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 2022

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

Mé poděkování patří všem vyučujícím na katedře logiky, kteří mě prováděli studiem a spousty mě toho naučili. Jmenovitě bych chtěl poděkovat zejména Doc. RNDr. Vítězslav Švejdar, CSc. za odborné vedení, trpělivost a ochotu, kterou mi v průběhu zpracování bakalářské práce věnoval.

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 nastínit hierarchii oborů dělitelnosti s vlastnostmi, které očekáváme, že budou platit obdobně jako při dělení na celých číslech. Pomocí ideálů zobecňujeme Čínskou zbytkovou větu a na ní demonstrujeme, že se může vyplatit oslabit obecnost teorie, protože máme poté efektivnější nástroje, jak hledat řešení. Práce je zpracovaná pro všechny zájemce o matematiku, kteří chtějí nahlednout do teorie dělitelnosti, proto teorii budujeme od počátku a srovnáváme ji s dělením na celých číslech.

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

Title: The Divisibility Relation in Rings

Author: Michal Ketner

Department: Name of the department

Supervisor: doc. RNDr. Vítězslav Švejdar, CSc., department

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

Obsah

Úvod

Dělitelnost standardně zkoumáme ve struktuře celých nebo přirozených čísel. Na 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, který je pojmenován 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 ale i zároveň Bezoutovým oborem, což je obor, kde platí Bezoutova věta, kterou v roce 1748 Leonhard Euler a Gabriel Cramer uvedli, ale ani jednomu se nepodařilo dokončit důkaz. O několik let později, v roce 1764, dal Etienne Bezout první uspokojivý důkaz jako výsledek dřívější práce Colina Maclaurina. Ve skutečnosti byl tento důkaz neúplný v několika bodech. Kompletní důkaz přišel o více než sto let později, v roce 1873, díky Georges-Henri Halphenovi. Tato věta nám říká, že největší společný násobek dvou čísel lze zapsat jako jeho lineární kombinaci. Existují ale i obory, kde tento požadavek neplatí. Takovým oborem je například obor polynomů nad celými čísly, ve kterém sice platí základní věta aritmetiky, ale neplatí v něm Bezoutova věta. Obory, kde platí základní věta aritmetiky, se jmenují Gaussovy obory. Platí to, že naopak existují i Bezoutovy obory, ve kterých neplatí základní věta aritmetiky - takový oborem je obor algebraických čísel. Dokonce existuje i obor hodnot, kde neexistuje největší společný dělitel. Takovým oborem jsou algebraická celá čísla, ale na těchto číslech funguje naše zevšeobecněná čínská zbytková věta.

1. Dělitelnost

1.1 Obory integrity a jejich vlastnosti

Dělitelnost se učíme zkoumat většinou na přirozených nebo celých číslech, pojďme důležité vlastnosti celých čísel zevšeobecnit a vytvořit algebraický pojem, kterému se říká okruh. Taková struktura je uzavřená na sčítání a násobení, pří sčítání nezáleží na pořadí ani závorkách. Víme jak roznásobovat a vytýkat a existuje tu takový prvek, který když k libovolnému prvku přičteme, tak se prvek nezmění. Poslední vlastností celých čísel, kterou budeme chtít zachovat, je existence opačného prvku vzhledem ke sčítání. Nyní si tyto vlastnosti zapíšeme axiomaticky.

Definice 1.1.1 (Okruh)**.**
Nosič R se dvěma binárními operacemi $+$ a $*$ nazveme okruhem, pravě tehdy když pro všechny x,y,$z \in R$ splňuje následující axiomy:

1. *Uzavřenost sčítání a násobení:*

$$(x + y \in R),$$
$$(x * y \in R).$$

2. *Asociativita operací:*

$$(x + y) + z = x + (y + z),$$
$$(x * y) * z = x * (y * z).$$

3. *Komutativita sčítání:*

$$x + y = y + x.$$

4. *Existence neutrálního prvku pro sčítání (budeme jej značit 0):*

$$(\exists 0 \in R)(x + 0 = x).$$

5. *Existence opačného prvku pro sčítání:*

$$(\exists o \in R)\,(x + o = 0).$$

6. *Oboustranná distributivita sčítání a násobení:*

$$x * (y + z) = (x * y) + (x * z),$$
$$(y + z) * x = (y * x) + (z * x).$$

Rozeberme si podrobněji, co tyto axiomy okruhu o této struktuře říkají. Začněme prvním axiomem uzavřenosti sčítání a násobení nám říká, že okruh je uzavřen na tyto dvě operace. To znamená, že pro každé dva prvky nosiče jsou v nosiči i výsledky těchto dvou operací. Pro usnadnění zápisu $(x * y)$ můžeme zapisovat i jako xy. Zaveďme si ještě zkratku pro součin n stejných prvků x jako x^n. Druhý axiom říká, že nezáleží na závorkách pří sčítání ani při násobení, proto například místo $(a+b)+c$, můžeme psát $a+b+c$. Podle třetího axiomu nezaleží na pořadí prvků při sčítání. Ve čtvrtém axiomu jsme označili neutrální prvek jako 0. Ukažme si, že tato definice je korektní a že neutrální prvek je určen jednoznačně.

Lemma 1.1.2.
V okruhu je neutrální prvek určen jednoznačně.

Důkaz:
Uvažujme, že máme h,$f \in R$, které oba jsou neutrální prvky.
Proto pro libovolné $x \in R$ platí jak $x + h = x$, tak $x + f = x$.
Dosadíme do rovnice $x + h = x$ oba prvky f i h.
Dostali jsme, že $f + h = f$ a $h + f = h$.
Ze třetího axiomu ale víme, že $f + h = h + f$.
Z čehož plyne, že $h = f$.

□

Dokázali jsme, že neutrální prvek v okruhu je určen jednoznačně. Označme si jej jako 0. Pokračujme k dalšímu axiomu, který nám říká, že ke každému prvku v okruhu existuje opačný prvek vůči sčítání. Dokážeme si, že tento prvek je pro každý prvek určen jednoznačně.

Lemma 1.1.3.
V okruhu je opačný prvek určen jednoznačně.

Důkaz:
Pro libovolné $x \in R$ uvažujme h,$f \in R$, které oba jsou opačnými prvky pro x.
Vezměme $x + f = 0$ a přičtěme k oběma stranám h.
Dostaneme $h + x + f = h$, ale z předpokladu víme, že i h je opačný prvek k x.
Proto platí $f = h$ a proto je opačný prvek určen pro libovolný prvek v okruhu jednoznačně.

□

Dokázali jsme, že pro libovolný prvek x existuje opačný prvek vzhledem ke sčítání, který je určený jednoznačně. Budeme ho značit $-x$. Pro přehlednější zápis pišme místo $a + (-x)$ zkráceně $a - x$.
Poslední axiom Oboustranná distributivita násobení a sčítání nám ukazujeme jak roznásobovat součty a vytýkat ze součtů.
Ještě jsme si neřekli, jak se bude chová neutrální prvek sčítání chová při násobení. Bude to standardně také jako v celých číslech. Proto jeho libovolný násobek bude zase on sám. Tuto vlastnost neutrálního prvku si nyní dokážeme.

Lemma 1.1.4.
Mějme okruh R a libovolné $a \in R$. Pak $a * 0 = 0$.

Důkaz:
Mějme okruh R a v něm prvek $a \in R$.
Podle distributivního zákonu platí, že $a * (a + 0) = a^2 + a * 0$.
Z definice nulového prvku máme $a = a + 0$.
Po přenásobení a a dostaneme $a^2 = a * (a + 0)$.
Tím pádem dostaneme $a^2 = a^2 + a * 0$.
Ale jsme okruhu proto $a^2 = b$ pro nějaké $b \in R$.
Z definice okruhu pro $b \in R$ musí existovat opačný prvek vzhledem ke sčítání.
Tento prvek můžeme přičíst k oběma stranám rovnice $b - b = b + a * 0 - b$.
Po úpravě dostaneme $0 = a * 0$.

□

Jednoznačnost nulového prvku vůči sčítání, jednoznačnost opačného prvku vůči sčítání pro každý prvek ve struktuře a násobení nulovým prvkem ve struktuře platí samozřejmě pro libovolný okruh. Ústředním tématem této práce je specifický druh okruhů, kterým jsou obory integrity. Jsou to další vlastnosti, celých čísel, které si přidáme k naší definici a to, že při násobení nezáleží na pořadí, že existuje prvek vzhledem k násobení, kterým když vynásobím libovolný prvek, tak se prvek nezmění. Nakonec budeme ještě požadovat, že neexistují dělitelé nuly, které by nebyly samy nulou. Nyní si tyto vlastnosti zformalizujme.

Definice 1.1.5 (Obor integrity)**.**
Mějme okruh R. Pak R je oborem integrity, právě tehdy když pro libovolné x,$y \in R$ splňuje následující axiomy:

1. *Komutativnost násobení:*

$$xy = yx.$$

2. *Existence neutrálního prvku vzhledem k násobení:*

$$(\exists y \in R)(\forall x \in R)\,(xy = x).$$

3. *Neexistence vlastních dělitelů nulového prvku:*

$$xy = 0 \rightarrow (x = 0 \vee y = 0).$$

Obor integrity je takový okruh ve kterém je násobení komutativní. To je takový obor integrity, při kterém nezáleží na pořadí. Z tohoto důvodu jsme si mohli dovolit zjednodušit definici neutrálního prvku pro násobení a psát jí jen pro použití neutrálního prvku pro násobení z jedné strany. V oboru integrity existuje i neutrální prvek vzhledem k této operaci, aby se nám to nepletlo s neutrálním prvkem vůči sčítání, tak říkejme neutrálnímu prvku vzhledem ke sčítání prvek nulový a neutrálnímu prvku vzhledem k násobení prvek jednotkový. Nyní si dokážeme, že jednotkový prvek je v oboru integrity určen také jednoznačně.

Lemma 1.1.6.
V oboru integrity je jednotkový prvek určen jednoznačně.

Důkaz:
Uvažujme, že máme dva jednotkové prvky h,$f \in R$.
Pro libovolné $x \in R$ platí $xh = x$ a $xf = x$.
Dosadíme f do první rovnice a h do druhé.
Dostaneme $fh = f$ a $hf = h$.
V oboru integrity platí komutativita násobení a proto $h = f$.

□

Dokázali jsme, že jednotkový prvek je určen v oboru integrity jednoznačně, budeme jej značit jako 1. Určitě se hodí otázka, jak je to s opačnými prvky vzhledem k násobení. Takové obory integrity samozřejmě existují a říká se jim tělesa. Tělesa jsou takové okruhy, které ke každému nenulovému prvku obsahují prvek opačný vzhledem k násobení. Lze dokázat, že tělesa jsou oborem integrity. Nás ale budou zajímat obory integrity obecně, protože v nich chceme zkoumat dělitelnost a v tělesech je dělitelnost triviální. Prvky s opačným prvkem vůči násobení nás rozhodně zajímat budou jen nezaručujeme jejich existenci. Prvek, který má opačný prvek vzhledem násobení, budeme nazývat prvkem invertibilním. Abychom nemuseli zdlouhavě psát opačný prvek vzhledem k násobení a opačný prvek vzhledem ke sčítání, tak opačným prvkem budeme dále nazývat opačný prvek vzhledem ke sčítání a prvkem inverzním opačný prvek vzhledem násobení. Defimujme si nejdříve formálně inverzní prvek.

Definice 1.1.7 (Inverzní prvek)**.**
Mějme obor integrity R. Pak říkáme, že prvek $x \in R$ je inverzní prvek k prvku $y \in R$, když platí $xy = 1$.

Máme definovaný inverzní prvek. V oborech integrity obecně nemusí pro každý prvek existovat jeho prvek inverzní. My si dokážeme, že pokud takový prvek už v oboru integrity existuje, tak je určen jednoznačně.

Lemma 1.1.8.
Pokud existuje inverzní prvek v oboru integrity, tak je určen jednoznačně.

Důkaz:
Uvažujme h,$f \in R$, které oba jsou inverzní prvky pro libovolné $x \in R$.
Vezměme $xf = 1$ a vynásobme obě strany h. Dostaneme $hxf = h$.
V oboru integrity platí asociativní zákon a komutativní zákon pro násobení.
Dostáváme proto, že $(xh)f = h$.

Z předpokladu víme, že i h je inverzní prvek k x .
Proto platí, že $f = h$ podle axiomu o jednotkovém prvku.

□

Dokázali jsme, že pokud inverzní prvek existuje, tak je určen jednoznačně, budeme inverzní prvek pro prvek x značit jako x^{-1}. Jak už bylo zmíněno, takový prvek nemusí pro nějaké prvky existovat, definujme si tedy takové prvky, pro které inverzní prvek existuje a následně si definujme množinu všech invertibilních prvků.

Definice 1.1.9 (Invertibilní prvek)**.**
Mějme obor integrity R. Pak prvek x je invertibilní prvek, pokud $x^{-1} \in R$.

Jelikož tyto prvky nemusíme zkoumat moc podrobně, tak všechny takové prvky, které reprezentují v oborech integrity tuto vlastnost definujme množinu všech takových to prvků v oboru integrity.

Definice 1.1.10 (Invertibilní třída)**.**
Mějme obor integrity R. Pak $R^* = \{x \in R; x^{-1} \in R\}$.

Nyní si dokažme, že i jednotkový prvek je vlastně prvkem invertibilním, a tedy o něm dále nemusíme mluvit yvlášť a budeme mluvit obecně o prvcích invertibilních a o jejich vlastnostech.

Lemma 1.1.11.
Nechť R je obor integrity. Pak jednotkový prvek je invertibilní.

Důkaz:
Z axiomu existence inverzního prvku víme, že pro libovolný nenulový prvek oboru integrity ($x \in R$) platí ($x = 1 * x$).
Jednotkový prvek je také prvkem R.
Po dosazení dostaneme $1 = 1 * 1$ a tedy jednotkový prvek je invertibilním prvkem. Protože je sám k sobě inverzní.

□

Dokázali jsme si tedy základní vlastnosti oborů integrity a jak se v nich chovají neutrální a jednotkový prvek. Poslední axiom nám říká, že neexistují takzvaní netriviální dělitelé nulového prvku. Proto si v nadcházející podkapitole budeme definovat dělení v oborech integrity a ukážeme si jeho základní vlastnosti.

1.2 Dělení v oborech integrity

Dělení bývá chápáno jako inverzní operace k násobení, z této vlastnosti také výjdeme při definici. Jak už jsme psali, jsme obecně v oborech integrity a ne jen v tělesech, proto se zde každé dva prvky se dělit vzájemně nemusí. Víme, že například v celých číslech je, že prvek a dělí prvek b je ekvivalentní s tím, že b je násobek a. Definujme tedy takto relace dělitelnosti obecně v oborech integrity. Tento vztah a dělí b budeme zapisovat jako $a \mid b$.

Definice 1.2.1 (Dělitelnost)**.**
Nechť R je obor integrity. Pak říkáme o prvcích a,$b \in R$, že $b \mid a$, existuje-li $c \in R$ takové, že $a = bc$.

Ukažme si nyní nejdříve jak se vůči této relaci chová nulový prvek, a proto si nejdříve dokážeme, že nulový prvek je dělitelný libovolným prvkem a že nulový prvek dělí jen sám sebe.

Lemma 1.2.2.
Mějme obor integrity R. Pak pro nulový prvek $0 \in R$ a libovolný prvek $a \in R$ platí, že $a \mid 0$.

Důkaz:
Mějme obor integrity R a vezměme libovolný prvek $a \in R$.
Podle definice relace dělitelnosti $a \mid 0$ znamená, že $0 = ac$ pro nějaké $c \in R$.
Takové c dle lemmatu 1.1.4 známe a je jím právě 0.

□

Lemma 1.2.3.
Mějme obor integrity R. Pak pro nulový prvek $0 \in R$ a libovolný prvek $a \in R$ platí. že $0 \mid a \rightarrow a = 0$.

Důkaz:
Mějme obor integrity R a libovolné $a \in R$.
Z $0 \mid a$ víme, že existuje $c \in R$ takové, že $a = c * 0$.
Podle lemmatu 1.1.4 dostáváme, že $a = 0$.

□

Tak jako jsme postupovali u neutrálního prvku, tak budeme stejně postupovat u prvku jednotkového, respektive v tomto případě budeme mluvit obecně o invertibilních prvcích, protože jak jsme dokázali, jednotkový prvek je prvkem invertibilním. Dokažme nejdříve, že invertibilní prvek naopak od neutrální dělí libovolný prvek, který není nulový, protože jak jsme dokázali, ten může dělit jen prvek neutrální a poté dokažme, že prvek invertibilní je dělitelný zas jen invertibilním prvkem.

Lemma 1.2.4.
Nechť R je obor integrity. Pak pro libovolný invertibilní prvek $e \in R^*$ a libovolný prvek oboru integrity $a \in R - 0$ platí, že $e \mid a$.

Důkaz:
Vezměme libovolné $a \in R - 0$ a $e \in R^*$.
Z definice invertibilního prvku víme, že existuje $e^{-1} \in R$ takové, že $1 = ee^{-1}$.
Pokud tuto rovnici vynásobíme a, tak dostaneme $a = (ee^{-1})a$.
Z definice okruhu víme, že násobení je asociativní a tedy dostaneme $a = e(e^{-1}a)$.
Máme tedy nějaké $c \in R$, pro které platí $c = e^{-1}a$.
A tedy máme $a = ec$ pro nějaké $c \in R$.
Což podle definice znamená, že $e \mid a$.

□

Dokázali jsme tedy, že invertibilní prvky dělí všechny nenulové prvky oboru integrity, dokažme si tedy ještě, že invertibilní prvek je dělitelný jen invertibilním prvkem.

