FILOZOFICKÁ FAKULTA
UNIVERZITA KARLOVA

BAKALÁŘSKÁ PRÁCE

Michal Ketner

Dělitelnost v okruzích

Katedra logiky

Vedoucí bakalářské práce: doc. RNDr. Vítězslav Švejdar, CSc.

Studijní program: Logika

Studijní obor: Logika

Praha 2024

Prohlašuji, že jsem tuto bakalářskou práci vypracoval(a) 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

Rád bych vyjádřil své upřímné poděkování všem vyučujícím na katedře logiky, kteří mě provázeli během studia a předali mi mnoho užitečných znalostí. Zvláštní dík patří Doc. RNDr. Vítězslavu Švejdarovi, CSc., za jeho odborné vedení, trpělivost a ochotu, které mi věnoval při zpracování bakalářské práce.

Název práce: Dělitelnost v okruzích

Autor: Michal Ketner

Katedra: Katedra logiky

Vedoucí bakalářské práce: doc. RNDr. Vítězslav Švejdar, CSc., katedra Logiky

Abstrakt: Práce si klade za cíl definovat teorii dělitelnosti pro obecné obory integrity a navrhnout hierarchii oborů dělitelnosti s vlastnostmi, které očekáváme, že budou platit obdobně jako při dělení celých čísel. Pomocí konceptu ideálů zobecňujeme Čínskou zbytkovou větu a demonstrovat, že oslabení obecnosti teorie může být výhodné, neboť disponujeme efektivnějšími nástroji pro hledání řešení. Tato práce je vhodná pro všechny zájemce o matematiku, kteří chtějí proniknout do teorie dělitelnosti, neboť budujeme teorii od základů a porovnáváme ji s dělením celých čísel.

Klíčová slova: Okruh, obor integrity, relace dělitelnosti, ideál, ireducibilní prvky a prvočísla

Title: The Divisibility Relation in Rings

Author: Michal Ketner

Department: Department of logic

Supervisor: doc. RNDr. Vítězslav Švejdar, CSc., Department of logic

Abstract: This thesis aims to define a theory of divisibility for general integral domains. A hiear- chy of divisibility domains with properties to those of division on the integers is outlined. Chinese residue theorem is generalized by means of ideals in order to demonstrate wea- kening of generalization, that provides more effective tools. The thesis is prepared for all those interested in mathematics who want to get an insight into the theory of divisibility, so we build the theory from the beginning and compare it with division on integers.

Keywords: Ring, integer domain, the divisibility relation, ideals, irreducibles and primes

Obsah

Úvod

Dělitelnost standardně zkoumáme ve struktuře celých nebo přirozených čísel. V této struktuře známe různé důležité věty z teorie čísel, například čínskou zbytkovou větu, která se využívá i v kryptografii. První zmínka o ní pochází ze třetího století našeho letopočtu z knihy Sun Tzu Suan Ching. V této práci si ukážeme, že tato věta lze zevšeobecnit pro libovolný obor integrity. Na struktuře celých čísel dále používáme Euklidův algoritmus, pojmenovaný podle starověkého filozofa Euklida, který jej uvedl ve svém díle Základy (cca 300 př. n. l.), přestože pravděpodobně není původním autorem. Ukážeme si, že tento algoritmus můžeme používat jen ve speciálních oborech, které nutně musí splňovat Základní větu aritmetiky, jejíž jednodušší verzi dokazuje už Euklides a je zapsána také v Základech.

Základní větu aritmetiky poté ve své knize Disquisitiones Arithmeticae Carl Friedrich Gauss dokázal i pro další struktury. Tato věta nám říká, že každé číslo lze jednoznačně rozložit. My tuto větu zevšeobecníme a ukážeme si, že můžeme používat rozklad jednoznačný až na asociativnost. Obor, kde lze použít Euklidův algoritmus, je také zároveň Bezoutovým oborem. To znamená, že platí Bezoutova věta, kterou v roce 1748 Leonhard Euler a Gabriel Cramer uvedli, avšak ani jednomu se nepodařilo dokončit důkaz. O několik let později, v roce 1764, Etienne Bezout přinesl první uspokojivý důkaz jako výsledek dřívější práce Colina MacLaurina. Tento důkaz však ve skutečnosti obsahoval několik neúplností. Kompletní důkaz byl představen o více než sto let později, v roce 1873, díky Georges-Henri Halphenovi.

Bezoutova věta nám říká, že největší společný násobek dvou čísel lze zapsat jako jeho lineární kombinaci. Existují však i obory, kde tento požadavek neplatí. Takovým příkladem je obor polynomů nad celými čísly, kde sice platí základní věta aritmetiky, ale neplatí v něm Bezoutova věta.

Obory, kde platí základní věta aritmetiky, se nazývají Gaussovy obory. Platí zde i opačný případ: existují Bezoutovy obory, kde základní věta aritmetiky neplatí. Dokonce existuje obor hodnot, kde neexistuje největší společný dělitel avšak i na těchto číslech funguje naše zevšeobecněná čínská zbytková věta.

1. Dělitelnost

1.1 Obory integrity a jejich vlastnosti

Dělitelnost obvykle bývá zkoumána na přirozených nebo celých číslech, a to vede k otázce, zda je tato teorie axiomatizovatelná a dá se popsat pro obecné struktury s vlastnostmi, které jsou spojeny s dělitelností.

V rámci této práce se zaměříme na takzvané unitární komutativní okruhy, což jsou algebraické struktury s dvěma operacemi + a ·, které jsou vzájemně distributivní a jsou asociativní a komutativní a obsahují neutrální prvky vůči oběma operacím. Tato struktura dále zahrnuje pro každý prvek svůj opačný prvek vzhledem k operaci sčítání. Nástin konstrukce a důkaz základních vlasností lze nahlédnout v Kořínek (1956)

Definujme strukturu $\mathbb{R} = (R, +, \cdot, 0, 1)$, kde R zastupuje nosič této struktury, a + a · jsou operace definované na tomto nosiči. Dále zahrnujeme konstanty nosiče 0 a 1.

Tyto dva prvky fungují jako neutrální prvky struktury, přičemž 0 je neutrálním prvkem pro operaci sčítání a 1 je neutrálním prvkem pro operaci násobení. Pro snazší pochopení použití nazývejme 0 jako nulový prvek a 1 jako jednotkový prvek.

Definice 1.1.1 (Unitární komutativní okruh)**.** *Struktura* $\mathbb{R}$ *bude je unitární komutativní okruh, právě tehdy když splňuje následující formule:*

1. *Asociativita operací:*

$$\forall x,y,z : (x + y) + z = x + (y + z),$$

$$\forall x,y,z : (x \cdot y) \cdot z = x \cdot (y \cdot z).$$

2. *Oboustranná distributivita sčítání a násobení:*

$$\forall x,y,z : x \cdot (y + z) = (x \cdot y) + (x \cdot z),$$

$$\forall x,y,z : (y + z) \cdot x = (y \cdot x) + (z \cdot x).$$

3. *Komutativita operací:*

$$\forall x,y : x + y = y + x.$$

$$\forall x,y : x \cdot y = y \cdot x.$$

4. *Existence neutrálních prvků:*

$$\forall x : x + 0 = x.$$

$$\forall x : x \cdot 1 = x.$$

5. *Existence opačného prvku pro sčítání:*

$$\forall x \exists y : x + y = 0.$$

Z výše popsané definice je zřejmé, že struktura $\mathbb{Z} = (Z,+,\cdot,0,1)$, tedy celá čísla s operací násobení a sčítání je také unitárním komutativním okruhem.

Obory integrity představují speciální typy unitárních komutativních okruhů, kde neexistují netriviální dělitelé nuly, což jsou nenulové prvky, jejichž součin dává nulu. Definujme strukturu $\mathbb{R} = (R,+,\cdot,0,1)$ jako obor integrity, pokud je unitárním komutativním okruhem a splňuje výše uvedenou formulaci, což si formálně zapíšeme.

Definice 1.1.2 (Obor integrity)**.** *Struktura $\mathbb{R}$ je oborem integrity, pokud je unitárním komutativním okruhem a platí následující formule:*

$$\forall x,y : x \cdot y = 0 \rightarrow (x = 0 \vee y = 0).$$

Dalším speciálním případem unitárních komutativních okruhů jsou tělesa, což jsou struktury, jež obsahují pro každý nenulový prvek jeho opačný prvek vzhledem k násobení, podobně jako u neutrálních prvků pro jasnost pojďme používat označení opačný pro prvek opačný vůči sčítání a inverzní pro prvek opačný vůči násobení.

Definice 1.1.3 (Těleso)**.** *Struktura $\mathbb{R}$ je tělesem, jestliže platí následující formule:*

$$\forall x \exists y : x * y = 1.$$

Nyní dokážeme, že pokud je struktura tělesem, nutně musí být i oborem integrity. Než se však do toho pustíme, dokažme nejprve jednoduché lemma, které říká, že v každém unitárním komutativním okruhu je součin s nulovým prvkem vždy nulový.

Lemma 1.1.4. *V unitárním komutativním okruhu platí formule:*

$$\forall a : a \cdot 0 = 0.$$

Důkaz. Zvolme libovolné a. Z definice nulového prvku dostaneme $a = a + 0$. Násobením obou stran a získáme $a^2 = a \cdot (a + 0)$. Díky distributivnímu zákonu platí, že $a^2 = a^2 + a \cdot 0$. V unitárním komutativním okruhu má a^2 opačný prvek, takže když přičteme tento prvek ke každé straně, získáme $0 = a \cdot 0$.

□

Věta 1.1.5. *Každé těleso je oborem integrity.*

Důkaz. Dokazujme sporem a uvažujme dva nenulové prvky a a b takové, že $ab = 0$. Z axiomu o inverzním prvku dostaneme prvek y takový, že $ya = 1$. Pokud nyní vynásobíme naši rovnici $ab = 0$ prvkem y, získáme $b = y \cdot 0$. Avšak podle předchozího lemmatu platí $y \cdot 0 = 0$, což znamená, že $b = 0$. To je v rozporu s předpokladem, že b je nenulový prvek, a tím jsme dospěli ke sporu.

□

V rámci studia dělitelnosti má smysl primárně zkoumat obory integrity, které nejsou tělesa. V tělesech, díky existenci inverzních prvků, je relace dělitelnosti triviálně splněna. Proto si definujme ty prvky, které mají inverzní prvky. Ukážeme si, že právě na těchto prvcích platí, že každý prvek dělí, a jsou dělitelné pouze invertibilními prvky, z nichž jeden zahrnuje i prvek jednotkový. Pro účely této práce můžeme tyto prvky identifikovat jako invertibilní třídu pro a pro nosič R jí značit jako R^*,

Definice 1.1.6 (Invertibilní prvek)**.** *V unitárním komutativním okruhu je prvek invertibilní, pokud k němu existuje inverzní prvek.*

Definice 1.1.7 (Invertibilní třída)**.** *Mějme unitárním komutativním s nosičem R, pak*

$$R^* = \{x \in R; \exists y : x \cdot y = 1\}.$$

Lemma 1.1.8. *V unitárním komutativním okruhu je jednotkový prvek invertibilní.*

Důkaz. Z axiomů unitárního komutativního okruhu víme, že pro libovolné x platí $(x = 1 \cdot x)$. Pokud dosadíme 1 za x, dostaneme $1 = 1 \cdot 1$. To implikuje, že jednotkový prvek je invertibilním prvkem, neboť je sám k sobě inverzní.

□

V závěrečné části tohoto oddílu dokážeme základní vlastnost oboru integrity, kterou je krácení, vyplývající přímo z axiomu o neexistenci vlastních dělitelů nulového prvku. Kromě toho také prokážeme, že pokud máme obor integrity, pak i polynomy nad tímto oborem tvoří obor integrity. Tím pádem jsme schopni konstruovat složitější struktury z jednodušších oborů integrity, pro které však budou platit stejné dokázané vlastnosti.

Lemma 1.1.9. *V oboru integrity platí formule:*

$$\forall x,y,z : (z \neq 0 \wedge xz = yz) \rightarrow x = y.$$

Důkaz. Uvažujme libovolné x, y a $z \neq 0$ takové, že $xz = yz$. Pro tyto prvky musí existovat opačný prvek. Přičteme tento opačný prvek k rovnici a dostaneme $xz - yz = 0$. S použitím axiomu distributivity získáme $(x - y) \cdot z = 0$. Avšak dle axiomu o neexistenci nenulového dělitele nuly musí platit buď $x - y = 0$ nebo $z = 0$. Vzhledem k předpokladu $z \neq 0$ musí platit $x - y = 0$, což implikuje $x = y$.

□

Nyní si ukážeme, jak konstruovat složitější okruh z jednoduššího tím, že rozšíříme obor integrity na polynomy.

Věta 1.1.10. *Nechť $\mathbb{R}$ je obor integrity. Potom $\mathbb{R}[x]$ je také obor integrity.*

Důkaz. Z definice sčítání a násobení polynomů je zřejmé, že asociativita, distributivita a komutativita operací, a také existence opačných prvků, plyne pouze z vlastností koeficientů, které splňují vlastnosti oboru integrity. V této struktuře existují nutně i nulový a jednotkový prvek, které odpovídají konstantním polynomům rovným nule, respektive jedné.

Nejdůležitější částí důkazu je prokázat, že součin dvou nenulových polynomů je také nenulový. Mějme dva polynomy $g(x) = \sum_{k=0}^{n} a_k x^k$ a $f(x) = \sum_{k=0}^{m} b_k x^k$. Bez újmy na obecnosti předpokládejme, že $a_n \neq 0$ a $b_m \neq 0$. Jelikož $a_n, b_m \in R$ a R je obor integrity, musí platit, že jejich součin $a_n \cdot b_m \neq 0$. To znamená, že $g(x)f(x) \neq 0$.

□

Tato věta naznačuje, že pokud máme obor integrity $\mathbb{R}$ (například reálná čísla, celá čísla nebo jiný obor integrity), pak i okruh polynomů nad tímto oborem $\mathbb{R}[x]$ (například polynomy s koeficienty z oboru $\mathbb{R}$) zůstává oborem integrity.

1.2 Dělitelnost

Definujme operaci dělitelnosti tak, jak je známa z celých čísel. Prvek a dělí prvek b, jestliže b je násobkem a. Dokažme, jak se vůči této relaci chová nulový prvek a jak se chovají invertibilní prvky.

Definice 1.2.11 (Dělitelnost)**.** *Nechť $\mathbb{R}$ je unitární komutativní okruh. Definujme relaci $|_{\mathbb{R}} \subseteq R \times R$ tímto předpisem*

$$|_{\mathbb{R}} = \{(a,b); \exists c : a = bc\}.$$

Pro účely této práce budeme pro relaci dělitelnosti místo $|_{\mathbb{R}}$ používat $|$. Zápis $a \mid b$ nám říká, že a dělí b. Dokažme, že relace dělitelnosti je kvaziuspořádáním. Nechceme dokazovat, že je relací úplného uspořádání, protože to obecně neplatí a vlastně to neplatí dokonce ani pro celá čísla, kde platí, že prvek a jeho opačný prvek se vzájemně dělí.

Věta 1.2.12. *Relace dělitelnosti v unitárním komutativním okruhu je kvaziuspořádáním.*

Důkaz. $\mathbb{R}$ je unitární komutativní okruh a podle definice existuje jednotkový prvek $a * 1 = a$ pro libovolné a.

To podle definice relace dělitelnosti znamená $a \mid a$. Dokázali jsme, že relace dělitelnosti je vždy v unitárním komutativním okruhu reflexivní.

Z předpokladu $a \mid b$ víme, že existuje $e \in R$ takové, že $b = ae$. Z $b \mid c$ víme, že existuje $f \in R$ takové, že $c = bf$. Dosadíme $b = ae$ do $c = bf$ a dostaneme $c = aef$.

Jsme v unitárním komutativním okruhu a tedy $g = ef$ pro nějaké $g \in R$. Dostali jsme $c = ag$ pro nějaké $g \in R$, což podle definice dělitelnosti znamená $a \mid c$.

Relace je tedy tranzitivní. Relace dělitelnosti je tedy kvaziuspořádáním.

□

V unitárním komutativním okruhu jsou přítomny nulový a jednotkový prvek, a proto je důležité ukázat, jak se tyto prvky chovají v relaci dělitelnosti. Nejdříve se podíváme na vlastnosti nulového prvku, který je přítomen v každém okruhu. Platí pro něj tyto formule, které jsou standardní a podobné jako v případě celých čísel.

Lemma 1.2.13. *Mějme unitární komutativní okruh* $\mathbb{R}$ *a* $e \in R^*$ *pak platí tyto formule:*

$$\forall a : a \mid 0.$$

$$\forall a : 0 \mid a \to a = 0.$$

$$\forall a : a \neq 0 \to e \mid a.$$

$$\forall a : a \mid e \to a \in R^*.$$

Důkaz. Mějme unitární komutativní okruh R a vezměme libovolný prvek a. Z definice relace dělitelnosti víme, že $a \mid 0$ odpovídá $0 = ac$ pro nějaké c. V lemmatu 1.1.4 jsme si dokázali, že platí $0 = ac$ pro $0 = c$. Podle definice tedy nutně musí platit $a \mid 0$ pro libovolné a.

Pokračujme důkazem druhé formule. Z $0 \mid a$ víme, že existuje $c \in R$ takové, že $a = c * 0$, což ale podle lemmatu 1.1.4 znamená, že $a = 0$. Vezměme libovolné nenulové a a $e \in R$.

Z definice invertibilního prvku víme, že existuje f takové, že $1 = ef$. Pokud tuto rovnici vynásobíme a, dostaneme $a = (ef)a$. S využitím asociativity násobení, která platí dle definice okruhu, získáme $a = e(fa)$, což podle definice znamená, že $e \mid a$.

Nechť e je libovolný invertibilní prvek a a je prvek z oboru integrity. Pokud platí $a \mid e$, víme, že $e = ag$ pro nějaké g. Protože e je invertibilní, existuje k němu inverzní prvek f takový, že $1 = ef$. Násobením rovnice $e = ag$ tímto inverzním prvkem získáme $ef = agf$, což je ekvivalentní s tím, že $1 = agf$. Tím pádem je gf inverzním prvkem k a, a tudíž je a invertibilní.

□

Nyní se zaměříme na definici dalších základních pojmů v teorii dělitelnosti. Mezi tyto pojmy rozhodně patří prvočísla, zejména v kontextu přirozených a následně celých čísel. Prvočísla definujeme pro přirozená čísla jako čísla dělitelná pouze samy sebou a jedničkou. Tato definice je pro unitární komutativní okruhy, jako jsou celá čísla, příliš restriktivní, protože invertibilní prvky mohou dělit libovolný prvek a může existovat více invertibilních prvků. Navíc jednička není vhodným kritériem, takže při definici prvočísel zaměníme jedničku za invertibilní prvky.

Tato definice prvočísel však není úplná, neboť v případě celých čísel jsou čísla obvykle dělitelná i číslem opačným k sobě. K tomu využijeme definici relace

asociování, která dáva do vztahu prvky, které se vzájemné dělí. Na základě tohoto pojmu poté definujeme vlastní dělitel jako prvek, který není invertibilní a není asociovaný s jiným prvkem.

Definice 1.2.14 (Asociování)**.** *Nechť $\mathbb{R}$ je unitární komutativní okruh. Definujme relaci $\|_{\mathbb{R}} \subseteq R \times R$ tímto předpisem:*

$$\|_{\mathbb{R}} = \{(a,b); a \mid_{\mathbb{R}} b \wedge b \mid_{\mathbb{R}} a\}.$$

Obdobně jako v předchozím případě relace dělitelnosti, budeme místo $a \|_{\mathbb{R}} b$ psát $a \| b$ a říkat, že a je asociováno s b. Jelikož, jak jsme dokázali, relace je symetrická, budeme říkat, že prvky a a b jsou asociovány. Dokažme si tedy o relaci asociování, že je ekvivalencí.

Věta 1.2.15. *Asociovaní na unitárním komutativním okruhu je ekvivalence.*

Důkaz. $\mathbb{R}$ je unitární komutativní okruh, a tedy existuje jednotkový prvek a prvky dělí samy sebe a proto $a \| a$ a relace je tedy reflexivní.

Pokud existuje $e \in R$ takové, že $a = be$, a zároveň existuje $f \in R$ takové, že $b = cf$, dosazením za b dostaneme $a = cef$. Máme nějaké $d \in R$ takové, že $d = ef$ a tedy $c = ad$, a tedy a dělí c. Máme tedy $a \mid c$. Relace asociování je tedy tranzitivní.

