

Marie Demlová

demlova@math.feld.cvut.cz
fel.cvut.cz

<http://pitbul.pcland.cz>

1

$$\mathbb{Z}_n \quad a \equiv b \pmod{n}$$

$$\mathbb{Z}_n = \{0, 1, \dots, n-1\} \quad \text{řízkové třídy}$$

• řízků po dělení

$$i \oplus j = \text{řízků při dělení } i+j \text{ číslem } n$$

$$i \odot j = ij$$

$(\mathbb{Z}_n, \oplus)$ asociativní grupa, komutativní

$(\mathbb{Z}_n, \odot)$ je komutativní monoid

• inverzní prvek - k i exist i^{-1} tak že $i \odot i^{-1} = 1$

$$i \odot x = 1$$

$$i \cdot x \equiv 1 \pmod{n}$$

$$ix - 1 = km$$

$$ix + ym = 1 \quad y = -k$$

$$1 = \gcd(i, m)$$

$$\mathbb{Z}_n^* = \{i \in \mathbb{Z}_n \mid i^{-1} \text{ existuje}\}$$

grupa

$$(G, *, e)$$

$*$ je operace na G

$*$ je asociativní, tj. pro každé

$$x, y, z \in G \text{ platí } x * (y * z) = (x * y) * z$$

e je jednotkový prvek, tj. pro každé x

$$\text{existuje } x^{-1} \text{ tak, že } x * x^{-1} = e = x^{-1} * x$$

$$\text{tj. } a^{-1} * (a * x) = a^{-1} * (a * y)$$

$$x = e * x = (a^{-1} * a) * x = (a^{-1} * a) * y = e * y = y$$

co tedy brát

$$\text{Pr} \quad (\mathbb{Z}_n, \odot, 1)$$

$$1 \odot i = i = i \odot 1$$

komutativní, tj. $i \odot j = j \odot i$

$$a) 1^{-1} = 1$$

$$b) (i^{-1})^{-1} = i \quad \text{neboť } i \odot i^{-1} = 1$$

$$c) (i \odot j)^{-1} = j^{-1} \odot i^{-1} \quad \text{kdykoli } i^{-1} \text{ a } j^{-1} \text{ existují}$$

$$\mathbb{Z}_n^* = \{ i \mid i \in \mathbb{Z}_n, i^{-1} \text{ existuje} \}$$

je grupa

$$|\mathbb{Z}_n^*| = |\{ i \mid i \text{ je nesoudělné} \}| = \varphi(n)$$

$i \in \mathbb{Z}_n$

$$\varphi_{\mathbb{Z}}(\mathbb{Z}_n, 0, 1)$$

$$\mathbb{Z}_7^* = \{1, 2, 3, 4, 5, 6\}$$

$$1^{-1} = 1$$

$$2^{-1} = 4$$

$$4 \odot 2 = 1$$

$$3^{-1} = 5$$

$$3 \odot 5 = 1$$

$$6^{-1} = 6$$

$$\varphi(7) = 6$$

$$(\mathbb{Z}_8, \cdot, 1)$$

$$\mathbb{Z}_8^* = \{1, 3, 5, 7\}$$

$$1^{-1} = 1$$

$$5^{-1} = 5$$

$$\varphi(8) = 4$$

$$3^{-1} = 3$$

$$7^{-1} = 7$$

Eulerova funkce

$$\varphi(n) = |\{i \mid 0 \leq i \leq n, \gcd(i, n) = 1\}|$$

$$\varphi(p) = p - 1 \text{ pro } p \text{ prvočíslo}$$

$$\varphi(p^k) = p^k - p^{k-1}$$

$$m, n \text{ nesoudělná} \quad \varphi(m \cdot n) = \varphi(m) \cdot \varphi(n)$$

Je-li a nesoudělné s n , pak

$$a^{\varphi(n)} \equiv 1 \pmod{n}$$

Máme grupu $(G, *, e)$. Podmnožina $H \subseteq G$

se nazývá podgrupa, jestliže $(H, *, e)$ je sama grupa
a to platí tehdy, když

1) když $h_1, h_2 \in H$, tak $h_1 * h_2 \in H$

2) $e \in H$

3) když $h \in H$, tak $h^{-1} \in H$

$(\mathbb{Z}, +, 0)$ $S = \{2n \mid n \in \mathbb{Z}\}$ je podgrupa

$$2n + 2m = 2(n+m)$$

$$0 = 2 \cdot 0$$

$$2n + (-2n) = 0$$

$(\mathbb{Z}_{12}, \oplus, 0)$

$$H_1 = \{0, 1, 2, \dots, 11\}$$

$$H_2 = \{0\}$$

$$H_3 = \{0, 6\}$$

$$H_4 = \{0, 3, 6, 9\}$$

$$H_5 = \{0, 4, 8\}$$

podgrupy

Řád grupy (konечно) je počet jejích prvků.

Platí: je-li $(G, *, e)$ konečná grupa a $(H, *, e)$ je její podgrupa, pak řád $(H, *, e)$ dělí řád $(G, *, e)$

$$\text{tj. } |H| \text{ dělí } |G|$$

$$(\mathbb{Z}_{12}, +, 0)$$

$$H = \{0, 4, 8\}$$

$$1+H = \{1, 5, 9\}$$

$$2+H = \{2, 6, 10\}$$

$$3+H = \{3, 7, 11\}$$

$$4+H = H \quad 5+H = 1+H$$

$$6+H = 2+H \quad 7+H = 3+H$$

$$8+H = H$$

H

$$g * H = \{g * h \mid h \in H\}$$

$$\{g * H \mid g \in G\}$$

1) $\bigcup_{g \in G} g * H = G$ *placi, protože*
 $g = g * e \quad g \in g * H$

2) kdylz $(g_1 * H) \cap (g_2 * H) \neq \emptyset$, tak $g_1 * H = g_2 * H$

Tj existuji $g_1 * h_1 = g_2 * h_2$

$$g_1 = g_2 * \underbrace{(h_2 * h_1^{-1})}_{\in H}$$

$$g_2 = g_1 * (h_1 * h_2^{-1})$$

$$g_1 * h = g_2 * \underbrace{(h_2 * h_1^{-1})}_{\in H} * h \in g_2 * H$$

3) $f: H \rightarrow g_1 * H \quad f(h) = g_1 * h$

kdylz $g_1^{-1} * g_1 * h_1 = g_1^{-1} * g_1 * h_2$

tak $h_1 = h_2$

$$|H| = |g_1 * H|$$

grupa $(G, *, e)$

$$g \in G \quad \{g, g^2 = g * g, g^3 = g * g * g, \dots\}$$

Musí existovat $i, j, i < j$ tak, že

$$g^i = g^j$$

$$\underbrace{g * g * g \dots * g}_{i\text{-krát}} = \underbrace{g * \dots * g}_{j\text{-krát}}$$

↓ krácení

$$e = \underbrace{g * \dots * g}_{j-i \text{ krát}}$$

$$(\mathbb{Z}_{12}, +, 0)$$

$$2, 2+2=4, 2+2+2=6$$

$$2+2+2+2=8$$

$$2+2+2+2+2=10$$

$$2+2+2+2+2+2=0$$

Řád prvku g v grupě $(G, *, e)$ je nejmenší $n > 0$

takové, že $\underbrace{g * \dots * g}_{n\text{-krát}} = e$

$(\{g, g^2, \dots, g^n = e\}, *, e)$ je podgrupa o n prvcích

je-li $(G, *, e)$ konečná grupa, pak řád libovolného prvku dělí řád $(G, *, e)$

$$|G| = n \quad g \in G$$

řád g je n

$$n = n \cdot 1$$

$$g^n = \underbrace{g * \dots * g}_{n\text{-krát}} = g^{n \cdot 1} = (g^n)^1 = e^1 = e$$

je-li $(G, *, e)$ konečná grupa, pak pro každé $g \in G$
 platí $g^n = e$.