Lemma 1.2.5.
Nechť R je obor integrity. Pak libovolné $f \in R^*$ a libovolné $e \in R$ platí, že $e \mid f \to e \in R^*$

Důkaz:
Mějme libovolné $e \in R$.
Z $e \mid f$ víme, že $f = eg$, pro nějaké $g \in R$.
f je ale invertibilní, a tedy existuje $f^{-1} \in R$.
Tímto prvkem vynásobíme $f = eg$.
Dostaneme tedy $ff^{-1} = egf^{-1}$.
V oboru integity tedy existuje prvek $h \in R$ takový, že pro něj platí $h = gf^{-1}$.
Dostaneme tedy $1 = eh$ pro nějaké $h \in R$.
Ž čehož je zřejmě, že k e existuje v oboru integrity inverzní prvek, a tedy e je invertibilní.

□

Dokažme si o relaci dělitelnosti, že je kvaziuspořádáním. Nebudeme dokazovat, že je relací uspořádání, protože jí být obecně ani nemusí, a dokonce jí není například na celých číslech. Protože prvek a jeho opačný prvek se vzájemně dělí.

Lemma 1.2.6.
Relace dělení v oboru integrity R je kvaziuspořádání na množině R.

Důkaz:
R je obor integrity. Podle definice existuje jednotkový prvek $a * 1 = a$.
To podle definice relace dělitelnosti znamená $a \mid a$.
Dokázali jsme, že relace dělitelnosti je vždy v oboru integrity 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 oboru integrity 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.

□

Máme dokázáno, že relace dělitelnosti je tedy kvaziuspořádáním, ale může obsahovat cykly, tento problém ovšem vyřešíme v následující podkapitole tím, že tyto prvky ztotožníme. Nejdříve, ale si definujme základní pojem z teorie dělitelnosti a tím je společný dělitel, respektive největší společný dělitel. V naší teorii, ale takových dělitelů může být klidně víc, například pokud je nějaký prvek největší společný dělitel, tak zároveň i prvek opačný je největším společný dělitelem. Definujme si nejdříve společné dělitele nějaké množiny, tedy prvky dělící všechny prvky nějaké množiny. Pro množinu M budeme tuto množinu značit jako $SD(M)$

Definice 1.2.7 (Společní dělitelé)**.**
Nechť R je obor integrity a $M \subseteq R$. Pak

$$SD(M) = \{y \in R; x \in M \to y \mid x\}.$$

Máme tedy množinu všech společných dělitelů. Definujme množinu největších společných dělitelů, jako dělitele, které dělí všichni společní dělitelé. Definujme si tedy množinu největších společných dělitelů. Budeme jí značit pro množinu M jako $NSD(M)$.

Definice 1.2.8 (Největší společní dělitelé)**.**
Nechť R je obor integrity a $M \subseteq R$. Pak

$$NSD(M) = \{x \in SD(M); y \in SD(M) \to y \mid x\}.$$

Největší společný dělitel však v oboru integrity nemusí existovat. Například pokud si vezmeme množinu celých čísel a přidáme k ní množinu násobků odmocnin ze záporného prvočísla, pak taková struktura je oborem integrity. Pro tento příklad zvolme $\mathbb{Z}[\sqrt{3}]$. V tomto oboru integrity platí $a = 2 * 2 = 4 = (1 + \sqrt{-3}) * (1 - \sqrt{-3})$ a $b = (1 + 1\sqrt{-3}) * 2$. Společným dělitelem takových prvků je jak $1 + 1\sqrt{-3})$ tak i 2, ale tyto prvky se vzájemně nedělí. Proto jak si ukážeme v následující kapitole podmínka existence největšího společného dělitele nějaké množiny je důležitý axiom. Proto si o největším společném dělitele nejdřív dokážeme, že pro dva prvky existuje právě tehdy, když existuje pro libovolnou konečnou množinu, ale proto si nejdříve budeme muset dokázat lemma, které nám říká, že největší společní dělitelé sjednocení dvou množin je největší společný dělitel největších společných dělitelů těchto množin.

Lemma 1.2.9.
Nechť R je obor integrity a A,$B \subset R$,$a \in NSD(A)$ a $b \in NSD(B)$. Pak

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

Důkaz:
Nejdříve si dokažme inkluzi $NSD(A \cup B) \subset NSD(a,b)$.

Mějme tedy nějaké $d \in NSD(A \cup B)$.
Z definice $NSD(A \cup B)$ víme, že pro libovolný prvek $c \in SD(A \cup B)$ platí $c \mid d$.
Pro libovolné $c \in SD(A \cup B)$ platí $c \in SD(A)$ i $c \in SD(B)$
Z předpokladu víme, že $a \in NSD(A)$ a $b \in NSD(B)$.
Což znamená, že $d \mid a$ a $d \mid b$, dokázali jsme tedy, že $d \in SD(\{a,b\})$.
Dokažme si, že pokud je nějaký prvek $f \in SD(\{a,b\})$, tak pak $f \mid d$.
Mějme nějaký prvek $f \in SD(\{a,b\})$, tedy $f \mid a$ a $f \mid b$.
Z předpokladu $a \in NSD(A)$ a $b \in NSD(B)$ máme, že a dělí každý prvek A a b dělí každý prvek B.
Z transitivity dostáváme, že $f \mid x$ pro libovolný prvek z $x \in A \cup B$.
Platí, tedy že $f \in SD(A \cup B)$, ale z předpokladu víme, že platí $d \in NSD(A \cup B)$ takže musí platit, že $f \mid d$.
Dokažme si opačnou inkluzi $NSD(\{a,b\}) \subset NSD(A \cup B)$.
Mějme nějaký $d \in NSD(\{a,b\})$. To znamená, že d dělí a i b.
Z předpokladu a dělí každý prvek A a z transitivity dostaneme, že d dělí každý prvek A.
Obdobně protože b dělí každý prvek B z transitivity dostaneme, že d dělí každý prvek B.
Máme tedy, že d dělí každý prvek $A \cup B$ a tedy $d \in SD(A \cup B)$.
Dokažme si, že d je největší společný dělitel.
Nechť tedy mějme nějaké $h \in SD(A \cup B)$.
Proto musí určitě platit $h \in SD(A)$ a $h \in SD(B)$, z čehož plyne, že $h \mid a$ a $h \mid b$, jinak by prvek a nebyl největší společný dělitel na A a b nebyl největší společný dělitel na B.
Z toho ale plyne, že $h \in SD(\{a,b\})$. Proto musí platit, že $h \mid d$ jinak by nebylo $d \in NSD(\{a,b\})$.
Dostáváme tedy $d \in NSD(A \cup B)$.

□

Dokázali jsme tedy, jak se chová největší společný dělitel vůči sjednocení. Dokažme si nyní, díky tomu že podmínky, že každá dvouprvková množina má v oboru integrity aspoň jeden největší společný dělitel a že každá konečná množina má v oboru integrity aspoň jeden největší společný dělitel jsou ekvivalentní podmínky.

Lemma 1.2.10.
Nechť R je obor integrity. Pak následující dvě podmínky jsou ekvivalentní:

1. *Každá dvouprvková množina z R má v R aspoň jednoho největšího společného dělitele.*

2. *Každá konečná množina z R má v R aspoň jednoho největšího společného dělitele.*

Důkaz:
Pokud každá konečná množina má společného dělitele, tak rozhodně bude mít i každá dvouprvková množina.
Dokazujme tedy teď opačnou implikaci. Mějme nějakou $M \subset R$ konečnou podmožinu.

Postupujme indukcí podle mohutnosti M:
Pokud $m = 1$ tak $M = \{x\}$.
Relace dělení podle lemmatu 1.2.6 je reflexivní.
Proto ($x \in SD(M)$), v $SD(M)$ jsou jen prvky, které dělí x a tedy podle definice $x \in NSD(M)$.
Pokud $m = 2$, tak lemma je tautologie.
Dokazujme tedy tvrzení pro $m \geq 3$ a máme indukční předpoklad, že tvrzení platí pro $m - 1$.
Vezmeme libovolné $a \in M$ a definujme $B = M - \{a\}$.
Podle indukčního předpokladu existuje $b \in NSD(B)$.
Z definice B víme, že $NSD(M) = NSD(B \cup \{a\})$.
Z lemmatu 1.2.9 dostaneme $NSD(\{a,b\}) = NSD(B \cup \{a\})$, z čehož dostaneme $NSD(M) = NSD(\{a,b\})$.
Množina $NSD(\{a,b\})$ je z předpokladu neprázdná, takže i množina $NSD(M)$ musí být neprázdná.

□

1.3 Prvočísla

Nyní zobecníme dvě vlastnosti prvočísel, jednou vlastností je, že pokud prvočíslo dělí nějaký součin, tak dělí jeden z činitelů součinu, proto prvek s touto vlastností budeme nazývat prvočinitel. Při definici na přirozených číslech je touto vlastností, že libovolný prvek nedělí žádné jiné prvky, které nejsou jedničkou nebo nejsou tím samým prvkem. Tato vlastnost v obecném okruhu je samozřejmě silná, protože můžeme mít více prvků, které stejně jako jednička, dělí všechny prvky. Tedy potom definici změníme na to, že to jsou takové prvky, které jsou dělitelné jen invertibilním prvkem nebo sebou samým. Když se ale podíváme například na celá čísla, tak podle naší definice, se vzájemně opačné prvky dělí vždy. Tedy bychom neměli, žádná taková čísla. Zobecněme tedy tuto vlastnost a takovým číslům dejme výjimku. Takovým prvkům budeme říkat prvky asociované. Na základě této vlastnosti, můžeme dovysvětlit poslední část definice oboru integrity, kde tvrdíme, že neexistují vlastní dělitelé nuly. Proto si definujeme pojem vlastního dělitele jako prvku takového, že je invertibilní a zároveň s prvkem není asociovaný. Díky tomu, také můžeme definovat druhou vlastnost prvočísel a tím je nedělitelnost. Takovým prvkům budeme říkat ireducibilní prvky. To jsou takové prvky, které nejsou nulovým ani jednotkovým prvkem a současně nemají žádné vlastní dělitele. Následně si ukážeme, že obecně je v oborech integrity prvočinitelnost silnější podmínkou než je ireducibilita. Jak si, ale ukážeme v následující kapitole, tak pokud budeme mít obor integrity, kde zaručíme existenci největšího společného dělitele. V takových oborech integrity jsou tyto dvě podmínky ekvivalentní. Začneme tedy definicí prvočinitele.

Definice 1.3.1 (Prvočinitel)**.**
Nechť R je obor integrity a pro libovolná $p,a,b \in R$, pro která platí, že $p \neq 0$ a $p \notin R^*$. Definujeme, že p je prvočinitel, právě tehdy když $p \mid ab \rightarrow (p \mid a \vee p \mid b)$.

Nyní si dokažme, že z této definice plyne už platnost pro libovolný konečný součin a ne jen součin dvou prvků.

Lemma 1.3.2.
Nechť R je obor integrity a a_1,...,a_n,$b \in R$. Pak $b \mid a_1$,..$a_n \rightarrow \bigvee_{i=1}^{n} b \mid a_i$

Důkaz:
Mějme obor integrity R.
Postupujme indukcí podle n.
Nechť $n = 1$, pak $b \mid a_1 \rightarrow b \mid a_1$.
Dokažme tedy indukční krok $b \mid a_1$,..$a_n \rightarrow \bigvee_{i=1}^{n} b \mid a_i$.
Pokud $b \mid a_1$,..a_n, tak podle definice $b \mid a_1$,..$a_{n-1} \vee b \mid a_n$.
Když bude platit, že $b \mid a_n$, tak rozhodně platí $\bigvee_{i=1}^{n} b \mid a_i$
Pokud platí, že $b \mid a_1$,..a_{n-1}, tak z indukčního předpokladu plyne, že $\bigvee_{i=1}^{n-1} b \mid a_i$, což ale nutně musí znamenat, že $\bigvee_{i=1}^{n} b \mid a_i$.

□

Nyní jsme dokázali, že definice prvočinitele platí pro libovolný součin. Pro definici ireducibilní ho prvku si budeme muset nejdříve nadefinovat relaci být vlastní dělitel, ale pro definici toho prvku potřebujeme nejdříve definovat relaci asociování, která nám například v celých číslech dá do relace číslo s jeho opačným číslem. Tyto dva prvky se vzájemně dělí. Definujme tedy asociovaní dvou prvků jako jejich vzájemné dělení.

Definice 1.3.3 (Asociování)**.**
Nechť R je obor integrity libovolné $a, b \in R$. Pak definujeme $a \parallel b \leftrightarrow a \mid b \wedge b \mid a$.

Víme, že invertibilní prvky dělí každý prvek. Dalším problém byly asociované prvky, proto při definici vlastního dělitele budeme požadovat vlastního dělitele jako prvek, který je dělitelem, není invertibilní a není s prvkem asociovaný.

Definice 1.3.4 (Vlastní dělitel)**.**
Nechť R je obor integrity. Pak x je vlastní dělitel y, jestliže $x \notin R^*$, $x \mid y$ a prvky x a y nejsou asociované.

Nyní, když máme definovaného vlastního dělitele, můžeme nyní definovat ireducibilní prvek. Jako nenulový neinvertibilní prvek, který nemá žádné vlastní dělitele.

Definice 1.3.5 (Ireducibilní prvek)**.**
Nechť R je obor integrity a $p \in R$, takže $p \neq 0$ a $p \notin R^*$. Pak p je ireducibilní prvek, právě tehdy když p nemá v R žádného vlastního dělitele.

Máme tedy nadefinovány dvě možnosti, jak definovat zobecnění prvočísel, ukážeme si, že každý prvočinitel je vždycky ireducibilním prvkem. Proto, ale budeme muset nejdřív dokázat, jaký vztah mají asociované prvky. Nejdříve si ale proto budeme muset ukázat, že relace asociování ekvivalence, a proto budeme moc z oboru integrity vytvořit faktorobor. Na základě faktoroboru budeme ukazovat vztah asociovaných prvků, protože jak si ukážeme, jsou ve stejné třídě ekvivalence.

Nyní si ukažeme, jaké spoĺu mají asociované prvky vztah, ale budeme si muset nejdřív dokázat, že asociování je v oboru integrity relace ekvivalence

1.4 Faktorobor

Dokažme si, že relace asociování je relací ekvivalence na faktoroboru.

Lemma 1.4.1.
Relace asociovaní v oboru integrity R je ekvivalencí na množině R.

Důkaz:
R je obor integrity.
Tedy existuje jednotkový prvek.
Proto $a \parallel a$ a relace je tedy reflexivní.
Pokud existuje $e \in R$, takové že $a = be$ a zároveň existuje $f \in R$ takové, že $b = cf$.
Tak dosazením za b,dostaneme $a = cef$.
Jsme v oboru integrity, a tedy máme nějaké $d \in R$ takové, že $d = ef$ a tedy že $c = ad$ a tedy a dělí c.
Máme tedy $a \mid c$. Relace asociovaní je na R tranzitivní.
Relace dělitelnosti je tedy také kvaziuspořádáním. My si ale dokážeme, že je tedy dokonce ekvivalencí. Dokažme si tedy symetrii relace. $a \parallel b$ znamená, že $a \mid b$ a současně $b \mid a$.
Logická spojka a současně je komutativní, a tedy definice pro $b \parallel a$ je ekvivalentní $a \parallel b$.
Relace asociování je symetrická.
Dokázali jsme tedy, že relace asociovaní je relace ekvivalence.

□

Touto ekvivalencí jsme ztotožnily prvky, které mohu býti vůči relaci dělitelnosti vzájemně dělitelné. Definujme si tedy přes tuto ekvivalenci faktorizaci na množině R. Tuto faktorovou množinu budeme značit $[R]$. Na této množině definujeme uspořádání $\preceq$. Je-li $a \in R$, pak třídu ekvivalence, kde je obsažen prvek a, budeme označovat $[a]$. Definujme si tedy pomocí $a \in R$ množinu $[R]$.

Definice 1.4.2 (Faktorobor)**.**
Nechť R je obor integrity. Pak $[R] = \{[a]; a \in R\}$.

Faktorová množina $[R]$ je množina tříd ekvivalence podle asociování. Ukažme si nyní postupně, jak jednotlivé třídy vypadají a definujeme uspořádání těchto tříd. Dokažme si nejdříve, jak vypadá taková třída, která obsahuje nulový prvek.

Lemma 1.4.3.
Nechť R je obor integrity. Pak $[0] = \{0\}$.

Důkaz:
Mějme obor integrity R.
Rozhodně platí $0 \subset [0]$, protože relace ekvivalence je reflexivní.
Vezměme si libovolné $a \in [0]$.
Podle definice víme, že $a \mid 0$.
To ale podle lemmatu 1.2.3 to znamená, že $a = 0$.

□

Víme tedy, jak vypadá třída, ve které je nulový prvek. Už dříve jsme dokázali, že jednotkový prvek je prvkem invertibilním a že invertibilní prvek dělí zas jen prvek invertibilní. Ukažme, že všechny invertibilní prvky jsou v jedné třídě ekvivalence společně.

Lemma 1.4.4.
Nechť R je obor integrity. Pak $R^* = [1]$.

Důkaz:
Nejdříve si dokážeme, že $R^* \subset [1]$.
Vezměme, nějaký libovolný prvek $e \in R^*$.
Podle lemmatu 1.2.4 víme, že pro libovolný prvek $a \in R$ platí $e \mid a$ a tedy to platí i pro $1 \in R$.
Ze stejného lem, že $1 \mid e$ a tedy z definice asociování dostáváme, že $1 \parallel e$-
Podle definice třídy ekvivalence $[1]$ dostaneme $e \in [1]$.
Pokračujme důkazem $[1] \subset R^*$.
Mějme nějaké $e \in [1]$, z definice víme, že $e \mid 1$.
Máme $1 = ef$ pro nějaký prvek $f \in R$, ale to tedy znamená, že prvek $e \in R^*$.
□

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

Lemma 1.4.5.
Nechť R je obor integrity a prvky a,$b \in R$ a $a \parallel b$. Pak a je ireducibilní, právě když je b ireducibilní.