Relace asociování je tedy také kvaziuspořádáním. Nicméně si dokážeme, že je tedy dokonce ekvivalencí. Dokažme si tedy symetrii relace.

$a \| b$ znamená, že $a \mid b$ a současně $b \mid a$. Logická spojka a současně je komutativní, a tedy definice pro $b \| a$ je ekvivalentní $a \| b$. Relace asociování je symetrická.

Dokázali jsme tedy, že relace asociování je relace ekvivalence.

□

Díky této vlastnosti nyní můžeme sloučit podobné prvky v následující kapitole si popíšeme dva způsoby konstrukce, jak s těmito stotožněními pracovat. Nejdříve si ale definujme ještě několik základních pojmů z teorie dělitelnosti.

Definice 1.2.16 (Vlastní dělitel)**.** *Nechť $\mathbb{R}$ je unitární komutativní okruh. Prvek x je vlastním dělitelem prvku y, jestliže $x \notin R^*$, $x \mid y$ a prvky x a y nejsou asociované.*

S definicí vlastního dělitele můžeme pokračovat k definici ireducibilního prvku jako prvku, který nemá žadné vlastní dělitele, což je vlastnost, kterou na přirozených číslech mají prvočísla. Takovým prvek je nenulový neinvertibilní prvek, který nemá žádného vlastního dělitele.

Definice 1.2.17 (Ireducibilní prvek)**.** *Nechť $\mathbb{R}$ je unitární komutativní okruh a p je nenulový neinvertibilní prvek, pak p je ireducibilním prvkem, právě když v $\mathbb{R}$ neexistuje žádný vlastní dělitel prvku p.*

Toto je rozhodně stížejní pojem naší teorie, obvykle po prvočíslech požadujeme, aby pro ně platilo, že pokud prvek dělí součin dvouprvků, tak dělí aspoň jeden z nich. Formálně zapišíme tuto vlastnost a definujeme pojem prvočinitele.

Definice 1.2.18 (Prvočinitel)**.** *Nechť* $\mathbb{R}$ *je unitární komutativní okruh, tak p je prvočinitel, pokud není nula a není invertibilní a platí pro nej následující formule:*

$$\forall a,b : p \mid ab \to (p \mid a \vee p \mid b).$$

Definujme si nyní jak vypadá největší společný dělitel respektive množina největších dělitelů. Nejdříve si musíme definovat, jak vypadají společní dělitelé nějaké množiny a největší společný dělitel je poté takový prvek, který dělí všichni společní dělitelé z této množiny.

Definice 1.2.19 (Společný dělitel)**.** *Nechť* $\mathbb{R}$ *je unitární komutativní okruh a mějme nějaké neprázdné* $M \subseteq R$*, pak*

$$SD(M) = \{d; \forall m \in M(d \mid m)\}.$$

Pokud máme všechny společné dělitele nějaké množiny, tak největší z nich vybereme, tak že jej dělí všechny dělitelé množiny největších společných dělitelů.

Definice 1.2.20 (Největší společný dělitel)**.** *Nechť* $\mathbb{R}$ *je unitární komutativní okruh a mějme nějakou neprázdné* $M \subseteq R$*, pak*

$$NSD(M) = \{d; d \in SD(M) \wedge \forall m \in SD(M)(m \mid d)\}.$$

Největší společný dělitel však v unitárním komutativním okruhu nemusí existovat. Ukažme si, ale, že platí následující lemma, které nám říká jak chovají největší společní dělitelé při sjednocování množin.

Lemma 1.2.21. *Nechť* $\mathbb{R}$ *je unitární komutativní okruh, A a B jsou jeho dvě podmnožiny, kde* $A,B \subseteq R$*. Nechť a je největší společný dělitel množiny A (*$a \in NSD(A)$*) a b je největší společný dělitel množiny B (*$b \in NSD(B)$*), pak platí*

$$NSD(A \cup B) = NSD(\{a,b\}).$$

Důkaz. Nejdříve dokážeme inkluzi $NSD(A \cup B) \subseteq NSD(a,b)$. Mějme $d \in NSD(A \cup B)$. Podle definice $NSD(A \cup B)$ platí pro libovolný prvek $c \in SD(A \cup B)$, že $c \mid d$. Pro libovolné $c \in SD(A \cup B)$ platí $c \in SD(A)$ i $c \in SD(B)$. Z předpokladu $a \in NSD(A)$ a $b \in NSD(B)$ plyne, že $d \mid a$ a $d \mid b$, tedy $d \in SD(a,b)$. Dále dokážeme opačnou inkluzi $NSD(a,b) \subseteq NSD(A \cup B)$. Mějme $d \in NSD(a,b)$, což znamená, že d dělí a i b. Z předpokladu a dělí každý prvek z A a z transitivity plyne, že d dělí každý prvek z A. Obdobně, protože b dělí každý prvek z B, z transitivity plyne, že d dělí každý prvek z B. Tedy d dělí každý prvek z $A \cup B$, a tudíž $d \in SD(A \cup B)$. Dále dokážeme, že d je největším společným dělitelem. Mějme $h \in SD(A \cup B)$. Musí platit $h \in SD(A)$ a $h \in SD(B)$, odkud plyne $h \mid a$ a $h \mid b$, jinak by prvek a nebyl největším společným dělitelem A a b nebyl největším společným dělitelem B. Z toho plyne, že $h \in SD(a,b)$. Proto $h \mid d$, jinak by neplatilo $d \in NSD(a,b)$. Tedy $d \in NSD(A \cup B)$.

□

Nyní přejděme k pojmu ideálu, což jsou objekty, které stotožňují podobné prvky. Například ideálem na množině celých čísel jsou sudá čísla.

1.3 Úvod do ideálů

V této části se zaměříme na základní vlastnosti ideálů, které budeme využívat k důkazům v teorii dělitelnosti. Jejich vlastnosti přímo souvisejí s dělitelností. Ideál je neprázdná podmnožina obsahující nulový prvek a je uzavřená vůči sčítání a násobení prvky nadmnožiny.

Tato definice se podobá definici podokruhu, ale v případě ideálů nemůžeme vyžadovat, aby obsahovaly jednotkový prvek. V opačném případě by totiž by ideál byl celá nadmnožina, což by nebyl vlastní ideál a proto naší definici oslabujeme předpoklad na všechny komutativní okruhy, abychom mohli hledat i ideály z ideálů. Druhým příkladem nevlastního ideálu je podmnožina, která obsahuje pouze nulový prvek.

Ideály lze uspořádat podle relace dělitelnosti a je zřejmé, že nevlastní ideály jsou maximální a minimální prvky. Jak je zřejmé, ideál nemůže obsahovat jednotkový prvek, jinak by byl roven celému okruhu.

Definice 1.3.22 (Ideál)**.** *Mějme komutativní okruh a jeho neprázdnou podmnožinu $I \subset R$, pak $I \trianglelefteq R$, pokud platí:*

1. *Neutrální prvek:*
$$0 \in I.$$
2. *Uzavřenost na součet:*
$$(\forall a,b \in I)\,(a+b \in I).$$
3. *Uzavření na násobky z R:*
$$(\forall a \in I)\,(\forall r \in R)\,(ra \in I).$$

Zápis $I \trianglelefteq R$ říká, že I je ideálem v komutativním okruhu R. Občas se spíše hodí používat pro oveření ideálů odčítání, kde místo neutrálního prvku a uzavřenosti na sčítání požadujeme uzavřenost na odčítání. Ukažme si že tuto vlastnost lze použít jako test, protože pokud platí, tak množina musí být ideálem.

Definice 1.3.23 (Ideál test)**.** *Mějme komutativní okruh a jeho neprázdnou podmnožinu $I \subset R$, pak $I \trianglelefteq R$, pokud platí:*

1. *Uzavřenost na rozdíl:*
$$(\forall a,b \in I)\,(a-b \in I).$$
2. *Uzavření na násobky z R:*
$$(\forall a \in I)\,(\forall r \in R)\,(ra \in I).$$

Věta 1.3.24 (Ideál)**.** *Nechť R je unitární komutativní okruh pak definice 1.3.22 plyne z 1.3.23.*

Důkaz. Uvažujme, že máme nějaké a,$b \in I$.
Pak určitě platí, že pokud máme uzavřenost na odčítání tak musí platit $0 \in I$, protože libovolné a musí platit $a - a \in I$. Pak pro libovolné dva prvky platí, že $a - b \in I$, pak ale musí být i $a - 2b \in I$, protože platí $(a - b) - b = a - 2b$, když ale odečteme tyto dva prvky od sebe dostaneme také $-b \in I$, a jelikož ideál je uzavřen na odčítání tak musí platit i $a - (-b) \in I$, ale to z definice znamená, že $a + b \in I$.

□

Dokažme si nyní, jak se chovají zanořené ideály.

Lemma 1.3.25. *Mějme komutativní okruh a $I, J \trianglelefteq R$ takové, že platí $I \subseteq J$, potom $I \trianglelefteq J$.*

Důkaz. Ideál J je podstrukturou komutativního unitárního okruhu a tudíž musí být také komutativním okruhem. Dále víme, že I je uzavřené na sčítání, protože je samo ideálem v R. Je rovněž uzavřené na násobení prvky z J, neboť $J \subseteq R$, a jelikož $I \trianglelefteq R$, je dokonce uzavřené na násobení libovolným prvkem z R.

□

Na těchto ideálech můžeme zobecnit jejich operace jako operace ideálů. Je zřejmé, že kdybychom násobení uzavřeli jen na součiny prvků, tak $I \cdot J$ nemusí být ideál, protože není uzavřen na konečné součty součinů, takže součin ideálů na něj uzavřeme.

Definice 1.3.26. *Mějme komutativní okruh a I,$J \trianglelefteq R$, pak definujme:*

1. *Sčítání:*

$$I + J = \{i + j; i \in I, j \in J\}.$$

2. *Násobení:*

$$I \cdot J = \left\{ \sum_{k=1}^{n} a_k b_k \mid n \in \mathbb{N}, a_k \in I, b_k \in J \text{ pro } k = 1,2,\ldots,n \right\}$$

Dokažme si, že tyto definice zachovájí vlastnosti ideálů a plati, že $I+J$ a $I \cdot J$ jsou také ideály. Nejdříve ale proto budeme muset dokázat základní vlastnosti těchto operací a že jejich chování zachovává vlastnosti komutativního okruhu.

Lemma 1.3.27. *Mějme komutativní okruh I,J,$K \trianglelefteq R$, pak pro tyto ideály platí, že:*

1. *Distributivita:*
$$I(J+K) = IJ + IK$$
2. *Idempotence sčítání:*
$$I = I + I,$$
3. *Komutativita násobení:*
$$IJ = JI,$$

Důkaz. Začneme důkazem distributivity. Vezměme nějaký prvek $x \in I(J+K)$. Z definice existuje nějaké $a \in \mathbb{N}$ takové, že i_1,...,$i_a \in I$, j_1,...,$j_a \in J$ a k_1,...,$k_a \in K$ takové, že $x = \sum_{q=1}^{a} i_q(j_q + k_q)$. Použitím distributivního zákona na každý součin v součtu můžeme zápis upravit na $x = \sum_{q=1}^{a}(i_q j_q + i_q k_q)$ a jelikož R je asociativní, tak u prvků nezáleží na uzávorkování a tedy platí, že $x = \sum_{i=1}^{a}(i_a j_a) + \sum_{i=1}^{a}(i_a k_a)$, což z definice součtu a součinu ideálu znamená, že $x \in IJ + IK$. Mějme nyní nějaké $x \in IJ + IK$. Z definice existuje nějaké $a \in \mathbb{N}$ takové, že i_1,...,$i_a \in I$, j_1,...,$j_a \in J$ a k_1,...,$k_a \in K$ takové, že $x = \sum_{i=1}^{a}(i_a j_a) + \sum_{i=1}^{a}(i_a k_a)$. Prvky ve formuli díky asociativitě na původním okruhu můžeme přezávorkovat a dostaneme, že $x = \sum_{i=1}^{a}(i_a j_a) + \sum_{i=1}^{a}(i_a j_a + i_a k_a)$. Na každý tento prvek použijeme distributivní zákon a dostaneme $x = \sum_{i=1}^{a} i_a(j_a + k_a)$, což ale pak znamená, že $x \in I(J+K)$. Pokračujme důkazem idempotence. Uvažujme, že máme nějaké $a \in I$. Jelikož $0 \in I$, tak pak musí být $a \in I+I$ a tedy jsme dokázali, že $I \subseteq I+I$. Mějme nyní nějaké $a+b \in I+I$ a z definice součtu ideálů tedy a,$b \in I$. Jelikož každý ideál obsahuje 0, tak ke každému prvku musí obsahovat i prvek opačný, protože obsahuje rozdíl prvků. Máme tedy nějaké $-b \in I$. Jelikož ale ideál je uzavřen na rozdíly, tak musí platit, že $a+b \in I$. Nakonec dokážeme komutativitu součinu. Vezměme nějaké $x \in IJ$. Fixujme nyní nějaké $a \in \mathbb{N}$ takové, že i_1,...,$i_a \in I$ a j_1,...,$j_a \in J$ takové, že $x = \sum_{q=1}^{a} i_q j_q$. Pak máme $i_1 j_1 + .. + i_k j_k \in IJ$. Z definice určitě platí $i_1 j_1$,...,$i_a j_a \in R$. Okruh R je komutativní, takže pro každé $l \leq k$ platí $i_1 j_1 = j_1 i_1$ a dostaneme tedy, že $i_1 j_1 + .. + i_k j_k = j_1 i_1 + .. + j_k i_k$, což je nutně ale prvek JI. Důkaz opačné inkluze je stejný.

□

Už dříve jsme zmínili, že dokážeme ideály uspořádat do inkluze pomocí relace dělitelnosti. Pojďme si nyní dokázat část této inkluze.

Lemma 1.3.28. *Mějme komutativní okruh a $I, J \trianglelefteq R$, pak platí:*

$$\mathrm{IJ} \subseteq I \subseteq I + J,$$

$$IJ \subseteq I \cap J.$$

Důkaz. Nejdříve si dokažme, že $I \subseteq I + J$. Mějme nějaké $x \in I$ a podle definice ideálu je $0 \in J$, tedy z definice součtu ideálů dostáváme $x + 0 = x$ a tedy $x \in I + J$. Pokračujme důkazem, že $IJ \subseteq I$ a fixujeme nějaké $k \in \mathbb{N}$ a mějme $i_1,..,i_k \in I$, $j_1,..,j_k \in J$. Jelikož $J \subseteq R$ a ideál je uzavřený na násobení prvkem z R, dostáváme $i_1j_1,..,i_kj_k \in I$. Ale I je ideál, takže je uzavřen i na sčítání, tedy $i_1j_1 + .. + i_kj_k \in I$. Mějme nyní $x \in IJ$, pak nutně platí, že $x \in I$ a $x \in J$, což znamená, že $x \in I \cap J$.

□

Dokažme si nyní díky této inkluzi, že je to opravdu inkluze ideálu a tedy, že součet a součin ideálů jsou opravdu ideály.

Lemma 1.3.29. *Mějme komutativní okruh a $I, J \trianglelefteq R$, pak platí:*

$$I + J \trianglelefteq R,$$

$$IJ \trianglelefteq R.$$

Důkaz. Z definice ideálu platí, že $I \subset R$. V lemmatu 1.3.28 jsme dokázali, že $IJ \subset I$. Z transitivity podmnožiny dostaneme $IJ \subset R$. Dokažme si, že IJ je uzavřené na sčítání. Mějme prvky $i_1 + j_1$, $i_2 + j_2 \in I + J$. Dokažme si, že $(i_1 + j_1) + (i_2 + j_2) \in I + J$. Z asociativity a komutativity dostaneme $(i_1 + j_1) + (i_2 + j_2) = (i_1 + i_2) + (j_1 + j_2)$. Jelikož $I, J \trianglelefteq R$, víme, že existuje $i_3 \in I$, takže $(i_1 + i_2) = i_3$. Dále existuje $j_3 \in J$, takže $(j_1 + j_2) = j_3$. Potom z definice $I + J$ musí platit, že $i_3 + j_3 \in I + J$. Nyní mějme $r(i + j)$ pro $r \in R$, $i \in I$ a $j \in J$. Z distributivity dostaneme $r(i + j) = ri + rj$. Jelikož $I, J \trianglelefteq R$, víme, že $ri \in I$ a $rj \in J$. Tím pádem nutně musí být $ri + rj \in I + J$. Podle lemmatu 1.3.28 platí $IJ \subset I$. Z definice ideálu platí $I \subset R$. Tím pádem z transitivity dostaneme $IJ \subset R$. Ověříme nyní, že IJ je uzavřeno na sčítání. Mějme prvky z,$y \in IJ$ a chceme dokázat, že $z + y \in IJ$. Fixujme tedy k,$l \in \mathbb{N}$, takže $z = \sum_{i=1}^{k} a_ib_i$ a $y = \sum_{j=1}^{l} a_ib_i$. Sčítání je asociativní, takže $\sum_{i=1}^{k} a_ib_i + \sum_{i=1}^{h} a_ib_i = \sum_{i=1}^{k+h} a_ib_i$. Podle definice součinu takový prvek je také v IJ. Mějme nyní $r \in R$ a $z \in IJ$ takové, že $z = \sum_{i=1}^{k} a_ib_i$. Z distributivity prvků R plyne, že $rz = \sum_{i=1}^{k} ra_ib_i$. Každý $ra_i = c_i$ pro nějaké $c_i \in A$, protože A je ideál. Dostáváme tedy $rz = \sum_{i=1}^{k} c_ib_i$. Pak ale nutně musí platit $rz \in AB$.

□

Dokažme si, že i průnik ideálů je stále ideálem.

Lemma 1.3.30. *Mějme komutivní okruh a neprázdnou podmnožinu $S \subseteq R$, kde pro každé $s \in S$ je dán ideál $I_s \trianglelefteq R$, pak platí:*

$$\bigcap_{s \in S} I_s \trianglelefteq R.$$

Důkaz. Pro každé $s \in S$ platí z definice ideálu $I_s \subseteq R$. Tedy určitě $\bigcap_{s\in S} I_s \subseteq R$. Uvažujme prvky a a b patřící do $\bigcap_{s\in S} I_s$. Pokud by platilo $a + b \notin \bigcap_{s\in S} I_s$, pak musí existovat nějaké s, pro které $a + b \notin I_s$. To by znamenalo, že I_s není rovné celému R, což je v rozporu s předpokladem, že a a b patří do I_s. Uvažujme prvek $a \in \bigcap_{s\in S} I_s$ a prvek $r \in R$. Pokud by platilo $ra \notin \bigcap_{s\in S} I_s$, pak musí existovat nějaké t, pro které $ra \notin I_t$. To by opět znamenalo, že I_t není rovno celému R, což je v rozporu s předpokladem, že a patří do I_t.

□

Díky tomuto důkazu, že průnik ideálů je také ideálem, získáváme způsob, jak definovat ideál generovaný nějakou podmnožinou. Tuto definici budeme následně využívat k zavedení pojmu dělitelnosti pomocí ideálů. Definujme tedy generovaný ideál a podívejme se na jeho vlastnosti.

Definice 1.3.31 (Generovaný ideál)**.** *Mějme komutativní okruh a $M \subseteq R$, pak definujme:*

$$(M) = \bigcap \{S \mid M \subseteq S \text{ a } S \trianglelefteq R\}.$$

Lemma 1.3.32. *Mějme komutativní okruh a $M \subseteq R$, kde $M = \{a_1, \ldots, a_n\}$, pak platí:*

$$(M) = \{r_1a_1 + \cdots + r_na_n \mid r_1, \ldots, r_n \in R\}.$$

Důkaz. Nejdříve dokážeme, že $\{r_1a_1 + \cdots + r_na_n \mid r_1, \ldots, r_n \in R\} \subset (M)$.
Mějme libovolný prvek $r_1a_1 + \cdots + r_na_n$.
Podle definice každého $s \in \{S \mid M \subset S \text{ a } S \trianglelefteq R\}$ obsahuje $r_1a_1 + \cdots + r_na_n$.
To vyplývá z toho, že každé s obsahuje prvky $a_1, \ldots, a_n$.
Zároveň z předpokladu $s \trianglelefteq R$ vyplývá, že je uzavřen na násobení prvky z R.
Takže každé s obsahuje prvky $r_1a_1, \ldots, r_na_n \in s$.
Jelikož ideál je uzavřen na sčítání svých prvků, platí i $r_1a_1 + \cdots + r_na_n \in s$.
To vede k závěru, že $r_1a_1 + \cdots + r_na_n \in (M)$.
Nyní ukažme, že je opačná inkluze. Mějme $M \subset R$ a prvek $d \notin \{r_1a_1 + \cdots + r_na_n \mid r_1, \ldots, r_n \in R\}$.
To znamená, že existuje S takové, že $M \subset S$, $S \trianglelefteq R$ a $d \notin S$.
Z toho vyplývá, že $d \notin (M)$.

