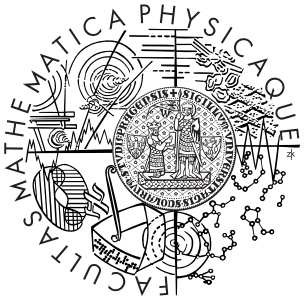
Univerzita Karlova v Praze
Matematicko-fyzikální fakulta

BAKALÁŘSKÁ PRÁCE



Aleš Fuchs

Dedekindovy obory a jejich zobecnění

Katedra algebry

Vedoucí bakalářské práce: Doc. RNDr. Jan Trlifaj, CSc., DSc.
Studijní program: Matematika, Obecná matematika
2009

Chtěl bych poděkovat zejména Doc. RNDr. Janovi Trlifajovi, DSc. za příkladné a trpělivé vedení mé bakalářské práce. Dále také své rodině za podporu a zázemí v době studia.

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

V Praze dne 2. března 2009 Aleš Fuchs

Obsah

Název práce: Dedekindovy obory a jejich zobecnění
Autor: Aleš Fuchs
Katedra: Katedra algebry
Vedoucí bakalářské práce: Doc. RNDr. Jan Trlifaj, CSc., DSc.
e-mail vedoucího: trlifaj@karlin.mff.cuni.cz

Abstrakt: V této práci studujeme vlastnosti Dedekindových oborů, jež patří mezi komutativní noetherovské okruhy, a jejich lomených ideálů. Dále se zabýváme konečně generovanými moduly nad Dedekindovými obory. Zkoumání projektivních modulů využíváme pro rozklad modulu na direktní součet torzní a beztorzní složky. Zkoumání modulů nad valuačními okruhy pak uplatňujeme při rozkladu torzní složky modulu, což nám dává jeho celkovou klasifikaci. V třetí kapitole uvádíme mimo jiné dva důležité a historicky motivační zdroje příkladů Dedekindových oborů, algebraická celá čísla a kvadratické řády. Nakonec zmiňujeme stěžejní poznatky z odvětví reprezentačních typů komutativních noetherovských okruhů.

Klíčová slova: Dedekindovy obory, komutativní noetherovské okruhy

Title: Dedekind and Dedekind-like rings
Author: Aleš Fuchs
Department: Department of Algebra
Supervisor: Doc. RNDr. Jan Trlifaj, CSc., DSc.
Supervisor's e-mail address: trlifaj@karlin.mff.cuni.cz

Abstract: In the present paper we study properties of Dedekind domains, which belong to commutative Noetherian rings, and their fractional ideals. Further we deal with finitely generated modules over Dedekind domains. We exploit properties of projective modules to decompose the module to the direct sum of it's torsion and torsion-free parts. We apply the investigation of modules over valuation rings to decomposing the torsion part, which gives us a complete classification of a module. In the third chapter We also present two important sources of examples of Dedekind domains, namely the algebraic integers and the quadratic orders. Finally we record crucial results from a branch of representation types of commutative Noetherian rings.

Keywords: Dedekind domains, commutative noetherian rings

Kapitola 1

Dedekindovy obory

V této kapitole uvedeme základní pojmy, jako lomený ideál, Dedekindův obor a grupa tříd. Kromě elementárních vlastností definovaných pojmů bude dokázána také Věta o jednoznačnosti rozkladu ideálů Dedekindova oboru.

Teorie Dedekindových oborů má kořeny na přelomu devatenáctého a dvacátého století, a vychází z práce slavného německého matematika Richarda Dedekinda (1831-1916), který byl posledním žákem Friedricha Gausse a během svého života spolupracoval například s Johannem Dirichletem nebo Georgem Riemannem. Dedekind během svého života významně přispěl k rozvoji matematiky a k terminologii, kterou dnes používáme.

Předpokládejme všechny okruhy v následujícím textu komutativní, tedy všechny ideály uvažujme oboustranné. Všechny moduly berme jako bimoduly.

1.1 Základní poznatky a invertibilní ideály

Definice 1.1.1 (Lomené ideály)**.** Buď $\mathcal{O}$ komutativní noetherovský obor integrity a $\mathcal{K}$ jeho podílové těleso. *Lomeným ideálem* oboru $\mathcal{O}$ nazveme nenulový konečně generovaný $\mathcal{O}$-podmodul tělesa $\mathcal{K}$. Mezi lomené ideály patří i hlavní ideály $\mathcal{O}x$, kde x je libovolný nenulový prvek $\mathcal{K}$ a také všechny ideály oboru $\mathcal{O}$. Lomené ideály které jsou zároveň ideály oboru $\mathcal{O}$ nazýváme *celistvé ideály.*

$\mathrm{Frac}(\mathcal{O})$ označuje množinu všech lomených ideálů, $\mathrm{Pr}(\mathcal{O})$ pak množinu všech hlavních ideálů.

Definujeme součin prvků $\mathfrak{a}, \mathfrak{b} \in \mathrm{Frac}(\mathcal{O})$ analogicky jako součin ideálů:

$$\mathfrak{ab} = \{a_1b_1 + \cdots + a_kb_k | a_i \in \mathfrak{a}, b_i \in \mathfrak{b}, k \geq 0\}.$$

O lomeném ideálu $\mathfrak{a}$ komutativního oboru integrity $\mathcal{O}$ řekneme, že je invertibilní, pokud existuje takový lomený ideál $\mathfrak{a}^{-1} \in \mathcal{O}$, pro který platí

$$\mathfrak{a}\mathfrak{a}^{-1} = \mathcal{O}.$$

Množina invertibilních lomených ideálů tvoří abelovskou multiplikativní grupu, která je podmnožinou Frac($\mathcal{O}$). Do této grupy zřejmě patří všechny nenulové hlavní lomené ideály. (Inverzní ideál každého invertibilního lomeného ideálu je určen jednoznačně)

Lemma 1.1.2. *Nechť $\mathcal{O}$ je komutativní noetherovský obor integrity, $\mathcal{K}$ jeho podílové těleso a $\mathfrak{a}$ buď $\mathcal{O}$-podmodul $\mathcal{K}$. Potom následující tvrzení jsou ekvivalentní:*

(i) $\mathfrak{a} \in$ *Frac($\mathcal{O}$),*

(ii) $\mathcal{O}c \subseteq \mathfrak{a} \subseteq \mathcal{O}d^{-1}$ *pro nějaké nenulové* $c, d \in \mathcal{O}$,

Důkaz. Toto je známým faktem, který lze nalézt v [BK]. ⊠

Definice 1.1.3. Nechť R je podokruh okruhu S a $s \in S$. Řekneme, že s je *celistvý* nad R právě když je kořenem nějakého monického polynomu z $R[x]$. Množina všech prvků z S celistvých nad R se nazývá *celistvý uzávěr* R v S.

Definice 1.1.4 (Dedekindův obor)**.** Komutativní noetherovský obor integrity $\mathcal{O}$ se nazývá *Dedekindův obor*, pokud je každý jeho lomený ideál invertibilní.

Existují i další alternativní definice, jejichž podmínky jsou s touto ekvivalentní. Některé pojmy, které zde uvedeme, budou definovány později:

(i) Každý jeho lomený ideál je projektivní (lomený ideál je invertibilní právě když je projektivní).

(ii) Podmodul jeho projektivního modulu je opět projektivní (dědičnost).

(iii) Jedná se o celistvě uzavřený noetherovský obor integrity s Krullovou dimenzí (menší) rovnou jedné (pro dimenzi rovnou nule se jedná o triviální případ, kdy každé těleso je Dedekindův obor a tedy ho nebudeme dále uvažovat). Jinými slovy komutativní obor integrity, který je celistvě uzavřen ve svém podílovém tělese, kde je každý nenulový celistvý ideál konečně generovaný a kde každý nenulový prvoideál je zároveň maximálním ideálem.

(iv) Jedná se o obor integrity, kde každý nenulový celistvý ideál je konečným součinem prvoideálů, které jsou (až na pořadí) jednoznačně určené.

Definice 1.1.5 (Grupa tříd)**.** $\mathrm{Pr}(\mathcal{O})$ je zřejmě podgrupa multiplikativní abelovské grupy $\mathrm{Frac}(\mathcal{O})$. *Třídou* lomeného ideálu $\mathfrak{a}$ je množina lomených ideálů tvaru $\mathfrak{a}x$, kde x je libovolným nenulovým prvkem $\mathcal{K}$. Množina všech takových tříd ideálů se součinem definovaným jako výše je tzv. *grupa tříd* a značíme ji $\mathcal{C}l(\mathcal{O})$. Je kvocientem

$$\mathcal{C}l(\mathcal{O}) = \mathrm{Frac}(\mathcal{O})/\mathrm{Pr}(\mathcal{O}).$$

Třídu lomeného ideálu $\mathfrak{a}$ značíme $[\mathfrak{a}] \in \mathcal{C}l(\mathcal{O})$. Zřejmě Dedekindův obor $\mathcal{O}$ je obor hlavních ideálů právě když platí $\mathcal{C}l(\mathcal{O}) = 1$.

Určení grupy tříd konkrétního Dedekindova oboru je obvykle obtížný problém. Na druhé straně je každá abelovská grupa izomorfní grupě tříd nějakého Dedekindova oboru, což dokazuje hluboká Věta Clabornova z roku 1966 (viz. [Cl]), o které je dále pojednáno ve [Foss, 14.10].

Pro důkaz následujícího tvrzení zavedeme pojem torzního modulu, tento ještě využijeme v druhé kapitole, kde budeme podrobněji zkoumat moduly nad Dedekindovými obory.

Definice 1.1.6 (Torzní modul)**.** Buď M modul nad komutativním oborem integrity $\mathcal{O}$. Řekneme, že prvek $m \in M$ je *torzní*, pokud $mr = 0$ pro nějaký $0 \neq r \in \mathcal{O}$. Množina všech torzních prvků M se značí $T(M)$ a nazývá torzní podmodul modulu M.

Řekneme, že M je *torzní modul*, jestliže $M = T(M)$, a naopak M je *beztorzní modul*, pokud $T(M) = 0$. Zřejmě $T(M)$ je torzní modul a $M/T(M)$ je beztorzní modul, stejně jako O^k a všechny jeho podmoduly.

Tvrzení 1.1.7. *Nechť $\mathfrak{a}, \mathfrak{b}$ jsou lomené ideály Dedekindova oboru $\mathcal{O}$. Potom $[\mathfrak{a}] = [\mathfrak{b}]$ v $\mathcal{C}l(\mathcal{O})$ právě když existuje $\mathcal{O}$-modulový izomorfismus $\mathfrak{a} \cong \mathfrak{b}$.*

Navíc pro daný lomený ideál $\mathfrak{a}$ existuje celistvý ideál $\mathfrak{b}$ takový, že $[\mathfrak{a}] = [\mathfrak{b}]$.

Důkaz. Jestliže $[\mathfrak{a}] = [\mathfrak{b}]$, potom dle definice $\mathfrak{a} = \mathfrak{b}x$ pro nějaký prvek x podílového tělesa $\mathcal{K}$ oboru $\mathcal{O}$, a izomorfismus je dán jednoduše násobením x.

Naopak předpokládejme, že $\alpha : \mathfrak{a} \to \mathfrak{b}$ je $\mathcal{O}$-modulový izomorfismus, bez újmy na obecnosti $\mathfrak{a} \neq 0$. Tedy $\alpha(\frac{p_1}{q_1}) = \frac{p_2}{q_2}$ pro nějaké $p_1, p_2, q_1, q_2 \in \mathcal{O}$,

kde $p_1 \neq 0, q_1 \neq 0, q_2 \neq 0 \in \mathcal{O}$ a $\frac{p_1}{q_1} \in \mathfrak{a}$. Definujme dále $\alpha' : \mathfrak{a} \to \mathcal{K}$, $k \mapsto (\frac{q_1}{p_1} \cdot \frac{p_2}{q_2})k$. Pak zřejmě platí $\mathrm{Ker}(\alpha - \alpha') \neq 0$. Potom ale homomorfismus $\mathfrak{a}/\mathrm{Ker}(\alpha - \alpha') \hookrightarrow \mathcal{K}$ zobrazuje torzní modul na beztorzní. Není tedy jiná možnost, než že $\mathrm{Ker}(\alpha - \alpha') = \mathfrak{a}$, a tedy $\alpha = \alpha'$ na $\mathfrak{a}$. Zobrazení α je tudíž definované násobením konstantou $x = \frac{q_1}{p_1} \cdot \frac{p_2}{q_2}$ a tedy $\mathfrak{a}x = \mathfrak{b}$.

