1 Úvod

Poznámka (Informační zdroje)
Stránky, diskuze na google docs, Moodle.

Poznámka (Proč algebra)
Diofanctické rovnice (Fermatovy věty, Gaussova celá čísla), kořeny polynomů (Grupy polynomů), geometrie (nekonstruovatelnost), studium abstraktních struktur běžných objektů.

2 Obory

Definice 2.1 (Okruh)

Okruh R je pětice $(R, +, \cdot, -, 0)$, kde $+, \cdot : R \times R \to R$, $- : R \to R$, $0 \in R$ tak, že $(\forall a, b, c \in R)$:

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

$$a + b = b + a, a + 0 = a, a + (-a) = 0,$$

$$a \cdot (b \cdot c) = (a \cdot b) \cdot c, a \cdot (b + c) = a \cdot b + a \cdot c, (b + c) \cdot a = b \cdot a + c \cdot b.$$

Definice 2.2 (Komutativní okruh)

Komutativní okruh je okruh, pro který platí $a \cdot b = b \cdot a$.

Definice 2.3 (Okruh s jednotkou)

Okruh s jednotkou je okruh, který má prvek $1 \in R : a \cdot 1 = a$.

Definice 2.4 (Obor (integrity))

Obor (integrity) je komutativní okruh s jednotkou tak, že $0 \neq 1 \wedge (a \neq 0 \wedge b \neq 0 \implies a \cdot b \neq 0)$.

Definice 2.5 (Těleso)

Těleso je komutativní okruh s 1, že $0 \neq 1$ a $\forall 0 \neq a \in R \ \exists b \in R : a \cdot b = 1$.

Definice 2.6 (Podokruh)

Podokruh S okruhu R je $(S, +|_S, \cdot|_S, -|_S, 0)$, kde $0 \in S$ a $\forall a, b \in S : a + b \in S \wedge a \cdot b \in S \wedge -a \in S$. Značíme $R \leq S$.

Definice 2.7 (Podobor)

S je podobor oboru R tehdy, když $S \leq R$ a S je obor.

Definice 2.8 (Podtěleso)

S je podtěleso tělesa R tehdy, když $S \leq R$ a S je těleso.

Definice 2.9 (Gaussova čísla)

$\mathbb{Z}[i] = \{a + b_i | a, b \in \mathbb{Z}\}$ jsou tzv. Gaussova celá čísla.

$\mathbb{Q}[i] = \{a + bi | a, b \in \mathbb{Q}\}$ jsou tzv. Gaussova racionální čísla..

2.1 Základní vlastnosti

Tvrzení 2.1

Mějme množinu X s asociativní (tj. $(a * b) * c = a * (b * c)$) operací $* : X \times X \to X$. Pak hodnota výrazu $a_1 * a_2 * a_3 * \ldots * a_n$ nezávisí na uzávorkování.

Důkaz

Indukcí. □

Tvrzení 2.2 (Základní vlastnosti oborů)

Buď R okruh a $a, b, c \in R$.

$$1) a + c = b + c \implies a = b,$$

$$2) a \cdot 0 = 0,$$

$$3) -(-a) = a, \ -(a + b) = -a + (-b),$$

$$4) -(a \cdot b) = (-a) \cdot b = a \cdot (-b), \ (-a) \cdot (-b) = a \cdot b,$$

$$5) \text{Je-li } R \text{ obor, pak } a \cdot c = b \cdot c \wedge c \neq 0 \implies a = b.$$

Důkaz

$$1)(a + c) + (-c) = (b + c) + (-c) \implies a + 0 = b + 0 \implies a = b,$$

$$2) 0 + a \cdot 0 = a \cdot 0 = a \cdot (0 + 0) = a \cdot 0 + a \cdot 0 \implies 0 = a \cdot 0.$$

□

Tvrzení 2.3 (Každé těleso je obor)

Z existence a^{-a} vyplývá $a \neq 0, b \neq 0 \implies ab \neq 0$.

Důkaz (Sporem)
$a \neq 0, b \neq 0, ab = 0 \implies b = (a^{-1} \cdot a) \cdot b = a^{-1} \cdot (ab) = a^{-1} \cdot 0$ a podle předchozího tvrzení (část 2) $b = 0$ ↯. □

Tvrzení 2.4

Každý konečný obor je těleso.

Důkaz
Viz skripta. □

Definice 2.10

Nechť R je okruh s jednotkou 1. Charakteristika R je nejmenší přirozené číslo n tak, že $\underbrace{1 + 1 + \ldots + 1}_{n\text{-krát}}$, pokud takové n neexistuje, říkáme, že charakteritika je 0 (případně ∞).

Prvek $\underbrace{1 + 1 + \ldots + 1}_{n\text{-krát}}$ značíme n, obdobně $\underbrace{-1 - 1 - \ldots - 1}_{n\text{-krát}}$ značíme $-n$.

Tvrzení 2.5

Každý obor má charakteristiku 0 nebo p.

Důkaz
Pro 1 je to cvičení. V případě, že charakteristika je $n = k \cdot l$, $k, l \neq 1$, pak $0 = k \cdot l$. Jsme v oboru, tedy $k = 0$ nebo $l = 0$. Spor s minimalitou n. □

2.2 Izomorfismus

Definice 2.11 (Homomorfismus)

Nechť R, S jsou okruhy. Zobrazení $\varphi : R \to S$ je homomorfismus okruhů, pokud $\forall a, b \in R :$

$$\varphi(a + b) = \varphi(a) + \varphi(b) \wedge \varphi(a \cdot b) = \varphi(a) \cdot \varphi(b).$$

Je-li homeomorfismus φ bijekce, nazývá se izomorfismus.

Poznámka
Inverzní zobrazení k izomorfismu je izomorfismus.

Definice 2.12

Okruhy R, S jsou izomorfní, pokud existuje izomorfismus $\varphi : R \to S$. Značíme $R \simeq S$.

Například
Tzv. prvookruh (tj. všechny prvky tvaru $1 + 1 + \ldots + 1$ nějakého okruhu s jedničkou) je izomorfní $\mathbb{Z}_n$ resp. (v tomto případě musíme zahrnout i $-1 - 1 - \ldots - 1$) $\mathbb{Z}$.

2.3 Podílové těleso

Definice 2.13 (Multiplikativní množina)

Nechť R je obor. Pak $M \subseteq R$ je multiplikativní množina, pokud $0 \notin M, 1 \in M$ a $a, b \in M \implies a \cdot b \in M$.

Například
Nejdůležitější MM je $M = R \setminus \{0\}$.

Definice 2.14 (Podílové těleso)

Nechť R je obor a M multiplikativní množina. Definujeme relaci $\sim$ na $R \times M$:

$$(a, b) \sim (c, d) \equiv ad = bc.$$

Blok $[(a, b)]_\sim$ nazýváme zlomek a značíme $\frac{a}{b}$.

Na $Q = \left\{\frac{a}{b} | a \in R, b \in M\right\}$ definujeme operace

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}, \ \frac{a}{b}\frac{c}{d} = \frac{ac}{bd}, \ -\frac{a}{b} = \frac{-a}{b}, \ 0 = \frac{0}{1}, 1 = \frac{1}{1}.$$

Tedy Q je okruh s jednotkou. $(Q, +, -, \cdot, 0, 1)$ se nazývá lokalizace oboru R v MM M. Pokud $M = R \setminus \{0\}$, pak se nazývá podílové těleso.

Tvrzení 2.6

Máme R, N, Q z předchozí definice. 1) Q je obor. 2) $\left\{\frac{a}{1} | a \in R\right\}$ je podobor Q, který je izomorfní s R. 3) Je-li $M = R \setminus \{0\}$, pak Q je těleso.

Důkaz
1) Ověříme axiomy. Triviální. Důležitý je hlavně součin ne0 prvků.

2) Ověříme uzavřenost a obsah jedničky. Ověříme, že zjevné zobrazení je izomorfizmus.

3) Ověříme axiomy. Na tři řádky. $\square$

3 Polynomy

3.1 Obory polynomů

Poznámka (Značení)
V celé sekci Polynomů je R komutativní okruh s jednotkou.

Definice 3.1 (Polynom)

Polynom v proměnné x nad okruhem R je výraz tvaru

$$a_0 + a_1 \cdot x + a_2 \cdot x^2 + a_n \cdot x^n,$$

kde $n \geq 0$, $a_1, \ldots, a_n \in R$ a $a_n \neq 0$ vyjma $n = 0$. $a_1, \ldots, a_n$ jsou koeficienty, x proměnná. Navíc se dodefinovává $a_m = 0 \forall m > n$.

Číslo $n = \deg f$ je stupeň polynomu f. $\deg 0 = -1$. a_n se nazývá vedoucí koeficient a a_0 absolutní člen.

f je monický, pokud $a_n = 1$. Množinu všech polynomů značíme $R[x]$.

Definice 3.2 (Operace na $R\,[x]$)

$$\sum_{i=0}^{m} a_i x^i + \sum_{i=0}^{n} b_i x^i = \sum_{i=0}^{max(m,n)} (a_i + b_i) x^i; \;\; -\sum_{i=0}^{m} a_i x^i = \sum_{i=0}^{m} -a_i x^i;$$

$$\left(\sum_{i=0}^{m} a_i x^i\right)\left(\sum_{i=0}^{n} b_i x^i\right) = \sum_{i=0}^{m+n} \sum_{j+k=i, j, j \geq 0} (a_j \cdot b_k) x^i$$

Tvrzení 3.1

$R[x]$ je komutativní okruh s jednotkou. Navíc je-li R obor, pak i $R[x]$ je obor $\wedge \deg(fg) = \deg f + \deg g \; \forall f, g \in R[x], f \neq 0 \neq g$.

Důkaz
Jednoduché, ve skriptech. Druhá část přes vedoucí koeficienty (jsou nenulové). $\square$

Definice 3.3 (Polynom více proměnných)

Induktivní definicí: Polynom v proměnných $x_1, x_2, \ldots, x_m$ nad okruhem R je polynom v proměnné x_m nad okruhem $R[x_1, \ldots, x_{m-1}]$.

Značíme $R[x_1, \ldots, x_m] = (R[x_1, \ldots, x_{m-1}])[x_m]$.

Každý $f \in R[x_1, \ldots, x_m]$ jde jednoznačně napsat v distribuovaném tvaru (je potřeba dokázat, ale tím pádem nezáleží na pořadí proměnných):

$$\sum_{k_1,\ldots,k_m}^{n} a_{k_1,\ldots,k_m} x_1^{k_1} \cdot \ldots \cdot x_m^{k_m}.$$

3.2 Hodnota polynomu

Definice 3.4

$R \leq S$ obory. $f = a_0 + a_1 \cdot x + \ldots + a_n \cdot x^n \in R[x], u \in S$. Hodnota polynomu f po dosazení u je definována:

$$f(u) := a_0 + a_1 \cdot u + \ldots + a_n \cdot u^n \in S.$$

(Operace jsou v oboru S.)

Zobrazení $S \to S$, $u \mapsto f(u)$ nazýváme polynomiální zobrazení dané polynomem f.

3.3 Dělení polynomu se zbytkem

Definice 3.5

$f, g \in R[x]$. g dělí f, zapisujeme $g|f$, $\equiv \exists h \in R[x]$ tak, že $f = gh$.

Je-li R obor a $g|f \neq 0 \implies \deg g \leq \deg f$ z tvrzení výše.

