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)

$\mathbb{Z}[i] = \{a + bi | a, b \in \mathbb{Z}\}$ 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^{-1} 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 $n \geq 0$, $a_1, \dots, a_n \in R$ a $a_n \neq 0$ vyjma $n = 0$. $a_1, \dots, a_n$ 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 $R\,[x]$)

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

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

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 $x_1, x_2, \dots, x_m$ nad okruhem R je polynom v proměnné x_m nad okruhem $R[x_1, \dots, x_{m-1}]$.

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

Každý $f \in R[x_1, \dots, x_m]$ 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
$\Longleftarrow$: $f = (x - a) \cdot g$ pro nějaké $g \in R[x] \implies f(a) = (a - a) \cdot g(a) = 0$.

$\implies$: 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 $(x-a)^{n+1} \nmid f$.

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, $a \in S$. 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 $f = a_0 + a_1 x + \ldots + a_n x^n \in \mathbb{Z}[x], f \neq 0$ nazvěme číslo $|a_0| + |a_1| + \ldots + |a_n| + n \in \mathbb{N}$. 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 $a = p_1^{k_1} \cdot \dots \cdot p_n^{k_n}$. 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 $p \nmid a$, tedy chceme, aby $p|b$. p je prvočíslo, tudíž nemá vlastní dělitele $\implies$ $\text{NSD}(p, a) =$ 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 $< a$. $\lightning$. □

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 ($a \equiv b \pmod{m}$), 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)

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

$$a + c \equiv b + d \pmod{m}, \qquad a - c \equiv b - d \pmod{m}, \qquad a \cdot c \equiv b \cdot d \pmod{m},$$

$$a^k \equiv b^k \pmod{m}, k \in \mathbb{N}, \qquad c \neq 0 \implies a \equiv b \mod m \Leftrightarrow ac \equiv bc \pmod{mc},$$

$$\text{NSD}(c, m) = 1 \implies a \equiv b \pmod{m} \Leftrightarrow ac \equiv bc \pmod{m}.$$

Důkaz
Z definice rozepsáním.

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

$$cu + mv = 1, cu = 1 - mv \implies$$

$$\implies (ac \equiv bc \pmod{m} \Leftrightarrow a \equiv a(1 - mv) \equiv auc \equiv buc \equiv b(1 - mv) \equiv b \pmod{m}).$$

□

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 $\{k \in [m] | \operatorname{NSD}(k,m) = 1\}$. $\varphi(m) = |\Phi_m|$.

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:

$\implies$: f zobrazí Φ do $\Phi_a \times \Phi_b$, čili, že $\mathrm{NSD}(x, a \cdot b) = 1$ implikuje $\mathrm{NSD}(x \mod a, a) = 1, \mathrm{NSD}(x \mod b, b) = 1$.

$\impliedby$: 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 $\Phi_{a,b}$.

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

□

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

$\implies$: $a = 0 \implies b = 0$. 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)

$a, b, m \in R : a \equiv b \bmod m$, 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 $\mathbb{Z}[\sqrt{s}]$)
Dokáže se uzavřenost. □

Definice 6.4

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

Tvrzení 6.2

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

1. $\nu(u \cdot v) = \nu(u) \cdot \nu(v)$,
2. $\nu(u) = 1 \Leftrightarrow u$ *je invertovatelné.*

3. Pokud $u|v$ a $v \nmid u$, pak $\nu(u)|\nu(v)$ (víme z 1)) a $\nu(u) \neq \nu(v)$.

Důkaz
1) vezmu a ověřím. Nebo využiji, že $\nu(u) = |u \cdot u'|$, 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) $\Longleftarrow: u \cdot u^{-1} = 1 \implies \nu(u \cdot u^{-1}) = \nu(1) = 1$. Následně už z 1) dostaneme $\nu(u) = 1$. $\implies: \nu(u) = 1 \implies u \cdot u' = 1 \implies u'$ je hledaná inverze.

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

Pozor
Norma nesplňuje trojúhelníkovou nerovnost!

Tvrzení 6.3 (Dělení Gaussových čísel se zbytkem)

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

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. $\nu(\delta) \leq \left(\frac{\sqrt{2}}{2}\right)^2 |\beta|^2 < 1 \cdot \nu(\beta)$. $\square$

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 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) $\forall d|a, d|b : d|c$.

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

Definice 6.6 (Nesoudělnost)

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

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

6.4 Ireducibilní prvky a rozklady

Definice 6.7 (Vlastní dělitel a ireducibilní prvek)

R obor. $a \in R \setminus \{0\}$. $b \in R$ je vlastní dělitel a, pokud $b|a$ a $b \nparallel 1$ a $b \nparallel a$.

$a \neq 0$ je ireducibilní, pokud $a \nparallel 1$ a nemá žádné vlastní dělitele.

Definice 6.8 (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 $p_i \nparallel p_j$, 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 6.9 (Prvočinitel)

R obor, pak $p \in R, p \nparallel 1$ 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 $\forall a \in R, a \neq 0, a \not\| 1$, 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 $\exists c : a = b \cdot c$. $c = q \cdot r^{-1} \cdot p_1^{k_1 - l_1} \cdot \ldots \cdot p_n^{k_n - l_n}$.

$\Longrightarrow: b|a \implies \exists c : a = b \cdot c$. 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 shodné ireducibilní prvky, ale $k_i \neq 0 \vee l_i \neq 0$).

Ať $a, b \neq 0$, potom existuje jednoznačný rozklad na ireducibilní. 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 $\nu(a) = k_1 + \ldots + k_n$. Jelikož máme jednoznačný ireducibilní rozklad, tak $\ni$ je dobře definovaná. Pokud $b|a$, pak $\nu(b) \leq \nu(a)$, pokud navíc $b \not\| a$, pak $\nu(b) < \nu(a)$. Posloupnost $\nu(a_i)$ je pak nekonečná klesající posloupnost v $\mathbb{N}$. ↯ $\square$

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* $a_1, a_2, a_3, \ldots \in R : a_{i+1} | a_i \wedge a_i \nparallel a_{i+1}$.

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

Důkaz (Existence rozkladů)
Sporem s druhou částí: Ať $a_1 = a$, $a_1 \nparallel 1$ a a nemá ireducibilní rozklad. Mějme $a_i \nparallel 1$ a nemá ireducibilní rozklad. Tedy není ireducibilní (jinak by bylo samo sobě rozkladem) $\implies a_i = b \cdot c$ pro nějaké $b, c \nparallel 1$. 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 $a_{i+1} | a_i \wedge a_{i+1} \nparallel 1 \wedge a_{i+1}$ nemá IR. Indukcí tedy vyrobíme nekonečnou posloupnost, kterou mi podmínky zakazují. $\lightning$. $\square$

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. $\square$

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 $\implies p | b$. $\square$

Důkaz (Jednoznačnost rozkladu)
Sporem: Mezi všemi prvky s nejednoznačnými rozklady vyberme ten, který má nejkratší ireducibilní 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. $\square$

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 $\nu : R \to \mathbb{N}_0$ tak, že $\nu(0) = 0$, $a|b \wedge b \neq 0 \implies \nu(a) \leq \nu(b)$, $\forall a, b \in R, b \neq 0\ \exists q, r \in R : a = bq + r \wedge \nu(r) < \nu(b)$.

Pozorování
$a = 0 \Leftrightarrow \nu(a) = 0$. (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…

Lemma 8.2

R eukleidovský obor, $a, b \in R \setminus \{0\}$. Pokud $a|b$ a $a \nmid b$, pak $\nu(a) < \nu(b)$.

Důkaz
Ať $b = a \cdot u$ pro nějaké $u \in R$. Víme, že $\exists q, r \in R$, $a = bq + r$, $\nu(r) < \nu(b)$. $a \nparallel b \implies b \nmid a \implies r \neq 0$. $r = a - bq = a(1 - uq) \implies a|r$. Z definice dělení se zbytkem je $\nu(a) \leq \nu(r) < \nu(b)$. $\square$

Věta 8.3

Eukleidovské obory jsou gaussovské.

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

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. □

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. $\mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right]$ 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
$\implies$: 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. $I = R = 1R$.

$\Rightarrow$: $aR = R = 1R$, $(a \neq 0)$, čili a je invertibilní. $\square$

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) $a, b \in I \cap J, r \in R$ $\implies$ $a, b \in I, a, b \in J$. 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 $bR \subseteq a_iR \subset a_{i+1}R \subset \ldots \subseteq I = bR$. ↯. □

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). $c(f) = \text{NSD}(a_0, a_1, \ldots, a_n)$ 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:

$$\exists\, \text{NSD}_{R[x]}(f, g) = c \cdot h, c = \text{NSD}_R(c(f), c(g)), h \in R[x]$$

je primitivní tak, že $h = \text{NSD}_{Q[x]}(f, g)$. 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 $\implies$ $R[x_1, \dots, x_n]$ gaussovský $\implies$ $R[x_1, x_2, x_3, \dots]$ 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 $s|a_n r^n \implies s|a_n$. $\square$

Tvrzení 9.6 (Eisensteinovo 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 $p|a_0, a_1, \dots, a_{n-1}, p^2 \nmid a_0$, 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 $p \nmid c_0$, neboť $p^2 \nmid a_0$. $p|a_1 = b_0 c_1 + b_1 c_0 \implies p|b_1$, ..., $p|b_i$ $\forall i \leq n-1$. 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. $p|g|f$. $\lightning$. $\square$

10 Čínská zbytková věta a interpolace

Věta 10.1 (ČZV pro polynomy)

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

Důkaz

Jednoznačnost: Ať f, g jsou řešení, $\deg f, \deg g < d$, čili $f \equiv g \equiv u_i \bmod m_i \forall i$. 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

$f \equiv f(a) \pmod{x - a}$ (už jsme ukázali), tedy $f \equiv u_i \pmod{x - a_i}$ 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 $f \odot g = f \cdot g \bmod m$.

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 $f \odot g = fg \bmod m = m \bmod m = 0$, 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: $1 = \mathrm{NSD}(f, m) = uf + vm$ pro nějaké $u, v \in T[\alpha]$. Buď $\tilde{u} = u \bmod m$. Pak v $\mathbb{T}[\alpha]/(m)$ platí: $\tilde{u} \odot f = \tilde{u}f \bmod m \equiv uf \equiv 1 \pmod m$. 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 $S \geq \mathbb{T}$ (neboť $\mathbb{T}$ jsou tam konstantní polynomy). Chceme $m(\alpha)$ má v S kořen (pak má triviálně i f kořen v S). Dosazujeme $\alpha \in \mathbb{T}[\alpha]/m(\alpha)$.

$$m(\alpha) = \sum a_i \odot (\alpha \odot \ldots \odot \alpha) = \sum (a_i \alpha^i \mod m) =$$
$$= a_0 \bmod m + a_1\alpha \bmod m + \ldots + a_n \alpha^n \bmod m =$$
$$= a_0 + a_1\alpha + \ldots + a_{n-1}\alpha^{n-1} + (-a_0 - a_1\alpha - \ldots - a_{n-1}\alpha^{n-1}) = 0.$$

□

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. $\square$

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. $\square$

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

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

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. □

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. □

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 $a \cdot x_1^{k_1} \dots x_i^{k_j} \dots x_j^{k_i} \dots x_n^{k_n}$ je taktéž v f, ale je větší než $l(f)$, což je spor. □

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

$$l(s_1^{l_1} \cdot \ldots \cdot s_n^{l_n}) = l(s_1)^{l_1} \cdot \ldots \cdot l(s_n)^{l_n} = x_1^{l_1} \cdot (x_1 x_2)^{l_2} \cdot \ldots \cdot (x_1 x_2 \ldots x_n)^{l_n} = x_1^{l_1 + l_2 + \ldots + l_n} \cdot \ldots \cdot x_n^{l_n}.$$

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, $f \in \mathbb{T}[x]$, $\deg f \geq 1$. Buď $\mathbb{U} \geq \mathbb{T}$ nadtěleso, kde $f || (x - u_1) \cdot \ldots \cdot (x - u_n)$. $\forall$ symetrický polynom $s \in \mathbb{T}[x_1, \ldots, x_n]$ 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

$$s = g(s_1, \ldots, s_n) \implies s(u_1, \ldots, u_n) = g(s_1(u_1, \ldots, u_n), \ldots, s_n(u_1, \ldots, u_n)) \in \mathbb{T}.$$

$\square$

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
Každé 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 $\forall a \in \mathbb{Z} \; \exists i < j : u_i + u_j + a u_i u_j$, tedy nějaká dvojice i, j se vyskytne nekonečněkrát (a je nekonečně, dvojic je konečně). Stačí, že $\exists a \neq b : u_i + u_j + a u_i u_j \in \mathbb{C}$ a $u_i + u_j + b u_i u_j \in \mathbb{C}$, 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 $x^2 - cx + (u_i u_j) \in \mathbb{C}[x]$, 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

$$\mathbb{C}_n = \{\text{kořeny } x^n - 1\} = \left\{\zeta_n^j | j \in [n]\right\}, \qquad \zeta_n = e^{2\pi i/n}.$$

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 $\prod G_i = G_1 \times \ldots \times G_n = \{(a_1, \ldots, a_n) | a_i \in G_i\}$, grupa, kde operace $*, ', e$ jsou definovány „po složkách“:

$$(a_1, \ldots, a_n) * (b_1, \ldots, b_n) = (a_1 *_1 b_1, \ldots, a_n *_n b_n), \qquad (a_1, \ldots, a_n)' = (a_1', \ldots),$$

$$e = (e_1, \ldots, e_n).$$

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. □

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 $\mathrm{ord}\,\pi = \min k = \mathrm{NSN}(\ldots)$. □

16 Podgrupy

Lemma 16.1

Průnik podgrup je podgrupa.