Pro dané $\mathfrak{a}$ existuje prvek $d \in \mathcal{O}$, pro který je $\mathfrak{b} = \mathfrak{a}d$ celistvý, což dává závěrečné tvrzení. ⊠

Lemma 1.1.8. *Buď $\mathfrak{a}$ lomený ideál Dedekindova oboru $\mathcal{O}$. Pak*

(i) $\mathfrak{a}^{-1} = \{x \in \mathcal{K} | x\mathfrak{a} \subseteq \mathcal{O}\}$,

(ii) jestliže je $\mathfrak{b}$ lomený ideál, pro který platí $\mathfrak{b} \subseteq \mathfrak{a}$, potom $\mathfrak{a}^{-1} \subseteq \mathfrak{b}^{-1}$.

Důkaz. Toto je známým faktem, který lze nalézt v [BK]. ⊠

Zde se dalšími vlastnostmi inverzních ideálů dále zabývat nebudeme. Lze je nalézt například v [Dr, III.4].

Následuje věta, jíž Bourbaki považuje za „úhelný kámen této teorie“, a která říká, že každý nenulový ideál Dedekindova oboru lze rozložit na součin konečně mnoha navzájem různých nenulových prvoideálů umocněných nějakým kladným exponentem. Byla uvedena například v [Ded]. My tuto větu předvedeme v obecnějším tvaru pro všechny lomené ideály Dedekindova oboru.

Věta 1.1.9 (Jednoznačnost rozkladu lomených ideálů Dedekindova oboru)**.** *Buď $\mathfrak{a}$ lomený ideál Dedekindova oboru $\mathcal{O}$ a buď $\mathcal{P}$ množina všech nenulových prvoideálů oboru $\mathcal{O}$. Potom existují jednoznačně určená $v(\mathfrak{p}, \mathfrak{a}) \in \mathbb{Z}$ pro skoro všechna $\mathfrak{p} \in \mathcal{P}$ nulová, pro která platí:*

$$\mathfrak{a} = \prod_{\mathfrak{p} \in \mathcal{P}} \mathfrak{p}^{v(\mathfrak{p}, \mathfrak{a})}.$$

Důkaz. Nejprve dokážeme existenci rozkladu pro daný celistvý ideál $\mathfrak{a}$. Pro spor předpokládejme, že $\mathfrak{a}$ nemá takový rozklad. Zřejmě $\mathfrak{a}$ není maximální ideál (ani samotný obor $\mathcal{O}$). Tedy existuje nějaký maximální ideál $\mathfrak{p}_1$ oboru $\mathcal{O}$ obsahující $\mathfrak{a}$. Položme $\mathfrak{a}_1 = \mathfrak{a}\mathfrak{p}_1^{-1}$, který je obsažen v $\mathfrak{a}\mathfrak{a}^{-1}$ podle Lemmatu 1.1.8. Tudíž $\mathfrak{a}_1$ je celistvý a $\mathfrak{a} \subsetneq \mathfrak{a}_1$ (protože $\mathfrak{p}_1 \subsetneq \mathcal{O}$). Naopak $\mathfrak{a}_1$ nemůže být maximální (nebo rovno $\mathcal{O}$), jinak by se jednalo o rozklad ideálu $\mathfrak{a}$. Analogicky můžeme nalézt maximální ideál $\mathfrak{p}_2$, pro který $\mathfrak{a}_1 \subsetneq \mathfrak{a}_1\mathfrak{p}_2^{-1} = \mathfrak{a}_2$. Takto bychom

získali nekonečný řetězec ideálů oboru $\mathcal{O}$, což je spor s noetherovskostí oboru $\mathcal{O}$. Každý celistvý ideál lze tedy rozložit na součin nenulových prvoideálů.

Z Lemmatu 1.1.2 plyne, že pro libovolný lomený ideál $\mathfrak{a}$ existuje nenulový $d \in \mathcal{O}$ takový, že $\mathfrak{a}d \subseteq \mathcal{O}$. Tudíž $\mathfrak{a} = \mathfrak{b}\mathfrak{c}^{-1}$ pro celistvé ideály $\mathfrak{b}$ a $\mathfrak{c}$, a tedy $\mathfrak{a}$ může být vyjádřen jako součin nenulových prvoideálů.

Předpokládejme, že lomený ideál $\mathfrak{a}$ lze rozložit dvěma způsoby:

$$\mathfrak{p}_1 \cdots \mathfrak{p}_k = \mathfrak{q}_1 \cdots \mathfrak{q}_l,$$

kde $\mathfrak{p}_1, \ldots, \mathfrak{p}_k, \mathfrak{q}_1, \ldots, \mathfrak{q}_l$ jsou prvoideály, $k \geq 1$, $l \geq 1$ a $\mathfrak{p}_i \neq \mathfrak{q}_j$ pro každou dvojici i, j. Zvolme nějaké $q \in \mathfrak{q}_1 \setminus \mathfrak{p}_1$. Potom $q(\mathfrak{q}_2 \cdots \mathfrak{q}_l) \subseteq \mathfrak{p}_1$ a tedy také $\mathfrak{q}_2 \cdots \mathfrak{q}_l \subseteq \mathfrak{p}_1$. Stejným postupem nakonec dostaneme $\mathfrak{q}_l \subseteq \mathfrak{p}_1$, ale $\mathfrak{q}_l$ je maximální ideál dle 1.1.4 (iii), tedy $\mathfrak{q}_l = \mathfrak{p}_1$, což je spor. ⊠

Kapitola 2

Moduly nad Dedekindovými obory

2.1 Projektivní moduly nad Dedekindovými obory

Nyní, když jsme ustanovili základní vlastnosti Dedekindových oborů, zaměříme se na problém klasifikace jejich konečně generovaných modulů. Nejprve uvedeme strukturní větu pro projektivní moduly nad libovolným Dedekindovým oborem. Poté se zaměříme na případ, kdy je Dedekindův obor valuačním okruhem, tedy má pouze jeden nenulový prvoideál. Nakonec výsledky těchto dvou případů použijeme při rozkladu modulu na torzní a beztorzní část.

Definice 2.1.1 (Projektivní modul)**.** Buď R okruh. Řekneme, že R-modul P je *projektivní*, pokud pro každý epimorfizmus $\pi \in \mathrm{Hom}_R(A, B)$ a pro každý $f \in \mathrm{Hom}_R(P, B)$ existuje $g \in \mathrm{Hom}(P, A)$ takový, že $\pi \circ g = f$, pro libovolné R-moduly A, B.

Ekvivalentně může být projektivní modul definován tak, že pro každý epimorfizmus $f \in \mathrm{Hom}_R(M, P)$ existuje takový $h \in \mathrm{Hom}_R(P, M)$, že $f \circ h = id_P$.

Je dobře známým faktem, že R-modul P je projektivní právě když je izomorfní direktnímu sčítanci nějakého volného R-modulu.

Lemma 2.1.2. *Nechť $\mathfrak{a}, \mathfrak{b}$ jsou celistvé ideály Dedekindova oboru $\mathcal{O}$. Potom existuje $\mathcal{O}$-modulový izomorfismus*

$$\mathfrak{a} \oplus \mathfrak{b} \cong \mathcal{O} \oplus \mathfrak{ab}.$$

Důkaz. Nejprve předpokládejme, že $\mathfrak{a}$ a $\mathfrak{b}$ jsou komaximální. Definujme homomorfismus $\alpha : \mathfrak{a} \oplus \mathfrak{b} \to \mathcal{O}$ pomocí $\alpha(a, b) = a - b$. Potom α je surjektivní a Ker$\alpha = \mathfrak{a} \cap \mathfrak{b}$. Zřejmě $\mathfrak{ab} \subseteq \mathfrak{a} \cap \mathfrak{b}$. Naopak z komaximality ideálů $\mathfrak{a}, \mathfrak{b}$ plyne existence prvků $a \in \mathfrak{a}, b \in \mathfrak{b}$ takových, že $a + b = 1$. Tedy pro každé $x \in \mathfrak{a} \cap \mathfrak{b}$ platí $x = x1 \in \mathfrak{ab}$, a tedy Ker$\alpha = \mathfrak{ab}$. Pro komaximální ideály lemma platí.

Obecně, Tvrzení 1.1.7 říká, že existuje celistvý ideál $\mathfrak{a}' \cong \mathfrak{a}$ takový, že $\mathfrak{a}'$ a $\mathfrak{b}$ jsou komaximální, tudíž $\mathfrak{a}'\mathfrak{b} \cong \mathfrak{ab}$. ⊠

Důsledek 2.1.3. Lze dokázat, že předchozí Lemma platí i pro lomené ideály $\mathfrak{a}, \mathfrak{b}$ oboru $\mathcal{O}$. Dle 1.1.7 existuje $r \in \mathcal{O}$ takové, že $r\mathfrak{a} \subseteq \mathcal{O}$ je již ideál celistvý, a platí $\mathfrak{a} \cong r\mathfrak{a}$ a $\mathfrak{b} \cong s\mathfrak{b}$ pro vhodná r, s. Tudíž

$$\mathfrak{a} \oplus \mathfrak{b} \cong r\mathfrak{a} \oplus s\mathfrak{b} \cong \mathcal{O} \oplus r\mathfrak{a}s\mathfrak{b} \cong \mathcal{O} \oplus \mathfrak{ab}.$$

Důsledek 2.1.4. Speciálně pro každý lomený ideál $\mathfrak{a}$ Dedekindova oboru $\mathcal{O}$ platí

$$\mathfrak{a} \oplus \mathfrak{a}^{-1} \cong \mathcal{O} \oplus \mathfrak{a}\mathfrak{a}^{-1} = \mathcal{O} \oplus \mathcal{O} = \mathcal{O}^2.$$

Jak vidíme, pokud obor $\mathcal{O}$ není oborem hlavních ideálů, tedy pokud $\mathcal{C}l(\mathcal{O}) \neq 1$, existuje více direktních rozkladů modulu $\mathcal{O}^2$, kde sčítanci nemusí být vzájemně izomorfní. Tudíž pro Dedekindovy obory neplatí obecně Krull-Schmidtova věta, která právě o takovém rozkladu na jednoznačný počet nerozložitelných modulů hovoří.

Důsledek 2.1.5. Na druhou stranu vidíme, že každý celistvý ideál Dedekindova oboru $\mathcal{O}$ je maximálně 2-generovaný a projektivní.

Věta 2.1.6 (Kaplanského věta)**.** *Nechť $\mathcal{O}$ je okruh, jehož každý pravý ideál je jako $\mathcal{O}$-modul projektivní. Potom platí následující:*

(i) každý projektivní modul je izomorfní direktní sumě pravých ideálů,

(ii) podmodul projektivního modulu je projektivní.

Důkaz. Buď P projektivní $\mathcal{O}$-modul. Pak existují $\mathcal{O}$-modul P' a volný modul $\mathcal{O}^{(\kappa)}$ takové, že platí:

$$P \oplus P' = \mathcal{O}^{(\kappa)} = \bigcup_{\alpha<\kappa} \mathcal{O}_\alpha,$$

kde $\mathcal{O}_\alpha = \bigoplus_{0<\beta\leq\alpha} 1_\beta\mathcal{O}$ a kde 1_β značí β-tý prvek kanonické báze volného modulu $\mathcal{O}^{(\kappa)}$ pro $\beta < \kappa$.