Tvrzení 3.2 (Dělení polynomů se zbytkem)

Nechť R je obor, Q podílové těleso. $f, g \in R[x], g \neq 0$. Pak existuje právě jedna dvojice $q, r \in Q[x]$:

$$f = gq + r \wedge \deg r < \deg g.$$

Je-li navíc g monický, pak $q, r \in R$.

$f div g := q$ *a* $f mod g := r$.

Důkaz
$q_0 = 0, r_0 = f$. Induktivně ($l(f) :=$ vedoucí koeficient polynomu f):

$$q_{i+1} = q_i + \frac{l(r_i)}{l(g)} x^{\deg r_i - \deg g},\ r_{i+1} = r_i - \frac{l(r_i)}{l(g)} x^{\deg r_i - \deg g} \cdot g.$$

Vidíme, že stupeň r_i se snižuje, a když $\deg r_i < \deg g$, tak skončíme a $r = r_i, q = q_i$.

Jednoznačnost:

$$f = gq + r = g\tilde{q} + \tilde{r} \implies g(q - \tilde{q}) = \tilde{r} - r \implies g|\tilde{r} - r \implies \tilde{r} - r = 0.$$

□

3.4 Kořeny a dělitelnost

Definice 3.6

Ať $R \leq S$ jsou obory, $f \in R[x]$, $a \in S$. Pak a je kořen $f \equiv f(a) = 0$.

Tvrzení 3.3

Buď R obor, $f \in R[x]$, $a \in R$. a je kořen $f \Leftrightarrow x - a|f$.

Důkaz
$\implies$: $f = (x - a) \cdot g$ pro nějaké $g \in R[x] \implies f(a) = (a - a) \cdot g(a) = 0$.

Buď $q, r \in R[x]$ podíl a zbytek při dělení f monickým polynomem $x - a$. $f = (x - a) \cdot q + r$, $\deg r < \deg(x - a) = 1 \implies r$ je konstantní polynom. Dosadíme a:

$$0 = f(a) = (a - a)q(a) + r(a) = r(a).$$

r je konstantní $\implies r = 0$. $f = (x - a) \cdot q + 0 \implies x - a|f$. □

Pozorování

$$f mod x - a = f(a)$$

Věta 3.4 (Počet kořenů)

R obor, $0 \neq f \in R[x]$. Pak f má nejvýše $\deg f$ kořenů v R.

Důkaz
Indukcí dělením $x -$ kořen. □

Definice 3.7 (Vícenásobný kořen)

Ať $f \in R[x], a \in R$. Pak a je n-násobný kořen $f \equiv (x-a)^n | f$ a $(x-a)^{n-1} \not| f$.

4 Číselné obory

4.1 Okruhová a tělesová rozšíření

Definice 4.1

Nechť $R \leq S$ jsou komutativní okruhy, $a_1, \ldots, a_n \in S$. Definujeme $R[a_1, \ldots, a_n]$ jako nejmenší podokruh okruhu S, který obsahuje R a $a_1, \ldots, a_n$. Ten nazveme okruhové rozšíření R o prvky $a_1, \ldots, a_n$.

Nechť $R \leq S$ jsou tělesa, $a_1, \ldots, a_n \in S$. Definujeme $R(a_1, \ldots, a_n)$ jako nejmenší podtěleso tělesa S, které obsahuje R a $a_1, \ldots, a_n$. To nazveme tělesové rozšíření R o prvky $a_1, \ldots, a_n$.

Tvrzení 4.1

Mějme $R \leq S$ komutativní okruhy s 1, $a \in R$. Pak $R[a] = \{f(a) | f \in R[x]\}$. Jsou-li R, S navíc tělesa, pak $R(a) = \left\{\frac{f(a)}{g(a)} | f, g \in q[R], g(a) \neq 0\right\}$.

Důkaz

Dokážeme, že je to podokruh, že obsahuje R i a a že je nejmenší takový. $\square$

Pozorování

Ať $T \leq S$ jsou tělesa, potom $T[a] \subseteq T(a)$.

Ale např. $\mathbb{Q}[i] = \mathbb{Q}(i)$.

Tvrzení 4.2

Nechť $T \leq S$ jsou tělesa, a není kořenem žádného nenulového polynomu z $T[x]$. Pak $T[a] \neq T(a)$.

Důkaz

Podle předchozího tvrzení $T[a] = \{f(a) | f \in T[x]\}$. Kdyby $T[a] = T(a)$, pak $T[a]$ je těleso, tedy $a^{-1} \in T[a] \implies a^{-1} = f(a)$ pro nějaký $f \in T[x]$, tedy $a \cdot f(a) - 1 = 0$. Tedy a je kořenem $x \cdot f - 1$. ↯. $\square$

4.2 Algebraická a transcendentní čísla

Definice 4.2

$a \in \mathbb{C}$ je algebraické, pokud je kořenem nějakého nenulového polynomu $f \in \mathbb{Z}[x]$.

Jinak a je transcendentní.

Poznámka (První důkaz transcendentního čísla)
Luvil? $\sum_{i=1}^{\infty} 10^{-i!}$.

Další čísla (19. stol): π, e.

Cantor: náhodné reálné číslo je transcendentní (tj. algebraická čísla jsou spočetná / mají míru 0).

Tvrzení 4.3

Množina algebraických čísel je spočetná.

Důkaz
Indexem polynomu $f = a_0 + a_1x + \ldots + a_nx^n \in \mathbb{Z}[x], f \neq 0$ nazvěme číslo $|a_0| + |a_1| + \ldots + |a_n| + n \in N$. Indexů existuje jen konečně mnoho daného indexu (díky započítání stupně do indexu). Všechny polynomy seřadím podle rostoucího indexu. Nyní už je zřejmě $\mathbb{Z}[x]$ spočetná. Navíc každý polynom má konečně kořenů, tedy, tedy i kořenů je spočetně mnoho. $\square$

Tvrzení 4.4

Množina reálných čísel je nespočetná.

5 Elementární teorie čísel

5.1 Dělitelnost a základní věta aritmetiky

Definice 5.1 (Dělitelnost v celých číslech)

Ať $a, b \in \mathbb{Z}$, b dělí a, značíme $b|a$, pokud $\exists c \in \mathbb{Z} : a = bc$.

± 1 a $\pm a$ se nazývají nevlastní dělitelé, ostatní jsou vlastní.

Tvrzení 5.1

Mějme $a, b \in \mathbb{Z}$, $b \neq 0$. Pak $\exists! q, r \in \mathbb{Z} : a = qb + r, 0 \leq r < |b|$. Značíme $a \div b = q$ a $a \mod b = r$. Navíc $b|a \Leftrightarrow a \mod b = 0$

Definice 5.2 (Prvočíslo a složené číslo)

Prvočíslo je $p \in \mathbb{Z}, p > 1$, které má pouze nevlastní dělitele. Ostatní přirozená čísla > 1 jsou složená.

Věta 5.2 (Základní věta aritmetiky)

$\forall a \in \mathbb{Z}, a > 1$ existují po dvou různá prvočísla $p_1, \dots, p_n$ a $k_1, \dots, k_n \in \mathbb{N}$ tak, že $a = p_1^{k_1} \cdot \ldots \cdot p_n^{k_n}$. Tento rozklad je až na pořadí jednoznačný.

Důkaz
Později. □

5.2 NSD

Definice 5.3 (NSD, NSN)

Největší společný dělitel $a, b \in \mathbb{Z}$ je největší $c \in \mathbb{N}$ takové, že $c|a, c|b$. Značíme ho $\mathrm{NSD}(a, b)$ (neexistuje pro $a = b = 0$).

Nejmenší společný násobek $a, b \in \mathbb{Z} \setminus \{0\}$ je nejmenší $c \in \mathbb{N}$ tak, že $a|c$ a $b|c$. Značíme ho $\mathrm{NSN}(a, b)$.

Poznámka
Základní věta aritmetiky $\implies a \cdot b = \mathrm{NSD}(a, b) \cdot \mathrm{NSN}(a, b)$.

Rychlý algoritmus na hledání NSN je Euklidův algoritmus.

Tvrzení 5.3 (Bézoutova rovnost)

$\forall a, b \in \mathbb{Z}$, $a \neq 0$ nebo $b \neq 0$, $\exists u, v \in \mathbb{Z}$ (Bézoutovy koeficienty) tak, že $a \cdot u + b \cdot v = \mathrm{NSD}(a, b)$.

Důkaz
Rozšířený Euklidův algoritmus. □

Lemma 5.4

Ať p je prvočíslo, $a, b \in \mathbb{Z}$. Pak $p|a \cdot b \implies p|a \vee p|b$.

Poznámka
V obecném oboru neplatí. Např. v $\mathbb{Z}[\sqrt{5}]$ $2|(\sqrt{5}+1)(\sqrt{5}-1) = 4$, ale $2 \nmid \sqrt{5} \pm 1$

Důkaz
BÚNO $p \not| a$, tedy chceme, aby $p|b$. p je prvočíslo, tudíž nemá vlastní dělitele $\implies$ NSD(p, a) = buď p (to by ale $p|a$), nebo 1. Dle tvrzení o Bézoutově rovnosti $\exists u, v \in \mathbb{Z}$: $pu + av = 1$. Vynásobíme b: $pbu + abv = b$. Ale $p|ab$, takže $p|pbu + abv = b$. □

Lemma 5.5

p prvočíslo, $a_1, \ldots, a_n \in \mathbb{Z}$. $p|a_1 \cdot \ldots \cdot a_n \implies \exists i : p|a_i$.

Důkaz
Indukcí z předchozího tvrzení. □

Důkaz (Základní věta aritmetiky)
Existence: pro spor ať a je nejmenší přirozené číslo, které nemá rozklad na součin. Buď je a prvočíslo, ale pak má rozklad $a = a^1$. Nebo je a složené, tedy $a = b \cdot c, 1 < b, c, < a$, ale a bylo nejmenší číslo, které nemá rozklad, tedy b i c mají rozklad. Ale pak součin těchto rozkladů je a.

Jednoznačnost: a nejmenší přirozené číslo, které má 2 rozklady: $a = p_1^{k_1} \cdot \ldots \cdot p_m^{k_m} = q_1^{l_1} \cdot \ldots \cdot q_n^{l_n}$. Pak $p_1 | q_1^{l_1} \cdot \ldots \cdot q_n^{l_n}$. Podle předchozího lemmatu $\exists i : p_1 | q_i$. Jsou to prvočísla, tedy $p_1 = q_i$. Potom $p_1^{k_1 - 1} \cdot \ldots \cdot p_m^{k_m} = q_1^{l_1} \cdot \ldots \cdot q_i^{k_i - 1} \ldots \cdot q_n^{l_n}$ jsou dva rozklady čísla $< a$. ↯. □

5.3 Kongruence

Poznámka (Historie)
Symbol $\equiv$ zavedl v roce 1801 Gauss.

Definice 5.4

$a, b, m \in \mathbb{Z}, m \neq 0$. a je kongruentní s b modulo m ($a \equiv b (\mod m)$), pokud $m|a - b$. (Ekvivalentně a, b dávají stejný zbytek po dělení m.)

Pozorování
Být kongruentní $\mod m$ je ekvivalence.

Tvrzení 5.6 (Vlastnosti kongruence)

$a, b, c, d, m \in \mathbb{Z}, m \neq 0$. $a \equiv b \mod m, c \equiv d \mod m$.