□

Speciálním případem generovaného ideálu je takzvaný hlavní ideál, kde M je jednoprvková množina.

Definice 1.3.33 (Hlavní ideál)**.** *Mějme komutativní okruh a nějaké $a \in R$, pak ideál $(a) = ra; r \in R$ nazýváme hlavní ideál generovaný prvkem a.*

Dokažme, že součet hlavních ideálů se rovná ideálu generovanému jejich sjednocením.

Lemma 1.3.34. *Mějme komutativní okruh a nějaké dva prvky a,$b \in R$ takové, že (a) a (b) jsou hlavní ideály, pak platí:*

$$(a,b) = (a) + (b).$$

Důkaz. Podle lemmatu 1.3.32 platí, že $(a,b) = \{r_1a + r_2b \mid r_1,r_2 \in R\}$.
Podle definice hlavního ideálu platí $(a) = \{ra \mid r \in R\}$ a $(b) = \{sb \mid s \in R\}$.
Podle definice součtu ideálů máme $(a) + (b) = \{ra + sb \mid r,s \in R\}$, což je zjevně to samé.

□

Dokažme, jak jsou hlavní ideály uspořádané vůči svému součtu.

Lemma 1.3.35. *Mějme komutativní okruh a nějaké dva prvky a,$b \in R$ takové, že (a) a (b) jsou hlavní ideály, pak platí:*

$$(a) \subseteq (a) + (b).$$

Důkaz. Mějme prvek $x \in (a)$. To znamená, že $x = sa$ pro nějaké $s \in R$. Komutativní okruh obsahuje nulový prvek. Protože součet ideálů obsahuje všechny možné kombinace koeficientů z R pro prvky a,b, musí obsahovat i prvek ve tvaru $sa + 0b$.

□

Samozřejmě, předchozí důkaz platí i pro druhý prvek součtu. Nyní si ukážeme, jaký vztah mají hlavní ideály vzhledem k dělení, abychom mohli zavést teorii dělitelnosti.

Lemma 1.3.36. *Mějme komutativní okruh a nějaké dva prvky a,$b \in R$ takové, že (a) a (b) jsou hlavní ideály, pak platí:*

$$a \mid b \leftrightarrow b \in (a) \leftrightarrow (b) \subseteq (a).$$

Důkaz. Podle definice hlavního ideálu platí $(a) = ra \mid r \in R$. Pokud $b \in (a)$, pak $b = ra$ pro nějaké $r \in R$, což odpovídá definici dělení, jak jsme ji definovali v předchozích částech. Mějme $q \in (b)$, což podle definice znamená, že $q = tb$ pro $t \in R$. Jestliže $b \in (a)$, existuje $g \in R$, pro které platí $b = ga$. Dosadíme-li za b, získáme $q = gra$ pro g,$t \in R$. Okruh je uzavřený na násobení, tudíž $tr = p$ pro nějaké $p \in R$. To znamená, že $q = pa$ pro nějaké $p \in R$ a tedy $q \in (a)$.

Pokud $a \mid b$, pak každý prvek z množiny (b) lze vyjádřit jako prvek z množiny (a) a tedy nutně platí $(b) \subset (a)$. Naopak, pokud platí $(b) \subset (a)$, to znamená, že

každý prvek z (b) lze vyjádřit jako prvek z (a). To však platí pouze v případě, že $a \mid b$, protože každý prvek b lze vyjádřit jako nějaký prvek z (a).

□

Nyní si definujme další dva důležité typy ideálů, které hrají v teorii dělitelnosti zásadní roli. Díky těmto pojmům, můžeme definovat prvočinitele a ireducibilní prvky. Pokud je (p) je maximální ideál, tak p je ireducibilní, pokud je (p) prvoideál, tak p je prvočinitel.

Definice 1.3.37 (Maximální ideál)**.** *Mějme komutativní okruh a $I \trianglelefteq R$, pak ideál I nazýváme maximální, pokud I je vlastní ideál a pro každý ideál $I \subseteq J$ platí:*

$$J = I \wedge J = R.$$

Definice 1.3.38 (Prvoideál)**.** *Mějme komutativní okruh a $I \trianglelefteq R$, pak ideál I nazýváme prvoideálem, pokud I je vlastní a platí:*

$$\forall a,b : ab \in I \rightarrow a \in I \wedge b \in I.$$

Nyní máme základní pojmy teorie dělitelnosti na ideálech. V další kapitole si ukážeme, jak tuto teorii využit k důkazu zobrazení mezi okruhy a také v důkazu Čínské zbytkové věty.

2. Okruhy a dělitelnost

2.1 Faktorokruhy

Jak lze nahlédnout v práci Přikrylová (2013) na okruzích lze dokázat dokázat věty o izomorfismech okruhů. Tyto věty následně využijeme, proto abychom pro libovolný okruh dokázali zobecněnou Čínskou zbytkovou větu, nebo ukázali konstrukci dalších zajímavých okruhů. Nejdříve si, ale musíme zadefinovat pojem relace modulo a faktorokruhu, které použijeme k důkazu.

Definujme si třídy rozkladu komutativního unitárního okruhu R pro $I \trianglelefteq R$, pro libovolné $a \in R$ takto $[a] = a + I = \{a + i | i \in I\}$. Sjednocením těchto tříd dostaneme faktorokruh.

Definice 2.1.1 (Relace modulo)**.** *Nechť R je komutativní okruh a $I \trianglelefteq R$, pak definujme relaci $|_I \subseteq I \times I$, pomocí formule:*

$$a \sim_I b \leftrightarrow a - b \in I.$$

Dokažme si nyní, že tato relace je relace ekvivalence a tudíž můžeme na základě této relace provést faktorizaci unitárního komutativního okruhu.

Věta 2.1.2. *Nechť R je komutativní okruh a $I \trianglelefteq R$, pak relace $\sim_I$ je relace ekvivalence.*

Důkaz. Dokažme nejdříve reflexivitu relace, což podle definice znamená $a \sim_I a$, což dává $a - a = 0$. Z definice okruhu víme, že $0 \in R$, a ideál je uzavřený na násobení prvky z R, tudíž musí platit $a - a \in I$.

Přejděme k důkazu symetrie. Víme, že platí $a - b \in I$. Jelikož $0 \in R$ a ideál je uzavřený na rozdíl, musí také platit $b - a \in I$.

Nakonec dokážeme transitivitu relace. Máme $a - b \in I$ a $b - c \in I$. Díky symetrii relace, kdy $c - b \in I$, a uzavřenosti ideálu na rozdíly, musí platit i $a - c \in I$.

Tím jsme ukázali, že $\sim_I$ je relace ekvivalence.

□

Máme tedy relaci ekvivalence přes nějaký ideál. Tato relace odpovídá chování relace modulo.

Zformalizujme a zapišme si tedy definici faktorokruhu přes ideál I. Označme tento faktorokruh jako $R \wr I$.

Definice 2.1.3 (Faktorokruh)**.** *Nechť R je okruh a $I \trianglelefteq R$. Na těchto třídách definujme operace a konstanty následovně:*

1. *Sčítání:*

$$(a + I) + (b + I) = (a + b) + I.$$

2. *Násobení:*

$$(a + I) \cdot (b + I) = (ab) + I.$$

3. Nulový prvek:

$$0_{R\wr I} = 0 + I.$$

4. Jednotkový prvek:

$$1_{R\wr I} = 1 + I.$$

5. Opačný prvek:

$$-(a + I) = (-a) + I.$$

Dokažme si nyní, jak vypadají podle této relace ekvivalence různé třídy v tomto faktorokruhu. Začneme tím, že dokážeme, jak vypadá nulová třída faktorokruhu.

Lemma 2.1.4. *Nechť R je unitární komutativní okruh a $I \trianglelefteq R$, pak $0_{R\wr I} = I$ a má vlastnost neutrálního prvku na faktorokruhu.*

Důkaz. Libovolný prvek v $0_{R\wr I}$ je ve tvaru $0+i$ pro nějaké $i \in I$. Neutrální prvek je neutrálním prvkem i v R, tudíž musí platit $0 + i = i$. Jinými slovy $0_{R\wr I} = I$.

Pokračujme tedy důkazem, že se chová jako neutrální prvek. Mějme nějaké a a $(a + I) + (0 + I)$, a nějaké j,$k \in I$, takže $(a + j) + (0 + k) = (a + 0) + (j + k)$, a z toho tedy dostaneme $(a + j) + (0 + k) = (a) + (j + k)$, což můžeme zapsat jako $a + I + I$. Podle lemma 1.3.27 to znamená, že je to $a + I$, takže $0 + I$ je neutrální prvek.

□

Lemma 2.1.5. *Nechť R je unitární komutativní okruh a $I \trianglelefteq R$, pak $1 + I_{R\wr I}$ má vlastnost jednotkového prvku na faktorokruhu.*

Důkaz. Dokažme, že $1 + I_{R\wr I}$ se chová jako jednotkový prvek. Z definice $(a + I) * (1 + I) = a * 1 + I$, což ale z definice jednotkového prvku na R znamená $(a + I) * (1 + I) = a + I$.

□

Dokažme si nyní, že faktorokruh je také okruhem, což je první ukázka toho, jak konstruovat složitější okruhy z unitárních komutativních okruhů.

Lemma 2.1.6. *Nechť R je unitární komutativní okruh a $I \trianglelefteq R$. Pak $R \wr I$ je unitární komutativní okruh.*

Důkaz. Z definice faktorokruhu máme $R \wr I = \{a + I \mid a \in R\}$.
Z vlastnosti $I \trianglelefteq R$ víme, že $I \subseteq R$, takže musí platit $a + I \in R$ pro libovolné $a \in R$ a tedy $R \wr I \subseteq R$. Mějme libovolný prvek $a + I \in R \wr I$.
Podle lemma 2.1.4 o faktorokruhu je zde nulový prvek $0_{R\wr I} = I$.
Dále podle lemma 2.1.5 existuje v faktorokruhu jednotkový prvek $1_{R\wr I}$.

Dokažme nyní, že přičtení I k libovolnému prvku vrátí tentýž prvek.
Mějme $a + I \in R \wr I$.

Pak $a + I + I = a + (I + I)$, ale podle lemma 1.3.27 víme, že $I + I = I$.
Takže $a + I + I = a + I$.

Nyní dokažme, že pro každý prvek existuje jeho opačný prvek.
Mějme $a + I \in R \wr I$. Podle definice okruhu víme, že pro libovolné $a \in R$ existuje $-a \in R$.
Z definice faktorokruhu tedy platí $-(a + I) \in R \wr I$.
Ověřme, že se jedná o skutečně opačný prvek.
Z definice faktorokruhu dostáváme $(a + I) - (a + I) = (a - a) + I = I$.
To podle lemma 2.1.4 znamená, že jsou skutečně opačné.

□

Dokažme si nyní, jak se chovají faktorokruhy zanořených ideálů.

Lemma 2.1.7. *Nechť R je unitární komutativní okruh a $I, J \trianglelefteq R$ takové, že platí $I \subseteq J$. Potom platí $J \wr I \trianglelefteq R \wr I$.*

Důkaz. Podle lemmatu 2.1.6 víme, že $R \wr I$ je komutativní okruh.
Z definice faktorokruhu a $J \subseteq R$ jasně plyne, že $J \wr I \subseteq R \wr I$.
Dokažme, že $J \wr I$ je uzavřené na sčítání.
Mějme prvky $a + I$ a $b + I \in J \wr I$. Z definice těchto prvků plyne, že $a, b \in J$. S ohledem na předpoklad $J \trianglelefteq R$ platí $a + b \in J$. Podle definice faktorokruhu dostaneme $(a+b)+I \in J \wr I$. Dále podle definice faktorokruhu platí $(a+b)+I = (a+I)+(b+I)$. Dokažme ještě uzavřenost na násobení prvky z okruhu. Mějme libovolné $(r + I) \in R \wr I$ a $a + I \in J \wr I$. Z vlastnosti $J \trianglelefteq R$ plyne $J \subseteq R$. Okruhy jsou uzavřené na násobení a $R \wr I$ je okruh podle lemmatu 2.1.6. Tím pádem $J \wr I$ je uzavřené na násobení prvky z okruhu.

□

Ukažme si, že díky faktorokruhům můžeme definovat test, zda je ideál prvoideál nebo maximální ideál, pokud známe strukturu faktorokruhu. Naopak můžeme také ukázat, že struktura je obor integrity nebo těleso. Tím samým můžeme dokázat, že každý prvoideál je zároveň maximální.

Věta 2.1.8. *Nechť R je unitární komutativní okruh a I je jeho ideál. Pak $R \wr I$ je obor integrity právě tehdy, když I je prvoideál.*

Důkaz. Předpokládejme, že I je prvoideál. Pro libovolné prvky $a, b \in R$ platí $(a + I)(b + I) = 0 + I$. Použijeme definici násobení ve faktorovém okruhu a dostaneme $(ab + I) = I$. To znamená, že $(a + I)(b + I) = 0 + I$, avšak jelikož I je prvoideál, musí platit $a \in I$ nebo $b \in I$. To vede k tomu, že $a + I = 0 + I$ nebo $b + I = 0 + I$, což znamená, že $R \wr I$ je obor integrity.

Nyní předpokládejme, že $R \wr I$ je obor integrity. Nechť $ab \in I$. Potom $ab + I = 0 + I$, což podle definice faktorového okruhu znamená $(a + I)(b + I) = 0 + I$. Z této rovnosti plyne, že $a + I = 0 + I$ nebo $b + I = 0 + I$, a to znamená, že $a \in I$ nebo $b \in I$. Tudíž je I prvoideál.

□

Dokažme si ještě nejdříve jedno jednoduché lemma, že tělesa nemají vlastní ideály.

Lemma 2.1.9. *R je těleso právě tehdy, když nemá žádné vlastní ideály.*

Důkaz. Dokažme to obě obměnou obou implikací:

Nechť $I \subset R$ je vlastní ideál. To znamená, že I neobsahuje žádný prvek $r \in R$, který by měl inverzní prvek v R. V opačném případě, kdyby takový prvek existoval, muselo by platit $I = R$, což je spor, neboť I je vlastní ideál. To dokazuje, že žádný prvek v I nemá inverzi v R.

Nechť R není těleso. To znamená, že existuje prvek $r \in R$, pro který $1 \notin rR$ (jinak by R bylo těleso). To znamená, že rR je vlastní ideál v R, protože neobsahuje jednotkový prvek.

Tím jsme dokázali obě implikace, což ukazuje, že tělesa nemají žádné vlastní ideály.

□

Tento důkaz ilustruje spojení mezi tělesem a absencí vlastních ideálů, který využijeme v následujícím důkazu, kdy ukážeme vztah maximálního ideálu a faktorokurhu, které je tělesem.

Věta 2.1.10. *Nechť R je komutativní unitární okruh a J je ideál v R. Pak $R \wr J$ je těleso právě tehdy, když J je maximální ideál.*

Důkaz. Dokažme nejprve implikaci, že těleso implikuje maximální ideál. Předpokládejme, že existuje ideál K v R, který obsahuje J a je obsažen v R. To znamená, že $K \supseteq J$, ale K není rovno celému R. Vezměme libovolný prvek $x \in K \setminus J$, což znamená, že $x + J \neq 0 + J$. Protože R/J je těleso, existuje prvek $y + J$ takový, že $(x + J) \cdot (y + J) = 1 + J$. To znamená, že existuje $j \in J$ takové, že $xy - j = 1$. Ale zároveň platí, že $J \subseteq K$, takže $j \in K$. To však implikuje, že $1 \in K$ a tudíž $K = R$, což je spor. Proto K musí být celé R, a tím pádem je J maximální ideál.

Dokažme opačnou implikaci. Předpokládejme, že J je maximální ideál v R. Definujme $I = a \in R : [a] \in K$, kde K je vlastní ideál v $R \wr J$. Je zřejmé, že I je ideál a platí $J \subseteq I$, protože $[0] \in K$, a jelikož K je vlastní ideál, musí platit I je vlastní ideál. To však vede ke sporu, protože J je maximální ideál. Podle předchozího lemmatu R/J je těleso, protože nemá žádné vlastní ideály.

□

Tento důkaz ukazuje spojitost mezi tělesem a vlastností maximálních ideálů v daném okruhu.

Věta 2.1.11. *Nechť R je komutativní unitární okruh, pak každý prvoideál je maximální.*

Důkaz. Tohle je přímý důsledek vět 1.1.5,2.1.10 a 2.1.8.

□

2.2 Okruhové homomorfismy

Ukažme si jak konstruovat různé další okruhy, nyní si definujme si nyní pojem okruhového homomorfismu. Okruhový homomorfismus je taková funkce, která mezi okruhy přenáší vlastnosti sčítání a násobení, což ukážeme k nastínění vztahů mezi různymi okruhy.

Definice 2.2.12 (Okruhový homomorfismus)**.** *Nechť R a S jsou okruhy. Funkce $f : R \to S$ je okruhový homomorfismus pokud:*

1. *Sčítání:*

$$f(a + b) = f(a) + f(b).$$

2. *Násobení:*

$$f(ab) = f(a)f(b).$$

3. *Nulový prvek:*

$$f(0_R) = 0_S.$$

Definujme si nyní ještě dva zásadní pojmy související s homomorfismy, prvním takovým pojmem je pojem jádra a obrazu zobrazení. Dokažme si, že takové jádro je dokonce ideálem našeho vzoru.

Definice 2.2.13 (Jádro a obraz homomorfismu)**.** *Nechť R a S jsou okruhy. Funkce $f : R \to S$ je okruhový homomorfismus pak definujeme:*

1. *Jádro:*

$$Ker(f) = \{a \in R | f(a) = 0\}.$$

2. *Obraz:*

$$Img(f) = \{f(a) | a \in R\} \subseteq S.$$

Lemma 2.2.14. *Nechť R a S jsou okruhy. Funkce $f : R \to S$ je okruhový homomorfismus. Pak platí $Ker(f) \trianglelefteq R$.*

Důkaz. Z definice funkce f plyne, že $Ker(f) \subseteq R$. Dokažme, že jádro je opravdu ideál a tudíž je uzavřené na sčítání a násobení prvky z R. Mějme tedy dva prvky $a, b \in Ker(f)$. Chceme dokázat, že i jejich součet bude v jádru. Z definice homomorfismu víme, že $f(a + b) = f(a) + f(b)$. Z předpokladu ale víme, že $a, b \in Ker(f)$, takže platí $f(a + b) = 0 + 0 = 0$. Tím pádem i $a + b$ je v jádru. Dokažme tedy, že je ještě uzavřené na násobení prvkem z okruhu. Mějme $r \in R$ a $a \in Ker(f)$. Podle definice homomorfismu víme, že $f(ra) = f(r) \cdot f(a)$. Z předpokladu víme, že $a \in Ker(f)$. Tím pádem $f(a)$ je nula. Jelikož pracujeme v okruhu, podle lemmatu 1.1.4 platí $f(r) \cdot f(a) = 0$ pro libovolné $r \in R$.

□

Teď dokážeme větu o homomorfismech, která nám ukáže, že pokud máme homomorfismus a nějaký ideál v definičním oboru, pak víme, jak zkonstruovat homomorfismus z faktorokruhu definičního oboru podle tohoto ideálu do stejného obrazu.