Pro obě tvrzení tedy stačí dokázat, že každý podmodul $M \subseteq \mathcal{O}^{(\kappa)}$ je projektivní. Při označení $M_\alpha = M \cap \mathcal{O}_\alpha$ a použití vztahu $(A + B)/A \simeq B/(A \cap B)$, kde dosadíme $A = \mathcal{O}_\alpha$ a $B = M \cap \mathcal{O}_{\alpha+1}$, dostáváme

$$M_{\alpha+1}/M_\alpha = (M \cap \mathcal{O}_{\alpha+1})/(M \cap \mathcal{O}_\alpha) = \\ = (\mathcal{O}_\alpha + (M \cap \mathcal{O}_{\alpha+1}))/\mathcal{O}_\alpha \subseteq \mathcal{O}_{\alpha+1}/\mathcal{O}_\alpha \cong \mathcal{O}.$$

Tedy $M_{\alpha+1}/M_\alpha$ je izomorfní nějakému pravému ideálu okruhu $\mathcal{O}$, a tedy je projektivní dle předpokladu. Tudíž existují podmoduly $N_\alpha \subseteq M_{\alpha+1}$ takové, že $M_{\alpha+1} = M_\alpha \oplus N_\alpha$ (viz def. 2.1.1). Potom $M = \bigcup_{\alpha<\kappa} M_\alpha = \bigoplus_{\alpha<\kappa} N_\alpha$ je projektivní podmodul. ⊠

Důsledek 2.1.7. Celistvé ideály Dedekindova oboru jsou invertibilní, tudíž i projektivní. Dedekindovy obory jsou tedy dědičné, tzn. mají vlastnost uvedenou v 2.1.6, (ii).

Tvrzení 2.1.8. *Buď M modul nad Dedekindovým oborem $\mathcal{O}$. Potom následující tvrzení jsou ekvivalentní:*

(i) $M \cong \mathfrak{a}_1 \oplus \cdots \oplus \mathfrak{a}_s$ *pro nějakou konečnou množinu* $\{\mathfrak{a}_1, \ldots, \mathfrak{a}_s\}$ *ideálů oboru* $\mathcal{O}$.

(ii) M je konečně generovaný a projektivní jako $\mathcal{O}$-modul.

(iii) Existuje prostý homomorfismus $\sigma : M \to \mathcal{O}^t$ *pro nějaké přirozené* t.

Důkaz. $(iii)\Rightarrow(ii)$ Jak již bylo poznamenáno v Důsledku 2.1.7, Dedekindovy obory splňují podmínku Věty 2.1.6. Podle jejího důkazu platí $M \cong \bigoplus_{j<t} N_j$, kde N_j jsou pravé ideály oboru $\mathcal{O}$. Tedy M je konečně generovaný projektivní modul podle Důsledku 2.1.5. Navíc dle bodu (ii) je modul M projektivní.
$(ii)\Rightarrow(i)$ Důkaz plyne přímo z Kaplanského věty 2.1.6 a konečné generovanosti modulu M.
$(i)\Rightarrow(iii)$ Každý ideál $\mathfrak{a}_i$ lze vnořit do oboru $\mathcal{O}$, tudíž tvrzení platí pro $t = s$. ⊠

Věta 2.1.9 (Steinitzova věta)**.** *Nechť $\mathcal{O}$ je Dedekindův obor a* $\mathfrak{a}_1, \ldots, \mathfrak{a}_r$, $\mathfrak{b}_1, \ldots, \mathfrak{b}_s$ *jeho celistvé ideály. Potom jsou následující tvrzení ekvivalentní:*

(i) $\mathfrak{a}_1 \oplus \cdots \oplus \mathfrak{a}_r \cong \mathfrak{b}_1 \oplus \cdots \oplus \mathfrak{b}_s$,

(ii) $r = s$ *a* $[\mathfrak{a}_1 \cdots \mathfrak{a}_r] = [\mathfrak{b}_1 \cdots \mathfrak{b}_r]$ *v* $\mathcal{C}l(\mathcal{O})$*.*

Důkaz. $(i) \Rightarrow (ii)$: Buď $\mathcal{K}$ podílové těleso oboru $\mathcal{O}$ a buď $\phi : \mathfrak{a}_1 \oplus \cdots \oplus \mathfrak{a}_r \to \mathfrak{b}_1 \oplus \cdots \oplus \mathfrak{b}_s$ daný izomorfismus. Buď $x = (x_1, \dots x_r)$ prvek $\mathcal{K}^r$. Potom každé x_i lze vyjádřit jako c_i/d_i pro nějaká $c_i \in \mathfrak{a}_i,\ d_i \in \mathcal{O}$, kde $i = 1, \dots, r$. Tedy pro $d = d_1 \cdots d_r$ platí $x = a/d$ pro nějaké $a \in \mathfrak{a}_1 \oplus \cdots \oplus \mathfrak{a}_r$. Rozšířením ϕ na zobrazení $\phi' : \mathcal{K}^r \to \mathcal{K}^s$, pro které $\phi'(x) = \phi(a)/d$. Není těžké ověřit, že ϕ je dobře definované $\mathcal{K}$-lineární zobrazení a navíc izomorfismus $\mathcal{K}$-prostorů. Tudíž $r = s$ a ϕ i ϕ' jsou reprezentována násobením zleva maticí $Q = (q_{ij})$ nad $\mathcal{K}$. Platí že matice Q je určena jednoznačně až na konjugovanost, tedy, že její determinant $\det(Q)$ je určen jednoznačně.

Mějme

$$a = \begin{pmatrix} \mathfrak{a}_1 \\ \vdots \\ \mathfrak{a}_r \end{pmatrix} \in \mathfrak{a}_1 \oplus \cdots \oplus \mathfrak{a}_r.$$

Z $Qa \in \mathfrak{b}_1 \oplus \cdots \oplus \mathfrak{b}_r$ plyne $\sum_j q_{ij} a_j \in \mathfrak{b}_i$ pro všechna i. Speciálně v případě $a_h = 0$ pro $h \neq j$, platí, že $q_{ij} a_j \in \mathfrak{b}_i$ pro všechna i, j. Tedy

$$\begin{aligned} \det(Q) \cdot a_1 \cdots a_r =& \det(Q \cdot \operatorname{diag}(a_1, \dots, a_r)) \\ =& \det \begin{pmatrix} q_{11}a_1 & \cdots & q_{1r}a_r \\ \vdots & \ddots & \vdots \\ q_{r1}a_1 & \cdots & q_{rr}a_r \end{pmatrix} \\ \in& \mathfrak{b}_1 \cdots \mathfrak{b}_r. \end{aligned}$$

Protože je $\mathfrak{a}_1 \oplus \cdots \oplus \mathfrak{a}_r$ generován všemi násobky $a_1 \cdots a_r$, platí

$$\det(Q)\mathfrak{a}_1 \cdots \mathfrak{a}_r \subseteq \mathfrak{b}_1 \cdots \mathfrak{b}_r.$$

Analogicky $\det(Q^{-1})\mathfrak{b}_1 \cdots \mathfrak{b}_r \subseteq \mathfrak{a}_1 \cdots \mathfrak{a}_r$, což dává

$$[\mathfrak{a}_1 \cdots \mathfrak{a}_r] = [\mathfrak{b}_1 \cdots \mathfrak{b}_r].$$

$(ii) \Rightarrow (i)$: Indukcí z 2.1.2 dostaneme:

$$\begin{aligned} \mathfrak{a}_1 \oplus \cdots \oplus \mathfrak{a}_r &\cong \mathcal{O}^{r-1} \oplus \mathfrak{a}_1 \cdots \mathfrak{a}_r, \\ \mathfrak{b}_1 \oplus \cdots \oplus \mathfrak{b}_r &\cong \mathcal{O}^{r-1} \oplus \mathfrak{b}_1 \cdots \mathfrak{b}_r. \end{aligned}$$

Avšak z $[\mathfrak{a}_1 \cdots \mathfrak{a}_r] = [\mathfrak{b}_1 \cdots \mathfrak{b}_r]$ plyne $\mathfrak{a}_1 \cdots \mathfrak{a}_r \cong \mathfrak{b}_1 \cdots \mathfrak{b}_r$ dle Tvrzení 1.1.7. ⊠

Důsledek 2.1.10. Z důkazu Steinitzovy věty plyne, že izomorfismus konečně generovaného projektivního $\mathcal{O}$-modulu M, který je dle 2.1.8 izomorfní nějakému $\mathfrak{a}_1 \oplus \cdots \oplus \mathfrak{a}_r$, je charakterizován dvěma invarianty, a to *hodností* (*rankem*), což je přirozené číslo r, a jeho *třídou* $[M] = [\mathfrak{a}_1 \cdots \mathfrak{a}_r]$ v $\mathcal{C}l(\mathcal{O})$.

Podle 2.1.2 a 1.1.7 je M izomorfní projektivnímu modulu ve *standardním tvaru* $\mathcal{O}^{r-1} \oplus \mathfrak{a}$, kde $\mathfrak{a}$ je celistvý ideál. V Důsledku 2.1.4 jsme přitom dokázali, že každý takový ideál je maximálně 2-generovaný.

2.2 Valuační okruhy

Definice 2.2.1 (Valuace)**.** Buď $\mathcal{O}$ Dedekindův obor s podílovým tělesem $\mathcal{K}$ a buď $\mathfrak{p}$ nenulový prvoideál oboru $\mathcal{O}$. Podle 1.1.9 lze každý lomený ideál $\mathfrak{a}$ oboru $\mathcal{O}$ rozložit na $\mathfrak{a} = \mathfrak{p}^{v(\mathfrak{a})}\mathfrak{a}'$, kde $v(\mathfrak{a}) = v(\mathfrak{p}, \mathfrak{a})$ je celé číslo, jednoznačně určené ideálem $\mathfrak{a}$ a $\mathfrak{a}'$ je součin mocnin prvoideálů různých od $\mathfrak{p}$. Číslu $v(\mathfrak{a})$ říkáme $\mathfrak{p}$-*adická valuace ideálu* $\mathfrak{a}$.

Širší výklad tohoto tématu lze nalézt například v [BK, 6.2].

Definice 2.2.2 (Valuační okruh)**.** *Valuační okruh* Dedekindova oboru $\mathcal{O}$ příslušná jeho nenulovému prvoideálu $\mathfrak{p}$ je definována jako podokruh $\mathcal{O}_\mathfrak{p} \subset \mathcal{K}$ obsahující všechny zlomky a/b, kde $a, b \in \mathcal{O}$ a $b \notin \mathfrak{p}$.

Uveďme ještě alternativní definici. $\mathcal{O}_\mathfrak{p} \subset \mathcal{K}$ nazýváme *valuační okruh*, pokud pro libovolný $0 \neq x \in \mathcal{K}$ platí: buď $x \in \mathcal{O}_\mathfrak{p}$, nebo $x^{-1} \in \mathcal{O}_\mathfrak{p}$.

Valuační okruhy jsou úzce spjaty s odpovídajícími valuacemi, jak nastiňuje následující Tvrzení.

Tvrzení 2.2.3. *Pro nenulový prvoideál* $\mathfrak{p}$ *Dedekindova oboru* $\mathcal{O}$ *platí*

(i) $\mathcal{O}_\mathfrak{p} = \{x \in \mathcal{K} | v(x) \geq 0\}$,

(ii) $\mathfrak{p}\mathcal{O}_\mathfrak{p} = \{x \in \mathcal{K} | v(x) \geq 1\}$,

(iii) $(\mathfrak{p}\mathcal{O}_\mathfrak{p})^i = \{x \in \mathcal{K} | v(x) \geq i\}$ *pro* $i \in \mathbb{Z}$.

Důkaz. Toto je známým faktem, který lze nalézt v [BK]. ⊠

Věta 2.2.4. *Nechť* $\mathcal{O}$ *je Dedekindův obor, pak* $\mathcal{O} = \bigcap_\mathfrak{p} \mathcal{O}_\mathfrak{p}$ *přes všechny nenulové prvoideály* $\mathcal{O}$.