$a+c = b+d \mod m, \quad a-c \equiv b-d \mod m, \quad a \cdot c \equiv b \cdot d \mod m, \quad a^k \equiv b^k \mod m, k \in \mathbb{N}.$

$c \neq 0 \implies a \equiv b \mod m \Leftrightarrow ac \equiv bc \mod mc, \quad \text{NSD}(c, m) = 1 \implies a \equiv b \mod m \Leftrightarrow ac \equiv bc$ m

Důkaz
Z definice rozepsáním.

$$a \equiv b \mod m \Leftrightarrow \exists q : a - b = mq \Leftrightarrow ac - bc = mcq \Leftrightarrow ac \equiv bc \mod mc.$$

$cu+mv = 1, cu = 1-mv \implies (ac \equiv bc \mod m \Leftrightarrow a \equiv a(1-mv) \equiv auc \equiv buc \equiv b(1-mv) \equiv b \mod m$

□

5.4 Eulerova věta a RSA

Definice 5.5 (Eulerova funkce)

Eulerova funkce $\varphi(n)$ značí (pro $n \in \mathbb{N}$) počet $k \in \{1, 2, \ldots, n\}$ nesoudělných s n, čili $\mathrm{NSD}(k, n) = 1$.

Tvrzení 5.7

$n = p_1^{k_1} \cdot \ldots \cdot p_m^{k_m}$ prvočíselný rozklad, $n > 1$. Pak $\varphi(n) = p_1^{k_1-1}(p_1 - 1) \cdot \ldots \cdot p_m^{k_m-1}(p_m - 1)$.

Důkaz
Příště. □

Věta 5.8 (Eulerova)

Pokud a, m jsou nesoudělná přirozená čísla, pak $a^{\varphi(m)} \equiv 1 \mod m$.

Speciálním případem je Malá Fermatova věta: p prvočíslo, $p \nmid a \implies a^{p-1} \equiv 1(\mod p)$.

Důkaz
Φ_m nechť značí množinu $\{k \in [m] | \mathrm{NSD}(k, m) = 1\}$. $\varphi(m) = |\Phi_m|$.

Lemma: a, m nesoudělná přirozená čísla, $m \neq 1$. Definujeme zobrazení $f_a : \Phi_m \to \Phi_m$, $k \mapsto ka \mod m$. Pak f_a je dobře definované $\wedge$ je to bijekce.

Důkaz k, a nesoudělná s $m \implies k \cdot a$ nesoudělné s $m \implies k \cdot a \mod m$ nesoudělné s $m \implies k \cdot a \mod m \in \Phi_m$. $f_a(k) = f_a(l) \implies k \cdot a \equiv l \cdot a \mod m \implies k \equiv l \mod m$ (a je nesoudělné s m, tedy můžeme použít tvrzeni výše) $\implies k = l$. f_a je prosté a na konečné množině, tedy je bijekce.

$$\prod_{b\in\Phi_m} b = \prod_{b\in\Phi_m} f_a(b) = \prod_{b\in\Phi_m} (ab \mod m) \equiv a^{\varphi(m)} \prod_{b\in\Phi_m} b$$

$c = \prod_{b\in\Phi_m} b$, $c \equiv a^{\varphi(m)}c \mod m$ a c je nesoudělné s m, tedy dle tvrzení výše je $1 \equiv a^{\varphi(n)} \mod m$. □

Poznámka
Lemma z posledního důkazu nám říká, že každý prvek z Φ_m má inverzi v okruhu $\mathbb{Z}_m$.

Ten můžeme najít buď přes Eulerovu větu, nebo přes Bézoutovu větu. (Druhý způsob je zpravidla rychlejší.)

Poznámka (RSA (Rivest Shamir Adleman))
Šifrovací algoritmus založený na Eulerově větě.

5.5 Čínská zbytková věta

Poznámka
Špatně: Uvedená v knize umění války (počítání vojáků).

Správně: vymyslel ji čínský matematik, který se jmenoval stejně jako legendární generál, autor knihy výše.

Věta 5.9 (Čínská zbytková)

Nechť $m_1, \ldots, m_n \in \mathbb{N}$ *po dvou nesoudělná čísla. Označíme* $M = m_1 \cdot \ldots \cdot m_N$*. Ať* $u_1, \ldots, u_n \in \mathbb{Z}$*. Pak*[a] $\exists! x \in [M-1]_0$ *tak, že* $x \equiv u_1 \mod m_1, \ldots, x \equiv u_n \mod m_n$*.*

Důkaz
Jednoznačnost: Ať $x, y \in [M-1]_0$, pro které platí všechny kongruence. Potom $\forall i : m_i | x-y$, tedy $M | x-y$. Ale $|x-y| < M$, tudíž $x - y = 0$.

Existence: $f : [M-1]0 \to [m_1-1]_0 \times \ldots \times [m_n-1]_0$, $x \mapsto (x \mod m_1, \ldots, x \mod m_n)$. Korektní definice zobrazení (mimochodem je to dokonce isomorfismus okruhů). f je prosté (díky jednoznačnosti). Množiny jsou stejně velké, tedy je to dokonce bijekce, a proto existuje inverze, tudíž prvek $(u_1, \ldots, u_n)$ musí mít obraz při zobrazení f^{-1}, který z definice splňuje vlastnosti hledaného prvku.. □

[a]
$$[M-1]_0 = \{0, 1, \ldots, M-1\}$$

Důkaz (Vzorec pro eulerovu formuli)
1) $\varphi(p^k) = p^{k-1}(p-1)$. 2) a, b nesoudělná $\implies \varphi(ab) = \varphi(a) \cdot \varphi(b)$. Následně se vzorec dokáže aplikováním hodněkrát 2 na rozklad a jedničky nakonec.

1) Počet čísel soudělných s p^k z množiny $[p^k]$ je p^{k-1}, tedy počet nesoudělných je $p^k - p^{k-1}$.

2) Funkce z důkazu čínské zbytkové věty je bijekce. Uvažujme zúžení f na $\Phi_{a \cdot b}$. Chceme:

obraz zúžení je $\Phi_a \times \Phi_b$, tedy $\varphi(ab) = |\Phi_{ab}| = |\Phi_a \times \Phi_b| = \varphi(a) \cdot \varphi(b)$. Důkaz:

a) f zobrazí Φ do $\Phi_a \times \Phi_b$, čili, že $\mathrm{NSD}(x, a \cdot b) = 1$ implikuje $\mathrm{NSD}(x \mod a, a) = 1, \mathrm{NSD}(x \mod b, b) = 1$. b) f zobrazí $\Phi_{a,b}$ na $\Phi_a \times \Phi_b$, čili pokud $\mathrm{NSD}(u, a) = 1, \mathrm{NSD}(v, b) = 1$, pak to jediné x, které se zobrazí na (u, v), leží v $\Phi_{a,b}$.

$\mathrm{NSD}(x, ab) == 1 \Leftrightarrow \mathrm{NSD}(x, a) = 1 \wedge \mathrm{NSD}(x, b) = 1 \Leftrightarrow \mathrm{NSD}(x \mod a, a) = 1 \wedge \mathrm{NSD}(x \mod b, b) = 1.$

a) je zleva doprava a b) je zprava doleva. □

6 Abstraktní dělitelnost

6.1 Dělitelnost a asociovanost

Definice 6.1 (Dělitelnost, asociovanost, inverz)

R obor, $a, b \in R$. b dělí a v R, značíme $b|a$, pokud existuje $c \in R$ tak, že $a = b \cdot c$.

a, b jsou asociované v R, pokud $a|b$, $b|a$. Značíme $a||b$.

$a \in R$ je invertibilní, pokud existuje $b \in R$ tak, že $a \cdot b = 1$ (značíme $b = a^{-1}$).

Pozorování
a je invertibilní $\Leftrightarrow a||1$.

Relace $|$ je reflexivní $\wedge$ tranzitivní.

Tvrzení 6.1

R obor, $a, b \in R$. Pak $a||b \Leftrightarrow \exists$ invertibilní prvek $q \in R$ tak, že $a = bq$.

Důkaz
$\Leftarrow$: $(a = bq \implies b|a) \wedge (b = aq^{-1} \implies a|b)$.

$\implies: a = 0 \implies b = 0$. Ať $a \neq 0$, $(b|a \implies a = bu) \wedge (a|b \implies b = av) \implies a = bu = auv$. Můžeme vykrátit $a \neq 0$, tj. $1 = uv$, a u, v jsou tedy invertibilní. □

Definice 6.2 (Kongruence)

$a, b, m \in R : a \equiv b \mod m$, pokud $m|a - b$.

Pozorování
Je to ekvivalence, zachovává se přičtením a odečtením, ale nemusí platit krácení.

6.2 Kvadratická rozšíření $\mathbb{Z}$

Definice 6.3 (Kvadratické rozšíření $\mathbb{Z}$)

Kvadratické rozšíření $\mathbb{Z}$ je $\mathbb{Z}[\sqrt{s}] = \{a + b\sqrt{s} | a, b \in \mathbb{Z}\}$, kde $s \in \mathbb{Z}$, s není druhá mocnina celého čísla.

Důkaz (Tvar $\mathbb{Z}\,[sqrts]$)
Dokáže se uzavřenost. □

Definice 6.4

Norma na oboru $\mathbb{Z}[\sqrt{s}]$ je zobrazení $\ni$: $\mathbb{Z}[\sqrt{s}] \to \mathbb{N} \cup \{0\}\,, a + b\sqrt{s} \mapsto |a^1 - b^2 s|$.

Tvrzení 6.2

$\forall u, v \in \mathbb{Z}[\sqrt{s}]$ platí:

1. $\ni (u \cdot v) = \ni (u) \cdot \ni (v)$,
2. $\ni (u) = 1 \Leftrightarrow u$ *je invertovatelné.*
3. *Pokud* $u|v$ *a* $v|u$*, pak* $\ni (u) | \ni (v)$ *(víme z 1)) a* $\ni (u) \neq \ni (v)$.

Důkaz
1) vezmu a ověřím. Nebo využiji, že $\ni (u) = |u \cdot u'|$, kde $u' = a - b\sqrt{s}$, $u = a + b\sqrt{s}$. Zjistíme, že $(u \cdot v)' = u' \cdot v'$. Potom $|u \cdot v \cdot (u \cdot v)'| = |u \cdot u'| \cdot |v \cdot v'|$.

2) $\Leftarrow$: $u \cdot u^{-1} = 1 \implies \ni (u \cdot u^{-1}) = \ni (1) = 1$. A z 1) už plyne $\ni (u) = 1$. $\implies$: $\ni (u) = 1 \implies u \cdot u' = 1 \implies u'$ je hledaná inverze.

3) $u = 0 \implies v = 0 \implies v|u$. Ať tedy $v = uc$ pro $c \in \mathbb{Z}[\sqrt{s}]$. Ať $\ni (u) = \ni (v) = \ni (u \cdot c) = \ni (u) \cdot \ni (c) \implies \ni (c) = 1 \implies c$ je invert $\implies v||u$, čili $v|u$ spor. □

Pozor
Norma nesplňuje trojúhelníkovou nerovnost!

Tvrzení 6.3 (Dělení Gaussových čísel se zbytkem)

$$\forall \alpha, \beta \in \mathbb{Z}[i], \beta \neq 0\ \exists \gamma, \delta \in \mathbb{Z}[i] : \alpha = \beta \cdot \gamma + \delta \wedge \ni (\delta) < \ni (\beta).$$

Důkaz
$\mathbb{Z}[i] \subseteq \mathbb{C}$, tudíž berme $\frac{\alpha}{\beta} \in \mathbb{C}$. Zvolme $\gamma \in \mathbb{Z}[i]$ jako nejbližší hodnotu k $\frac{\alpha}{\beta}$. Položme $\delta = \alpha - \beta \cdot \gamma$. $\frac{\delta}{\beta} = \frac{\alpha}{\beta} - \gamma$, tj. $|\frac{\delta}{\beta}| \leq \frac{\sqrt{2}}{2}$, tj. $\ni \delta \leq \left(\frac{\sqrt{2}}{2}\right)^2 |\beta|^2 < 1 \ni (\beta)$. □

Poznámka
Takováto definice dělení se zbytkem funguje ještě pro $\mathbb{Z}[\sqrt{-2}]$ a $\mathbb{Z}[\sqrt{2}]$, ale pro ostatní $\mathbb{Z}[\sqrt{s}]$ už nefunguje.