Věta 2.2.15 (O homomorfismu)**.** *Nechť R a S jsou okruhy, a funkce $f : R \to S$ je okruhový homomorfismus a $I \trianglelefteq R$ je ideál pro který platí $I \subseteq Ker(f)$, pak existuje okruhový homomorfismus $h : R \wr I \to S$ takový, že:*

1. *Hodnota:*
$$h(a + I) = f(a).$$
2. *Jádro:*
$$Ker(h) = Ker(f) \wr I.$$
3. *Obraz:*
$$Img(h) = Img(f).$$

Důkaz. Nejdříve ověřme, zda je funkce. Uvažujme $a+I$ a $b+I \in R \wr I$, pro které platí $a + I = b + I$.
To znamená, že máme $a + i = b + j$ pro nějaké i,$j \in I$.
Protože $I \trianglelefteq R$, je uzavřen vzhledem k opačným prvkům.
Dostáváme $a + i - i = b + j - i$, což plyne ve $a = b + k$ pro nějaké $k \in I$.
Z definice platí $h(a + I) = f(a)$ a podle našeho předpokladu tedy $h(a + I) = f(b + k)$.
Z definice homomorfismu dostáváme $h(a + I) = f(b) + f(k)$.
Protože platí $I \subseteq Ker(f)$, je $k \in Ker(f)$. Potom $h(a + I) = f(b)$.
To znamená, že $h(a + I) = h(b + I)$.
Mějme $(a + I) + (b + I)$, což podle definice znamená $(a + b) + I$.
Pak musí platit $h((a + I) + (b + I)) = h((a + b) + I)$.
Podle definice funkce h znamená, že $h((a + I) + (b + I)) = f(a + b)$.
Z definice homomorfismu dostáváme $h((a + I) + (b + I)) = f(a) + f(b)$.
Z definice funkce h dostáváme $h((a + I) + (b + I)) = h(a + I) + h(b + I)$.
Mějme $(a + I)(b + I)$, což podle definice znamená $(ab) + I$.
Pak $h((a + I)(b + I)) = h(ab + I)$.
Podle definice funkce h znamená, že $h((a + I)(b + I)) = f(ab)$.
Z definice homomorfismu dostáváme $h((a + I) + (b + I)) = f(a)f(b)$.
Proto z definice funkce h dostaneme $h((a + I)(b + I)) = h(a + I)h(b + I)$.
Podle definice $Ker(f) \wr I = \{a + I | a \in Ker(f)\}$.
Z definice funkce víme, že $Ker(f) \wr I = \{a + I | a \in Kerf\}$.
Dále víme, že $h(a + I) = 0 \leftrightarrow f(a) = 0$.
Z toho dostáváme $a \in Ker$

□

Ukažme si, že pro homomorfismy platí, že funkce je prostá tedy máme injektivní homomorfismus, pokud se na nulové prvky, zobrazí jen nulové prvky.

Lemma 2.2.16. *Nechť R a S jsou okruhy a funkce $f : R \to S$ je okruhový homomorfismus. Jestliže platí $f(a) = 0 \to a = 0$, pak f je injektivní.*

Důkaz. Uvažujme libovolné, vzájemně odlišné prvky a,$b \in R$. Jelikož pracujeme v okruhu, existuje prvek $a - b \in R$, pro který platí $a - b \neq 0$. Z předpokladu $f(a - b) \neq 0$ dostaneme $f(a) - f(b) \neq 0$ díky definici homomorfismu. To vede k závěru, že $f(a) \neq f(b)$, a tedy funkce f je injektivní.

□

Nyní si dokažme první větu o izomorfismu okruhu, který nám říká, že pokud máme okruhový homomorfismus, tak můžeme najít z faktorokruhu, který vznikne ze vzoru faktorizací přes jádro tohoto homomorfismu, izomorfismus do obrazu původní funkce.

Věta 2.2.17 (1. o izomorfismu)**.** *Nechť R a S jsou okruhy a funkce $f : R \to S$ je okruhový homomorfismus, pak $R \wr Ker(f)$ a $Img(f)$ jsou isomorfní.*

Důkaz. Využijeme větu o homomorfismu, vezměme $I = \mathrm{Ker}(f)$.
Získáme zobrazení $h : R \wr \mathrm{Ker}(f) \to S$. Zároveň platí $\mathrm{Img}(f) = \mathrm{Img}(h)$ a tudíž máme $h : R \wr \mathrm{Ker}(f) \to \mathrm{Img}(f)$. Tato funkce z definice obrazu je na. Nyní dokážeme, že platí $h(a) = 0 \to a = 0$, protože pak podle lemma 2.2.16 je zobrazení injektivní a je tedy izomorfismem. Uvažujme $a = b + \mathrm{Ker}(f)$. Pak nechť $h(a + \mathrm{Ker}(f)) = 0$. Z definice funkce získáme $f(a) = 0$, tudíž platí $a \in \mathrm{Ker}(f)$. Z toho vyplývá, že $a + \mathrm{Ker}(f) = \mathrm{Ker}(f)$. Dle lemma 2.1.4 faktorování okruhu znamená, že $a + \mathrm{Ker}(f) = [0]$.

□

Nyní si dokážeme třetí větu o izomorfismu, která nám říká, že když máme dva ideály, kde jeden je druhému podmonožinu. Tak pokud vytvoříme faktorokruh, kde okruhem je faktorokruh okruhu přes menší množinu a ideálem je faktorokruh z většího ideálu přes menší, tak je ekvivalentní s faktorokruhem okruhu přes větší ideál.

Věta 2.2.18 (3. o izomorfismu)**.** *Nechť R je okruh, I,$J \trianglelefteq R$ takové, že $J \subseteq I$, pak $(R \wr J) \wr (I \wr J)$ a $R \wr J$ jsou isomorfní.*

Důkaz. Uvažujme funkci $f : R \to R \wr I$ s předpisem $f(a) = a + I$. Nejdříve dokážeme, že tato funkce je na. Každý prvek $a + I$ v obrazu má ve vzoru prvek, který se na něj zobrazí. Dále dokážeme, že platí $Ker(f) = I$. Nejdříve dokážeme $I \subseteq Ker(f)$. Mějme $x \in I$, potom z definice funkce $x + I$. Jelikož $I \trianglelefteq R$ a je uzavřené na sčítání, platí $x + I \in I$. Dle lemma 2.1.4 znamená, že se prvek zobrazil do nulového prvku $R \wr I$. Tím pádem $x \in Ker(f)$. Nyní předpokládejme, že máme prvek $x \in R$, který není v I. Jinak by podle lemma 2.1.4) to znamená, že by platilo $x + I \in I$. To ale není možné, protože ideál je uzavřený na odečítání a tím pádem by musel obsahovat i x. Nyní použijeme větu o homomorfismu na tuto funkci. Ověříme její předpoklady. Máme, že $Ker(f) = I$, takže z předpokladu máme $J \subseteq Ker(f)$. Podle lemma 2.1.7 je J ideál v R. Máme tedy funkci

$h : R \wr J \to R \wr I$. Podle věty o homomorfismu platí $Img(h) = Img(f)$. Dokázali jsme tedy, že f je funkce na.
Z definice funkce a toho, že je na, dostáváme $Img(f) = R \wr I$. To znamená, že máme $Img(h) = R \wr I$. Dále z věty o homomorfismu dostáváme $Ker(h) = Ker(f) \wr J$. To znamená, že $Ker(h) = I \wr J$. Podle první věty o izomorfismu víme, že $(R \wr J) \wr Ker(h)$ je izomorfní s $Img(h)$. Dosadíme a dostáváme, že $(R \wr J) \wr (I \wr J)$ je izomorfní s $R \wr I$.

□

2.3 Komaximalita ideálů

Prokázali jsme, že součin je vždy podmnožinou průniku. V této části se zaměříme na speciální typy ideálů, pro které platí i opačná inkluze a kdy je součin právě průnikem těchto ideálů. Těmto speciálním ideálům budeme říkat komaximální. Nejdříve budeme muset nadefinovat tyto ideály.

Komaximální ideály jsou definovány jako ideály, jejichž součet je roven celému okruhu. Dále se zaměříme na definici nesoudělných ideálů a ukážeme si, že tyto nesoudělné ideály jsou právě komaximální ideály.

Poté dokážeme opačnou inkluzi, tedy že průnik ideálů je podmnožinou jejich součinu, pokud jsou tyto ideály komaximální. Tento důkaz rozšíříme pro libovolný počet ideálů.

Tímto způsobem se postupně zaměříme na studium komaximálních ideálů a jejich vztahů, což nám umožní aplikovat tyto poznatky v zobecněné Čínské zbytkové větě pro libovolný unitární komutativní okruh, proto zde v definici budeme používat unitární komutativní okruhy.

Definice 2.3.19 (Komaximalita)**.** *Nechť R je unitární komutativní okruh a I,$J \trianglelefteq R$, definujme : Ideály I,J jsou vzájemně komaximální, právě tehdy když $I+J = R$.*

Dále si nadefinujeme nesoudělnost ideálů, která je pro nesoudělna čásla obdobná s Bezoutovou větou, kterou si zachvíli také představíme.

Definice 2.3.20 (Nesoudělnost ideálů)**.** *Nechť R je unitární komutativní okruh a I,$J \trianglelefteq R$ a mějme $i \in I$ a $j \in J$, pak definujme : Ideály I,J jsou vzájemně nesoudělné, právě tehdy když $\exists i \in I$ a $\exists j \in J$ takové, že $i + j = 1$.*

Lemma 2.3.21. *Nechť R je unitární komutativní okruh a I,$J \trianglelefteq R$ jsou ideály. Definujme ideály I a J jako vzájemně komaximální právě tehdy, když jsou nesoudělné.*

Důkaz. Předpokládejme prvky $i \in I$ a $j \in J$ takové, že $i + j = 1$. Za prvé, je zřejmé, že $I + J \subseteq R$.

Nyní vezměme libovolný prvek $r \in R$ a vynásobme rovnici $i + j = 1$ tímto prvkem, což nám dá $r(i + j) = r$. Využitím distributivity dostaneme $ri + rj = r$. Jelikož I a J jsou ideály v R, platí $ri \in I$ a $rj \in J$. To následně znamená, že $r \in I + J$.

Nyní dokážeme opačnou implikaci. V unitárním komutativním okruhu platí $1 \in R$. Z definice $I + J = R$ víme, že existují prvky $i \in I$ a $j \in J$ takové, že $i + j = 1$.

□

Tento důkaz ilustruje vztah mezi komaximálními ideály a nesoudělností pro unitární komutatuvní okruhy. Dokažme si tedy nyní, že pokud máme komaximální ideály, jejichž součet je roven celému okruhu, pak jejich součin se rovná jejich průniku.

Lemma 2.3.22. *Nechť R je unitární komutativní okruh a I,$J \trianglelefteq R$ jsou komaximální. Pak platí $I \cap J = IJ$.*

Důkaz. Podle lemmatu 1.3.28 víme, že $IJ \subseteq I \cap J$. Dokažme nyní, že $I \cap J \subseteq IJ$.

Nejprve dokážeme, že $I \cap J = (I \cap J)(I + J)$. Mějme libovolný prvek $r \in I \cap J$. Podle lemmatu 1.3.30 platí $I \cap J \trianglelefteq R$. Z lemma 1.3.28 víme, že $I + J \trianglelefteq R$. Musí tedy platit, že $I + J \subseteq R$.

Podle lemmatu 1.3.30 je $I \cap J \trianglelefteq R$, což znamená, že je uzavřený na násobení prvky z okruhu. Tedy musí platit $r(i + j) \in I \cap J$ a tím pádem jsme dokázali $I \cap J \subseteq (I \cap J)(I + J)$.

Nyní dokážeme opačnou implikaci. Mějme prvek $m \in I \cap J$. Podle předpokladu z lemmatu 2.3.21 víme, že $1 \in I+J$ a tedy pro každý prvek platí $m \in (I \cap J)(I+J)$.

Z lemmatu 1.3.27 dostáváme $(I \cap J)(I + J) = (I \cap J)I + (I \cap J)J$. Dokázali jsme tedy $(I \cap J) = (I \cap J)I + (I \cap J)J$. Nyní dokažme, že $(I \cap J)I + (I \cap J)J \subseteq JI + IJ$.Nejprve dokážeme, že platí $(I \cap J)I \subseteq JI$. Každý prvek v $I \cap J$ musí být z definice průniku v J.Potom ale musí platit $(I \cap J)I \subseteq JI$.

Dokázali jsme tedy $I \cap J \subseteq IJ + JI$. Z lemma 1.3.27 dostáváme $IJ + JI = IJ$, takže dostáváme $I \cap J \subseteq IJ$.

□

Tento důkaz ukazuje platnost vztahu, kde průnik komaximálních ideálů je roven jejich součinu.

Rozšiřme nyní předchozí lemma pro libovolný počet prvků.

Lemma 2.3.23. *Nechť R je unitární komutativní okruh a $I_1, \ldots, I_n \trianglelefteq R$ jsou po dvou komaximální ideály, kde $n \geq 2$. Potom platí $I_1 \cap \cdots \cap I_n = I_1 \cdot \ldots \cdot I_n$ a ideály $I_1 \cap \cdots \cap I_{n-1}$ a I_n jsou komaximální.*

Důkaz. Budeme postupovat indukcí. Pro $n = 2$ jsme již důkaz provedli díky lemmatu o komaximálním průniku.

Pokračujme důkazem pro $n > 2$.

Podle lemmatu 1.3.29 je $I_1 \cdot \ldots \cdot I_{n-1}$ ideál.

Nyní dokažme, že $I_1 \cdot \ldots \cdot I_{n-1}$ a I_n jsou komaximální.

Pro všechna $i < n$ platí, že $I_i + I_n = R$.

V okruhu určitě platí $R \trianglelefteq R$.

Okruh R je uzavřen na násobení a sčítání, takže určitě nutně musí platit $R \cdot R = R$.

Pak ale nutně platí $R = (I_1 + I_n) \cdot \ldots \cdot (I_{n-1} + I_n)$.

Podle lemmatu 1.3.27 to upravíme na $R = I_1 \cdot \ldots \cdot I_{n-1} + I_n \cdot X$, kde X je určitě ideál.

Protože produkt $n - 2$ prvků je také ideál a součty ideálů jsou také ideály, a to je přesně ten výraz, který zapisujeme jako X.

Podle předpokladu $I_n \trianglelefteq R$ a tedy je uzavřen na násobení prvky z R.

Z toho, že $X \trianglelefteq R$, víme, že $X \subseteq R$.

Pak, ale musí platit $I_n \cdot X \subseteq I_n$.

Tím pádem dostaneme $R \subseteq I_1 \cdot \ldots \cdot I_{n-1} + I_n$.

Každý výraz je složen jen z prvků okruhu a součtů a součinů, na něž je okruh uzavřen. Rozhodně platí $I_1 \cdot \ldots \cdot I_{n-1} + I_n \subseteq R$.

Dokázali jsme tedy, že $I_1 \cdot \ldots \cdot I_{n-1}$ a I_n jsou komaximální.

Použitím lemma 2.3.22 dostaneme tedy $(I_1 \cdot \ldots \cdot I_{n-1}) \cdot I_n = (I_1 \cdot \ldots \cdot I_{n-1}) \cap I_n$.

Z indukčního předpokladu víme, že $(I_1 \cdot \ldots \cdot I_{n-1}) \cap I_n = (I_1 \cap \cdots \cap I_{n-1}) \cap I_n$. □

Nyní se zaměříme na dokázání, že pokud máme komaximální ideály, umíme sestrojit homomorfismus z unitárních komutativních okruhů do jejich faktorokruhů. Tento homomorfismus má jako jádro průnik těchto ideálů a je dokonce prosté, což nám poskytuje řešení pro modulární rovnice modulo tyto ideály.

Věta 2.3.24 (Komaximalita a homomorfismus)**.** *Nechť R je unitární komutativní okruh a $I_1, \ldots, I_n \trianglelefteq R$. Mějme homomorfismus $f : R \to R \wr I_1 \times \ldots \times R \wr I_n$ definovaný předpisem $f(a) = (a + I_1, \ldots, a + I_n)$. Pak platí $Ker(f) = I_1 \cap \ldots \cap I_n$ a f je surjektivní právě tehdy, když $I_1, \ldots, I_n$ jsou po dvou komaximální.*

Důkaz. Nejdříve dokážeme, že $Ker(f) = I_1 \cap \ldots \cap I_n$. Mějme $x \in I_1 \cap \ldots \cap I_n$, pak pro každé $i \leq n$ platí $x \in I_i$. Z definice funkce f pak víme, že $f(x) = x + I_i$. Pokud $x \in I_i$ a $I_i \trianglelefteq R$, je uzavřený na sčítání. Tedy nutně platí $f(x) = I_i$ a tedy $x \in Ker(f)$. Bez újmy na obecnosti uvažujeme nyní $x \notin I_1$, pak $x \notin Ker(f)$. Protože prvek z jádra se zobrazí vždy na prvek ideálu podle lemmatu 2.1.4. Kdyby $x + I \notin I_1$, podle lemmatu rozdílů ideálů bychom dostali $x \in I_1$, což je spor.

Nyní dokažme druhou část této věty. Předpokládejme, že f je surjektivní a mějme dva různé indexy $i \neq j$. Definujme funkci $h : R \wr I_1 \times \ldots \times R \wr I_n \to R \wr I_i \times R \wr I_j$ takovou, že pro $h(p_1 + I_1, \ldots, p_i + I_i, \ldots, p_j + I_j, \ldots, p_n + I_n) = f(p_i + I_i, p_j + I_j)$. Tato funkce je určitě také surjektivní, takže i složení těchto dvou funkcí musí být také surjektivní. Podle předpokladu $I_i, I_j \trianglelefteq R$. Potom podle lemmatu 1.3.29 je $I_i + I_j \trianglelefteq R$ a $I_i \subseteq I_i + I_j$. Pak podle lemmatu 2.1.4 je ideál $(I_i + I_j) \wr I_i$ v $R \wr I_i$. Podle lemmatu 2.1.6 je $R \wr I_i$ okruh. Dále jsme ve větě 3. o izomorfismu dokázali, že existuje bijekce do $R \wr (I_i + I_j) \times R \wr (I_i + I_j)$, která samozřejmě musí být surjektivní. Složením dvou surjektivní funkci získáme opět surjektivní funkci $v : R \to R \wr (I_i + I_j) \times R \wr (I_i + I_j)$, protože zobrazení v zobrazuje prvek na dvojici stejných prvků, což znamená, že $R \wr (I_i + I_j)$ musí mít jen jeden prvek. Pokud by tu byly aspoň dva různé prvky $a, b \in R \wr (I_i + I_j)$, pro tuto funkční hodnotu $(a + I_i + I_j, b + I_i + I_j)$ by neexistoval obraz, což je spor s tím, že funkce je surjektivní. Podle lemmatu 2.1.6 je $R \wr (I_i + I_j)$ okruhem, tudíž musí obsahovat neutrální prvek vzhledem ke sčítání. Podle lemmatu 2.1.4 platí $R \wr (I_i + I_j) = I_i + I_j$, což nám říká, že libovolný prvek $x \in R$ lze zapsat jako součet prvků z I_i, I_j, a tedy ideály jsou komaximální.