Důkaz. Vezměme $x \in \mathcal{K}$. Zřejmě $x \in \mathcal{O}$, pravě když ideál $x\mathcal{O}$ je celistvý. Z Věty 1.1.9 vyplývá, že toto nastává právě když $v_\mathfrak{p}(x) \geq 0$ pro všechny nenulové prvoideály $\mathfrak{p}$. ⊠

Věta 2.2.5 (Jednoznačný rozklad konečně generovaného modulu)**.** *Buď $\mathcal{O}$ Dedekindův obor a buď M konečně generovaný $\mathcal{O}_\mathfrak{p}$-modul, pak*

$$M \cong \mathcal{O}_\mathfrak{p}/(\mathfrak{p}\mathcal{O}_\mathfrak{p})^{\delta(1)} \oplus \cdots \oplus \mathcal{O}_\mathfrak{p}/(\mathfrak{p}\mathcal{O}_\mathfrak{p})^{\delta(l)} \oplus (\mathcal{O}_\mathfrak{p})^s,$$

kde $\delta(1) \leq \cdots \leq \delta(l)$ jsou přirozená čísla a $s \in \mathbb{N}$.

Důkaz. Věta vyplývá z jednoznačné faktorizace konečně generovaných modulů nad eukleidovskými obory, viz [BK, 3.3.6]. Platí totiž

$$M \cong \mathcal{O}_\mathfrak{p}/d_1\mathcal{O}_\mathfrak{p} \oplus \cdots \oplus \mathcal{O}_\mathfrak{p}/d_l\mathcal{O}_\mathfrak{p} \oplus (\mathcal{O}_\mathfrak{p})^s,$$

kde $d_1, \ldots, d_l$ jsou neinvertibilní v $\mathcal{O}_\mathfrak{p}$, $d_1|d_2|\cdots|d_l$ a $s \geq 0$. Stačí položit $\delta(i) = v(d_i)$ pro $i = 1, \ldots, l$ a zbytek plyne z 2.2.3 (iii). ⊠

2.3 Torzní moduly nad Dedekindovými obory

Nyní se zaměříme na pojem torzních a beztorzních modulů nad Dedekindovými obory, jak jsme slíbili v definici 1.1.6.

Nechť $\mathcal{O}$ je komutativní obor integrity a M je beztorzní $\mathcal{O}$-modul. Definujme $S = \mathcal{O} \setminus \{0\}$ množinu uzavřenou na násobení a relaci $\sim$ na uspořádaných dvojicích $(m, s) \in M \otimes S^{-1}$, pro kterou $(m, s) \sim (m', s')$ právě když $(ms' - m's)x = 0$ pro nějaké $x \in S$. Snadno dokážeme, že $\sim$ je ekvivalencí na dané množině. M je beztorzní, tudíž pokud platí $nr = 0$ pro nějaké $n \in M, r \in \mathcal{O}$, pak je n nebo r rovno nule. s je ale prvkem $\mathcal{O} \setminus \{0\}$, tedy $(m, s) \sim (m', s')$ právě když $m's = ms'$. Označme m/s třídu ekvivalence danou (m, s) a M_S množinu takových tříd. Není těžké ověřit, že sčítání prvků M_S a násobení prvkem a z podílového tělesa $\mathcal{K}$ oboru $\mathcal{O}$, dané vztahem

$$\tfrac{m}{s} + \tfrac{n}{t} := \tfrac{mt+ns}{st}, \qquad a\tfrac{m}{s} = \tfrac{am}{s},$$

je na této množině dobře definované, a tudíž M_S je vektorovým prostorem nad $\mathcal{K}$ s nulovým prvkem $0/1$.

Definice 2.3.1 (Lokalizace modulu)**.** Množina tříd M_S výše definované ekvivalence je tzv. *lokalizace modulu M v S*. Níže budeme užívat také lokalizaci okruhu R v jeho maximálním ideálu m, čímž se všeobecně rozumí lokalizace v komplementu tohoto ideálu.

Tvrzení 2.3.2. *Buď M konečně generovaný beztorzní modul nad komutativním oborem integrity $\mathcal{O}$, potom*

$$M \hookrightarrow \mathcal{O}^k \text{ pro nějaké přirozené } k.$$

Důkaz. Nejprve ukážeme, že $\mathcal{O}$-modul M může být vnořený do nějakého vektorového prostoru V nad podílovým tělesem $\mathcal{K}$ tak, že M generuje V jako $\mathcal{K}$-modul. Vezměme za V lokalizaci modulu M v množině $S = \mathcal{O} \setminus \{0\}$ a definujme $\nu : M \to V$ pomocí $\nu(m) = m/1$. Pak ν je homomorfizmus $\mathcal{O}$-modulů (pokud V uvažujeme jako $\mathcal{O}$-modul při restrikci skalárů). Pokud $\nu(m) = 0/1$, pak $m = 0$ a tedy ν je prosté. Tudíž M generuje V jako $\mathcal{K}$-prostor.

Protože je M konečně generovaný, má V konečnou dimenzi nad $\mathcal{K}$. Vezměme množinu generátorů $\{m_1, \ldots, m_l\}$ modulu M a bázi $\{e_1, \ldots, e_k\}$ prostoru V a vyjádřeme

$$m_j = \sum_i x_{ij} e_i, \text{ kde } x_{ij} \in \mathcal{K}.$$

Pokud koeficienty v součtu vynásobíme součinem jmenovatelů d, dostáváme

$$M \cong Md \subseteq e_1\mathcal{O} \oplus \cdots \oplus e_k\mathcal{O}.$$

⊠

Důsledek 2.3.3. Nechť M je konečně generovaný beztorzní modul nad Dedekindovým oborem $\mathcal{O}$, pak podle 2.1.1 a předchozího tvrzení je M projektivní.

Důsledek 2.3.4. Buď M konečně generovaný modul nad Dedekindovým oborem $\mathcal{O}$, pak existuje $\mathcal{O}$-modulový izomorfismus

$$M \cong T(M) \oplus M/T(M).$$

Definice 2.3.5 (Primární moduly)**.** Pro daný $\mathcal{O}$-modul M definujeme jeho anihilátor jako ideál $\mathrm{Ann}(M)$ oboru $\mathcal{O}$ předpisem

$$\mathrm{Ann}(M) = \{r \in \mathcal{O} |\ mr = 0 \text{ pro všechna } m \in M\}.$$

Zřejmě konečně generovaný $\mathcal{O}$-modul má nenulový anihilátor právě když je torzní.

Buď $\mathfrak{p}$ nenulový prvoideál oboru $\mathcal{O}$. $\mathcal{O}$-modul M se nazývá $\mathfrak{p}$-*primární*, pokud $\mathrm{Ann}(M) = \mathfrak{p}^\delta$ pro nějaké přirozené δ. Pokud se jedná o hlavní ideál, tedy $\mathfrak{p} = p\mathcal{O}$, dáváme přednost označení p-*primární* modul.

Zřejmě faktorový modul $\mathcal{O}/\mathfrak{p}^\delta$ je $\mathfrak{p}$-primární, stejně jako konečná direktní suma takovýchto modulů (s různými exponenty).

Tvrzení 2.3.6. *Buď $\mathfrak{p}$ nenulový prvoideál oboru $\mathcal{O}$, pak existuje izomorfizmus $\mathcal{O}$-modulů (i okruhů)*

$$\iota : \mathcal{O}/\mathfrak{p}^\delta \xrightarrow{\sim} \mathcal{O}_\mathfrak{p}/(\mathfrak{p}\mathcal{O}_\mathfrak{p})^\delta \text{ pro libovolné } \delta > 0.$$

Důkaz. Přirozený okruhový homomorfismus z $\mathcal{O}$ do $\mathcal{O}_\mathfrak{p}/(\mathfrak{p}\mathcal{O}_\mathfrak{p})^\delta$ má zřejmě jádro $\mathfrak{p}^\delta$, a tedy indukuje prosté zobrazení $\iota : \mathcal{O}/\mathfrak{p}^\delta \to \mathcal{O}_\mathfrak{p}/(\mathfrak{p}\mathcal{O}_\mathfrak{p})^\delta$.

Zbývá dokázat, že ι je zároveň na. Vezměme $a/b \in \mathcal{O}_\mathfrak{p}$, kde $a \in \mathcal{O}$ a $b \in \mathcal{O} \setminus \mathfrak{p}$, a uvažme ideál $b\mathcal{O} + \mathfrak{p}^\delta$ Dedekindova oboru $\mathcal{O}$. Jestli je tento ideál vlastní, pak ho dle 1.1.9 lze jednoznačně rozložit na součin prvoideálů $\prod_{\mathfrak{q}\in\mathcal{P}} \mathfrak{q}^{v(\mathfrak{q},\mathfrak{p})}$. Tedy platí $\mathfrak{p}^\delta \subseteq \mathfrak{q}$ pro každé $\mathfrak{q}$ s kladným exponentem. $\mathfrak{q}$ je prvoideál, tudíž $\mathfrak{p} \subseteq \mathfrak{q}$. Ale $\mathfrak{p}$ je z definice Dedekindova oboru zároveň maximální ideál, tudíž $\mathfrak{p} = \mathfrak{q}$. Jediný ideál, který by se mohl vyskytovat v tomto rozkladu je tedy $\mathfrak{p}$ samotné. Protože $b \notin \mathfrak{p}$, dostáváme $b\mathcal{O} + \mathfrak{p}^\delta = \mathcal{O}$. Tudíž $1 = bc + z$, neboli $a = abc + az$ pro nějaké $c \in \mathcal{O}$ a $z \in \mathfrak{p}^\delta$, tedy $(a/b - \iota(ac)) \in (\mathfrak{p}\mathcal{O}_\mathfrak{p})^\delta$, což dává surjektivitu. ⊠

Věta 2.3.7. *Buď $\mathfrak{p}$ nenulový prvoideál Dedekindova oboru $\mathcal{O}$ a buď M konečně generovaný $\mathfrak{p}$-primární $\mathcal{O}$-modul.*

Potom M je také konečně generovaný $\mathcal{O}_\mathfrak{p}$-modul a existuje rozklad M na direktní součet

$$M \cong \mathcal{O}/\mathfrak{p}^{\delta(1)} \oplus \cdots \oplus \mathcal{O}/\mathfrak{p}^{\delta(k)},$$

kde $\delta(1) \leq \cdots \leq \delta(k)$ jsou přirozená čísla.

Důkaz. Podle definice je $\mathrm{Ann}(M) = \mathfrak{p}^\delta$ pro nějaké $\delta > 0$. Tedy M je přirozeně $\mathcal{O}/\mathfrak{p}^\delta$-modul, tudíž $\mathcal{O}_\mathfrak{p}/(\mathfrak{p}\mathcal{O}_\mathfrak{p})^\delta$-modul, a tudíž i $\mathcal{O}_\mathfrak{p}$-modul podle předchozího Tvrzení. Dále dle 2.2.5 existuje rozklad M jako $\mathcal{O}_\mathfrak{p}$-modulu na direktní sumu, která je zřejmě zároveň direktní sumou $\mathcal{O}$-modulu. ⊠

Definice 2.3.8 (Elementární divizory)**.** Pokud má Dedekindův obor $\mathcal{O}$ více než jeden nenulový prvoideál, pak ideály $\mathfrak{p}^{\delta(1)}, \ldots, \mathfrak{p}^{\delta(k)}$ vyskytující se v rozkladu $\mathfrak{p}$-primárního modulu M nazýváme *elementární divizory* modulu M.

Pokud $\mathfrak{p} = p\mathcal{O}$ je hlavní ideál, speciálně pokud je $\mathcal{O}$ obor hlavních ideálů, pak odpovídající mocniny $p^{\delta(\mathfrak{p},1)}, \ldots, p^{\delta(\mathfrak{p},k(\mathfrak{p}))}$ irreducbilního prvku p nazýváme *elementární divizory* modulu M.

Tato definice je přípravou na definici elementárních divizorů libovolného torzního modulu. Elementární divizory $\mathfrak{p}$-primárního $\mathcal{O}$-modulu M jsou to samé, jako činitelé v rozkladu M coby $\mathcal{O}_\mathfrak{p}$-modulu. Každému rozkladu $\mathfrak{p}$-primárního modulu v direktní sumu cyklických modulů přiřadíme posloupnost

$$\mathrm{edt}_{\mathfrak{p}}(M) = (\alpha_1, \alpha_2, \ldots)$$

přirozených čísel, kde α_i zastupuje počet výskytů výrazu $\mathcal{O}/\mathfrak{p}^i$ v daném rozkladu. Díky jednoznačnosti rozkladu je jednoznačně určená i tato posloupnost. Budeme ji nazývat *typ* $\mathfrak{p}$*-elementárních divizorů* modulu M.

