeJ = deIJ \subset \mathcal{O}_K$. Definici lomeného ideálu splňuje dělitel de. □

Příklad. Položíme-li $K = \mathbb{Q}$, potom $\mathcal{O}_K = \mathbb{Z}$. Příklad lomeného ideálu je $\frac{2}{3}\mathbb{Z} = \left\{ \frac{2}{3}z \;\middle|\; z \in \mathbb{Z} \right\}$. Společný dělitel d pak může být libovolný násobek trojky. Označme ho $3k, k \in \mathbb{N}$, pak zřejmě $(3k)\frac{2}{3}\mathbb{Z} = 2k\mathbb{Z} \subset \mathbb{Z}$.

Tvrzení 15 ([4, Theorem 2.7])**.** *Nechť I je lomený ideál K. Pak množina $I^{-1} = \{x \in K \mid xI \subset \mathcal{O}_K\}$ je také lomený ideál, který nazveme inverzním ideálem. Navíc platí $I \cdot I^{-1} = \mathcal{O}_K$.*

2.2 Třídové číslo

Cílem této sekce je zadefinovat klíčové pojmy třídové grupy a třídového čísla. Motivace za třídovým číslem je vědět, jak funguje ireducibilní rozklad v různých oborech. Nejen, že ne všude je jednoznačný, ale také může nabývat různých délek. To právě určuje ono třídové číslo. Čím nižší je, tím jednoznačnější je ireducibilní rozklad.

Definice 16. Definujme množiny $\mathcal{J}_K = \{I \mid I \text{ je lomený ideál } K\}$ a $\mathcal{P}_K = \{\iota\mathcal{O}_K \mid \iota \in K^\times\}$.

Lemma 17. *Pro množiny $\mathcal{J}_K, \mathcal{P}_K$ definované výše platí:*

1. $(\mathcal{J}_K, \cdot, ^{-1}, \mathcal{O}_K)$ je abelovská grupa. Nazveme ji grupou lomených ideálů.

2. $(\mathcal{P}_K, \cdot, ^{-1}, \mathcal{O}_K)$ je normální podgrupa $\mathcal{J}_K$. Nazveme ji grupou hlavních ideálů.

Důkaz. 1. $\mathcal{J}_K$ je uzavřená na násobení dle lemmatu 14, část 3. Existence inverzního prvku je jasná z tvrzení 15. Triviálně $\mathcal{O}_K \in \mathcal{J}_K$ a splňuje funkci jednotky v grupě. Komutativitu násobení není těžké ukázat: Ať $I, J \in \mathcal{J}_K$, pak platí

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

Zbývá ukázat asociativitu násobení. Nechť $I, J, H \in \mathcal{J}_K$ a $d, e, f \in K^\times$ jsou jejich společní dělitelé, to jest platí $dI, eJ, fH \subset \mathcal{O}_K$. Z první části lemmatu 14 víme, že dI, eJ, fH jsou ideály. Víme, že násobení ideálů je asociativní, tudíž platí $(dI \cdot eJ)fH = dI(eJ \cdot fH)$. Z druhé části stejného lemmatu potom platí $(deIJ) \cdot fH = dI \cdot (efJH)$, použito znovu pak $def(IJ)H = defI(JH)$. Také víme, že $def \neq 0$, neboť $def \in K^\times$, z čehož vyplývá, že existuje jeho inverze $(def)^{-1}$. Můžeme poslední rovnost vynásobit touto inverzí a dostáváme kýžený výsledek $(IJ)H = I(JH)$.

2. Přímo z definice lomeného ideálu plyne, že $\iota\mathcal{O}_K$ pro $\iota \in K^\times$ je lomený ideál v K. Tudíž $\mathcal{P}_K$ obsahuje lomené ideály, tj. je to podmnožina $\mathcal{J}_K$. Množina $\mathcal{P}_K$ je uzavřená na násobení: Vezměme $I, J \in \mathcal{P}_K$, pak z definice existují $\iota, \lambda \in K^\times$ takové, že $I = \iota \cdot \mathcal{O}_K, J = \lambda \cdot \mathcal{O}_K$, a tedy

$$\begin{aligned} I \cdot J = \iota\mathcal{O}_K \cdot \lambda\mathcal{O}_K &= \left\{ \sum_{i=1}^{n} \iota a_i \cdot \lambda b_i \;\middle|\; a_i, b_i \in \mathcal{O}_K, n \in \mathbb{N} \right\} = \\ &= \left\{ \iota\lambda \sum_{i=1}^{n} a_i b_i \;\middle|\; a_i, b_i \in \mathcal{O}_K, n \in \mathbb{N} \right\} = \iota\lambda\mathcal{O}_K \in \mathcal{P}_K, \end{aligned}$$

jelikož $\iota\lambda \in K^\times$.

Dostáváme, že $\mathcal{P}_K$ je podgrupa $\mathcal{J}_K$. Jakožto inverzní prvek ideálu $\iota\mathcal{O}_K \in \mathcal{P}_K$ položíme ideál $\iota^{-1}\mathcal{O}_K$. Protože $\iota \in K^\times$, pak zřejmě $\iota^{-1} \in K^\times$, takže $\iota^{-1}\mathcal{O}_K \in \mathcal{P}_K$ a $\iota\mathcal{O}_K \cdot \iota^{-1}\mathcal{O}_K = \mathcal{O}_K$, což je jednotka v $\mathcal{P}_K$, jelikož se jedná o jednotku v $\mathcal{J}_K$.

Konečně $\mathcal{P}_K$ je normální podgrupa v $\mathcal{J}_K$, poněvadž $\mathcal{J}_K$ je abelovská a víme, že každá podgrupa abelovské grupy je normální. □

Definice 18. Třídovou grupu $\mathcal{O}_K$ definujeme jako $C(\mathcal{O}_K) = \mathcal{J}_K \big/ \mathcal{P}_K$. Velikost této grupy nazveme třídovým číslem.

Poznámka. Třídová grupa bude vždy konečná dle [8, Theorem 10.3], proto i třídové číslo je dobře definované a $|C(\mathcal{O}_K)| \in \mathbb{N}$.

Díky lemmatu 17 vidíme, že třídová grupa je dobře definovaná a že se jedná o grupu. Uvedeme ještě druhou definici třídové grupy a následně ukážeme, že jsou ekvivalentní. K tomu nejprve zadefinujeme následující ekvivalenci na množině ideálů.

Definice 19. Na $\mathcal{I}(\mathcal{O}_K)$ definujeme relaci ekvivalence následovně. Nechť $I, J \in \mathcal{I}(\mathcal{O}_K)$. Řekneme, že $I \sim J$, pokud existují nenulové $\alpha, \beta \in \mathcal{O}_K$ takové, že $(\alpha)I = (\beta)J$. Třídy této ekvivalence značíme $[I]$.

Lemma 20. *Nechť $I, J \in \mathcal{I}(\mathcal{O}_K)$ a $[I]$ značí třídu ekvivalence definovanou výše. Operace $[I] \cdot [J] = [IJ]$ je dobře definována.*

Důkaz. Ať $[I] = [I'], [J] = [J']$ a $[I] \cdot [J] = [IJ]$. Z definice existují nenulové $\alpha, \beta, \alpha', \beta' \in \mathcal{O}_K$ takové, že platí $(\alpha)I = (\alpha')I', (\beta)J = (\beta')J'$, načež $(\alpha)(\beta)IJ = (\alpha')(\beta')I'J'$. Stačí položit $\gamma = \alpha'\beta', \delta = \alpha\beta$, $\gamma, \delta \in \mathcal{O}_K \setminus \{0\}$, aby platilo $(\gamma)I'J' = (\delta)IJ$. Z toho už dostáváme chtěný výsledek $[IJ] = [I'J']$. □

Věta 21. *Zobrazení* $\Phi\colon \mathcal{I}(\mathcal{O}_K)/_\sim \to C(\mathcal{O}_K)$ *definované předpisem* $[I] \mapsto I\mathcal{P}_K$ *je bijekce, která navíc pro* $I, J \in \mathcal{I}(\mathcal{O}_K)$ *splňuje* $\Phi([I] \cdot [J]) = \Phi([I]) \cdot \Phi([J])$. *Tedy* $\mathcal{I}(\mathcal{O}_K)/_\sim$ *je ekvivalentní definici třídové grupy a platí*

$$|\mathcal{I}(\mathcal{O}_K)/_\sim| = \left|\mathcal{J}_K\big/\mathcal{P}_K\right|.$$

Důkaz. Nejprve ukážeme, že je zobrazení Φ dobře definované. Ať $I, J \in \mathcal{I}(\mathcal{O}_K)$ a $[I] = [J]$, to jest existují nenulové $\alpha, \beta \in \mathcal{O}_K$ takové, že $(\alpha)I = (\beta)J$. Poté

$$\Phi([I]) = I\mathcal{P}_K = (\alpha)I\mathcal{P}_K = (\beta)J\mathcal{P}_K = J\mathcal{P}_K = \Phi([J]),$$

kde druhá rovnost platí proto, že $\alpha \in K^\times$, z čehož $(\alpha)\mathcal{P}_K = \mathcal{P}_K$, podobně platí čtvrtá rovnost.