Pokračujme důkazem druhé části implikace. Mějme $I_1, \ldots, I_n$ komaximální ideály a postupujeme indukcí podle počtu ideálů. Ukažme případ, kdy $n = 2$. Tedy pro libovolné $a \in R \wr I_1$ a libovolné $b \in R \wr I_2$ existuje $r \in R$, pro které platí $a + I = r$ a $b + I = r$. Podle lemmatu 2.3.21 jsou tedy I_1, I_2 nesoudělné a existuje $c \in I_1$ a $d \in I_2$ takové, že $c + d = 1$. Definujme nyní $r = ad + bc$. Ukážeme, že $r \sim_{I_1} a$ a $r \sim_{I_2} b$. Podle definice ekvivalence to znamená, že $r - a \in I_1$ a $r - b \in I_2$. Z definice r dostaneme $r - a = (ad + bc) - a$ a $r - b = (ad + bc) - b$, což po úpravách

dá $r-a=bd-ad$ a $r-b=ac-bc$. Když použijeme distributivitu a odstraníme závorky, dostaneme $r-a=ad+bc-ac-ad$ a $r-b=ad+bc-bc-bd$. Na obě rovnice použijeme distributivitu a získáme $r-a=c(b-a)$ a $r-b=d(a-c)$. Podle předpokladů $a-c$,$b-a\in R$ a $d\in I_1$ a $d\in I_2$, a protože I_1,$I_2\trianglelefteq R$, jsou uzavřené na násobení prvky z R, a tedy platí $r-a\in I_1$ a $r-b\in I_2$. Předpokládejme nyní, že máme dokázáno pro $n-1$. Definujme $I=I_1\cdot\ldots\cdot I_{n-1}$. Podle lemmatu 2.3.23 víme, že $I=I_1\cap\ldots\cap I_{n-1}$ a také, že I,I_n jsou vzájemně komaximální. Tak máme zobrazení $h:R\to R\wr I_1\times\ldots\times R\wr I_{n-1}$ s předpisem $h(a)=(a+I_1,\ldots,a+I_n)$ takové, že $Ker(h)=I$. V kroku pro $n=2$ jsme dokázali, že situaci umíme řešit pro libovolné dva faktorokruhy s komaximálními ideály. Máme tedy i $g:R\to R\wr I\times R\wr I_n$. Dokážeme, že $R\wr I_1\times\ldots\times R\wr I_{n-1}$ je okruh, což plyne z toho, že $R\wr I_i$ pro $i\leq n$ je podle lemmatu 2.1.6 okruhem, a operace na produktech okruhů jsou prováděny po složkách, tudíž i jejich součin bude okruhem. Nyní si dokažme, že h je homomorfismus. Nejdříve dokažme součet. Mějme tedy $h(a)=(a+I_1,\ldots,a+I_n)$ a $h(b)=(b+I_1,\ldots,b+I_n)$. Potom $h(a)+h(b)=(a+I_1,\ldots,a+I_n)+(b+I_1,\ldots,b+I_n)$. Po sčítání po složkách získáme $h(a)+h(b)=(a+b+I_1,\ldots,a+b+I_n)$, což je definice $h(a+b)$, takže $h(a)+h(b)=h(a+b)$. Důkaz pro násobení je analogický. Podle definice $h(0)=(I_1,\ldots,I_n)$ je zobrazení h homomorfismus. Použitím věty 1. o izomorfismu získáme izomorfismus $i:R\wr I\to R\wr I_1\times\ldots\times R\wr I_{n-1}$. Tak získáme zobrazení, kde složíme h a vnější zobrazení bude $i\times id$, kterému budeme říkat f. Zobrazení f je surjektivní, protože je složeno ze dvou surjektivních zobrazení.

□

Důsledkem této věty je zobecněná forma Čínské zbytkové věty.

Věta 2.3.25 (Čínská zbytková věta)**.** *Nechť R je unitární komutativní okruh a $I_1,\ldots,I_n\trianglelefteq R$ jsou komaximální ideály takové, že $I_1\cap\ldots\cap I_n=0$. Potom pro libovolné prvky $r_1,\ldots,r_n\in R$ existuje právě jedno $r\in R$, pro které platí $r\sim r_i, mod, I_i$ pro všechna $i\leq n$.*

Důkaz. Podle věty o komaximalitě a homomorfismu víme, že díky komaximalitě ideálů je zobrazení $f:R\to R\wr I_1\times\ldots\times R\wr I_n$ injektivní. Tedy pro libovolné $r_1,\ldots,r_n\in R$ existuje $r=r_i+I_i$.

Předpokládejme, že existují dva různé prvky r a s v R, oba jsou různými řešeními. Pro každé $i\leq n$ platí, že existuje $x\in I_i$ takové, že $r+x=s$.

Zde využijeme skutečnost, že $0\in I_i$ pro každé $i\leq n$. Poté $r+0=s$, což znamená, že rovnice má pouze jedno řešení.

Podle věty o komaximalitě a homomorfismu $x\in I_1\cap\ldots\cap I_n$. Pokud by bylo $x\neq 0$, došli bychom k sporu s předpokladem $I_1\cap\ldots\cap I_n=0$.

□

Tato verze Čínské zbytkové věty potvrzuje existenci a jednoznačnost řešení systému kongruencí na unitárním komutativním okruhu, pokud jsou ideály, na které modulo bereme, komaximální a tedy průnik ideálů je nulový.

3. Konstrukce oboru a jejich hiearchie

3.1 Obory integrity a jejich nroma

Jak ukazuje 3. věta o izomorfismu, funkce, která zobrazuje x na odmocninu z $-p$ pro nějaké p, které není násobkem druhé mocniny žádného celého čísla, nám ukazuje, jak je $\mathbb{Z}$ adjungované o ideál této odmocniny, označované jako $\mathbb{Z}[(i\sqrt{p}]$, isomorfní podle tohoto okruhového homomorfismu s faktorovým okruhem $\mathbb{Z}[x]$ přes ideál generovaný $x^2 + p$. Jelikož podle věty 1.1.10 polynomy jsou obory integrity, tak $\mathbb{Z}[x]$ musí být také oborem integrity. Na něm můžeme aplikovat větu, která nám říká, že pokud máme prvoideál, přes který provedeme rozklad, tak výsledek je také oborem integrity. Být oborem integrity je prvořadová vlastnost a proto je zachovávána izomorfismem, jak můžeme vidět v Kunen (2021), a přenáší se se tedy mezi strukturami, a proto i $\mathbb{Z}[(i\sqrt{p}]$, musí být oborem integrity. Toto nám dává návod, jak počítat normy na těchto oborech integrity. Definujme normu jako vlastnost, kde chceme přenést vlastnosti dělitelnosti na nějakém složitějším oboru integrity a testovat ji pomocí přirozených čísel.

Definice 3.1.1. *Nechť R je obor integrity a funkci $f : R \setminus \{0\} \longrightarrow \mathbb{N}$ nazveme multiplikativní normou, pokud splňuje následující pravidla pro libovolné a, b:*

1. $f(a) = 0 \Leftrightarrow a = 0$,
2. $f(ab) = f(a) \cdot f(b)$.

Lemma 3.1.2. *Mějme obor integrity R a jeho multiplikativní normu f. Platí:*

1. $u \in R^* \rightarrow N(u) = 1$
2. $((N(u) = 1 \rightarrow u \in R^*) \rightarrow (N(p)$ *je prvočíslo* $\rightarrow p$ *je ireducibilní v* $R))$

Důkaz. Začneme nejdříve zvláště důkazem pro jedničku, což pak využijeme u dalších invertibilních prvků. Je zřejmé z definice, že platí $f(1) = f(1*1) = f(1)*f(1)$, což znamená na přirozených číslech, že $f(1) = 0 \wedge f(1) = 1$, ale podle předpokladu nula nemůže být, takže musí platit $N(1) = 1$. Pokračujme důkazem pro nějaké invertibilní číslo x, pro které tedy existuje inverzní číslo y a máme $xy = 1$, což znamená $1 = f(1) = f(x*y) = f(x)*f(y)$, ale v přirozených číslech je invertibilní pouze jednotka. Nakonec mějme nějaké x, pro které $f(x)$ je prvočíslo v N. Mějme $x = yz$, tak dostaneme $f(x) = f(y) * f(z)$, ale jelikož $f(x)$ je prvočíslo, tak jeden z prvků musí být roven jedné a tím pádem podle předpokladu je invertibilní, a tím je x ireducibilní.

□

Nejjednodušší formou takové normy je samozřejmě absolutní hodnota na celých číslech. To teď využijeme a definujeme další faktorový okruh.

V předchozí kapitole jsme zkoumali dělitelnost v oborech integrity. Nyní budeme přidávat další vlastnosti k oboru integrity a zkoumat vzájemný vztah těchto vlastností.

První podmínkou je existence největšího společného dělitele pro libovolnou konečnou množinu. Druhá podmínka byla již dříve zmíněna; jedná se o tvrzení, že každý ireducibilní prvek je prvočinitelem. Ukážeme si, že pokud máme zaručeného největšího společného dělitele, tak tato podmínka také platí. Z této podmínky dále plyne, že pokud máme dva asociované součiny, jejich prvky rozkladu jsou vzájemně asociované.

Čtvrtá podmínka se týká toho, že relace $\preceq$ na $[R]$ je fundovaná. Z této podmínky plyne, že každé číslo má ireducibilní rozklad. Ukážeme si, že pokud vezmeme Gaussův obor, což je obor, kde platí třetí a pátá podmínka, tak v něm platí všechny ostatní podmínky. Tento obor je přesně takový, kde platí zobecněná forma Základní věty aritmetiky, která říká, že každý prvek má jednoznačný rozklad až na asociativitu prvků.

Standardní věta o přirozených číslech je přirozeným důsledkem, protože neobsahuje asociativní prvky. Pro celá čísla to znamená, že v rozkladu mohou být i záporná čísla.

Definujme tento faktorový okruh prostřednictvím relace asociaciování na množině R. Tuto faktorovou množinu budeme značit jako $[R]$. Na této množině zavedeme uspořádání $\preceq$. Jestliže $a \in R$, pak třídu ekvivalence, která obsahuje prvek a, označíme jako $[a]$. Definujme tedy pomocí $a \in R$ množinu $[R]$. Inspirací pro podmínky dělitelnosti byla kniha Procházka (1990)

Definice 3.1.3 (Faktorový okruh)**.** *Nechť R je obor integrity. Pak $[R] = \{[a]; a \in R\}$.*

Faktorová množina $[R]$ je množina tříd ekvivalence podle relace asociování. Nyní se podívejme postupně, jak vypadají jednotlivé třídy, a definujme uspořádání těchto tříd.

Definice 3.1.4 (Uspořádání na faktorové množině)**.** $[a] \preceq [b] \leftrightarrow a \mid b$

Relace $e \preceq d$ je zřejmě relací uspořádání na množině $[R]$. Nyní to dokážeme.

Věta 3.1.5 (Uspořádání)**.** *Relace $\preceq$ na množině $[R]$ je relací uspořádání.*

Důkaz. V větě 1.2.12 jsme si dokázali, že $a \mid a$ a tedy $[a] \preceq [a]$, což znamená, že relace je reflexivní. Pokud $[a] \preceq [b]$, tak $a \mid b$, a $[b] \preceq [c]$, tak $b \mid c$. Jak jsme si ukázali v Lemma 1.2.12, relace dělitelnosti je tranzitivní. Dostáváme tedy $a \mid c$, což znamená $[a] \preceq [c]$. Relace $\preceq$ je tedy na R tranzitivní. Pokud $a \preceq b$, znamená to, že $a \mid b$, a zároveň $b \preceq a$ znamená, že $b \mid a$. Takže $b \mid a$ a $a \mid b$, což odpovídá definici $b \parallel a$, tudíž relace je symetrická. Dokázali jsme tedy, že relace je uspořádání.

□

Nejdříve ukažme, jak vypadá třída obsahující nulový prvek a jak třída obsahující jednotkový prvek.

Lemma 3.1.6. *Nechť R je obor integrity. Pak $[0] = \{0\}$.*

Důkaz. Mějme obor integrity R.

Rozhodně platí $0 \subseteq [0]$, protože relace ekvivalence je reflexivní.

Vezměme libovolný prvek $a \in [0]$. Podle definice víme, že $a \mid 0$. To ale podle lemmatu 1.1.4 znamená, že $a = 0$.

□

Víme tedy, jak vypadá třída, ve které je nulový prvek. Už dříve jsme dokázali, že jednotkový prvek je invertibilní a že invertibilní prvek dělí zase jen prvek invertibilní. Ukažme, že všechny invertibilní prvky jsou ve stejné třídě ekvivalence.

Lemma 3.1.7. *Nechť R je obor integrity. Pak $R^* = [1]$.*

Důkaz. Nejdříve dokážeme, že $R^* \subseteq [1]$.

Vezměme libovolný prvek $e \in R^*$. Podle lemmatu 1.3.29 víme, že pro libovolný prvek $a \in R$ platí $e \mid a$, a tedy to platí i pro $1 \in R$. Ze stejného lemmatu plyne, že $1 \mid e$ a tedy z definice asociace dostáváme, že $1 \parallel e$. Podle definice třídy ekvivalence $[1]$ dostaneme $e \in [1]$.

Nyní dokažme $[1] \subseteq R^*$. Mějme prvek $e \in [1]$. Podle definice víme, že $e \mid 1$. Máme tedy $1 = ef$ pro nějaký prvek $f \in R$, což znamená, že prvek e je invertibilní v R.

□

Dokažme, že následující prvky jsou maximální a minimální prvky v tomto uspořádání. Vzhledem k tomu, že relace $\preceq$ je slabě antisymetrická, pokud $a \preceq b$ a $b \preceq a$, pak $[a] = [b]$. Abyste odlišili takové prvky v uspořádání, použijeme $a \prec b$, pokud $a \preceq b$ a $[a] \neq [b]$. Nyní si dokážeme, jak se v tomto uspořádání chovají nulová a invertibilní třída. Ukážeme si, že třída ekvivalence neutrálního prvku je maximálním prvkem relace a třída ekvivalence jednotkového prvku je prvkem minimálním.

Lemma 3.1.8. *Mějme obor integrity R a nějaké $a \in R - R^*$ takové, že $a \neq 0$. Pak $[1] \prec [a] \prec [0]$.*

Důkaz. Mějme libovolné nenulové $a \in R - R^*$. Z lemmat 1.1.8 a 1.2.13 a definice uspořádání dostaneme $[1] \preceq [a]$. Avšak platit nemůže $a \preceq [1]$. To by totiž znamenalo, že a dělí nějaký invertibilní prvek. Z lemmatu 1.2.13 víme, že invertibilní prvek dělí jenom jiný invertibilní prvek, což je spor s předpokladem, že a není invertibilní. Máme tedy $[1] \prec [a]$. Z lemmatu 1.2.21 a definice uspořádání dostaneme, že $[a] \preceq [0]$. Pokud by platilo $[0] \preceq [a]$, znamenalo by to $a \parallel 0$ a podle lemma 3.1.6 by to znamenalo, že $a = 0$, což je spor s předpokladem. Takže máme $[a] \prec [0]$.

□

Nyní dokažme, jaký vzájemný vztah mají prvek a jeho vlastní dělitel vzhledem k uspořádání a že uspořádání skutečně rozšiřuje dělitelnost.

Lemma 3.1.9. *Mějme obor integrity R, kde $[R]$ je faktorový obor. Prvek $b \in R$ je vlastním dělitelem prvku $a \in R$ právě tehdy, když platí v $[R]$: $[1] \prec [b] \prec [a]$.*

Důkaz. Pokud je b vlastním dělitelem, nemůže být invertibilní ani nulou. Z Lemma 3.1.6 dostáváme $[1] \prec [b]$. Dle definice vlastního dělitele platí $b \mid a$, což znamená $[b] \preceq [a]$. Pokud by platilo $[a] \preceq [b]$, znamenalo by to $b \parallel a$, což ovšem neplatí, protože podle definice vlastního dělitele prvky a a b nejsou asociované. Takže máme $[b] \prec [a]$.

Dokažme opačnou implikaci. Z $[1] \prec [b]$ víme, že $b \notin R^*$. Z $[b] \prec [a]$ víme, že $b \mid a$ a neplatí $b \parallel a$. Tak jsme dokázali, že b je vlastním dělitelem.

□

Tímto jsme ukázali, že relace uspořádání odpovídá dělitelnosti a že invertibilní prvky jsou minimální vzhledem k této relaci uspořádání. Dále, zkoumáním uspořádání, zjistíme, že v případě množiny, kde nejsou invertibilní prvky, minimálním prvkem na této množině je ireducibilní prvek, pokud se zde vyskytuje.

Lemma 3.1.10. *Mějme obor integrity R, jeho faktorový obor $[R]$ a libovolný prvek $p \in R - R^*$ takový, že $p \neq 0$. Pak p je ireducibilní, právě když $[p]$ je minimálním prvkem množiny $[R] - [1]$.*

Důkaz. Uvažujme případ, kdy je p ireducibilní a $[p]$ není minimální prvek. To znamená, že existuje $[c]$ pro $c \in R$ takové, že $[c] \prec [p]$. Podle Lemma 3.1.9 to znamená, že c je vlastní dělitel p. Tím pádem p není ireducibilní.

Nyní, předpokládejme, že p není ireducibilní. Z předpokladu víme, že není nulový a není invertibilní. Pokud není ireducibilní, musí mít vlastního dělitele $q \in R$. To podle Lemma 3.1.8 znamená, že $[1] \prec [q] \prec [p]$. Tím pádem $[p]$ není minimálním prvkem v množině $[R] - [1]$.

□

Lemma 3.1.11 (Třída největších společných dělitelů)**.** *Nechť R je obor integrity a mějme neprázdnou množinu $M \subseteq R$. Pokud existuje $d \in NSD(M)$, pak $NSD(M) = [d]$.*

Důkaz. Mějme prvek $e \in NSD(M)$. Podle definice největšího společného dělitele platí $e \mid d$. Avšak z předpokladu máme také $d \in NSD(M)$, což znamená, že $d \mid e$. Tedy $e \in [d]$.

Dokažme opačnou inkluzi. Nechť $f \in [d]$. Jelikož $d \in NSD(M)$, platí pro každý prvek $m \in M$, že $d \mid m$. Z $f \in [d]$ vyplývá $f \mid d$, a díky transitivitě relace dělitelnosti máme pro každý prvek $m \in M$, že $f \mid m$. To znamená, že $f \in SD(M)$. Dále, jelikož pro každý prvek $a \in SD(M)$ platí, že $a \mid d$ a z $f \in [d]$ vyplývá $d \mid f$, pak z tranzitivity dělitelnosti máme, že pro každý prvek $a \in SD(M)$ platí $a \mid f$. To znamená, že $f \in NSD(M)$.

Tím jsme ukázali, že $f \in NSD(M)$, a tedy platí $NSD(M) = [d]$.

□

Lemma 3.1.12 (Tvar asociovantů)**.** *Nechť R je obor integrity. Pro každé a,$b \in R$ platí $a a \parallel b$ právě když $a = be$ a pro nějaké $e \in R^*$.*

Důkaz. Nechť $a = 0$, poté $b = 0$, protože podle lemma o nasobení nulou je 0 jediný asociovaný prvek s 0. Máme tedy $0 = 0 * e$, tohle podle lemma Násobení nulou platí pro všechny $e \in R$, ale R je podle předpokladu obor hodnot a tudíž v něm je minimálně jeden invertibilní prvek kterým je 1. Nechť tedy $a \neq 0$. Mějme $a \parallel b$, tedy $a = be$ a $b = af$ pro nějaké f,$g \in R$. Tedy z toho máme $a = afe$, jelikož jsme o oboru hodnot, tak můžeme krátit a tedy. $1 = fe$ a tedy $e \in R^*$.

Dokažme teď druhou stranu implikace. Mějme nějaké $a = be$, takže $e \in R^*$, což zaprvé implikuje že $b \mid a$, ale zároveň to zmanená, že existuje inverzni prvek $f \in R^*$. Takový, že $e * f = 1$. Tedy z $a = be$ dostaneme $af = bef$, což znamená, že $af = b$ a tedy $a \mid b$.

□

Dokažme si nyní, že pokud máme třídu, ve které je ireducibilní prvek, pak všechny prvky v této třídě jsou ireducibilní. To však neznamená, že existuje jen jedna ireducibilní třída. Typicky ve stejné třídě jsou, jak si následně ukážeme, pouze násobky ireducibilního prvku s nějakým invertibilním.

Lemma 3.1.13. *Nechť R je obor integrity a prvky $a, b \in R$ takové, že $a \parallel b$. Pak a je ireducibilní, právě když b je ireducibilní.*

Důkaz. Uvažujme, že a je ireducibilní a b není ireducibilní. To může znamenat tři možnosti:
Buď $b = 0$. Z $a \parallel b$ víme, že $b \mid a$. To podle lemmatu 3.1.6 znamená $a = 0$, což je spor, protože a je ireducibilní.
Nechť $b \in R^*$. Existuje inverzní prvek w k b, takový, že platí $wb = 1$. Z $a \parallel b$ víme, že $a \mid b$. Tedy $b = ac$ pro nějaké $c \in R$. Vynásobíme tuto rovnici w, dostaneme $bw = acw$, což znamená $1 = acw$. V oboru integrity existuje $x \in R$ takové, že $cw = x$. To vede k $1 = ax$, což znamená, že a je invertibilní prvek, což je spor s tím, že a je ireducibilní.
Nechť $c \in R$ je vlastní dělitel b takový, že $c \mid b$. Z předpokladu víme, že $b \mid a$. Podle věty 1.2.12 platí dělitelnost tranzitivně, takže $c \mid a$, což znamená, že i a má vlastního dělitele, a tedy není ireducibilní.
Tedy b musí být také ireducibilní.
Druhá strana implikace se dokazuje obdobně.

□

Toto tvrzení rozhodně neznamená, že ireducibilní prvky tvoří jen jednu třídu ekvivalence, protože ireducibilní prvky se nemusí vzájemně dělit. Nyní si ukážeme, jak obecně vypadají všechny třídy v definovaném faktoroboru, což nám zároveň ukáže, jaký vztah mají mezi sebou asociované prvky.