Poznamenejme, že $\alpha_i = 0$ pro skoro všechna i. Maximální index, pro který je $\alpha_i \neq 0$ se nazývá *délka* $\mathrm{edt}_{\mathfrak{p}}(M)$. Zřejmě pro $\mathfrak{p}$-elementární modul M typu délky k platí $\mathrm{Ann}(M) = \mathfrak{p}^k$. Nulový modul odpovídá nulové posloupnosti $(0, 0, \ldots)$, která má délku 0. $\mathcal{O}_{\mathfrak{p}}^k$ má typ $(0, \ldots, 0, 1, 0, \ldots)$ délky k.

Věta 2.3.9. *Nechť M, N jsou konečně generované $\mathfrak{p}$-primární moduly nad Dedekindovým oborem $\mathcal{O}$. Potom $M \cong N$ právě když $edt_{\mathfrak{p}}(M) = edt_{\mathfrak{p}}(N)$.*

Důkaz. Důkaz lze nalézt v [BK, 6.3.11]. ⊠

Nyní uvažme rozklad konečně generovaného torzního $\mathcal{O}$-modulu M na direktní sumu $\mathfrak{p}$-primárních podmodulů jdoucí přes množinu P všech nenulových prvoideálů Dedekindova oboru $\mathcal{O}$. Tento *primární rozklad* nám charakterizuje modul M vzhledem k množině $\{\mathrm{edt}_{\mathfrak{p}}(M) | \mathfrak{p} \in P\}$ typů elementárních divizorů.

Lemma 2.3.10. *Pro každý $\mathfrak{p} \in P$ existuje maximální $\mathfrak{p}$-primární podmodul modulu M, neboli maximální podmodul T, pro který platí $Ann(T) = \mathfrak{p}^k$ pro nějaké přirozené k.*

Důkaz. Pokud jsou M', M'' $\mathfrak{p}$-primární podmoduly modulu M, potom je $\mathfrak{p}$-primární i podmodul $M' + M''$. Tudíž z neexistence maximálního $\mathfrak{p}$-primárního podmodulu by plynula existence nekonečné stoupající posloupnosti podmodulů M, což je ve sporu s tím, že M je noetherovský. Konečně generovaný modul nad noetherovským okruhem je totiž také noetherovský. ⊠

Definice 2.3.11 ($\mathfrak{p}$-komponenta)**.** Můžeme tedy definovat $\mathfrak{p}$-*komponentu* $T_{\mathfrak{p}}(M)$ modulu M jako maximální $\mathfrak{p}$-primární podmodul modulu M. Říká se jí také $\mathfrak{p}$-*torzní část* nebo $\mathfrak{p}$-*primární část* modulu M. Protože je M noetherovský, je $T_{\mathfrak{p}}(M)$ konečně generovaný.

Následující výsledek je klíčový pro existenci primárního rozkladu.

Lemma 2.3.12. *Buďte $\mathfrak{a}, \mathfrak{b}$ komaximální ideály Dedekindova oboru $\mathcal{O}$ a buď M $\mathcal{O}$-modul takový, že $\mathrm{Ann}(M) = \mathfrak{ab}$.*

Potom $M = \mathfrak{a}M \oplus \mathfrak{b}M$, $\mathrm{Ann}(\mathfrak{a}M) = \mathfrak{b}$ a $\mathrm{Ann}(\mathfrak{b}M) = \mathfrak{a}$.

Důkaz. Komaximalita říká, že $\mathfrak{a} + \mathfrak{b} = \mathcal{O}$. Tudíž $a + b = 1$ pro nějaké prvky $a \in \mathfrak{a}, b \in \mathfrak{b}$, a tedy $M = \mathfrak{a}M + \mathfrak{b}M$.

Předpokládejme, že $m \in \mathfrak{a}M \cap \mathfrak{b}M$. Potom $am = bm = 0$, protože $\mathfrak{a}\mathfrak{b}M = 0$, tudíž $m = (a + b)m = 0$, což dává rozklad v direktní součet.

Zřejmě $\mathfrak{b} \subseteq \mathrm{Ann}(\mathfrak{a}M)$. Nechť $x \in \mathrm{Ann}(\mathfrak{a}M)$. Potom $x\mathcal{O}\cdot\mathfrak{a} \subseteq \mathrm{Ann}(M) = \mathfrak{a}\mathfrak{b}$, a tudíž $x\mathcal{O} \subseteq \mathfrak{b}$, protože $\mathfrak{a}$ je invertibilní ideál. ⊠

Pro daný modul M a nenulový prvoideál $\mathfrak{p}$ vyjádřeme anihilátor ve tvaru

$$\mathrm{Ann}(M) = \mathfrak{p}^k c(\mathfrak{p}),$$

kde $k \geq 0$ je $\mathfrak{p}$-adická valuace anihilátoru $\mathrm{Ann}(M)$ a kde $\mathfrak{p}$ a $c(\mathfrak{p})$ jsou komaximální. $c(\mathfrak{p})$ nazveme *doplněk prvoideálu* $\mathfrak{p}$. Poznamenejme, že pro skoro všechny prvoideály platí $k = 0$ a $c(\mathfrak{p}) = \mathrm{Ann}(M)$.

Tvrzení 2.3.13. *Nechť M je konečně generovaný torzní modul nad Dedekindovým oborem $\mathcal{O}$. Potom platí:*

(i) $T_{\mathfrak{p}}(M) = c(\mathfrak{p})M$.

(ii) $T_{\mathfrak{p}}(M) = 0$ *pro skoro všechny prvoideály* $\mathfrak{p}$.

(iii) $M = \bigoplus_{\mathfrak{p}\in P} T_{\mathfrak{p}}(M)$, *kde P je množina všech nenulových prvoideálů oboru $\mathcal{O}$.*

Důkaz. Zřejmě $c(\mathfrak{p})M \subseteq T_{\mathfrak{p}}(M)$. Podle předchozího Lemmatu, $M = \mathfrak{p}^k M \oplus c(\mathfrak{p})M$ a $\mathrm{Ann}(\mathfrak{p}^k M) = c(\mathfrak{p})$. Pokud $m = x+n$ je prvkem $T_{\mathfrak{p}}(M)$, kde $x \in \mathfrak{p}^k M$ a $n \in c(\mathfrak{p})M$, je x anihilován oběma komaximálními ideály $\mathfrak{p}^k$ a $c(\mathfrak{p})$, tedy musí být roven 0. Tudíž (i) platí a (ii) plyne z rovnosti $c(\mathfrak{p}) = \mathrm{Ann}(M)$ pro skoro všechny prvoideály.

Poslední část plyne indukcí dle počtu různých prvoideálů z $\mathrm{Ann}(M)$. Všimněme si , že pokud je $\mathfrak{p}$ prvek $\mathrm{Ann}(M)$, platí podle předchozího Lemmatu

$$M = c(\mathfrak{p})M \oplus \mathfrak{p}^k M = T_{\mathfrak{p}}(M) \oplus \mathfrak{p}^k M.$$

Nyní $\mathrm{Ann}(\mathfrak{p}^k M) = c(\mathfrak{p})$ má méně prvků než $\mathrm{Ann}(M)$, a $T_{\mathfrak{q}}(\mathfrak{p}^k M) = T_{\mathfrak{q}}(M)$, pokud $\mathfrak{q}$ je prvoideál různý od $\mathfrak{p}$. ⊠

Poznámka 2.3.14 (Homomorfizmy)**.** Předpokládejme, že $\lambda : M \to N$ je homomorfizmus mezi konečně generovanými torzními $\mathcal{O}$-moduly, kde $\mathcal{O}$ je Dedekindův obor. Z definice $\mathfrak{p}$-komponent modulů M a N je zřejmé, že λ indukuje skupinu $\mathcal{O}$-modulových homomorfizmů

$$T_{\mathfrak{p}}(\lambda) : T_{\mathfrak{p}}(M) \longrightarrow T_{\mathfrak{p}}(N),$$

kde pro skoro všechny $\mathfrak{p}$ je $T_{\mathfrak{p}}(\lambda)$ nulové zobrazení mezi nulovými moduly.

Naopak, pro danou skupinu $\{\lambda(\mathfrak{p}) : T_{\mathfrak{p}}(M) \to T_{\mathfrak{p}}(N)\}$ $\mathcal{O}$-modulových homomorfizmů je direktní suma $\lambda = \bigoplus_{\mathfrak{p}} \lambda(\mathfrak{p})$ homomorfizmus z M do N, pro který platí $T_{\mathfrak{p}}(\lambda) = \lambda(\mathfrak{p})$ pro všechny $\mathfrak{p}$.

Důsledek 2.3.15. Buďte M a N konečně generované torzní $\mathcal{O}$-moduly, kde $\mathcal{O}$ je Dedekindův obor. Potom $M \cong N$ právě když $T_{\mathfrak{p}}(M) \cong T_{\mathfrak{p}}(N)$ pro všechny prvoideály $\mathfrak{p}$ oboru $\mathcal{O}$.

Věta 2.3.16 (Primární rozklad konečně generovaných torzních modulů)**.** *Buďte M, N konečně generované torzní moduly nad Dedekindovým oborem $\mathcal{O}$. Potom*

(i) $$M \cong \bigoplus_{\mathfrak{p}} (\mathcal{O}/\mathfrak{p}^{\delta(\mathfrak{p},1)} \oplus \cdots \oplus \mathcal{O}/\mathfrak{p}^{\delta(\mathfrak{p},s(\mathfrak{p}))}),$$
kde $\delta(\mathfrak{p},1) \leq \cdots \leq \delta(\mathfrak{p},s(\mathfrak{p}))$ jsou přirozená čísla a $s(\mathfrak{p}) = 0$ pro skoro všechny prvoideály $\mathfrak{p}$,

(ii) přirozená čísla $\delta(\mathfrak{p},1) \leq \cdots \leq \delta(\mathfrak{p},s(\mathfrak{p}))$ a množina prvoideálů $\mathfrak{p}$, pro které platí $s(\mathfrak{p}) \neq 0$ jsou jednoznačně určeny modulem M a naopak,

(iii) $M \cong N$ právě když $\mathrm{edt}(M) = \mathrm{edt}(N)$*, což znamená, že* $\mathrm{edt}_{\mathfrak{p}}(M) = \mathrm{edt}_{\mathfrak{p}}(N)$ *pro všechny nenulové prvoideály $\mathfrak{p}$ oboru $\mathcal{O}$.*

Důkaz. Věta plyne z rozkladu modulu na $\mathfrak{p}$-komponenty 2.3.13, rozkladu $\mathfrak{p}$-primárního modulu 2.3.7 a z faktu, že typy elementárních divizorů charakterizují primární moduly 2.3.9. ⊠

Všechny naše dosavadní výsledky shrneme v jedné větě, která kompletně klasifikuje konečně generované moduly nad Dedekindovými obory.

Věta 2.3.17. *Buď M konečně generovaný modul nad Dedekindovým oborem $\mathcal{O}$, pak platí*

(i) $M = P \oplus T$, kde P je konečně generovaný projektivní $\mathcal{O}$-modul a $T = T(M)$ je konečně generovaný torzní $\mathcal{O}$-modul.

(ii) $P \cong \mathcal{O}^{r-1} \oplus \mathfrak{a}$, kde $\mathfrak{a}$ je ideál oboru $\mathcal{O}$ a $r \geq 1$ beztorzní hodnost P.

(iii) $T \cong \bigoplus_{\mathfrak{p}} T(\mathfrak{p})$, kde součet jde přes všechny nenulové prvoideály $\mathfrak{p}$ oboru $\mathcal{O}$, každý $T(\mathfrak{p}) = T_{\mathfrak{p}}(M)$ je konečně generovaný $\mathfrak{p}$-primární $\mathcal{O}$-modul a $T(\mathfrak{p}) = 0$ pro skoro všechna $\mathfrak{p}$.