Dále ověříme, že platí rovnost $\Phi([I] \cdot [J]) = \Phi([I]) \cdot \Phi([J])$. Protože je $\mathcal{O}_K$ komutativní a $I, J \in \mathcal{J}_K$, můžeme ve faktorgrupě $\mathcal{J}_K\big/\mathcal{P}_K$ (kde $\mathcal{P}_K$ je jednotka) rovnou psát:

$$\Phi([I] \cdot [J]) = \Phi([IJ]) = (IJ) \cdot \mathcal{P}_K = I\mathcal{P}_K \cdot J\mathcal{P}_K = \Phi([I]) \cdot \Phi([J]).$$

Pro ověření surjektivity zvolme libovolný prvek $I\mathcal{P}_K \in \mathcal{J}_K\big/\mathcal{P}_K$. Chceme najít jeho vzor. Platí $I \in \mathcal{J}_K$ je lomený ideál v K. Z definice lomeného ideálu proto existuje $d \in \mathcal{O}_K \setminus \{0\}$ splňující $dI \subset \mathcal{O}_K$. Díky lemmatu 14 části 1. víme, že dI je ideál v $\mathcal{O}_K$, to jest $dI \in \mathcal{I}(\mathcal{O}_K)$. Navíc $\Phi([dI]) = dI\mathcal{P}_K = I\mathcal{P}_K$, neboť $d \in K^\times$. Našli jsme vzor prvku $I\mathcal{P}_K$, je jím $[dI]$.

Zbývá ukázat, že je Φ prosté. Zvolme reprezentanty $I, J \in \mathcal{I}(\mathcal{O}_K)$ takové, že $\Phi([I]) = \Phi([J])$. Rozepišme si rovnost jako

$$I\mathcal{P}_K = J\mathcal{P}_K \iff \left\{I \cdot (\alpha) \;\middle|\; \alpha \in K^\times\right\} = \left\{J \cdot (\beta) \;\middle|\; \beta \in K^\times\right\}.$$

Položme $\beta = 1$. Pak existuje $\alpha \in K$ takové, že platí $(\alpha)I = J$. Z tvrzení 1 existují $\nu \in \mathcal{O}_K, n \in \mathbb{N}$ takové, že platí $\alpha = \frac{\nu}{n}$. Můžeme tedy psát $\left(\frac{\nu}{n}\right)I = J$, což je ekvivalentní výrazu $(\nu)I = nJ$, z čehož už plyne ekvivalence $I \sim J$, tedy $[I] = [J]$. Tímto je důkaz kompletní. □

Ukázali jsme, že $\mathcal{I}(\mathcal{O}_K)/_\sim$ je v bijekci s $\mathcal{J}_K\big/\mathcal{P}_K$, z čehož plyne, že $\mathcal{I}(\mathcal{O}_K)/_\sim$ má také strukturu grupy. Všimneme si, že ona bijekce je ve skutečnosti izomorfismem mezi těmito grupami, které jsou tedy izomorfní. Značme proto rozkladové třídy $I\mathcal{P}_K$ také $[I]$.

Z ekvivalentní definice je snadno vidět, že pokud má okruh pouze hlavní ideály, jsou si všechny ekvivalentní. Třídová grupa bude izomorfní grupě s jedním prvkem a třídové číslo bude jedna. Z toho můžeme odvodit následující pozorování.

Pozorování. $\mathcal{O}_K$ je obor hlavních ideálů $\iff$ platí $C(\mathcal{O}_K) = 1$.

Protože obor hlavních ideálů implikuje gaussovskost ([5, tvrzení 1.8]), platí následující implikace: $|C(\mathcal{O}_K)| = 1 \Rightarrow \mathcal{O}_K$ je gaussovský. V okruzích, jejichž třídová grupa má velikost 1, jsou všechny ireducibilní rozklady jednoznačné (až na pořadí a asociovanost). V příští kapitole se proto podíváme na případy okruhů, jejichž třídová grupa má velikost ostře větší než 1.

Příklad. Jeden z nejjednodušších příkladů je pro $K = \mathbb{Q}$. Potom triviálně $\mathcal{O}_K = \mathbb{Z}$, což je obor hlavních ideálů. Z pozorování platí $|C(\mathbb{Z})| = 1$ a $\mathbb{Z}$ je gaussovský. Víme, že v $\mathbb{Z}$ opravdu existuje jednoznačný ireducibilní rozklad každého čísla, a to rozklad na prvočísla (opět až na pořadí a asociovanost prvků).

Poznámka. Pojem třídového čísla se vztahuje pouze k třídové grupě. Usnadníme si však značení a budeme mluvit o třídovém čísle okruhu $\mathcal{O}_K$, přičemž mu budeme rozumět jako třídovému číslu třídové grupy $C(\mathcal{O}_K)$. Dále poznamenejme, že jelikož $\mathcal{O}_K$ je úzce spjaté s K a navzájem se jednoznačně určují, můžeme také říkat, že těleso K má třídové číslo. Opět tím číslem budeme rozumět velikost třídové grupy $\mathcal{O}_K$.

3. Okruhy s třídovým číslem 2 a 3

V této kapitole se zaměříme na rozklady prvků na ireducibilní činitele v okruzích s třídovým číslem 2. Poté některé výsledky zobecníme pro okruh s třídovým číslem 3. Nejdůležitějším výsledkem bude znění a důkaz Carlitzovy věty, která je stěžejní v charakterizaci okruhů s třídovým číslem 2.

3.1 Třídové číslo 2

Naším prvním cílem je znění a důkaz následujícího lemmatu, které bude klíčové ve výsledné charakterizaci okruhů s třídovým číslem 2. Postupně z něj odvodíme spoustu dalších tvrzení. V celé této sekci čerpáme z [2].

Lemma 22. *Nechť $n \in \mathbb{N}$ a x je nenulový neinvertibilní prvek okruhu $\mathcal{O}_K$. Navíc ať $(x) = \mathfrak{p}_1 \cdots \mathfrak{p}_n$ je rozklad hlavního ideálu (x) na prvoideály (dle základní věty teorie ideálů 3), tj. $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ jsou prvoideály v $\mathcal{O}_K$. Pak platí:*

1. $\prod_{i=1}^{n} [\mathfrak{p}_i] = 1$.

2. Prvek x je ireducibilní v $\mathcal{O}_K$ právě tehdy, když $\prod_{i=1}^{n} [\mathfrak{p}_i] = 1$ a pro každou neprázdnou podmnožinu $S \subsetneq \{1, \ldots, n\}$ platí $\prod_{i \in S} [\mathfrak{p}_i] \neq 1$.

Důkaz. 1. Plyne z definice třídové grupy, kde hlavní ideály tvoří jednotku.

2. $\Rightarrow$ Pro spor nechť existuje neprázdná $S \subsetneq \{1, \ldots, n\}$ taková, že $\prod_{i \in S} [\mathfrak{p}_i] = 1$, označme potom $S' = \{1, \ldots, n\} \setminus S$. Potom platí:

$$\prod_{i \in S} [\mathfrak{p}_i] = \prod_{i \in S'} [\mathfrak{p}_i] = 1.$$

Z toho plyne existence neinvertibilních prvků $y, z \in R$ takových, že

$$(y) = \prod_{i \in S} \mathfrak{p}_i, (z) = \prod_{i \in S'} \mathfrak{p}_i,$$

jelikož jednotkou v třídové grupě jsou právě hlavní ideály. Takže existuje invertibilní prvek $u \in \mathcal{O}_K^{\times}$ takový, že platí $x = uyz$, což je spor s ireducibilitou x.

$\Leftarrow$ Pro spor předpokládejme, že $x = yz$, kde $y, z \in \mathcal{O}_K$ nejsou invertibilní. Ze základní věty teorie ideálů 3 v $\mathcal{O}_K$ existují neprázdné $S, S' \subsetneq \{1, \ldots, n\}$ takové, že

$$(y) = \prod_{i \in S} \mathfrak{p}_i, (z) = \prod_{i \in S'} \mathfrak{p}_i,$$

z čehož $\prod_{i \in S} [\mathfrak{p}_i] = 1$, což je spor. □

Pro formulaci tvrzení o ireducibilních prvcích v obecných číselných okruzích se nejprve seznámíme s následující definicí.

Definice 23. Ať $\mathfrak{p} \in \mathcal{I}(\mathcal{O}_K)$. Řád prvku $[\mathfrak{p}]$ v třídové grupě $C(\mathcal{O}_K)$ budeme značit $\mathrm{ord}([\mathfrak{p}])$. Platí $\mathrm{ord}([\mathfrak{p}]) = n \in \mathbb{N}$, je-li n nejmenší možné takové, že platí $([\mathfrak{p}])^n = 1$. To jest nejmenší takové, že $\mathfrak{p}^n$ je rovno hlavnímu ideálu.

Tvrzení 24. *Nechť $\mathfrak{p}$ je nehlavní prvoideál $\mathcal{O}_K$, $\mathrm{ord}([\mathfrak{p}]) = n \in \mathbb{N}$ a ať $\mathfrak{q}$ je prvoideál z třídy $[\mathfrak{p}]^{-1}$. Potom platí následující:*

1. $\mathfrak{p}^n = (x)$ a $x \in \mathcal{O}_K$ je v $\mathcal{O}_K$ ireducibilní;

2. $\mathfrak{p} \cdot \mathfrak{q} = (y)$ a $y \in \mathcal{O}_K$ je v $\mathcal{O}_K$ ireducibilní.