6.3 Největší společný dělitel

Definice 6.5 (Největší společný dělitel, nesoudělnost a největší společný násobek)

Pro $a, b \in R$, R obor řekneme, že $c \in R$ je největší společný dělitel a, b, značíme $c = \mathrm{NSD}(a, b)$, pokud 1) $c|a \wedge c|b$ a 2) $\forall d|a, d|b : d|c$.

a, b jsou nesoudělné, pokud $\mathrm{NSD}(a, b) = 1$.

Obdobně definujeme $\mathrm{NSN}(a, b) = c \equiv a|c \wedge b|c \wedge \forall d, a|d, b|d : c|d$.

Poznámka
NSD nemusí existovat. Zároveň není jednoznačně určený. Ale je jednoznačně určený až na asociovanost.

6.4 Ireducibilní prvky a rozklady

Definice 6.6 (Vlastní dělitel a ireducibilní prvek)

R obor. $a \in R \setminus \{0\}$. $b \in R$ je vlastní dělitel a, pokud $b|a$ a $b \not\parallel 1$ a $b \not\parallel a$.

$a \neq 0$ je ireducibilní, pokud $a \not\parallel 1$ a nemá žádné vlastní dělitele.

Definice 6.7 (Ireducibilní rozklad)

Ireducibilní rozklad prvku a je zápis $a || p_1^{k_1} p_2^{k_2} \dots p_n^{k_n}$, kde $p_1, \dots, p_n$ jsou ireducibilní prvky a $p_i \not\parallel p_j$, pro $i \neq j$, a kde $k_1, \dots, k_n \in \mathbb{N}$.

Řekneme, že a má jednoznačný ireducibilní rozklad, pokud má právě 1 rozklad až na pořadí a asociovanost.

6.5 Prvočinitelé

Definice 6.8 (Prvočinitel)

R obor, pak $p \in R, p \nmid\mid 1$ je prvočinitel, pokud $\forall a, b \in R : p|a \cdot b \implies p|a \vee p|b$.

Pozorování

p je prvočinitel $\implies$ p je ireducibilní.

Důkaz

Ať $p = ab$. Pak $p|a \cdot b \overset{\text{prvočinitel}}{\implies} p|a \vee p|b$. Zároveň zřejmě $a|p$ a $b|p$, tedy $p||a \implies b||1$ nebo $p||b \implies a||1$. Tedy a, b jsou nevlastní dělitelé. $\square$

7 Existence a jednoznačnost ireducibilního rozkladu

7.1 Gaussovské obory

Definice 7.1 (Gaussovský obor)

Obor R je gaussovský, pokud $\forall a \in R, a \neq 0, a \nmid\mid 1$, má jednoznačný ireducibilní rozklad.

Příklad (Otevřený problém)

$\mathbb{Z}[\sqrt{s}]$ je gaussovský pro ∞ mnoho s. (Čeká se, že ano.)

Poznámka (Rozšíření definice ireducibilního rozkladu)

$a||1$, pak řekneme, že ireducibilní rozklad a je $a||1 = \ldots^0$.

Tvrzení 7.1 (Vlastnosti gaussovských oborů)

R je gaussovský obor a $a, b \in R$, $a, b \neq 0$. Ať navíc je $a||p_1^{k_1} \cdot \ldots \cdot p_n^{k_n}$ je ireducibilní rozklad. Pak $b|a \Leftrightarrow b||p_1^{l_1} \cdot \ldots \cdot p_n^{l_n}$ (nemusí být rozklad, protože l_i smí být 0), kde $\forall i : 0 \leq l_i \leq k_i$.

Důkaz
$\Rightarrow$: Ať $b = rp_1^{l_1} \cdot \ldots \cdot p_n^{l_n}$ a $a = q \cdot p_1^{k_1} \cdot \ldots \cdot p_n^{k_n}$, kde $r||1||q$. Chci: $b|a$, čili $\exists c : a = b \cdot c$. $c = q \cdot r^{-1} \cdot p_1^{k_1-l_1} \cdot \ldots \cdot p_n^{k_n-l_n}$.

$\implies : b|a \implies \exists c : a = b \cdot c$. Ať $b||q_1^{s_1} \cdot \ldots \cdot q_u^{s_u}$, $c||r_1^{t_1} \cdot \ldots \cdot r_v^{t_v}$ jsou ireducibilní rozklady. Zkombinujeme na rozklad $b \cdot c : B \cdot C||q_1^{s_1'} \cdot \ldots \cdot q_u^{s_u'} \cdot r_{i_1}^{t_{i_1}} \cdot \ldots \cdot r_{i_w}^{t_{i_w}}$ (vyfiltrujeme z rozkladu c ty r_i, který jsou asociovány s nějakým q_j). Máme 2 rozklady $b \cdot c = a$. Z jednoznačnosti rozkladů $q_i = p_{\pi(i)} \wedge s_i' = k_{\pi(i)} \geq s_i$. Tudíž $b||p_{\pi(1)}^{s_1} \cdot \ldots \cdot p_{\pi(n)}^{s_n}$, kde $s_i \leq k_{\pi(i)}$ (a doplníme chybějící p_j^0). $\square$

Důsledek (Dělitelnost v gaussovských oborech)
R gaussovský obor. Pak $\forall a, b \in R$, $a \neq 0 \vee 0 \neq b \implies$ existuje NSD(a, b). Každý ireducibilní prvek je prvočinitel. Neexistuje posloupnost $a_1, a_2, a_3, \ldots \in R : a_{i+1}|a_i \wedge a_i \not| a_{i+1}$.

Důkaz
Mějme rozklady $a||p_1^{k_1} \cdot \ldots \cdot p_n^{k_n}$ a $b||p_1^{l_1} \cdot \ldots \cdot p_n^{l_n}$ (doplněné tak, aby měli shodná prvočísla, ale $k_i \neq 0 \vee l_i \neq 0$).

Ať $a, b \neq 0$, potom existuje jednoznačný rozklad na prvočinitele. Potom každé (a jenom ty) $c||p_1^{m_1} \cdot \ldots \cdot p_n^{m_n}$, kde $0 \leq m_i \leq \min(k_i, l_i)$ dělí a i b, tedy c s největšími m_i a to už je zřejmě NSD(a, b).

Nechť $p|a{\cdot}b$ a zároveň je ireducibilní, tj. $p = p_i$ pro nějaké i. Toto p_i musí být v nenulové mocnině v a nebo v b, tedy p dělí jedno z nich.

Definujeme normu $\ni (a) = k_1 + \ldots + k_n$. Jelikož máme jednoznačný ireducibilní rozklad, tak $\ni$ je dobře definovaná. Pokud $b|a$, pak $\ni (b) \leq \ni (a)$, pokud navíc $b \not| a$, pak $\ni (b) < \ni (a)$. Posloupnost $\ni (a_i)$ je pak nekonečná klesající posloupnost v $\mathbb{N}$. $\lightning$. $\square$

7.2 Zobecněná základní věta aritmetiky

Věta 7.2 (Zobecněná základní věta aritmetiky)

R je gaussovský $\Leftrightarrow$ existuje NSD *všech dvojic prvků (krom 0, 0) $\wedge$ neexistuje nekonečná posloupnost vlastních dělitelů $a_1, a_2, a_3, \ldots \in R : a_{i+1}|a_i \wedge a_i \not| a_{i+1}$.*

Důkaz ($\implies$)
Je dokázáno. $\square$

Důkaz (Existence rozkladů)
Sporem s druhou částí: Ať $a_1 = a$, $a_1 \nmid\mid 1$ a a nemá ireducibilní rozklad. Mějme $a_i \nmid\mid 1$ a nemá ireducibilní rozklad. Tedy není ireducibilní (jinak by bylo samo sobě rozkladem) $\implies$ $a_i = b \cdot c$ pro nějaké $b, c \nmid\mid 1$. Kdyby b, c měly ireducibilní rozklad, pak by i. rozklad mělo i a_i. Takže aspoň jeden z nich nemá IR. Označíme ho a_{i+1}. Tudíž $a_{i+1} | a_i \wedge a_{i+1} \nmid\mid 1 \wedge a_{i+1}$ nemá IR. Indukcí tedy vyrobíme nekonečnou posloupnost, kterou mi podmínky zakazují. ↯. □

Lemma 7.3

R obor, $a, b \in R$, $c \in R$, $c \neq 0$. Předpokládejme, že existuje $\mathrm{NSD}(a, b)$, $\mathrm{NSD}(ca, cb)$. *Pak* $\mathrm{NSD}(ca, cb) = c \cdot \mathrm{NSD}(a, b)$.

Důkaz
Ve skriptech. Triviální. □

Lemma 7.4

Buď R obor, ve kterém existuje NSD *všech dvojic prvků. Pak je každý ireducibilní prvek prvočinitel.*

Důkaz
Buď p ireducibilní a ať $p | a \cdot b$. Ať $p \nmid a$. $\mathrm{NSD}(p, a)$ existuje, tedy $\mathrm{NSD}(p, a) = 1$, neboť p je ireducibilní. Podle předchozího lemmatu $\mathrm{NSD}(pb, ab) = b \cdot \mathrm{NSD}(p, a) = b$. Zároveň $p | pb$ a $p | ab$, b je NSD $\implies$ $p | b$. □

Důkaz (Jednoznačnost rozkladu)
Sporem: Mezi všemi prvky s nejednoznačnými rozklady vyberme ten, který má nejkratší rozklad, čili má minimální $k_1 + \ldots + k_n$. Nechť tedy $a || p_1^{k_1} \cdot \ldots \cdot p_n^{k_n} || q_1^{l_1} \cdot \ldots \cdot q_m^{l_m}$. p_1 je ireducibilní a dělí a, tedy (podle předchozího lemmatu) dělí q_i pro nějaké i. To ale znamená, že $p_1^{k_1 - 1} \cdot \ldots \cdot p_n^{k_n} || \ldots$. To jsou ale zase dva různé ireducibilní rozklady, ale to je spor s minimalitou. □

8 Eukleidův algoritmus a Bézoutova rovnost

8.1 Eukleidovské obory

Definice 8.1 (Eukleidovský obor)

R je obor. R je eukleidovský, pokud na něm existuje tzv. eukleidovská norma, čili zobrazení $\ni : R \to \mathbb{N}_0$ tak, že $\ni(0) = 0$, $a | b \wedge b \neq 0 \implies \ni(a) \leq \ni(b)$, $\forall a, b \in R, b \neq 0\ \exists q, r \in R : a = bq + r \wedge \ni(r) < \ni(b)$.

Pozorování
$a = 0 \Leftrightarrow \ni(a) = 0$. (Z ostré nerovnosti v třetí podmínce.)

Pozorování
Tělesa jsou eukleidovská ($\ni(0) = 0$, $\ni(a \neq 0) = 1$). $\mathbb{Z}$ je eukleidovské $\ni(a) = |a|$. $\mathbb{Z}[i]$ je eukleidovské. $\mathbb{T}$ těleso, $R = T[x]$ je eukleidovský obor ($\ni(f) = 1 + \deg f$).