(iv) (a) *Pokud* $T(\mathfrak{p}) \neq 0$, *potom*

$$T(\mathfrak{p}) \cong \mathcal{O}/\mathfrak{p}^{\delta(\mathfrak{p},1)} \oplus \cdots \oplus \mathcal{O}/\mathfrak{p}^{\delta(\mathfrak{p},s(\mathfrak{p}))},$$

kde $0 < \delta(\mathfrak{p},1) \leq \cdots \leq \delta(\mathfrak{p},s(\mathfrak{p}))$.

(b) *Pokud* $T(\mathfrak{p}) = 0$, *položíme* $s(\mathfrak{p}) = 0$.

Navíc modul M *určuje a je určen jednoznačně až na izomorfizmus následujícím:*

- *beztorzní hodností* $r \in \mathbb{N}$,
- $s(\mathfrak{p})$ *a* $\delta(\mathfrak{p},i)$ *z* $\mathbb{N}$ *pro všechna* $1 \leq i \leq s(\mathfrak{p})$ *a všechna* $\mathfrak{p}$,
- *třídou* $[\mathfrak{a}]$ *z grupy tříd* $\mathcal{C}l(\mathcal{O})$.

Modul N *je izomorfní* M, *pokud se ve všech těchto invariantech shoduje s modulem* M. *Speciálně, torzní část modulu* M *je určena jednoznačně až na izomorfizmus množinou jejich elementárních divizorů*

$$\{\mathfrak{p}^{\delta(\mathfrak{p},1)}, \ldots, \mathfrak{p}^{\delta(\mathfrak{p},s(\mathfrak{p}))} | \mathfrak{p} \in P\}.$$

Kapitola 3

Příklady Dedekindových oborů

Mezi Dedekindovy obory patří obor celých čísel $\mathbb{Z}$ nebo okruhy polynomů $F[x]$ jedné proměnné nad libovolným tělesem F. Tyto spadají do případů, kdy je Dedekndův obor oborem hlavních ideálů, tedy jeho grupa tříd je rovna jedné.

3.1 Algebraická celá čísla

Velmi důležité a v historii motivační příklady Dedekindových oborů vycházejí z těles algebraických čísel.

Definice 3.1.1. *Tělesy algebraických čísel* F nazýváme konečná (a tudíž algebraická) tělesová rozšíření tělesa racionálních čísel $\mathbb{Q}$.

Definice 3.1.2. Prvek x tělesa algebraických čísel F nazveme *algebraickým celým číslem*, pokud je kořenem nějakého monického polynomu nad oborem celých čísel.

Naším cílem v této části bude dokázat, že celistvý uzávěr oboru celých čísel v libovolném tělese algebraických čísel je Dedekindův obor. Toho docílíme pomocí zkoumání dvou zobecněných případů. Nejprve se zaměříme pouze na noetherovské obory a dokážeme Krull-Akizukiho větu. Poté se naopak od podmínky noetherovskosti oprostíme a dokážeme větu pro tzv. Prüferovy obory.

Při dokazování Krull-Akizukiho věty budeme následovat postup uvedený v [Bo], jenž formuluje původní důkaz (viz [Aki]) pomocí lineární algebry. Tato látka je dále rozepsána v [Ma].

Definice 3.1.3. Buď A okruh. *Krullova dimenze*, nebo pouze *dimenze* tohoto okruhu značí maximální délku ostře klesajícího řetězce jeho prvoideálů. Pokud maximální délka neexistuje, je dimenze okruhu nekonečno.

Definice 3.1.4. Buď A okruh. *Délkou modulu* M nad tímto okruhem rozumíme maximální délku ostře klesajícího řetězce podmodulů modulu M a značíme ji $l_A(M)$. Pokud maximální délka neexistuje, je délka modulu nekonečno.

Definice 3.1.5. Buď A obor integrity, M modul nad tímto oborem a $\mathcal{K}$ podílové těleso oboru A. *Beztorzní rank* vyjadřuje maximální počet prvků z M lineárně nezávislých nad A. To je rovno dimenzi $M \otimes_A \mathcal{K}$ jako vektorového prostoru nad $\mathcal{K}$.

Definice 3.1.6. Buď A okruh a M modul nad tímto okruhem. Prvoideál P okruhu A nazýváme *asociovaný prvoideál* modulu M, pokud je P anihilátorem nějakého prvku $x \in M$. Množina všech asociovaných prvoideálů M se značí $\mathrm{Ass}(M)$.

Poznámka 3.1.7. Je dobře známým faktem, že $\mathrm{Ass}(M) \neq \emptyset$ pro nenulový A-modul M, konkrétně, maximální prvek množiny $F = \{\mathrm{Ann}(x) \mid 0 \neq x \in M\}$ je asociovaný prvoideál modulu M.

Lemma 3.1.8. *Nechť A je noetherovský okruh a M nenulový konečně generovaný A-modul. Pak existuje řetězec $0 = M_0 \subset M_1 \subset \cdots \subset M_n = M$ podmodulů M takový, že pro každé $i = 1, \ldots n$ platí $M_i/M_{i-1} \simeq A/P_i$ pro nějaký prvoideál P_i okruhu A.*

Důkaz. Zvolme nějaký asociovaný prvoideál $P_1 \in \mathrm{Ass}(M)$. Pak existuje cyklický podmodul M_1 modulu M, pro který platí $M_1 \simeq A/P_1$. Pokud $M_1 \neq M$, vybereme nějaký $P_2 \in \mathrm{Ass}(M/M_1)$. Pak existuje $M_2 \subset M$ takový, že $M_2/M_1 \simeq A/P_2$. Tento postup lze díky noetherovskosti modulu M opakovat jen konečně mnohokrát, než získáme $M_n = M$. ⊠

Lemma 3.1.9. *Nechť A je noetherovský obor integrity dimenze 1 a $\mathcal{K}$ jeho podílové těleso. Dále buď M beztorzní A-modul ranku $r < \infty$. Potom pro libovolný nenulový prvek $a \in A$ platí*

$$l(M/aM) \leq r \cdot l(A/aA).$$

Důkaz. Nejprve předpokládejme, že M je konečně generovaný. Vyberme prvky $\xi_1, \ldots, \xi_r \in M$ lineárně nezávislé nad A a množinu $E = \sum A\xi_i$. Potom pro libovolné $\eta \in M$ existuje $0 \neq t \in A$ takové, že $t\eta \in E$. Položme $C = M/E$, potom z předpokladu pro M vidíme, že C je také konečně generovaný, tudíž pro vhodné $0 \neq t \in A$ platí $tC = 0$. Použitím 3.1.8 na C můžeme zvolit $C = C_0 \supset C_1 \supset \cdots \supset C_m = 0$ takové, že $C_i/C_{i+1} \simeq A/\mathfrak{p}_i$, pro vlastní prvoideály $\mathfrak{p}_i$ oboru A, tedy musí platit $t \in \mathfrak{p}_i$. Protože A je dimenze 1, je každý prvoideál $\mathfrak{p}_i$ i maximální, tudíž $l(C) = m < \infty$. Zvolme $0 \neq a \in A$. Potom exaktní posloupnost

$$E/a^nE \to M/a^nM \to C/a^nC \to 0$$

dává

$$l(M/a^nM) \leq l(E/a^nE) + l(C) \quad \text{pro všechna} \quad n > 0.$$

Oba A-moduly E i M jsou beztorzní a zřejmě platí $a^iM/a^{i+1}M \simeq M/aM$, podobně pro E. Tudíž poslední nerovnost lze zapsat ve tvaru

$$n \cdot l(M/aM) \leq n \cdot l(E/aE) + l(C) \quad \text{pro všechna} \quad n > 0,$$

což dává $l(M/aM) \leq l(E/aE)$. Protože $E \simeq A^r$, máme

$$l(E/aE) = r \cdot l(A/aA).$$

Při předpokladu konečně generovaného modulu M je důkaz ukončen.

Pokud M není konečně generovaný, vezměme konečně generovaný podmodul $\bar{N} = A\bar{\omega}_1 + \ldots + A\bar{\omega}_s$ modulu $\bar{M} = M/aM$ pro nějaké $0 \neq a \in A$. Dále pro každé $\bar{\omega}_i$ vezměme inverzní prvek ω_i v M a definujme $M_1 = \sum_i A\omega_i$. Dostáváme

$$l(\sum_i A\bar{\omega}_i) = l(M_1/(M_1 \cap aM)) \leq l(M_1/aM_1) \leq r \cdot l(A/aA).$$

Pravá strana je nyní nezávislá na $\bar{N}$, tudíž $\bar{M}$ je konečně generovaný a $l(\bar{M}) \leq r \cdot l(A/aA)$. ⊠

Věta 3.1.10 (Krull-Akizukiho věta)**.** *Buď A noetherovský obor integrity dimenze 1 a $\mathcal{K}$ jeho podílové těleso. Buď F konečné algebraické rozšíření tělesa $\mathcal{K}$ a B okruh, pro který platí $A \subseteq B \subseteq F$. Potom B je noetherovský okruh dimenze nanejvýš 1. Navíc, pokud J je nenulový ideál okruhu B, je B/J A-modul konečné délky.*

Důkaz. Za F můžeme dosadit podílové těleso okruhu B. Mějme $[F : K] = r$. Potom B je beztorzní A-modul ranku r. Tudíž podle přípravného Lemmatu máme $l_A(B/aB) < \infty$ pro nějaké $0 \neq a \in A$. Pokud $J \neq 0$ je ideál okruhu B a $0 \neq b \in J$, potom, protože je b algebraické nad A, platí rovnost

$$a_m b^m + a_{m-1} b^{m-1} + \cdots + a_1 b + a_0 = 0 \quad \text{pro nějaká} \quad a_i \in A.$$

B je obor integrity, čili můžeme předpokládat $a_0 \neq 0$. Potom $a_0 \in J \cap A$ a tedy

$$l_A(B/J) \leq l_A(B/a_0 B) < \infty.$$

Z nerovnosti $l_B(J/a_0 B) \leq l_A(J/a_0 B) \leq l_A(B/a_0 B) < \infty$ vyplývá, že $J/a_0 B$ je konečně generovaný B-modul. Tudíž i J samotný je konečný B-modul, a tudíž B je noetherovský.

Jestliže je P nenulový prvoideál okruhu B, potom B/P je artinovský okruh a obor integrity, a tedy těleso. Tudíž P je maximální a B je dimenze 1. ⊠

Důsledek 3.1.11. Buď A noetherovský obor integrity dimenze 1, $\mathcal{K}$ jeho podílové těleso a F konečné algebraické rozšíření tělesa $\mathcal{K}$. Buď B celistvý uzávěr oboru A v F. Pak B je Dedekindův obor.

Důkaz. Dle právě dokázané věty je B noetherovský obor integrity dimenze 1 a je celistvě uzavřený ve svém podílovém tělese podle konstrukce. Tedy se jedná o Dedekindův obor podle 1.1.4 (iii). ⊠

Nyní budeme zkoumat zobecnění Dedekindových oborů bez vlastnosti noetherovskosti. V důkazu budeme postupovat dle [FS, 1.2].

Definice 3.1.12 (Prüferův obor)**.** Obor integrity se nazývá *Prüferův*, pokud je každý jeho nenulový konečně generovaný ideál invertibilní.

Existuje mnoho alternativních definic Prüferova oboru. V našem textu využijeme tuto: Obor integrity R je Prüferův, pokud pro každý maximální ideál M v R je lokalizace R_M valuačním okruhem. Vztah platí i pro prvoideály.

Definice 3.1.13 (Lokální okruh)**.** Okruh se nazývá lokální, pokud má právě jeden maximální ideál.