Důkaz. Když se na součiny v 1. i 2. podíváme jako na prvky třídové grupy, jejich výsledek bude zřejmě jednotka, tj. pro samotné prvoideály bude výsledek hlavní ideál. Z lemmatu 22 části 2. vidíme, že jsou prvky x, y ireducibilní, poněvadž součin v třídové grupě je roven 1 (jak jsme již řekli), ale pro žádnou podmnožinu roven 1 není. □

Aplikujeme-li tvrzení na okruhy $\mathcal{O}_K$ splňující $|C(\mathcal{O}_K)| = 2$, za pomoci lemmatu 22 dostaneme plnou charakterizaci všech ireducibilních prvků v daném okruhu.

Důsledek 25. *Nechť $|C(\mathcal{O}_K)| = 2$. Potom x je ireducibilní prvek v $\mathcal{O}_K$ právě tehdy, pokud platí právě jedno z následujícího:*

1. $(x) = \mathfrak{p}$, kde $\mathfrak{p}$ je hlavní prvoideál v $\mathcal{O}_K$;

2. $(x) = \mathfrak{p} \cdot \mathfrak{q}$, kde $\mathfrak{p}, \mathfrak{q}$ jsou ne nutně různé nehlavní prvoideály v $\mathcal{O}_K$.

Důkaz. $\Rightarrow$ Nechť x je ireducibilní v $\mathcal{O}_K$. Dle základní věty teorie ideálů 3 existují $\mathfrak{p}_1, \ldots, \mathfrak{p}_n \in \mathcal{I}(\mathcal{O}_K), n \in \mathbb{N}$, takové, že $(x) = \mathfrak{p}_1 \cdots \mathfrak{p}_n$. Potom dle lemmatu 22 části 2. je $\prod_{i=1}^{n} [\mathfrak{p}_i] = 1$, ale pro žádnou podmnožinu $\{1, \ldots, n\}$ rovno 1 není. Protože je třídové číslo $\mathcal{O}_K$ rovno 2, třídová grupa je izomorfní grupě o dvou prvcích, grupě $\mathbb{Z}/2\mathbb{Z}$. Abychom dostali v třídové grupě jednotku, máme na výběr pouze 2 možnosti. Buď vzít samotnou jednotku, tj. hlavní prvoideál, z čehož plyne případ 1. Nebo vzít druhý prvek, jenž je vlastní inverzí, a tudíž dostaneme dva nehlavní prvoideály, což odpovídá případu 2.

$\Leftarrow$ Obojí plyne přímo z tvrzení 24. □

Nacházíme se v pozici, kdy můžeme poskytnout konkrétní informace i o ireducibilním rozkladu v $\mathcal{O}_K$, je-li jeho třídové číslo 2.

Tvrzení 26. *Nechť $|C(\mathcal{O}_K)| = 2$ a $x \in \mathcal{O}_K$ nenulové neinvertibilní. Dle základní věty teorie ideálů (věta 3) existuje posloupnost hlavních prvoideálů $\{\mathfrak{p}_i\}_{i=1}^{n}$ a posloupnost nehlavních prvoideálů $\{\mathfrak{q}_j\}_{j=1}^{m}$ v $\mathcal{O}_K$ splňující $(x) = \mathfrak{p}_1 \cdots \mathfrak{p}_n \cdot \mathfrak{q}_1 \cdots \mathfrak{q}_m$. Potom platí následující:*

1. m je sudé;

2. každý ireducibilní rozklad prvku x má délku $n + \frac{m}{2}$.

Důkaz. 1. Z důsledku 25 z 2. části vidíme, že pro dva nehlavní prvoideály $\mathfrak{q}_i, \mathfrak{q}_j$, kde $i, j \in \{1, \ldots, m\}$, existuje $y \in \mathcal{O}_K$ ireducibilní takové, že $\mathfrak{q}_i\mathfrak{q}_j = (y)$. Neboť na levé straně rovnosti máme hlavní ideál (x), na pravé straně bude také hlavní ideál. Na to se nám však musí všechny nehlavní ideály spárovat předcházejícím způsobem, a tudíž m nemůže být liché, ergo je sudé.

2. Hlavní ideál (x) je tvořen násobky n hlavních prvoideálů, který každý odpovídá jednomu ireducibilnímu prvku. Ireducibilní rozklad prvku x v $\mathcal{O}_K$ proto bude mít délku minimálně n. Dále m nehlavních ideálů spárujeme, jak bylo ukázáno v 1., do $\frac{m}{2}$ ireducibilních prvků. Výsledný ireducibilní rozklad je délky právě $n + \frac{m}{2}$. □

Všimneme si, že pokud by prvek x byl ireducibilní, dle důsledku 25 by nastala situace buď $n = 1$, nebo $m = 2$.

Pro případ, že nehlavní prvoideály v rozkladu (x) jsou navzájem různé, můžeme ještě snadno dostat následující tvrzení. Tvrzení lze dostat i pro případ, že prvoideály nejsou nutně různé, avšak tímto se kvůli kombinatorické obtížnosti nebudeme zabývat.

Tvrzení 27. *Nechť $|C(\mathcal{O}_K)| = 2, x \in \mathcal{O}_K$ je nenulové a neinvertibilní. Ať stejně jako v předchozím tvrzení $\{\mathfrak{p}_i\}_{i=1}^n$ je posloupnost hlavních prvoideálů a $\{\mathfrak{q}_j\}_{j=1}^m$ je posloupnost po dvou* ***různých*** *nehlavních prvoideálů v $\mathcal{O}_K$ taková, že platí $(x) = \mathfrak{p}_1 \cdots \mathfrak{p}_n \cdot \mathfrak{q}_1 \cdots \mathfrak{q}_m$. Potom počet ireducibilních rozkladů prvku x v $\mathcal{O}_K$ je*

$$(m-1) \cdot (m-3) \cdots 3 \cdot 1.$$

Důkaz. Výsledný počet závisí pouze na konstantě m. Konkrétně na tom, jakým způsobem dáme m nehlavních ideálů do dvojic. Jelikož každý hlavní prvoideál automaticky určuje právě jeden ireducibilní prvek, nemáme u nich možnost volby. Počet ireducibilních rozkladů se dá převést na úlohu, kolika způsoby můžeme uspořádat m prvků do dvojic bez opakování a nezávisle na pořadí dvojice.

Výpočet ukážeme induktivně. Pro $m = 0$ zřejmě existuje pouze jediný ireducibilní rozklad sestávající pouze z hlavních prvoideálů. Pro $m = 2$ už sice ireducibilní rozklad netvoří pouze hlavní prvoideály, avšak stále není možnost výběru a nezbývá než spárovat dva nehlavní provideály spolu. Pro $m = 4$ máme přesně $(4-1)$ možností, s čím spárovat první nehlavní prvoideál. Zbylá dvojice už je jednoznačně určena a více možností není, celkový počet je tedy 3. Pro $m = 6$ máme $(6-1)$ možností, s čím spárovat první nehlavní prvoideál. Pro zbylé 4 prvoideály si všimneme, že to odpovídá předchozímu případu pro $m = 4$. Tyto dvě volby na sobě nezávisí a více možností není, počet způsobů spárování je proto $5 \cdot 3 = 15$. Nyní pro libovolné m vždy bude $(m-1)$ možností, s čím spárovat první prvoideál a pro každý jednotlivý případ bude situace odpovídat počtu případů pro $m-2$. Dostáváme tedy následující vzorec pro počet ireducibilních rozkladů prvku x:

$$(m-1) \cdot (m-3) \cdots 3 \cdot 1. \qquad \square$$

3.2 Carlitzova věta

V návaznosti na předchozí sekci o třídovém čísle 2 dokážeme Carlitzovu větu. Ta nám dává úplnou charakterizaci okruhů s třídovým číslem nižším nebo rovno 2. Než přejdeme k samotné Carlitzově větě, v následujícím lemmatu se podíváme, jak může situace vypadat v $\mathcal{O}_K$, je-li jeho třídové číslo větší než 2. Následující dvě tvrzení jsou opět převzata z [2].

Lemma 28. *Nechť $|C(\mathcal{O}_K)| > 2$. Pak v $\mathcal{O}_K$ existují ne nutně rozdílné ireducibilní prvky $\alpha_1, \alpha_2, \alpha_3, \beta_1, \beta_2$ takové, že platí $\alpha_1 \cdot \alpha_2 \cdot \alpha_3 = \beta_1 \cdot \beta_2$.*

Důkaz. Celý důkaz si rozdělíme na dvě části dle toho, jestli v $C(\mathcal{O}_K)$ existují neinvertibilní prvky řádu většího než 2.

1. Ať v $C(\mathcal{O}_K)$ existuje prvek s takový, že $\mathrm{ord}(s) = n \in \mathbb{N}, n > 2$. Zvolme prvoideály $\mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_3, \mathfrak{p}_4 \in \mathcal{I}(\mathcal{O}_K)$ takové, že jsou po řadě z tříd s, s^2, s^{-2}, s^{-1}. Pokud $n = 3$, nebo 4, volme tyto ideály navzájem různé. Prvky $\rho, \sigma, \xi, \zeta \in \mathcal{O}_K$ definované jako

$$\begin{aligned}(\rho) &= \mathfrak{p}_1\mathfrak{p}_4,\\ (\sigma) &= \mathfrak{p}_1^2\mathfrak{p}_3,\\ (\xi) &= \mathfrak{p}_2\mathfrak{p}_3,\\ (\zeta) &= \mathfrak{p}_2\mathfrak{p}_4^2,\end{aligned}$$

jsou ireducibilní dle tvrzení 24. Potom díky rovnosti ideálů

$$(\mathfrak{p}_1^2\mathfrak{p}_3)(\mathfrak{p}_2\mathfrak{p}_4^2) = (\mathfrak{p}_1\mathfrak{p}_4)^2(\mathfrak{p}_2\mathfrak{p}_3)$$

platí následující rovnost:

$$\sigma\zeta = u\rho^2\xi,$$

kde u je nějaký invertibilní prvek okruhu $\mathcal{O}_K$, což už je výsledek, jejž jsme chtěli.