$\mathbb{Z}[x]$ není eukleidovské (ale je gaussovské). ($\mathrm{NSD}(x+1, x-1) \neq f(x)\cdot(x+1)+g(x)\cdot(x-1)$. Tj. neplatí Bézoutova rovnost.)

Poznámka
Eukleidův algoritmus funguje normálně, jen dělení se zbytekm je určené podle definice Eukleidovských oborů.

Věta 8.1 (Správnost eukleidova algoritmu)

V eukleidovském oboru R najde rozšířený Eukleidův algoritmus pro jakýkoliv vstup $a, b \in R$ hodnotu $\mathrm{NSD}(a, b)$ a Bézoutovy koeficienty u, v splňující $\mathrm{NSD}(a, b) = u \cdot a + v \cdot b$.

Důkaz
EA skončí, neboť norma se zmenšuje a je nezáporná. Stačí ukázat, že $\mathrm{NSD}(a_{i-1}, a_i) = \mathrm{NSD}(a_{i+1}, a_i)$ a $a_i = u_i \cdot a + v_i \cdot b$. Obojí plyne z $a_{i-1} = a_i q + a_{i+1}$ □

Poznámka (Oprava)
$\mathrm{NSD}(0, 0) = 0$, tento případ tedy nemusel být v tvrzení výše vynecháván...<F2>

Lemma 8.2

R eukleidovský obor, $a, b \in R \setminus \{0\}$. Pokud $a|b$ a $a \not| b$, pak $\ni(a) < \ni(b)$.

Důkaz
Ať $b = a \cdot u$ pro nějaké $u \in R$. Víme, že $\exists q, r \in R$, $a = bq + r$, $\ni(r) < \ni(b)$. $a \not| b \implies b \not| a \implies r \neq 0$. $r = a - bq = a(1 - uq) \implies a|r$. Z definice dělení se zbytkem je $\ni(a) \leq \ni(r) < \ni(b)$. □

Věta 8.3

Eukleidovské obory jsou gaussovské.

Důkaz
R eukleidovský. Podle jedné z předchozích vět: gaussovský $\Leftrightarrow \exists\,\mathrm{NSD}$ a $\nexists$ řetězec vlastních dělitelů. NSD v eukleidovském existuje. Podle lemmatu výše se norma vlastních dělitelů zmenšuje, tedy opravdu takový řetězec neexistuje. □

Důsledek
$\mathbb{Z}[i]$ je gaussovský. $\mathbb{T}[x]$ je gaussovský.

8.2 Diofantické rovnice, rozklad v $\mathbb{Z}[i]$

Viz přednáška, nebude u zkoušky.

8.3 Obory hlavních ideálů

Definice 8.2

R je komutativní okruh. Ideál v R je neprázdná podmnožina $I \subseteq R$ tak, že $a, b \in I \implies a + b \in I, -a \in I$, $a \in I, r \in R \implies r \cdot a \in I$.

Například
$R = \mathbb{Z}$, $I = n\mathbb{Z}$ pro libovolné $n \in \mathbb{Z}$. (Dále dokážeme, že jiný v $\mathbb{Z}$ neexistuje.)

Tvrzení 8.4 (Definice hlavních ideálů)

R komutativní okruh, $a \in R$. Pak $a \cdot R = \{a \cdot r | r \in R\} = \{u \in R \,|\, a|u\}$ je ideál v R. Navíc je to nejmenší (vůči inkluzi) ideál v R, který obsahuje a. Takovému ideálu se říká hlavní.

Důkaz
$ar, as \in aR \implies ar + as = a(r + s) \in aR, -ar = a \cdot (-r) \in aR$, $ar \in aR, t \in R \implies art \in aR$. Tedy R je ideál.

Buď I ideál v R, $a \in I$. Z uzavřenosti plyne, že $ar \in I \forall r \in R \implies aR \subseteq I$. Tedy aR je nejmenší. $\square$

Poznámka
Hlavní, protože je tam ten hlavní prvek a, který ho vytváří.

Definice 8.3

Hlavním ideálům $0R = \{0\}$ a $1R = R$ se říká nevlastní, ostatním se říká vlastní.

Pozorování

$$a|b \Leftrightarrow aR \supseteq bR.$$

Důkaz
Triviální, viz přednáška. □

Důsledek

$$a||b \Leftrightarrow aR = bR.$$

Věta 8.5

V eukleidovském oboru je každý ideál hlavní.

Důkaz
R eukleidovský obor, I ideál. Pokud $I = \{0\} \implies I = 0R$. Ať $I \supset \{0\}$. Buď $0 \neq a \in I$ (libovolný) prvek s nejmenší možnou normou $\ni (a)$. Dokážeme, že $I = aR$. Zřejmě $aR \subseteq I$, protože $a \in I$. Pro spor ať existuje $b \in I \setminus aR$. Vydělíme se zbytkem: $b = aq + r, \ni (r) <\ni (a)$. Ale máme $r = b - aq$, přičemž $b, a, aq \in I$, tudíž $r = b - aq \in I$, ale z minimality normy a je $r = 0$, tudíž $a|b$. ↯. □

Definice 8.4 (Obor hlavních ideálů (OHI))

Pokud R je obor tak, že každý ideál je hlavní, pak se R nazývá obor hlavních ideálů (OHI).

Například
$\mathbb{Z}[x]$ není OHI. $\mathbb{Z}[\frac{1+\sqrt{-19}}{2}$ je OHI, ale není euklidovský (těžké dokázat).

Tvrzení 8.6

R komutativní okruh s 1. R je těleso $\Leftrightarrow$ R má pouze nevlastní ideály.

Důkaz
Ať $I \neq \{0\}$. Buď $0 \neq a \in I$. R těleso $\implies a^{-1} \in R$. Z uzavřenosti na násobení $1 = a \cdot a^{-1} \in I$, tudíž $R = 1 \cdot R \in I$, tj. $I = R = 1R$. □

Tvrzení 8.7

R komutativní okruh.

1) I, J ideály v $R \implies I \cap J$ je ideál v R.

2) I, J ideály v R. Pak $I + J = \{a + b | a \in I, b \in J\}$ je ideál. Navíc je to nejmenší ideál, který obsahuje I, J.

3) Mějme ideály I_j v R pro $j \in \mathbb{N}$ tak, že $I_1 \subseteq I_2 \subseteq I_3 \subseteq \ldots$. Pak $\bigcup_{j=\mathbb{N}} I_j$ je ideál v R.

Důkaz
1) $a, b \in I \cap J, r \in R \implies a, b \in I, a, v \in J$. I ideál $\implies a+b, -a, ra \in I$. J ideál $\implies a+b, -a, ra \in J$. Tedy $a+b, -a, ra \in I \cap J$.

2) Ať $a+b \in I+J, c+d \in I+J, r \in R$, kde $a, c \in I$, $b, d \in J$. Pak $(a+b)+(c+d) = (a+c)+(b+d) \in I+J$. $\cdot \wedge -$ obdobně. $I+J$ ideál.

Zřejmě $I \subseteq I+J$, neboť je $a+0 \in I+J$. Stejně tak pro J, tj. $I \cup J \subseteq I+J$. Druhý 'směr' plyne z uzavřenosti na součet.

3) Uzavřenost na $+$: Ať $a, b \in \bigcup I_j$. Tudíž $a \in I_j, b \in I_k$ pro nějaká j, k, BÚNO $j \leq k$. Máme $I_j \subseteq I_k$, tedy $a \in I_k$. I_k je ideál, tedy je uzavřený na součet. Uzavřenost na $\cdot \wedge -$ snadná (stačí vzít 1 ideál). $\square$

Věta 8.8

Buď R OHI. Pak R je gaussovský a platí v něm Bézoutova rovnost.

Důkaz
R OHI. Chceme 1) existuje NSD 2) neexistují řetězce vlastních dělitelů (zobecněná věta algebry):

1) $a, b \in R$. Buď $I = aR + bR$, (protože OHI) existuje $c \in R, cR = I$. $aR, bR \subseteq cR \implies c|a, b$. Buď $d|a, b \implies aR, bR \subseteq dR \implies aR + bR = cR \subseteq dR \implies d|c$. Tedy $c = \text{NSD}(a, b)$. Navíc $c \in aR + bR = \{ar + bs\}$, tj. $c = ar + bs$ pro nějaké $r, s \in R$.

2) Pro spor uvažujme takovou posloupnost dělitelů $\ldots |a_2|a_1$, tj. $a_1R \subset a_2R \subset \ldots$. $I = \bigcup_{i=1}^{\infty} a_iR$ je ideál, tj. (protože OHI) $I = bR$, pro nějaké $b \in I$. Ale tím pádem $\exists i : b \in a_iR$. Pak $bR \subseteq a_iR \subset a_{i+1}R \subset \ldots \subseteq I = bR$. $\lightning$. $\square$

9 Polynomy nad gaussovskými obory (bez důkazů)

Definice 9.1 (Primitivní polynom)

R obor, $f \in R[x]$ je primitivní, pokud jsou jeho koeficienty nesoudělné (čili $\forall c \in R$: pokud c dělí všechny koeficienty, pak $c||1$).

Věta 9.1 (Gaussovo lemma)

R gaussovský obor, f, g primitivní polynomy v $R[x]$ $\implies$ $f \cdot g$ primitivní v $R[x]$.

Tvrzení 9.2

R je gaussovský, Q podílové těleso R. f, g primitivní polynomy v $R[x]$. Pak $f|g$ v $R[x] \Leftrightarrow f|g$ v $Q[x]$.

Definice 9.2 (Značení)

$f = \sum_{i=0}^{n} a_i x^i \in R[x], a_n \neq 0$ (R gaussovský). $c(f) = \mathrm{NSD}(a_0, a_1, \ldots, a_n)$ je obsah (content) polynomu.

$PP(f) = \frac{1}{c(f)} \cdot f$ je primitivní část (primitive part) f.

Věta 9.3

R gaussovský, Q podílové těleso, $f, g \in R[x]$. Pak:

$\exists\, \mathrm{NSD}_{R[x]}(f, g) = c{\cdot}h, c = \mathrm{NSD}_R(c(f), c(g)), h \in R[x]$ je primitivní tak, že $h = \mathrm{NSD}_{Q[x]}(f, g)$.

f je ireducibilní v $R[x] \Leftrightarrow \deg f = 0$ a f je ireducibilní v R, nebo $\deg f > 0$, f je primitivní a f je ireducibilní v $Q[x]$.

Věta 9.4 (Gaussova)

R gaussovský obor $\implies R[x]$ gaussovský obor.

Důsledek
R gaussovský $\implies R[x_1, \ldots, x_n]$ gaussovský $\implies R[x_1, x_2, x_3, \ldots]$ gaussovský.

9.1 Ireducibilita polynomů (i s důkazy)

Tvrzení 9.5 (Existence racionálního kořene)

Nechť R je gaussovský, Q je podílové těleso. Má-li $f = \sum_{i=1}^{n} a_i x^i \in R[x]$, $a_n \neq 0$ kořen $\frac{r}{s} \in Q$ (pro $\mathrm{NSD}(r, s) = 1$), pak $r|a_0, s|a_n$.

Důkaz
$0 = f\left(\frac{r}{s}\right) = \sum a_i \left(\frac{r}{s}\right)^i$ přenásobíme s^n: $0 = a_0 s^n + a_1 r s^{n-1} + \ldots + a_n r^n \implies r|a_0 s^n$. Ale $\mathrm{NSD}(r, s) = 1$, tedy z gaussovskosti $r|a_0$. Stejně tak $s|a_n r^n \implies s|a_n$. □

Tvrzení 9.6 (Einsteinovo kritérium)

R obor, $f = \sum_{i=0}^{n} a_i x^i \in R[x]$ primitivní, $a_n \neq 0$. Pokud existuje prvočinitel $p \in R$ tak, že $p|a_0, a_1, \ldots, a_{n-1}, p^2 \nmid a_0$, pak f je ireducibilní.