$$\underbrace{g * \dots * g}_{n\text{-krát}} = e$$

kde $n = |G|$

Euler-Fermatova věta

je-li a nesoudělné s n , pak $a^{\varphi(n)} \equiv 1 \pmod{n}$

je-li $a \in \mathbb{Z}_n^*$, pak

$$\underbrace{a^{\varphi(n)} = 1 \text{ v } \mathbb{Z}_n^*}$$

$$|\mathbb{Z}_n^*| = \varphi(n)$$

(2)

$(G, *, e)$ je grupa konečná

$a \in G$ $\{a, \dots, a^n = e\}$ n nejmenší je řád prvku

Lemma: Platí $a^k = e$ iff k je dělitelné n řádem prvku a .

a) Když $k = d \cdot n$, pak $a^k = a^{d \cdot n} = (a^n)^d = e^d = e$

b) Když $a^k = e$ $k \geq n$ $k = q \cdot n + r$ $0 \leq r < n$

$$a^{q \cdot n + r} = a^{q \cdot n} \cdot a^r = e \cdot a^r = a^r \quad \text{tj } r = 0 \quad \text{tj } k = q \cdot n$$

$(G, *, e)$ je grupa konečná

$a \in G$ n je rád a , d je dělitel n ($n = q \cdot d$)

$b = a^d$ $b^q = (a^d)^q = a^{dq} = a^n = e$ $\therefore$ je q rád b ?

Jestliže $(b^d)^k = e = a^{d \cdot k}$ $\therefore d \cdot k$ je dělitel n ,

$$d \cdot k = n \cdot m$$

$$dk = n \cdot q \cdot d$$

(Když $b^k = e$, tak k je dělitel q)

Twzení: 1) Je-li rád prvku a roven n a číslo d dělí n ,

pak a^d má rád $q = \frac{n}{d}$

2) Je-li rád prvku a roven n , pak a^k má rád

$$\frac{n}{\gcd(n, k)}$$

Def: Jestliže pro prvek a platí, že jeho rád je $n = |G|$ (řád grupy), pak a se nazývá generátor grupy $(G, *, e)$

Pr. $Z_7^* = \{1, 2, 3, 4, 5, 6\}$

$$3, 3^2 = 2, 3^3 = 6 = -1, 3^4 = -3 = 4, 3^5 = 5, 3^6 = 1$$

3 je generátor $(Z_7^*, \cdot, 1)$

$$1 \quad 3^0 = 3^6$$

$$2 \quad 3^2$$

$$3 \quad 3^1$$

$$4 \quad 3^4$$

$$5 \quad 3^5$$

$$6 \quad 3^3$$

$$5^{-1} = (3^5)^{-1} = 3$$

$$4^{-1} = (3^4)^{-1} = 3^2$$

Def: Grupa G se nazývá cyklická, má-li generátor.

Př: $\mathbb{Z}_8^* = \{1, 3, 5, 7\}$

$3^2 = 1, 5^2 = 1, 7^2 = 1$ nemá generátor

G je cyklická grupa o n prvcích. Pak má

$G = \{a, a^2, \dots, a^n = 1\}$

chceme, aby a^k mělo stejný řád
jako a , tj. k ~~relativně~~ nesoudělné
s n

a má řád n

a^k má řád $\frac{n}{\gcd(n, k)}$

$\frac{n}{\gcd(n, k)} = n$ iff $\gcd(n, k) = 1$

G má $\varphi(n)$ různých generátorů. {

$\varphi(n) = |\{k \mid 1 \leq k \leq n, \gcd(k, n) = 1\}|$ }

Máme grupu $(G, *, e)$ a její dvě podgrupy H_1, H_2 .

Pak $H_1 \cap H_2$ je podgrupa grupy $(G, *, e)$.

1) $e \in H_1 \cap H_2$, protože $e \in H_1, e \in H_2$

2) Když $a, b \in H_1 \cap H_2$, tak $a, b \in H_1$ i $a, b \in H_2$,
tudíž $a * b \in H_1, a * b \in H_2$, tj. $a * b \in H_1 \cap H_2$

3) Když $a \in H_1 \cap H_2$, tak $a \in H_1, a \in H_2$, tudíž $a^{-1} \in H_1, a^{-1} \in H_2$,
 $a^{-1} \in H_1 \cap H_2$

- Ujednotčení $H_1 \cup H_2$ nemusí být podgrupa.

- nemusí platit 2)

Př. $(\mathbb{Z}_{12}, +, 0)$ $H_1 = \{0, 4, 8\}$ $H_2 = \{0, 3, 6, 9\}$

$$H_1 \cup H_2 = \{0, 3, 4, 6, 8, 9\}$$

$$3 + 4 = 7 \notin H_1 \cup H_2$$

- Máme dvě grupy $(G_1, *, e_1)$, $(G_2, \circ, e_2)$

Pak ^(kartézský) součin těchto grup je grupa

$$(G_1 \times G_2, \square, (e_1, e_2)) \text{ , kde } (a, b) \square (c, d) = (a * c, b \circ d)$$

$$a, c \in G_1, b, d \in G_2$$

$$(a, b)^{-1} = (a^{-1}, b^{-1})$$

Př. G_1

	0	1
$\mathbb{Z}_2, +$	0	1
	1	0

G_2

	id	f
id	id	f
f	f	id

$\begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$	$\begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}$
f	id

$$\begin{aligned} 0 &\mapsto \text{id} \\ 1 &\mapsto f \end{aligned}$$

jsou izomorfní

Př. $(\mathbb{R}^+, \cdot, 1) \xrightarrow{\log} (\mathbb{R}, +, 0)$

$$x \cdot y \longrightarrow \log(x \cdot y) = \log x + \log y$$

$$\log 1 = 0 \quad \log x^{-1} = -\log x$$

$\rightarrow$ netriviální izomorfismus

Def: Máme dvě grupy $(G_1, *, e_1)$, $(G_2, \circ, e_2)$.

Isomorfismus grupy $(G_1, *, e_1)$ na $(G_2, \circ, e_2)$

(knačímef: $(G_1, *, e_1) \rightarrow (G_2, \circ, e_2)$) je zobrazení

$f: G_1 \rightarrow G_2$, které je prosté a na a

$$1) f(e_1) = e_2$$

$$2) f(a * b) = f(a) \circ f(b)$$

$$3) f(a^{-1}) = (f(a))^{-1}$$

Je-li $f: G_1 \rightarrow G_2$ zobrazení prosté a na a splňuje-li

$f(a * b) = f(a) \circ f(b)$, pak f je isomorfismus.

Zdůvodnění:

$$- e_1 * a = a = a * e_1$$

$$f(e_1 * a) = \boxed{f(e_1) \circ f(a) = f(a) = f(a * e_1) = f(a) \circ f(e_1)}$$

$$f(e_1) \circ f(a) = f(a) = f(a) \circ f(e_1)$$

$$f(e_1) = f(e_1 * e_1) = f(e_1) \circ f(e_1)$$

$$\underline{f(e_1) = e_2}$$

$$= a^{-1} * a = e_1 = a * a^{-1}$$

$$f(a^{-1}) \circ f(a) = f(a^{-1} * a) = f(e_1) = e_2 = f(a * a^{-1}) = f(a) \circ f(a^{-1})$$

$$f(a^{-1}) \circ f(a) = e_2 = f(e) \circ f(a^{-1})$$

$$f(a^{-1}) = (f(a))^{-1}$$

(3)

Cyklická grupa $G = \{a, a^2, a^3, \dots, a^m = e\}$ e je jednotkový prvek

a^k má řád $\frac{m}{\gcd(m, k)}$

máme d , které dělí m , tj. $m = k \cdot d$, jak podgrupa řádu d ?