Důkaz:
Uvažujme, že a je ireducibilní a b ireducibilní není, což tedy může znamenat tři možnosti:
Buď $b = 0$. Z $a \parallel b$ víme, že $b \mid a$.
To podle lemmatu 1.1.8 znamená, že $a = 0$.
To je spor, protože a je ireducibilní.
Nechť $b \in R^*$.
Existuje inverzní prvek w k b, že pro něj platí, že $wb = 1$.
Z $a \parallel b$ víme, že $a \mid b$.
Tedy $b = ac$ pro nějaké $c \in R$. Vynásobíme tuto rovnici w.
Dostaneme $bw = acw$, ale to znamená, že $1 = acw$.
Jsme v oboru integrity, takže existuje $x \in R$ takové, že $cw = x$.
Máme tedy $1 = ax$ a tedy v R existuje inverzní prvek k a.
Což znamená, že a je invertibilní prvek.
Což je spor s tím, že a je ireducibilní.
Mějme nějakého vlastního dělitele $c \in R$ takové, že $c \mid b$.
Z předpokladu víme, že $b \mid a$.
Podle lemmatu 1.2.6 je dělitelnost tranzitivní.
Dostaneme $c \mid a$, a tedy i a by mělo vlastního dělitele, a tedy by nebylo ireducibilní.

Tedy b musí být také ireducibilní.
Druhá strana implikace je obdobná.

□

Toto tvrzení rozhodně neznamená, že ireducibilní prvky tvoří jen jednu třídu ekvivalence, protože ireducibilní prvky se nemusí ani vzájemně dělit. Dokažme si nyní, že sice může existovat více největších společných dělitelů, ale tyto dělitelé jsou poté ve stejné třídě ekvivalence, a tedy jsou vzájemně asociované.

Lemma 1.4.6.
Nechť R je obor integrity a $M \subseteq R$. Pak $d \in NSD(M) \rightarrow NSD(M) = [d]$.

Důkaz:
Dokažme si tedy nejdříve $[d] \subset NSD(M)$.
Mějme nějaký prvek $e \in [d]$.
Pro tento prvek z definice třídy ekvivalence platí, že $e \parallel d$.
To znamená, že $d \mid e$.
Z předpokladu víme, že $d \in NSD(M)$ a tedy d dělí každý prvek M.
Z lemmatu 1.2.6 víme, že relace dělení je transitivní.
Tedy pokud e dělí libovolný prvek z M, tak i d dělí každý prvek M.
Dále víme, že e dělí každý společný dělitel M a z transitivity opět dostaneme, že d dělí každý společný dělitel M.
Tím pádem d je největší společný dělitel.
Budeme dokazovat opačnou inkluzi $NSD(M) \subset [d]$.
Dokažme si, že každý největší společný dělitel je asociovaný s d.
Nechť tedy máme největšího společného dělitel e.
Z definice největšího společného dělitele tedy pro d máme $e \mid d$.
Zároveň i e je největší společný dělitel, tedy z definice dostáváme $d \mid e$.
A tedy $e \parallel d$.

□

Nyní si dokážeme, jak obecně vypadají všechny třídy na definovaném faktoroboru, ale zároveň tím, jak máme faktorobor definovaný, tak ukazujeme, jaký k sobě vztah mají asociované prvky.

Lemma 1.4.7.
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 $a = 0$, tak podle lemmatu 1.4.3 musí $b = 0$ také.
Protože podle lemmatu 1.1.2 víme, že platí pro všechna $x \in R$ $0 = 0 * x$.
R je obor integrity a tedy $1 \in R$.
Proto určitě platí i $0 = 0 * 1$.
Máme invertibilní prvek z R.
Mějme tedy $a \neq 0$.
Dosazením $b = ae$ do $a = bf$ dostaneme $a = aef$.

Jelikož jsme v oboru integrity a $a \neq 0$, můžeme krátit a dostaneme $1 = ef$.
Tím jsme dokázali, že e,$f \in R^*$.
Mějme $a = bf$, kde $f \in R^*$.
Z definice dělení dostaneme $b \mid a$.
Z definice invertibilního prvku dostaneme, že existuje g takové, že $1 = fg$.
Pokud s tímto g vynásobíme, rovnici $a = bf$, dostaneme $ag = bfg$.
Víme ale, že $fg = 1$, máme tedy $b = ag$ a tedy $a \mid b$.

□

Nyní si dokažme, že podmínka být ireducibilním prvkem plyne z podmínky být prvočinitelem. Mohlo by se zdát, že opačná implikace by mohla platit v také libovolném okruhu integrity, ale to není pravda. Vezměme si Gausova čísla $\mathbb{Z}[i\sqrt{7}]$ a ireducibilní prvek 2 rozhodně platí, že $2 \mid 8$, ale současně, $(1+\sqrt{7})*(1-\sqrt{7}) = 8$, ale 2 nedělí $1+\sqrt{7}$ ani $1-\sqrt{7}$. Dokázali jsme, že existují obory integrity, ve kterých opačná implikace neplatí. To znamená, že v nich existují ireducibilní prvky, které nejsou prvočiniteli. My si v následující kapitole ukážeme, že pokud máme obory integrity, kde zaručíme existenci největšího společného dělitele, tak už v nich opačná implikace platit musí.

Lemma 1.4.8.
Nechť R je obor integrity a mějme libovolné $p \in R$. Pak když p je prvočinitel, tak je ireducibilním prvkem

Důkaz:
Budeme postupovat obměnou, nechť tedy p není ireducibilní.
Pokud $p = 0$, tak p podle definice není prvočinitel.
Pokud $p \in R^*$, tak p podle definice není prvočinitel.
Nechť tedy $p \in R - R^*$ a $p \neq 0$ a mějme libovolné $x \in R$ takové, že x je vlastní dělitel p.
Tedy máme $e \in R$ takové, že $p = xe$ Podle definice vlastního dělitele víme, že $p \nmid x$.
Tedy podle lemmatu 1.4.7 je $e \in R - R^*$.
Určitě tedy platí, že $p \mid xe$.
Ale kdyby platilo $p \mid x$, tak existuje $f \in R$ takové, že $x = pf$.
Dosadíme za p a dostaneme $x = xef$.
Jsme v oboru integrity a musí platit, že $x \neq 0$, protože jinak by muselo být $x = 0$ a to je v rozporu s předpokladem.
Dostaneme tedy $1 = ef$, Z toho, ale plyne, že $e \in -R^*$, což je spor, protože jsme dokázali, že $e \in R - R^*$.
Předpokládejme, že platí $p \mid e$.
Z toho plyne, že $e = ph$. Do této rovnice dosadíme za p.
Dostaneme tedy $e = exh$.
Z předpokladu ale plyne, že $e \neq 0$, protože jinak by bylo $p = 0$.
Jsme v oboru integrity a tedy můžeme krátit.
Dostaneme tedy $1 = xh$.
Tedy $x \in R^*$, což je ve sporu s definicí vlastního dělitele.

□

Dokázali jsme tedy, že každý prvočinitel je ireducibilním prvkem. Už dříve jsme o relaci dělitelnosti dokázali, že je kvaziuspořádáním, protože může obsahovat cykly, což jsou vzájemně asociované prvky, ale přesně tyto prvky jsme na faktoroboru odstranili, proto si nyní budeme moci dokázat, že na faktoroboru existuje uspořádání.

1.5 Uspořádání faktoroboru

Pojďme se nyní podívat, jaký vzájemný vztah třídy ekvivalence na faktorové množině mají. Definujme si tento vztah na naší faktorové množině, budeme jej značit $\preceq$. Tato relace rozšiřuje relaci dělení z kvaziuspořádání na uspořádání. Dokážeme si poté, jak vypadají extrémy tohoto uspořádání a že jimi jsou třída invertibilních prvků a třída kde je neutrální prvek. Dále si ukážeme, jaký vztah při naší definici uspořádání mají vlastní dělitelé a že pokud z faktoroboru odstraníme třídu invertibilních prvků, tak jeho minimálním prvkem je ireducibilní prvek.

Definice 1.5.1 (Uspořádání faktoroboru)**.**
Mějme obor integrity R a $[R]$ je jeho faktorobor. Pak pro všechny a,$b \in R$. $[a] \preceq [b] \leftrightarrow a \mid b$

Nyní když jsme si definovali uspořádání na faktoroboru. Dokažme si, že relace $\preceq$ je opravdu relací uspořádání na množině $[R]$.

Lemma 1.5.2.
Mějme obor integrity R. Pak relace $\preceq$ na množině $[R]$ je relací uspořádání.

Důkaz:
V lemmatu 1.2.6 jsme si dokázali, že $a \mid a$.
Podle definice uspořádání $\preceq$ dostaneme $[a] \preceq [a]$.
Relace $\preceq$ je tedy reflexivní.
Budeme postupovat důkazem transitivity.
Mějme $[a] \preceq [b]$ a $[b] \leq [c]$.
Z definice tedy $a \mid b$, a $b \mid c$.
Jak jsme si dokázali v lemmatu 1.2.6, tak relace dělitelnosti je tranzitivní.
Dostáváme tedy $a \mid c$.
To ale podle definice $\preceq$ znamená, že $[a] \preceq [c]$.
Relace $\preceq$ je tedy na R tranzitivní.
Dokažme si nakonec slabou antisymetrii.
Z předpokladu máme $a \preceq b$ a $b \preceq a$.
To z definice uspořádání znamená, že $a \mid b$ a $b \mid a$.
Podle definice asociování, ale to tedy znamená, že $b \parallel a$.
Tím pádme platí $[a] = [b]$.
Relace je tedy slabě antisymetrická.
Dokázali jsme tedy, že relace je uspořádáním.

□

Vzhledem k tomu, že relace $\preceq$ je slabě antisymetrická, tak pokud $a \preceq b$ a $b \preceq a$ pak $[a] = [b]$, abychom takové prvky od sebe v uspořádání odlišily, budeme používat $a \prec b$, 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 1.5.3.
Mějme obor integrity R a nějaké $a \in R - R^*$ tak, že $a \neq 0$. Pak $[1] \prec [a] \prec [0]$.

Důkaz:
Mějme libovolné nenulové $a \in R - R^*$.
Z lemmat 1.1.11,1.2.5 a definice uspořádání dostaneme $[1] \preceq [a]$.
Ale $a \preceq [1]$ platit nemůže.
Jinak by to podle definice uspořádání znamenalo, že a dělí nějaký invertibilní prvek.
Z lemmatu 1.2.5 víme, že invertibilní prvek dělí, jen invertibilní prvek.
To je spor s předpokladem, že a není invertibilní.
Máme tedy $[1] \prec [a]$.
Z lemmatu 1.1.8 a definice uspořádání dostaneme, že $[a] \leq [0]$, pokud by platilo $[0] \leq [a]$, tak pak jsou $a \parallel 0$ a podle lemma 1.4.3 by to znamenalo, že $a = 0$, což je spor s předpokladem, máme tedy $[a] \prec [0]$.

□

Dokažme si jaký vzájemný vztah vzhledem k uspořádání spolu mají prvek a jeho vlastní dělitel a že opravdu tedy uspořádání rozšiřuje dělitelnost.

Lemma 1.5.4.
Mějme obor integrity R a $[R]$ je faktorobor. Pak prvek $b \in R$ je vlastním dělitelem prvku $a \in R$, právě když v $[R]$ platí $[1] \prec [b] \prec [a]$.

Důkaz:
Pokud b je vlastním dělitelem, tak nemůže být invertibilním prvkem a ani nulou.
Podle lemmatu 1.5.3 dostáváme $[1] \prec [b]$.
Z definice vlastního dělitele víme, že $b \mid a$.
To znamená, že $[b] \preceq [a]$.
Kdyby platilo $[a] \preceq [b]$, tak by to znamenalo, že $b \parallel a$.
To však platit nemůže, protože podle definice vlastního dělitele prvky a,b nejsou asociované.
Proto platí $[b] \prec [a]$.
Dokažme si opačnou implikaci.
Z $[1] < [b]$ víme, že $b \notin R^*$.
Z $[b] < [a]$ víme, že $b \mid a$ a neplatí $b \parallel a$.
Dokázali jsme tedy, že je to vlastní dělitel.

□

Máme tedy relaci uspořádanou opravdu podle dělitelnosti a víme, že invertibilní prvky jsou minimální vůči naší relaci uspořádání. Pokud budeme zkoumat uspořádání dále, zjistíme, že pokud máme množinu, kde nejsou invertibilní prvky, tak minimální prvek na této množině je ireducibilní prvek, pokud se zde vyskytuje.

Lemma 1.5.5.
Mějme obor integrity R, jeho faktorobor $[R]$ a nějaké $p \in R - R^*$ tak, že $p \neq 0$. Pak p je ireducibilní, právě tehdy když $[p]$ je minimálním prvkem množiny $[R] - [1]$.

Důkaz:
Uvažujme, že p je ireducibilní a že $[p]$ není minimální.
To znamená, že existuje nějaké $[c]$ pro $c \in R$ takové, že $[c] \prec [p]$.
To podle lemmatu 1.5.4 znamená, že c je vlastní dělitel p.
Tím pádem p není ireducibilní.
Uvažujme, že p není ireducibilní.
Z předpokladu víme, že není nula a není invertibilní.
Pokud není ireducibilní, tak musí mít vlastního dělitele $q \in R$.
To podle lemmatu 1.5.4 znamená, že $[1] \prec [q] \prec [p]$.
Tím pádem, ale $[p]$ není minimálním prvkem podmnožiny $[R] - [1]$.

□

Dokázali jsme tedy, jak vypadá uspořádání na faktoroboru. Už máme tedy dokázanou spousty obecný vlastnost o oborech integrity proto si v další kapitole. Popíšeme takzvané podmínky dělitelnosti a ukážeme jejich vzájemný vztah.

2. Podmínky Dělitelnosti

2.1 Vztahy oboru integrity

V předchozí kapitole jsme zkoumali dělitelnost v oborech integrity. Nyní budeme k oboru integrity přidávat další vlastnosti a budeme zkoumat vzájemný vztah těchto vlastností. První podmínkou je existence největšího společného dělitele pro libovolnou konečnou množinu. Druhá podmínka byla už dříve zmíněna, a je jí tvrzení, že každý ireducibilní prvek je prvočinitelem. Ukážeme si, že pokud máme zaručeného největšího společného dělitele, proto podmínka, že každý ireducibilní prvek je prvočinitel, také platí. Z této podmínky dále plyne, že pokud máme nějaké dva asociované součiny, potom jejich prvky rozkladu jsou vzájemně asociované. Čtvrtá podmínka mluví o tom, že relace $\preceq$ je na $[R]$ fundovaná. Z této podmínky plyne, že pak 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 už všechny ostatní podmínky. To je přesně takový obor, kde platí zobecněná forma Základní věty aritmetiky, která říká, že každý prvek má jednoznačný rozklad až na asociativitu prvků. Standardní věta z přirozených čísel je přirozeným důsledkem, protože nemá asociativní prvky. Pro celá čísla to znamená, že v rozkladu mohou být i záporná čísla.

Dokážeme si nyní distributivitu největšího společného dělitele vůči násobení, což znamená, že pokud je nějaký prvek největším společným dělitelem nějaké množiny, tak pokud vynásobíme prvky této množiny nějakým prvkem, jejich největší společný dělitel je součin tohoto prvku a původního největšího společného dělitele. Pro toto lemma však budeme muset předpokládat, že existence největšího společného dělitele je zaručena. Uvažujeme $\mathbb{Z}[\sqrt{3}]$ a $1-\sqrt{-3}$ a 2. Pro tyto prvky je největším společným dělitelem jen jednička. Pokud tyto prvky vynásobíme $1+\sqrt{-3}$, dostaneme $2*(1-\sqrt{-3})$ a $(1+\sqrt{-3})*(1-\sqrt{-3})=4$. Oba tyto prvky mají společné dělitele $2{,}1-\sqrt{-3}$, ale ty se vzájemně nedělí. Proto neexistuje největší společný dělitel. Ukažme si, že pokud předpokládáme existenci největšího společného dělitele, tak můžeme dokázat distributivitu největšího společného dělitele vůči násobení.

Lemma 2.1.1.
Mějme obor integrity R, $A=\{a_1,a_2,..,a_n\}$ tak, 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:
Protože podle lemmatu 1.1.2 platí pro libovolné $b\in R$, že $b*0=0$.
Podle lemmatu 1.2.3 jen nula dělí nulu, takže $0\in NSD(\{0,..,0\})$.
Mějme $r\neq 0$.
Z předpokladu víme, že $d\mid a_i$ pro všechny $i\leq n$.
To znamená $a_i=de_i$ pro nějaké $e_i\in R$.
To je ekvivalentní s tím, že $ra_i=(rd)e_i$.
To znamená, 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 $h \in R$.
Vynásobíme nenulovým r a 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 1.4.6 znamená, že i rd musí být největší společný dělitel.

□

Definice 2.1.2 (Podmínka D)**.**
Mějme obor integrity R. Pak každá konečná množina prvků z R má v R aspoň jednoho největšího společného dělitele.

V předchozích kapitole jsme dokázali, 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 opačné implikace.

Definice 2.1.3 (Podmínka P)**.**
Mějme obor integrity R. Pak každý ireducibilní prvek okruhu R je prvočinitel.

Další podmínka definuje takové obory integrity, kde, pokud spolu asociují součiny, tak spolu musí asociovat i ireducibilní prvky, ze kterých se součiny skládají. Dokonce takových prvků je vždy stejně.