Lemma 3.1.14. *Nechť R je obor integrity. Pro libovolné $a, b \in R$ platí $a \parallel b$, právě tehdy, když $a = be$ pro nějaké $e \in R^*$.*

Důkaz. Z $a \parallel b$ dostaneme $a \mid b$ a $b \mid a$. To znamená, že existují $e, f \in R$ takové, že $b = ae$ a $a = bf$. Pokud $a = 0$, pak podle lemmatu 3.1.6 musí být také $b = 0$. To vyplývá z lemmatu 1.1.4, kde pro všechna $x \in R$ platí $0 = 0 * x$. Jelikož R je

obor integrity, obsahuje prvek 1, a proto platí i $0 = 0 * 1$. Tedy máme invertibilní prvek v R. Nechť tedy $a \neq 0$. Dosazením $b = ae$ do rovnice $a = bf$ dostaneme $a = aef$. Jelikož jsme v oboru integrity a $a \neq 0$, můžeme obě strany rovnice vydělit a, čímž získáme $1 = ef$. Tím jsme dokázali, že $e, f \in R^*$. Pokud platí $a = bf$, kde $f \in R^*$, z definice dělení vyplývá $b \mid a$. Z definice invertibilního prvku plyne, že existuje g takové, že $1 = fg$. Pokud tedy vynásobíme rovnici $a = bf$ tímto g, dostaneme $ag = bfg$. Víme však, že $fg = 1$, a tedy $b = ag$ a z toho plyne $a \mid b$.

□

Nyní si dokažme, že podmínka být ireducibilním prvkem plyne z podmínky být prvočinitelem. Určitě na řadu přichází otázka, zda-li tyto tyto vlasnosti nejsou v oborech integrity ekvivalentní, což jak si ukážeme později rozhodně nutně nejsou. Opačná implikace platí, jen ve speciálních případech oborů integrity. Ukážeme, že pokud máme obory integrity, kde zaručíme existenci největšího společného dělitele, tak už v nich musí platit i opačná implikace.

Lemma 3.1.15. *Nechť R je obor integrity a mějme libovolné $p \in R$. Pak když p je prvočinitel, tak je ireducibilním prvkem*

Důkaz. Postupujeme sporem a nechť tedy p není ireducibilní

Pokud $p = 0$, pak podle definice není p prvočinitelem.

Pokud $p \in R^*$, pak podle definice není p prvočinitelem.

Nechť tedy $p \in R - R^*$ a $p \neq 0$. Mějme libovolné $x \in R$ takové, že x je vlastní dělitel p. To znamená, že existuje $e \in R$ takové, že $p = xe$.

Podle definice vlastního dělitele víme, že p není nesoudělné s x, tedy $p \nparallel x$. Z toho podle lemmatu 2.2.14 plyne, že $e \in R - R^*$.

Platí $p \mid xe$. Pokud by platilo $p \mid x$, pak by existovalo $f \in R$ takové, že $x = pf$. Dosazením za p dostaneme $x = xef$. V oboru integrity musí platit $x \neq 0$, protože jinak by $x = 0$, což je v rozporu s naším předpokladem. Tedy $1 = ef$. Z toho však vyplývá, že $e \in -R^*$, což je spor, neboť jsme dokázali, že $e \in R - R^*$.

Předpokládejme nyní, že platí $p \mid e$. Z toho vyplývá, že $e = ph$. Dosazením za p dostaneme $e = exh$. Z našeho předpokladu ale plyne, že $e \neq 0$, protože jinak by $p = 0$. V oboru integrity můžeme tedy vynásobit rovnicí xh a získáme $1 = xh$. Tím jsme ale dospěli k závěru, že $x \in R^*$, což je v rozporu s definicí vlastního dělitele.

□

Nyní máme představu, jak vypadají třídy faktorokruhu. Definujme si nyní postupně podmínky dělitelnosti, které nám ukažou jak konstruovat složitější obor integrity. Začneme s první podmínkou o existenci největšího společného dělitele.

Definice 3.1.16 (Podmínka D)**.** *Mějme obor integrity R. Každá konečná množina prvků z R má v R alespoň jeden největší společný dělitel.*

Dokázali jsme, že v oboru integrity je každý prvočinitel ireducibilním prvkem. V obecném oboru integrity opačná implikace, jak jsme si ukázali, nemusí platit. Proto další podmínkou pro obory integrity bude platnost této opačné implikace.

Definice 3.1.17 (Podmínka P)**.** *Mějme obor integrity R. Pak každý ireducibilní prvek v okruhu R je prvočinitel.*

Další podmínka definuje obory integrity, kde pokud asociují součiny, tak asociují i ireducibilní prvky, ze kterých se tyto součiny skládají. Navíc počet těchto prvků je vždy stejný.

Definice 3.1.18 (Podmínka J)**.** *Mějme obor integrity R a dvě přirozená čísla m a n s m-ticí $p_1, p_2, \ldots, p_m$ a n-ticí $q_1, q_2, \ldots, q_m$ ireducibilních prvků z R takové, že $p_1, p_2, \ldots, p_m \parallel q_1, q_2, \ldots, q_m$. Potom platí $m = n$ a existuje permutace π taková, že $p_i \parallel q_{\pi(i)}$ pro $i \leq n$.*

Další podmínka vyžaduje, aby každá podmnožina v faktoroboru oboru integrity měla nějaký minimální prvek vzhledem k naší relaci uspořádání.

Definice 3.1.19 (Podmínka K)**.** *Mějme obor integrity R. Relace $\preceq$ na $[R]$ je fundovaná.*

Poslední podmínka definuje takové obory integrity, ve kterých každý prvek, který není nula a není invertibilní, lze rozložit na součin ireducibilních prvků.

Definice 3.1.20 (Podmínka I)**.** *Mějme obor integrity R. Pak každý neinvertibilní prvek z R, který není nula, je součinem ireducibilních prvků z R.*

Dokázali jsme, že největší společný dělitel je distributivní vůči násobení. Můžeme už nyní dokázat, že v oboru integrity, ve kterém každá konečná množina má největší společný dělitel, tak v tomto oboru integrity už musí platit, že každý ireducibilní prvek je prvočinitel. Neboli podmínka P plyne z podmínky D.

Věta 3.1.21 (DP)**.** *V oboru integrity R podmínka P plyne z podmínky D.*

Důkaz. Nechť R splňuje D a nechť $p \in R$ je libovolný ireducibilní prvek.
Předpokládejme, že $p \mid ab$ pro a,$b \in R$.
Pokud by platilo $p \mid a$, tak podmínka P platí pro p.
Předpokládejme, že p nedělí a.
Z ireducibility p plyne, že největším společným dělitelem p a a je 1.
Podle lemmatu 1.2.21 je b největším společným dělitelem pb a ab.
Je evidentní, že $p \mid pb$.
Z předpokladu víme, že $p \mid ab$.
p je společný dělitel a vzhledem k tomu, že b je největší společný dělitel, tak $p \mid b$.
Dokázali jsme, že p je prvočinitel a obor hodnot splňuje podmínku P.

□

Nejdříve však definujme obor NSD, což je právě takový obor, ve kterém pro každou konečnou množinu existuje největší společný dělitel. Tedy obory, které splňují podmínku D.

Definice 3.1.22 (NSD obor)**.** *Nechť R je obor integrity. Obor integrity je NSD oborem právě tehdy, pokud splňuje podmínku D.*

Uvažujme obor integrity $\mathbb{Z}[\sqrt{-5}]$. Definujeme si nyní normu, jak jsme ji popisovali na začátku této kapitoly $f(a+b\sqrt{-5}) = a^2+5b^2$. Zřejmě platí, že $f(0) = 0$. Ověřme nyní, zda platí $f((a+\sqrt{-5}b)*(c+\sqrt{-5}d)) = f(a+\sqrt{-5}b)*f(c+\sqrt{-5}d)$. Nalevo roznásobíme a napravo použijeme definici normy a dostaneme rovnici: $f((ac-5bd)+\sqrt{-5}(cb+ad)) = (a^2+5b^2)*(c^2+5d^2)$. Dalším úpravou obou stran dostaneme $(ac-5bd)^2+5(cb+ad)^2 = (ac)^2+5(cb)^2+5(cd)^2+(5bd)^2$., což už je jednoduché ověřit, že platí vždy a je tedy zřejmé, že se jedná o multiplikativní normu.

Vezměme nyní číslo 6, pro které platí $(1+\sqrt{-5})*(1-\sqrt{-5}) = 6 = 2*3$. Spočítáme-li normy, máme $f(2) = 4$, $f(3) = 9$, $f(1-\sqrt{-5}) = 6$, $f(1+\sqrt{-5}) = 6$. Je zjevné, že všechny tyto čísla jsou ireducibilní, protože neexistuje žádné $f(a)$ takové, aby dělilo nějakou normu těchto čísel. Tedy tento obor nevyhovuje podmínce P, protože číslo 2 dělí součin $(1+\sqrt{-5})$ a $(1-\sqrt{-5})$, ale nedělí ani jeden z prvků. To tedy podle předchozí věty znamená, že takovýto obor není NSD obor.

Dokážeme nyní jestliže nějaký prvek je největším společným dělitelem nějaké množiny, pak pokud vynásobíme prvky této množiny nějakým dalším prvkem, největší společný dělitel nové množiny je součinem tohoto prvku a původního největšího společného dělitele. Musíme však předpokládat, že existence největšího společného dělitele je zaručena.

Lemma 3.1.23. *Mějme obor integrity R, $A = a_1,a_2,..,a_n$ takovou, že $A \subseteq R$ a $e \in NSD(A)$, potom pro každý prvek $r \in R$ je $rd \in NSD(ra_1,ra_2,..,ra_n)$.*

Důkaz. Podle lemmatu 1.1.4 platí pro libovolné $b \in R$ vynásobení nulou: $b \cdot 0 = 0$. Takže $0 \in NSD(0,..,0)$ podle lemmatu 1.3.28, kde jen nula dělí nulu. Mějme $r \neq 0$. Z předpokladu víme, že $d \mid a_i$ pro všechny $i \leq n$, což znamená $a_i = de_i$ pro nějaké $e_i \in R$. To lze vyjádřit jako $ra_i = (rd)e_i$, což implikuje, že $rd \mid ra_i$ a rd je společný dělitel. Z předpokladu existuje e, které je největší společný dělitel $ra_1,ra_2,..,ra_n$. Jelikož e je největší společný dělitel, musí jej dělit i jiní společní dělitelé, a $rd \mid e$. To znamená, že $e = rdf$ pro nějaké $f \in R$. Rozhodně $r \mid ra_i$ pro $i \leq n$. r je společný dělitel a jelikož e je největší společný dělitel, tak musí také platit, že $r \mid e$. To znamená, že $e = rg$ pro nějaké vhodné $g \in R$. Z toho plyne, že rg je největší společný dělitel $ra_1,ra_2,..,ra_n$. Tudíž pro $i \leq n$ máme $rg \mid ra_i$. Díky tomu musí platit $ra_i = rgb_i$ pro nějaké $b_i \in R$. r je ale nenulové a jsme v oboru integrity, takže musí platit $a_i = gb_i$ pro nějaké $b_i \in R$. To znamená, že pro všechny $i \leq n$ platí $g \mid a_i$. Musí platit $g \mid d$, protože d je největší společný dělitel. Z toho plyne, že $d = gh$ pro vhodné $h \in R$. Vynásobením nenulovým r dostaneme $rd = rgh$ pro nějaké vhodné $h \in R$. Proto $rg \mid rd$, ale $rg = e$, takže $e \mid rd$. Tím pádem $e \parallel rd$, což podle lemmatu 2.1.9 znamená, že i rd musí být největší společný dělitel.

□

Obory integrity, kde každá konečná množina má největšího společného dělitele, již mají každý ireducibilní prvek jako prvočinitele. Dokážeme si, že pokud v oboru integrity každý ireducibilní prvek je prvočinitel, tak rozklady spolu již asociují. To znamená, že podmínka J plyne z podmínky P. To kvůli transitivitě znamená, že když si dokážeme, že podmínka J plyne z podmínky P, potom jsme jistě dokázali, že podmínka J plyne i z podmínky D.

Věta 3.1.24 (PJ)**.** *V oboru integrity plyne podmínka J z podmínky P.*

Důkaz. Nechť R splňuje P a nechť $p_1,..,p_n,q_1,..,q_m$ jsou ireducibilní prvky tak, že platí $p_1..p_n \parallel q_1..q_m$. Platnost podmínky J ověříme indukcí. Pro $m = n = 1$ máme $p_1 \parallel q_1$. Dokažme teď tvrzení pro $n+m$. Z $p_1..p_n \parallel q_1..q_m$ dostaneme $p_1..p_n \mid q_1..q_m$. Podle definice relace dělitelnosti dostaneme $q_1..q_m = p_1..p_n a$ pro nějaké $a \in R$. Jsme v oboru integrity, proto R je uzavřené na asociativnost a násobení. Tím pádem máme $q_1..q_m = p_1 d$, pro $d \in R$ kde $d = p_2..p_n a$. Máme $p_1 \mid q_1..q_m$ a z podmínky P plyne, že p_1 je prvočinitel. Podle lemmatu 1.3.36 dostáváme, že $p_1 \mid q_i$ pro nějaké $i \leq N$. Při vhodném očíslování dostaneme $p_1 \mid q_1$. Podle předpokladu q_1 je ireducibilní, proto musí platit $p_1 \parallel q_1$. Pokud na tyto skutečnosti použijeme lemma 2.2.14, dostaneme, že $p_1 = q_1 e$ pro nějaké $e \in R$. Dále máme $p_1..p_n = q_1..q_m f$ pro nějaké $f \in R$. Po dosazení a použití komutativního zákona dostaneme $p_1..p_n = p_1 q_2..q_m fe$, ale jsme v oboru integrity, takže můžeme krátit, protože p_1 je ireducibilní, tedy $p_1 \neq 0$. Dostaneme $p_2..p_n = q_2..q_m g$ pro nějaké invertibilní $g \in R$ takové, že $g = fe$, načež použijeme indukční předpoklad.

□

Budeme pokračovat nastíněním vztahu našich podmínek, ukážeme si, že pokud máme obor integrity takový, že $\preceq$ je na $[R]$ fundovaná, tak pak každé číslo lze rozložit na součin ireducibilních prvků. Dokažme ale nejdříve, že takové uspořádání implikuje existenci ireducibilního prvku, který neireducibilní prvek dělí.

Lemma 3.1.25 (Rozklad)**.** *Nechť R je obor integrity, který splňuje podmínku K, a mějme nenulové $a \in R - R^*$. Pak existuje ireducibilní prvek $p \in R$ takový, že $p \mid a$.*

Důkaz. Z lemmatu 3.1.8 máme $[1] \prec [a] \prec [0]$.
Definujme

$$A = \{[x] \in [R]; [1] \prec [x] \preceq [a]\}$$

. Do této množiny rozhodně patří $[a]$. Proto množina určitě bude neprázdná.
Z definice A dále plyne, že $A \subseteq [R]$.
Podle podmínky K má tato podmnožina minimální prvek $[p]$.
Z definice A víme, že musí platit $[1] \prec [p]$.
Z definice A, $[1] \prec [a] \prec [0]$ a transitivity dostaneme pro $[p]$ $[p] \prec [0]$.
Proto $[p]$ je minimální na $[R] - [1]$. To podle lemmatu 3.1.9 znamená, že p je ireducibilní prvek.
Z definice A víme, že platí $[p] \preceq [a]$, což znamená, že $p \mid a$.

□

Nyní si konečně můžeme ukázat vztah mezi podmínkou K a I. To znamená, že fundovanost relace na faktorovém oboru integrity implikuje existenci ireducibilního rozkladu pro libovolné neinvertibilní nenulové číslo v tomto oboru integrity.

Věta 3.1.26 (KI)**.** *V oborech integrity plyne podmínky z K podmínka I.*

Důkaz. Předpokládejme, že R splňuje podmínku K, ale nesplňuje podmínku I. Definujme množinu

$$M = \{a \in R; 0 \neq a \notin R^* \texttt{ a není součinem ireducibilních prvků}\}.$$

Jelikož podmínka I neplatí, množina M je neprázdná.

Vezměme libovolné $a \in M$ a dokažme, že platí $[a] \subseteq M$. Pro každý prvek $b \in [a]$ platí, že $b \parallel a$. Z definice množiny M víme, že $b \neq 0$.

Podle lemmatu 3.1.6 víme, že a není ve třídě s 0. Z $b \parallel a$ plyne, že b i a jsou ve stejné třídě, tudíž $b \neq 0$ podle lemmatu 3.1.6.

Víme, že $b \in R - R^*$, protože z lemmatu 3.1.7 plyne, že invertibilní prvky jsou ve stejné třídě. Z $b \parallel a$ také víme, že b a a jsou ve stejné třídě a a není invertibilní.

Předpokládejme, že b je součinem ireducibilních prvků $p_1, \ldots, p_n$. Z $b \parallel a$ dostaneme $b = ae$ pro nějaké $e \in R^*$. Ukázali jsme, že $ae = p_1 \ldots p_n$. Jelikož e je invertibilní, existuje k němu inverzní prvek $f \in R$. Pak vynásobením rovnice dostaneme $aef = p_1 \ldots p_n f$, což znamená, že $a = p_1 \ldots p_n f$.

Použitím asociativního zákona získáme $a = p_1 \ldots p_{n-1}(p_n f)$. Označme $p_n f = q$ pro nějaké $q \in R$. Podle lemmatu 3.1.14 musí být q ireducibilní prvek. Z lemmatu 3.1.7 vyplývá, že všechny prvky ve stejné třídě jsou buď ireducibilní nebo žádný z nich není ireducibilní.

Zároveň podle lemmatu 3.1.14 prvek q patří do stejné třídy jako p_n, který je ireducibilní. Dostáváme tedy $a = p_1 \ldots p_{n-1} q$, kde a je součinem ireducibilních prvků, což je spor s naším původním předpokladem.

Dokázali jsme tedy, že $[a] \subseteq M$. Definujme $A = \{[a] \in [R]; a \in M\}$. Z definice je zřejmé, že $A \subseteq [R]$. Podle podmínky K existuje nějaký minimální prvek $[m]$ v množině A.

Jelikož $m \in M$, tak $m \in R - R^*$ není nula ani ireducibilní. Dostáváme $m = pc$, kde c,$p \in R$ a p je ireducibilní prvek.

Jistě platí $c \neq 0$, jinak by podle lemmatu 1.1.9 muselo být $m = 0$. Také $c \in R - R^*$, protože kdyby c bylo invertibilní prvek, podle lemmatu 2.2.14 by bylo ve stejné třídě jako m, což je spor, protože podle lemmatu 3.1.7 je $c \in R^*$ a $m \in R - R^*$.

Zároveň c nemůže být součinem ireducibilních prvků, jinak by i m bylo součinem ireducibilních prvků, protože m je součinem c s ireducibilním prvkem. Nutně tedy musí být $c \in M$. Víme, že $c \nparallel m$, $c \in R - R^*$ a $c \mid m$, tudíž c je vlastním dělitelem prvku m.

Podle lemmatu 2.3.23 platí $[c] \prec [m]$. Víme, že $[c] \in A$, což je spor s tím, že $[m]$ je minimální.

Tím jsme dokázali, že platí podmínka I.

□

3.2 Gaussův obor

Jak jsme ukázali, obory integrity, které splňují podmínku I, také splňují podmínku K. Také jsme dokázali, že obory integrity, které splňují podmínku D, nutně splňují podmínku P. A ty obory integrity, které splňují podmínku P, nutně splňují podmínku J. Podmínky I a J jsou v této hierarchii nejslabšími podmínkami. Dokážeme, že tyto podmínky společně jsou dostačující a pokud platí současně, pak platí libovolná z podmínek. Nejdříve si proto definujme takzvaný Gaussův obor, což je obor, který splňuje podmínky I a J, tyto podmínky zároveň zaručují platnost Základní věty aritmetiky o jednoznačnosti rozkladu.

Definice 3.2.27 (Gaussův obor)**.** *Nechť R je obor integrity a splňuje podmínky I a J. Pak jej nazýváme Gaussův obor.*

Nyní dokážeme, že v Gaussově oboru má každý prvek kanonické vyjádření pomocí ireducibilních prvků. Dokážeme první část důkazu základní věty aritmetiky, který dokazuje existenci rozkladu.