Důkaz
Pro spor $f = g \cdot h$, $g = \sum_{i=0}^{k} b_i x^i$, $h = \sum_{i=0}^{l} c_i x^i \in R[x]$, l, k > 0.

$a_0 + a_1 x + a_2 x^2 + \ldots = (b_0 + b_1 x + \ldots)(c_0 + c_1 x + \ldots) = b_0 c_0 + (b_0 v_1 + b_1 c_0)x + \ldots \implies a_0 = b_0 c_0$.

Tudíž $p | a_0 = b_0 c_0 \implies$ BÚNO $p | b_0$, pak $p \not| c_0$, neboť $p^2 \not| a_0$. $p | a_1 = b_0 c_1 + b_1 c_0 \implies p | b_1$, ..., $p | b_i \; \forall i \leq n-1$. p dělí všechny koeficienty b_i pro $i \leq k \leq n-1$, ale jelikož h má stupeň alespoň 1, tak p dělí všechny koeficienty b_i, tj. $p | g | f$. ↯. □

10 Čínská zbytková věta a interpolace

Věta 10.1 (ČZV pro polynomy)

$\mathbb{T}$ těleso. Ať $m_1, m_2, \ldots, m_n \in \mathbb{T}[x]$ jsou po 2 nesoudělné polynomy, $d = \sum \deg m_i$. Ať $u_1, \ldots, u_n \in \mathbb{T}[x]$. Pak $\exists! f \in \mathbb{T}[x]$ stupně $< d$ tak, že $f \equiv u_1 \mod m_1, \ldots, f \equiv u_n \mod m_n$.

Důkaz
Jednoznačnost: Ať f, g jsou řešení, $\deg f, \deg g < d$, čili $f \equiv g \equiv u_i \mod m_i \forall i$. Tedy $m_i | f - g \forall i$. m_i jsou po dvou nesoudělné a $\mathbb{T}[x]$ je gaussovské, tj. $m_1 \cdot \ldots \cdot m_n | f - g$, tj. $\deg(f - g) > d$ (↯) nebo $f - g = 0$.

Existence: $P_k = \{f \in T[x] | \deg f < k\}$ je vektorový prostor nad $\mathbb{T}$ dimenze k (x^i je báze). $d_i = \deg m_i$. $\varphi : P_d \to P_{d_1} \times \ldots \times P_{d_n}$, $f \mapsto (f \mod m_1, \ldots, f \mod m_n)$. Zřejmě P_{d_i} má dimenzi d_i a φ je dobře definované a navíc homomorfismus vektorových zobrazení. Navíc z jednoznačnosti (1. bodu důkazu) je prosté, tj. z porovnání dimenzí je φ bijekce. Tedy hledaný polynom je $\varphi^{-1}(u_1 \mod m_1, \ldots, u_n \mod m_n)$. □

Důsledek (Věta o interpolaci)
$\mathbb{T}$ těleso. Mějme po 2 různé body $a_1, \ldots, a_n \in \mathbb{T}$ a libovolné hodnoty $u_1, \ldots, u_n \in \mathbb{T}$. $\exists! f \in \mathbb{T}[x], \deg f < n$ tak, že $\forall i : f(a_i) = u_i$.

Důkaz
$f \equiv f(a)(\mod x - a)$ (už jsme ukázali), tedy $f \equiv u_i(\mod x - a_i)$ a použijeme čínskou zbytkovou větu. □

Důsledek (Zobrazení na konečných tělesech jsou polynomiální)
$\mathbb{T}$ je konečné těleso. Pro $\forall \varphi : \mathbb{T} \to \mathbb{T}$ zobrazení $\exists! f \in \mathbb{T}[x]$, $\deg f < |\mathbb{T}|$ tak, že $\varphi(a) = f(a)$.

11 Faktorokruh modulo polynom

Definice 11.1 (Faktorokruh)

$\mathbb{T}$ těleso. Buď $m \in \mathbb{T}[\alpha]$ polynom stupně $n \geq 1$. Faktorokruh $\mathbb{T}[\alpha]/(m)$ je množina všech polynomů z $T[\alpha]$ stupně $< n$ se standardním $+$ a $-$ a s operací násobení modulo m, čili $f \odot g = f \cdot g \mod m$.

Čili $\mathbb{T}[\alpha]/(m) = (\{f \in \mathbb{T}[\alpha] | \deg f < n\}, +, -, \odot, 0, 1)$.

Pozorování
Jde o komutativní okruh s 1. (Ověříme axiomy.)

Tvrzení 11.1 (Faktor podle ireducibilního polynomu)

$\mathbb{T}$ těleso, $m \in \mathbb{T}[\alpha], \deg m \geq 1$. Pak následující je ekvivalentní: 1) $T[\alpha]/(m)$ je těleso, 2) $T[\alpha]/(m)$ je obor, 3) m je ireducibilní prvek v $\mathbb{T}[\alpha]$.

Důkaz
$1 \implies 2$ zřejmé (jedno z prvních tvrzení), $2 \implies 3$: Ať $m = fg$ pro $f, g \in \mathbb{T}[\alpha]$, $\deg f, \deg g \geq 1$. Pak v $\mathbb{T}[\alpha]/(m)$ platí $f \odot g = fg \mod m = m \mod m = 0$, čili $\mathbb{T}[\alpha]/(m)$ není obor.

$3 \implies 1$: Buď $f \neq 0$ polynom, $\deg f < \deg m$. m ireducibilní, f má menší stupeň než $m \implies m, f$ jsou nesoudělné. Bézout: $1 = \text{NSD}(f, m) = uf + vm$ pro nějaké $u, v \in T[\alpha]$. Buď $\tilde{u} = u \mod m$. Pak v $\mathbb{T}[\alpha]/(m)$ platí: $\tilde{u} \odot f = \tilde{u}f \mod m \equiv uf \equiv 1(\mod m)$. Tedy $\tilde{(u)} \odot f = 1$ v $\mathbb{T}[\alpha]/(m)$. Tedy $\tilde{u}$ je inverz. □

Poznámka
Dál budeme $\odot$ značit jako $\cdot$.

11.1 Kořenová, rozkladová nadtělesa

Tvrzení 11.2

$\mathbb{T}$ těleso, $f \in \mathbb{T}[x]$, $\deg f \geq 1$. Pak existuje $S \geq T$, ve kterém ma f kořen.

Důkaz

Buď $m = \sum_{i=0}^{n} a_i x^i \in \mathbb{T}[x]$ nějaký ireducibilní dělitel f. $S = T[\alpha]/(m(\alpha))$. Z předchozího tvrzení je S tělesso a $S \geq T$ (neboť $\mathbb{T}$ jsou tam konstantní polynomy). Chceme $m(x)$ má v S kořen (pak má triviálně i f kořen v S).

$$m(\alpha) = \sum a_i \odot (\alpha \odot \ldots \odot \alpha) = \sum (a_i \alpha^i \mod m) =$$

$$= a_0 \mod m + a_1\alpha \mod m + \ldots + a_n\alpha^n \mod m = a_0 + a_1\alpha + \ldots + a_{n-1}\alpha^{n-1} + (-a_0 - a_1\alpha - \ldots - a_{n-1}\alpha^{n-1}$$

□

Věta 11.3

$\mathbb{T}$ *těleso,* $f \in \mathbb{T}[x]$, $\deg f \geq 1$. *Pak existuje těleso* $S \geq T$, *kde se* f *rozkládá na součin polynomů stupně 1.*

Důkaz

Indukcí podle f. $\deg f = 1 \implies f = ax + b$ a má kořen $-a^{-1}b \in \mathbb{T}$.

$\deg f > 1$. Podle předchozího tvrzení buď $U \geq T$ tak, že $f(u) = 0$ pro nějaké $u \in U$. Pak $f = (x - u) \cdot g$ pro nějaké $g \in U[x]$, $\deg g = \deg f - 1$. Následně použijeme indukční předpoklad pro g. □

Definice 11.2

$\mathbb{T}$ těleso, $f \in \mathbb{T}[x]$, $\deg f \geq 1$. Kořenové nadtěleso je (libovolné) těleso $\mathbb{S} \geq \mathbb{T}$, ve kterém existuje $a \in \mathbb{S}$ tak, že $\mathbb{S} = \mathbb{T}(a)$ a $f(a) = 0$.

Rozkladové nadtěleso f je (libovolné) těleso $\mathbb{S} \geq \mathbb{T}$, že existují $a_1, \ldots, a_n \in \mathbb{S} : \mathbb{S} = \mathbb{T}(a_1, \ldots, a_n)$ a $f || (x - a_1) \cdot \ldots \cdot (x - a_n)$.

Důsledek (Existence kořenového a rozkladového nadtělesa)
$\mathbb{T}$ těleso, $f \in [x]$, $\deg \geq 1$. Pak existuje kořenové i rozkladové nadtěleso f nad $\mathbb{T}$.

Důkaz

$\exists \mathbb{S} \geq \mathbb{T}$ tak, že $f(a) = 0$ pro $a \in \mathbb{S}_0$. Kořenové nadtěleso pak je $\mathbb{S} = \mathbb{T}(a) \leq \mathbb{S}_0$. Obdobně rozkladové. □

12 Konečná tělesa

Pozorování (Konečná tělesa)
Nechť $\mathbb{T} = \mathbb{Z}_p[\alpha]/(m)$, kde p je prvočíslo, m ireducibilní polynom v $\mathbb{Z}_p[\alpha]$, $\deg m = k$.

Potom $\mathbb{T}$ je těleso s p^k prvky. Značíme ho $\mathbb{F}_{p^k}$ (podle dalšího pozorování je jediné této mohutnosti).

Pozorování (Vlastnosti konečných těles)

- $\forall k\ \forall p$ prvočíslo $\exists$ ireducibilní polynom stupně k v $\mathbb{Z}_p[\alpha] \implies \exists$ konečné těleso velikosti p^n.
- Každé konečné těleso lze takto zkonstruovat.
- Na volbě m (daného stupně) nezáleží.

Důkaz
Bez důkazu. □

Poznámka
Díky pozorování, že nad konečným tělesem je každá funkce polynomiální a že posloupnost jedniček je vlastně $\mathbb{F}_{2^k}$, stačí v kryptografii zkoumat jen polynomy.

Navíc násobení na tomto tělese používá symetrická šifra AES (advanced encryption standard), která počítá s maticemi 4×4 nad $\mathbb{F}_{256}$.

Poznámka
Další využití je v konečné geometrii, např. eliptické křivky jsou Diofantické rovnice tvaru $y^2 = x^3 + ax + b$ nad $\mathbb{F}_{p^k}$ (řešení tvoří grupu a dělá se s tím něco jako v RSA).

12.1 Sdílení tajemství

Definice 12.1

(k, n)-schéma sdílení tajemství je situace, kdy se n lidí dělí o tajemství a k odhalení je potřeba alespoň (libovolných) k z nich.

Definice 12.2 (Tajemství)

Za tajemství budeme uvažovat posloupnost 0 a 1, na kterou se budeme dívat v $\mathbb{Z}_2^m$ nebo $\mathbb{F}_{2^m}$.