Definice 2.1.4 (Podmínka J)**.**
Mějme obor integrity R a dvě přirozená čísla m,n m-tici p_1,p_2,..,p_m a n-tici q_1,q_2,..,q_m ireducibilních prvků z R takové, že p_1,p_2,..,$p_m \parallel q_1$,q_2,..,q_m, potom $m = n$ a existuje permutace π taková, že $p_i \parallel q_{\pi(i)}$ pro $i \leq n$

Další podmínka vybírá takové obory integrity, u kterých má v jejich faktoroboru podle asociování každá podmnožina nějaký minimální prvek vůči naší relaci uspořádání.

Definice 2.1.5 (Podmínka K)**.**
Mějme obor integrity R. Pak 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 2.1.6 (Podmínka I)**.**
Mějme obor integrity R. Pak každý neinvertibilní prvek z R, který není nula, je součinem ireducibilních prvků z R.

Nyní jsme dokázali, 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 2.1.7 (DP)**.**
Mějme obor integrity R . Pak 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 bez újmy na obecnosti největším společným dělitelem p a a je 1.
Podle lemmatu 2.1.1 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.
□

Obory integrity, kde každá konečná množina má největšího společného dělitele, už mají každý ireducibilní prvek jako prvočinitele. Dokážeme si, že pokud v oboru integrity každý ireducibilní prvek je prvočinitel, tak rozklady spolu už asociují, neboli 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 2.1.8 (PJ)**.**
Nechť R je obor integrity. Pak podmínka J plyne z podmínky P.

Důkaz:
Nechť R splňuje P a nechť p_1,..,p_n,q_1,..,q_m jsou ireducibilní prvky, pro které 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 1.3.2 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 teď na tyto skutečnosti použijeme lemma 1.4.7, 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, proto $p_1 \neq 0$.
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 2.1.9 (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 1.5.3 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 $A \subset [R]$.
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 1.5.5 znamená, že p je ireducibilní prvek.
Z definice A víme, že platí $[p] \preceq [a]$, což znamená, že $p \mid a$.

□

Nyní si už konečně můžeme dokázat vztah podmínky K a I. To znamená, že fundovanost relace na faktoroboru oboru integrity implikuje pro tento obor integrity existenci ireducibilního rozkladu pro libovolné neinvertibilní nenulové číslo.

Věta 2.1.10 (KI)**.**
Nechť $\mathbb{R}$ je obor integrity. Pak podmínka I plyne z podmínky K.

Důkaz:
Nechť R splňuje K a nesplňuje I. Definujme množinu

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

Neplatí podmínka I, tak M je neprázdná.
Vezměme nějaké $a \in M$, dokažme si, že platí $[a] \subset M$.
Pro každý prvek $b \in [a]$ platí, že $b \parallel a$.
Z definice M víme, že $b \neq 0$.
Protože podle lemmatu 1.4.3 není a ve třídě s 0.

Z $b \parallel a$ víme, že b i a jsou ve stejné třídě, proto b nemůže být ve stejné třídě jako 0 a tím pádem podle lemmatu 1.4.3 dostáváme $b \neq 0$.
Víme, že $b \in R - R^*$, protože z lemmatu 1.4.4 víme, že invertibilní prvky jsou spolu ve stejné třídě.
Z $b \parallel a$ víme, že b a a jsou ve stejné třídě a a není invertibilní.
Uvažujme b součin nějakých ireducibilních prvků p_1,..,p_n.
Z $b \parallel a$ dostaneme $b = ae$ pro nějaké $e \in R^*$.
Dokázali jsme, že $ae = p_1..p_n$.
Jelikož e je invertibilní, proto existuje k němu inverzní prvek $f \in R$. Tím, pokud rovnici vynásobíme, tak dostaneme $aef = p_1..p_nf$, což znamená, že $a = p_1..p_nf$.
Použijeme asociativní zákon a dostaneme $a = p_1..p_{n-1}(p_nf)$.
Označme $p_nf = q$ pro nějaké $q \in R$.
Podle lemmatu 1.4.7 ale musí být q ireducibilní prvek,
protože podle lemmatu 1.4.5 jsou ve stejné třídě buď všechny prvky ireducibilní anebo žádný prvek není ireducibilní.
Dále víme, že prvek q je podle lemmatu 1.4.7 ve stejné třídě jako p_n, které ireducibilní je.
Dostaneme $a = p_1..p_{n-1}q$, kde a je součin ireducibilní prvků a to je spor s předpokladem.
Dokázali jsme, že $[a] \subset M$.
Vezměme $A = \{[a] \in [R]; a \in M\}$.
Z definice je jasné, že $A \subset [R]$.
Podle podmínky K tu je nějaký minimální prvek $[m]$ množiny A.
Jelikož $m \in M$, tak $m \in R - R^*$ není nula ani ireducibilní.
Podle lemmatu 2.1.9 dostaneme $m = pc$, kde c,$p \in R$ a p je ireducibilní prvek.
Určitě platí $c \neq 0$, jinak by podle lemmatu 1.1.4 muselo být i $m = 0$.
Také $c \in R - R^*$, protože kdyby c bylo invertibilní prvek, tak podle lemmatu 1.4.7 je c ve stejné třídě jako m.
To je spor, protože podle lemmatu 1.4.4 je $c \in R^*$ a $m \in R - R^*$.
Také c nemůže být součinem ireducibilních prvků, jinak by i m bylo součinem ireducibilních prvků, protože m je součin c s ireducibilním prvkem.
Z toho ale dostáváme, že nutně musí být $c \in M$.
Víme, že $c \nparallel m$, $c \in R - R^*$ a $c \mid m$, proto c je vlastní dělitel prvku m.
Podle lemmatu 1.5.4 víme, že platí $[c] \prec [m]$.
Víme, že $[c] \in A$, což je spor s tím, že $[m]$ je minimální.
Dokázali jsme, že podmínka I platí.

□

2.2 Gaussův obor

Jak jsme si ukázali, tak obory integrity, které splňují podmínku I, už splňují i podmínku K. Také jsme dokázali, že obory integrity, které splňují podmínku D, už nutně splňují podmínku P a ty obory integrity, které splňují podmínku P, už nutně splňují podmínku J. Podmínky K a J jsou v těchto hierarchiích nejslabší z naších podmínek. Dokážeme, že tyto podmínky jsou společně dostačující a pokud platí současně, tak platí už libovolná z podmínek. Nejdříve si proto nadefinujme takzvaný Gaussův obor, což je obor splňující podmínky I a J.

Definice 2.2.1 (Gaussův obor)**.**
Nechť R je obor integrity a splňuje podmínky I a J. Pak jej nazýváme Gaussův obor.

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

Lemma 2.2.2 (Kanonické vyjádření)**.**
Mějme Gaussův obor R. Pak každý nenulový prvek $a \in R - R^*$ má vyjádření tvaru $a = ep_1^{k_1}..ep_n^{k_n}$, kde $p_1,..,p_n \in R$ jsou vzájemně neasociované ireducibilní prvky a $e \in R^*$ a $n,k_1,..,k_n$ jsou přirozená čísla.

Důkaz:
Podle podmínky I máme $a = q_1..q_m$.
Pokud prvky jsou vzájemně neasociované, tak lemma platí.
Nechť 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 všechny $j \leq n$.
Můžeme je teď zapisovat 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 $d \leq m - n$.
Postupujme nyní indukcí podle d.
Pokud $d = 1$, tak $a = q_1^{l_1}..{q_n}^{l_n}{q_{n+1}}^{l_{n+1}}$ a při vhodném očíslování $q_1 \parallel q_{n+1}$.
Pro nějaké $f_1 \in R^*$ musí platit $q_{n+1} = q_1 f_1$ podle lemmatu 1.4.7.
Můžeme používat komutativnost a asociativnost a díky tomu dostaneme $q_{n+1}^{l_{n+1}} = q_1^{l_{n+1}} f_j^{l_{n+1}}$.
Dosadíme v původním zápisu a dostaneme $a = f^{l_{n+1}} q_1^{k_1} q_n^{k_n}$. Kde $r_1 = l_1 + l_{n+1}$ a $k_i = l_i$ pro $1 < i \leq n$.
R je uzavřené na násobení, $e = f^{l_{n+1}}$ pro nějaké $e \in R^*$
. Dostali jsme $a = eq_1^{r_1}..q_n^{r_n}$.
Máme už dokázáno pro k a chceme dokázat tvrzení pro $k + 1$.
Máme nějaké $a = eq_1^{r_1}..q_k^{r_k} q_{k+1}^{r_{k+1}}$, ale tam je důkaz zcela obdobný, jako jsme dokazovali v prvním kroku.

□

Dokázali jsme, že každé nenulové neinvertibilní číslo lze rozložit pomocí ireducibilních čísel. Dokažme si nyní, 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 si vezmeme přirozená čísla, tam invertibilním prvkem je jen 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 můžou lišit ve znaménku a invertibilní prvek bude buď 1 nebo -1.

Lemma 2.2.3 (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 $p_1,..,p_m \in R$ je $q_i \parallel p_i$ 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 z $q_1..q_n$.
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.
Kdyby byl asociován i s jiným prvkem q_j, tak by z transitivity asociování platilo $q_j \parallel q_i$, což je spor s lemmatem 2.2.2.
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 dokázali, 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. Dokažme si nyní, jaký vztah mají kanonická vyjádření dvou čísel, kde jedno dělí druhé.

Lemma 2.2.4 (Kanonického vyjádření při dělení)**.**
Mějme Gaussův obor R. Mějme nenulové a,$b \in R - R^*$, takže $q_1^{l_1}..q_n^{l_n} = a$ $b = p_1^{k_1}..p_m^{k_m}$ jsou dvě kanonická vyjádření. Potom $b \mid a$ právě, když $m \leq n$ a při vhodném očíslování prvků p_1,..,$p_m \in R$ je $q_i \parallel p_i$ a $k_i \leq l_i$ pro $i \leq n$.

Důkaz:
Když $b \mid a$, tak $a = bc$ pro vhodné $c \in R$.
Kdyby bylo $c = 0$, tak by bylo $a = 0$ a to je spor s předpokladem.
Je-li $c \in R^*$, pak podle lemmatu 1.4.7 je $a \parallel b$.
Podle lemmatu 2.2.3 pro $c \in R^*$ lemma platí.
Nechť $c \in R - R^*$, takže $c \neq 0$.
Potom pro $c \in R$ existuje podle lemmatu 2.2.2 vyjádření ve tvaru $c = hg_1^{j_1}..g_o^{j_o}$ pro $1 \leq o \leq n - m$.
Dostáváme součin $bc = hg_1^{j_1}..g_o^{j_o}p_1^{k_1}..p_m^{k_m}$.
Z toho dostáváme $q_1^{l_1}..q_n^{l_n} = hg_1^{j_1}..g_o^{j_o}p_1^{k_1}..p_m^{k_m}$.
Podle lemmatu 2.2.3 dostáváme $n = o + m$.
Jelikož $1 \leq o$, dostáváme $m \leq n$.
Z lemmatu 2.2.3 vidíme, že každé q_i pro $i \leq n$ může být vyjádřeno třemi způsoby:

1. q_i je jen 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 jen některé z g_j pro $i \leq o$.
   Při vhodném očíslování $o_i = l_i$ pro $q_i \parallel g_i$, ale tím pádem $k_i = 0$, proto $k_i < l_i$.

3. Nechť q_i má vyjádření mezi oběma čísly při vhodném očíslování.
   Podle lemmatu 2.2.3 dostaneme, že platí $l_i = k_i + o_i$.
   Jelikož q_i má vyjádření mezi p_i i g_i, tak 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 1.4.7 platí, že $q_i = e_i g_i$ pro $e_i \in R^*$.
Zasubstituujeme do 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 $a = p_1^{l_1} .. p_m^{l_m} .. q_n^{l_n} y$, proto platí $b \mid a$.

□

Dokázali jsme, jak vypadá vztah dvou kanonických vyjádření dvou prvků, kde jeden dělí druhý. Ukažme si nyní, jak vypadá kanonické vyjádření společného dělitele nějaké množiny.

Lemma 2.2.5 (Kanonického vyjádření společného dělitele)**.**
Mějme Gaussův obor R a nějaké nenulové $a,b \in R - R^*$ 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 taková, že $0 \leq i \leq r \leq min(m,n)$ a ostatní prvky společně neasociují. Pak prvek $t \in R$ je společným dělitelem 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 nějaké $t \in R$.
Pokud $t \mid b$ a $t \mid a$, tak podle lemmatu 2.2.4 dostaneme, že $fp_1^{k_1} .. p_m^{k_m} = tx$ a $eq_1^{l_1} .. q_n^{l_n} = ty$ pro $x,y \in R$.
Máme nějaké r takové, že pro všechny $d \leq r$ víme, že $p_d = q_d z_d$ pro nějaká $z_d \in R^*$.
Substituci 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 2.2.3 vidíme, že a,b mají společné prvky rozkladu $p_1 .. p_r$, proto $t = hp_1^{v_1} .. p_r^{v_r}$, 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 $q_i = w_i p_i$.
Uděláme substituci a dostaneme $a = w_1^{l_1} p_1^{l_1} .. w_r^{l_r} p_r^{l_r} .. q_n^{l_n}$.
Z komutativnosti dostaneme $a = p_1^{l_1} .. p_r^{l_r} .. q_n^{l_n} w_1^{l_1} ... w_r^{l_r}$.
Proto t je společným dělitelem.

□

Známe nyní vztah kanonických vyjádření prvků a jejich společných dělitelů. Ukažme, které z kanonických vyjádření společných dělitelů odpovídá tomu největšímu společnému děliteli.

Lemma 2.2.6 (Kanonického vyjádření největšího společného dělitele)**.**
Mějme Gaussův obor R a nějaké nenulové $a,b \in R - R^*$ takové, že $a = eq_1^{l_1} .. q_n^{l_n}$ a $b = fp_1^{k_1} .. p_m^{k_m}$ a nechť očíslování je takové, že $q_i \parallel p_i$ pro nějaké r, že pro všechna i taková, že $0 \leq i \leq r \leq min(m,n)$ a ostatní prvky společně nejsou asociovány. Pak prvek $0 \neq t \in R$ je největším společným dělitelem a,b právě tehdy, když $t = hp_1^{v_1} .. p_r^{v_r}$, kde $h \in R^*$ a $v_i = u_i$ pro $u_i = min(k_i,l_i)$ pro všechna $i \leq r$.

Důkaz:
Vzhledem k lemmatu 2.2.5 víme, že všechny dělitelé lze zapsat ve tvaru $t = hp_1^{v_1} .. h_r^{v_r}$, kde $h \in R^*$ a $0 \leq v_i \leq u_i$ pro $u_i = min(k_i,l_i)$.

Největší společný dělitel je takový dělitel, kterého dělí ostatní společní dělitelé.
Pokud $v_i < u_i$, tak pak $p_1^{u_1}$ nedělí $p_1^{v_1}$.
Proto největší společný dělitel je ve tvaru $t = hp_1^{u_1}..h_r^{u_r}$.

□

Jak jsme si ukázali v lemmatu 2.2.3, tak součin mocnitelů je stejný pro každý prvek nezávisle na jeho kanonickém vyjádření. Dokázali jsme si také, že dokážeme vyjádřit v Gaussově oboru největšího společného dělitele dvou prvků. V lemmatu 1.2.10 jsme si dokázali, že podmínku D můžeme dokázat jen pro dvouprvkovou množinu, a proto Gaussův obor už nutně splňuje podmínku D, že každá konečná množina má aspoň jednoho největšího společného dělitele.

Věta 2.2.7 (I+J=D)**.**
Mějme Gaussův obor R. Pak v něm platí podmínka D.

Důkaz:
Mějme Gaussův obor R, pak podle lemmatu 2.2.6 můžeme v Gaussově oboru najít největšího společného dělitele pro dvouprvkovou množinu.
Podle lemmatu 1.2.10 to znamená, že existuje i největší společný dělitel pro libovolnou konečnou množinu, a proto podmínka D platí.

□

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

Věta 2.2.8 (I+J=P)**.**
Mějme Gaussův obor R. Pak v něm platí podmínka P.

Důkaz:
Mějme Gaussův obor R.
Pak podle věty I+J=D dostaneme, že zde musí platit D.
To podle věty DP znamená, že tu musí platit i P.

□

Ukazuje se zatím, že všechny tyto podmínky platí v Gaussově oboru. Ukažme si nakonec, že zde platí i podmínka K. Nejdříve si dokažme, kolik vzájemně neasociovaných vlastních dělitelů čísla v Gaussově oboru mají.

Lemma 2.2.9 (Počet vlastních dělitelů)**.**
Mějme Gaussův obor R. Pak počet vzájemně neasociovaných vlastních dělitelů pro číslo $a = ep_1^{u_1}..p_n^{u_n}$ je roven $\prod_{i=1}^{n}(u_i + 1) - 2$.

Důkaz:
Dokazujeme indukcí podle n.
Nechť $n = 1$, potom platí, že $a = ep_1^{u_1}$.
e je invertibilní, tudíž nemůže být vlastním dělitelem.
Víme, že $p_1^0 = 1$, proto $0 < v_i$.
Zároveň podle lemmatu 1.4.7 $p_1^{u_1}$ je asociován s a a proto není vlastní dělitel, proto platí, že $v_i < u_i$.

Z definice v_i musí být přirozené číslo.
Mezi $0 < v_i < u_i$ je přesně $u_i - 1$.
Mějme tedy dokázáno, že pro $n = m$ $\prod_{i=1}^{m}(u_i + 1) - 2$ platí.
Chceme dokázat indukční krok pro $n = m + 1$.
Z předpokladu $\prod_{i=1}^{m}(u_i + 1) - 2$ je jich takové, které to splňují pro délku $n = m$.
Chceme se tedy vyvarovat takovému vyjádření, kde všechny indexy jsou nula, a nebo jsou maximální.
Ty už ale nejsou obsaženy ani v indukčním kroku.
Tedy máme $u_{n+1}+1$, jak je vytvořit ze všech vlastních dělitelů pro indukční krok.
Z toho nám pro $n = m + 1$ vznikne $(\prod_{i=1}^{m}(u_i + 1) - 2)(u_{m+1} + 1)$.
Pak nás ale zajímají případy, kdy pro všechny indexy $i \leq n$ platí $v_i = 0$.
To můžeme u_{m+1} možnostmi rozšířit na $m + 1$ prvků.
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 máme počet vlastních dělitelů $(\prod_{i=1}^{m}(u_i + 1) - 2)(u_{m+1} + 1) + u_{m+1} + u_{m+1}$,
což po upravení je $(\prod_{i=1}^{m+1}(u_i + 1) - 2)$ - což jsme chtěli dokázat.