Věta 3.1.14. *Buď R Prüferův obor a F algebraické rozšíření jeho podílového tělesa $\mathcal{K}$. Potom celistvý uzávěr S oboru R v F je Prüferův obor.*

Důkaz. Musíme ověřit, že S_L je valuační okruh pro každý maximální ideál L oboru S tedy že pro libovolný nenulový $x \in F$ platí $x \in S_L$ nebo $x^{-1} \in S_L$. Ideál $P = L \cap R$ je prvoideál, tudíž R_P je valuační obor, díky prüferovskosti oboru R. Protože je x algebraické nad $\mathcal{K}$, existuje polynom $f(X) \in R_P(X)$ takový, že $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = 0$. Bez újmy na obecnosti můžeme předpokládat, že alespoň jeden koeficient je jednotka v R_P. Vynásobení prvkem a_n^{n-1} ukazuje, že $a_n x$ je celistvý nad R_P, tudíž $a_n x \in S_L$, protože S je celistvý uzávěr oboru R. Pokud je $a_n x$ jednotkou v S_L, pak zřejmě $a_n = x^{-1} \in S_L$. Jestliže $a_n x$ není jednotkou, pak z vyjádření $(a_n x + a_{n-1})x^{n-1} + \cdots + a_1 x + a_0 = 0$ plyne, že $(a_n x + a_{n-1})x$, jako celistvý prvek nad R_P, leží v S_L. Pokud je a_{n-1} jednotka v S_L, je i prvek $a_n x + a_{n-1}$ jednotka, protože S_L je lokální, tedy $x \in S_L$. Pokud a_{n-1} není jednotka, pokračujeme stejným způsobem, dokud nenarazíme na jednotkový koeficient. ⊠

Spojením těchto dvou zobecnění dostaneme tvrzení pro Dedekindovy obory.

Důsledek 3.1.15. Okruh G algebraických celých čísel v tělese algebraických čísel F, neboli celistvý uzávěr oboru celých čísel v F je Dedekindovým oborem.

3.2 Kvadratická tělesa

Speciálním případem těles algebraických čísel jsou *kvadratická tělesa* $\mathbb{Q}(\sqrt{n}) = \{p + q\sqrt{n} |\ p, q \in \mathbb{Q}\}$, která jsou rozšířeními tělesa racionálních čísel stupně dva. Není těžké dokázat, že zobrazení $n \to \mathbb{Q}(\sqrt{n})$ je bijekcí pro množinu celých nenulových čísel neobsahujících čtverec, tj. takových, které nejsou dělitelné druhou mocninou žádného přirozeného čísla. (Pro n rovno jedné nastává triviální případ $\mathbb{Q}(\sqrt{n}) = \mathbb{Q}$, tedy jej dále nebudeme uvažovat.)

Definice 3.2.1. *Kvadratickým řádem* rozumíme obor integrity $\mathbb{Z}[\sqrt{n}] = \{a + b\sqrt{n} |\ a, b \in \mathbb{Z}\}$, kde n je celé číslo neobsahující čtverec.

Věta 3.2.2. *Buď G okruh algebraických celých čísel v kvadratickém tělese $F = \mathbb{Q}(\sqrt{n})$, kde n je celé číslo neobsahující čtverec. Potom*

$$G = \mathbb{Z}[\sqrt{n}] \text{ právě když } n \equiv 2, 3 \ (mod\ 4),$$
$$G = \mathbb{Z}[(1 + \sqrt{n})/2] \text{ právě když } n \equiv 1 \ (mod\ 4).$$

V druhém případě $G = \{a + b(1+\sqrt{n})/2 |\ a, b \in \mathbb{Z}\}$ *a* $(1+\sqrt{n})/2$ *má minimální polynom* $X^2 - X + (1+n)/4$.

Důkaz. Nechť $x = x_0 + x_1\sqrt{n} \in F$. Je dobře známým faktem, že $x \in G$ právě když má jeho minimální polynom koeficienty v $\mathbb{Z}$. Pokud $x \in \mathbb{Q}$ je tento polynom jednoduše $X - x$, tudíž $x \in \mathbb{Z}$. Předpokládejme nyní, že $x \notin \mathbb{Q}$, tedy jeho minimální polynom je tvaru $X^2 - Tx \cdot X + Nx$. Musíme určit, kdy oba prvky $Tx = 2x_0$ a $Nx = x_0^2 - nx_1^2$ náleží do $\mathbb{Z}$. To určitě nastává, pokud jsou x_0 i x_1 v $\mathbb{Z}$, ovšem zpětná implikace platit nemusí.

Víme, že $\mathbb{Z}$ je Dedekindův obor a obor hlavních ideálů (prvky jednoznačně korespondují s ideály až na prvky opačné), tedy každý prvek $a \in \mathbb{Q}$ lze díky Větě 1.1.9 rozložit do tvaru $a = \prod p^{v(p,a)}$, kde součin jde přes všechny prvočísla $p \in \mathbb{Z}$ a kde exponenty $v(p,a) = v(p\mathbb{Z}, a\mathbb{Z})$ jsou jednoznačně určené, skoro všechny nulové. Pokud nyní vezmeme $w \in \mathbb{Q}$ takový, že $nw^2 \in \mathbb{Q}$, musí platit $w \in \mathbb{Z}$, protože n neobsahuje čtverec.

Předpokládejme, že $Tx, Nx \in \mathbb{Z}$ a vezměme $x_0 = y_0/2$, čili $y_0 = Tx \in \mathbb{Z}$ a $x_1 = y_1/2$, čili $y_1 \in \mathbb{Q}$. Potom $y_0^2 - ny_1^2 \in 4\mathbb{Z}$, tudíž $ny_1^2 \in \mathbb{Z}$, a tedy $y_1 \in \mathbb{Z}$ podobně jako výše.

Předpokládejme, že existuje algebraické celé číslo x, pro které $x_0 \notin \mathbb{Z}$, což znamená $y_0 \equiv 1 \pmod 2$. Potom $y_0^2 \equiv 1 \pmod 4$, což dává kongruenci $n \equiv 1 \pmod 4$. To dokazuje první ekvivalenci.

Konečně předpokládejme, že $n \equiv 1 \pmod 4$. Potom lze lehce ověřit, že $(1+\sqrt{n})/2$ má uvedený minimální polynom a tudíž patří do G. Z důkazu je patrné, že pokud je $x \in G$, potom buď $x \in \mathbb{Z}[\sqrt{n}]$, nebo $x = (y_0 + y_1\sqrt{n})/2$, kde $y_0 \equiv y_1 \equiv 1 \pmod 2$, a tedy $x - (1-\sqrt{n})/2 \in \mathbb{Z}[\sqrt{n}]$. ⊠

Speciálním příkladem pro $n \equiv 2, 3 \pmod 4$ je okruh Gaussových celých čísel $\mathbb{Z}[\sqrt{-1}]$, který je celistvým uzávěrem okruhu $\mathbb{Z}$ v tělese $\mathbb{Q}(\sqrt{-1}) = \{p + q\sqrt{-1} |\ p, q \in \mathbb{Q}\}$.

Také okruh $\mathbb{Z}[\sqrt{-5}]$ je Dedekindovým oborem, avšak ne Gaussovým. Jeho prvky totiž nemají jednoznačný rozklad, kupříkladu $6 = 2 \cdot 3 = (1 - \sqrt{-5})(1 + \sqrt{-5})$.

Okruh $\mathbb{Z}[\sqrt{n}]$, kde $n \equiv 1 \pmod 4$, není Dedekindův obor, ale přesto byly kategorie konečně generovaných modulů nad těmito okruhy klasifikovány, jak ukážeme v následující kapitole.

Kapitola 4

Zobecnění Dedekindových oborů

V následující kapitole uvedeme stěžejní poznatky z odvětví reprezentačních typů komutativních noetherovských okruhů. Tato teorie je oproti teorii Dedekindových oborů velice mladá. My se budeme zabývat známým problémem krotkosti a divokosti, ve kterém sehrávají důležitou roli zobecněné Dedekindovy okruhy poprvé popsané Levym v roce 1985 (viz. [Le]).

4.1 Krotkost, divokost

Značení 4.1.1. Buď R komutativní okruh. Množinu všech jeho maximálních ideálů budeme značit $\max(R)$. $\mathrm{fingen}(R)$ označme množinu konečně generovaných R-modulů. $\mathrm{finlen}(R)$ označme množinu modulů nad R konečné délky. Délku modulu jsme definovali v 3.1.4.

Definice 4.1.2. Buď K těleso a A vektorový prostor nad K s binární operací násobení. Potom A je *K-algebra*, pokud platí oboustranná distributivita a $(ax)(by) = (ab)(xy)$ pro libovolné $x, y \in A$, $a, b \in K$. Podle toho, zda je, či není operace násobení v A komutativní, říkáme ji komutativní či nekomutativní K-algebra.

Definice 4.1.3. *Konkrétní kategorie* je základní pojem teorie kategorií. Kategorie C a skládá se z třídy objektů $\mathrm{ob}(C)$ a třídy morfizmů $\mathrm{hom}(C)$ mezi objekty kategorie. Objekty jsou zde množiny a morfizmy jsou zobrazení. Pro $a, b \in \mathrm{ob}(C)$ značíme $\mathrm{hom}_C(a, b)$ množinu všech morfizmů z a do b. Pro každé tři objekty $a, b, c \in C$ je definována operace skládání morfizmů $\circ$:

$\hom_C(a,b)\times\hom_C(a,b) \to \hom_C(a,c)$, pro kterou platí asociativita, a pro každý objekt x existuje právě jeden morfizmus identita $1_x : x \to x$.

Podkategorie S kategorie C je dána podmnožinou objektů $\mathrm{ob}(S)$ a podmnožinou morfizmů $\hom(S)$ mezi těmito objekty. $\hom(S)$ je uzavřená na skládání morfizmů. Pokud pro každou dvojici $a, b \in \mathrm{ob}(S)$ platí $\hom_S(a,b) = \hom_C(a,b)$, nazýváme podkategorii S *úplnou kovariantní podkategorií.*

Definice 4.1.4. Buďte C, D kategorie. *Funktor* F z C do D je zobrazení, které každému objektu $x \in \mathrm{ob}(C)$ přiřadí objekt $F(x) \in \mathrm{ob}(D)$, každému morfizmu $f \in \hom_C(x,y)$ přiřadí morfizmus $F(f) \in \hom_D(F(x),F(y))$, a pro které platí $F(1_x) = 1_F(x)$ a $F(f \circ g) = F(f) \circ F(g)$ pro $x, y, z \in \mathrm{ob}(C)$, $f \in \hom_C(y,z)$ a $g \in \hom_C(x,y)$.

Definice 4.1.5 (fingen-krotkost)**.** Buď R komutativní noetherovský okruh. Řekneme, že fingen(R) má *krotký reprezentační typ*, nebo že R je *fingen-krotký*, pokud lze klasifikovat všechny třídy izomorfizmů konečně generovaných modulů, relace mezi jejich direktními sumami.

Definice fingen-krotkosti se může zdát poněkud neurčitá, avšak po doplnění formální definicí finlen-divokosti a vztahu těchto dvou pojmů se více zprůhlední.

Definice 4.1.6 (finlen-divokost)**.** Buď $K = R/\mathfrak{m}$ těleso zbytků komutativního noetherovského okruhu R pro nějaký $\mathfrak{m} \in \max(R)$. Řekneme, že finlen(R) má *divoký reprezentační typ* vzhledem k $\mathfrak{m}$, nebo že R je *finlen-divoký* vzhledem k $\mathfrak{m}$, pokud pro každou (ne nutně komutativní!) K-algebru A existuje úplná podkategorie $\mathcal{W} = \mathcal{W}_A$ kategorie finlen(R) a aditivní funktor $\Phi = \Phi_A : \mathcal{W} \to$ finlen(A) (kategorie levých A-modulů), který je *reprezentační ekvivalencí*, tj.

(i) Φ zobrazuje na všechny třídy homomorfizmů ve finlen(A).

(ii) Pro $M, N \in \mathcal{W}$ platí $M \cong N$ právě když $\Phi(M) \cong \Phi(N)$ ve finlen(A).

(iii) Φ je surjekce na grupách Hom.

Z této definice plyne, že M je nerozložitelný právě když $\Phi(M)$ je nerozložitelný. Pokud řekneme, že R je *finlen-divoký* bez zmínky o $\mathfrak{m}$, myslíme tím, že je finlen-divoký vzhledem k nějakému $\mathfrak{m} \in \max(R)$.