Poznámka
Pro $k = n$ se (k, n)-schéma nazývá maskování hodnot: Pro každého člověka vyberu hodnotu $a_i \in T$ a zveřejním hodnotu $c = t + \sum_{i=1}^{n} a_i$. ($t$ je tajemství.)

Definice 12.3 (Shamirův protokol)

Vlastník zvolí polynom $f \in \mathbb{T}[x]$, $\deg f < k$ tak, že $f(0) = t$. Vyberu n po dvou různých prvků $0 \neq a_1, \ldots, a_n \in \mathbb{T}$, které se zveřejní, a jednotlivým účastníkům se dá $f(a_1), \ldots, f(a_n)$.

Když se potká k lidí, tak mají k hodnot polynomu, tedy mohou polynom interpolovat a zjistit konstantní člen, tj. $f(0) = t$.

13 Symetrické polynomy

Definice 13.1

R komutativní okruh. Polynom $f \in R[x_1, \ldots, x_n]$ je symetrický, pokud po libovolném permutování proměnných se f nezmění. (formálně: $f(x_1, \ldots, x_n) = f(x_{\pi(1)}, \ldots, x_{\pi(n)})$ pro každou permutaci $\pi \in S_n$.)

Tvrzení 13.1 (Viétovy vztahy)

$\mathbb{T}$ těleso, $f = \sum a_i x^i \in \mathbb{T}[x]$, $\deg f = n \geq 1$. Ať $f = a_n(x - u_1) \cdot \ldots \cdot (x - u_n)$ v nějakém nadtělese $\mathbb{S} \geq \mathbb{T}$. Pak

$$\frac{a_{n-i}}{a_n} = (-1)^i s_i(u_1, \ldots, u_n) = \sum_{j_1 < j_2 < \ldots < j_i} x_{j_1} \cdot \ldots \cdot x_{j_i}.$$

Důkaz
Berme $g = a_n^{-1} f$. Z rovnosti

$$(y - x_1) \cdot \ldots \cdot (y - x_n) = y^n - s_1 y^{n-1} + \ldots + (-1)^n s_n$$

dostaneme

$$g = \sum \frac{a_i}{a_n} x^i = (x - u_1) \cdot \ldots \cdot (x - u_n) = x^n + \sum_{i=1}^{n} (-1)^i s_i(u_1, \ldots, u_n) x^{n-i}.$$

Porovnáním koeficientů dostaneme chtěnou rovnost. □

Věta 13.2 (Základní věta o symetrických polynomech)

Buď R obor, $f \in R[x_1, \ldots, x_n]$ symetrický polynom. Pak $\exists! g \in R[z_1, \ldots, z_n]$ tak, že $f = g(s_1, \ldots, s_n)$.

Důkaz
Později. $\square$

Definice 13.2 (Term)

Term v proměnných $x_1, \ldots, x_n$ je výraz $x_1^{k_1} x_2^{k_2} \ldots x_n^{k_n}, k_i \in \mathbb{N}_0$.

Definice 13.3 (Uspořádání termů)

Relaci $<$ na termech definujeme jako $x_1^{k_1} \ldots x_n^{k_n} < x_1^{l_1} \ldots x_n^{l_n}$, pokud $\exists i \geq 0$ tak, že $k_1 = l_1, k_2 = l_2, \ldots, k_i = l_i, k_{i+1} < l_{i+1}$.

Definujeme $t \leq s$, pokud $t = s \vee t < s$.

Lemma 13.3

Relace $\leq$ má vlastnosti: 1) Je to lineární uspořádání. 2) Pro libovolné termy $t_1 > t_2$, $s_1 > s_2$ platí $t_1 s_1 > t_2 s_2$. 3) Neexistuje ∞ klesající řetězec termů $t_1 > t_2 > \ldots$

Důkaz
Domácí cvičení. $\square$

Definice 13.4 (Vedoucí člen polynomu)

R obor, $f \in R[x_1, \ldots, x_n]$. Vedoucí člen f je ten člen, který má největší term. Značí se $l(f)$.

Lemma 13.4

R obor, $f, g \in R[x_1, \ldots, x_n]$. Pak 1) $l(fg) = l(f) \cdot l(g)$. 2) Je-li f symetrický a $l(f) = a \cdot x_1^{k_1} \ldots x_n^{k_n}$, potom $k_1 \geq k_2 \geq \ldots \geq k_n$.

Důkaz
1) $l(f), l(g)$ jsou největší členy v f, g. Podle předchozího lemmatu víme, že $>$ se zachovává násobením $\implies$ $l(f) \cdot l(g)$ je největší ze všech členů v fg. Navíc R je obor $\implies$ koeficient v $l(f) \cdot l(g)$ není nulový.

2) Kdyby $k_i < k_j$ pro $i < j$, mohli bychom prohodit proměnné x_i, x_j. Ze symetrie f je $a \cdot x_1^{k_1} \ldots x_i^{k_j} \ldots x_j^{k_i} \ldots x_n^{k_n}$ je taktéž v f, ale je větší než $l(f)$, což je spor. $\square$

Lemma 13.5

$k_1 \geq k_2 \geq \ldots \geq k_n$ nezáporná celá. Pak $\exists!$ $(l_1, \ldots, l_n)$ nezáporné celé tak, že $l(s_1^{l_1} \ldots s_n^{l_n}) = x_1^{k_1} \cdot \ldots \cdot x_n^{k_n}$.

Důkaz

$$l(s_1^{l_1} \cdot \ldots \cdot s_n^{l_n}) = l(s_1)^{l_1} \cdot \ldots \cdot l(s_n)^{l_n} = x_1^{l_1} \cdot (x_1x_2)^{l_2} \cdot \ldots \cdot (x_1x_2 \ldots x_n)^{l_n} = x_1^{l_1+l_2+\ldots+l_n} \cdot \ldots \cdot x_n^{l_n}.$$

Tedy řeším systém $l_1 + \ldots l_n = k_1$, $l_2 + \ldots + l_n = k_2$, ..., $l_n = k_n$, tj. $l + n = k_n \geq 0$, $l_i = k_i - k_{i+1} \geq 0$. □

Definice 13.5 (Gaussův algoritmus)

R obor, vstup $f \in R[x_1, \ldots, x_n]$ symetrický, výstup $g \in R[z_1, \ldots, z_n]$ tak, že $g(s_1, \ldots, s_n) = f$.

$f_1 = f$, $g_1 = 0$.

$i = 1, 2, 3, \ldots$: dělej: Najdi $l_1, \ldots, l_n$ tak, že $l(f_i) = c \cdot l(s_1^{l_1} \cdot \ldots \cdot s_n^{l_n})$ pro nějaké $c \in R$ podle předchozího lemmatu. $f_{i+1} = f_i - c \cdot s_1^{l_1} \cdot \ldots \cdot s_n^{l_n}, g_{i+1} = g_i + c \cdot z_1^{l_1} \cdot \ldots \cdot z_n^{l_n}$. Pokud je f_{i+1} konstantní, zastavím se a vrátím $g_{i+1} + f_{i+1}$.

Důkaz
Ověříme, že f_i je symetrický polynom – zřejmé z definice f_i. $g_i \in R[z_1, \ldots, z_n]$ – jasné z definice g_i. $f_i + g_i(s_1, \ldots, s_n) = f$ – vidíme, nebo ověříme indukcí. A skončí, jelikož zmenšujeme vedoucí člen a neexistuje nekonečná klesající posloupnost. □

Důkaz (Základní věta o symetrických polynomech)
Existenci dokazuje Gaussův algoritmus. Jednoznačnost: Ať $f = g_1(s_1, \ldots, s_n) = g_2(s_1, \ldots, s_n)$, $g_1 \neq g_2$. $g = g_1 - g_2 = \sum a_i t_i$, kde t_i jsou po dvou různé jednotlivé termy (v proměnných z_i), $a_i \neq 0$. $t_i(s_1, \ldots, s_n)$ mají různé vedoucí členy podle lemmatu výše. Vezměme lexikograficky největší z vedoucích členů $t_i(s_1, \ldots, s_n)$. Ten je tedy striktně větší než ostatní, tedy $\sum a_i t_i(s_1, \ldots, s_n) \neq 0$, tudíž $0 = g(s_1, \ldots, s_n) - g_2(s_1, \ldots, s_n)$. □

Důsledek (Hodnota symetrického polynomu na kořenech)
$\mathbb{T}$ těleso, $f \in T[x]$, $\deg f \geq 1$. Buď $\mathbb{U} \geq \mathbb{T}$ nadtěleso, kde $f||(x - u_1) \cdot \ldots \cdot (x - u_n)$. $\forall$ symetrický polynom $s \in T[x_1, \ldots, x_n$ platí: $s(u_1, \ldots, u_n) \in \mathbb{T}$.

Důkaz
$f = \sum a_i x^i$. Viétovy vztahy $s_i(u_1, \ldots, u_n) = (-1)^i \frac{a_{n-i}}{a_n} \in \mathbb{T}$. Z předchozí věty $\exists g \in \mathbb{T}[z_1, \ldots, z_n$ tak, že $f = g(s_1, \ldots, s_n) \implies f(u_1, \ldots, u_n) = g(s_1(u_1, \ldots, u_n), \ldots, s_n(u_1, \ldots, u_n)) \in \mathbb{T}$. □

14 Základní věta algebry

Věta 14.1 (Základní věta algebry)

Každý komplexní polynom stupně ≥ 1 má kořen.

Důsledek

$$\forall f \in \mathbb{C}[x], \deg f \geq 1 : f||(x-u_1)\cdot \ldots \cdot (x-u_n).$$

Důsledek

Každý polynomiální zobrazení $\mathbb{C} \to \mathbb{C}$ je na.

Důkaz (Jeden z mnoha, nejvíce algebraický)

Lemma: předpokládejme, že každý reálný polynom stupně ≥ 1 má (komplexní) kořen. Pak má každý komplexní polynom stupně ≥ 1 nějaký kořen.

Důkaz: $f \in \mathbb{C}[x], \deg f \geq 1, f = \sum a_i x^i$. $\overline{f} = \sum \overline{a_i} x^i$. Uvažujme $g = f \cdot \overline{f} = \sum_k \left(\sum_{i+j=k} a_i \overline{a_j}\right) x^k$. Ten má pro $i = j$ reálný koeficient a pro $i \neq j$ má koeficienty $a_i\overline{a_j} + \overline{a_i}a_j \in \mathbb{R}$. Buď $z \in \mathbb{C}$ kořen g. Potom $f(z) = 0$ (OK) nebo $\overline{f}(z) = 0$ (tj. $f(\overline{z}) = 0$, OK).

Lemma: Komplexní polynom stupně 2 má komplexní kořen. Důkaz $\frac{-b\pm\sqrt{b^2-4a\cdot c}}{2} \in \mathbb{C}$. (Jediný zádrhel je odmocnina, ale existenci odmocniny z komplexního čísla ukážeme přes exponenciální tvar.)

Lemma: Reálný polynom lichého stupně má kořen. Důkaz: Vynechán (věta o střední hodnotě a spojitost polynomů).

Díky 1. lemmatu stačí, že $\forall f \in \mathbb{R}[x], \deg f \geq 1$, má kořen v $\mathbb{C}$. $\deg f = n = 2^k m, m$ liché. Indukcí podle k: $k = 0 \implies f$ má lichý stupeň, tedy tvrzení je splněno díky přdchozímu lemmatu.