□

Dokázali jsme, kolik vlastních společných dělitelů má libovolný nenulový neinvertibilní prvek. Pro nás podstatné je zejména to, že takové číslo je konečné.

Věta 2.2.10 (I+J=K)**.**
Mějme Gaussův obor R. Pak v něm platí všechny podmínky K.

Důkaz:
Zbývá tedy dokázat, že v Gaussově oboru platí K.
Mějme tedy nějakou podmnožinu $[R]$.
Pokud $a \in R^*$, tak podle lemmatu 1.4.4 je a minimální prvek naší podmnožiny.
Mějme libovolné nenulové $a \in R - R^*$.
Předpokládejme $A \subset [R] - [1]$ tedy neobsahuje $[1]$.
Nechť tedy a je ireducibilní, podle lemmatu 1.5.5 je $[a]$ minimální na A.
Tedy nechť a není ireducibilní, pak podle J existuje rozklad $a = ex_1^{k_1}..x_m^{k_m}$.
Vezměme průnik $A \cap D$, kde D je množina vlastních dělitelů a.
Pokud $A \cap D = \emptyset$, tak a je minimální prvek.
Podle lemmatu 2.2.9 je $A \bigcap D$ je vždy konečná.
Tedy v ní vždy najdeme minimální prvek.
Tento prvek bude i minimální v množině A.
Tedy relace $\preceq$ je na $[R]$ fundovaná.

□

Pojďme si to nyní všechno shrnout a dokázat, že Gaussův obor splňuje všech pět podmínek.

Věta 2.2.11 (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. Ideály

3.1 Úvod do ideálů

Další vlastnosti, které zkoumáme na celých číslech, jsou Bezoutova věta, Čínská zbytková věta a poté způsob, jak najít největší společný dělitel, respektive, jak vůbec dělit efektivně. Tím postupem je Euklidův algoritmus. Ukážeme si, že Čínskou zbytkovou větu sice můžeme zevšeobecnit pro libovolný obor integrity, ale obecně v těchto oborech 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. Pro tuto část práce použijeme tedy odlišenou teorii dělitelnosti pomocí ideálů. Ideály hrají v teorii okruhů významnou roli. Nejdříve se seznámíme se samotnými ideály a jejich vlastnostmi.

Definujeme si ideál jako podmnožinu okruhu, která je uzavřená na sčítání a obsahuje s každým prvkem i všechny jeho násobky z okruhu. Budeme říkat, že A je ideál R a budeme značit $A \trianglelefteq R$. Tedy například ideálem celých čísel mohou být násobky nějakého čísla.

Definice 3.1.1 (Ideál)**.**
Nechť R je obor integrity a $I \subset R$. Pak $I \trianglelefteq R$, pokud platí:

1. *Uzavřenost sčítání:*

$$(\forall a,b \in I)\,(a + b \in I).$$

2. *Uzavření na násobky z R:*

$$(\forall a \in I)\,(\forall r \in R)\,(ra \in I).$$

Lemma 3.1.2.
Nechť I je ideál nad oborem integrity R. Pak I je okruh.

Důkaz:
Z toho, že $I \trianglelefteq R$, víme $I \subset R$.
Tedy jediné, co nám stačí dokázat, jsou existence opačného prvku a existence nulového prvku.
Protože I je ideál a je uzavřen na násobení libovolným prvkem $x \in R$ a R je obor integrity, tak obsahuje opačný prvek k jednotkovému prvku, takže pro libovolné $y \in I$ máme $-y \in I$.
Jelikož R je obor integrity, tak obsahuje neutrální prvek.
Takže $0 \in I$, protože pro libovolný prvek podle lemmatu 1.1.2 platí, že výsledek násobení bude neutrální prvek.

□

Dokažme si nyní, že každý ideál je uzavřen i na rozdíl prvků.

Lemma 3.1.3.
Mějme obor integrity R a $A \trianglelefteq R$. Pak $(\forall a,b \in I)(a - b \in I)$.

Důkaz:
Uvažujme, že máme nějaké a,$b \in I$.
R je obor integrity takže, $1 \in R$.
Obor integrity je uzavřený na opačné prvky, takže $-1 \in R$.
Ideál je uzavřený na násobení prvky z R, takže nutně musí platit $-b \in I$.
Zároveň ideál je uzavřen na sčítání.
Tím pádem dostáváme $a - b \in I$.

□

S ideály rozhodně budeme chtít provádět nějaké operace, proto nejdříve definujme, jak mezi sebou budeme ideály násobit a sčítat.

Definice 3.1.4.
Nechť R je obor integrity a I,$J \trianglelefteq R$ definujme:

1. *Sčítání:*

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

2. *Násobení:*

$$IJ = \sum_{k=1}^{n} i_k j_k; n \in \mathbb{N}, i_k \in I, j_k \in J.$$

Dokažme si nyní vlastnosti těchto operací. Dokažme si, že součet i součin ideálů jsou opět ideály a že pokud k ideálu přičteme jiný ideál, tak původní ideál je tohoto ideálu podmnožinou. Naopak součin dvou ideálů je vždy podmnožinou obou ideálů ze součinu. Začneme nejdříve důkazem, že $I \subset I + J$.

Lemma 3.1.5.
Nechť R je oborem integrity R a I,$J \trianglelefteq R$. Pak $I \subset I + J$.

Důkaz:
Mějme nějaké $x \in I$.
Podle definice ideálu je $0 \in J$.
Z definice součtu ideálů dostáváme $x + 0 = x$.
Tedy x $I + J$.

□

Nyní si dokážeme, že součin je naopak vždy podmnožinou ideálů v součinu.

Lemma 3.1.6.
Nechť R je oborem integrity R a I,$J \trianglelefteq R$. Pak $IJ \subset I$.

Důkaz:
Fixujeme nějaké $k \in \mathbb{N}$ a máme i_1,..,$i_k \in I$,j_1,..,$j_k \in J$.
Jelikož $J \subset R$ a ideál je uzavřený na násobení prvkem z R dostáváme $i_1 j_1$,..,$i_k j_k \in I$.
Ale I je ideál, takže je uzavřen i na sčítání a tedy $i_1 j_1 + .. + i_k j_k \in I$.

□

Jelikož na oborech integrity je násobení i sčítání komutativní, tak lemmata samozřejmě fungují i pro druhý ideál v operaci. Tím pádem musí platit i pro jejich průnik, což si nyní dokážeme.

Lemma 3.1.7 (Uspořádání produktu a průniku)**.**
Nechť R je oborem integrity R a I,$J \trianglelefteq R$. Pak $IJ \subset I \cap J$.

Důkaz:
Mějme nějaké $x \in IJ$.
Podle lemmatu 3.1.6 platí $x \in I$ a $x \in J$.
Pak ale musí platit $x \in I \cap J$

□

Pro sčítání je komutativita na ideálech lehce nahlédnutelná hned z definice. Komutativitu součinu ideálu si dokážeme.

Lemma 3.1.8.
Nechť R je oborem integrity R a I,$J \trianglelefteq R$, pak $IJ = JI$.

Důkaz:
Mějme nějaké $k \in \mathbb{N}$,$i \in I$,$j \in J$. Pak máme $i_1j_1 + .. + i_kj_k \in IJ$.
Určitě platí i_1j_1,...,$i_kj_k \in R$.
Obor integrity R je komutativní, takže pro každé $l \leq k$ platí $i_1j_1 = j_1i_1$.
Dostáváme tedy $i_1j_1 + .. + i_kj_k = j_1i_1 + .. + j_ki_k$, což je prvek JI.
Tím pádem ale $i_1j_1 + .. + i_kj_k \in JI$.
Důkaz opačné inkluze je stejný.

□

Nyní o součinu i o součtu ideálů dokážeme, že jsou také ideály. Začneme důkazem pro součet.

Lemma 3.1.9.
Nechť R je obor integrity a I,$J \trianglelefteq R$. Pak $I + J \trianglelefteq R$.

Důkaz:
Z definice ideálu platí, že $I \subset R$.
V lemmatu 3.1.5 jsme dokázali, že $IJ \subset I$.
Z transitivity podmnožiny dostaneme $IJ \subset R$.
Dokažme si, že IJ je uzavřené na sčítání.
Mějme nějaké $i_1 + j_1$,$i_2 + j_2 \in I + J$.
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 $(j_1 + j_2) = j_3$.
Pak ale z definice $I + J$ musí platit, že $i_3 + j_3 \in I + J$.
Mějme nějaké $r(i + j)$ 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 ale nutně musí být $ri + rj \in I + J$.

□

Dokázali jsme, že množina všech součtu prvků ze dvou ideálů je také ideálem. Dokažme si to nyní i o součinu

Lemma 3.1.10.
Nechť R je obor integrity a I,$J \trianglelefteq R$. Pak $IJ \trianglelefteq R$.

Důkaz:
Podle lemmatu 3.1.6 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 nějaké prvky z,$y \in IJ$ a chceme dokázat, že $z + y \in IJ$.
Fixujme tedy k,$l \in \mathbb{N}$, takže $z = \sum_{i=1}^{k} a_i b_i$ a $y = \sum_{j=1}^{l} a_i b_i$.
Sčítání je asociatívní, takže $\sum_{i=1}^{k} a_i b_i + \sum_{i=1}^{h} a_i b_i = \sum_{i=1}^{k+h} a_i b_i$.
Podle definice součinu takový prvek je také v IJ.
Mějme nějaké $r \in R$ a $z \in IJ$ takové, že $z = \sum_{i=1}^{k} a_i b_i$.
Z distributivity prvků R plyne, že $rz = \sum_{i=1}^{k} r a_i b_i$.
Každý $ra_i = c_i$ pro nějaké $c_i \in A$, protože A je ideál.
Dostaneme tedy $rz = \sum_{i=1}^{k} c_i b_i$.
Ale pak musí být $rz \in AB$.

□

Dokažme si nyní, že pokud ideály v součtu jsou stejné, tak pak jejich součet se rovná ideálu samotnému.

Lemma 3.1.11.
Nechť R je obor integrity a $I \trianglelefteq R$, pak $I = I + I$.

Důkaz:
Uvažujme, že máme, $a \in I$.
Protože $O \in I$, tak pak musí být $a \in I + I$.
Tedy jsme dokázali $I \subset I + I$.
Mějme nyní nějaké $a + b \in I + I$.
Z definice tedy a,$b \in I$.
Z předpokladu $I \trianglelefteq R$, takže je uzavřen na sčítání a $a + b \in I$

□

Lemma 3.1.12.
Nechť R je obor integrity a I,J,$K \trianglelefteq R$. Pak $I(J + K) = IJ + IK$.

Důkaz:
Vezměme nějaký prvek $x \in I(J + K)$ a nějaké $a \in \mathbb{N}$, $i_a \in I$, $j_a \in J$ a $k_a \in K$ pro všechny.
Pak $x = \sum_{i=1}^{a} i_a(j_a + k_a)$.

Použitím distributivního zákona na každý součin v součtu dostaneme $x = \sum_{i=1}^{a} i_a j_a + i_a k_a$).
U prvků změníme uzávorkování, a tedy určitě $x = \sum_{i=1}^{a}(i_a j_a) + \sum_{i=1}^{a}(i_a k_a)$.
To ale z definice součtu a součinu ideálu znamená, že $x \in IJ + IK$).
Mějme nyní nějaké $x \in IJ + IK$.
Z definice součtu a součinu ideálu znamená, že $x = \sum_{i=1}^{a}(i_a j_a) + \sum_{i=1}^{a}(i_a k_a)$.
Prvky můžeme přezávorkovat a tedy určitě $x = \sum_{i=1}^{a} i_a j_a + i_a k_a$).
Na každý tento prvek použijeme distributivní zákon a dostaneme $x = \sum_{i=1}^{a} i_a(j_a + k_a)$.
To ale pak znamená, že $x \in I(J + K)$.

□

Dokažme si, že průnik ideálů je také ideálem.

Lemma 3.1.13.
Mějme obor integrity R a neprázdnou množinu S tak, že pro každé $s \in S$ je dán $I_s \trianglelefteq R$. Pak $\bigcap_{s\in S} I_s \trianglelefteq R$.

Důkaz:
Pro každé $s \in S$, platí z definice ideálu $I_s \subset R$.
Tedy určitě $\bigcap_{s\in S} I_s \subset R$.
Uvažujme, že máme a,$b \in \bigcap_{s\in S} I_s$.
Kdyby $a + b \notin \bigcap_{s\in S} I_s$.
Pak musí existovat nějaké s, že $a + b \notin I_s$.
To by znamenalo, že I_s není R, protože podle předpokladu a,$b \in I_s$.
Uvažujme, že máme $a \in \bigcap_{s\in S} I_s$ a $r \in R$. Kdyby $ra \notin \bigcap_{s\in S} I_s$, pak musí existovat nějaké t, že $ra \notin I_t$.
To by znamenalo, že I_s není R, protože podle předpokladu $a \in I_s$.

□

Díky tomuto důkazu, že průnik ideálů je také ideálem, dostáváme zároveň způsob, jak můžeme definovat ideál generovaný nějakou podmnožinou.

Definice 3.1.14 (Generovaný ideál)**.**
Nechť R je obor integrity a mějme $M \subset R$, definujme $(M) = \bigcap\{S; M \subset S \wedge S \trianglelefteq R\}$.

Dokažme si, jak vypadají tyto ideály.

Lemma 3.1.15.
Mějme obor integrity R a neprázdnou množinu $M = \{a_1,..,a_n\}$. Pak $(M) = \{r_1a_1 + .. + ..r_na_n; r_1,..,r_n \in R\}$.

Důkaz:
Nejdříve dokažme, že $\{r_1a_1 + .. + ..r_na_n; r_1,..,r_n \in R\} \subset (M)$.
Mějme nějaké $r_1a_1 + .. + ..r_na_n$.
Podle definice každé $s \in \{S; M \subset S \wedge S \trianglelefteq R\}$ obsahuje $r_1a_1 + .. + ..r_na_n$.
Protože každé s obsahuje $a_1,..,a_n$.
Z předpokladu zároveň je $s \trianglelefteq R$, takže musí být uzavřené na násobení prvkem z

R.
Tedy každé s obsahuje r_1a_1,...,$r_na_n \in s$.
Ideál je zároveň uzavřen na sčítání svých prvků, tedy $r_1a_1 + ... + r_na_n \in s$.
Ale tím pádem musí platit $r_1a_1 + ... + r_na_n \in (M)$.
Mějme danou $M \subset R$ a mějme nějaký prvek $d \notin \{r_1a_1 + .. + ..r_na_n; r_1,..,r_n \in R\}$.
Pak existuje S takové, že $M \subset S$, $S \trianglelefteq R$ a $d \notin S$.
Potom tedy $d \notin (M)$.

□

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

Definice 3.1.16 (Hlavní ideál)**.**
Nechť R je obor integrity a mějme $a \in R$. Pak ideál $(a) = ra; r \in R$ nazýváme hlavní ideál oboru integrity R generovaný prvkem a.

Dokažme si, že součet hlavních ideálů se rovná ideálu generovaného jeho sjednocením.

Lemma 3.1.17.
Mějme obor integrity R a dva prvky a,$b \in R$ takové, že (a) a (b) jsou hlavní ideály. Pak $(a$,$b) = (a) + (b)$.

Důkaz:
Podle lemmatu 3.1.15 $(a$,$b) = \{r_1a_1 + r_2b; r_1$,$r_2 \in R\}$.
Podle definice hlavního ideálu je $(a) = ra; r \in R$ a $(b) = sb; s \in R$.
Podle definice součet ideálů je $(a) + (b) = \{ra + sb; r$,$s \in R\}$, což je tedy uplně to samé.

□

Lemma 3.1.18.
Mějme obor integrity R a dva libovolné prvky a,$b \in R$ takové, že (a) a (b) jsou hlavní ideály. Pak platí $(a) \subset (a) + (b)$.

Důkaz:

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

□

Samozřejmě předchozí důkaz platí i pro druhý prvek součtu. Ukažme si nyní jaký vztah mají hlavní ideály vzhledem k dělení abychom na nich mohli zavést právě teorii dělitelnosti.

Lemma 3.1.19.
Mějme obor integrity R a dva prvky a,$b \in R$ kde (a) a (b) jsou hlavní ideály. Pak $a \mid b \leftrightarrow b \in (a) \leftrightarrow (b) \subset (a)$.

Důkaz:
Podle definice hlavního ideálu je $(a) = ra; r \in R$.
Pokud $b \in (a)$, tak pak $b = ra$ pro nějaké $r \in R$.
To je ale stejné jako definice dělení, jak jsme ji definovali v první kapitole.
Dokažme tedy další ekvivalenci.
Mějme nějaké $q \in (b)$ a podle definice je $q = tb$ pro $t \in R$.
Pokud $b \in (a)$, tak existuje $g \in R$ tak, že $b = ga$.
Dosadíme za b a dostaneme $q = gra$ pro g,$t \in R$.
Obor integrity R je uzavřený na násobení a tedy $tr = p$ pro nějaké $p \in R$.
To znamená, že máme $q = pa$ pro nějaké $p \in R$ a tedy $q \in (a)$.
Předpokládejme že $b \notin (a)$.
V oboru integrit R musí platit $1 \in R$ a tedy $b \in (b)$.
Pak ale $(b) \not\subset (a)$.