2. Tentokrát předpokládejme, že všechny neinvertibilní prvky grupy $C(\mathcal{O}_K)$ jsou řádu 2. Zvolíme různé třídy nehlavních ideálů $s_1, s_2 \in C(\mathcal{O}_K)$, načež označíme $s_3 = s_1 + s_2$. Platí, že $s_1, s_2, s_3 \in C(\mathcal{O}_K)$ jsou různé prvky, všechny řádu 2. Vezměme jako v předchozím případě prvoideály $\mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_3 \in \mathcal{I}(\mathcal{O}_K)$ postupně z tříd s_1, s_2, s_3 a definujme prvky $\eta_1, \eta_2, \eta_3, \theta \in \mathcal{O}_K$ následovně:

$$\begin{aligned}(\eta_1) &= \mathfrak{p}_1^2,\\ (\eta_2) &= \mathfrak{p}_2^2,\\ (\eta_3) &= \mathfrak{p}_3^2,\\ (\theta) &= \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3.\end{aligned}$$

Opět se jedná o ireducibilní prvky dle tvrzení 24. Nyní platí požadovaná rovnost

$$\theta^2 = v\eta_1\eta_2\eta_3,$$

kde v je nějaký invertibilní prvek okruhu $\mathcal{O}_K$. Tím je lemma dokázáno. □

Před seznámením s charakterizační Carlitzovou větou připomene, že okruh je pologaussovský právě tehdy, kdy všechny ireducibilní rozklady jednoho prvku mají stejnou délku (definice 10).

Věta 29 (Carlitzova věta)**.** *Číselný okruh $\mathcal{O}_K$ má třídové číslo nejvýše 2 právě tehdy, když je $\mathcal{O}_K$ pologaussovský obor.*

Důkaz. $\Rightarrow$ Ať $x \in \mathcal{O}_K$ nenulové neinvertibilní. Dle základní věty teorie ideálů 3 existují hlavní prvoideály $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ a nehlavní prvoideály $\mathfrak{q}_1, \ldots, \mathfrak{q}_m, n, m \in \mathbb{N}$ takové, že platí $(x) = \mathfrak{p}_1 \cdots \mathfrak{p}_n \cdot \mathfrak{q}_1 \cdots \mathfrak{q}_m$. Protože $|C(\mathcal{O}_K)| = 2$ z předpokladu, je pouze jedna třída nehlavních ideálů. Z tvrzení 26 je m sudé a všechny ireducibilní rozklady x mají délku $n + \frac{m}{2}$, ergo $\mathcal{O}_K$ je pologaussovský.

$\Leftarrow$ Je-li $\mathcal{O}_K$ pologaussovský, všechny ireducibilní rozklady mají stejnou délku. Z rovnosti v lemmatu 28 vidíme, že třídové číslo $\mathcal{O}_K$ je nejvýše 2. □

3.3 Třídové číslo 3

Zkusíme některé výsledky z předchozí sekce o třídovém čísle 2 zobecnit pro okruh $\mathcal{O}_K$ s třídovým číslem 3.

Je-li třídové číslo $\mathcal{O}_K$ rovno 3, třídová grupa $C(\mathcal{O}_K)$ je izomorfní grupě se třemi prvky. Existuje však pouze jediná grupa o třech prvcích, a to aditivní grupa $\mathbb{Z}/3\mathbb{Z}$. Z tohoto izomorfismu dostáváme, že v $C(\mathcal{O}_K)$ existují 2 navzájem různé třídy nehlavních ideálů, jejichž řád v této grupě je 3. Použijeme-li tvrzení 24 na okruhy s třídovým číslem 3, jako jsme to předtím udělali s třídovým číslem 2, dostaneme obdobu důsledku 25 o tom, jakých forem mohou být ireducibilní prvky v $\mathcal{O}_K$.

Důsledek 30. *Nechť $|C(\mathcal{O}_K)| = 3$. Prvek x je ireducibilní v $\mathcal{O}_K$ právě tehdy, když platí právě jedno z následujícího:*

1. $(x) = \mathfrak{p}$, kde $\mathfrak{p}$ je hlavní prvoideál v $\mathcal{O}_K$;

2. $(x) = \mathfrak{p} \cdot \mathfrak{q} \cdot \mathfrak{r}$, kde $\mathfrak{p}, \mathfrak{q}, \mathfrak{r}$ jsou ne nutně různé nehlavní prvoideály ze stejné třídy nehlavních ideálů v $C(\mathcal{O}_K)$;

3. $(x) = \mathfrak{p} \cdot \mathfrak{q}$, kde $\mathfrak{p}, \mathfrak{q}$ jsou různé nehlavní prvoideály a každý je z jiné třídy nehlavních ideálů v $C(\mathcal{O}_K)$, to jest ideál $\mathfrak{q}$ je z třídy $[\mathfrak{p}]^{-1}$.

Důkaz. $\Rightarrow$ Nechť x je ireducibilní v $\mathcal{O}_K$. Dle základní věty teorie ideálů 3 existují $\mathfrak{p}_1, \ldots, \mathfrak{p}_n \in \mathcal{I}(\mathcal{O}_K), n \in \mathbb{N}$, takové, že $(x) = \mathfrak{p}_1 \cdots \mathfrak{p}_n$. Dle lemmatu 22 části 2. je $\prod_{i=1}^{n} [\mathfrak{p}_i] = 1$, ale pro žádnou podmnožinu $\{1, \ldots, n\}$ rovno 1 není. Třídové číslo $\mathcal{O}_K$ je rovno 3, tudíž třídová grupa $C(\mathcal{O}_K)$ je izomorfní aditivní grupě $\mathbb{Z}/3\mathbb{Z}$. Způsoby, jak dostat v této grupě jednotku, jsou právě tři. Buďto rovnou vezmeme jednotku, tj. hlavní prvoideál v $\mathcal{O}_K$, což odpovídá našemu případu 1. Nebo vezmeme jeden ze zbývajících dvou prvků, který má řád roven 3, tedy dostaneme 3 nehlavní prvoideály ze stejné třídy, což odpovídá případu 2. Poslední možnost je vzít oba prvky různé od jednotky, jež jsou si navzájem inverzní. Z toho dostanu dva nehlavní prvoideály, každý z jiné třídy, což odpovídá případu 3.

$\Leftarrow$ Všechny 3 případy plynou přímo z tvrzení 24. □

Naším cílem je dostat obdobu tvrzení 26 pro číselný okruh s třídovým číslem 3. Mějme $\mathcal{O}_K$ takový, že $|C(\mathcal{O}_K)| = 3$. V $C(\mathcal{O}_K)$ jsou 3 třídy ideálů. Jedna třída obsahuje všechny hlavní ideály, druhá je třída nehlavních ideálů, označme si ji T. Třetí třída odpovídá třídě inverzní k T, označíme ji T^{-1}. Zvolme posloupnost hlavních prvoideálů $\{\mathfrak{p}_i\}_{i=1}^{n}$ v $\mathcal{O}_K$. Dále zvolme posloupnost nehlavních prvoideálů $\{\mathfrak{q}_j\}_{j=1}^{m}$ z třídy T, a konečně posloupnost nehlavních prvoideálů $\{\mathfrak{r}_l\}_{l=1}^{k}$ z třídy T^{-1} tak, aby existovalo $x \in \mathcal{O}_K$ splňující

$$(x) = \mathfrak{p}_1 \cdots \mathfrak{p}_n \cdot \mathfrak{q}_1 \cdots \mathfrak{q}_m \cdot \mathfrak{r}_1 \cdots \mathfrak{r}_k.$$

Neboť je na levé straně rovnice hlavní ideál, součin na pravé straně musí dát hlavní ideál.

Nechť x má následující ireducibilní rozklad: $x = x_1 \cdots x_s, s \in \mathbb{N}$. Poté triviálně platí také $(x) = (x_1) \cdots (x_s)$. Z důsledku 30 vidíme, že pro ireducibilní prvek $x_i, i \in \{1, \ldots, s\}$, musí platit právě jedno z následujícího:

$$(x_i) = \begin{cases} \mathfrak{p}_j \\ \mathfrak{q}_{j_1} \mathfrak{q}_{j_2} \mathfrak{q}_{j_3} \\ \mathfrak{r}_{j_1} \mathfrak{r}_{j_2} \mathfrak{r}_{j_3} \\ \mathfrak{q}_{j_4} \mathfrak{r}_{j_4}, \end{cases}$$

kde $\mathfrak{p}_j \in \{\mathfrak{p}_i\}_{i=1}^{n}, \mathfrak{q}_{j_1}, \ldots, \mathfrak{q}_{j_4} \in \{\mathfrak{q}_j\}_{j=1}^{m}, \mathfrak{r}_{j_1}, \ldots, \mathfrak{r}_{j_4} \in \{\mathfrak{r}_l\}_{l=1}^{k}$.