$$a^k \quad \gcd(k, m) = k \quad \frac{m}{k} = d$$

$$\{a^k, a^{2k}, a^{3k}, \dots, a^{dk} = e\}$$

$x^d = e$ má d řešení

Čínská věta o zbytcích

Máme čísla $m_1, m_2, \dots, m_k$ po dvou nesoudělná

Pak pro každá čísla $a_1, a_2, \dots, a_k$ existuje číslo x tak,

$$x \equiv a_1 \pmod{m_1}$$

$$x \equiv a_2 \pmod{m_2}$$

(1)

$$x \equiv a_k \pmod{m_k}$$

a jestliže y splňuje (1) pak $x \equiv y \pmod{m_1 \cdot m_2 \cdot \dots \cdot m_k}$

D. ①

$$q_1 \equiv 1 \pmod{m_1}$$

$$q_2 \equiv 1 \pmod{m_2} \quad q_k \equiv 1 \pmod{m_k}$$

$$q_i \equiv 0 \pmod{m_i} \quad i \neq 1$$

$$q_2 \equiv 0 \pmod{m_i} \quad i \neq 2 \quad q_k \equiv 0 \pmod{m_i} \quad i \neq k$$

$$x = a_1 q_1 + a_2 q_2 + \dots + a_k q_k \quad \text{má vlastnosti (1)}$$

$$c \equiv d \pmod{m}$$

$$h \equiv k \pmod{m}$$

$$c + h \equiv d + k \pmod{m}$$

$$c \cdot h \equiv d \cdot k \pmod{m}$$

$$x \equiv a_1 \pmod{m_1}$$

$$x \equiv a_2 \pmod{m_2}$$

⋮

$$x \equiv a_k \pmod{m_k}$$

$$q_i \quad m_i \quad M_i = \prod_{j \neq i} m_j \quad q_i \stackrel{\text{def}}{=} S \cdot M_i$$

$$1 = r m_i + \boxed{S \cdot M_i}$$

pro nějaká r, s celá
(Bézoutova věta)

$$S M_i \equiv 0 \pmod{m_j} \quad j \neq i$$

$$S M_i \equiv 1 \pmod{m_i}$$

jednoznačnost:

$$x \equiv a_1 \pmod{m_1}$$

$$x \equiv a_2 \pmod{m_2}$$

$$x \equiv a_k \pmod{m_k}$$

$$\left. \begin{array}{l} y \equiv a_1 \pmod{m_1} \\ \vdots \\ y \equiv a_k \pmod{m_k} \end{array} \right\} \begin{array}{l} x \equiv y \pmod{m_1} \\ x \equiv y \pmod{m_2} \\ x \equiv y \pmod{m_k} \end{array}$$

~~$$x - y = \alpha_1 m_1$$~~
~~$$x - y = \alpha_2 m_2$$~~

$$\alpha_i \in \mathbb{Z}$$

$$x - y = \alpha_1 m_1$$

$$x - y = \alpha_2 m_2$$

$\vdots$

$$x - y = \alpha_k m_k$$

$$x - y = \alpha_1 m_1 = \alpha_2 m_2$$

m_1, m_2 nesoudělná

$$m_2 \mid \alpha_1$$

$$\alpha_1 = \alpha_{12} m_2$$

$$\alpha_1 = \alpha_{12} m_2$$

$$x - y = \alpha_{12} m_1 m_2$$

$$x - y = \alpha_1 m_1 = \alpha_{12} m_2 m_1$$

$$x - y = \alpha_3 m_3$$

$$\alpha_{12} \cdot m_1 \cdot m_2 = \alpha_3 m_3$$

$$m_3 \mid \alpha_{12}$$

$$x - y = \alpha_{123} m_1 m_2 m_3 \dots \alpha_{123\dots k} m_1 m_2 \dots m_k$$

$$x \equiv y \pmod{\prod_{i=1}^k m_i}$$

Modulární aritmetika

N ... největší číslo (křes v PC)

vzvolíme $m_1, m_2, \dots, m_k$ po dvou nesoudělná
tak, aby $\prod_{i=1}^k m_i > N$

$$x \mapsto (x_1, x_2, \dots, x_k) \quad x_i \equiv x \pmod{m_i}$$

$$y \mapsto (y_1, y_2, \dots, y_k)$$

$$x, y \mapsto (x_1 y_1, x_2 y_2, \dots, x_k y_k)$$

pomocí č. vč. a sčítání se vrátit, celkem jednodušší
v hardware
takže lze rychle násobit velká čísla

② m, m nesoudělná

$$f: \mathbb{Z}_{nm}^* \longrightarrow \mathbb{Z}_n^* \times \mathbb{Z}_m^*$$

f je izomorfismus

$$|\mathbb{Z}_{nm}^*| = \varphi(n \cdot m)$$

$$|\mathbb{Z}_n^* \times \mathbb{Z}_m^*| = \varphi(n) \cdot \varphi(m)$$

$$x \in \mathbb{Z}_{n,m}^*$$

$$x \mapsto (x_n, x_m) \quad \begin{aligned} x_n &\equiv x \pmod{n} \\ x_m &\equiv x \pmod{m} \end{aligned}$$

line

$$x \mapsto (x_n, x_m)$$

$$y \mapsto (y_n, y_m)$$

$$x \cdot y \mapsto (x_n \cdot y_n, x_m \cdot y_m)$$

Ukaze

$$\text{Ukazuje jime } \varphi(n \cdot m) = \varphi(n) \cdot \varphi(m)$$

③ $\mathbb{Z}_n^*$, kde n je square free $n = p_1 \cdot p_2 \cdots p_k$ ^{rusia} _{prvočísla}

$$\mathbb{Z}_n^* \cong \mathbb{Z}_{p_1}^* \times \mathbb{Z}_{p_2}^* \times \cdots \times \mathbb{Z}_{p_k}^*$$

$$\begin{array}{cccc} x^2 = 1 & 1 & 1 & 1 \\ & -1 & -1 & -1 \end{array}$$

2^k odmocnin x 1

$$G_1, * \quad G_2, \circ$$

$f: G_1 \rightarrow G_2$, kde f je prostě a na
je izomorfismus

$$\text{if } f(a * b) = f(a) \circ f(b)$$

Millerův test prvocelnosti

výstup: velké liché n

výstup: "složené" správně

"prvocíslo" pravděpodobně 50% správně

1. $n-1 = 2^k \cdot m$, m je liché
2. náhodně zvolíme $a \in \{1, \dots, n-1\}$
3. $a^m \equiv 1 \pmod{n}$, tak stop - "prvocíslo"
4. jinak $a^m, a^{2m}, a^{2^2m}, \dots, a^{2^{k-1}m} \neq a^{n-1}$
Když $a^{n-1} \not\equiv 1 \pmod{n}$ stop "složené"
5. jinak. Označme k to největší, že $a^{2^k m} \not\equiv 1$.
Když $a^{2^k m} \equiv -1 \pmod{n}$ stop "prvocíslo"
 $a^{2^k m} \not\equiv -1 \pmod{n}$ stop "složené"

n je prvocíslo

$$\mathbb{Z}_n^* = \{1, \dots, n-1\}$$

pro každé a $a^{n-1} = a^{2^k m} \equiv 1 \pmod{n}$

→ nemůžeme každé a v bodě 4

$$a^{2^k m} \not\equiv 1 \quad a^{2^{k+1} m} \equiv 1 \quad a \text{ je odmocnina z } 1$$

Když $a^{2^k m} \not\equiv -1$, tak n nemohlo být prvocíslo

n složené

n není prv. Carmichaelova tj. platí, že ne pro všechna

$$a \in \mathbb{Z}_n^* \quad \text{je} \quad a^{n-1} \equiv 1 \pmod{n} \quad \dots \text{to je složitější při}$$

$$n \text{ složené} \quad \varphi(n) \neq n-1$$

dokázat

$$\text{tj. ex } a \in \mathbb{Z}_n^* \text{ s } a^{n-1} \not\equiv 1 \pmod{n}$$

$$L = \{a \mid a \in \mathbb{Z}_n^*, \\ a^{n-1} \equiv 1\}$$

$$L \subsetneq \mathbb{Z}_n^* \quad L \text{ je podgrupa}$$

$$|\mathbb{Z}_n^* \setminus L| > 0 \quad |L| \leq \frac{1}{2} |\mathbb{Z}_n^*|$$

(4)