□

Definujme si Bezoutův obor, což je obor, kde součet hlavní ideálů je zase hlavní ideál. Nejdříve si, ale definujme obor NSD, což je právě takový obor, ve kterém pro každou konečnou množinu existuje největší společný dělitel. Ukážeme následně, že Bezoutův obor je jeho speciálním případem.

Definice 3.1.20 (NSD obor)**.**
Nechť R je obor integrity. obor je NSD oborem právě tehdy, pokud splňuje podmínku D.

Definice 3.1.21 (Bezoutův obor)**.**
Nechť R je obor integrity a jeho libovolné dva prvky a,$b \in R$ takové, že (a) a (b) jsou hlavní ideály. Pak říkáme, že obor je Bezoutův obor, pokud platí $(a)+(b) = (d)$ a (d) je hlavní ideál.

Ukažme si nyní dvě vlastnosti Bezoutova oboru. Těmi vlastními jsou, že v něm platí zobecněná Bezoutova věta a že libovolný Bezoutův obor je NSD oborem.

Věta 3.1.22 (Bezoutova rovnost)**.**
Mějme obor integrity R, obor je Bezoutův právě tehdy, když splňuje Bezoutovu 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 $t \in R$ existuje r,$s \in R$ takové, že $ra + sb = td$.
Ale R je obor integrity, takže obsahuje i jednotkový prvek.
Tedy dostaneme, že existuje q,$p \in R$ takové, že $qa + pb = d$.
Dokažme, že platí, že $d = NSD(a,b)$.
Podle lemmatu 3.1.18 víme, že $(a) \subset (a) + (b)$ a $(b) \subset (a) + (b)$.
Z definice Bezoutova oboru dostaneme $(a) \subset (d)$ a $(b) \subset (d)$.
To podle lemmatu 3.1.19 znamená, že dostaneme, že $d \mid a$ a $d \mid b$.
Tím pádem d je společný dělitel a,b.
Mějme nějaké $c \mid a$ a $c \mid b$ a podle lemmatu 3.1.19 platí $(a) \subset (c)$ a $b \subset (c)$.
To znamená, že libovolný prvek z $x \in (a)$ lze zapsat ve tvaru $x = yc$ pro nějaké

$y \in R$.
Zároveň také, že libovolný prvek z $z \in (b)$ lze zapsat ve tvaru $z = wc$ pro nějaké $w \in R$.
Tím pádem prvky $(a) + (b)$, lze zapisovat jako $yc + wc$ pro nějaké y,$w \in R$.
Podle lemmatu 3.1.9 $(a) + (b) \trianglelefteq R$.
Tedy na něj lze aplikovat distributivní zákon.
Dostaneme $yc + wc = (y + w)c$.
Jsme oboru integrity, takže $y + w = v$ pro nějaké v a tedy$yc + wc = vc$.
Z předpokladu (c) je hlavní ideál a tedy obsahuje všechny násobky c.
Tím pádem i vc, tedy dostáváme $(a) + (b) \subset (c)$.
Z definice Bezuotova oboru, ale víme že $(a) + (b) = (d)$.
Tedy z transitivity podmnožiny máme $(d) \subset (c)$.
To podle lemmatu 3.1.19 znamená $c \mid d$.
Tím jsme dokázali, že d je tedy největší společný dělitel.
Naopak mějme (a) a (b)a 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 $(a) + (b) \subset (d)$.
Mějme $x \in (a) + (b)$ a d je společný dělitel a i b.
Musí tedy platit $a = de$ a $b = df$.
Tedy x lze zapsat jako $x = red + sfd$.
Podle lemmatu 3.1.9 $(a) + (b) \trianglelefteq R$.
Tedy na něj lze aplikovat distributivní zákon.
Můžeme tedy psát $x = d(re+sf)$. Obor integrity je uzavřený na sčítání a násobení a tedy máme $h \in R$ takové, že platí $h = re + sf$. Dosadíme do x a dostaneme $x = dh$.
Tím pádem $x \in (d)$.
Mějme tedy nějaké $z \in (d)$.
Všechny prvky v (d) jsou tvaru $z = rd$ pro nějaké $r \in R$.
Podle Bezoutovy věty máme tedy, že libovolný prvek vypadá $z = r(ax + by)$.
Podle distributivního zákona platí $z = (rx)a + (ry)b$.
Určitě r,x,$y \in R$ a tedy existuji prvky o,$p \in R$ tak že $o = rx$ a $p = ry$.
Máme tedy $z = oa + pb$, ale to znamená, že $z \in (a) + (b)$.

□

Dokažme si důsledek tohoto tvrzen jako větu. Jelikož v Bezoutově oboru platí Bezoutova věta, tak určitě pro každé dva prvky existuje největší společný dělitel.

Věta 3.1.23 (Bezout a NSD)**.**
Mějme obor integrity R, pokud je obor Bezoutův, tak potom už je NSD.

Důkaz:
Podle věty Bezoutova rovnost víme, jak pro každé dva prvky najít největší společný dělitel a tedy pro libovolnou dvojici největší společný dělitel nutně existuje.

□

Víme tedy, že jak Bezoutovy tak Gaussovy obory jsou obory NSD, protože jsme dokázali, že v nich plat podmínka D. otázkou je jestli existují tedy obory

které jsou jen Bezoutovy nebo které jsou jen Gaussovy, protože pokud takové obory existují, tak jsou vzájemnými protipříklady. Pokud vezmeme obor polynomů dvou promněných nad celými čísly, ten je Gaussovým oborem, ale pro nesoudělná x,y máme, že $NSD(x,y) = 1$ a v celých číslech neexistují inverzní prvky, tedy nemůže najít dva takové prvky, jejichž lineární kombinace bude jedna. Naopak, pokud veme množinu všech řešení nad těmito polynomy, tak to je potom Bezout protože libovolné číslo dokážeme vyjádřit jako lineární kombinaci nějakých dvou prvků naopak relace vlastní dělitel nebude fundovaná, protože každý prvek a lze vydělit $a^{\frac{1}{2}}$. Tyto dva protipříklady jsou zároveň protipříklady, že ne všechny Bezoutovy respektive Gaussovy obory jsou obory hlavních ideálů, které si za chvíli nadefinujeme.

3.2 Obor hlavních ideálů

Ukázali jsme si tedy protipříklady, že ne každý Gaussův obor je Bezoutův a ne každý Bezoutův obor je oborem Gaussovým. Nadefinujme obor hlavních ideálů, o kterém si dokážeme, že je to právě takový obor, který je Gaussův a zároveň je Bezoutův. Dokážeme si dále, že speciálním oborem hlavních ideálů je Euklidův obor, což je obor, kde se zastaví Euklidův algoritmus. Definujme si nejdříve pojem obor hlavních ideálů.

Definice 3.2.1 (Obor hlavních ideálů)**.**
Nechť R je obor integrity a pokud jsou všechny ideály hlavní. Pak říkáme že obor je Obor 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 normy, které analogicky odpovídají normám nad vektorovým prostorem.

Definice 3.2.2 (Dediken-Hasse norma)**.**
Nechť R je obor integrity a funkci $f : R - \{0\} \longrightarrow \mathbb{N}$ nazýváme Dediken-Hasse norma, pokud pro libovolná nenulová a,$b \in R$ splňuje jednu z 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 na oboru integrity existuje Dediken-Hasse norma, tak pak obor integrity, už je oborem hlavních ideálů.

Lemma 3.2.3.
Mějme obor integrity R, pokud je obor splňuje Dediken-Hasse normu, tak potom už je oborem hlavních ideálů.

Důkaz:
Nechť $I = \{0\}$, pak $b = 0$ a $I = (b)$.

Tedy nechť $I \neq \{0\}$, z existence Dediken-Hessovi normy, která je do přirozených čísel, a proto lze dobře uspořádat víme, že existuje $b \in I - \{0\}$ takové, že $\forall r \in I - \{0\} f(b) \leq f(r)$.
Vezmeme libovolné $a \in I$.
Když $a = 0$, tak určitě $a \in (b)$.
Kdyby existovalo nějaké $r \in (a,b)$, které splňuje druhou podmínku Dediken-Hesse normy.
Tak je to spor s výběrem našeho b.
Takže pro všechny musí platit $a \in (b)$ a tedy $I \subset (b)$.
Naopak $b \in I$, to ale podle lemmatu 3.1.19 platí $(b) \subset I$.
Tedy jsme dokázali, že $I = (b)$.

□

Definujme si nyní další normu a tou je ostře multiplikativní norma a dokažme, že rozklad v Gaussově oboru je takovou normou.

Definice 3.2.4 (Ostře multiplikativní monotónní norma)**.**
Nechť R je obor integrity a funkci $f : R - \{0\} \longrightarrow \mathbb{N}$ nazýváme ostře multiplikativní monotónní norma, pokud pro libovolná nenulová $a,b \in R$ splňuje:

1. *Monotónnost násobení:*

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

2. *Ostrost normy:*

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

Lemma 3.2.5.
Mějme Gaussův obor R. Pak délka rozkladu prvku je ostře monotónní multiplikativní norma.

Důkaz:
Definujme $f : R - \{0\} \longrightarrow \mathbb{N}$ takovou, že $f(u) = 0$, pokud $u \in R$ je invertibilní.
Podle lemmatu 2.2.3 $f(up_1^{k_1}..p_n^{k_n}) = k_1 + .. + k_n$ je hodnot a funkce pro každý prvek jednoznačná.
Dokažme, že platí podmínky pro ostře multiplikativní normu.
Mějme tedy dva nenulové prvky $a,b \in R$ označme $l(a),l(b)$ jejích délky.
Bez újmy na obecnosti předpokládejme, že $l(a) \leq l(b)$.
Evidentně platí $l(ab) = l(a) + l(b)$.
Jelikož $l(a)$ je přirozené číslo, rozhodně bude platit $l(ab) \geq l(b)$.
Rovnost $l(ab) = l(b)$, ale platí jen když a je invertibilní prvek.
To podle lemmatu 1.4.7 znamená, že $ab \parallel b$.

□

Ukažme si nyní, že ostře monotónní multiplikativní norma na Bezoutově oboru je Dediken-Hesse norma.

Lemma 3.2.6.
Mějme Bezoutův obor R. Pak ostře monotónní multiplikativní norma je Dediken-Hesse norma.

Důkaz:
Mějme ostře monotónní multiplikativní normu f a dva nenulové prvky a,$b \in R$.
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 $d \mid b$.
Kdyby platilo $b \mid d$, tak z transitivity dostaneme $b \mid a$.
Nechť tedy $b \nmid d$ a tedy $b \nparallel d$.
Podle lemmatu 1.4.7 $b = dc$ pro nějaké neinvertibilní $c \in R$.
Určitě tedy platí $f(d) < f(b)$.

□

Věta 3.2.7 (Gaussův-Bezoutův obor a obor hlavních ideálů)**.**
Mějme obor integrity R, který je Gaussův a Bezoutův zároveň, poté už oborem hlavních ideálů.

Důkaz:
Podle lemmatu 3.2.5 máme ostře monotónní multiplikativní normu.
Podle předpokladu zároveň jsme v Bezoutově oboru.
To podle lemmatu 3.2.6 znamená, že to je také Dediken-Hesse norma.
Ale to podle lemmatu 3.2.3, znamená, že R je oborem hlavních ideálů

□

Dokázali jsme, že pokud máme obor, který je Gaussův a zároveň Bezoutův, tak už je oborem hlavních ideálů. Ukažme si, že ještě že každý obor hlavních ideálů je Gaussův i Bezoutův. Na konci minulé podsekce jsme si ukázali, že existují Bezoutovy obory, které nejsou Gaussovy. To pak budou protipříklady pro Bezoutovy obory, který nejsou obory hlavních ideálů. Obory, které jsou Gaussovy ale nejsou Bezoutovy, jsou pak protipříkladem pro Gaussovy obory, který nejsou obory hlavních ideálů. Dokažme nyní že obor hlavních ideálů je vždycky Bezoutův obor.

Věta 3.2.8 (Obor hlavních ideálů a Bezoutův obor)**.**
Mějme obor integrity R, který je Oborem hlavních ideálů. Pak je Bezoutův.

Důkaz:
Z definice součtu ideálů víme, že $(a) + (b) = (a,b)$.
Z předpokladu R je oborem hlavních ideálů.
Tedy existuje $d \in R$ takže $(d) = (a,b)$.
Dostáváme tedy $(a) + (b) = (d)$.
Tím pádem R je Bezoutův obor.

□

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

Věta 3.2.9 (Obor hlavních ideálů a Gaussův obor)**.**
Mějme obor integrity R, který je Oborem hlavních ideálů. Pak je Gaussův.

Důkaz:
Z věty Obor hlavních ideálů a Bezoutův obor víme, že Obor hlavních ideálů je Bezoutův, což nutně znamená že v něm platí podmínka D.
Tedy podle věty DP, zde platí podmínka P.
Což podle věty PJ, znamená že tu platí J podmínka.
Gaussův obor jsme definovali jako obor integrity, ve kterém platí podmínky I a J.
Budeme tedy dokazovat, že platí podmínka I.
To podle věty KI, znamená, že můžeme dokázat, že zde platí podmínka K.
Předpokládejme, že tedy neplatí a relace $\preceq$ není fundovaná na $[R]$.
Tedy existuje nekonečná posloupnost prvků z R taková že $a_{i+1} \mid a_i$.
Podle lemmatu 3.1.19 to znamená, že $(a_i) \subset (a_{i+1})$.
Definujme $I = \bigcup_{i=1}^{\infty} (a_i)$.
Dokážeme si nyní, že v $I \subset R$.
Uvažujeme nějaký prvek $x \in I$.
Z definice I víme, že musí existovat $k \in \mathbb{N}$ takové, že $x \in (a_k)$.
Víme ale, že $(a_k) \trianglelefteq R$, takže určitě platí $(a_k) \subset R$.
Z transitivity podmnožiny dostáváme tedy $I \subset R$.
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 $y \in (a_j)$.
Vezměme tedy větší z i,j, takže bez újmy na obecnosti $i < j$.
Pak ale musí platit $x \in (a_j)$ a $y \in (a_j)$, protože platí $(a_i) \subset (a_{i+1})$ a podmnožinyjsou transitivní.
Pak ale musí platit $x + y \in (a_j)$, protože $(a_j) \trianglelefteq R$.
Z definice I dostáváme, že $x + y \in I$.
Pak ale musí platit $rx \in (a_j)$, protože $(a_j) \trianglelefteq R$.
Z definice I dostáváme, že $rx \in I$.
Tedy $I \trianglelefteq R$.
Jsme ale v oboru hlavních ideálů a tedy existuje $x \in R$, takové že $I = (x)$.
V oboru integrity R existuješ jednotkový prvek, tedy musí platit $x \in I$.
Podle definice I tedy existuje k, takové že $x \in (a_k)$.
Podle lemmatu 3.1.19 platí $(a) \subset (a_k)$.
Z předpokladem, že $I = (a)$ dostaneme $I \subset a_k$.
Z definice I ale víme, že $(a_k) \subset I$.
Dostáváme tedy $I = (a_k)$ pro nějaké k.
Pak podle předpokladu máme $(a_k) \subset (a_{k+1})$.
Mějme nějaké $x \in (a_{k+1}) - (a_k)$. Pak z definice I musí platit $x \in I$, ale to je spor, protože jsme dokázali, že $I = (a_k)$.
Takže musí platit podmínka K.

□

Definujme Euklidovu normu, u které ukážeme, že je nutně Dediken-Hasse norma a díky které můžeme definovat Euklidův obor, o kterém můžeme dokázat že v něm funguje Euklidův algoritmus.

Definice 3.2.10 (Euklidova norma)**.**
Nechť R je obor integrity a funkci $f : R - \{0\} \longrightarrow \mathbb{N}$ nazýváme ostře Euklidovská norma, pokud splňuje pro libovolné nenulové a,$b \in R : b \mid a \vee (a = bc + r \wedge d(r) <$

$d(b)$).

Definujme si nyní pomocí Euklidovy normy Euklidův obor jako obor, ve kterém Euklidova norma existuje.

Definice 3.2.11 (Euklidův obor)**.**
Nechť R je obor integrity a existuje na něm Euklidova norma. Pak obor nazveme Euklidův obor.

Věta 3.2.12 (Euklidův obor a algoritmus)**.**
Nechť R je Euklidův obor. Pak právě v něm lze použít Euklidův algoritmus.

Důkaz:
Euklidův algoritmus zní:
Mějme dáne dva prvky, uložená v proměnných u a w.
Dokud $w = 0$ opakuj:
$r =$ `u mod w`
$u = w$
$w = r$
Po konci algoritmu, v u je uložen největší společný dělitel původních čísel. Z definice Euklidovy normy vidíme, že existuje ostře klesající řetězec funkční hodnot našich zbytků při provádění algoritmu.
Jelikož je to funkce do přirozených čísel, tak posloupnost musí být konečná, protože bude mít maximálně $f(u)$ kroků.
Naopak pokud takové posloupnost neexistuje, tak se Euklidův algoritmus nezastaví.

□

Dokažme si nyní, že Euklidův obor je oborem hlavních ideálů, opačně to však platit nemusí a existují obory hlavních ideálů, které nejsou Euklidovké. Například $\mathbb{Z}[\frac{1+\sqrt{-19}}{2}]$ je obor, který není Euklidův viz. článek An example of a PID which is not a Euclidean domai od R. A. Wilson.

Věta 3.2.13 (Euklidův obor a obor hlavních ideálů)**.**
Každý Euklidův obor je oborem hlavních ideálů.