Důkaz

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

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

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

Tvrzení 16.2

G grupa, $\emptyset \neq X \subseteq G$. Pak

$$\langle X \rangle_G = [a_1^{k_1} \cdot \ldots \cdot a_n^{k_n} | n \in \mathbb{N}_0, a_1, \ldots, a_n \in X, k_1, \ldots, k_n \in \mathbb{Z}].$$

Pozor

a_i nemusí být různé.

Vyjádření typicky není jednoznačné.

Důkaz
$M =$ množina napravo. Chceme M je podgrupa, $M \supseteq X$, M je nejmenší podgrupa.

1. $(a_1^{k_1} \cdot \ldots \cdot a_n^{k_n}) \cdot (b_1^{l_1} \cdot \ldots \cdot b_m^{k_m}) \in M$. $(a_1^{k_1} \cdot \ldots \cdot a_n^{k_n})^{-1} = a_n^{-k_n} \cdot \ldots \cdot a_1^{-k_1} \in M$. $1 \in M$ (pro $n = 1$ nebo $k_i = 0$).

2. $a \in X \implies a^1 \in M$. 3. Buď $H \leq G$, $H \supseteq X$. $\forall a \in X : a \in H \implies \forall k \in \mathbb{Z} : a^k \in H$. $a_1, \ldots, a_n \in X \implies a_1^{k_1}, \ldots \in H \implies a_1^{k_1} \cdot \ldots \in H \implies M \subseteq H$. □

Poznámka (Značení)

$$\langle\{b_1, \ldots, b_m\}\rangle_G \equiv \langle b_1, \ldots, b_m\rangle_G .$$

Důsledek
G grupa $a \in G$. $\langle a\rangle_G = \left\{a^k | k \in \mathbb{Z}\right\}$.

Důsledek
G abelovská grupa, $a_1, \ldots, u_n \in G$. $\langle u_1, \ldots, u_n\rangle_G = \left\{u_1^{k_1} \cdot \ldots \cdot u_n^{k_n} | k_i \in \mathbb{Z}\right\}$.

Tvrzení 16.3 (Generátory permutačních grup)

1. Grupa S_n je generovaná množinou všech transpozic (viz Lingebra).

2. Grupa A_n je generována množinou všech trojcyklů.

Tvrzení 16.4 (Řád prvku a řád podgrupy)

G je grupa, $a \in G$. Pak $\operatorname{ord} a = |\langle a\rangle_G|$.

Důkaz
Z minulého tvrzení $\langle a\rangle_G = \left\{a^k | k \in \mathbb{Z}\right\}$. $a^i = a^j \Leftrightarrow a^{i-j} = 1 \Leftrightarrow \operatorname{ord} a | i - j$ nebo $i - j = 0$ pro $\operatorname{ord} a = \infty$. Pro $\operatorname{ord} a = \infty$ je tvrzení jasné, pro $\operatorname{ord} a = n < \infty$ víme, že $a^i = a^j \Leftrightarrow n | i - j \Leftrightarrow i \equiv j \mod n$. Pak $\langle a\rangle_G = \{a^0, a^1, \ldots, a^{n-1}\}$, tj. $|\langle a\rangle_G| = n = \operatorname{ord} a$. □

16.1 Lagrangeova věta

Věta 16.5

G grupa, $H \leq G$. Pak $|H|$ dělí $|G|$.

Definice 16.2 (Rozkladové třídy, transverzála, index podgrupy)

$H \leq G$. Množiny $aH = \{a \cdot b | b \in H\}$ pro $a \in G$ nazýváme rozkladové třídy podgrupy H.

Podmnožina $T \subseteq G$ s vlastností $|T \cap aH| = 1$ pro $\forall a \in G$ se nazývá transverzála rozkladu G podle H.

Počet různých rozkladových tříd se nazývá index podgrupy H v grupě G a značí se $[G : H] = |\{aH | a \in G\}|$.

Poznámka

Někdy se těmto definicím říká levá transverzála a levá rozkladová třída. Pravé by se definovaly symetricky. Index je shodný (viz dále).

Lemma 16.6 (Disjunktnost rozkladových tříd)

$H \leq G$. $\forall a, b \in G : aH = bH$ *nebo* $aH \cap bH = \emptyset$.

Důkaz

Ať $aH \cap bH \neq \emptyset$. Buď $c \in aH \cap bH$. Tedy $c = ah_1 = bh_2$ pro nějaké $h_1, h_2 \in H$. Vezmeme $ah \in aH$ a máme $ah = ch_1^{-1}h = bh_2h_1^{-1}h \in bH$. Symetricky $bh \in aH$, tedy $aH = bH$. □

Důsledek

Mohutnost transverzály se rovná mohutnosti množiny rozkladových tříd.

Lemma 16.7 (Velikost rozkladových tříd)

$H \leq G$. *Pro* $\forall a \in G : |aH| = |H|$.

Důkaz

Zobrazení $f : G \to G$, $x \mapsto ax$ je prosté: $ax = ay \implies x = y$. $f(H) = aH$, tedy $f|_H$ je bijekce mezi H a aH. Tedy $|H| = |aH|$. □

Věta 16.8 (Lagrangeova věta podruhé)

$H \leq G$. *Pak* $|G| = |H| \cdot [G : H]$.

Důkaz

Buď T nějaká transverzála. Pak $G = \bigcup_{a \in T} aH$ je disjunktní sjednocení podle lemmatu výše. Tedy

$$|G| = \sum_{a \in T} |aH| = \sum_{a \in T} |H| = |H| \cdot |T| = |H| \cdot [G : H].$$

□

Důsledek
G grupa, $a \in G$. Pak $\operatorname{ord} a \mid |G|$.

Poznámka
Z Lagrangeovy věty plyne Eulerova věta.

Tvrzení 16.9 (Rovnost rozkladových tříd)

$H \leq G$. $\forall a, b \in G$ platí $aH = bH \Leftrightarrow a^{-1}b \in H$. $Ha = Hb \Leftrightarrow ab^{-1} \in H$.

Důkaz
$\Longrightarrow$: $aH = bH \ni b = b \cdot 1$, čili $b \in aH$, tedy $b = ah$ pro nějaké $h \in H$. Pak $a^{-1}b = h \in H$.

$$\Longleftarrow : a^{-1}b = h \text{ pro nějaké } h \in H \implies b \cdot 1 = a \cdot h \in aH \cap bH \implies aH = bH.$$

Analogicky pro pravé. □

Důsledek
Levých a pravých rozkladových tříd je stejně, neboť zobrazení $aH \to Ha^{-1}$ je bijekce.

16.2 Loydova patnácka (nebude se zkoušet)

Místo prázdného políčka uvažujme 16. Každý stav hry lze popsat permutací $\pi \in S_{16}$. Tah je přechod z π do $\pi \circ (ij)$, kde $\pi(i) = 16$.

Pozorování
Každý tah změní znaménko permutace.

Definice 16.3 (Invariant pro L. 15)

$I(\pi) = \operatorname{sgn}(\pi) \cdot (-1)^{d(\pi)}$, kde $d(pi)$ je Newyorská vzdálenost prázdného pole od pravého dolního rohu.

Důkaz (Invariant)
Tah změní $\operatorname{sgn} \pi$ i $d(\pi)$. □

Věta 16.10

Loydova 15 je řešitelná $\Leftrightarrow I(\pi) = 1$.

Důkaz

$\Longrightarrow$: Zřejmé (z toho, že je $I(\pi)$ invariant a na konci má být $I = 1$). $\Longrightarrow$: BÚNO $\pi(16) = 16$. Dívejme se tedy na $\pi \in A_{15}$. Potom pomocí $\pi \circ (5, 6, 7, 8, 11, 10, 9)$ (dolní obdélníček 2×4), $\pi \circ (1, 2, 3, 4, 7, 6, 5)$ (prostřední obdélníček), $\pi \circ (9, 10, 11, 12, 15, 14, 13)$ (dolní obdélníček). Toto už generuje A_{15} (cvičení). □

17 Grupové homomorfismy

17.1 Základní vlastnosti

Definice 17.1

$G = (G, \cdot, ^{-1}, 1), H = (H, *, ', e)$ jsou grupy. Zobrazení $\varphi : G \to H$ je homomorfismus grup, pokud $\forall a, b \in G : \varphi(a \cdot b) = \varphi(a) * \varphi(b)$, $\varphi(a^{-1}) = \varphi(a)'$, $\varphi(1) = e$.

Lemma 17.1

G, H jsou grupy jako výše, $\varphi : G \to H$ zobrazení. Pak φ je homomorfismus $\Leftrightarrow \varphi(a \cdot b) = \varphi(a) * \varphi(b)$.

Důkaz

$\Longleftarrow$: $\varphi(1) \stackrel{?}{=} e$: $e * \varphi(1) = \varphi(1) = \varphi(1 \cdot 1) = \varphi(1) * \varphi(1)$. Zkrátíme $\varphi(1)$ na obou stranách $\Longrightarrow$ $e = \varphi(1)$.

$\varphi(a) * \varphi(a)' = e = \varphi(1)' = \varphi(a \cdot a^{-1}) = \varphi(a) * \varphi(a^{-1})$. Zkrátíme $\varphi(a)$ a dostáváme $\varphi(a^{-1}) = \varphi(a)'$.

$\Longrightarrow$: triviální □

Definice 17.2 (Obraz a jádro homomorfismu)

$\varphi : G \to H$ homomorfismus. Obraz φ je jeho obor hodnot, čili množina:

$$\mathrm{Im}(\varphi) = \{\varphi(a) | a \in G\} \subseteq H.$$

Jádro φ je množina

$$\mathrm{Ker}(\varphi) = \{a \in G | \varphi(a) = e\} \subseteq G.$$

Tvrzení 17.2 (Jádro a obraz jsou podgrupy)

$\varphi : G \to H$ homomorfismus grup. Pak $\mathrm{Im}(\varphi) \leq H$ a $\mathrm{Ker}(\varphi) \leq G$.

Důkaz
$e = \varphi(1) \implies e \in \mathrm{Im}(\varphi)$. Pokud $\varphi(a), \varphi(b) \in \mathrm{Im}(\varphi)$, pak $\varphi(a)' = \varphi(a^{-1})' \in im(\varphi)$ a $\varphi(a) * \varphi(b) = \varphi(a \cdot b) \in \mathrm{Im}(\varphi)$.

$\varphi(1) = e \implies 1 \in \mathrm{Ker}(\varphi)$. Pokud $a, b \in \mathrm{Ker}\,\varphi$, pak $\varphi(a^{-1}) = \varphi(a)' = e' = e \implies a^{-1} \in \mathrm{Ker}(\varphi)$. $a \cdot b$ podobně. □

Tvrzení 17.3

$\varphi : G \to H$ homomorfismus grup. Pak φ je prosté $\Leftrightarrow$ $\mathrm{Ker}(\varphi) = \{1\}$.

Důkaz
$\implies$: Pro $a \neq 0$, prostota $\implies \varphi(a) \neq \varphi(1) = e \implies a \notin \mathrm{Ker}(\varphi)$.

$\impliedby$: $\varphi(a) = \varphi(b) \Leftrightarrow \varphi(a \cdot b^{-1}) = e \Leftrightarrow a \cdot b^{-1} \in \mathrm{Ker}(\varphi)$. Ale $\mathrm{Ker}(\varphi) = \{1\}$, tedy $a \cdot b^{-1} = 1 \implies a = b$. Tedy φ je prosté. □

Pozorování (Bez důkazu)
Homomorfismus je určený svými hodnotami na generátorech. Na rozdíl od LA však nelze volit libovolně.

Tvrzení 17.4 (Řád prvku a jeho obrazu)

$\varphi : G \to H$ homomorfismus. Pro $a \in G$ platí: $\mathrm{ord}_H(\varphi(a)) | \mathrm{ord}_G(a)$. ($\forall x : x | \infty$). Je-li φ prosté, pak $\mathrm{ord}(\varphi(a)) = \mathrm{ord}(a)$.

Důkaz
$\mathrm{ord}(a) = \infty$ zřejmé. Ať $\mathrm{ord}(a) = n \in \mathbb{N}$. Pak $\varphi(a)^n = \varphi(a^n) = \varphi(1) = e$. Tedy $\mathrm{ord}(\varphi(a)) | n$ (neboť vydělím n číslem $\mathrm{ord}(\varphi(a))$ se zbytkem a dostanu, že zbytek $= 0$).