Okruhy, tělesa

$$\mathbb{Z}, \mathbb{Q}, \mathbb{R}, M_{n \times n}, \mathbb{Z}_n, \mathbb{Z}_p$$

$$\mathbb{Z}, +, -, 0, \cdot, 1$$

$(\mathbb{Z}, +, 0, -)$ komutativní grupa

$(\mathbb{Z}, \cdot, 1)$ komutativní monoid

$$a \cdot (b + e) = a \cdot b + a \cdot e$$

obruh (ring) $(R, +, \cdot)$

$(R, +, 0, -)$ je komutativní grupa

$(R, \cdot)$ je pologrupa

platí distributivní zákony

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

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

obruh s jednotkou $(R, \cdot, 1)$

Komutativní obruh $(R, \cdot)$ je komutativní

Dělitelé nuly jsou taková 2 čísla, která po vynásobení dají nulu

$$a, b, a \neq 0, b \neq 0 \text{ a platí } a \cdot b = 0$$

$$\textcircled{1} \quad a \cdot 0 = 0$$

$$a \cdot 0 = a \cdot (0 + 0) = a \cdot 0 + a \cdot 0$$

$$0 = a \cdot 0$$

Jsou-li a, b dělitelé nuly, pak $a \cdot 0 = a \cdot b$
a přesto $b \neq 0$ (nebo krátit a)

Těleso je komutativní obruh s jednotkou,

pro který $(R \setminus \{0\}, \cdot, 1)$ je grupa

tj. 1) pro každé $a \neq 0$ existuje a^{-1}

$$2) \quad 0 \neq 1$$

Pr. Teleso jeon $(\mathbb{Z}_p, +, \cdot, 0, 1)$ p prvoušlo
 $\mathbb{Q}, \mathbb{R}, \mathbb{C}$

$$\{a + bi \mid a, b \in \mathbb{Z}_3\}$$

$$i^2 = -1 = 2$$

$$(a+ib) + (c+id) = (a+c) + i(b+d)$$

$$(a+ib) \cdot (c+id) = a \cdot c - b \cdot d + i(ad+bc)$$

je teleso

$$\alpha = (2+i), (2+i)^2 = 0+i, (2+i)^3 = i(2+i) = 2+2i,$$

$$(2+i)^4 = i^2 = -1 = 2, (2+i)^5 = -2-i = 1+2i,$$

$$(2+i)^6 = -1-2i, (2+i)^7 = -2-2i = 1+i, (2+i)^8 = 1$$

0	1	2	i	1+i	2+i	2i	1+2i	2+2i
α^8	α^4	α^2	α^7	α	α^6	α^5	α^3	

$$x^2 + 1 = 0$$

$\mathbb{Z}_3$

$$x=0 \quad 0^2+1 = 1 \neq 0$$

$$1 \quad 1^2+1 = 2 \neq 0$$

$$2 \quad 2^2+1 = 1+1 = 2 \neq 0$$

?

F ... je těleso (field)

Polynom nad F je výraz

$$p(x) = a_0 + a_1x + a_2x^2 + \dots + a_nx^n \quad a_i \in F$$

nulový polynom $a_0 = a_1 = \dots = a_n = 0 \quad p(x) = 0$

stupěň polynomu - největší n , že $a_n \neq 0$ (když nenulový)

stupěň nulového polynomu - 1

Sčítání, odčítání, násobení

$$F[x] = \{ p(x) \mid p(x) \text{ je polynom nad } F \}$$

$(F[x], +, \cdot, 0, 1)$ je okruh

$$\begin{aligned} \text{sd}(p(x) \cdot q(x)) &= \text{sd}(p(x)) + \text{sd}(q(x)) & p(x), q(x) \text{ nenulové} \\ \text{sd}(p(x) + q(x)) &\leq \max(\text{sd}(p), \text{sd}(q)) \end{aligned}$$

Věta o dělení : pro daný dva polynomy f, g , $g \neq 0$.

Pak existují jednoznačně polynomy $p(x), r(x)$ tak,
že $f(x) = p(x) \cdot g(x) + r(x) \quad \text{sd}(r) < \text{sd}(g)$

indukcí podle stupně $f(x)$

a) $\text{sd}(f) < \text{sd}(g) \quad f(x) = 0 \cdot g(x) + f(x)$

b) $\text{sd}(f) \geq \text{sd}(g)$

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$$

$$g(x) = b_k x^k + b_{k-1} x^{k-1} + \dots + b_1 x + b_0$$

$$a_m x^m : b_k x^k = a_m b_k^{-1} x^{m-k}$$

$$f(x) - a_m b_k^{-1} x^{m-k} \cdot g(x) = f_1(x)$$

$$a_m x^{m-k} () - a_m b_k^{-1} x^{m-k} (b_k x^k + (cosi)) \quad \text{st } f_1 < \text{st } f$$

Kdyby

$$f(x) = p(x) \cdot g(x) + r(x)$$

$$\text{st } r < \text{st } g$$

$$f(x) = p_1(x) \cdot g(x) + r_1(x)$$

$$\text{st } r_1 < \text{st } g$$

$$\text{tak } p(x) \cdot g(x) + r(x) = p_1(x) \cdot g(x) + r_1(x)$$

$$\underbrace{(p(x) - p_1(x)) \cdot g(x)}_{\text{musí být nulový polynom}} = \underbrace{r_1(x) - r(x)}_{\text{st } < \text{st } g}$$

musí být nulový
polynom

Prvek $a \in F$ se nazývá kořen polynomu $f(x)$, if $f(a) = 0$

Př 1) $\mathbb{Z}_2[x]$ $f(x) = x^2 + 1$ $f(1) = 1^2 + 1 = 1 + 1 = 0$

$g(x)$ má kořen 1 v $\mathbb{Z}_2[x]$ iff má sudý počet členů

$$f(x) = x^2 + 1 \quad 0 \mapsto f(0) = 0^2 + 1 = 1$$

$$1 \mapsto f(1) = 1^2 + 1 = 0$$

$$g(x) = x + 1 \quad \nearrow$$

$$h(x) = x^3 + x^2 + x + 1$$

$\overline{F[x]}$ $g(x) \cdot (x-a)$ $f(x)$ vydělíme $g(x)$

$$f(x) = p(x) \cdot (x-a) + r(x)$$

$$\text{st } r < \text{st } (x-a) = 1$$

$$f(x) = p(x) \cdot (x-a) + r_0$$

dosadit a

$$f(x) = p(a) \underbrace{(a-1)}_0 + k_0$$

$$f(x) = p(x)(x-a) + f(a)$$

Lemma: Je-li $f(x)$ polynom nad F , pak $a \in F$ je kořen
 $f(x)$ iff $(x-a)$ dělí $f(x)$

Máme polynom $f(x)$ stupně $k > 0$, pak $f(x)$ má
nejvýše k kořenů.