Důkaz:
Podle lemmatu 3.2.3 stačí dokázat, že každá Euklidova norma je Dediken-Hasse norma.
Mějme tedy nějakou Euklidovnu normu f.
Tedy musíme dokázat, že existuje prvek $d \in (a,b)$, že $f(d) \neq f(b)$.
My víme z Euklidovy normy, že máme $f(r) < f(b)$ takové, že $a = bc + r$.
Tedy nyní stačí dokázat, že $r \in (a,b)$.
Z $a = bc + r$ dostaneme $r = a - bc$.
Jelikož ideál uzavřen na násobení prvkem z R, tak i $bc \in (a,b)$.
Ideál je podle lemmatu 3.1.3 je ideál uzavřen na rozdíly a tedy $a - bc \in (a,b)$.
Takže je to opravdu Dediken-Hasse norma.

□

Máme tedy dokázáno, že každý Euklidův obor je oborem hlavní ideálů. Dokázali jsme tedy, že máme hierarchii oborů Gaussovy obory, Bezoutovy obory $\subset$ NSD obory $\subset$ obory integrity $\subset$ okruh. Dále víme že platí Euklidův obor $\subset$ Obor hlavních ideálů = Bezout obor + Gaussův obor

3.3 Faktorokruh

V lemmatu 3.1.3 jsme dokázali, že každý ideál je uzavřen i na rozdíly. Proto si definujeme rozdíl jako ekvivalenci na množině. Na základě této ekvivalence definujeme faktorokruh podobně jako první kapitole. Tento faktorokruh ale je jen okruhem tudíž nemusí obsahovat jednotkový prvek.

Definujme si jak vypadá součet ideálů

Definice 3.3.1 (Relace modulo)**.**
Nechť R je obor integrity a I a je ideál R, definujme : $a \sim b \leftrightarrow a - b \in I$

Dokažme si tedy o této relaci, že je to relace ekvivalence.

Lemma 3.3.2.
Nechť R je obor integrity a $I \trianglelefteq R$. Pak relace $\sim$ je relace ekvivalence.

Důkaz:
Dokažme nejdříve, že relace je reflexivní.
Podle definice $a \sim a$, znamená $a - a = 0$.
Z definice ideálu ale víme, že $0 \in R$.
Pak z lemmatu 1.1.4 plyne, že $0 \in I$.
Dokažme si, že relace je symetrická.
Víme že platí $a - b \in I$.
Z definice ideálu ale víme, že $b - a \in R$.
Jelikož $-1 \in R$ a ideál je uzavřený na násobení prvkem z oboru integrity.
Dokažme si nakonec, že relace je transitivní.
Víme, že platí $a - b \in I$ a $b - c \in I$.
Podle lemmatu 3.3.6 je rozdíl těchto prvků také prvkem ideálu. Takže nutně musí platit $a - c \in I$.
Dokázali jsme tedy, že $\sim$ je relace ekvivalence.

□

Máme tedy relaci ekvivalence přes nějaký ideál, tato relace odpovídá chování relace modulo. Definujme si třídy rozkladu $[a] = a + I = \{a + i | i \in I\}$. Sjednocením těchto dřív dostaneme faktorokruh. Množina tříd ekvivalence podlé ideálu I značíme $R \wr I$.

Definice 3.3.3 (Faktorokruh)**.**
Nechť R je obor integrity $I \trianglelefteq R$ a $R \wr I$. Na těchto třídách definujme operace a konstanty takto:

1. *Sčítání:*

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

2. Násobení:

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

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 v tom faktorokruhu vypadají různé třídy. Začneme tím, že dokážeme, jak vypadá nulová třída faktorokruhu a že jím je vlastně samotný ideál.

Lemma 3.3.4.
Nechť R je obor integrity a $I \trianglelefteq R$. Pak $0_{R\wr I} = I$.

Důkaz:
Libovolný prvek v $0_{R\wr I}$ je ve tvaru $0 + i$ pro $i \in I$.
Nula je neutrální prvek a tedy platí $0 + i = i$.
Tedy každý prvek z $0_{R\wr I}$ odpovídá nějakému prvku z I.

□

Dokažme si nyní, že faktorokruh je podmnožinou samotného oboru integrity.

Lemma 3.3.5.
Nechť R je obor integrity a $I \trianglelefteq R$. Pak $R \wr I \subset R$.

Důkaz:
Z definice faktorokruhu máme $R \wr I = \{a + I | a \in R\}$.
Z toho, že $I \trianglelefteq R$, tak víme, že $I \subset R$.
Obor integrity R je uzavřen na sčítání takže $a + I \in R$.
Dostáváme tedy $R \wr I \subset R$.

□

Dokažme si nyní, že faktorokruh je okruhem.

Lemma 3.3.6.
Nechť R je obor integrity a $I \trianglelefteq R$. Pak $R \wr I$ je okruh.

Důkaz:
Podle lemma 3.3.5 nám stačí ověřit jen existenci nulového prvku a existenci opačných prvků.
Mám nějaké $a + I \in R \wr I$.

Podle lemmatu 3.3.4 faktorokruhu je zde nula $0_{R\wr I} = I$.
Dokažme si, že pokud přičteme I k libovolnému prvku, tak dostaneme stejný prvek.
Mějme nějaké $a + I \in R \wr I$.
Pak $a + I + I = a + (I + I)$, ale z 3.1.11 víme, že $I + I = I$.
Takže dostáváme $a + I + I = a + I$ Nyní si dokažme, že pro každý prvek existuje jeho opačný prvek.
Mějme $a + I \in R \wr I$. Pak z definice okruhu víme, že pro libovolné $a \in R$ existuje $-a \in R$.
Z definice faktorokruhu, ale tedy platí $-(a + I) \in R \wr I$.
Ověříme ještě, že se opravdu jedná o opačný prvek.
Z definice faktorokruhu dostaneme $(a + I) - (a + I) = (a - a) + I = I$.
To podle lemmatu 3.3.4 znamená, že jsou opravdu vzájemně opačné.

□

Dokažme si nyní jak se se chovají do sebe zanořené ideály, a ukažme jak se chovají jejich faktorokruhy.

Lemma 3.3.7.
Nechť R je okruh a I,$J \trianglelefteq R$ pro které platí $I \subset J$. Pak $I \trianglelefteq J$

Důkaz:
Podle lemmatu 3.1.2 víme, že J je okruh.
I je uzavřené na sčítání, protože je samo ideálem v R.
Dokonce je uzavřeno na násobení, protože $J \subset R$.
Jelikož je $IJ \trianglelefteq R$ je dokonce uzavřena na násobení libovolným prvkem z R.

□

Lemma 3.3.8.
Nechť R je okruh a I,$J \trianglelefteq R$ pro které platí $I \subset J$. Pak $J \wr I \trianglelefteq R \wr I$.

Důkaz:
Podle lemmatu 3.1.2 víme, že $R \wr I$ je okruh.
Z definice faktorokruhu a $J \subset R$ jasně plyne $J \wr I \subset R \wr I$.
Dokažme že $J \wr I$ je uzavřené na sčítání.
Mějme nějaké $a + I, b + I \in J \wr I$.
Z definice těchto prvků dostaneme $a, b \in J$. Podle předpokladu $J \trianglelefteq R$ a tudíž $a + b \in J$.
Pak tedy ale podle definice faktorokruhu dostaneme $(a + b) + I \in J \wr I$.
Podle definice faktorokruhu platí $(a + b) + I = (a + I) + (b + I)$.
Dokažme ještě uzavřenost na násobení prvkem z okruhu.
Mějme libovolné $(r + I) \in R \wr I$ a $a + I \in J \wr I$.
Z toho, že $J \trianglelefteq R$, tak musí platit $J \subset R$.
Okruhy jsou uzavřený na násobení a $R \wr I$ je okruh podle lemmatu 3.1.2. Tím pádem $J \wr I$ je uzavřené na násobení prvkem z okruhu.

□

3.4 Okruhové homomorfismy

Definujme si nyní pojem okruhového homomorfismu. Okruhový homomorfismus je taková funkce, která mezi okruhy přenáší vlastnosti sčítání a násobení.

Definice 3.4.1 (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 zobrazení, což je množina prvků, které se zobrazí na nulu a poté si ještě nadefinujeme pojem obrazu, což jsou prvky na které se náš homomorfismus zobrazí. Dokažme si, že takové jádro je dokonce ideálem našeho vzoru.

Definice 3.4.2 (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:*

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

Lemma 3.4.3.
Nechť R a S jsou okruhy. Funkce $f : R \to S$ je okruhový homomorfismus. Pak $Ker(f) \trianglelefteq R$.

Důkaz:
Z definice funkce f plyne, že $Ker(f) \subset R$.
Dokažme, že jádro je opravdu ideál a tedy je uzavřené na sčítání a na násobení prvkem z R.
Mějme tedy nějaké 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 překladu 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 si tedy, že je ještě uzavřené na násobení prvek z okruhu.
Mějme tedy nějaké $r \in R$ a $a \in Kerf$.
Podle definice homomorfismu víme, že $f(ra) = f(r)f(a)$. Z předpokladu víme, že $a \in Ker(f)$.
Tím pádem $f(a)$ je nula.
Jsme v okruhu, tak podle lemmatu 1.1.4 je i $f(r)f(a) = 0$ pro libovolné $r \in R$.
Tím pádem i ra bude v jádru.

□

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

Věta 3.4.4 (O homomorfismu)**.**
Nechť R a S jsou okruhy a funkce $f : R \to S$ je okruhový homomorfismus a současně máme ideál $I \trianglelefteq R$ a platí pro něj $I \subset Ker(f)$, tak 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:
Ověřme nejdříve, že je to funkce. Uvažujme, že máme nějaké $a + I$,$b + I \in R \wr I$ pro které platí $a + I = b + I$.
To znamená, že máme $a + i = b + j$ pro nějaké i,$j \in I$.
Jelikož $I \trianglelefteq R$, tak je uzavřen na opačné prvky.
Dostaneme $a + i - i = b + j - i$, z čehož plyne, že $a = b + k$ pro nějaké $k \in I$.
Podle definice platí $h(a + I) = f(a)$ a podle našeho předpokladu dostáváme tedy $h(a + I) = f(b + k)$.
Z definice homomorfismu dostáváme tedy $h(a + I) = f(b) + f(k)$.
Z předpokladu platí $I \subset Ker(f)$ a tedy $k \in Ker(f)$. Pak ale platí, že $h(a + I) = f(b)$.
To podle definice znamená, že $h(a + I) = h(b + I)$.
Mějme $(a + I) + (b + I)$, podle definice víme, že $(a + I) + (b + I) = (a + b) + I$.
Potom musí platit $h((a + I) + (b + I)) = h((a + b) + I)$.
To podle definice funkce h znamená, že $h((a + I) + (b + I)) = f(a + b)$.
Z definice homomorfismu, dostaneme $h((a + I) + (b + I)) = f(a) + f(b)$.
Z definice funkce h dostaneme $h((a + I) + (b + I)) = h(a + I) + h(b + I)$.
Mějme $(a + I)(b + I)$, podle definice víme, že $(a + I)(b + I) = (ab) + I$.

Potom $h((a+I)(b+I)) = h(ab+I)$.
To podle definice funkce h znamená, že $h((a+I)(b+I)) = f(ab)$.
Z definice homomorfismu, dostaneme $h((a+I)+(b+I)) = f(a)f(b)$.
Tím pádem 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 dostaneme, že $a \in Ker(f) \leftrightarrow a+I \in Ker(h)$.
Tím pádem $Ker(f) \wr I = Ker(h)$.
Nakonec si dokažme, že obrazy jsou stejné.
Mějme nějaký prvek $x \in Img(f)$. Pak existuje nějaké $y \in R$ takové, že $x = f(y)$.
Bez újmy na obecnosti můžeme říct, že tento prvek má faktorovou třídu $[y]$ do které patří.
Tyto prvky jsou ve tvaru $y+I$, ale my víme že platí $y+I \in R \wr I$.
Můžeme tedy na něj použít funkci h a dostaneme $h(y+I) = f(y)$.
To je ale naše x, máme tedy $x \in Img(h)$. Mějme nějaké $v \in Img(h)$, podle definice tedy existuje nějaké $h(a+I) = v$.
Víme tedy že $a \in R$, podle definice $h(a+I) = f(a)$.
Máme tím pádem $v \in Imgf$.

□

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

Lemma 3.4.5.
Nechť R a S jsou okruhy a funkce $f : R \to S$ je okruhový homomorfismus. Pokud $f(a) = 0 \to a = 0$, pak f je injektivní.

Důkaz:
Mějme nějaké dvě od sebe různé a,$b \in R$.
Jsme v okruhu, a tedy máme i $a - b \in R$ pro které platí $a - b \neq 0$.
Z předpokladu tedy dostaneme $f(a-b) \neq O$.
Z definice homomorfismu tedy dostaneme $f(a) - f(b) \neq 0$.
Potom ale $f(a) \neq f(b)$ a funkce je tedy 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 3.4.6 (1. o izomorfismu)**.**
Nechť R a S jsou okruhy a funkce $f : R \to S$ je okruhový homomorfismus, pak $R \wr Kerf$ a $Imgf$ jsou isomorfní.

Důkaz:
Ve větě o homomorfismu vezměme $I = Ker(f)$.
Dostaneme $h : R \wr Ker(f) \to S$.
Současně $Img(f) = Img(h)$ a dostaneme tedy $h : R \wr Ker(f) \to Img(f)$. Tato

funkce z definice obrazu je na.
Dokážeme, že platí $h(a) = 0 \to a = 0$.
Podle lemmatu 3.4.5 je pak zobrazení surjektivní a je tedy izomorfismem.
Mějme tedy nějaké $a = b + Ker(f)$.
Pak nechť $h(a + Ker(f)) = 0$.
Z definice funkce dostaneme $f(a) = 0$ a víme tedy, že platí $a \in Ker(f)$.
Z toho plyne že $a + Ker(f) = Ker(f)$.
Podle lemmatu 3.3.4 faktorokruhu znamená, že $a + Ker(f) = [0]$.

□

Nyní si dokážeme druhý izomorfismus, který nám říká, že když máme dva ideály, kde jeden je druhému podmonožinu. Tak pokud vytvoříme faktorokruh, kde okruhem je faktorokruh z oboru integrity přes menší množinu a ideálem je faktorokruh z většího ideálu přes menší, tak je ekvivalentní s faktorokruhem z oboru integrity přes větší ideál.

Věta 3.4.7 (2. o izomorfismu)**.**
Nechť R je okruh,I,$J \trianglelefteq R$ takové, že $J \subset I$, 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 $f(a) = a + I$.
Dokažme si nejdříve, že tato funkce je na.
Protože pro každé $a + I$ v obrazu existuje ve vzoru prvek, který se na něj zobrazí.
Dokažme si nyní, že platí $Ker(f) = I$.
Nejdříve si dokažme inkluzi $I \subset Ker(f)$.
Mějme nějaké $x \in I$, z definice naší funkce dostaneme $x + I$.
Jelikož ale $I \trianglelefteq R$, tak je uzavřen na sčítání.
Tím pádem platí ale $x + I \in I$.
Podle lemmatu 3.3.4 znamená, ze 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.
Podle lemma 3.3.4 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 na tuto funkci použijeme větu 0 homomorfismu. Ověřme její předpoklady.
Máme, že $Ker(f) = I$, takže z předpokladu máme $J \subset Ker(f)$.
Podle lemmatu 3.3.8 je J ideál v R.
Takže máme 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 dostáváme a z toho, že je funkce na dostaneme $Img(f) = R \wr I$.
To ale znamená, že máme tedy $Img(h) = R \wr I$.
Dále z věty O homomorfismu dostáváme $Ker(h) = Ker(f) \wr J$.
To znamená, že $Ker(h) = I \wr J$.
Podle věty 1. o izomorfismu, víme že platí, že $(R \wr J) \wr Ker(h)$ je izomorfní s $Img(h)$.
Dosadíme a máme tedy, že $(R \wr J) \wr (I \wr J)$ je izomorfní s $R \wr I$.

□

3.5 Komaximalita ideálů

V lemmatu 3.1.7 jsme dokázali, že součinem je vždy podmnožinou průniku. V této kapitole si dokážeme, že pro speciální ideály platí i opačná inkluze a pak je součin právě průnik ideálu. Budeme si muset nejdříve tyto ideály nadefinovat, budeme jim říkat komaximální. Dále si ukážeme ještě definici nesoudělných ideálů, jejíž definice bude připomínat Bezoutovu větu. Následně si ukážeme ekvivalenci těchto definic. Poté si dokážeme opačnou inkluzi, že průnik je podmnožinou součinu, pokud jsou ideály komaximální tento důkaz rozšířen pro libovolný počet ideálů. Následně si ukážeme, vztah komaximálních ideálů vůči homomorfismům. Díky níž bude moc dokázat zobecněnou Čínskou zbytkovou větu pro libovolný obor integrity.

Budeme definovat komaximální ideály jako ideály, jejiž součet už dává celý obor integrity.

Definice 3.5.1 (Komaximalita)**.**
Nechť R je obor integrity 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 obdobná s Bezoutovou větou pro nesoudělná čísla-

Definice 3.5.2 (Nesoudělnost ideálů)**.**
Nechť R je obor integrity 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 3.5.3.
Nechť R je obor integrity a I,$J \trianglelefteq R$, definujme : Ideály I,J jsou vzájemně komaximální, právě tehdy když jsou nesoudělné.

Důkaz:
Mějme $i \in I$,$j \in J$ takové, že $i + j = 1$.
Evidentně platí $I + J \subset R$.
Mějme nějaký prvek $r \in R$, vynásobíme takovým prvkem rovnici a dostaneme $r(i + j) = r$.
Použijeme distributivitu a dostaneme $ri + rj = r$.
Jelikož I,$J \trianglelefteq R$ musí platí $ri \in I$ a $rj \in J$.
Pak ale máme, že $r \in I + J$. Dokažme si nyní opačnou implikaci.
V oboru integrity musí platit $1 \in R$.
Pak ale z předpisu $I + J = R$ víme že existují $i \in I$ a $j \in J$ takové, že $i + j = 1$.
□

Dokažme si tedy nyní, že pokud máme komaximální ideály, tak jejich součin se rovná jejich průniku.