Prostota: cvičení. □

Tvrzení 17.5

Mějme grupy G, H, K a homomorfismy $\varphi : G \to H, \psi : H \to K$. Pak $\psi \circ \varphi$ je homomorfismus $G \to K$. Je-li φ bijekce, pak $\varphi^{-1} : H \to G$ je homomorfismus.

Důkaz
Viz skripta. □

17.2 Izomorfismus

Definice 17.3 (Izomorfismus)

Bijektivní homomorfismus $\varphi : G \to H$ je izomorfismus.

Důsledek

Inverze k izomorfismu je izomorfismus.

Definice 17.4

Grupy G, H jsou izomorfní, pokud existuje izomorfismus $\varphi : G \to H$. Značíme $G \simeq H$.

Pozorování

Relace „být izomorfní" je ekvivalence na třídě všech grup.

Důkaz

Reflexivní (identita je izomorfismus), tranzitivní (tvrzení výše o homomorfismu a skládání bijekcí), reflexivní (dusledek výše). $\square$

Tvrzení 17.6 (Algebraická verze ČZV)

Mějme $m_1, \ldots, m_n$ po dvou nesoudělná přirozená čísla, $M = m_1 \cdot \ldots \cdot m_n$. Zobrazení $\varphi : \mathbb{Z}_M \to \mathbb{Z}_{m_1} \times \ldots \times \mathbb{Z}_{m_n}$, $a \mapsto (a \mod m_1, \ldots, a \mod m_n)$ je izomorfismus okruhů. Restrikce $\varphi|\mathbb{Z}_M^*$ je izomorfismus multiplikativních grup $\mathbb{Z}_M^* \to \mathbb{Z}_{m_1}^* \times \ldots \times \mathbb{Z}_{m_n}^*$.

Důkaz

$\varphi : \mathbb{Z}_M \to \mathbb{Z}_{m_1} \times \ldots \times \mathbb{Z}_{m_n}$ je bijekce, viz ČZV. Snadno se ověří, že je to homomorfismus pro operace $+$ i $\cdot$. $\square$

17.3 Neizomorfismus

Tvrzení 17.7

Buď $\varphi : G \to H$ surjektivní homomorfismus. Pokud $G = \langle X \rangle$, pak $H = \langle \varphi(X) \rangle$, kde $\varphi(X) = \{\varphi(a) | a \in X\}$.

Důkaz

Cvičení / skripta. $\square$

Pozor

Na rozdíl od VP generující množiny mohou být různě velké, např. $\mathbb{Z} = \langle 1 \rangle = \langle 3 \rangle$.

18 Cyklické grupy

18.1 Základy

Definice 18.1

Grupa G je cyklická, pokud je generovaná 1 prvkem, čili $G = \langle a \rangle_G$ pro nějaké $a \in G$.

Důsledek (Různých předchozích tvrzení)
$\langle a \rangle = \left\{a^k | k \in \mathbb{Z}\right\} \implies \langle a \rangle$ je abelovská (násobení je akorát sčítání mocnin).

$\operatorname{ord} a = |\langle a \rangle|$.

Věta 18.1 (Klasifikace cyklických grup)

G cyklická grupa. 1) Je-li G nekonečná, pak je izomorfní $(Z, +, -, 0)$. 2) Je-li G konečná řádu n, pak je izomorfní $(Z_n, +, -, 0)$.

Důkaz
1) $|G| = \infty$. Pak $G = \{\ldots, a^{-1}, a^0, a^1, a^2, \ldots\}$ (po dvou různé mocniny). Definujeme izomorfismus $\varphi : G \to Z$, $a^k \mapsto k$. Už víme, že je bijekce. Homomorfismus je to, protože $k + l = \varphi(a^k) + \varphi(a^l) = \varphi(a^k \cdot a^l) = \varphi(a^{k+l}) = k + l$.

2) $|G| = n$. $\varphi : G = \{1, a, \ldots, a^{n-1}\} \to Z_n$, $a^k \mapsto k$. To že je φ bijekce už víme, homomorfismus: $k + l \mod n = \varphi(a^k) + \varphi(a^l) \mod n = \varphi(a^k \cdot a^l) = \varphi(a^{k+l \mod n}) = k + l \mod n$. □

Tvrzení 18.2

Každá podgrupa cyklické grupy je cyklická.

Důkaz
$H \leq G = \langle a \rangle$. 1) $H = \{1\}$, pak je generována 1. 2) H obsahuje prvek a^l pro $l \neq 0$. Tedy $a^{l'} \in H$ pro $l' > 0$. Buď $k > 0$ nejmenší tak, že $a^k \in H$. Pak $H = \left\langle a^k \right\rangle$. Buď $a^n \in H$, vydělíme se zbytkem: $n = ki + j$, $0 \leq j < k$. Pak ale $a^k > a^j = a^{ki+j} \cdot a^{k(-i)} \in H$. Tudíž $a^k | a^n$ (když $a^j = 1$) nebo ↯. Tedy $H \subseteq \left\langle a^k \right\rangle$. A triviálně $\left\langle a^k \right\rangle \subseteq H$. □

Tvrzení 18.3 (Generátory podgrup)

$G = \langle a \rangle$. 1) $\left\langle a^k, a^l \right\rangle = \left\langle a^{\mathrm{NSD}(k,l)} \right\rangle$. 2) Je-li $|G| = n \in \mathbb{N}$, pak $\left\langle a^k \right\rangle = \left\langle a^{\mathrm{NSD}(k,n)} \right\rangle$.

Důkaz
1) $\subseteq$: jasný, neboť $\mathrm{NSD}(k,l)|k,l$. $\supseteq$: použijeme Bézoutovu rovnost, $\mathrm{NSD}(k,l) = kx + ly$. Tedy $a^{\mathrm{NSD}(k,l)} = \left(a^k\right)^x \cdot \left(a^l\right)^y \in \left\langle a^k, a^l \right\rangle$.

2) Volíme v 1) $l = n$. Víme, že $a^n = 1$, tedy

$$\left\langle a^{\mathrm{NSD}(k,n)} \right\rangle = \left\langle a^k, a^n \right\rangle = \left\langle a^k, 1 \right\rangle = \left\langle a^k \right\rangle.$$

□

Tvrzení 18.4 (Generátory cyklických grup)

$G = \langle a \rangle$. 1) $|G| = \infty$, pak generátory jsou právě a^1, a^{-1}. 2) $|G| = n$, pak generátory jsou právě a^k, kde $k \in \{1, \ldots, n\}$ a $\mathrm{NSD}(k,n) = 1$.

Důkaz
1) jasné (viz skripta). 2) Z tvrzení výše $\left\langle a^k \right\rangle = \left\langle a^{\mathrm{NSD}(k,n)} \right\rangle = H$, $H = G \Leftrightarrow \mathrm{NSD}(k,n) = 1$. $\implies$: Kdyby $d = \mathrm{NSD}(k,n) > 1$, pak $H = \left\langle c^d \right\rangle = \left\{1, a^d, \ldots, a^{d(\frac{n}{d}-1)}\right\} \neq G$. $\impliedby$: triviální. □

Tvrzení 18.5 (Řády prvků)

Cyklická grupa konečného řádu n obsahuje právě $\varphi(d)$ prvků řádu $d|n$. (A 0 řádu $d \nmid n$.)

Důkaz
G cyklická, $|G| = n$. Každý prvek řádu $d|n$ je generátor cyklické podgrupy řádu d. Víme, že taková podgrupa existuje v G právě 1, neboť podle tvrzení výše jsou všechny podgrupy tvaru $\left\langle a^k \right\rangle$ pro $k|n$ a taková podgrupa má řád n/k. Tedy b je generátor $\left\langle a^{n/d} \right\rangle$. Ta má podle předchozího tvrzení právě $\varphi(d)$ generátorů. □

Tvrzení 18.6

Pro $n \in \mathbb{N} : \sum_{d|n} \varphi(d) = n$.

Důkaz
Spočteme $|\mathbb{Z}_N|$ dvěma způsoby: 1) $|\mathbb{Z}_n| = n$. 2) $\mathbb{Z}_n = \bigcup_{d|n} \{b \in \mathbb{Z}_n | \operatorname{ord} b = d\}$. Tj. $|\mathbb{Z}_n| = \sum_{d|n} \varphi(d)$. □

18.2 Multiplikativní grupy konečných těles

Lemma 18.7

G konečná grupa taková, že $\forall k$ grupa G obsahuje nejvýše k prvků a: $a^k = 1$. Pak G je cyklická.

Důkaz
$n = |G|$. U_k = počet prvků řádu k v G. Lagrange $\implies U_k = 0$ pro $k \nmid n$. Spočtu prvky G podle řádů (jako v předchozím tvrzení): $n = \sum_{k|n} U_k$. Buď a prvek řádu k. $\langle a \rangle$ je cyklická řádu k a všechny prvky $b \in \langle a \rangle$ splňují $b^k = 1$. $\langle a \rangle$ obsahuje k takových prvků.

Předpoklad: G obsahuje nejvýše k prvků c tak, že $c^k = 1$. Tedy $c \in \langle a \rangle$. Speciálně každý prvek řádu k leží v $\langle a \rangle$ a je generátor $\langle a \rangle$. Z tvrzení výše $\langle a \rangle$ má $\varphi(k)$ generátorů $\implies U_k = \varphi(k)$. Tedy pro $k|n$ máme $U_k = 0$ nebo $\varphi(k)$.

$\sum_{k|n} \varphi(k) = n \leq \sum_{k|n} U_k \leq \sum_{k|n} \varphi(k)$. Tedy platí rovnost, tedy $U_k = \varphi(k) \forall k|n$. Speciálně $U_N = \varphi(n) > 1$ a existuje prvek řádu n a ten generuje G. □

Věta 18.8

Buď $\mathbb{T}$ těleso a G konečná podgrupa multiplikativní grupy $\mathbb{T}^*$. Pak G je cyklická.

Důkaz
Pro předchozí lemma chci G obsahuje nejvýše k prvků tak, že $a^k = 1$. Ale každé takové a je kořen polynomu $x^k - 1$. Nad tělesem $\mathbb{T}$ má $x^k - 1$ nejvýše $\deg(x^k - 1) = k$ kořenů. □

Důsledek
Speciálně $|\mathbb{T}| < \infty$, pak $\mathbb{T}^*$ je cyklické. Její generátory se nazývají primitivní prvky.

$\mathbb{T} = \mathbb{Z}_p \implies \mathbb{Z}_p^* = \{1, 2, \ldots, p-1\}$ je cyklická, čili existuje g tak, že

$$\mathbb{Z}_p^* = \left\{ g^0, g^1, \ldots, g^{p-2} \right\}.$$

18.3 Diskrétní logaritmus a kryptografie

Definice 18.2 (Diskrétní logaritmus a exponenciála)

$|G| = n$, zobrazení $G = \langle a \rangle = \{a_0, a_1, \ldots, a^{n-1}\} \xrightarrow{\cong} \mathbb{Z}_n, a^k \mapsto k$ je tzv. diskrétní logaritmus. Diskrétní exponenciála je pak $\mathbb{Z}_n \xrightarrow{\cong} G, k \mapsto a^k$.

Poznámka
Počítání diskrétní exponenciály je rychlé (rozdělení na mocniny 2), ale diskrétního logaritmu pomalé.

19 Působení grupy na množině

19.1 Abstraktní grupa jako grupa permutací

Definice 19.1 (Působení grupy na množině)

Působení grupy G na množině X je libovolný homomorfismus $\pi : G \to S_X$. Hodnotu permutace $\pi(g)$ na prvku $x \in X$ často značíme $g(x)$.

Důsledek
$\pi(1) = \mathrm{id}$, $\pi(g^{-1}) = \pi(g)^{-1}$, $(g \cdot h)(x) = g(h(x))$.

Věta 19.1 (Cayleyova representace)

Každou grupu jde vnořit do nějaké symetrické grupy. (Čili existuje homomorfismus $\varphi : G \to S_x$).

Důkaz
Dokonce vezmeme $X = G$. (Tedy pokud je G konečná, pak vnořujeme do $S_{|G|}$). Pro $a \in G$ uvažujeme levou translaci $L_a : G \to G, x \mapsto a \cdot x$. L_a je zřejmě permutace na G, neboť můžeme zinvertovat a. Zobrazení $G \to S_G$, $a \mapsto L_a$ je homomorfismus (čili také G působí na $X = G$), což snadno ověříme. □

Definice 19.2

Relace tranzitivity $\sim$ na X: $x \sim y$ pokud $\exists g \in G : g(x) = y$.

Lemma 19.2

$\sim$ je ekvivalence na X.

Důkaz
Cvičení / skripta. □

Definice 19.3 (Orbita)

Třídy ekvivalence $\sim$ se nazývají orbity.

Orbitu obsahující $x \in X$ značíme $[x] = \{y \in X | y \sim x\} = \{g(x) | g \in G\}$.