Plati: Je-li F nekonečné těleso, pak pro dva
polynomy $f(x), g(x) \in F[x]$ platí

$$f = g \text{ iff } f(a) = g(a) \text{ pro každé } a \in F$$

f, g představují stejné funkce, $f(x) - g(x)$ má
kořeni jako F prvků (nekonečně)

$\Rightarrow f - g$ je nulový polynom

$\mathbb{F}_4$ $\mathbb{Z}_2$

$$f(x) = 3x^5 + 5x^2 + x + 2$$

$$g(x) = 4x^2 + 2$$

$$4^{-1} = 2$$

$$(3x^5 + 5x^2 + x + 2) : (4x^2 + 2) = 3 \cdot 2x^3 + 2 \cdot 2x + 5 \cdot 2$$

$$-(3x^5 + 5x^3)$$

$$2x^3 + 5x^2 + x + 2$$

$$-(2x^3 + x)$$

$$4x + 5x^2 + 2$$

$$-(5x^2 + 6)$$

3

(5)

$g(x)$ dělí $f(x)$ znamená: existuje polynom $h(x)$ tak, že
$$f(x) = h(x) \cdot g(x) \stackrel{c \neq 0}{=} (c \cdot g(x)) \cdot (c^{-1} \cdot h(x))$$

Př.: $(x^2 + 2) = (x+2)(x+1) \text{ v } \mathbb{Z}_3[x]$

$$2^{-1} = 2 = (2x+2)(2x+1) \\ 2(x+1) \quad 2(x+2)$$

asociované polynomy $f_1(x), f_2(x)$ znamená: existuje $c \neq 0$,
že $f_1(x) = c \cdot f_2(x)$

Lemma: Prvek $a \in F$ je kořen $f(x)$ iff $f(x)$ je dělitelné $(x-a)$

Důsledek: Každý polynom stupně $n \geq 1$ má nejvýše
 n kořenů (počítáno s jejich násobností).

Když a_1 je kořen, tak $f(x) = g_1(x) \cdot (x-a_1)$ s $g_1 = n-1$
 $g_1(x)$ má max. $n-1$ kořenů

— úvahy polynomy nad tělesem

Polynom $f(x) \in F[x]$ se nazývá ireducibilní,
jestliže nejde napsat jako $f(x) = g(x) \cdot h(x)$,
kde $\deg g, \deg h < \deg f$

(tj. když $f(x) = g(x) \cdot h(x)$, tak $\deg g = 0$ nebo $\deg h = 0$)

Je-li $F = \mathbb{Z}_p$, pro p prvočíslo, pak pro každé n
existuje ireducibilní polynom stupně n v $\mathbb{Z}_p[x]$

Plati: Je-li f stupně ≤ 3 , pak f je ireducibilní
iff nemá kořen.

Ireducibilní:

$\mathbb{Z}_2[x]$ $x+1, x$ 1. st.

x^2+x+1 2. st.

x^3+x+1, x^3+x^2+1

x^4+x+1

$x^2, x^2+1, x^2+x, x^2+x+1$
 $x \cdot x \quad (x+1)(x+1), x(x+1)$

$x^3, x^3+1, x^3+x+1, x^3+x^2, x^3+x^2+1,$
 $x^3+x^2+x+1 \quad x^3+x^2+x$

Polynom je nazývá monický, má-li $a_n=1$ pro n stupeň polynomu.

Věta: Každý polynom $f(x) \in F[x]$ lze psát

$$f(x) = c \cdot p_1(x) \cdot p_2(x) \cdot \dots \cdot p_n(x)$$

$p_1(x), \dots, p_n(x)$ jsou různé monické ireducibilní polynomy

$F[x]$ Máme polynomy $f(x), g(x)$. Polynom $h(x)$ je společný dělitel $f(x), g(x)$, if $h(x) | f(x), h(x) | g(x)$

$d(x)$ je největší spol. dělitel $f(x), g(x)$ if

1) $d(x) | f(x), d(x) | g(x)$

(2) když $h(x) | f(x), h(x) | g(x)$, tak $h(x) | d(x)$
 $d(x)$ má největší stupeň

jestli $d_1(x), d_2(x)$ dva největší spol. dělitele, pak jsou asociovány.

Eukleidův algoritmus

Vstup: $a(x), b(x)$ polynomy z $F[x]$

Výstup: největší a nejv. spol. dělitel

1) if $\deg a \geq \deg b$, then $u(x) := a(x)$, $v(x) := b(x)$
else $u(x) := b(x)$, $v(x) := a(x)$

2) Vydělíme $u(x)$ polynomen $v(x)$
 $u(x) = h(x) \cdot v(x) + r(x)$ $\deg r < \deg v$

3) if $r(x) = 0$, then $d(x) := v(x)$, stop
else $u(x) := v(x)$, $v(x) := r(x)$, goto 2

každý spol. dělitel $u(x)$ a $v(x)$ je spol. dělitel $v(x)$ a $r(x)$
a naopak každý dělitel $v(x)$ a $r(x)$ je dělitel
 $u(x)$ a $v(x)$ $u(x) = h(x) \cdot v(x) + r(x)$
 $= u(x) - h(x) \cdot v(x)$

Bezoutova věta

Je-li $d(x)$ největší spol. dělitel $a(x), b(x)$, pak existují polynomy $h(x)$ a $k(x)$ tak, že $a(x) \cdot h(x) + b(x) \cdot k(x) = d(x)$

V $\mathbb{Z}_2[x]$, $a(x) = x^5 + 1$, $b(x) = x^2 + 1$

$$\begin{array}{r} (x^5 + 1) : (x^2 + 1) = x^3 + x \\ \underline{x^3 + 1} \\ x + 1 \end{array}$$

$$\begin{array}{r} (x^2 + 1) : (x + 1) = x + 1 \\ \underline{x + 1} \\ 0 \end{array}$$

$$\begin{array}{ccccc} (x+1) & = & (x^5+1) & + & (x^3+x) \cdot (x^2+1) \\ a_1(x) & & a(x) & & h(x) \cdot b(x) \end{array}$$

$$\begin{array}{c} x^5 + 1 = (x^3 + x)(x^2 + 1) + (x + 1) \\ \underbrace{}_{a(x)} \quad \underbrace{}_{b(x)} \quad \underbrace{}_{r(x)} \\ \swarrow \quad \searrow \\ x^2 + 1 = (x + 1)(x + 1) + 0 \end{array}$$

gcd... $x + 1$

$$h(x) = 1 \quad k(x) = x^3 + x$$

Věta: Pro polynomy $a(x), b(x) \in F[x]$ existují polynomy $h(x), k(x) \in F[x]$ tak, že

$$a(x) \cdot h(x) + b(x) \cdot k(x) = 1$$

iff 1 je největší spol. dělitel (tj $a(x), b(x)$ nesoudělné)

Twreňi: Jestliže ireducibilní polynom $m(x)$ dělí $a(x) \cdot b(x)$, pak $m(x)$ dělí $a(x)$ nebo $b(x)$

- Když $m(x)$ dělí $a(x)$, tak platí

Když $m(x)$ nedělí $a(x)$.. $a(x), m(x)$ nesoudělné

$$1 = h(x) \cdot m(x) + k(x) \cdot a(x) \quad | b(x)$$

$$b(x) = h(x) b(x) m(x) + k(x) \cdot a(x) \cdot b(x) \quad \text{tj } m(x) | b(x)$$

$m(x)$ je polynom z $F[x]$

Na $F[x]$ definujeme relaci $\equiv (\text{mod } m(x))$ takto:

$$a(x) \equiv b(x) (\text{mod } m(x)) \quad \text{iff}$$

$a(x) - b(x)$ je dělitelný $m(x)$

Platí: $a(x) \equiv b(x) (\text{mod } m(x))$ iff

$a(x)$ i $b(x)$ mají stejný zbytek při dělení polynomen $m(x)$

$\equiv (\text{mod } m(x))$ je ekvivalence na $F[x]$ a navíc

$$\left. \begin{array}{l} a(x) \equiv b(x) (\text{mod } m(x)) \\ c(x) \equiv d(x) (\text{mod } m(x)) \end{array} \right\} \Rightarrow \begin{array}{l} a(x) + c(x) \equiv b(x) + d(x) (\text{mod } m(x)) \\ a(x) \cdot c(x) \equiv b(x) \cdot d(x) (\text{mod } m(x)) \end{array}$$