Tedy z jednotlivých nehlavních ideálů můžeme udělat ideál hlavní a tím získat ireducibilní prvek právě jedním ze dvou způsobů. Buďto vynásobíme tři prvoideály ze stejné třídy, přičemž je jedno, zda jsou ideály různé či nikoli, nebo vynásobíme jeden prvoideál z třídy T s prvoideálem z třídy T^{-1}. Při tvoření ireducibilního rozkladu označme jako t počet hlavních ideálů vzniklých vynásobením dvojice ideálů z třídy T a T^{-1}, což odpovídá dle důsledku 30 způsobu 3. Konečně můžeme formulovat následující tvrzení.

Tvrzení 31. *Nechť* $|C(\mathcal{O}_K)| = 3, x \in \mathcal{O}_K$ *nenulové neinvertibilní a jak bylo popsáno výše,* $(x) = \mathfrak{p}_1 \cdots \mathfrak{p}_n \cdot \mathfrak{q}_1 \cdots \mathfrak{q}_m \cdot \mathfrak{r}_1 \cdots \mathfrak{r}_k$ *a* $x = x_1 \dots x_s$ *je ireducibilní rozklad prvku* x*. Buď* t *jako výše počet* x_i *v ireducibilním rozkladu* x *takových, že mají rozklad typu 3. z důsledku 30. Pak platí následující:*

1. $m \equiv k \equiv t \pmod 3$*;*
2. $s = n + t + \frac{m-t}{3} + \frac{k-t}{3}$*.*

Důkaz. 1. Kdyby $m \not\equiv k \pmod 3$, pak bez újmy na obecnosti $m \not\equiv 0 \pmod 3$. V tomto případě musíme nějaký hlavní ideál vytvořit pomocí druhého způsobu uvedeného před tvrzením, to jest vzít dvojici ideálů z T a T^{-1}. Opakováním tohoto způsobu bude m neustále různé od k, a zároveň alespoň jedno z nich různé od 3, abychom vytvořili hlavní ideál prvním způsobem, to jest vynásobením tří nehlavních ideálů ze stejné třídy. Nebude proto možné dostat na pravé straně hlavní ideál.

Podobná myšlenka se použije pro důkaz toho, že $m \equiv t \pmod 3$. V případě, že $m \not\equiv 0 \pmod 3$, musíme vytvořit minimálně 1 nebo 2 dvojice nehlavních ideálů z různých tříd pro dostání hlavního ideálu, a to právě v závislosti na kongruenci m modulo 3. Potom nehledě na to, kolik dvojic máme vytvořených, musíme buďto vytvořit další 3, nebo žádnou, abychom zbývající nehlavní ideály v třídě mohli rozdělit do trojic. Volíme tedy t libovolně jako násobky 3 plus zbytek m po vydělení 3.

2. Není těžké dokázat. Z každého hlavního ideálu $\mathfrak{p}_j$ uděláme právě jeden ireducibilní prvek dle důsledku 30 a hlavních ideálů je n. Dále dostaneme prvek x v závislosti na tom, kolik uděláme ireducibilních prvků z dvojic, to jest dvou nehlavních ideálů různých tříd a počet těchto dvojic jsme si označili t. Nakonec nám zbude právě $m-t$ prvoideálů v třídě T, které musíme rozdělit do trojic, tedy nám vznikne právě $\frac{m-t}{3}$ ireducibilních prvků. Úplně stejným způsobem dostaneme $\frac{k-t}{3}$ ireducibilních prvků z prvoideálů v T^{-1}. Celkem je tedy délka rozkladu

$$n + t + \frac{m-t}{3} + \frac{k-t}{3}. \qquad \square$$

Opět pro případ, že nehlavní prvoideály v rozkladu (x) jsou navzájem různé, spočteme počet ireducibilních rozkladů prvku x. Stejně jako v případě s třídovým číslem 2 nebudeme dopočítávat, kolik existuje rozkladů, pokud se prvoideály opakují.

Tvrzení 32. *Nechť* $|C(\mathcal{O}_K)| = 3, x \in \mathcal{O}_K$ *nenulové neinvertibilní a* $(x) = \mathfrak{p}_1 \cdots \mathfrak{p}_n \cdot \mathfrak{q}_1 \cdots \mathfrak{q}_m \cdot \mathfrak{r}_1 \cdots \mathfrak{r}_k$ *jako v předchozím tvrzení, kde navíc všechny prvoideály z* $\{\mathfrak{q}_j\}_{j=1}^m$ *a* $\{\mathfrak{r}_l\}_{l=1}^k$ *jsou navzájem* ***různé****. Potom v závislosti na* t*, definovaném výše jako počet ireducibilních prvků vzniklých dle 3. z důsledku 30, je počet ireducibilních rozkladů prvku* x *roven*

$$t!\binom{m}{t}\binom{k}{t}\prod_{i=1}^{\frac{m-t}{3}}\binom{3i-1}{2}\prod_{j=1}^{\frac{k-t}{3}}\binom{3j-1}{2}.$$

Důkaz. Nejprve si pro $m \equiv 0 \pmod 3$ spočteme, kolika způsoby můžeme m prvků rozdělit do trojic. Přitom použijeme podobnou myšlenku jako v důkazu tvrzení 27. Pro $m = 0, 3$ je zřejmě počet způsobů 1. Pro $m = 6$ si vezmeme

trojici, která bude obsahovat první prvek m (kde jako první prvek fixujeme libovolný prvek), a dostaneme $\binom{5}{2}$ možností, jak k prvnímu prvku přidat do trojice zbylé dva prvky, aniž by se opakovaly. Druhá trojice je určena jednoznačně, takže více možností není. Pro $m = 9$ si opět vezmeme první prvek m a tentokrát je $\binom{8}{2}$ možností, jak k němu do trojice vybrat zbylé dva prvky. Pro každý případ potřebujeme z šestice prvků udělat 2 trojice, což už je stejný případ jako $m = 6$. Celkově tedy vždy pro m prvků si libovolně zvolíme jeden prvek, poté bude $\binom{m-1}{2}$ způsobů, jak z něj udělat trojici, načež vždy dostaneme známý případ, jen pro $m - 3$. Celkem je počet způsobů, jak rozdělit m prvků do trojic roven

$$\binom{m-1}{2} \cdot \binom{m-4}{2} \cdots \binom{5}{2} \cdot \binom{2}{2} = \prod_{i=1}^{\frac{m}{3}} \binom{3i-1}{2}.$$

Teď se pojďme podívat, jak můžeme dostat různé ireducibilní rozklady prvku x. Vždy nejprve určíme počet t, kolik nehlavních prvoideálů budeme spojovat do dvojic. t může nabývat hodnot od 0 až do $\min\{m, k\}$, v případě, že $m \equiv 0 \pmod 3$, může být t rovno 0, pokud ne, jsme nuceni alespoň jednu dvojici vytvořit. Způsobů, jak vybrat prvky z $\{\mathfrak{q}_j\}_{j=1}^{m}$ a $\{\mathfrak{r}_l\}_{l=1}^{k}$ prvoideály, které budou tvořit ony dvojice, je přesně $\binom{m}{t} \cdot \binom{k}{t}$. Potom možností, jak spárovat prvky dvou t-prvkových množin, je právě $t!$. Stačí prvky jedné množiny libovolně pevně uspořádat, v druhé množině pak máme $t!$ možností, jak uspořádat druhou množinu, načež už jen prvky poskládáme dohromady, a to první s prvním, druhý s druhým, atd.

Na konec po vytvoření t dvojic zbude $m-t$ a $k-t$ nehlavních prvoideálů, které chceme rozdělit do trojic. To už jsme si spočetli výše. Dáme-li vše dohromady, dostaneme požadovaný výsledek, a totiž, že počet ireducibilních rozkladů prvku x je:

$$t!\binom{m}{t}\binom{k}{t} \prod_{i=1}^{\frac{m-t}{3}} \binom{3i-1}{2} \prod_{j=1}^{\frac{k-t}{3}} \binom{3j-1}{2}. \qquad \square$$

Toto tvrzení lze alespoň trochu zobecnit do následujícího důsledku.

Důsledek 33. *Nechť jako v předchozím tvrzení $|C(\mathcal{O}_K)| = 3, x \in \mathcal{O}_K$ nenulové neinvertibilní, $(x) = \mathfrak{p}_1 \cdots \mathfrak{p}_n \cdot \mathfrak{q}_1 \cdots \mathfrak{q}_m \cdot \mathfrak{r}_1 \cdots \mathfrak{r}_k$, kde všechny prvoideály z $\{\mathfrak{q}_j\}_{j=1}^{m}, \{\mathfrak{r}_l\}_{l=1}^{k}$ jsou navzájem různé, a t značí jako výše počet ireducibilních prvků vzniklých vzetím dvou nehlavních prvoideálů z dvou různých tříd. Potom počet ireducibilních rozkladů prvku x je:*

$$\sum_{\substack{t \in \{0,\ldots,\min\{m,k\}\} \\ t \equiv m \pmod 3}} \left(t!\binom{m}{t}\binom{k}{t} \prod_{i=1}^{\frac{m-t}{3}} \binom{3i-1}{2} \prod_{j=1}^{\frac{k-t}{3}} \binom{3j-1}{2} \right),$$

kde sčítáme přes každé třetí t počínaje $t = m \bmod 3$ (tj. zbytkem m po vydělení 3), až po $t = \min\{m, k\}$.