Ať $k \geq 1$. Ať $S \geq \mathbb{C}$ je nadtěleso, ve kterém $f||(x-u_1)\cdot\ldots\cdot(x-u_n)$ (díky větě z dřívějška). Chceme $\exists i : u_i \in \mathbb{C}$. Trik. Vezmeme $a \in \mathbb{Z}$ a definujeme $h_a = \prod_{i<j}(x - (u_i + v_j + a \cdot u_i \cdot u_j)) \in S[x]$. Chceme $h_a \in \mathbb{R}[x]$. $\tilde{h}_a = \prod_{i<j}(x - (y_i + y_j + a \cdot y_i \cdot y_j)) \in (\mathbb{Z}[x])[y_1, \ldots, y_n]$ je symetrický polynom v proměnných $y_1, \ldots, y_n$ (s koeficienty ze $\mathbb{Z}[x]$).

Z věty výše $\exists g_a \in (\mathbb{Z}[x])[z_1, \ldots, z_n]$ tak, že $\tilde{h}_a = g_a(s_1, \ldots, s_n)$. Dosadíme $y_i = u_i$: $h_a = \tilde{h}_a(u_1, \ldots, u_n) = g_a(s_1(u_1, \ldots, u_n), \ldots)$. Z viétových vztahů $s_1(u_1, \ldots, u_n), \ldots, s_n(u_1, \ldots, u_n) \in \mathbb{R}$. Tedy h_a je polynom v $\mathbb{R}[x]$. $\deg h_a = \binom{n}{2} = 2^{k-1} \cdot (m \cdot (2^k \cdot m - 1))$, takže má menší mocninu dvojky ve stupni, tedy aplikujeme IP. Proto má h_a kořen v $\mathbb{C}$, tudíž $\forall a \in \mathbb{Z}\ \exists i < j : u_i + u_j + au_iu_j$, tedy nějaká dvojice i, j se vyskytne nekonečněkrát (a je nekonečně, dvojic je konečně). Stačí, že $\exists a \neq b : u_i + u_j + au_iu_j \in \mathbb{C}$ a $u_i + u_j + bu_iu_j \in \mathbb{C}$, tudíž $(a-b)v_i \cdot u_j \in \mathbb{C}$ a $c = u_i + u_j \in \mathbb{C}$. Tedy u_i, u_j jsou kořeny $x^2 - cx + (u_iu_j) \in \mathbb{C}[x]$, tedy podle 3. lemmatu existuje kořen $x \in \mathbb{C}$, tj. $u_i \in \mathbb{C}$ nebo $u_j \in \mathbb{C}$. $\square$

15 Grupy

Definice 15.1 (Grupa, abelovská grupa)

Grupa je čtveřice $(G, *, ', e)$, kde G je množina (tzv. nosná), $*$ je binární operace na G, $'$ je unární operace (a' je tzv. inverzní prvek k a) a $e \in G$ (tzv. jednotka) tak, že $\forall a, b, c \in G$:

$$a * (b * c) = (a * b) * c, \qquad a * e = e * a = a, \qquad a * a' = a' * a = e.$$

Jestliže $\forall a, b \in G : a * b = b * a$, pak je grupa abelovská (čili komutativní).

Poznámka
Existují 2 zápisy: aditivní $(G, +, -, 0)$ (typicky abelovská) a multiplikativní $(G, \cdot, ^{-1}, 1)$.

Definice 15.2 (Podgrupa)

Ať $(G, *, ', e)$ je grupa, $H \subseteq G$ podmnožina. Pokud je H uzavřené na operace, čili $e \in H, \forall a, b \in H : a * b \in H, a' \in H$, pak H je podgrupa G. Značíme $H \leq G$.

$G, \{e\}$ jsou nevlastní podgrupy, ostatní jsou vlastní.

Například (Symetrická grupa)
X neprázdná množina, ($S_X :=$ {permutace na X}, operace $\circ$ skládání, $^{-1}$ inverzní, id_X) je symetrická grupa. Pokud je $X = \{1, 2, \ldots, n\}$, pak značíme $S_n := S_X$.

15.1 Vlastnosti permutací

Definice 15.3 (Cyklus)

Cyklus je posloupnost $a_1, \ldots, a_k \in X$ navzájem různých prvků přičemž $\pi(a_1) = a_2, \pi(a_2) = a_3, \ldots, \pi(a_k) = a_1$. Cyklus značíme $(a_1 a_2 \ldots a_k)$.

Definice 15.4 (Rozklad na cykly)

Rozklad na cykly je zápis $(a_{11} a_{12} \ldots a_{1k_1})(a_{21} \ldots a_{2k_2}) \ldots (a_{m1} \ldots a_{mk_m})$, kde a_{ij} jsou po dvou různé prvky. Cykly délky 1 typicky nepíšeme.

Každá permutace na konečné množině jde (jednoznačně) rozložit na cykly.

Definice 15.5 (Transpozice)

Transpozice je cyklus délky 2.

Každá permutace (X konečná, stejně jako kdekoliv dále) jde napsat jako složení transpozic.

Definice 15.6 (Sudá a lichá permutace, znaménko)

Sudá permutace je ta permutace, kterou lze rozložit na sudý počet transpozic. Jinak je permutace lichá.

Znaménko permutace $\operatorname{sgn}\pi = 1$ pokud je daná permutace sudá, jinak $\operatorname{sgn}\pi = -1$. $\operatorname{sgn}(\pi^{-1}) = \operatorname{sgn}\pi$. $\operatorname{sgn}\pi = (-1)^{n-m} = (-1)^{m_0}$, kde m je počet cyklů a m_0 je počet sudých cyklů (n počet prvků v množině).

Definice 15.7 (Konjugované)

$\pi, \sigma \in S_n$ jsou konjugované, pokud $\exists \varrho \in S_n : \sigma = \varrho \circ \pi \circ \varrho^{-1}$.

Tvrzení 15.1

π, σ jsou konjugované, právě když mají stejný počet cyklů každé délky.

Důkaz
Viz skripta. □

Například (Permutační grupy)
Permutační grupy = podgrupy S_n: Alternující grupa $A_n \leq S_n$ jsou všechny sudé permutace $n \geq 2$. Digedrální grupa $D_{2n} \leq S_n$ jsou všechny symetrie pravidelného n-úhelníku.

$|S_n| = n!$, $|A_n| = \frac{n!}{2}$, $|D_{2n}| = 2n$.

Například (Geometrické grupy)
D_{2n}, E_n (euklidovská grupa – symetrie $\mathbb{R}^n$), symetrie projektivního prostoru.

Například (Maticové grupy)
$GL_n(\mathbb{T})$ je grupa regulárních matic $n \times n$ nad $\mathbb{T}$, $SL_n(\mathbb{T})$ je grupa podgrupa regulárních matic s $\det = 1$, $O_n(\mathbb{T})$ je grupa ortogonálních matic, čili $A \cdot A^T = I_n$.

Například (Okruhové grupy)
R okruh. $(R, +, -, 0)$ je aditivní grupa okruhu R (je ablovská), pokud je navíc R (komutativní) okruh s 1 a R^* množina všech invertibilních prvků, pak $(R^*, \cdot, ^{-1}, 1)$ je multiplikativní grupa okruhu R.

Například (Komplexní jednotky)
$(\{z \in \mathbb{C} \mid |z| = 1\}, \cdot, ^{-1}, 1)$ a její podgrupy tzv. cyklotomické grupy $\mathbb{C}_n = \{\text{kořeny } x^n - 1\} = \{\zeta_n^j | j \in [n]\}$, kde $\zeta_n = e^{2\pi i/n}$.

Priferova p-grupa $\mathbb{C}_{p^\infty} = \bigcup_{k=1}^{\infty} \mathbb{C}_{p^k}$.

Definice 15.8 (Direktní součin grup)

Direktní součin grup $(G_i, *_i, '_i, e_i)$, $i \in [n]$, je grupa $\prod G_i = G_1 \times \ldots \times G_n = \{(a_1, \ldots, a_n) | a_i \in G_i\}$, kde operace $*, ', e$ jsou definovány „po složkách“:

$$(a_1, \ldots, a_n) * (b_1, \ldots, b_n) = (a_1 *_1 b_1, \ldots, a_n *_n b_n), \qquad (a_1, \ldots, a_n)' = (a_1^{'1}, \ldots), \qquad e = (e_1, \ldots, e_n).$$

Pro $G_1 = \ldots = G_n = G$ jde o direktní mocniny G^n.

Tvrzení 15.2 (Základní vlastnosti grup)

$(G, *, ', e)$, $a, b, c \in G$:

$$a * c = b * c \implies a = b,$$

$$a * c = a \implies c = e,$$

$$(a')' = a, \qquad (a * b)' = b' * a'.$$

15.2 Mocniny a řád prvku

Definice 15.9 (Mocnina prvku)

G grupa, $a \in G$, $n \in \mathbb{Z}$.

$$a^n = \begin{cases} 1 & n = 0 \\ \underbrace{a \cdot a \cdot \ldots \cdot a}_{n\times} & n > 0 \\ \underbrace{a^{-1} \cdot a^{-1} \cdot \ldots \cdot a^{-1}}_{n\times} & n < 0 \end{cases}.$$

Tvrzení 15.3

G grupa, $a, b \in G$, $k, l \in \mathbb{Z}$. Pak $a^{k+l} = a^k \cdot a^l$, $a^{k \cdot l} = (a^k)^l = (a^l)^k$. Pokud je navíc G abelovská, potom $(ab)^k = a^k b^k$.

Důkaz
Pro $k, l > 0$ je to jasné: $a^{k+l} = \underbrace{a \cdot a \cdot \ldots \cdot a}_{k+l} = \underbrace{a \cdot a \cdot \ldots \cdot a}_{k} \cdot \underbrace{a \cdot a \cdot \ldots \cdot a}_{l} = a^k \cdot a^l$. Když $k = 0$ nebo $l = 0$, pak je to ještě jasnější. $k > 0, l < 0, k + l > 0$ a podobně rozebereme každé zvlášť.

Zbytek analogicky. $\square$

Definice 15.10 (Řád grupy)

Řád grupy G je počet prvků nosné množiny G (tj. $|G|$), resp. ∞.

Řád prvku $a \in G$ je nejmenší $n \in \mathbb{N}$ tak, že $a^n = 1$ (pokud neexistuje, pak ∞). Značíme $\mathrm{ord}(a)$.

Tvrzení 15.4 (Řád permutace)

Řád permutace $\pi \in S_n$ je nejmenší společný násobek délek cyklů π.

Důkaz
Cyklus délky k má zřejmě řád k. Pro disjunktní cykly $C_1, \ldots, C_m$ máme $\pi = (C_1 \circ \ldots \circ C_m)^k$. Protože jsou disjunktní, tak je to to samé jako $C_1^k \circ \ldots \circ C_m^k$. Tedy $\pi^k = \mathrm{id} \Leftrightarrow C_1^k = \mathrm{id}, \ldots, C_m^k = \mathrm{id} \Leftrightarrow k$ je násobek délek všech cyklů. Tedy $\mathrm{ord}\,\pi = \min k = \mathrm{NSN}(\ldots)$. $\square$

16 Grupy

Lemma 16.1

Průnik podgrup je podgrupa.

Důkaz
G grupa, $H_i \leq G$ pro $i \in I$. $H = \bigcup_{i \in I} H_i \subseteq G$. H je uzavřené na operace: jednoduché ověřit. $\square$

Definice 16.1

Buď $X \subseteq G$ podmnožina G. Podgrupa generovaná množinou X je nejmenší (vzhledem k inkluzi) podgrupa G, která obsahuje X. Značíme $\langle X \rangle_G$.

Důkaz
$\langle X \rangle_G = \bigcap \{H \leq G | X \subseteq H\}$. $\square$