$F[x]/m(x) \dots$ množina všech tříd ekvivalence
 $\equiv (\text{mod } m(x))$

$$\{f(x) \mid f(x) \in F[x], \text{st } f < \text{st } m\}$$

$f(x) + g(x)$ obvyklé sečítání polynomů

$f(x) \odot g(x) = h(x)$ $h(x)$ je zbytek při dělení

$f(x) \cdot g(x)$ polynomem $m(x)$

Př

$$\mathbb{Z}_2[x] \quad m(x) = x^2 + 1$$

$$\mathbb{Z}_2[x]/x^2+1$$

$$\mathbb{Z}_2[x]/x^2+1 = \{0, 1, x, x+1\}$$

+	0	1	x	x+1
0	0	1	x	x+1
1	1	0	x+1	x
x	x	x+1	0	1
x+1	x+1	x	1	0

$\odot$	0	1	x	x+1
0	0	0	0	0
1	0	1	x	x+1
x	0	x	1	x+1
x+1	0	x+1	x+1	0

$$x^2 : (x^2 + 1) = 1$$

①

$$(x+1)(x+1) = x^2 + 1$$

$$(x^2 + x) : (x^2 + 1) = 1$$

x+1

4 stránky Karlosak

T *Seteno*

$T[x]$... polynomy nad T
 $\equiv \text{mod } m(x)$ relace na $T[x]$

Platí: ^{když} $a(x) \equiv c(x) \pmod{m(x)}$
 $b(x) \equiv d(x) \pmod{m(x)}$, pak

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

3.4.07

iff $a(x) - b(x)$ je dělitelné $m(x)$

$$[a(x) - b(x) = k(x) \cdot m(x) \text{ pro nějaké } k(x) \in T[x]]$$

$$(a(x) + b(x)) \equiv (c(x) + d(x)) \pmod{m(x)}$$

$$a(x) \cdot b(x) \equiv c(x) \cdot d(x) \pmod{m(x)}$$

$$\mathbb{Z} \equiv (\text{mod } n)$$

$i + j$ = zbytek při dělení

$$\mathbb{Z}_m = \{[0]_m, \dots, [m-1]_m\}$$

$$i \cdot j$$

$$\mathbb{Z}_m = \{0, 1, \dots, m-1\}$$

$$T[x] / m(x)$$

$$\{[f(x)]_{m(x)} \mid f(x) \in T[x]\}$$

$$[f(x)]_{m(x)} = \{g(x) \mid f(x) \equiv g(x) \pmod{m(x)}\}$$

$$\mathbb{R}[x] / x^2 + 1$$

$$f(x) = q(x) \cdot m(x) + r(x) \quad \text{sd } r < \text{sd } m$$

$$= \{a+bx \mid a, b \in \mathbb{R}\}$$

$$(a+bx) + (c+dx) = (a+c) + (b+d)x$$

$$(a+bx) \cdot (c+dx) = ac + (bc+ad)x + bdx^2$$

$$(bdx^2 + (bc+ad)x + ac) : (x^2+1) = bd$$

$$\begin{array}{r} bdx^2 \quad - bdx^2 \\ \hline -bd \end{array}$$

$$\boxed{ac - bd + (bc+ad)x}$$

→ podobná se násobení komplexních čísel:

$$\boxed{i^2 + 1 = 0}$$

$$\boxed{i^2 = -1}$$

$$T[x]/m(x) = \{f(x) \mid \text{st } f < \text{st } m\}$$

+ sčítání

$f_1(x) \cdot f_2(x) = h(x)$ -- $h(x)$ je zbytek při dělení $f_1(x)f_2(x)$ polynomen $m(x)$.

$(T[x]/m(x), +, 0)$ grupa komutativní

$(T[x]/m(x), \cdot, 1)$ komutativní monoid

→ platí distributivní zákony

$(T[x]/m(x), +, \cdot)$ komutativní okruh s 1.

Jestliže $m(x) = h(x) \cdot g(x)$, $\text{st } h, \text{st } g < \text{st } m$

$h(x), g(x) \in T[x]/m(x)$

$$h(x) \cdot g(x) = 0 \text{ v } T[x]/m(x)$$

příčina:
 $h(x) \neq 0 \neq g(x)$

$h(x), g(x)$ dělitele nuly

$T[x]/m(x)$ není těleso

f -li $m(x)$ ireducibilní, pak $(\mathbb{Z}[x]/m(x), +, \cdot)$ je těleso.

$$f(x) \neq 0 \text{ ať } f < \text{ať } m$$

hledáme $g(x)$ tak, že $f(x) \odot g(x) = 1$

$f(x), m(x)$ jsou nesoudělné, Bezoutova věta říká:

$$1 = a(x) \cdot f(x) + b(x) \cdot m(x) \rightarrow f(x) \cdot g(x) = 1 + k(x) \cdot m(x)$$

hledáme $g(x)$:

$$f(x) \cdot g(x) - 1 = k(x) \cdot m(x)$$

$$a(x) \cdot f(x) + b(x) \cdot m(x) = 1$$

$$f^{-1}(x) \equiv a(x) \pmod{m(x)}$$

Pr.: $\mathbb{Z}_2[x]/x^4+x+1$
 $\hookrightarrow$ je ireducibilní

$$GF(2^4) = GF(16)$$

$\hookrightarrow$ Galoisovo těleso

$$f(x) = x^4 + x + 1$$

	x^4+x+1	x^3+x+1
x^2+1	1	x
x^2+x+1	0	1
$x(x^2+1)$	x	x^2
1	x	$(1+x^2)$

zkontroluj:

$$\begin{array}{r} x^5 + x^2 + x + 1 \\ x^4 + x + 1 \\ \hline x^2 + x + 1 \end{array} \quad \begin{array}{r} (x^5 + x^2 + x + 1) : (x^4 + x + 1) = x \\ x^5 + x^2 + x \\ \hline 1 \end{array}$$

$$(x^4+x+1) : (x^3+x+1) = x$$

$$(x^4+x+1) = x \cdot (x^3+x+1) + (x^2+1)$$

$$(x^3+x+1) : (x^2+1) = x$$

$$(x^3+x+1) = x \cdot (x^2+1) + 1$$

$$1 = x \cdot m(x) + (1+x^2) \cdot f(x)$$

$\mathbb{Z}_p$ p je prvočíslo, $m(x)$ je ireducibilní polynom v $\mathbb{Z}_p[x]$ stupně k ,
 pak $\mathbb{Z}_p[x]/m(x)$ je těleso o p^k prvcích

Máme konečné těleso T , $1 \in T$

existuje číslo p , nejmenší takové, že:

$$\underbrace{1+1+\dots+1}_{p\text{-krát}} = 0$$

$$1, 1+1, 1+1+1, \dots$$

$$\underbrace{1+1+\dots+1}_{i\text{-krát}} = \underbrace{1+1+\dots+1}_{j\text{-krát}} \quad i < j \rightarrow \underbrace{0}_{j-i\text{-krát}} = 1+1+\dots+1$$

Platí: p je prvočíslo

→ důkaz sporem: kdyby $p = r \cdot s$

$$\underbrace{(1 + \dots + 1)}_r \cdot \underbrace{(1 + \dots + 1)}_s = \underbrace{1 + \dots + 1}_{r \cdot s = p} = 0$$