Důkaz. Plyne z předchozího tvrzení 32. Stačí pouze sečíst počet ireducibilních rozkladů prvku x v závislosti na t přes všechna možná t, jaká můžeme dostat. Z tvrzení 31, části 1. víme, že $m \equiv t \pmod 3$ a také to, že pokud nejsou obě

kongruentní 0, jsme nuceni alespoň nějakou dvojici tvořit. Budeme všechny ireducibilní rozklady sčítat přes t, počínaje $t = m \bmod 3$ (tj. zbytkem m po vydělení 3), což je minimální počet vytvořených dvojic. Budeme sčítat každé třetí t, aby byla splněna podmínka kongruence s m modulo 3. Nejvyšší počet možných vytvořených dvojic je právě $\min\{m, k\}$, což odpovídá tomu, že jsme všechny nehlavní ideály z menší třídy rozdělili do dvojic s ideály ve druhé třídě. □

4. Okruh $\mathbb{Q}\left[\sqrt{-23}\right]$

Na závěr celé práce ukážeme příklad okruhu s třídovým číslem 3, rozkladu hlavního ideálu na prvoideály a získávání ireducibilních rozkladů.

Dokázat o okruhu, jaké je jeho třídové číslo, není vůbec triviální (ani za použití Carlitzovy věty), nebudeme se tím proto zabývat. Z [6] využijeme, že $\left|C\left(\mathbb{Q}\left[\sqrt{-23}\right]\right)\right| = 3$ a položíme $K = \mathbb{Q}\left[\sqrt{-23}\right]$. Neboť $-23 \equiv 1 \pmod 4$, z tvrzení 4 je $\mathcal{O}_K = \mathbb{Z}\left[\frac{1+\sqrt{-23}}{2}\right]$. Jak jsme poznamenali dříve, je i třídové číslo tohoto okruhu 3. Pojďme se v této kapitole podívat, jak vypadá třídová grupa $\mathbb{Z}\left[\frac{1+\sqrt{-23}}{2}\right]$ a pojďme najít všechny ireducibilní rozklady prvku 126 v tomto okruhu.

Označme $\omega = \frac{1+\sqrt{-23}}{2}$. Libovolný prvek okruhu $\mathbb{Z}[\omega]$ je tvaru $\frac{a}{2} + \frac{b}{2}\sqrt{-23}$ pro $a, b \in \mathbb{Z}$, splňující $a \equiv b \pmod 2$. V sekci 1.2 jsme si spočetli, jakého tvaru je norma v kvadratických rozšířeních. Norma libovolného prvku je $\frac{a^2}{4} + 23\frac{b^2}{4}$, což je dokonce přirozené číslo a pro nulový prvek 0. Dle lemmatu o vlastnostech normy 7 části 3. totiž víme, že norma v libovolném číselném okruhu $\mathcal{O}_K$ je celé číslo.

K hledání ireducibilních rozkladů v číselném okruhu budeme potřebovat [5, věta 4.20 a 4.21]. Bez těchto vět by se rozklad hledal velmi těžko. Poněvadž věty potřebujeme pouze pro tuto kapitolu a budeme hledat ireducibilní rozklad pouze v konkrétním okruhu $\mathbb{Z}[\omega]$, upravíme si ony dvě věty do jedné následující.

Věta 34. *Nechť D je nečtvercové číslo, $K = \mathbb{Q}\left[\sqrt{D}\right]$ je číselné těleso a $\mathcal{O}_K = \mathbb{Z}[\tau]$, kde $\tau = \frac{1+\sqrt{D}}{2}$. Potom τ má minimální polynom tvaru $f(x) = x^2 - x + \frac{1-D}{4}$. Je-li $p \in \mathbb{Z}$ prvočíslo, rozklad (p) na prvoideály je následující:*

1. (p) je sám o sobě prvoideál s normou p^2, pokud $f(x)$ je ireducibilní modulo p;

2. $(p) = (p, \tau - c)(p, \tau - d)$ a navíc $\mathcal{N}((p, \tau - c)) = \mathcal{N}((p, \tau - d)) = p$, pokud $f(x) \equiv (x - c)(x - d) \pmod p$.

Aplikujeme-li větu rovnou na číselný okruh $\mathbb{Z}[\omega]$, dostaneme minimální polynom $g_\omega(x) = x^2 - x + 6$. Postupně ukážeme ireducibilní rozklady prvků 6 a 18, než dojdeme k rozkladu 126.

4.1 Ireducibilita čísel 2, 3 a 7

Nejprve potřebujeme najít nějaké ireducibilní prvky v $\mathbb{Z}[\omega]$. Dokážeme, že 2, 3 i 7 jsou ireducibilní, a najdeme rozklad na prvoideály hlavních ideálů z nich vytvořených.

Lemma 35. *V číselném okruhu $\mathbb{Z}[\omega]$ je číslo 3 ireducibilní. Hlavní ideál (3) není prvoideál a jeho rozklad na prvoideály je následující:*

$$(3) = (3, \omega)(3, \omega - 1).$$

Důkaz. Sporem ať 3 není ireducibilní. Potom existují neinvertibilní $\psi_1, \psi_2 \in \mathbb{Z}[\omega]$ takové, že $\psi_1\psi_2 = 3$. Spočteme, že $\mathcal{N}(3) = 9 = 3 \cdot 3$. Díky multiplikativitě normy pak $\mathcal{N}(\psi_1\psi_2) = \mathcal{N}(3) = 9$, a jelikož víme, že norma všech prvků v $\mathbb{Z}[\omega]$ je přirozené číslo (nebo 0), nutně $\mathcal{N}(\psi_1) = \mathcal{N}(\psi_2) = 3$. Prvky ψ_1, ψ_2 nejsou

invertibilní, jejich norma je větší než 1, takže existuje prvek normy 3. Je tvaru $\frac{a}{2} + \frac{b}{2}\sqrt{-23}$ a jeho norma splňuje:

$$\frac{a^2}{4} + 23\frac{b^2}{4} = 3;$$

$$a^2 + 23b^2 = 12.$$

Je vidět, že rovnice nemá řešení v celých číslech, jelikož by muselo platit $b = 0$ a 12 není čtverec, a tudíž prvek normy 3 neexistuje, což je spor. Dokázali jsme, že 3 je ireducibilní v $\mathbb{Z}\left[\frac{1+\sqrt{-23}}{2}\right]$.

Jelikož $g_\omega(x) \equiv x^2 - x \equiv x(x-1) \pmod 3$, z věty 34 vidíme, že (3) není prvoideál v $\mathbb{Z}[\omega]$ a rozklad na prvoideály je následující:

$$(3) = (3, \omega)(3, \omega - 1). \qquad \square$$

Lemma 36. *V číselném okruhu $\mathbb{Z}[\omega]$ je číslo 2 ireducibilní. Hlavní ideál (2) není prvoideál a jeho rozklad na prvoideály je následující:*

$$(2) = (2, \omega)(2, \omega - 1).$$

Důkaz. Stejně jako v předchozím lemmatu stačí ukázat, že v $\mathbb{Z}[\omega]$ neexistuje prvek normy 2. Kdyby existoval, pak by dělitel čísla 2 musel mít normu 2, poněvadž $\mathcal{N}(2) = 2 \cdot 2$. Předpokládejme tedy, že norma prvku $\frac{a}{2} + \frac{b}{2}\sqrt{-23}$ je 2. Potom musí mít rovnice

$$a^2 + 23b^2 = 2 \cdot 4 = 8$$

řešení v celých číslech, což vidíme, že nemá (muselo by platit $b = 0$ a 8 není čtverec).

Pro druhou část tvrzení opět využijeme větu 34. Protože $g_\omega(x) \equiv x^2 - x \equiv x(x-1)$, poté stejně jako v předchozím lemmatu $(2) = (2, \omega)(2, \omega - 1)$ je rozklad na prvoideály. $\square$

Víme, že $(3, \omega), (3, \omega - 1), (2, \omega), (2, \omega - 1)$ jsou prvoideály a vidíme, že nejsou hlavní. Čísla 2 a 3 jsou ireducibilní prvky, jež vznikly dle důsledku 30 3. způsobem. Prvoideály tedy musejí po dvojicích být z inverzních tříd ideálů v třídové grupě $\mathcal{O}_K$. Označme si třídu, jejímž prvkem je ideál $(3, \omega)$, jako T. Potom nutně $(3, \omega - 1)$ leží v inverzní třídě T^{-1}. Zbývá určit, ve kterých třídách leží zbývající dva prvoideály.

Lemma 37. *Nechť $\mathcal{O}_K = \mathbb{Z}[\omega]$. Prvoideály $(3, \omega), (2, \omega - 1)$ leží ve stejné třídě ideálů třídové grupy $C(\mathcal{O}_K)$, označme onu třídu T. Prvoideály $(2, \omega), (3, \omega - 1)$ jsou oba prvky třídy T^{-1}.*

Důkaz. Zkusme vynásobit $(3, \omega)(2, \omega)$. Pokud výsledkem bude hlavní ideál, z důsledku 30 bude $(2, \omega) \in T^{-1}$.

$$(3, \omega)(2, \omega) = (6, 3\omega, 2\omega, \omega^2) = (6, \omega, \omega^2) = (6, \omega),$$

kde druhá rovnost platí, neboť $3\omega - 2\omega = \omega$, třetí rovnost je zřejmá.