Definice 19.4 (Pevný bod, stabilizátor)

Bod $x \in X$ je pevný bod prvku $g \in G$, pokud $g(x) = x$.

Množinu všech pevných bodů $g \in G$ značíme $X_g = \{x \in X | g(x) = x\}$.

Stabilizátor prvku $x \in X$ je množina $G_x = \{g \in G | g(x) = x\}$.

Lemma 19.3

Stabilizátor G_x je podgrupa G.

Důkaz
$1 \in G_x$, neboť $1(x) = x$. $g, h \in G_x$, čili $g(x) = x, h(x) = x$, pak $(g \cdot h)x = g(h(x)) = g(x) = x \implies g \cdot h \in G_x$, $g^{-1}(x) = x \implies g^{-1} \in G_x$. □

Tvrzení 19.4 (Velikost orbity vs. index stabilizátoru)

$$\forall x \in X : |[x]| = [G : G_x].$$

Důkaz
Najdeme bijekci mezi $[x]$ a množinou $\{gG_x | g \in G\}$. Uvažujme $\varphi : \{gG_x | g \in G\} \to [x]$, $gG_x \mapsto g(x)$. $g(x) \in [x]$. Je φ vůbec dobře definovaná? $gG_x = hG_x \implies g(x) = h(x)$, neboť podle dřívějšího tvrzení $gG_x = hG_x \Leftrightarrow h^{-1}g \in G_x \Leftrightarrow h^{-1}g(x) = x \Leftrightarrow g(x) = h(x)$. Zároveň je φ prosté (díky zpětným implikacím v předchozím) a je na, neboť pro $g(x) \in [x]$ mám $g(x) = \varphi(gG_x)$. □

Důsledek (Spolu s lagrangeovou větou)

$$|G| = |G_x| \cdot [G : G_x] = |G_x| \cdot |[x]|.$$

19.2 Burnside

Věta 19.5 (Burnsideova)

Ať konečná grupa G působí na konečné množině X. Pak:

$$|X/\sim| = \frac{1}{|G|} \cdot \sum_{g \in G} |X_g|.$$

Důkaz
Nechť $M = \{(g, x) \in G \times X | g(x) = x\}$. Spočtu velikost M dvěma způsoby:

$$|M| = \sum_{g \in G} |X_g| = \sum_{x \in X} |G_x|.$$

$$\frac{1}{|G|} \cdot \sum_{g} |X_g| = \frac{1}{|G|} \cdot \sum_{x} |G_x| = \sum_{x \in X} \frac{1}{|[x]|} = \sum_{o \in X/\sim} \sum_{x \in o} \frac{1}{|o|} = \sum_{o \in X/\sim} 1 = |X/\sim|.$$

□

Definice 19.5 (Tranzitivní)

Buď G permutační grupa, čili $G \leq S_X$. G je tranzitivní, pokud má jenom 1 orbitu ve svém působení na X.

Věta 19.6 (Jordanova)

Každé konečná tranzitivní grupa G, $|G| \geq 2$, obsahuje aspoň 1 permutaci bez pevného bodu.

Důkaz

Burnside: počet orbit (= 1 z tranzitivity) = průměrný počet pevných bodů. id $\in G$ má $n \geq 2$ pevných bodů, tedy nadprůměrný počet. To znamená, že $\exists g \in G$, které má podprůměrný počet pevných bodů, tedy 0. $\square$

Věta 19.7 (Cauchyova)

Buď G konečná grupa a p prvočíslo tak, že $p \mid |G|$. Pak v G existuje prvek řádu p.

Důkaz

$X = \{(a_1, a_2, \ldots, a_p) \in G^p | a_1 a_2 \ldots a_p = 1\}$. Mohutnost X spočítáme tak, že víme, že $a_1, \ldots, a_{p-1}$ můžeme zvolit libovolně a následně dopočítáme $a_p = a_{p-1}^{-1} \ldots a_1^{-1}$, tedy $|X| = |G|^{p-1}$. Z_p působí na X rotací složek (0 je identita, 1 rotace o 1, …). $|[x]| \mid |Z_p| = p$, tudíž každá orbita má velikost 1 nebo p. Existuje orbita velikosti 1 a sice $(1, 1, \ldots, 1)$. Zároveň X je disjunktní sjednocení orbit, p dělí $|X| = |G|^p$. Tedy počet 1-prvkových orbit je kp pro nějaké $k \geq 1$, tudíž existuje alespoň $p - 1$ 1-prvkových orbit různých od $1, 1, \ldots, 1$.

Buď $(a_1, \ldots, a_p)$ tato jiná orbita. Pak $a_1 = a_2$, $a_2 = a_3$, …, tedy je tvaru $(a, a, \ldots, a) \in X$. Ale z definice X je $a^p = 1$, zároveň není $a = 1$, tedy $\operatorname{ord} a = p$. $\square$

20 Faktorgrupy

20.1 Normální podgrupy

Tvrzení 20.1

G je grupa, $H \leq G$. NTJE: 1) $aH = Ha$ $\forall a \in G$, 2) $aha^{-1} \in H$ pro každé $h \in H$, $a \in G$.

Definice 20.1 (Normální podgrupa)

Podgrupa H je normální v grupě G, pokud splňuje tyto podmínky. Značíme $H \trianglelefteq G$.

Důkaz

$\Longrightarrow$: Buď $h \in H$, $a \in G$. Víme: $ah \in aH = Ha \implies$ existuje $h' \in H$ tak, že $ah = h'a \implies aha^{-1} = h' \in H$.

$\Longleftarrow$: Dokážeme $aH \subseteq Ha$ (a analogicky $Ha \subseteq aH$). Buď $ah \in aH$. Pak $h' = aha^{-1} \in H$, a tedy $ah = h'a \in Ha$. $\square$

Například
$\{1\} \trianglelefteq G$ a $G \trianglelefteq G$. V abelovských grupách jsou všechny podgrupy normální. $SL_n(T) \trianglelefteq GL_n(T)$. Naopak $\{\mathrm{id}, (1\ 2)\} \ntrianglelefteq S_3$. Ale $A_n \trianglelefteq S_n$.

Tvrzení 20.2

Jádro homomorfismu je normální podgrupa.

Důkaz
Hom. $\varphi : G \to H$. $\operatorname{Ker}\varphi = \{g \in G | \varphi(g) = 1_H\} \leq G$. Buď $a \in G$, $k \in \operatorname{Ker}\varphi$. $aka^{-1} \in \operatorname{Ker}\varphi$, protože

$$\varphi(aka^{-1}) = \varphi(a)\varphi(k)\varphi(a)^{-1} = \varphi(a)\varphi(a)^{-1} = 1.$$

$\square$

20.2 Konstrukce faktorgrupy

Definice 20.2

G grupa, $N \trianglelefteq G$. Definujeme relaci na G: $a \sim b \Leftrightarrow ab^{-1} \in N$. $ab^{-1} \in N \Leftrightarrow Na = Nb \Leftrightarrow aN = bN$ (z normality). Třídy ekvivalence $[a] = aN = Na$.

Faktorgrupa G podle podgrupy N = množina těchto bloků = $\{aN | a \in G\}$ (neboli $G/\sim = \{[a] | a \in G\}$), kde operace jsou $[a] \cdot [b] = [ab]$, $[a]^{-1} = [a^{-1}]$ a neutrální prvek je $[1]$.

Důkaz (Operace jsou dobře definované a $G/\sim$ je fakt grupa)
Ať $[a] = [c]$, $[b] = [d]$. Potom $[ab] = [cd]$, protože $a \sim c$ a $b \sim d$, tedy $ac^{-1} \in N$ a $bd^{-1} \in N$, tudíž $ab(cd)^{-1} = abd^{-1}c^{-1} = (ac^{-1}) \cdot (c(bd^{-1})c^{-1}) \in N$. Obdobně pro $^{-1}$.

Ověříme axiomy grupy… $\square$

Věta 20.3

$\varphi : G \to H$ homomorfismus grup.

1) (věta o homomorfismu) Je-li $N \subseteq \operatorname{Ker}\varphi$ a $N \trianglelefteq G$, pak zobrazení $\psi : G/N \to H$, $[a] \mapsto \varphi(a)$ je dobře definované a je to grupový homomorfismus.

Důkaz
Dobře definované: $[a] = [b] \implies ab^{-1} \in N \implies ab^{-1} \in \operatorname{Ker}\varphi \implies \varphi(ab^{-1}) = 1$. Tedy $\varphi(a) = \varphi(b)$.

Homomorfismus: $\psi([a]) \cdot \psi([b]) = \varphi(a) \cdot \varphi(b) = \varphi(ab) = \psi([ab]) = \psi([a] \cdot [b])$. $\square$

2) (1. věta o isomorfismu) $G/\operatorname{Ker}\varphi \simeq \operatorname{Im}\varphi$.

Důkaz
Použiji 1) pro $N = \operatorname{Ker}\varphi$. $\psi : G/\operatorname{Ker} \to H$. ψ je prosté: $[a] = [b] \Leftrightarrow ab^{-1} \in \operatorname{Ker}\varphi \Leftrightarrow \varphi(ab^{-1}) = 1 \Leftrightarrow \varphi(a) = \varphi(b) \Leftrightarrow \psi([a]) = \psi([b])$. Když se na ψ dívám jenom jako na zobrazení $G/\operatorname{Ker}\varphi \to \operatorname{Im}\varphi \leq H$, tak je na. □

Tvrzení 20.4 (2. věta o isomorfismu)

$N \trianglelefteq G$. 1) $N \trianglelefteq H \trianglelefteq G$, pak H/N je normální podgrupa G/N.

2) Je-li $K \trianglelefteq G/N$, pak existuje $H \trianglelefteq G$ tak, že $K = H/N$.

3) $N \trianglelefteq H \trianglelefteq G$, pak $(G/N)/(H/N) \simeq G/H$.

(Tvrzení 1) i 3) platí i pro podgrupy, které nejsou normální.)

Důkaz
1) se ověří.

2) $K \trianglelefteq G/N \implies K = H/N$ pro nějaké H, a sice $H = \{a \in G | [a] = aN \in K\}$. Ověří se, že $K = H/N$.

3) 1. věta o isomorfismu: Uvažujme homomorfismus $\varphi : G/N \to G/H$, $aN \mapsto aH$. Ověříme, že je dobře definován: $aN = bN \Leftrightarrow ab^{-1} \in N \implies ab^{-1} \in H \Leftrightarrow aH = bH$ a že je to homomorfismus: $\varphi(aN \cdot bN) = \varphi(abN) = (ab)H \stackrel{?}{=} \varphi(aN) \cdot \varphi(bN) = aH \cdot bH = (ab)H$. $\operatorname{Im}\varphi = G/H$ zřejmě, $\operatorname{Ker}\varphi = \{aN | \varphi(aN) = aH = 1 \cdot H\}$, ale $aH = 1 \cdot H \Leftrightarrow a \cdot 1^{-1} = a \in H$. Tedy $\operatorname{Ker}\varphi = H/N$. □

Tvrzení 20.5 (3. věta o isomorfismu)

$N \trianglelefteq G$, $H \leq G$. Pak HN je podgrupa G. $H \cap N \trianglelefteq H \wedge HN/N \simeq H/(H \cap N)$.

Důkaz
Bez důkazu (jednoduchý). □

20.3 Řešitelné grupy

Definice 20.3 (Řešitelná grupa, stupeň řešitelnosti)

Grupa G je řešitelná, pokud $\exists k \in \mathbb{N}$ a normální podgrupy $N_0, N_1, \ldots, N_k \trianglelefteq G$ tak, že $\{1\} = N_0 \leq N_1 \leq \ldots \leq N_k = G$ a každá faktorgrupa N_i/N_{i-1}, pro $i \in [k]$, je abelovská.

Nejmenší k, pro které tento řetězec v G existuje, se nazývá stupeň řešitelnosti G.

Definice 20.4 (Metaabelovská grupa)

Grupa stupně řešitelnosti 2 se nazývá metaabelovská.

Věta 20.6 (Feit-Thompson)

Každá grupa lichého řádu je řešitelná.

Jednodušší varianta: Každá grupa řádu p^k (p prvočíslo) je řešitelná.

Důkaz

Extrémně těžký. $\square$

Definice 20.5 (Derivovaná podgrupa)

G grupa. Její derivovaná podgrupa je $G' = \langle aba^{-1}b^{-1} | a, b \in G \rangle$.

Lemma 20.7

$N \trianglelefteq G$. 1) $N' \trianglelefteq G$. 2) G/N je abelovská $\Leftrightarrow G' \leq N$.

Důkaz

1) ověří se (viz skripta). 2) G/N abelovská $\Leftrightarrow [a][b] = [b][a] \Leftrightarrow [aba^{-1}b^{-1}] = [1] \Leftrightarrow aba^{-1}b^{-1} \in N \Leftrightarrow G' \subseteq N$. $\square$

Tvrzení 20.8 (Řešitelnost podgrup a faktogrup)

G grupa. 1) G řešitelná a $H \leq G \implies H$ řešitelná.