Lemma 3.5.4.
Nechť R je obor integrity a I,$J \trianglelefteq R$ jsou komaximální, pak $I \cap J = IJ$

Důkaz:
Podle lemmatu 3.1.7 víme, že $IJ \subset I \cap J$.
Dokažme nyní, že $I \cap J \subset IJ$.
Dokažme si nyní nejdříve, že $I \cap J = (I \cap J)(I + J)$.
Mějme nějaké $r \in I \cap J$.
Podle lemmatu 3.1.13 je $I \cap J \trianglelefteq R$.
Z lemma 3.1.9 víme, že $I + J \trianglelefteq R$.
Nutně tedy musí platit, že $I + J \subset R$
Podle lemmatu 3.1.13 je $I \cap J \trianglelefteq R$, takže je uzavřen na násobení prvkem z oboru integrity.
Tím pádem musí platit $r(i + j) \in I \cap J$.
Máme dokázáno, že $I \cap J \subset (I \cap J)(I + J)$. Dokažme opačnou implikaci. Mějme nějaký prvek $m \in I \cap J$.
Podle předpokladu z lemmatu 3.5.3 víme ,že $1 \in I + J$.
Pak ale pro každý prvek platí $m \in (I \cap J)(I + J)$.
Z lemmatu 3.1.12 dostaneme $(I \cap J)(I + J) = (I \cap J)I + (I \cap J)J$.
Máme tedy dokázáno $(I \cap J) = (I \cap J)I + (I \cap J)J$.
Dokažme si nyní, že $(I \cap J)I + (I \cap J)J \subset JI + IJ$. Dokažme si nejdříve, že platí $(I \cap J)I \subset JI$. Každý prvek v $(I \cap J)$ musí být z definice průniku v J.
Potom ale musí platit $(I \cap J)I \subset JI$.
Máme tedy dokázáno, že $I \cap J \subset IJ + JI$.
Kombinací lemmat 3.1.8 a 3.1.11 dostáváme $IJ + JI = IJ$.
Takže dostáváme $I \cap J \subset IJ$.

□

Rozšiřme si předchozí lemma pro libovolný počet prvků.

Lemma 3.5.5.
Nechť R je obor integrity a I_1,..,$I_n \trianglelefteq R$ jsou po dvou komaximální a $n \geq 2$, pak $I_1 \cap ... \cap I_n = I_1..I_n$ a $I_1 \cap ... \cap I_{n-1}$a I_n jsou komaximální.

Důkaz:
Budeme postupovat indukcí pro $n = 2$ máme dokázáno, díky lemmatu komaximální průnik.
Pokračujme důkazem pro $n > 2$.
Podle lemmatu 3.1.10 je $I_1..I_{n-1}$ ideál.
Dokažme si nyní, že $I_1..I_{n-1}$ a I_n jsou komaximální.
Pro všechna $i < n$, platí že $I_i + I_n = R$.
Pro obor integrity určitě platí $R \trianglelefteq R$.
Obor integrity R je uzavřen na násobení a sčítání, takže určitě nutně musí být $RR = R$.
Pak ale nutně platí $R = (I_1 + I_n)..(I_{n-1} + I_n)$.
To když upravíme podle lemmatu 3.1.12.
Tak dostaneme $R = I_1..I_{n-1} + I_nX$, 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 prvkem z R.
Z toho, že $X \trianglelefteq R$ víme, že $X \subset R$.
Pak, ale musí platit $I_n X \subset I_n$.
Tím pádem dostaneme $R \subset I_1..I_{n-1} + I_n$.
Každý výraz je složen je z prvků oboru integrity a součtů a součinů, na něž je obor integrity uzavřen.
Rozhodně platí $I_1..I_{n-1} + I_n \subset R$.
Dokázali jsme tedy, že $I_1..I_{n-1}$ a I_n jsou komaximální,
Můžeme použít lemma 3.5.4 a dostaneme tedy $(I_1...I_{n-1})I_n = (I_1...I_{n-1}) \cap I_n$.
Z indukčního předpokladu víme, že $(I_1...I_{n-1}) \cap I_n = (I_1 \cap ... \cap I_{n-1}) \cap I_n$.
□

Nyní si dokážeme, že pokud máme komaximální ideály, tak dokážeme sestrojit homomorfismus z oboru integrity do jejich faktorokruhů. Tento homomorfismus má jako jádro průnik těchto ideálů a je dokonce surjektivní, tím pádem nám dává nám dává řešení pro modulární rovnice modulo tyto ideály.

Věta 3.5.6 (Komaximalita a homomorfismus)**.**
Nechť R je obor integrity a I_1,..,$I_n \trianglelefteq R$. Mějme homomorfismus $f : R \to R \wr I_1 \times ... \times R \wr I_n$ s předpisem $f(a) = (a + I_1,..,a + I_n)$, pak $Ker(f) = I_1 \cap ... \cap I_n$ a f je surjektivní právě tehdy když I_1,...,I_n jsou po dvou komaximální.

Důkaz:
Dokažme si nejdříve, že $Ker(f) = I_1 \cap ... \cap I_n$.
Mějme nějaké $x \in I_1 \cap ... \cap I_n$, pak pro každé $i \leq n$ platí $x \in I_i$.
Z definice funkce f víme, že $f(x) = x + I_i$.
Pokud $x \in I_i$ a $I_i \trianglelefteq R$, tak je uzavřený na sčítání platí.
Tedy nutně platí $f(x) = I_i$ a tedy $x \in Ker(f)$.
Bez újmy na obecnosti uvažujme nyní $x \notin I_1$, pak $x \notin Ker(f)$.
Protože prvek z jádra se zobrazí vždy na prvek ideálu podle lemmatu 3.3.4.
Jenže kdyby $x + I \notin I_1$, tak podle lemmatu rozdíl ideálů je $x \in I_1$, což je spor.
Dokažme druhou část této věty.
Předpokládejme, že f je surjektivní a mějme dvě $i \neq j$.
Definujme poté funkcí $h : R \wr I_1 \times ... \times R \wr I_n \to R \wr I_i \times R \wr I_j$ takovou, že pro $h(p_1 + I_1,...,p_i + I_i,...,p_j + I_j,...,p_n + I_n) = (p_i + I_i,p_j + I_j)$.
Tato funkce je určitě surjektivní.
Nyní podle předpokladu I_i,$I_j \trianglelefteq R$.
Pak podle lemmatu 3.1.9 je $I_i + I_j \trianglelefteq R$.
Podle lemmatu 3.1.5 je $I_i \subset I_i + I_j$.
Pak podle lemmatu 3.3.8 je ideál $(I_i + I_j) \wr I_i$ v $R \wr I_i$.
Podle lemmatu 3.3.6, je $R \wr I_i$, okruh.
Nyní můžeme uvažovat funkci podobnou jako ve větě v 2. o izomorfismu, která je také surjektivní.
Dále jsme větě 2. o izomorfismu dokázali, že existuje bijekce do $R \wr (I_i + I_j) \times R \wr (I_i + I_j)$, která samozřejmě je také surjektivní.
Pokud složíme dvě funkce surjektvní máme opět funkci surjektivní.
Protože pokud se libovolný prvek z konečné obrazu zobrazí nějaký prvek ze vzoru, jež má vzor v podle druhé zobrazení v konečném vzoru, tak pak musí mít složení

těchto zobrazení tento vzor také. Složením těchto funkcí tedy dostáváme funkci $v : R \leftrightarrow R \wr (I_i + I_j) \times R \wr (I_i + I_j)$ s předpisem $v(x) = (x + I_i + I_j, x + I_i + I_j)$.
Tedy zobrazuje prvek na dvojici stejných prvků.
To znamená, že $R \wr (I_i + I_j)$ musí mít jen jeden prvek.
Pokud by tu byly aspoň dva různé prvky $a,b \in R \wr (I_i + I_j)$.
Pak potom pro tuto funkční hodnotu $(a + I_i + I_j, b + I_i + I_j)$ neexistuje obraz.
Tím jsme dokázali, že funkce je surjektivní.
Podle lemmatu 3.3.6 je $R \wr (I_i + I_j)$ okruhem.
Tudíž musí obsahovat neutrální prvek vzhledem ke sčítání a tedy podle lemmatu 3.3.4 víme, že platí $R \wr (I_i + I_j) = I_i + I_j$.
To nám říká, že libovolný prvek $x \in R$ jde zapsat jako součet prvků z I_i, I_j.
Pak tedy musí být platit $x \in I_i + I_j$.
Tedy $R \subset I_i + I_j$.
Podle lemmatu 3.1.9 je $I_i + I_j \trianglelefteq R$.
Pak z definice ideálu musí platit $I_i + I_j \subset R$.
Máme tedy $I_i + I_j = R$, ale tím jsme dokázali, že ideály jsou komaximální.
Pokračujme důkazem druhé části implikace.
Mějme $I_1,...,I_n$ komaximální ideály a budeme postupovat indukcí podle počtu ideálů.
Dokažme tedy případ, kdy $n = 2$
Tedy pro libovolné $a \in R \wr I_1$ a libovolné $b \in R \wr I_2$, existuje $r \in R$ takové, že $a + I = r$ a $b + I = r$.
Podle lemmatu 3.5.3 jsou tedy I_1, I_2 nesoudělné a tedy existuje $c \in I_1$ a $d \in I_2$ takové, že $c + d = 1$.
Definujme nyní $r = ad + bc$. Dokažme si nyní, že opravdu $r \sim a \, mod \, I_1$ a $r \sim b \, mod \, I_2$.
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 $r - b = (ad + bc) - b$, z předpokladu víme, že $c + d = 1$, dostaneme tedy $r - a = (ad + bc) - a(c + d)$ a $r - b = (ad + bc) - b(c + d)$.
Když použijeme distributivitu a poté odstraníme závorky dostaneme $r - a = ad + bc - ac - ad$ a $r - b = ad + bc - bc - bd$.
Máme tedy $r - a = bd - ad$ a $r - b = ac - bc$.
Na obě použijeme distributivitu a dostaneme $r - a = c(b - a)$ a $r - b = d(a - c)$.
Podle předpokladu $a - c, b - a \in R$ a $d \in I_1$ a $d \in I_2$.
Jelikož $I_1, I_2 \trianglelefteq R$, tak musí být uzavřené na násobení prvkem z R.
Máme tedy $r - a \in I_1$ a $r - b \in I_2$.
Předpokládejme tedy nyní, že máme dokázáno, pro $n - 1$.
Definujme $I = I_1...In - 1$.
Podle lemmatu 3.5.5, víme že $I = I_1 \cap ... \cap I_{n-1}$ a také, že I, I_n jsou vzájemně komaximální.
Máme tedy zobrazení $h : R \to R \wr I_1 \times ... \times R \wr I_{n-1}$ s předpisem $h(a) = (a + I_1,...,a + I_n)$ takové, že $Ker(h) = I$. V kroku pro $n = 2$ dokázali, že situaci umíme řešit pro libovolné dva faktorokruhy s komaxilmálnimi ideály.
Máme tedy i $g : R \to R \wr I \times R \wr I_n$.
Dokažme si, že $R \wr I_1 \times ... \times R \wr I_{n-1}$ je okruh.
Ten jím ale musí být, protože $R \wr I_i$ pro $i \leq n$ je podle lemmatu 3.3.6 okruhem, ale na produktu všechny operace probíhají po složkách a tedy i produkt okruhů

musí být okruhem.
Nyní si dokažme tedy, že h je homomorfismus.
Dokažme si nejdříve součet.
Mějme tedy $h(a) = (a + I_1,...,a + I_n)$ a $h(b) = (b + I_1,...,b + I_n)$.
Potom $h(a) + h(b) = (a + I_1,...,a + I_n) + (b + I_1,...,b + I_n)$.
Budeme sčítat po složkách a dostaneme $h(a) + h(b) = (a + b + I_1,...,a + b + I_n)$.
To je ale definice $h(a + b)$, takže máme $h(a) + h(b) = h(a + b)$.
Důkaz pro násobení je víceméně obdobný.
Mějme tedy $h(a) = (a + I_1,...,a + I_n)$ a $h(b) = (b + I_1,...,b + I_n)$.
Poté $h(a)h(b) = (a + I_1,...,a + I_n)(b + I_1,...,b + I_n)$.
Budeme násobit po složkách to když po složkách a dostaneme $h(a)h(b) = (ab + I_1,...,ab + I_n)$.
To ale je definice $h(ab)$, takže máme $h(a)h(b) = h(ab)$. .
Podle definice $h(0) = (I_1,...,I_n)$ a tedy zobrazení je homomorfismus.
Použijeme tedy nyní větu 1. o izomorfismu a dostaneme izomorfismu $i : R \wr I \to R \wr I_1 \times ... \times R \wr I_{n-1}$.
Dostáváme tedy zobrazení, kde složíme h a vnější zobrazení bude $i \times id$.
Budeme mu říkat f. Zobrazení f je surjektivní, protože je složeno ze dvou surjektivních zobrazení.

□

Důsledkem této věty je jak si dokážeme zobecněná forma Čínské zbytkové věty.

Věta 3.5.7 (Čínska zbytková věta)**.**
Nechť R je obor integrity a $I_1,...,I_n \trianglelefteq R$ jsou komaximální takové, že $I_1 \cap ... \cap I_n = 0$, pak $\forall r_1,...,r_n \in R \exists! r \in R$ takové, že $r \sim r_i \, mod \, I_i$ pro všechna $i \leq n$.

Důkaz:
Podle věty komaximalita a homomorfismus víme, že díky komaximalitě ideálů je $f : R \to R \wr I_1 \times ... \times R \wr I_n$ funkce surjektivní. Tím pádem pro každé $r_1,...,r_n \in R$ máme $r = r_i + I_i$.
Víme tedy, že takové $r \in R$ existuje.
Kdyby ale existovalo víc řešení, tak mějme $r,s \in R$, což jsou dvě různé řešení.
Potom pro každé $i \leq n$ platí pro nějaké $x \in I_i$, $r + x = s$.
Určitě platí pro každé $i \leq n$ je $0 \in I_i$.
To znamená, že $r + 0 = s$ a rovnice tedy má jen jedno řešení.
Podle věty komaximalita a homomorfismus $x \in I_1 \cap ... \cap I_n$.
Kdyby bylo $x \neq 0$, tak je to spor, protože podle předpokladu $I_1 \cap ... \cap I_n = 0$.

□

Máme tedy Zobecněnou čínskou zbytkovou větu, pokud za obor integrity vezmeme celá čísla dostaneme naší známou Čínskou zbytkovou větu pro celá čísla.

Závěr

V rámci práce jsme nadefinovali dvě verze teorie dělitelnosti. Jednu, na které jsme definovali Gaussova čísla, na nichž jsme ukázali jaké podmínky dělitelnosti můžeme na oboru integrity definovat a jaký mají vzájemný vztah.Také jsme dokázali, že to jsou přesně ty obory integrity, které chceme používat pro dělitelnost, pokud požadujeme platnost Zobecněné základní věty aritmetiky. V poslední kapitole jsme definovali dělitelnost pomocí ideálů a ukázali si nejdříve Bezoutovy obory, což jsou obory, kde platí Zobecněná Bezoutova věta, a tedy pro libovolné dva prvky je jejich společný největší dělitel linerání kombinací těchto prvků. Dále jsme ukázali, že pokud budeme mít obor integrity, který je zároveň Bezoutův a Gaussův, tak potom v něm každý ideál je hlavní, tedy lze jej generovat jedním prvkem. Speciálním případem tohoto oboru integrity Euklidův obor, který reprezentuje obory, kde se zastaví Euklidův algoritmus. Tedy máme polynomiální řešení vůči délce vstupu. Jak jsme na konci dokázali, tak existuje Zobecněná Čínská zbytková věta pro libovolný okruh. Tedy někdy rozhodně dává smysl zkoumat a řešit dělitelnost na obecných oborech integrity, které nejsou Bezoutovy. Na Zobecněné Čínské zbytkové větě, ale můžeme demonstrovat, že někdy se opravdu vyplatí, přidat k teorii další axiomy a teorie je poté sice není tak zobecněná a univerzální, ale za to je o dost efektivnější. Protože jak jsme ukázali, pokud přidáme axiom, že existuje pro každou konečnou množinu aspoň jeden největší společný dělitel, tak můžeme dokázat distributivitu největšího společného dělitele vůči násobení. Poté pokud k této teorii přidáme ještě axiom, že na faktoroboru tohoto oboru integrity je relace vlastního dělitele fundovaná anebo každý nenulový neinvertibilní prvek má ireducibilní rozklad, tak dostaneme teorii, kde už nutně musí platit základní věta aritmetiky. Pokud k této teorii přidáme Bezoutovu větu, tak díky ní nejen, že máme zaručeno, že největší společný dělitel dvou čísel je jejich lineární kombinací. Pokud k této teorii přidáme ještě axiom, že existuje na oboru euklidovká norma, tak dostávám konečně obor, kde máme efektivní algoritmus pro řešení pro Zobecněnou Čínskou zbytkvou nebo nalezení největšího společného dělitele.

Seznam použité literatury

[5] Dummit David S. and Foote Richard M. Abstract algebra. John Wiley and Sons, 2004.

[2] Přikrylová Katrin. Pojem ideálu a filtru v algebře a logice. Bakalářská práce, Katedra logiky Filozofické fakulty, Karlova Univerzita v Praze, 2013.

[3] Procházka Ladislav. Algebra. Academia, 1990.

[4] Kořínek Vladimír. Základy Algebry. Academia, 1956.

[5] Howie John M. Fields and Galois theory. Springer, 2006.

[6] R. A. Wilson An example of a PID which is not a Euclidean. Paper, 2015