Platí

$$\mathcal{N}((6, \omega)) = \mathcal{N}((2, \omega)) \cdot \mathcal{N}((3, \omega)) = 2 \cdot 3 = 6,$$

kde hodnoty norem ideálů $(2,\omega)$ a $(3,\omega)$ známe z věty 34. Spočteme normu ω:

$$\mathcal{N}(\omega) = \mathcal{N}\left(\frac{1+\sqrt{-23}}{2}\right) = \frac{1}{4} + \frac{23}{4} = \frac{24}{4} = 6.$$

Zřejmě $\omega \in (6,\omega)$, což implikuje $(\omega) \subset (6,\omega)$. Jelikož mají stejné normy (norma prvku je stejná jako norma hlavního ideálu oním prvkem generovaným), musejí se rovnat. Spočetli jsme, že $(2,\omega)(3,\omega) = (\omega)$, totiž hlavní ideál, z čehož plyne, že $(2,\omega) \in T^{-1}$ a $(2,\omega-1) \in T$. □

Zbývá ukázat ireducibilitu čísla 7.

Lemma 38. *V číselném okruhu $\mathbb{Z}[\omega]$ je číslo 7 ireducibilní a hlavní ideál (7) je prvoideál.*

Důkaz. Aplikujeme větu 34 a podíváme se na polynom $g_\omega(x)$ jakožto na prvek okruhu $\mathbb{Z}/7\mathbb{Z}[x]$. Pokud by nebyl ireducibilní, platila by rovnost $x^2 - x + 6 = (x-a)(x-b), a, b \in \mathbb{Z}/7\mathbb{Z}$. Potom by čísla a i b byla kořeny polynomu $g_\omega(x)$. Dosazením všech prvků tělesa $\mathbb{Z}/7\mathbb{Z}$ zjistíme, že polynom nemá žádný kořen, tudíž musí být ireducibilní. Ideál (7) je proto dle zmiňované věty prvoideál v $\mathbb{Z}[\omega]$.

Jelikož je (7) hlavní prvoideál, z důsledku 30 plyne, že 7 je ireducibilní prvek. □

Pro shrnutí jsme nabyli vědomostí, že čísla 2, 3 a 7 jsou ireducibilní v $\mathbb{Z}[\omega]$, (7) je hlavní prvoideál, $(3,\omega), (2,\omega-1)$ jsou nehlavní prvoideály z třídy T a $(3,\omega-1), (2,\omega)$ jsou prvky třídy T^{-1}.

4.2 Ireducibilní rozklad čísla 6

Už se můžeme podívat na ireducibilní rozklad čísla 6.

Tvrzení 39. *V číselném okruhu $\mathbb{Z}[\omega]$ má číslo 6 právě dva následující ireducibilní rozklady:*

$$6 = 2 \cdot 3 = \frac{1+\sqrt{-23}}{2} \cdot \frac{1-\sqrt{-23}}{2}.$$

Důkaz. V $\mathbb{Z}$ je $6 = 2{\cdot}3$, stejná rovnost platí i pro hlavní ideály, to jest $(6) = (2){\cdot}(3)$. Díky lemmatům 35 a 36 víme, že 2 i 3 jsou ireducibilní v $\mathbb{Z}[\omega]$ a známe rozklad na prvoideály příslušných hlavních ideálů (2) a (3). Tudíž můžeme psát:

$$(6) = (2,\omega)(2,\omega-1)(3,\omega)(3,\omega-1),$$

kde $(3,\omega), (2,\omega-1)$ jsou nehlavní prvoideály z třídy T a $(2,\omega), (3,\omega-1)$ jsou nehlavní prvoideály z třídy T^{-1} (lemma 37). Protože máme pouze 2 nehlavní prvoideály z jedné třídy, ireducibilní rozklad nebude příliš zajímavý. Z důsledku 30 vidíme, že jediný způsob, jak získat ireducibilní rozklad, je vynásobení dvou nehlavních prvoideálů z jiných tříd. Číslo 6 lze tedy v $\mathbb{Z}[\omega]$ rozložit právě dvěma

způsoby na ireducibilní prvočinitele, které budou odpovídat následujícím dvěma možnostem:

$$(6) = \Big((2,\omega)(2,\omega-1)\Big)\cdot\Big((3,\omega)(3,\omega-1)\Big);$$

$$(6) = \Big((2,\omega)(3,\omega)\Big)\cdot\Big((2,\omega-1)(3,\omega-1)\Big).$$

Všimněme si, že tyto hodnoty už známe. Součiny z první možnosti jsou rozklady na prvoideály postupně (2) a (3), proto první z možností odpovídá ireducibilnímu rozkladu $6 = 2\cdot 3$. Z důkazu lemmatu 37 máme $(3,\omega)(2,\omega) = (\omega)$, takže druhý činitel z rozkladu 6 odpovídá výrazu $\frac{6}{\omega}$, což už není těžké dopočíst. Ireducibilní rozklad z druhé možnosti tedy odpovídá rozkladu $6 = \frac{1+\sqrt{-23}}{2}\cdot\frac{1-\sqrt{-23}}{2}$. □

Pro tento případ můžeme počet ireducibilních rozkladů zkontrolovat s důsledkem 33, jelikož všechny prvoideály v rozkladu (6) jsou navzájem různé. Dosazením do vzorce, kde v našem případě $n = 0, m = k = 2$, dostaneme výpočet:

$$\left(2!\binom{2}{2}\binom{2}{2}\prod_{i=1}^{0}\binom{3i-1}{2}\prod_{j=1}^{0}\binom{3j-1}{2}\right) = 2,$$

což odpovídá počtu rozkladů, jež jsme spočetli.

4.3 Ireducibilní rozklad čísla 18

V této sekci spočteme ireducibilní rozklady čísla 18 v $\mathbb{Z}[\omega]$. Tam už nastane zajímavější situace.

Tvrzení 40. *V číselném okruhu $\mathbb{Z}[\omega]$ má číslo 18 právě následující ireducibilní rozklady:*

$$18 = \left(\frac{7}{2}+\frac{\sqrt{-23}}{2}\right)\left(\frac{-7}{2}+\frac{\sqrt{-23}}{2}\right) = 3\left(\frac{1+\sqrt{-23}}{2}\right)\left(\frac{1-\sqrt{-23}}{2}\right) = 3\cdot 3\cdot 2.$$

Důkaz. Nejprve pišme $18 = 3\cdot 3\cdot 2$, převedeno do řeči hlavních ideálů pak

$$(18) = (3)(3)(2) = (3,\omega)(3,\omega-1)(3,\omega)(3,\omega-1)(2,\omega)(2,\omega-1),$$

kde $(3,\omega), (2,\omega-1)$ jsou prvoideály v T a $(2,\omega), (3,\omega-1)$ jsou prvoideály v T^{-1}, dle lemmat ze sekce 4.1. Protože máme právě 3 nehlavní prvoideály z každé třídy, počet t ireducibilních prvků v rozkladu 18 vzniklých vynásobením dvou ideálů z tříd T, T^{-1} bude dle tvrzení 31 roven buďto 0, nebo 3. Případy si rozebereme zvlášť.

$\underline{t = 0}$: V tomto případě máme pouze jednu možnost, jak vytvořit ireducibilní rozklad, a to vynásobit všechny 3 prvoideály z T a zvlášť z T^{-1}. Ireducibilní rozklad odpovídá následujícímu rozkladu na prvoideály:

$$(18) = \Big((3,\omega)^2(2,\omega-1)\Big)\cdot\Big((2,\omega)(3,\omega-1)^2\Big).$$

To je dle lemmatu 41 rovno $18 = \left(\frac{7}{2}+\frac{\sqrt{-23}}{2}\right)\left(\frac{-7}{2}+\frac{\sqrt{-23}}{2}\right)$.

$\underline{t=3}$: Toto je zajímavější případ, neboť je potřeba vytvořit ireducibilní prvky z dvou prvoideálů různých tříd. Protože prvoideálů není příliš a navíc jsou nějaké stejné, dostaneme jen 2 možnosti na ireducibilní rozklad odpovídající následujícím součinům:

$$(18) = \Big((3,\omega)(2,\omega)\Big)\cdot\Big((3,\omega)(3,\omega-1)\Big)\cdot\Big((2,\omega-1)(3,\omega-1)\Big);$$
$$(18) = \Big((3,\omega)(3,\omega-1)\Big)^2\cdot\Big((2,\omega)(2,\omega-1)\Big).$$

Tyto součiny už známe z tvrzení 39 o ireducibilním rozkladu čísla 6. Odpovídají po řadě rozkladům:

$$18 = 3\left(\frac{1+\sqrt{-23}}{2}\right)\left(\frac{1-\sqrt{-23}}{2}\right) = 3\cdot 3\cdot 2. \qquad \square$$

Lemma 41. *V číselném okruhu $\mathbb{Z}[\omega]$ platí následující rovnost ideálů:*

$$(18) = \Big((3,\omega)^2(2,\omega-1)\Big)\cdot\Big((2,\omega)(3,\omega-1)^2\Big) = \left(\frac{7}{2}+\frac{\sqrt{-23}}{2}\right)\left(\frac{-7}{2}+\frac{\sqrt{-23}}{2}\right).$$

Důkaz. Místo samotného násobení nehlavních ideálů na levé straně, které je složité, opět využijeme normy. Z multiplikativity normy a za využití věty 34, díky které známe normu všech nehlavních prvoideálů ze znění lemmatu, spočteme

$$\mathcal{N}\Big(\Big((3,\omega)^2(2,\omega-1)\Big)\Big) = \mathcal{N}\Big(\Big((2,\omega)(3,\omega-1)^2\Big)\Big) = 3\cdot 3\cdot 2 = 18.$$

Dále využijeme znalosti, že výsledek bude součin dvou hlavních ideálů (tvrzení 30), jelikož všechny tři nehlavní prvoideály v obou závorkách jsou ve stejných třídách dle lemmatu 37. Navíc budou také normy 18. Stačí nám proto zjistit, jaká čísla normy 18 v $\mathbb{Z}[\omega]$ existují. Vezměme si obecný prvek tvaru $\frac{a}{2}+\frac{b}{2}\sqrt{-23}, a, b \in \mathbb{Z}$ a řešme následující rovnici:

$$\frac{a^2}{4} + 23\cdot\frac{b^2}{4} = 18;$$
$$a^2 + 23b^2 = 72.$$

Pro $b = 0$ rovnice nemá řešení, poněvadž 72 není čtverec. Pro $b = 1$ dostaneme:

$$a^2 + 23 = 72;$$
$$a^2 = 49;$$
$$a = \pm 7.$$

Pro $b > 1$ už rovnice zřejmě nemá řešení.