2) G řešitelná, $K \trianglelefteq G \implies G/K$ řešitelná.

3) Pokud $\exists N \trianglelefteq G$ tak, že N je řešitelná a G/N je řešitelná, pak je G řešitelná.

Důkaz

1) $N_i \trianglelefteq G$, $\{1\} = N_0 \leq N_1 \leq \ldots \leq N_k = G$, N_i/N_{i-1} abelovská. Uvažujme $\{1\} = N_0 \cap H \leq N_1 \cap H \leq \ldots \leq N_k \cap H = H$, dokážeme, že tato posloupnost prokazuje řešitelnost H. Triviálně $N_i \cap H \trianglelefteq H$. $(N_i \cap H)/(N_{i-1} \cap H) = (N_i \cap H)/((N_i \cap H) \cap N_{i-1})$. Podle 3. věty o isomorfismu je to isomorfní s $N_{i-1}(N_i \cap H)/N_{i-1} \leq N_i/N_{i-1}$, která je abelovská, tedy i její podgrupa je abelovská, tedy $(N_i \cap H)/(N_{i-1} \cap H)$ je abelovská.

2) analogicky (2. a 3. věta o isomorfismu). 3. podobně (nezkouší se, viz skripta). $\square$

Důsledek

G grupa s normálními podgrupami $N_0, \ldots, N_k$ tak, že $\{1\} = N_0 \leq N_1 \leq \ldots \leq N_k = G$ a N_i/N_{i-1} jsou řešitelné. Pak G je řešitelná.

Důkaz
Indukcí podle k a použitím třetího bodu předchozího tvrzení. □

21 Číselná tělesa a kořeny polynomů

21.1 Okruhové homeomorfismy a faktorokruhy

Tvrzení 21.1 (Obraz a jádro)

R, S okruhy, $\varphi : R \to S$ homomorfismus okruhů. 1) $\operatorname{Im} \varphi$ *je podokruh S. 2)* $\operatorname{Ker} \varphi$ *je ideál v R.*

Důkaz
1) $\varphi(a) + \varphi(b) = \varphi(a + b) \in \operatorname{Im} \varphi$. $\varphi(a) \cdot \varphi(b) = \varphi(a \cdot b) \in \operatorname{Im} \varphi$.

2) $\operatorname{Ker} \varphi$ je uzavřené na + (ověří se). Také je uzavřené na násobení R: $a \in \operatorname{Ker} \varphi, r \in R \implies \varphi(ra) = \varphi(r) \cdot \varphi(a) = \varphi(r) = 0$. □

Tvrzení 21.2

$\varphi : R \to S$ je prostý homomorfismus okruhů $\Leftrightarrow \operatorname{Ker} \varphi = \{0\}$.

Tvrzení 21.3

$\varphi : R \to S, \psi : S \to T$ homomorfismy okruhů. Pak 1) $\psi \circ \varphi : R \to T$ je homomorfismus okruhů.

2) Je-li φ bijekce (čili φ je isomorfismus), pak $\varphi^{-1} : S \to R$ je homomorfismus okruhů (a tedy isomorfismus).

21.2 Faktorokruh podle ideálu

Definice 21.1

R okruh, I ideál v R. Definujeme ekvivalenci na R $a \sim b \Leftrightarrow a - b \in I$.

Uvažujme jenom grupu $(R, +, -, 0)$. Potom $\sim$ je ta stejná ekvivalence podle podgrupy I.

$a \sim b \Leftrightarrow a + I = b + I$ ... třídy ekvivalence jsou rozkladové třídy podle podgrupy. $[a] = a + I$.

Na blocích definujeme $[a]+[b] = [a+b]$, $-[a] = [-a]$, $[0]$ je neutrální prvek, $[a]\cdot[b] = [a\cdot b]$.

Množina bloků $[a]$ s těmito operacemi je faktorokruh podle ideálu I:

$$R/I = (\{[a]|a \in R\}, +, -, [0], \cdot).$$

Důkaz (Dobrá definovanost)
1) Operace na blocích jsou dobře definované: $+, -$ víme z grup. Buď nyní $[a] = [c]$, $[b] = [d]$, chceme $[ab] = [cd]$. Z definice bloků víme, že $a - c \in I$ a $b - d \in I$, tudíž $ab - cd = a(b - d) + (a - c)d \in I$.

2) R/I je okruh: Ověří se axiomy okruhu pro R/I z axiomů pro R. (Pozor, axiomy oboru se nezachovávají.) □

Věta 21.4

$\varphi : R \to S$ homomorfismus okruhů.

1) (věta o homomorfismu) $I \subseteq \operatorname{Ker} \varphi$ ideál v R. Pak $\varphi : R/I \to S$, $[a] \mapsto \varphi(a)$ je dobře definovaný okruhový homomorfismus.

2) (1. věta o isomorfismu) $R/\operatorname{Ker} \varphi \simeq \operatorname{Im} \varphi$, $[a] \mapsto \varphi(a)$.

Důkaz
Použije se věta pro grupy a člověk si rozmyslí, že tato zobrazení jsou homomorfismy i vůči násobení. □

Poznámka
Platí i 2. a 3. věta o isomorfismu. (Viz skripta.)

21.3 Kdy je faktorokruh obor / těleso?

Definice 21.2 (prvoideál, maximální ideál)

Ideál I v okruhu R je prvoideál, pokud $\forall a, b \in R : ab \in I \implies a \in I$ nebo $b \in I$. A je maximální, pokud je I maximální vlastní ideál v R, čili neexistuje ideál j tak, že $I \subset J \subset R$.

Věta 21.5

R komutativní okruh s 1, I ideál. 1) Pak R/I je obor $\Leftrightarrow$ I prvoideál. 2) Potom R/I je těleso $\Leftrightarrow$ I je maximální.

Důkaz
1) R/I obor $\Leftrightarrow$ $([a]\cdot[b]=0 \implies [a]=0 \vee [b]=0) \Leftrightarrow (a\cdot b\in I \implies a\in I \vee b\in I) \Leftrightarrow I$ je prvoideál.

2) Z tvrzení 7.6: R/I těleso $\Leftrightarrow$ nemá žádné vlastní ideály. Z druhé věty o isomorfismu: Ideály v R/I jsou právě J/I pro $J \supseteq I$. Tedy R/I je těles $\Leftrightarrow$ I je maximální ideál. $\square$

22 Tělesové rozšíření jako vektorový prostor

Definice 22.1 (Rozšíření těles)

Rozšíření těles jsou tělesa $\mathbb{T}$, $\mathbb{S}$ tak, že $\mathbb{T} \leq \mathbb{S}$. (Čili $\mathbb{T}$ je podtěleso $\mathbb{S}$ a $\mathbb{S}$ je rozšíření $\mathbb{T}$).

Definice 22.2 (Stupeň rozšíření)

Dimenze vektorového prostoru $\mathbb{S}_{\mathbb{T}}$ (vektorový prostor nad $\mathbb{T}$ odpovídající $\mathbb{S}$) je stupeň rozšíření $\mathbb{S} \geq \mathbb{T}$. Neboli $[\mathbb{S}:\mathbb{T}] = \dim \mathbb{S}_{\mathbb{T}}$.

Definice 22.3 (Prvotěleso)

Nejmenší podtěleso v jiném tělesu se nazývá prvotěleso.

Tvrzení 22.1

Počet prvků konečného tělesa je mocnina prvočísla.

Důkaz
$\mathbb{T}$ konečnétěleso, $\mathbb{P}$ prvotěleso, tj. $\mathbb{P} \simeq \mathbb{Z}_p$. Tedy VP $\mathbb{T}_p$ je izomorfní VP $(\mathbb{Z}_p)^k$, kde $k = [\mathbb{T}:\mathbb{P}] < \infty$. Ale $|\mathbb{Z}_p^k| = p^k = |\mathbb{T}|$. $\square$

23 Algebraické prvky, rozšíření konečného stupně

23.1 Minimální polynom

Definice 23.1 (Algebraické a transcendentní číslo)

$\mathbb{T} \leq \mathbb{S}$ rozšíření těles, $\alpha \in \mathbb{S}$. α je algebraické nad $\mathbb{T}$, pokud $\exists 0 \neq f \in \mathbb{T}[x] : f(\alpha) = 0$. Jinak je α transcendentní nad $\mathbb{T}$.

Definice 23.2 (Minimální polynom)

$\mathbb{T} \leq \mathbb{S}$ rozšíření těles, $\alpha \in \mathbb{S}$ algebraické nad $\mathbb{T}$. Minimální polynom prvku α nad tělesem $\mathbb{T}$ je ireducibilní monický polynom $m_{\alpha,\mathbb{T}} \in \mathbb{T}[x]$, který má kořen α.

Tvrzení 23.1 (Vlastnosti minimálního polynomu)

$m_{\alpha,\mathbb{T}}$ existuje a je jednoznačný. α je kořen $f \in \mathbb{T}[x] \Leftrightarrow m_{\alpha,\mathbb{T}}|f$.

Důkaz

$I = \{f \in \mathbb{T}[x] | f(\alpha) = 0\}$ je ideál v $\mathbb{T}[x]$. $\mathbb{T}[x]$ je OHI $\implies$ I je hlavní. Buď $m \in \mathbb{T}[x]$ monický tak, že $I = m\mathbb{T}[x]$. Tedy $f(\alpha) = 0 \Leftrightarrow f \in I = m\mathbb{T}[x] \Leftrightarrow m|f$.

$m \stackrel{?}{=} m_{\alpha,\mathbb{T}}$: monický je, $m(\alpha) = 0$, tedy zbývá ireducibilita: Kdyby $m = f \cdot g$, pak $f(\alpha) \cdot g(\alpha) = 0$, tj. $f(\alpha) = 0$ nebo $g(\alpha) = 0 \implies m|f$ nebo $m|g$, $\lightning$. Tedy je ireducibilní.

Jednoznačnost: $\tilde{m} \in \mathbb{T}[x]$ ireducibilní, monický, $\tilde{m}(\alpha)$. $m|\tilde{m}$. Ale $\tilde{m}$ je ireducibilní, tedy $m||\tilde{m}$, čili $m = c\tilde{m}$, $c \in \mathbb{T}^*$. Ale $m, \tilde{m}$ jsou monické $\implies$ $c = 1$, $m = \tilde{m}$. $\square$

Tvrzení 23.2 (Struktura jednoduchých rozšíření)

Buď $\mathbb{T} \leq \mathbb{S}$ rozšíření těles, $\alpha \in S$. Pak $\mathbb{T}(\alpha) = \mathbb{T}[\alpha] \Leftrightarrow \alpha$ je algebraické nad $\mathbb{T}$.

Důkaz

$\mathbb{T}[\alpha] = \{f(\alpha) | f \in \mathbb{T}[x]\}$.

$\impliedby$: Uvažujme homomorfismus okruhů $\varphi : \mathbb{T}[x] \to \mathbb{T}[\alpha]$, $f \mapsto f(\alpha)$. $\operatorname{Im} \varphi = \mathbb{T}[\alpha]$. $\operatorname{Ker} \varphi = \{f | f(\alpha) = 0\} = m_{\alpha,\mathbb{T}}\mathbb{T}[x]$. Víme, že $m = m_{\alpha,\mathbb{T}}$ je ireducibilní, tedy $m\mathbb{T}[x]$ je maximální. Podle 1. věty o izomorfismu $\mathbb{T}[\alpha] \simeq \mathbb{T}[x]/m\mathbb{T}[x]$, což je faktor podle maximálního ideálu $\implies$ $\mathbb{T}[\alpha]$ je těleso. A protože $\mathbb{T}[\alpha]$ je těleso $\implies$ nejmenší těleso obsahující α $\implies$ $\mathbb{T}[\alpha] = T(\alpha)$.

$\implies$ α transcendentní. Pro spor ať $\mathbb{T}[\alpha] = \mathbb{T}(\alpha)$. Tedy $\exists f(\alpha \in \mathbb{T}[\alpha])$ tak, že $f(\alpha) = \alpha^{-1}$. Pak ale α je kořen polynomu $x \cdot f - 1$, $\lightning$. $\square$

Tvrzení 23.3 (Stupeň jednoduchého rozšíření)

$\mathbb{T} \leq \mathbb{S}$ rozšíření, $\alpha \in \mathbb{S}$ algebraické nad $\mathbb{T}$. $[\mathbb{T}(\alpha) : \mathbb{T}] = \deg m_{\alpha,\mathbb{T}}$.

Důkaz

$n = \deg m_{\alpha,\mathbb{T}}$. Dokážeme, že $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$ tvoří bázi VP $\mathbb{T}(\alpha)_{\mathbb{T}}$. Lineární nezávislost: Kdyby $\sum_{i=0}^{n-1} t_i\alpha^i = 0$ pro nějaké $t_i \in \mathbb{T}$, pak $f = \sum_{t_i} x^i$ má α za kořen, $m_{\alpha,\mathbb{T}}|f \implies f = 0$ (jelikož $m_{\alpha,\mathbb{T}}$ má větší stupeň), tedy máme triviální lineární kombinaci.