Lemma 3.2.28 (Kanonické vyjádření)**.** *Mějme Gaussův obor R. Pak každý nenulový prvek $a \in R - R^*$ má vyjádření ve tvaru $a = ep_1^{k_1}..ep_n^{k_n}$, kde $p_1,..,p_n \in R$ jsou vzájemně neasociované ireducibilní prvky, $e \in R^*$ a $n,k_1,..,k_n$ jsou přirozená čísla.*

Důkaz. Podle podmínky I máme $a = q_1..q_m$.
Pokud prvky jsou vzájemně neasociované, pak lemma platí.
Předpokládejme, že prvky jsou asociované.
Pokud $q_i = q_j$ pro $i \neq j$.
Můžeme díky asociativnosti a komutativnosti seskupit stejné prvky k sobě.
Při vhodném očíslování skupina kolem q_j obsahuje l_j prvků pro všechna $j \leq n$.
Zapišme tyto prvky jako mocniny a dostaneme $a = q_1^{l_1}..{q_n}^{l_n}{q_{n+1}}^{l_{n+1}}..{q_{n+d}}^{l_{n+d}}$ pro nějaké $d \leq m - n$.
Pokračujeme indukcí podle d.
Pokud $d = 1$, pak $a = q_1^{l_1}..{q_n}^{l_n}{q_{n+1}}^{l_{n+1}}$ a při vhodném očíslování platí $q_1 \parallel q_{n+1}$.
Pro nějaké $f_1 \in R^*$ musí platit $q_{n+1} = q_1 f_1$ podle lemmatu 2.2.14.
Použitím komutativity a asociativity dostáváme $q_{n+1}^{l_{n+1}} = q_1^{l_{n+1}} f_j^{l_{n+1}}$.
Dosazením do původního zápisu získáme $a = f^{l_{n+1}} q_1^{k_1} q_n^{k_n}$, kde $r_1 = l_1 + l_{n+1}$ a $k_i = l_i$ pro $1 < i \leq n$.
Protože R je uzavřené na násobení, můžeme napsat $e = f^{l_{n+1}}$ pro nějaké $e \in R^*$.
Dostali jsme $a = eq_1^{r_1}..q_n^{r_n}$.
Máme dokázáno pro k, a chceme dokázat tvrzení pro $k + 1$.
Máme $a = eq_1^{r_1}..q_k^{r_k}q_{k+1}^{r_{k+1}}$, ale důkaz je zcela obdobný jako jsme provedli v prvním kroku.

□

Dokázali jsme, že každé nenulové neinvertibilní číslo lze rozložit pomocí ireducibilních čísel. Nyní se pokusme dokázat, že takový rozklad je jednoznačný až na invertibilní prvek, jinak jsou prvky dvou rozkladů vzájemně asociované. Toto je druhá část důkazu Základní věty aritmetiky, respektive její zobecněné verze. Pokud vezmeme přirozená čísla, tam je invertibilním prvkem pouze 1 a žádné prvky nejsou asociované. Proto z této verze plyne Základní věta aritmetiky pro

přirozená čísla. Pro celá čísla to znamená, že se ireducibilní prvky mohou lišit ve znaménku a invertibilní prvek bude buď 1 nebo -1.

Lemma 3.2.29 (Jednoznačnost kanonického vyjádření)**.** *Mějme Gaussův obor R a nějaký prvek $a \in R - R^*$ se dvěma kanonickými vyjádřeními $fq_1^{l_1}..q_n^{l_n} = a = ep_1^{k_1}..p_m^{k_m}$. Potom $m = n$ a při vhodném očíslování prvků $p_1,..,p_m \in R$ platí $q_i \parallel p_i$ a $k_i = l_i$ pro $i \leq n$.*

Důkaz. Asociování je reflexivní, proto určitě platí $q_1^{l_1}..q_n^{l_n} \parallel p_1^{k_1}..p_m^{k_m}$.
Podle podmínky J platí $m = n$ a prvek p_1 je asociován s některým z prvků $q_1..q_n$.
Při vhodném očíslování platí $p_i \parallel q_i$ pro $i \leq n$.
Prvek p_i je asociován na levé straně jen s prvkem q_i.
Pokud by byl asociován i s jiným prvkem q_j, pak by z transitivity asociování platilo $q_j \parallel q_i$, což je spor s lemmatem 3.1.8.
Takže počet výskytů napravo p_i a výskytů nalevo q_i pro $i \leq n$ je stejný.
Proto $k_i = l_i$ pro $i \leq n$.

□

Dokázali jsme nyní, že kanonické vyjádření je jednoznačné, až na vzájemně asociované prvky. Dále jsme ale ukázali, že součet mocnin všech vyjádření je pro libovolný rozklad každého čísla totožný. Tím pádem máme dokázáno, že pro libovolný Gaussův obor platí Základní věta aritmetiky. Nyní se pokusme dokázat, jaký vztah mají kanonická vyjádření dvou čísel, kde jedno dělí druhé.

Lemma 3.2.30 (Kanonického vyjádření při dělení)**.** *Mějme Gaussův obor R. Mějme nenulové a,$b \in R - R^*$ tak, že $q_1^{l_1}..q_n^{l_n} = a$ $b = p_1^{k_1}..p_m^{k_m}$ jsou dvě kanonická vyjádření. Potom $b \mid a$ právě tehdy, když $m \leq n$ a při vhodném očíslování prvků $p_1,..,p_m \in R$ platí $q_i \parallel p_i$ a $k_i \leq l_i$ pro $i \leq n$.*

Důkaz. Když $b \mid a$, pak $a = bc$ pro vhodné $c \in R$.
Pokud by bylo $c = 0$, bylo by $a = 0$, což je spor s předpokladem.
Je-li $c \in R^*$, pak podle lemmatu 2.2.14 je $a \parallel b$.
Pro $c \in R^*$ lemma platí podle lemmatu 3.1.9.
Nechť $c \in R - R^*$, takže $c \neq 0$.
Pro $c \in R$ existuje podle lemmatu 3.1.8 vyjádření ve tvaru $c = hg_1^{j_1}..g_o^{j_o}$ pro $1 \leq o \leq n - m$.
Získáme součin $bc = hg_1^{j_1}..g_o^{j_o}p_1^{k_1}..p_m^{k_m}$.
Odtud plyne $q_1^{l_1}..q_n^{l_n} = hg_1^{j_1}..g_o^{j_o}p_1^{k_1}..p_m^{k_m}$.
Podle lemmatu 3.1.9 dostaneme $n = o + m$.
Jelikož $1 \leq o$, dostáváme $m \leq n$.
Z lemmatu 3.1.9 vidíme, že každé q_i pro $i \leq n$ může být vyjádřeno třemi způsoby:

1. q_i je některé z p_j pro $j \leq m$.
   Při vhodném očíslování platí $k_i = l_i$ pro $q_i \parallel p_i$.

2. q_i je některé z g_j pro $i \leq o$.
   Při vhodném očíslování $o_i = l_i$ pro $q_i \parallel g_i$, a tím pádem $k_i = 0$, takže $k_i < l_i$.

3. Nechť q_i má vyjádření mezi oběma čísly při vhodném očíslování.
   Podle lemmatu 3.1.9 dostaneme, že platí $l_i = k_i + o_i$.
   Jelikož q_i má vyjádření mezi p_i i g_i, dostáváme $k_i \leq l_i$ a $q_i \parallel g_i$ pro $i \leq m$.

Dokažme opačnou implikaci.
Z předpokladu máme $q_i \parallel p_i$ pro $i \leq m$.
Podle lemmatu 2.2.14 platí, že $q_i = e_i g_i$ pro $e_i \in R^*$.
Dosadíme do a a dostaneme $a = e_1^{l_1} p_1^{l_1} .. e_m^{l_m} p_m^{l_m} .. q_n^{l_n}$.
Díky komutativnosti upravíme $a = p_1^{l_1} .. p_m^{l_m} .. q_n^{l_n} e_1^{l_1} .. e_m^{l_m}$ $y = e_1^{l_1} .. e_m^{l_m}$ pro nějaké $y \in R^*$.
Proto $a = p_1^{l_1} .. p_m^{l_m} .. q_n^{l_n} y$, takže platí $b \mid a$.

□

Poznáváme nyní vztah mezi kanonickými vyjádřeními prvků a jejich společnými děliteli. Ukážeme, které z kanonických vyjádření společných dělitelů odpovídá největšímu společnému děliteli.

Lemma 3.2.31 (Kanonického vyjádření společného dělitele)**.** *Mějme Gaussův obor R a nenulové prvky a,$b \in R - R^*$ takové, že $a = eq_1^{l_1} .. q_n^{l_n}$ a $b = fp_1^{k_1} .. p_m^{k_m}$ jsou dvě kanonická vyjádření a a b. Nechť očíslování je takové, že $q_i \parallel p_i$ pro nějaké r, a pro všechna i platí $0 \leq i \leq r \leq \min(m,n)$ a ostatní prvky nesdílí asociaci. Pak prvek $t \in R$ je společným dělitelem a a b právě tehdy, když $t = hp_1^{v_1} .. p_r^{v_r}$, kde $h \in R^*$ a $0 \leq v_i \leq u_i$ pro $u_i = \min(k_i,l_i)$ pro všechna $i \leq r$.*

Důkaz. Mějme prvek $t \in R$.
Pokud t dělí b i a, podle lemmatu 3.1.10 platí $fp_1^{k_1} .. p_m^{k_m} = tx$ a $eq_1^{l_1} .. q_n^{l_n} = ty$ pro x,$y \in R$.
Existuje r takové, že pro všechny $d \leq r$ platí, že $p_d = q_d z_d$ pro nějaké $z_d \in R^*$.
Substitucí a použitím komutativního zákona dostaneme $ez_1^{l_1} .. z_r^{l_r} p_1^{l_1} .. p_r^{l_r} .. q_n^{l_n} = ty$.
Podle lemmatu 3.2.30 vidíme, že a a b mají společné prvky rozkladu $p_1 .. p_r$, takže $t = hp_1^{v_1} .. p_r^{v_r}$, kde $h \in R^*$ a $0 \leq v_i \leq u_i$ pro $u_i = \min(k_i,l_i)$ pro všechna $i \leq r$.
Pokračujme opačnou implikací.
Z předpokladu $q_i \parallel p_i$ pro i $0 \leq i \leq r$ máme $q_i = w_i p_i$.
Substitucí získáme $a = w_1^{l_1} p_1^{l_1} .. w_r^{l_r} p_r^{l_r} .. q_n^{l_n}$.
Díky komutativnosti získáme $a = p_1^{l_1} .. p_r^{l_r} .. q_n^{l_n} w_1^{l_1} ... w_r^{l_r}$.
Proto t je společným dělitelem.

□

Jak jsme ukázali součin mocnitelů je stejný pro každý prvek nezávisle na jeho kanonickém vyjádření. Také jsme dokázali vyjádřit největšího společného dělitele dvou prvků v Gaussově oboru. Proto Gaussův obor nutně splňuje podmínku D, která říká, že každá konečná množina má alespoň jednoho největšího společného dělitele.

Věta 3.2.32 (I+J=D)**.** *Mějme Gaussův obor R. Pak v něm platí podmínka D.*

Důkaz. Mějme Gaussův obor R. Podle lemmatu 3.2.31 víme, že v Gaussově oboru můžeme najít největšího společného dělitele pro libovolnu konečnou množinu prvků. To znamená, že platí podmínka D.

□

Díky tomu však víme, že v Gaussově oboru platí i P, protože, jak jsme dokázali pomocí věty DP, v každém oboru integrity, kde platí D, platí také P.

Věta 3.2.33 (I+J=P)**.** *Mějme Gaussův obor R. Pak v něm platí podmínka P.*

Důkaz. Mějme Gaussův obor R. Podle věty I+J=D dostaneme, že zde musí platit D. Podle věty DP to znamená, že zde musí platit i P.

□

Zatím se ukázalo, že všechny tyto podmínky platí v Gaussově oboru. Nakonec ukažme, že zde platí také podmínka K. Nejprve si dokážeme, kolik vzájemně neasociovaných vlastních dělitelů čísla v Gaussově oboru existuje.

Lemma 3.2.34 (Počet vlastních dělitelů)**.** *V Gaussově oboru počet vzájemně neasociovaných vlastních dělitelů čísla $a = ep_1^{u_1} \cdot \ldots \cdot p_n^{u_n}$ je roven $\prod_{i=1}^{n}(u_i+1)-2$.*

Důkaz. Dokazujeme indukcí podle n. Nechť $n = 1$, potom platí, že $a = ep_1^{u_1}$. Prvek e je invertibilní, tudíž nemůže být vlastním dělitelem. Víme, že $p_1^0 = 1$, proto $0 < v_i$. Zároveň podle lemmatu 2.2.14 je $p_1^{u_1}$ asociován s a, a proto není vlastním dělitelem, což implikuje $v_i < u_i$. Podle definice v_i musí být přirozené číslo. Mezi $0 < v_i < u_i$ je přesně $u_i - 1$. Předpokládejme, že pro $n = m$ platí $\prod_{i=1}^{m}(u_i+1)-2$. Chceme dokázat indukční krok pro $n = m+1$. Podle předpokladu $\prod_{i=1}^{m}(u_i+1)-2$ existuje m vlastních dělitelů, které splňují podmínku pro délku $n = m$. Chceme se vyhnout vyjádření, kde jsou všechny indexy nulové nebo maximální. Tyto případy však již nejsou obsaženy v indukčním kroku. Tedy máme $u_{n+1}+1$, což odpovídá všem vlastním dělitelům pro indukční krok. Pro $n = m+1$ to přinese $(\prod_{i=1}^{m}(u_i+1)-2)(u_{m+1}+1)$. Poté nás zajímají případy, kdy pro všechny indexy $i \leq n$ platí $v_i = 0$. Tuto možnost můžeme rozšířit na $m+1$ prvků u_{m+1} možnostmi. Pro případy, kdy pro všechny indexy $i \leq n$ platí $v_i = u_i$, můžeme u_{m+1} možnostmi rozšířit na $m+1$ prvků. Takže celkový počet vlastních dělitelů bude $(\prod_{i=1}^{m}(u_i+1)-2)(u_{m+1}+1)+u_{m+1}+u_{m+1}$, což se po úpravě rovná $(\prod_{i=1}^{m+1}(u_i+1)-2)$ - což jsme chtěli dokázat.

□

Dokázali jsme, kolik vlastních společných dělitelů má libovolný nenulový neinvertibilní prvek. Pro nás podstatné je, že takový počet dělitelů je konečný.

Věta 3.2.35 (I+J=K)**.** *Mějme Gaussův obor R. Pak v něm platí všechny podmínky K.*

Důkaz. Zbývá tedy dokázat platnost podmínky K v Gaussově oboru. Mějme tedy libovolnou podmnožinu $[R]$. Pokud je $a \in R$, pak je a minimálním prvkem v naší podmnožině. Nechť a je libovolný nenulový prvek $a \in R - R$. Předpokládejme $A \subseteq [R] - [1]$, tedy neobsahuje prvek $[1]$. Pokud je a ireducibilní je $[a]$ minimální prvkem v A. Pokud a není ireducibilní, pak podle podmínky J existuje rozklad

$a = ex_1^{k_1} \dots x_m^{k_m}$. Vezměme průnik $A \cap D$, kde D je množina vlastních dělitelů a. Pokud $A \cap D = \emptyset$, pak a je minimálním prvkem. Podle lemmatu 3.2.34 je $A \cap D$ vždy konečný. Takže v této množině vždy najdeme minimální prvek, který bude zároveň minimálním prvkem v množině A. Tím pádem je relace $\preceq$ na $[R]$ fundovaná.

□

Nyní pojďme shrnout všechny důkazy a dokázat, že Gaussův obor splňuje všech pět podmínek.

Věta 3.2.36 (Gaussův obor)**.** *Mějme Gaussův obor R. Pak v něm platí všechny podmínky D,P,J,K,I.*

Důkaz. Podmínky I,J platí z definice Gaussova oboru.
Díky větě $I + J = D$ víme, že zde platí i D.
Podle věty $I + J = P$ víme, že v Gaussově oboru platí podmínka P.
Nakonec, díky větě $I + J = K$ víme, že zde platí i podmínka K. Tedy v Gaussově oboru platí všechny tyto podmínky o dělitelnosti.

□

3.3 Bezoutovy obory

Další vlastnosti, které zkoumáme na celých číslech, je platnost Bezoutovy věty, což je dokonce návod jak definovat největší společný dělitel, respektive,jak vůbec dělit efektivně pomocí Euklidova algoritmu. Pro libovolný obor integrity však nemusí fungovat Euklidův algoritmus. Jak si ukážeme, obory, kde Euklidův algoritmus funguje, jsou speciálním případem oborů, ve kterých platí Základní věta aritmetiky a zároveň v nich platí Bezoutova věta. To jsou však nutné, nikoliv dostačující podmínky.

Definujme si Bezoutův obor, což je obor, kde součet hlavní ideálů je zase hlavní ideál.

Definice 3.3.37 (Bezoutův obor)**.** *Nechť R je obor integrity a pro libovolné dva prvky a,$b \in R$ takové, že (a) a (b) jsou hlavní ideály. Pak nazýváme obor Bezoutovým, jestliže platí $(a) + (b) = (d)$ a (d) je také hlavní ideál.*

Nyní ukažme dvě vlastnosti Bezoutova oboru. Těmito vlastnostmi jsou, že v něm platí Zobecněná Bezoutova věta a že každý Bezoutův obor je také NSD oborem.

Věta 3.3.38 (Bezoutova rovnost)**.** *Mějme obor integrity R. Obor je Bezoutův právě tehdy, když platí Bezoutova rovnost.*

Důkaz. Vezměme libovolné a,$b \in R$. Podle definice Bezoutova oboru víme, že platí $(a) + (b) = (d)$ pro nějaké $d \in R$. Z definice součtu ideálů víme, že pro libovolné $t \in R$ existují r,$s \in R$ takové, že $ra + sb = td$. Ale R je obor integrity, takže obsahuje i jednotkový prvek. Tedy existuje q,$p \in R$ takové, že $qa + pb = d$. Dokažme, že platí $d = NSD(a,b)$. Podle lemmatu 1.3.35 platí $(a) \subseteq (a) + (b)$

a $(b) \subseteq (a) + (b)$. Z definice Bezoutova oboru dostáváme $(a) \subseteq (d)$ a $(b) \subseteq (d)$. To podle lemmatu 1.3.36 znamená, že $d \mid a$ a $d \mid b$. Tím pádem d je společným dělitelem a,b. Mějme nyní $c \mid a$ a $c \mid b$, podle lemmatu 1.3.36 platí $(a) \subseteq (c)$ a $(b) \subseteq (c)$. To znamená, že libovolný prvek $x \in (a)$ lze zapsat jako $x = yc$ pro nějaké $y \in R$. Zároveň libovolný prvek $z \in (b)$ lze zapsat jako $z = wc$ pro nějaké $w \in R$. Prvky $(a) + (b)$ lze tedy zapsat jako $yc + wc$ pro nějaké y,$w \in R$. Podle lemmatu 1.3.29 platí $(a) + (b) \trianglelefteq R$. Tedy na něj lze aplikovat distributivní zákon. Dostáváme $yc + wc = (y + w)c$. Jelikož jsme v oboru integrity, platí $y + w = v$ pro nějaké v a tedy $yc + wc = vc$. Podle předpokladu (c) je hlavní ideál a tedy obsahuje všechny násobky c. Tím pádem obsahuje i vc, a tedy dostáváme $(a) + (b) \subseteq (c)$. Z definice Bezuotova oboru víme, že $(a) + (b) = (d)$. Tedy z transitivity podmnožiny máme $(d) \subseteq (c)$. Podle lemmatu 1.3.36 to znamená $c \mid d$. Tím jsme dokázali, že d je tedy největší společný dělitel.

Naopak, mějme (a) a (b). Podle Bezoutovy věty platí $xa + yb = NSD(a,b)$ pro x,$y \in R$. Označme $NSD(a,b) = d$ a dokážeme, že $(a) + (b) = (d)$. Nejdříve dokažme $(a) + (b) \subseteq (d)$. Mějme $x \in (a) + (b)$ a d je společný dělitel a i b. Musí tedy platit $a = de$ a $b = df$. Potom x lze zapsat jako $x = red + sfd$. Podle lemmatu 1.3.29 platí $(a) + (b) \trianglelefteq R$. Tedy na něj lze aplikovat distributivní zákon a můžeme psát $x = d(re + sf)$. Jelikož obor integrity je uzavřený na sčítání a násobení, existuje $h \in R$ takové, že platí $h = re + sf$. Dosazením dostaneme $x = dh$. Tím pádem $x \in (d)$. Mějme nyní $z \in (d)$. Všechny prvky v (d) jsou tvaru $z = rd$ pro nějaké $r \in R$. Podle Bezoutovy věty tedy libovolný prvek vypadá jako $z = r(ax + by)$. Podle distributivního zákona platí $z = (rx)a + (ry)b$. Určitě r,x,$y \in R$, a tedy existují prvky o,$p \in R$ tak, že $o = rx$ a $p = ry$. Takže máme $z = oa + pb$, což znamená, že $z \in (a) + (b)$.