Poznámka 4.1.7. V literatuře se běžně setkáme se zkráceným označením *krotké* a *divoké okruhy.*

Poznámka 4.1.8 (Divoký okruh)**.** Předpokládejme nyní, že víme, že R je finlen-divoký vzhledem k nějakému $\mathfrak{m}$ a že známe všechny asociované funktory Φ_A. Buď $K = R/\mathfrak{m}$, A nějaká konečně dimenzionální K-algebra a vyberme libovolné dva moduly $X, Y \in \text{finlen}(A)$. Zajímá nás, jestli jsou izomorfní.

Protože $\Phi = \Phi_A$ je na všechny třídy izomorfizmu, existují $M, N \in \text{finlen}(R)$ takové, že $\Phi(M) \cong X$ a $\Phi(N) \cong Y$. Navíc, dle předchozí definice je $M \cong N \iff X \cong Y$. Tedy jsme převedli otázku izomorfnosti A-modulů (pro libovolnou konečně dimenzionální K-algebru) na otázku izomorfnosti modulů nad vlastním okruhem R.

Tedy finlen(R) je tak bohatý systém modulů konečné délky, že jakákoli klasifikace jeho tříd izomorfizmu by znamenala odpovídající klasifikaci A-izomorfizmů ve finlen(A) pro každou konečně generovanou K-algebru A. Domnělá beznadějnost ve vyjádření takové klasifikace je zodpovědná za název „divoký reprezentační typ“. Ještě nikdy nebyla explicitně popsána kategorie finlen(R) finlen-divokého okruhu R. (Na druhou stranu neexistuje věta z matematické logiky říkající, že taková klasifikace je nemožná.)

Poznámka 4.1.9. Uvědomme si, že každý homomorfní obraz fingen-krotkého okruhu je fingen-krotký. Naopak pokud se okruh zobrazuje nějakým homomorfizmem na finlen-divoký okruh, je sám finlen-divoký.

Následuje dobře známá věta dokázaná Drozdem a Crawley-Boeveyem.

Věta 4.1.10 (O krotkosti a divokosti)**.** *Buď K těleso zbytků komutativního noetherovského okruhu R. Pokud je K algebraicky uzavřené těleso, potom každá konečně dimenzionální K-algebra je buď krotká, nebo divoká, ale nikdy obojí.*

Důkaz. Lze nalézt v [CB, Theorem B]. ⊠

Věta 4.1.11. *Nechť R je noetherovský okruh. Pokud R není finlen-divoký vzhledem k žádnému $\mathfrak{m} \in max(R)$, potom*

(i) buď R je fingen-krotký,

(ii) nebo je R jeden z výjimečných okruhů popsaných dále v Poznámce 4.2.9.

4.2 Zobecnění Dedekindových oborů

Definice 4.2.1. Buď R okruh. Řekneme, že R je *redukovaný*, jestliže nemá žádné nenulové nilpotentní prvky, tj. každý prvek $x \in R$, pro který existuje $k \in \mathbb{N}$ takové, že $x^k = 0$, je roven nule.

Definice 4.2.2. *Nedělitelem nuly* nazýváme takový prvek a okruhu R, pro který neexistuje nenulový $b \in R$ takový, že $ab = 0$.

Definice 4.2.3. Buď R okruh. *Normalizací* nazveme celistvý uzávěr R v jeho podílovém tělese.

Definice 4.2.4. *Jacobsonovým radikálem* $J(R)$ komutativního okruhu R definujeme ideál, který je roven průniku všech maximálních ideálů tohoto okruhu.

Definice 4.2.5. Buď R komutativní okruh. Nenulový modul nad tímto okruhem se nazývá *jednoduchý*, pokud má pouze triviální podmoduly, tedy 0 a sebe sama.

Definice 4.2.6 (Zobecnění Dedekindových oborů)**.** Komutativní noetherovský okruh Λ nazýváme *zobecněným Dedekindovým okruhem*, pokud Λ je redukovaný a jeho normalizace Γ má následující vlastnosti:

(i) Γ je direktním součtem Dedekindových oborů,

(ii) $(\Gamma/\Lambda)_{\mathfrak{m}}$ je buď jednoduchý $\Lambda_{\mathfrak{m}}$-modul nebo 0,

(iii) $\mathfrak{m}_{\mathfrak{m}} = J(\Gamma_{\mathfrak{m}})$ a

(iv) $\Lambda_{\mathfrak{m}}$ není nikdy těleso (podmínka netriviálnosti)

pro každé $\mathfrak{m} \in \max(R)$.

Okamžitý důsledek bodu (ii) je, že pro každý $\mathfrak{m} \in \max(\Lambda)$ je normalizace $\Gamma_{\mathfrak{m}}$ lokalizace $\Lambda_{\mathfrak{m}}$ konečně generovaný $R_{\mathfrak{m}}$-modul. Avšak Γ nemusí být nutně konečně generovaný modul. Dále platí, že pokud popíšeme vlastnosti okruhu Λ, můžeme je téměř kdykoli vztáhnout na vlastnosti normalizace Γ, potažmo fingen(Γ).

Příklad 4.2.7. zobecněným Dedekindovým okruhem je například okruh $\Lambda = \mathbb{Z}[\sqrt{5}]$, který není Dedekindovým oborem, jak bylo poznamenáno na konci Kapitoly 3. Jeho normalizací je $\Gamma = \mathbb{Z}[1 + \frac{\sqrt{5}}{2}]$.

Obecně, každý okruh $\mathbb{Z}[\sqrt{n}]$, kde n je celé číslo neobsahující čtverec, je zobecněným Dedekindovým okruhem. Důkaz lze nalézt v [KL3, Example 36.3].

Lemma 4.2.8. *Buď Λ zobecněný Dedekindův okruh. Potom každý jeho ideál je generovaný dvěma prvky.*

Důkaz. Lze nalézt v [KL3, 10.9]. ⊠

Poznámka 4.2.9 (Výjimečné zobecněné Dedekindovy okruhy)**.** Mezi zobecněnými Dedekindovými okruhy existují tzv. *výjimečné zobecněné Dedekindovy okruhy*, u kterých se doposud neví, zdali jsou divoké nebo krotké. Jsou přesně definované v 4.2.9, avšak my se jimi nebudeme nadále zabývat. Uveďme si pouze důležité tvrzení, hovořící o „nevýjimečných“ okruzích.

Věta 4.2.10. *Každý zobecněný Dedekindův okruh, který nepatří mezi „výjimečné“ případy, je fingen-krotký.*

Důkaz. Důkaz této věty pokrývá podstatnou část textů [KL2] a [KL3]. ⊠

Na závěr uvedeme větu, která je zásadní v otázce určení krotkosti nebo divokosti nerozložitelných komutativních noetherovských okruhů. Zobecněné Dedekindovy okruhy hrají v tomto zařazení významnou roli. Stejně tak je potřeba zavést pojmy dalších okruhů. Jejich vlastnosti však pro stručnost dokazovat nebudeme a pouze odkážeme na texty [KL1], [KL2] a [KL3] zabývající se hlouběji problematikou krotkosti a divokosti.

Definice 4.2.11. Buď Ω komutativní noetherovský okruh a $M \in \mathrm{fingen}(\Omega)$. Zápis $\mu_\Omega(M)$ značí minimální počet prvků, potřebných ke generování modulu M.

Definice 4.2.12. Nechť Ω je komutativní artinovský a noetherovský lokální okruh, $\mathfrak{m} \in \max(\Omega)$ a k je příslušné těleso zbytků.

$(\Omega, \mathfrak{m}, k)$ nazýváme *artinovská triáda*, pokud $\mu_\Omega(\mathfrak{m}) = 3$ a $\mathfrak{m}^2 = 0$.

$(\Omega, \mathfrak{m}, k)$ nazýváme *Drozdův okruh*, pokud $\mu_\Omega(\mathfrak{m}) = \mu_\Omega(\mathfrak{m}^2) = 2$, $\mathfrak{m}^3 = 0$ a existuje prvek $x \in \mathfrak{m} - \mathfrak{m}^2$ takový, že $x^2 = 0$.

$(\Omega, \mathfrak{m}, k)$ nazýváme *Kleinův okruh*, pokud $\mu_\Omega(\mathfrak{m}) = 2$, $\mu_\Omega(\mathfrak{m}^2) = 1$, $\mathfrak{m}^3 = 0$ a pro každé $x \in \mathfrak{m}$ platí $x^2 = 0$.

Věta 4.2.13 (Okruhově-teoretická dichotomie)**.** *Buď R nerozložitelný komutativní noetherovský okruh. Potom nastává právě jedna ze dvou možností:*

(i) R se nějakým homomorfizmem zobrazuje na artinovskou triádu, nebo Drozdův okruh.

(ii) R je Kleinův okruh nebo homomorfní obraz zobecněného Dedekindova okruhu.

Důkaz. Divokost artinovských triád je dokázána v [GLW, Lemma 3], Drozdových okruhů pak v [KL1, 4]. Tedy na artinovské triády a Drozdovy okruhy nahlížíme jako na minimální finlen-divoké okruhy.

V [KL2, 11] je dokázáno, že Kleinovy okruhy jsou krotké. O situaci v zobecněných Dedekindových okruzích jsme se zmínili v 4.2.10. Tedy na Kleinovy a „nevýjimečné“ zobecněné Dedekindovy okruhy nahlížíme jako na maximální fingen-krotké okruhy.

Důkaz věty vyplývá přímo z těchto vlastností a Poznámky 4.1.9. ⊠

Literatura

[Aki] *Akizuki Y.:* **On the uniqueness of the coefficient ring in a polynomial ring,** J. Alg., 1972, 310-42.

[BK] *Berrick A. J., Keating M. E.:* **An Introduction to Rings and Modules, CSAM vol. 65,** Cambridge University Press, Cambridge, 2000.

[Bo] *Bourbaki N.:* **Algèbre commutative,** Hermann, 1961-83, Chap. 5.

[CB] *Crawley-Boevey W. W.:* **On tame algebras and BOCS's,** Proc. LMS, 1988, 451-483.

[Cl] *Claborn L.:* **Every abelian group is a class group,** Pacific J. Math **18**, 1966, 219-222.

[Ded] *Dedekind L.:* **Ůber die Theorie der Ganzenalgebraischen Zahlen, Supplement XI von Dirichlets Vorlesungen über Zahlentheorie,** 1894, 434-657.

[Dr] *Drápal A.:* **Komutativní algebra,** www.karlin.mff.cuni.cz/∼drapal/, 2006.

[Foss] *Fossum R. M.:* **The Divisor Class Group Of a Krull Domain, Ergebnisse der Mathnmatik und ihrer Grenzgebiete, 3. Floge, Band 1,** Springer-Verlag, Berlin, 1973.

[FS] *Fuchs L., Salce L.:* **Modules Over Non-Noetherian Domains** American Mathematical Society, 2000.

[GLW] *Guralnick R. M., Levy L. S., Warfield R. B. Jr.:* **Cancellation counterexamles in Krull Dimension 1,** Proc. Amer. Math. Soc., 1990, 323-326.

[KL1] *Klinger L. C., Levy L. S.:* **Representation type of commutative noetherian rings I: Local wildness,** Pacific J. Math, 2001.

[KL2] *Klinger L. C., Levy L. S.:* **Representation type of commutative noetherian rings II: Local tameness,** Pacific J. Math., 2001.

[KL3] *Klinger L. C., Levy L. S.:* **Representation type of commutative noetherian rings III: Global Wildness and Tameness,** Memoirs of the American Mathematical Society, 2005.

[Le] *Levy L. S.:* **Modules over Dedekind-like rings,** J. Algebra, 1985, 1-116.

[LT] *Levy L. S., Trlifaj J.:* **Γ-separated covers - Abelian Groups, Rings, Modules, and Homological Algebra,** Chapman & Hall/CRC, 2006, 203-216.

[Ma] *Matsumura H.:* **Commutative Ring Theory,** Cambridge University Press, 1989.

[Tr] *Trlifaj J.:* **Algebra I,** www.karlin.mff.cuni.cz/∼trlifaj/, 2009.