Generování: $f(\alpha) \in \mathbb{T}[\alpha] = \mathbb{T}(\alpha)$, kde $f \in \mathbb{T}[x]$. Ať $f = m_{\alpha,\mathbb{T}} \cdot q + r$, $q, r \in \mathbb{T}[x]$, $\deg r < degm_{\alpha,\mathbb{T}} = n$, tj. $r = \sum_{i=0}^{n-1} r_i\alpha^i \implies f(\alpha) = m_{\alpha,\mathbb{T}}(\alpha) \cdot q(\alpha) + r(\alpha) = 0 + r(\alpha)$. Tím jsme $f(\alpha)$ vyjádřili v $1, \alpha, \ldots, \alpha^{n-1}$. $\square$

Důsledek
$\mathbb{T} \leq \mathbb{S}$, $\alpha \in \mathbb{S}$, α je algebraické nad $\mathbb{T} \Leftrightarrow [\mathbb{T}(\alpha) : \mathbb{T}] < \infty$.

Důkaz
α je transcendentní $\implies 1, \alpha, \alpha^2, \dots$ je lineární nezávislá množina $\implies [\mathbb{T}(\alpha) : \mathbb{T}]$ není konečný.

α algebraické $\implies [\mathbb{T}(\alpha) : \mathbb{T}] = \deg m_{\alpha,\mathbb{T}} < \infty$ podle předchozího tvrzení. □

23.2 Vícenásobné rozšíření

Tvrzení 23.4 (Stupeň vícenásobného rozšíření)

Buď $\mathbb{T} \leq \mathbb{S} \leq \mathbb{U}$ rozšíření těles, pak $[\mathbb{U} : \mathbb{T}] = [\mathbb{U} : \mathbb{S}] \cdot [\mathbb{S} : \mathbb{T}]$.

Důkaz
A je báze VP $\mathbb{S}_\mathbb{T}$ a B je báze VP $\mathbb{U}_\mathbb{S}$. Dokážeme, že $C = \{a \cdot b | a \in A, b \in B\}$ je báze $\mathbb{U}_\mathbb{T}$. Generování: $C \subseteq \mathbb{U}$, tedy C generuje podprostor $\mathbb{U}_\mathbb{T}$. $u \in \mathbb{U}$. B báze $\mathbb{S}_\mathbb{S} \implies u = \sum_j s_j b_j$, $s_j \in \mathbb{S}$, $b_j \in B$. A báze $\mathbb{S}_\mathbb{T} \implies s_j = \sum_i t_{ij} a_i$, $t_{ij} \in \mathbb{T}$, $a_i \in A$. Tudíž $u = \sum_j \sum_i t_{ij}(a_i b_i)$ $\implies u$ jsme vyjádřili v C s koeficienty z $\mathbb{T}$.

LN viz skripta. Pak $[\mathbb{U} : \mathbb{T}] = |C| = |A| \cdot |B| = [\mathbb{S} : \mathbb{T}] \cdot [\mathbb{U} : \mathbb{S}]$. □

Důsledek

$$[\mathbb{T}(\alpha_1, \alpha_2) : \mathbb{T}] = \deg m_{\alpha_2, \mathbb{T}(\alpha_1)} \cdot \deg m_{\alpha_1,\mathbb{T}} \leq \deg m_{\alpha_2,\mathbb{T}} \cdot \deg m_{\alpha_1,\mathbb{T}}.$$

Důsledek
$\mathbb{T} \leq \mathbb{S}$, $\alpha_1, \dots, \alpha_n \in \mathbb{S}$ algebraické nad $\mathbb{T}$. Pak $\mathbb{T}(\alpha_1, \dots, \alpha_n)$ je rozšíření konečného stupně nad $\mathbb{T}$.

Důkaz
Indukcí. □

Definice 23.3

$\mathbb{T} \leq \mathbb{S}$ rozšíření těles je algebraické, pokud $\forall \alpha \in \mathbb{S}$ je algebraický prvek nad $\mathbb{T}$.

Tvrzení 23.5

Každé rozšíření konečného stupně je algebraické.

Důkaz
$u = [\mathbb{S} : \mathbb{T}]$. Buď $\alpha \in \mathbb{S}$. α je algebraické $\Leftrightarrow$ $[\mathbb{T}(\alpha) : \mathbb{T}] < \infty$. Tedy $[\mathbb{T}(\alpha) : \mathbb{T}] \leq n \implies \alpha$ algebraické nad $\mathbb{T}$. $\square$

Poznámka
Opačná implikace neplatí! Existuje algebraické rozšíření nekonečného stupně (např. algebraický uzávěr $\mathbb{Q}$).

Věta 23.6

$\mathbb{T} \leq \mathbb{S}$. *Prvky* $\mathbb{S}$*, jež jsou algebraické nad* $\mathbb{T}$*, tvoří podtěleso* $\mathbb{S}$.

Důkaz
$\alpha, \beta \in \mathbb{S}$ algebraické nad $\mathbb{T}$. Chceme $\alpha + \beta, -\alpha, \alpha \cdot \beta, \alpha^{-1}$ jsou algebraická nad $\mathbb{T}$.

$$\mathbb{T} \leq \mathbb{T}(\alpha + \beta) \leq \mathbb{T}(\alpha, \beta).$$

Víme, že $[\mathbb{T}(\alpha, \beta) : \mathbb{T}] < \infty \implies [\mathbb{T}(\alpha + \beta) : \mathbb{T}] < \infty \implies \alpha + \beta$ je algebraické. Úplně stejně pro $-\alpha$, $\alpha \cdot \beta$, α^{-1}. $\square$

24 Geometrické úlohy

Poznámka (Staré řecké úlohy)
Zdvojení krychle. Trisekce úhlu. Kvadratura kruhu. Konstrukce pravidelných n-úhelníků pro dané n (17-úhelník – Gauss).

Použijeme metodu Piere Wantzel 1837: M_0 je počáteční množina bodů v rovině (to, co máme zadáno). $M_i \supseteq M_{i-1}$ vytvoříme tak, že zkonstruujeme nový bod jako průsečík 2 nerovnoběžných přímek (vedoucích skrz body v M_{i-1}) nebo průsečík přímky a kružnice (přímka vedoucí skrz body v M_{i-1} a kružnice se středem v M_{i-1} a poloměrem vzdáleností dvou bodů z M_{i-1}) nebo průsečík dvou kružnic (se středy v M_{i-1} a poloměry „tamtéž“).

Tedy zavedeme systém souřadnic v rovině, čili ztotožníme rovinu s $\mathbb{R}^2$. Definujeme $\mathbb{T}_i$ = nejmenší těleso, které obsahuje všechny x-ové a y-ové souřadnice bodů z $M_i \leq \mathbb{R}$. Dostaneme tak tělesové rozšíření $Q(x_B, y_B | B \in M_i)$. Přidáním bodu X do M_i je totéž, co $\mathbb{T}_{i+1} = \mathbb{T}_i(x_X, y_X)$.

Lemma 24.1

Pro každou konstrukci pravítkem a kružítkem máme $[\mathbb{T}_{i+1} : \mathbb{T}_i] = 1, 2$, $\forall i$.

Důkaz
1) Průsečík 2 přímek. $ax+by=c$, $dx+ey=f$ jsou obecné rovnice 2 přímek. $a,b,c,d,e,f \in \mathbb{T}_i$. $ax+by=c$ je přímka procházející body $A=(k,l)$ a $B=(m,n) \in M_i \implies (l-n)x+(m-k)y=l\cdot m-k\cdot n$. Tedy $a=l-n,\ldots \in \mathbb{T}_i$, protože $k,l,m,n \in \mathbb{T}_i$. Řešení je bod (u,v), kde $u,v \in \mathbb{T}_i$. A tedy $T_{i+1}=\mathbb{T}_i(u,v)=\mathbb{T}_i$ a máme $[\mathbb{T}_{i+1}:\mathbb{T}_i]=1$.

2) Přímka a kružnice: $ax+by=c$, $(x-d)^2+(y-e)^2=(k-l)^2+(l-n)^2$, pro $a,b,c,d,e,k,l,m,n \in \mathbb{T}_i$. Pokud $b \neq 0$, pak vyjádříme y z rovnice přímky $y=\frac{c-ax}{b}$ a dosadíme to do rovnice kružnice. Dostaneme, že x je kořenem kvadratické rovnice s koeficienty z $\mathbb{T}_i$, kde buď f je ireducibilní, tedy $[\mathbb{T}_{i+1}:\mathbb{T}_i]=2$, nebo f není ireducibilní, potom minimáľní polynom pro x má stupeň 1, tedy $[\mathbb{T}_{i+1},\mathbb{T}_i]=1$. Případ $b=0$ se vyjádří obdobně.

3) viz skripta. □

Tvrzení 24.2 (Stupeň rozšíření pro konstrukce pravítkem a kružítkem)
Pro každou konstrukci pravítkem a kružítkem je $[\mathbb{T}_n:\mathbb{T}_0]=2^k$ *pro nějaké* $0 \leq k \leq n$.

Důkaz
Indukcí z předchozího tvrzení. □

Příklad (Zdvojení krychle)
Volíme $\mathbb{T}_0=\mathbb{Q}$, protože na začátku máme úsečku délky BÚNO 1. Chceme sestrojit $\sqrt[3]{2}$. Ale z předchozího tvrzení $[\mathbb{T}_n:\mathbb{Q}]=2^k$. $\mathbb{Q} \leq \mathbb{Q}(\sqrt[3]{2}) \leq \mathbb{T}_n$, tedy $[\mathbb{T}_n:\mathbb{Q}]=[\mathbb{T}_n:\mathbb{Q}(\sqrt[3]{2})]\cdot[\mathbb{Q}(\sqrt[3]{2}):\mathbb{Q}]$. A víme, že $x^3-2=m_{\sqrt[3]{2},\mathbb{Q}}$, tedy $[\mathbb{Q}(\sqrt[3]{2}:\mathbb{Q})]=3$. Tj. $3|[\mathbb{T}_n:\mathbb{Q}]=2^k]$, $\lightning$.

Příklad (Retifikace kružnice nebo kvadratura kruhu)
Podobně jako v minulé úloze bychom měli, že $\pi \in K_n$. Ale mi víme, že π (těžké dokázat), takže nemůže ležet v rozšíření konečného stupně $K_n \geq \mathbb{Q}$ (resp. se dá dokázat, že ani $K_n \geq \mathbb{Q}(\sqrt{2})$).

Příklad (Trisekce úhlu)
Dokonce nejde zkonstruovat úhel 20°, protože $\cos 20°$ má minimální polynom stupně 3.

25 Izomorfismy tělesových rozšíření

25.1 Galoisova věta

Definice 25.1 (T-izomorfismus)

$\mathbb{T}$, $\mathbb{S}$, $\mathbb{U}$ tělesa tak, že $\mathbb{T} \leq \mathbb{S}, \mathbb{T} \leq \mathbb{U}$. $\varphi : \mathbb{S} \to \mathbb{U}$ okruhový izomorfismus tak, že $\varphi(t) = t$ pro $\forall t \in \mathbb{T}$ se nazývá T-izomorfismus.

Definice 25.2

$\mathbb{T} \leq \mathbb{S}$, T-izomorfismy $\mathbb{S} \to \mathbb{S}$ jsou T-automorfismy.

Definice 25.3

Grupa všech T-automorfismů $\mathbb{S} \to \mathbb{S}$, $\mathbb{T} \leq \mathbb{S}$, se nazývá Galoisova grupa rozšíření $\mathbb{T} \leq \mathbb{S}$ a značí se $\mathrm{Gal}(\mathbb{S}/\mathbb{T})$.

Důkaz

Grupa je to triviálně, jelikož T-automorfismy jsou uzavřené na skládání a tedy tvoří podgrupu symetrické grupy na množině $\mathbb{S}$. □

Pozorování

$\varphi \in \mathrm{Gal}(\mathbb{S}/\mathbb{T})$ je jednoznačně určené (pokud existují) hodnotami $\varphi(a_1), \ldots, \varphi(a_n)$, kde $\mathbb{T}(a_1, \ldots, a_n) = \mathbb{S}$ a $a_1, \ldots, a_n$ jsou algebraická nad $\mathbb{T}$.

Důkaz

$\mathbb{S} = \mathbb{T}(a_1, \ldots, a_n) = \mathbb{T}[a_1, \ldots, a_n]$ (z algebraičnosti). Každý prvek $s \in \mathbb{S}$ jde vyjádřit jako $s = \sum c_{i_1 \ldots i_n} a_1^{i_1} \ldots a_n^{i_n}$ pro $c_{i_1, \ldots, i_n} \in \mathbb{T}$. Teď $\varphi(s) = \sum \varphi(c_{i_1 \ldots i_n}) \varphi(a_1)^{i_n} \ldots \varphi(a_n)^{i_n}$, ale obraz $c_{\ldots}$ je ono samo, tedy stačí mít obrazy $a_1, \ldots, a_n$. □

Pozor

Ne každá volba $\varphi(a_1), \ldots$ funguje.