□

Dokažme nyní důsledek tohoto tvrzení ve formě věty. V Bezoutově oboru platí tedy Bezoutova věta, což zaručuje existenci největšího společného dělitele pro každý dvojici prvků. Tím pádem podmínka pro platnost Bezoutovy věty představuje silnější podmínku než pouhá existence největšího společného dělitele. Platnost Bezoutovy věty je dokonče přvořádová podmínka, která však, jak je vidět v definici Bezoutova oboru, lze dokonce vyjádřit v jazyce ideálů.

Věta 3.3.39 (Bezout a NSD)**.** *Mějme obor integrity R. Pokud je obor Bezoutův, pak je také NSD oborem.*

Důkaz. Podle věty o Bezoutově rovnosti víme, jak pro každou dvojici prvků najít největší společný dělitel. Tedy pro libovolnou dvojici prvků existuje největší společný dělitel.

□

Víme tedy, že jak Bezoutovy, tak Gaussovy obory jsou obory NSD, protože jsme dokázali, že v nich platí podmínka D. Otázkou je, jestli existují obory, které jsou pouze Bezoutovy nebo pouze Gaussovy, protože pokud takové obory existují, jsou vzájemnými protipříklady.

Uvažujme obor polynomů dvou proměnných nad celými čísly. Tento obor je Gaussovým oborem, ale pro nesoudělná x a y máme, že $NSD(x,y) = 1$, a v celých

číslech neexistují inverzní prvky. Proto nemůžeme najít dva takové prvky, jejichž lineární kombinace by byla rovna jedné.

Naopak, pokud vezmeme množinu všech řešení nad těmito polynomy, bude to Bezoutův obor, protože libovolné číslo dokážeme vyjádřit jako lineární kombinaci nějakých dvou prvků. Naopak, relace vlastního dělitele nebude fundovaná, protože každý prvek a lze vydělit číslem $a^{\frac{1}{2}}$.

Tyto dva protipříklady jsou zároveň protipříklady toho, že ne všechny Bezoutovy respektive Gaussovy obory jsou obory hlavních ideálů, které si za chvíli nadefinujeme.

3.4 Obor hlavních ideálů

Ukázali jsme si tedy protipříklady, že ne každý Gaussův obor je Bezoutův a ne každý Bezoutův obor je oborem Gaussovým. Nyní si nadefinujme obor hlavních ideálů, který je zároveň Gaussovým i Bezoutovým oborem. Dále dokážeme, že speciálním případem oboru hlavních ideálů je Euklidův obor, kde se zastaví Euklidův algoritmus.

Nejprve si definujme pojem oboru hlavních ideálů, což jak si ukážeme jsou obory, kde zároven platí Bezoutova věta i Základní věta aritmetiky.

Definice 3.4.40 (Obor hlavních ideálů)**.** *Nechť R je obor integrity. Pokud jsou všechny jeho ideály hlavní, nazýváme ho oborem hlavních ideálů.*

Ukažme si že Obor takový obor, kde platí bezoutova věta a i Základní věta aritmetiky, neboli pokud obor je Gaussův a Bezoutův zároveň musí být oborem hlavních ideálů. Definujme si nejdříve další normu.

Definice 3.4.41 (Dedekind–Hasse norma)**.** *Nechť R je obor integrity, pak funkci $f : R - \{0\} \longrightarrow \mathbb{N}$ nazýváme Dedekind–Hasse norma, pokud pro libovolná nenulová a,$b \in R$ splňuje jednu z následujících podmínek:*

1. *Být násobkem:*
$$b \mid a.$$
2. *Menší prvek v ideálu:*
$$(\exists d \in (a,b) f(d) < f(b)).$$

Dokažme si, že pokud v oboru integrity existuje Dedekind–Hasse norma, pak tento obor integrity je také oborem hlavních ideálů.

Lemma 3.4.42. *Mějme obor integrity R. Pokud obor splňuje Dedekind–Hasse normu, pak je také oborem hlavních ideálů.*

Důkaz. Nechť $I = 0$, pak $b = 0$ a $I = (b)$. Nechť tedy $I \neq 0$. Z existence Dedekind–Hasse normy, která je zobrazením do přirozených čísel a tedy lze dobře uspořádat, víme, že existuje $b \in I - 0$ takové, že $\forall r \in I - 0 : f(b) \leq f(r)$. Vezmeme libovolné $a \in I$. Pokud $a = 0$, pak rovněž $a \in (b)$. Pokud by existovalo nějaké $r \in (a,b)$, které splňuje druhou podmínku Dedekind–Hasse normy, byl by to spor s výběrem našeho prvku b. Tudíž pro všechny a musí platit $a \in (b)$, a tedy $I \subseteq (b)$. Naopak, $b \in I$, a podle lemmatu 1.3.36 platí $(b) \subseteq I$. Tím jsme dokázali, že $I = (b)$.

□

Definujme si nyní další normu, která je zesílením naší normy pro obory integrity a tou je ostře multiplikativní norma. Dokažme, že rozklad v Gaussově oboru je takovou normou.

Definice 3.4.43 (Ostře monotónní multiplikativní norma)**.** *Nechť R je obor integrity a funkci $f : R - \{0\} \longrightarrow \mathbb{N}$ nazýváme ostře monotónní multiplikativní norma, pokud pro libovolná nenulová a,$b \in R$ platí následující:*

1. *Monotónnost násobení:*

$$f(ab) \geq max\{f(a),f(b)\}.$$

2. *Ostrost normy:*

$$f(ab) = f(a) \leftrightarrow ab \parallel a.$$

Dokažme si, že rozklad na Gaussově oboru je ostře monotonní multiplikativní norma.

Lemma 3.4.44. *Mějme Gaussův obor R. Pak délka rozkladu prvku je ostře monotónní multiplikativní normou.*

Důkaz. Definujme $f : R - \{0\} \longrightarrow \mathbb{N}$ takovou, že $f(u) = 0$, pokud $u \in R$ je invertibilní. Podle lemmatu o jednoznačnosti rozkladu je $f(up_1^{k_1}..p_n^{k_n}) = k_1 + .. + k_n$ je hodnota funkce pro každý prvek jednoznačná. Dokažme, že platí podmínky pro ostře monotónní multiplikativní normu. Mějme dva nenulové prvky a,$b \in R$ označme $l(a)$,$l(b)$ jejich délky. Bez ztráty obecnosti předpokládejme, že $l(a) \leq l(b)$. Evidentně platí $l(ab) = l(a) + l(b)$. Jelikož $l(a)$ je přirozené číslo, rozhodně platí $l(ab) \geq l(b)$. Rovnost $l(ab) = l(b)$ platí pouze tehdy, když a je invertibilní prvek. Podle lemmatu 3.1.14 to znamená, že $ab \parallel b$.

□

Nyní ukažme, že ostře monotónní multiplikativní norma na Bezoutově oboru je ekvivalentní s Dedekind–Hasse normou.

Lemma 3.4.45. *Mějme Bezoutův obor R. Pak ostře monotónní multiplikativní norma je Dedekind–Hasse normou.*

Důkaz. Mějme ostře monotónní multiplikativní normu f a nenulové prvky a,b.
Jsme v Bezoutově oboru, a tedy platí, že pro nějaké $d \in R$ platí $(a,b) = (d)$.
Z toho plyne, že $d \mid a$ a $d \mid b$.
Pokud by platilo $b \mid d$, pak bychom získali z transitivity $b \mid a$.
Nechť tedy $b \nmid d$ a tedy $b \not\parallel d$.
Podle lemmatu 3.1.14 platí $b = dc$ pro nějaké neinvertibilní $c \in R$.
Tedy rozhodně platí $f(d) < f(b)$.

□

Věta 3.4.46 (Gaussův-Bezoutův obor a obor hlavních ideálů)**.** *Mějme obor integrity R, který je zároveň Gaussový a Bezoutův. Potom je také oborem hlavních ideálů.*

Důkaz. Podle lemmatu 3.4.44 máme ostře monotónní multiplikativní normu. Na základě předpokladu, že se nacházíme v Bezoutově oboru (dle lemmatu 3.4.45), tato norma je také Dedekind–Hasse normou. Pak podle lemmatu 3.4.42 obor R splňuje vlastnosti oboru hlavních ideálů.

□

Tato věta zdůrazňuje souvislost mezi vlastnostmi oboru a postupně ukazuje, jak kombinace vlastností Gaussova oboru a Bezoutova oboru implikuje vlastnost oboru hlavních ideálů. Ukažme, že každý obor hlavních ideálů je zároveň Gaussový i Bezoutův. V minulé podsekci jsme si ukázali příklady Bezoutových oborů, které nejsou Gaussovy. Tyto příklady slouží jako protipříklady Bezoutových oborů, které nejsou obory hlavních ideálů. Obory, které jsou Gaussovy, ale nejsou Bezoutovy, jsou naopak protipříklady pro Gaussovy obory, které nejsou obory hlavních ideálů. Nyní dokážeme, že obor hlavních ideálů je vždy Bezoutův obor.

Věta 3.4.47 (Obor hlavních ideálů a Bezoutův obor)**.** *Mějme obor integrity R, který je oborem hlavních ideálů. Pak je také Bezoutův.*

Důkaz. Z definice součtu ideálů víme, že $(a) + (b) = (a,b)$. Podle předpokladu, že R je oborem hlavních ideálů, existuje prvek $d \in R$ takový, že $(d) = (a,b)$. Tím pádem platí $(a) + (b) = (d)$. To znamená, že obor R je Bezoutův.

□

Tedy pro každé dva prvky oboru hlavních ideálů dokážeme najít společného dělitele, což znamená, že takový obor je zároveň Gaussův, pokud dokážeme, že relace uspořádání je fundovaná.

Věta 3.4.48 (Obor hlavních ideálů a Gaussův obor)**.** *Mějme obor integrity R, který je oborem hlavních ideálů. Pak je také Gaussův.*

Důkaz. Z věty o Oboru hlavních ideálů a Bezoutově oboru víme, že Obor hlavních ideálů je Bezoutův, což nutně znamená, že v něm platí podmínka D.
Tedy podle věty o DP zde platí podmínka P.
Podle věty o PJ to znamená, že tu platí podmínka J.
Gaussův obor jsme definovali jako obor integrity, ve kterém platí podmínky I a J.
Nyní budeme dokazovat, že tu platí podmínka I.
To podle věty o KI znamená, že můžeme dokázat, že zde platí podmínka K.
Předpokládejme tedy, že K neplatí a relace $\preceq$ není fundovaná na $[R]$.
To znamená, že existuje nekonečná posloupnost prvků z R taková, že $a_{i+1} \mid a_i$.
Podle lemmatu 1.3.36 to znamená, že $(a_i) \subseteq (a_{i+1})$.
Definujme $I = \bigcup_{i=1}^{\infty} (a_i)$.
Dokážeme si nyní, že $I \subseteq R$.
Uvažujeme nějaký prvek $x \in I$.

Podle definice I musí existovat $k \in \mathbb{N}$ takové, že $x \in (a_k)$.
Víme ale, že $(a_k) \trianglelefteq R$, takže určitě platí $(a_k) \subseteq R$.
Z transitivity podmnožiny dostáváme tedy $I \subseteq R$.
Dokažme si tedy, že množiny jsou uzavřené na sčítání.
Vezměme x,$y \in I$, pak existují i,$j \in \mathbb{N}$ takové, že $x \in (a_i)$ a $y \in (a_j)$.
Bez újmy na obecnosti předpokládejme, že $i < j$.
Pak ale musí platit $x + y \in (a_j)$, protože $(a_j) \trianglelefteq R$.
Z definice I dostáváme, že $x + y \in I$.
Analogicky platí, že $rx \in I$ pro každé $r \in R$.
Tedy $I \trianglelefteq R$.
Ale v oboru hlavních ideálů existuje jednotkový prvek, tedy musí platit $1_R \in I$.
Podle definice I existuje k, takové, že $1_R \in (a_k)$.
Podle lemmatu 1.3.36 platí $(a_k) \subseteq I$.
Avšak jsme dříve dokázali, že $I \subseteq (a_k)$.
Tedy dostáváme, že $I = (a_k)$ pro nějaké k.
Ale podle předpokladu platí $(a_k) \subseteq (a_{k+1})$.
Nechť $x \in (a_{k+1}) - (a_k)$. Pak z definice I musí platit $x \in I$, ale to je spor, protože jsme dokázali, že $I = (a_k)$.
To znamená, že musí platit podmínka K.

□

Definujme Euklidovu normu, u které ukážeme, že je nutně Dedekind–Hasse normou a pomocí které můžeme definovat Euklidův obor, kde dokážeme, že funguje Euklidův algoritmus a tedy máme efektivní způsob, jak najít největšího společného dělitele.

Definice 3.4.49 (Euklidova norma)**.** *Nechť R je obor integrity a funkci $f : R - \{0\} \longrightarrow \mathbb{N}$ nazýváme ostře Euklidovskou normou, pokud pro libovolné nenulové a,$b \in R$ platí: $b \mid a \vee (a = bc + r \wedge f(r) < f(b))$.*

Definice 3.4.50 (Euklidův obor)**.** *Nechť R je obor integrity a existuje v něm Euklidova norma. Pak obor nazveme Euklidovým oborem.*

Věta 3.4.51 (Euklidův obor a algoritmus)**.** *Nechť R je Euklidův obor. Pak v něm lze použít Euklidův algoritmus.*

Důkaz. Euklidův algoritmus je definován následovně:
Mějme dány dva prvky uložené v proměnných u a w.
Dokud $w \neq 0$, opakuj:
$r =$ `u mod w`
$u = w$
$w = r$
Po skončení algoritmu je v u uložen největší společný dělitel původních čísel.

Z definice Euklidovy normy vidíme, že existuje ostře klesající řetězec hodnot funkcí našich zbytků při provádění algoritmu. Jelikož je to funkce do přirozených čísel, posloupnost musí být konečná, protože bude mít maximálně $f(u)$ kroků. Pokud taková posloupnost neexistuje, Euklidův algoritmus se nezastaví.

□

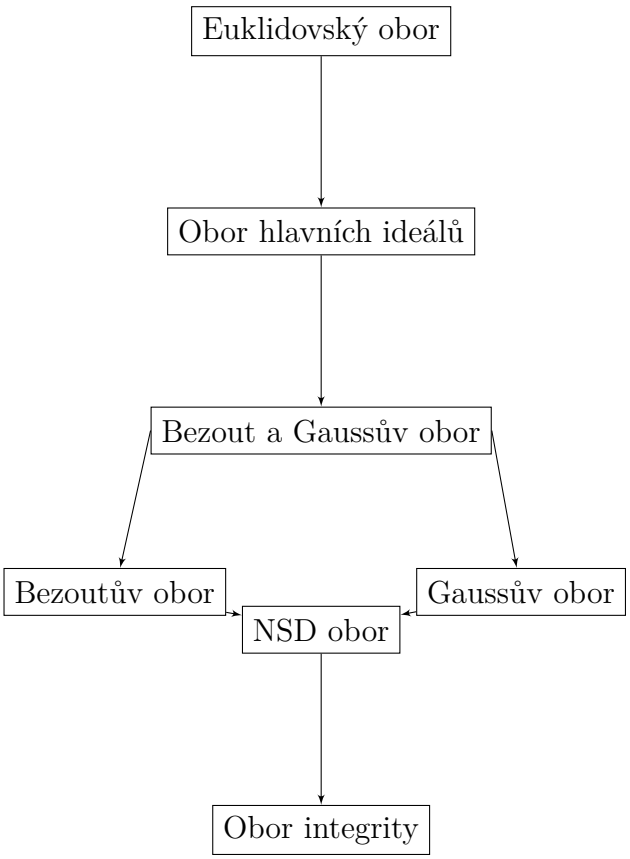
Nyní dokážeme, že Euklidův obor je oborem hlavních ideálů, avšak opačně to platit nemusí. Existují obory hlavních ideálů, které nejsou Euklidovské. Například $\mathbb{Z}[\frac{1+\sqrt{-19}}{2}]$ je obor, který není Euklidovský viz. článek Wilson (2015)

Věta 3.4.52 (Euklidův obor a obor hlavních ideálů)**.** *Každý Euklidův obor je oborem hlavních ideálů.*

Důkaz. Podle lemmatu 3.4.42 stačí dokázat, že každá Euklidova norma je Dedekind–Hasse normou.
Mějme tedy Euklidovu normu f. Musíme dokázat, že existuje prvek $d \in (a,b)$ takový, že $f(d) \neq f(b)$.
Podle Euklidovy normy máme $f(r) < f(b)$ takové, že $a = bc + r$.
Stačí dokázat, že $r \in (a,b)$. Z $a = bc + r$ dostáváme $r = a - bc$. Jelikož ideál je uzavřen na násobení prvky z R, tak i $bc \in (a,b)$. Ideál je uzavřen na rozdíly, a tedy $a - bc \in (a,b)$. To dokazuje, že $r \in (a,b)$, a tudíž je Euklidova norma Dedekind–Hasse normou.

□

Tím jsme dokázali, že každý Euklidův obor je oborem hlavních ideálů. Máme tedy hierarchii oborů: Gaussovy obory, Bezoutovy obory ⊂ NSD obory ⊂ obory integrity ⊂ okruhy. Dále víme, že platí Euklidovy obory ⊂ obory hlavních ideálů = Bezoutovy obory + Gaussovy obory.



Závěr

V rámci práce jsme definovali dvě verze teorie dělitelnosti. První verze popisuje jak definovat Gaussova čísla, na kterých jsme ukázali podmínky dělitelnosti definované na oboru integrity a jejich vzájemné vztahy. Také jsme dokázali, že tyto obory integrity jsou přesně ty, které chceme využívat pro studium dělitelnosti.

Ukázali jsme, že přidáním axiomu, který stanovuje existenci největšího společného dělitele pro každou konečnou množinu, můžeme dokázat distributivitu největšího společného dělitele vzhledem k násobení. Přidáním dalšího axiomu, který určuje, že na faktorovém oboru daného oboru integrity je relace vlastního dělitele fundovaná, anebo že každý nenulový neinvertibilní prvek má ireducibilní rozklad, získáme teorii, kde platí Zobecněná základní věta aritmetiky.

V druhé verzi pomocí ideálů jsme definování dělitelnosti prováděli pomocí ideálů a díky tomu, jsme dokázali platnost Zobecněné Čínské zbytkové věty. Tedy existuje opodstatnění zkoumat a řešit dělitelnost na obecných unitárních komutativních okruzích, ale pokud neplatí Bezoutova věta, tak nevíme jak tuto úlohu vyřešit. Proto jsme pomocí ideálů definovali Bezoutovy obory, které nám dávají návod, jak tuto úlohu vyřešit.

Tyto obory jsou charakterizovány platností Zobecněné Bezoutovy věty, která říká, že pro libovolné dva prvky je jejich společný největší dělitel lineární kombinací těchto prvků. Dále jsme demonstrovali, že pokud máme obor integrity, který je zároveň Bezoutův a Gaussův, pak v něm každý ideál je hlavní, tj. lze jej generovat jedním prvkem. Zvláštním případem takového oboru integrity je Euklidův obor, který reprezentuje obory, kde se Euklidův algoritmus zastaví a umožňuje polynomiální řešení v závislosti na délce vstupu a tedy dokonce máme algoritmus pro nalezení největšího společného dělitele.

Seznam použité literatury

Koříněk, V. (1956). *Základy Algebry.* Academia.

Kunen, K. (2021). *Set Theory.* College Publications.

Procházka, L. (1990). *Algebra.* Academia.

Přikrylová, K. (2013). *Pojem ideálu a filtru v algebře a logice.* Bakalářská práce, Katedra logiky Filozofické fakulty, Karlova Univerzita, Praha.

Wilson, R. (2015). *An example of a PID which is not a Euclidean.* Internet.