↑ součin v tělese dává 0

v tělese, tj. buď $\underbrace{1 + \dots + 1}_{r\text{-krát}} = 0$

nebo $\underbrace{1 + \dots + 1}_{s\text{-krát}} = 0$

p je charakteristika tělesa:

$$\mathbb{Z}_p \subseteq T$$

$$0 \mapsto 0$$

$$1 \mapsto 1$$

$$2 \mapsto 1+1$$

$$3 \mapsto 1+1+1$$

$$\vdots$$

$$p-1 \mapsto \underbrace{1+1+\dots+1}_{p-1\text{ krát}}$$

Př.: $\mathbb{Z}_2[x]/x^3+x+1$

Platí: Je-li F konečné těleso, pak $(F \setminus \{0\}, \cdot, 1)$ je cyklická grupa,
tj. má generátor, tj. $\alpha \in F$ takový: $\{\alpha, \alpha^2, \dots, \alpha^{p-1}\} = F \setminus \{0\}$

$$\alpha = x$$

$$\alpha^2 = x^2$$

$$\alpha^3 = x+1$$

$$\alpha^4 = x^2+x$$

$$\alpha^5 = x^2+x+1$$

$$\alpha^6 = x^2+1$$

$$\alpha^7 = 1$$

$$x^3+x+1=0$$

$$x^3 = x+1$$

$$x(x^2+x) = \underbrace{x^3}_{x+1} + x^2 = x^2+x+1$$

$$x^3 = x+1$$

$$x^3+x^2+x = x+1+x^2+x$$

$$x^3+x = x+1+x = 1$$

$$(x^2+1)^{-1} = (\alpha^6)^{-1} = \alpha = x$$

0	----	0
1	----	α^7
x	----	α^1
x+1	----	α^3
x ²	----	α^2
x ² +1	----	α^6
x ² +x	----	α^4
x ² +x+1	----	α^5

⑦

① F je konečné těleso. Pak existuje prvotnílo p tak, že

$$\mathbb{Z}_p \subseteq F \quad \{0, 1, 2, \dots, p-1\} \dots 1 \in F \quad 1, 1+1, \dots \underbrace{1+1+\dots+1}_{p-1}, 0$$

② Je-li F těleso charakteristiky p , pak $(a+b)^p = a^p + b^p$

$$\text{tj. } (a_1 + a_2 + \dots + a_k)^p = a_1^p + a_2^p + \dots + a_k^p$$

binom. věta

$$(a+b)^p = a^p + \binom{p}{1} a^{p-1} b + \dots + \binom{p}{p-1} a b^{p-1} + b^p$$

$$\binom{p}{i} = \frac{p!}{i!(p-i)!} \quad \binom{p}{i} \cdot \underbrace{i!}_{\substack{\text{není} \\ \text{děl} \\ p}} \cdot \underbrace{(p-i)!}_{\substack{\text{není} \\ \text{děl} \\ p}} = p!$$

$$1 \leq i \leq p-1$$

dělitelné p

p je prvotnílo!

$p \nmid i!, p \nmid (p-i)!$

$$\text{tedy } p \mid \binom{p}{i}$$

$$\begin{aligned} (a_1 + a_2 + \dots + a_k)^p &= (a_1 + \dots + a_{k-1} + a_k)^p = (a_1 + \dots + a_{k-1})^p + a_k^p = \dots = \\ &= a_1^p + a_2^p + \dots + a_k^p \end{aligned}$$

③ Pro každé konečné těleso F existuje $\alpha \in F$ tak, že

$$\{\alpha, \alpha^2, \dots, \alpha^{|F|-1} = 1\} = F \setminus \{0\}.$$

tj. α je generátor $(F \setminus \{0\}, \cdot)$. Takové α se nazývá
primitivní prvek tělesa F .

Primitivních prvků je $\varphi(m-1)$, kde $m = |F|$

④ Je-li p prvočíslo a $m(x)$ ireducibilní polynom
v $\mathbb{Z}_p[x]$, pak $\mathbb{Z}_p[x]/m(x)$ je konečné těleso
o p^k prvcích, kde $k = \deg m$.

⑤ Pro každé prvočíslo p a každé $k \geq 1$ existuje
(až na isomorfismus) jediné konečné těleso
o p^k prvcích. Tj. pro každé k existuje
ireducibilní polynom stupně k .

$\mathbb{Z}_p[x]/m(x)$ z je kořen polynomu

$$z = x$$

$$m(z) = 0$$

Př. $\mathbb{Z}_2[x]/x^4+x+1 = \{f(z), \deg f < 4\}$

$$z = [x] \quad z^4 + z + 1 = 0 \quad \boxed{z^4 = -z - 1}$$

$$m(x) = x^4 + x + 1$$

$$[x]^4 + [x] + 1 = [x^4 + x + 1] = 0$$

Kódování

Zpráva $\{0,1\}^k \rightsquigarrow \{0,1\}^n$

$$\psi: \{0,1\}^k \rightarrow \{0,1\}^n \quad n > k$$

ψ je prosté

$$\psi(\{0,1\}^k) = K \subseteq \mathbb{Z}_2^n$$

informační
slovo

Kód

Př. 1) Kód kontroly parity

$$n = k + 1$$

$$n \in \mathbb{Z}_2$$

$$\psi(x_1, \dots, x_k) = \underbrace{x_1 \dots x_k}_{\text{informační slovo}} \underbrace{x_{k+1}}_{\text{kontrolní slovo}}$$

$$x_1 + \dots + x_k + x_{k+1} = 0$$

2) Opakovací kód

$$\psi(x) = \underbrace{xxxxx}_{\substack{\text{inf.} \\ \text{slovo} \\ 4 \text{ kontrolní}}}$$

$K \dots$ kód blokový $K \subseteq \mathbb{Z}^n$

Hammingova vzdálenost

$$u, v \in K \quad d_H(u, v) = |\{i \mid u_i \neq v_i\}|$$

Minimální vzdálenost kódu

$$d = \min \{d_H(u, v) \mid u \neq v, u, v \in K\}$$

Je-li d minimální vzdálenost k , pak je možné
dostát k $t < d$ chybám, pak jsme dostali slovo,
které není kódové, tj. K objevuje t -násobné chyby.
Opravuje $t < \frac{d}{2}$ chyb.

Lineární blokové kódy

$K \subseteq \mathbb{Z}_p^n$, kde K je lineární podprostor $\mathbb{Z}_p^n$

$$\mathbb{R}^n = \{a_1, \dots, a_n \mid a_i \in \mathbb{R}\}$$

$$\mathbb{Z}_p^n = \{a_1, \dots, a_n \mid a_i \in \mathbb{Z}_p\}$$

$$a_1 \dots a_m + b_1 \dots b_m = (a_1 + b_1)(a_2 + b_2) \dots (a_m + b_m)$$

$$c \cdot (a_1 \dots a_m) = ca_1 ca_2 \dots ca_m$$

K je lineární iff součet dvou kódových slov je kódové slovo a násobek kódového slova je kódové slovo

váha $u \in \mathbb{Z}_p^n$, $\|u\|$ = počet nenulových bitů

$$d = \min \{ \|u\| \mid u \in K \}$$

$$d = d_H(u, v) = \|u - v\| \quad \|u\| = d_H(u, 0)$$

$$u - v \in K$$

K je lineární blokový (n, k) kód parametř, kde

K je lin. podprostor $\mathbb{Z}_p^n$ dimenze k .