Tvrzení 25.1 (Galoisova grupa a kořeny polynomů)

$\mathbb{T} \leq \mathbb{S}$, $f \in \mathbb{T}[x]$, $A \subseteq \mathbb{S}$ *je množina všech kořenů polynomu* f *v* $\mathbb{S} \setminus \mathbb{T}$. *Pro každé* $\varphi \in \mathrm{Gal}(\mathbb{S}/\mathbb{T})$ *je* $\varphi|_A$ *permutace množiny* $A \wedge$ *zobrazení* $\mathrm{Gal}(\mathbb{S}/\mathbb{T}) \to S_A$, $\varphi \mapsto \varphi|_A$ *je grupový homomorfismus.*

Důkaz
$f = \sum c_i x^i$, $\alpha \in S$ kořen.

$$0 \stackrel{?}{=} f(\varphi(\alpha)) = \sum c_i \varphi(\alpha)^i = \sum \varphi(c_i)\varphi(\alpha)^i = \varphi(\sum c_i \alpha^i) = \varphi(f(\alpha)) = \varphi(0) = 0.$$

Tedy $\varphi(\alpha)$ je také kořen. Ale pokud $\alpha \in \mathbb{T}$, pak $\varphi(\alpha) = \alpha \in \mathbb{T}$. φ je prosté $\implies$ žádný jiný kořen α' se mi na α nezobrazí. Tedy $\varphi|A$ je prosté zobrazení na A. A je konečná množina, tedy jelikož $\varphi|_A$ je bijekce, tak je i permutace.

Grupový homomorfismus se snadno ověří. □

25.2 Jednoznačnost kořenových a rozkladových nadtěles (bez důkazů)

Věta 25.2 (Jednoznačnost koř. a roz. nadtěles)

$\mathbb{T}$ *těleso,* $f \in \mathbb{T}[x]$, $\deg f \geq 1$. *Je-li* f *ireducibilní, pak každé dvě kořenová nadtělesa* f *nad* $\mathbb{T}$ *jsou T-izomorfní. 2) Každá dvě rozkladová nadtělesa* f *nad* $\mathbb{T}$ *jsou T-izomorfní.*

Důkaz (Nástřel)
Kořenová nadtělesa $\mathbb{T}(a)$, $T(b)$. a, b algebraické nad $\mathbb{T}$ $\implies$ $\mathbb{T}(a) = [a] = \{g(a) | g \in \mathbb{T}[x]\}$. Definujeme $\mathbb{T}(a) \to \mathbb{T}(b)$, $g(a) \mapsto g(b)$. Toto zobrazení je hledaný T-izomorfismus (musí se dokázat dobrá definovanost). □

25.3 Galoisova grupa polynomů

Definice 25.4

$f \in \mathbb{T}[x], \deg f \geq 1$. Galoisova grupa polynomu f nad $\mathbb{T}$ je $\mathrm{Gal}(f/\mathbb{T}) := \mathrm{Gal}(\mathbb{S}/\mathbb{T})$ pro libovolné rozkladové nadtěleso $\mathbb{S}$ polynomu f nad $\mathbb{T}$.

Tvrzení 25.3 (Základní vlastnosti Galoisovy grupy)

$\mathbb{T}$ *těleso,* $f \in \mathbb{T}[x]$, $\deg f \geq 1$, $\mathbb{S}$ *rozkladové nadtěleso* f *nad* $\mathbb{T}$.

1) $\mathrm{Gal}(\mathbb{S}/\mathbb{T})$ *je izomorfní podgrupě symetrické grupy* S_m*, kde* m *je počet různých kořenů v* $\mathbb{S} \setminus \mathbb{T}$.

2) f *ireducibilní* $\implies$ $\forall$ *kořeny* $a, b \in \mathbb{S}$ $\exists \varphi \in \mathrm{Gal}(\mathbb{S} \setminus \mathbb{T}) : \varphi(a) = b$.

3) $\mathbb{T} \leq \mathbb{S} \leq \mathbb{U}$*, kde* $\mathbb{U}$ *je rozkladové nadtěleso nějakého polynomu nad* $\mathbb{T}$*. Pak* $\mathrm{Gal}(\mathbb{U}/\mathbb{S}) \trianglelefteq \mathrm{Gal}(\mathbb{U}/\mathbb{T})$ *a* $\mathrm{Gal}(\mathbb{U}/\mathbb{T}) / \mathrm{Gal}(\mathbb{U}/\mathbb{S}) \simeq \mathrm{Gal}(\mathbb{S}/\mathbb{T})$.

Důkaz (Zkouší se jen 1)
1) Ať $A = \{a_1, \dots, a_m\}$ jsou kořeny f v $\mathbb{S}\backslash\mathbb{T}$. Z tvrzení výše pak je pak $\forall\varphi \in \operatorname{Gal}(\mathbb{S}/\mathbb{T}) : \varphi|_A$ je permutace A a $\psi : \operatorname{Gal}(\mathbb{S}/\mathbb{T}) \to S_A$, $\varphi \mapsto \varphi|_A$ je homomorfismus.

Důkaz, že ψ je prosté: $\mathbb{S}$ rozkladové nadtěleso $\implies$ $\mathbb{S} = \mathbb{T}(a_1, \dots, a_m)$, čili $\forall\varphi$ je jednoznačně určené hodnotami $\varphi(a_1), \dots, \varphi(a_m)$, čili $\varphi|_A$ jednoznačně určuje $\varphi \implies \psi$ je prosté. Tedy podle 1. věty o izomorfismu $\operatorname{Gal}(\mathbb{S}/\mathbb{T}) \simeq \operatorname{Im}\psi \leq S_A \simeq S_m$.

2) plyne z důkazu jednoznačnosti rozkladových nadtěles.

3) Použijeme 1. větu o izomorfismu: $\Phi : \operatorname{Gal}(\mathbb{U}/\mathbb{T}) \to \operatorname{Gal}(\mathbb{S}/\mathbb{T})$, $\varphi \mapsto \varphi|_{\mathbb{S}}$. Ověříme, že to funguje. Pak si všimneme $\operatorname{Im}\Phi = \operatorname{Gal}(\mathbb{S}/\mathbb{T})$ (s využitím jednoznačnosti rozkladových nadtěles). $\operatorname{Ker}\Phi \ni \varphi \Leftrightarrow \varphi|_S = \mathrm{id} \Leftrightarrow \varphi(s) = s\ \forall s \in \mathbb{S} \Leftrightarrow \varphi \in \operatorname{Gal}(\mathbb{U}/\mathbb{S})$. $\operatorname{Ker}\Phi = \operatorname{Gal}(\mathbb{U}/\mathbb{S}) \trianglelefteq \operatorname{Gal}(\mathbb{U}/\mathbb{T})$. □

Lemma 25.4

$0 \neq a \in \mathbb{Q}$. *Rozkladové nadtěleso polynomu* $f = x^4 - a$ *nad* $\mathbb{Q}$ *je* $\mathbb{Q}(\zeta_n, b)$, *kde* b *je libovolný komplexní kořen* f.

Důkaz
Komplexní kořeny $x^n - a$ jsou právě $b \cdot \zeta_n^k$, $k = 0, \dots, n-1$. Tedy máme n kořenů polynomu stupně n, tudíž máme všechny. Rozkladové nadtěleso $= \mathbb{S} = \mathbb{Q}(b, b\zeta_n, \dots, b\zeta_n^{n-1}) \overset{?}{=} \mathbb{Q}(b, \zeta_n) = \mathbb{S}'$. $\supseteq$: $b \in \mathbb{S}$, $\zeta_n = b^{-1} \cdot (b\zeta_n) \in \mathbb{S}$. $\subseteq$ $b\zeta_n^k \in \mathbb{S}'$. □

Tvrzení 25.5 (Galoisovy grupy pro odmocniny)

$\mathbb{Q} \leq \mathbb{T} \leq \mathbb{C}$ *těleso,* $n \in \mathbb{N}$, $a \in \mathbb{T}$. *Pak 1)* $\operatorname{Gal}(x^n - 1/\mathbb{T})$ *je abelovská, 2)* $\operatorname{Gal}(x^n - a/\mathbb{T}(\zeta_n))$ *je abelovská, 3)* $\operatorname{Gal}(x^n - a/\mathbb{T})$ *je řešitelná grupa stupně* ≤ 2.

Důkaz
$\mathbb{S} = \mathbb{T}(\zeta_n)$, $\mathbb{U} = \mathbb{T}(\zeta_n, b)$, kde $b \in \mathbb{C}$ je nějaký kořen $x^n - a$.

1) Důkaz, že je izomorfní podgrupě $\mathbb{Z}_n^*$: $\mathbb{S}$ = rozkladové nadtěleso $x^n - 1$ (neboť kořeny jsou $1 = \zeta_n^0, \ldots, \zeta_n^{n-1}$). $\forall \varphi \in \mathrm{Gal}(\mathbb{S}/\mathbb{T})$ permutuje kořeny $x^n - 1$, čili $\varphi(\zeta_n) = \zeta_n^k$. Co můžeme říct o k? φ je automorfismus tělesa $\mathbb{S} \implies \varphi$ je také automorfismus grupy $\mathbb{S}^*$ $\implies \varphi$ zachovává řády prvků v S^*. Tj. $\mathrm{ord}(\zeta_n) = n \implies \mathrm{ord}(\zeta_n^k) = 1 \Leftrightarrow \mathrm{NSD}(k, n) = 1$.

Tedy máme zobrazení $\Phi : \mathrm{Gal}(\mathbb{S}/\mathbb{T}) \to \mathbb{Z}_n^*$, $\varphi(\zeta_n) = \zeta_n^k \mapsto k$. Toto zobrazení je prosté, neboť $\varphi(\zeta_n)$ jednoznačně určuje φ na $\mathbb{S} = \mathbb{T}(\zeta_n)$. Navíc je Φ grupový homomorfismus (jednoduše se rozepíše). Podle 1. věty o izomorfismu je tedy $\mathrm{Gal}(\mathbb{S}/\mathbb{T}) \simeq \Im\Phi \leq \mathbb{Z}_n^*$.

2) (náznak, nezkouší se): $\mathrm{Gal}(x^n - a/\mathbb{S}) = \mathrm{Gal}(\mathbb{U}/\mathbb{S}) \ni \varphi$. Dokáže se, že $\mathrm{Gal}(\mathbb{U}/\mathbb{S})$ je izomorfní podgrupě $\mathbb{Z}_n$: Kořeny $x^n - a$ jsou $b \cdot \zeta_n^k \implies \varphi(b) = b\zeta_n^k$. A to nám dává homomorfismus $\mathrm{Gal}(\mathbb{U}/\mathbb{S}) \to \mathbb{Z}_n$, $\varphi(b) = b\zeta_n^k \mapsto k$. Ověříme, že je vše OK a máme to.

3) $\mathrm{Gal}(x^n - a/\mathbb{T}) = \mathrm{Gal}(\mathbb{U}/\mathbb{T})$. $\mathbb{U} = \mathbb{T}(\zeta_n, b)$ je rozkladové nadtěleso pro $x^n - a$. $\mathbb{S} = \mathbb{T}(\zeta_n)$. Rozšíření $\mathbb{T} \leq \mathbb{S} \leq \mathbb{U}$. Z tvrzení 24.5(3) máme $\mathrm{Gal}(\mathbb{U}/\mathbb{S}) \trianglelefteq \mathrm{Gal}(\mathbb{U}/\mathbb{T})$. K řešitelnosti potřebujeme řetězec podgrup TODO. Máme triviálně takový řetězec délky nejvýše 2 (může být dokonce i 1, když jsou 2 totožné). $\square$

26 (Ne)řešitelnost polynomů v radikálech (=odmocninách)

Definice 26.1 (Vyjádřitelnost v radikálech)

Buď $\mathbb{T} \leq \mathbb{U}$ tělesové rozšíření a $a \in U$. Potom a je vyjádřitelný v radikálech na $\mathbb{T}$, pokud existuje řada rozšíření $\mathbb{T} = \mathbb{T}_0 \leq \ldots \leq \mathbb{T}_k \leq U$ tak, že $a \in \mathbb{T}_k$ a $\forall i : \mathbb{T}_i$ je rozkladové nadtěleso nějakého polynomu $x^{n_i} - a_i \in \mathbb{T}_{i-1}[x]$.

Definice 26.2

Ať $\mathbb{T}$ je těleso, $f \in \mathbb{T}[x]$. f je řešitelný v radikálech nad $\mathbb{T}$, pokud existuje $\mathbb{T} = \mathbb{T}_0 \leq \ldots \leq \mathbb{T}_k$ tak, že $\forall i$, $\mathbb{T}_i$ je rozkladové nadtěleso nějakého polynomu $x^{n_i} - a_i \in \mathbb{T}_{i-1}[x]$. f se rozkládá v $\mathbb{T}_k$ na lineární činitele, čili rozkladové nadtěleso f je obsažené v $\mathbb{T}_k$.