Zjišťujeme, že prvky normy 18 jsou v $\mathbb{Z}[\omega]$ právě dva (až na vynásobení invertibilními prvky, tj. -1), a to prvky $\frac{7}{2}+\frac{\sqrt{-23}}{2}, \frac{-7}{2}+\frac{\sqrt{-23}}{2}$. Není těžké ověřit, že jediná možnost, jak z těchto dvou čísel dostat rozklad (18), je právě $(18) = \left(\frac{7}{2}+\frac{\sqrt{-23}}{2}\right)\left(\frac{-7}{2}+\frac{\sqrt{-23}}{2}\right)$. $\square$

Tímto je důkaz věty 40 o ireducibilních rozkladech 18 kompletní. Poznamenejme, že sice nevíme, jaký z ireducibilních prvků odpovídá jakému ze součinů nehlavních prvoideálů. To nám ale nevadí, využili jsme pouze znalost toho, že výsledkem bude hlavní ideál normy 18, a z toho už jsme onen ireducibilní rozklad zvládli najít. Víc to pro nás už není důležité.

Dále poznamenejme, že jsme našli rozklady 18 různých délek. Jasně proto vidíme, že $\mathbb{Z}[\omega]$ opravdu není pologaussovský, a tudíž jeho třídové číslo je větší než 2.

4.4 Ireducibilní rozklad čísla 126

Máme ireducibilní rozklad čísla 18, v rozkladu na prvoideály (18) se však nevyskytuje žádný hlavní prvoideál. Zkusíme najít takové číslo, jímž generovaný hlavní ideál bude obsahovat provideály ze všech tří tříd ideálů třídové grupy $C(\mathbb{Z}[\omega])$. Díky lemmatu 38 víme, že (7) je hlavní prvoideál a 7 je ireducibilní prvek. Protože $126 = 18 \cdot 7$, můžeme už poměrně snadno dostat ireducibilní rozklad 126.

Tvrzení 42. *V číselném okruhu $\mathbb{Z}[\omega]$ mají hlavní ideál* (126) *a číslo* 126 *následující rozklad na prvoideály a ireducibilní rozklad:*

$$\begin{aligned}(126) &= (7)(3)(3)(2) = (7)(3,\omega)(3,\omega-1)(3,\omega)(3,\omega-1)(2,\omega)(2,\omega-1);\\ 126 &= 7\left(\frac{7}{2}+\frac{\sqrt{-23}}{2}\right)\left(\frac{-7}{2}+\frac{\sqrt{-23}}{2}\right) = 7\cdot 3\left(\frac{1+\sqrt{-23}}{2}\right)\left(\frac{1-\sqrt{-23}}{2}\right) =\\ &= 7\cdot 3\cdot 3\cdot 2.\end{aligned}$$

Důkaz. Plyne z ireducibilního rozkladu 18 (tvrzení 40) a lemmatu o ireducibilitě 7 (lemma 38). □

Vidíme, že přidáním libovolného násobku čísla 7 se nemění počet ireducibilních rozkladů a pouze se přidávají mocniny 7 do rozkladu. Tudíž určit ireducibilní rozklad není vůbec těžké a můžu si přidávat libovolný počet těchto hlavních ideálů. Takže už dokážu snadno určit následující ireducibilní rozklady:

$$\begin{aligned}882 &= 7^2\left(\frac{7}{2}+\frac{\sqrt{-23}}{2}\right)\left(\frac{-7}{2}+\frac{\sqrt{-23}}{2}\right) =\\ &= 7^2\cdot 3\left(\frac{1+\sqrt{-23}}{2}\right)\left(\frac{1-\sqrt{-23}}{2}\right) = 7^2\cdot 3\cdot 3\cdot 2;\\ 43\,218 &= 7^4\left(\frac{7}{2}+\frac{\sqrt{-23}}{2}\right)\left(\frac{-7}{2}+\frac{\sqrt{-23}}{2}\right) =\\ &= 7^4\cdot 3\left(\frac{1+\sqrt{-23}}{2}\right)\left(\frac{1-\sqrt{-23}}{2}\right) = 7^4\cdot 3\cdot 3\cdot 2;\\ 14\,823\,774 &= 7^7\left(\frac{7}{2}+\frac{\sqrt{-23}}{2}\right)\left(\frac{-7}{2}+\frac{\sqrt{-23}}{2}\right) =\\ &= 7^7\cdot 3\left(\frac{1+\sqrt{-23}}{2}\right)\left(\frac{1-\sqrt{-23}}{2}\right) = 7^7\cdot 3\cdot 3\cdot 2.\end{aligned}$$

A dokonce obecně pro $k \in \mathbb{N}$:

$$\begin{aligned}7^k\cdot 18 &= 7^k\left(\frac{7}{2}+\frac{\sqrt{-23}}{2}\right)\left(\frac{-7}{2}+\frac{\sqrt{-23}}{2}\right) =\\ &= 7^k\cdot 3\left(\frac{1+\sqrt{-23}}{2}\right)\left(\frac{1-\sqrt{-23}}{2}\right) = 7^k\cdot 3\cdot 3\cdot 2.\end{aligned}$$

Závěr

Přirozená otázka, která po přečtení práce vyplyne, je, zda by se dalo v duchu třetí kapitoly pokračovat i v okruzích s vyššími třídovými čísly. Už pro třídové číslo rovno 4 by pravděpodobně nastala zajímavá a komplikovanější situace, jelikož grupy o 4 prvcích známe 2. Třídová grupa by tedy neměla jednoznačně určenou strukturu a byla by izomorfní buď $\mathbb{Z}/4\mathbb{Z}$, nebo $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Charakterizační věty by pak asi závisely na tom, jakou podobu by třídová grupa měla. Pro ještě vyšší čísla by těchto grup mohlo být ještě víc. Vyplývá poté například otázka, pro jaké grupy vůbec existuje číselný okruh $\mathcal{O}_K$ takový, že jeho třídová grupa je izomorfní dané grupě. Ve své práci jsem se věnovala nejednoznačným ireducibilním rozkladům, k čemuž se hodila definice třídového čísla a práce s ideály. Samotná definice třídové grupy byla spíše pomocná pouze k dostání těchto vět. Jistě by bylo také zajímavé se zaměřit na to, co samotná třídová grupa a její struktura říká o okruzích a jejich ideálech.

Dále by šlo dopočítat počet ireducibilních rozkladů z důsledků 25 a 33. Jsou to zajímavé kombinatorické úlohy, které však pro mou práci nejsou zásadní. Proto jsem se jimi kvůli netriviální kombinatorické stránce nezabývala.

Seznam použité literatury

[1] Anderson, D., Anderson, D. a Zafrullah, M. (1991). Rings between d[x] and k[x]. *Houston Journal of Mathematics*, **17**.

[2] Chapman, S. T. (2019). So what is class number 2? *The American Mathematical Monthly*, **126**(4), 330–339. doi: 10.1080/00029890.2019.1562827. URL https://doi.org/10.1080/00029890.2019.1562827.

[3] Chapman, S. T. a Coykendall, J. (2000). *Half-Factorial Domains, a Survey*, pages 97–115. Springer US, Boston, MA. ISBN 978-1-4757-3180-4. doi: 10.1007/978-1-4757-3180-4_5. URL https://doi.org/10.1007/978-1-4757-3180-4_5.

[4] Conrad, K. (2023). Ideal fatorization. URL https://kconrad.math.uconn.edu/blurbs/gradnumthy/idealfactor.pdf. [Online; accessed 18 March 2024].

[5] Kala, V. (2023). Úvod do komutativní algebry. URL https://karlin.mff.cuni.cz/~kala/files/UKA22.pdf. [Online; accessed 18 March 2024].

[6] LMFDB Collaboration, T. (2024). The L-functions and modular forms database, home page of the number field 2.0.23.1. https://www.lmfdb.org/NumberField/2.0.23.1. [Online; accessed 20 March 2024].

[7] Marcus, D. A. (2018). *Number fields*. Universitext. Springer, Cham, second edition. ISBN 978-3-319-90232-6; 978-3-319-90233-3. doi: 10.1007/978-3-319-90233-3. URL https://doi.org/10.1007/978-3-319-90233-3. With a foreword by Barry Mazur.

[8] Pollard, H. a Diamond, H. G. (1998). *The theory of algebraic numbers*. Dover Publications, Inc., Mineola, NY, third edition. ISBN 0-486-40454-4.