Věta 26.1 (Galoisova věta)

$\mathbb{T}$ těleso charakteristiky 0, $f \in \mathbb{T}[x]$, $\deg f \geq 1$. Polynom f je řešitelný v radikálech nad $\mathbb{T}$ $\Leftrightarrow$ $\mathrm{Gal}(f/\mathbb{T})$ je řešitelná grupa.

Důsledek
$\forall$ polynom stupně ≤ 4 je řešitelný v radikálech.

Naopak jsme viděli, že S_n, $n \geq 5$ nejsou řešitelné, tedy pokud najdeme f, $\deg f = 5$ tak, že $\mathrm{Gal}(f/\mathbb{Q}) \simeq S_5$, pak je tento polynom neřešitelný.

Tvrzení 26.2

p prvočíslo, $f \in \mathbb{Q}[x]$ ireducibilní polynom, $\deg f = p$ *tak, že f má $p-2$ reálných a 2 komplexní nereálné kořeny. Pak* $\mathrm{Gal}(f/\mathbb{Q}) \simeq S_5$.

Důkaz
Buď $\mathbb{U}$ rozkladové nadtěleso f nad $\mathbb{Q}$, z tvrzení výše je pak $\mathrm{Gal}(\mathbb{U}/\mathbb{Q}) \simeq H \leq S_p$. Chceme H obsahuje transpozici a p-cyklus, jelikož pak $H = S_p$.

f má $p-2$ reálných a 2 imaginární kořeny, $\mathbb{Q} \leq \mathbb{U} \leq \mathbb{C}$. Na $\mathbb{C}$ máme $\mathbb{Q}$-automorfismus = komplexní konjugaci. Uvažujme její zúžení na $\mathbb{U}$, což je $\mathbb{Q}$-automorfismus $\mathbb{U}$. Fixuje reálné kořeny a prohazuje imaginární, tedy jako permutace na kořenech je to transpozice.

H působí na množině kořenů f. Dle tvrzení výše je její působení tranzitivní (neboli má jen 1 orbitu) ta má velikost p (=počet kořenů f). Velikost orbity dělí řád H, tedy H obsahuje prvek řádu p, což je právě hledaný p-cyklus. $\square$

Například
$x^5 - 4x + 2$ je ireducibilní díky Eisensteinovi pro 2. Počet reálných kořenů spočítáme z MA (najdeme extrémy a spočítáme, zda jsou kladné/záporné), má jich 3. 2 jsou tedy imaginární.

Důsledek (Abelova-Ruffiniho věta)
Existují racionální polynomy stupně ≥ 5, které nejsou řešitelné v radikálech nad $\mathbb{Q}$.

Důkaz (Galoisova věta, pouze 1 implikace (druhá nás nezajímá))
Myšlenka: Pokud je f Řešitelná, tak posloupnost z definice nám dává indukovanou posloupnost Galoisových grup, jejichž faktogrupy jsou řešitelné.

Lemma 26.3

$\mathbb{S}$ je rozkladové nadtěleso nějakého polynomu f nad tělesem $\mathbb{T}$. $g \in \mathbb{T}[x]$ ireducibilní polynom. Pokud g má v S nějaký kořen, pak se tam rozkládá na lineární činitele.

Důkaz (Nezkouší se, jen myšlenka)
Když $\mathbb{U}$ je rozkladové nadtěleso fg a a kořen g v $\mathbb{S}$, b kořen g v $\mathbb{U}$, pak z jednoznačnosti rozkladového nadtělesa plyne, že $\exists \varphi \in \mathrm{Gal}(\mathbb{U}/\mathbb{T})$ tak, že $\varphi(a) = b$. φ permutuje kořeny polynomu f v $(\mathbb{U})$, ty generují $\mathbb{S}$, tedy $\varphi(\mathbb{S}) \subseteq \mathbb{S}$. Pak $b = \varphi(a) \in \mathbb{S}$. $\square$

Lemma 26.4

$\mathbb{T}$ těleso charakteristiky 0, $\mathbb{T} \leq \mathbb{S} \leq \mathbb{U}$ tělesová rozšíření, kde $\mathbb{S}$ je rozkladové nadtěleso nějakého polynomu nad $\mathbb{T}$ a $\mathbb{U}$ je rozkladové nadtěleso $x^n - a \in \mathbb{S}[x]$ nad $\mathbb{S}$. Pak $\exists$ rozšíření $\mathbb{U} \leq \mathbb{V}$ tak, že $\mathbb{V}$ je rozkladově nadtěleso nějakého polynomu nad $\mathbb{T}$ a $\mathrm{Gal}(\mathbb{V}/\mathbb{S})$ je řešitelná grupa.

Důkaz
BÚNO $\mathbb{U} \leq \mathbb{C}$. $g = m_{a;\mathbb{T}}(x^n) \in \mathbb{T}[x]$. $\mathbb{C} \geq \mathbb{V}$ je rozkladové nadtěleso fg nad $\mathbb{T}$. $\mathbb{U} \leq \mathbb{V}$ neboť $x - a | m_{a;\mathbb{T}}$ v $\mathbb{S}[x]$, tedy $x^n - a | m_{a;\mathbb{T}}(x^n) = g$, tedy navíc se $x^n - a$ v $\mathbb{V}$ rozkládá na lineární činitele.

$m_{a;\mathbb{T}}$ je ireducibilní a má kořen v $\mathbb{S}$. Tedy $m_{a;\mathbb{T}}$ se v $\mathbb{S}$ rozkládá na lineární činitele, tedy $g = (x^n - a_1)(x^n - a_2) \ldots \in \mathbb{S}[x]$. Chceme, že $\mathrm{Gal}(\mathbb{V}/\mathbb{S})$ je řešitelné, tedy máme $\mathbb{S} = \mathbb{S}_0 \leq \ldots \leq \mathbb{S}_m = \mathbb{V}$. $\mathbb{S}_i$ je rozkladové nadtěleso $x^n - a_i$ nad $\mathbb{S}_{i-1}$. Všechny $\mathbb{S}_i$ jsou rozklad nad $\mathbb{S}$, tedy můžeme použít tvrzení výše a máme $\mathrm{Gal}(\mathbb{V}/\mathbb{S})$ je řešitelná. $\square$

Chceme f řešitelný $\implies$ $\mathrm{Gal}(f/\mathbb{T})$ řešitelná. Máme z definice $\mathbb{T} = \mathbb{T}_0 \leq \ldots \leq \mathbb{T}_k$ a $\mathbb{W} \leq \mathbb{T}_k$, kde $\mathbb{W}$ je rozkladové nadtěleso f nad $\mathbb{T}$. Chceme $\mathrm{Gal}(f/\mathbb{T}) = \mathrm{Gal}(\mathbb{W}/\mathbb{T})$ je řešitelná.

Vyrobíme $\mathbb{T} = \mathbb{U}_0 = \mathbb{V}_0 \leq \mathbb{U}_1 \leq \mathbb{V}_1 \leq \ldots \leq \mathbb{U}_k \leq \mathbb{V}_k$ tak, že $\mathbb{U}_i$ je rozkladové nadtěleso $x^{n_i} - a_i$ nad tělesem $\mathbb{V}_{i-1}$ a $\mathbb{V}_i$ je těleso $\mathbb{V}$ z lemmatu výše aplikovaného na $\mathbb{T} \leq \mathbb{V}_{i-1} \leq \mathbb{U}$. Čili $\mathbb{V}_i$ je rozkladové nadtěleso nějakého polynomu nad $\mathbb{T}$ a $\mathrm{Gal}(\mathbb{V}_i/\mathbb{V}_{i-1})$ je řešitelná. Tedy $\mathrm{Gal}(\mathbb{V}_k/\mathbb{T})$ je řešitelná a nakonec $\mathrm{Gal}(\mathbb{W}/\mathbb{T})$ také. $\square$

27 Konečná tělesa

27.1 Derivace

Definice 27.1 (Derivace polynomu)

Pro $f = \sum_{i=0}^{n} a_i x^i \in R[x]$ definujeme derivaci polynomu f jako $f' = \sum_{i=1}^{n} i a_i x^{i-1}$.

Lemma 27.1 (Cvičení)

$(f+g)' = f' + g'$ a $(fg)' = f'g + fg'$.

Důsledek (O derivaci a vícenásobných kořenech)
Je-li R obor, $0 \neq f \in R[x]$. Pak pokud $\mathrm{NSD}(f, f') = 1$, pak f nemá žádný vícenásobný kořen v R.

Důkaz

a je n-násobný kořen, $n \geq 2$, $f = (x-a)^2 g$.

$$f' = [(x-a)^2 g]' = 2(x-a)g + (x-a)^2 g' \implies x - a | f' \implies x - a | NSD(f, f').$$

□

Tvrzení 27.2 (Frobeniův endomorfismus)

R je komutativní okruh s 1 a prvočíselnou charakteristikou p. Uvažujme zobrazení (tzv. Frobeniův endomorfismus) $\varphi_p : R \to R$, $a \mapsto a^p$.

1. *φ_p je homomorfismus okruhů,*
2. *R obor $\implies$ φ_p prosté,*
3. *R konečné těleso $\implies$ φ_p automorfismus (tj. tzv. Frobeniův automorfismus).*

Důkaz

Jednoduchý (násobení triviálně, sčítání podle binomické věty, 2 z toho, že je jádro prosté, 3 z toho, že je to prosté zobrazení na konečné množině). □

27.2 Klasifikace konečných těles

Lemma 27.3

Rozkladové nadtěleso polynomu $x^{p^k} - x$ nad tělesem $\mathbb{Z}_p$ má přesně p^k prvků.

Důkaz

Kořeny f v $\mathbb{T}$ tvoří podtěleso: Frobeniův endomorfismus $\varphi : \mathbb{T} \to \mathbb{T}, a \mapsto a^p$ je homomorfimus. φ^k je tedy také homomorfismus. Jsou-li $a, b \in \mathbb{T}$ kořeny f, pak také součet, opačná hodnota a inverzní prvek jsou kořeny. Tedy kořeny jsou těleso.

f se v $\mathbb{T}$ rozkládá na kořenové činitele. Pokud f nemá vícenásobné kořeny, pak $|T| = p^k$. A vícenásobné kořeny nemá, protože $f' = p^k x^{p^k - 1} - 1 = -1$, tj. $\mathrm{NSD}(f, f') = 1$. □

Lemma 27.4

$\mathbb{T}$ konečné těleso, $|\mathbb{T}| = p^k = q$. Pak $\mathbb{T}$ je rozkladové nadtěleso polynomu $x^q - x$ nad $\mathbb{Z}_p$ a v $\mathbb{T}[x]$ platí

$$x^q - x = \prod_{a \in \mathbb{T}} (x - a).$$

Důkaz
$\forall a \in \mathbb{T}$ je kořen f. Pro $a = 0$ platí, pro $a \neq 0$ máme $a \in \mathbb{T}^*$ a můžeme použít Lagrangeovu větu, tj. $a^{q-1} = 1$, tj. $a^q = a$ a $f(a) = 0$.

$\prod_{a \in \mathbb{T}}(x - a)|f$, ale tyhle polynomy mají oba stupeň q, oba jsou monické, takže se rovnají. $\square$

Věta 27.5 (Klasifikace konečných těles)

Konečné těleso velkosti n existuje $\Leftrightarrow n = p^k$ pro nějaké prvočíslo p a $k \in \mathbb{N}$.

Konečná tělesa stejné velikosti jsou izomorfní.

Důkaz
1. $\Longrightarrow$ tvrzení kdesi dříve, $\Longleftarrow$ rozkladové nadtělesa existují a předposlední lemma.

2. Konečné těleso velikosti $q = p^k$ je rozkladové nadtěleso $x^q - x$ nad $\mathbb{Z}_p$. Ale rozkladová nadtělesa jsou jednoznačná až na izomorfismus. $\square$

Věta 27.6 (Reprezentace konečných těles)

Pro každé prvočíslo p a $k \in \mathbb{N}$ existuje ireducibilní polynom $m \in \mathbb{Z}_p[\alpha]$ stupně k a $\mathbb{F}_{p^k} \simeq \mathbb{Z}_p[\alpha]/m$.

Důkaz
Podle předchozí věty $\exists \mathbb{T} \geq \mathbb{Z}_p$, $|\mathbb{T}| = p^k$. $\mathbb{T}^*$ je konečná multiplikativní grupa v tělese, tedy $\mathbb{T}^*$ je cyklické, čili generované BÚNO a. Pak $\mathbb{T} = \{0, 1 = a^0, \ldots\} = \mathbb{Z}_p(a)$. Búď $m = m_{a\mathbb{Z}_p} = [\mathbb{Z}_p(a) : \mathbb{Z}_p] = [\mathbb{T} : \mathbb{Z}_p] = k$. Tedy m je ireducibilní a má stupeň k.

$$\mathbb{Z}_p(a) \simeq \mathbb{Z}_p[\alpha]/(m(\alpha)).$$

$\square$