$g_1, \dots, g_k \dots$ báze K

$$u \in K \Leftrightarrow u = \alpha_1 g_1 + \dots + \alpha_k g_k \quad \alpha_i \in \mathbb{Z}_p$$

generující matice kodu K

$$G = \begin{pmatrix} g_1 \\ g_2 \\ \vdots \\ g_k \end{pmatrix} \quad (\alpha_1, \dots, \alpha_k) \begin{pmatrix} g_1 \\ g_2 \\ \vdots \\ g_k \end{pmatrix} = \alpha_1 g_1 + \alpha_2 g_2 + \dots + \alpha_k g_k$$

$$\underbrace{\mu_1 \dots \mu_k}_{\text{inf. směr}} \left(E_k \mid B \right) = \underbrace{\mu_1 \dots \mu_k}_{\text{inf. směr}} \underbrace{\mu_{k+1} \dots \mu_n}_{\text{stavová mat. - systematický kód}}$$

$$\psi: \mu_1 \dots \mu_k \longrightarrow \underbrace{\mu_1 \dots \mu_k}_{\text{inf. sm.}} \underbrace{\mu_{k+1} \dots \mu_n}_{\text{konst. směr}}$$

Ke každému lin. prostoru $K \subseteq \mathbb{Z}_p^n$ existuje matice H s lin. nezávislými řádky tak, že

$$u \in K \text{ iff } H \cdot u^T = 0^T$$

Je-li K systematický, $G = (E_k | B)$

Pak $H = (-B^T | E_{n-k})$ splňuje

$$H \cdot G^T = (-B^T | E_{n-k}) \cdot \begin{pmatrix} E_k \\ B^T \end{pmatrix} = -B^T + B^T = 0$$

H je kontrolní matice a platí

$$u \in K \text{ iff } H \cdot u^T = 0^T$$

$u \in K$ bylo vysláno, přijali jsme $v = u + e$ chybové slovo
syndrom

$$H \cdot v^T = H \cdot (u + e)^T = H \cdot (u^T + e^T) = \underbrace{H \cdot u^T}_{0^T} + H \cdot e^T = H \cdot e^T \neq 0^T$$

přijata chyba

Kód K objevuje t -násobně chyby iff každých t sloupců matice H je lineárně nezávislých.

(8)

Cyklické kódy

lineární blokové kódy, kde pro každé kódové slovo $v = v_0 v_1 \dots v_{m-1}$ je $v_{m-1} v_0 \dots v_{m-2}$ také kódové slovo

Pr $m=4$ 0000, 1001, 0101, 0011, 1100, 0110, 1010, 1111 $x^4=1$

$$u(x) = u_0 + u_1 x + u_2 x^2 + u_3 x^3$$

$$x \cdot u(x) = u_0 x + u_1 x^2 + u_2 x^3 + u_3 x^4$$

$$u_3 + u_0 x + u_1 x^2 + u_2 x^3$$

u ... polynomy $\mathbb{Z}_p[x]/x^m-1$

$$= T^{(m)}$$

$$u(x) = u_0 + u_1 x + \dots + u_{m-1} x^{m-1} \leftrightarrow u_0 \dots u_{m-1}$$

k Pr představá jako polynomy

$$0, 1+x^3, 1+x^2, 1+x, x^2+x^3, x+x^2, x+x^3, 1+x+x^2+x^3$$

Máme cyklický kód K a $g(x) \in K$, pak

$f(x)g(x) \in K$ pro každé $f(x) \in T^{(m)}$

$$\begin{matrix} a_0 & g(x) + a_1 x \cdot g(x) + a_2 x^2 g(x) + \dots + a_{m-1} x^{m-1} g(x) \\ & \in K & \in K & \in K \end{matrix}$$

$$(a_0 + a_1 x + a_2 x^2 + \dots + a_{m-1} x^{m-1}) \cdot g(x) \in K$$

$0, 1+x$.. polynom nižšího stupně

$$1+x^3 = (1+x)(1+x+x^2)$$

$$1+x^2 = (1+x)(1+x)$$

$$x+x^2 = (1+x)x$$

$$1+x+x^2+x^3 = (1+x)(1+x^3)$$

$$x+x^3 = (1+x)(x+x^2)$$

$$x^2+x^3 = (1+x)x^2$$

$$1+x = (1+x) \cdot 1$$

každý jím dělitelný

Twzení: Je-li K cyklický (n, k) kód.

Pak existuje polynom $g(x)$ takový, že

- 1) $K = \{ f(x) \cdot g(x) \mid f(x) \in T(n) \}$
- 2) $g(x), x \cdot g(x), \dots, x^{k-1} \cdot g(x)$ je báze K
- 3) $g(x)$ dělí $x^n - 1$

$g(x)$ polynom K nerulový, nejmenšího stupně

$$v(x) \in K \quad v(x) = a(x) \cdot g(x) + \cancel{b(x)} \quad \text{st } b < \text{st } g$$

$$\underbrace{v(x)}_{\in K} = \underbrace{a(x) \cdot g(x)}_{\in K} + \cancel{b(x)}$$

$$\uparrow \quad \text{tj } b(x) \in K$$

$$b(x) = 0 \quad \text{a i } b(x) = 0$$

kdyby

$$a_0 g(x) + a_1 x g(x) + \dots + a_{k-1} x^{k-1} g(x) = 0$$

$$\underbrace{(a_0 + a_1 x + \dots + a_{k-1} x^{k-1})}_{\in T(n)} \cdot g(x) = 0$$

$$(a_0 + a_1 x + \dots + a_{k-1} x^{k-1}) g(x) = 0$$

muselo by být děl x^{n-1}

$$(x^n - 1) = a(x) \cdot g(x) + b(x) \quad \text{st } b < \text{st } g$$

$$\in T(n) \quad 0 = a(x) \cdot g(x) + b(x) \quad b(x) = 0 \in T(n)$$

$$b(x) = 0$$

$$g(x) \text{ dělí } x^{n-1}, \text{ tj } x^n - 1 = g(x) \cdot h(x)$$

$h(x)$... kontrolní polynom

$g(x)$ - generující polynom

$$v(z) \in K \text{ iff } h(z) \cdot v(z) = 0$$

$$v(z) = a(z) \cdot g(z) \quad h(z) \cdot v(z) = h(z) \cdot a(z) \cdot g(z) = 0$$

$$\text{kdýř } h(z) \cdot v(z) = 0 \quad v \in T^{(n)}$$

$$h(x) \cdot v(x) = a(x) \cdot g(x) + b(x) \quad \text{[ad b and g]}$$

$$h(x) \cdot v(x) = h(x) \cdot a(x) \cdot g(x) + h(x) \cdot b(x)$$

$$h(z) \cdot b(z) = 0$$

$$h(x) \cdot b(x) \text{ je dělitel } x^{n-1}$$

$$g(z) = g_0 + g_1 z + \dots + g_{m-k} z^{m-k}$$

generující polynom

$$G = \begin{pmatrix} g(z) \\ z g(z) \\ \vdots \\ z^{k-1} g(z) \end{pmatrix} = \begin{pmatrix} g_0 & g_1 & \dots & g_{m-k} & 0 & \dots & 0 \\ 0 & g_0 & g_1 & \dots & g_{m-k} & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & \dots & \dots & g_0 & \dots & \dots & \dots & \dots \end{pmatrix}$$

$$P_1 \quad 1+z$$

$$G = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix}$$

$$h(z) = h_0 + h_1 z + \dots + h_k z^k$$

$$H = \begin{pmatrix} \overbrace{0 \dots 0}^{n-k-1} & h_k & \dots & h_1 & h_0 \\ 0 & \dots & h_k & \dots & h_0 & 0 \\ \vdots & & & & & \\ h_k & \dots & h_0 & 0 & \dots & 0 \end{pmatrix} \begin{pmatrix} v_0 \\ v_1 \\ \vdots \\ v_{n-1} \end{pmatrix}$$

$$h_0 v_{n-1} + h_1 v_{n-2} + h_2 v_{n-3} + \dots + h_k v_{n-k}$$

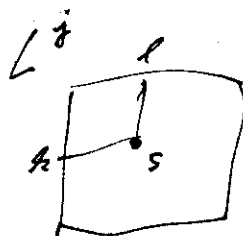
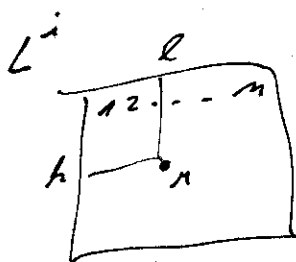
Latinský čtverec

je "matice" $n \times n$, kde v každém řádku jsou
všechny $1, \dots, n$, v každém sloupci jsou všechny od 1 do n

je-li G grupa $G = 1, \dots, n$

+	1	2	3	...	n
1	1	2	3	...	n
2	2	3	4	...	1
3	3	4	5	...	2
...	...	...	...	...	...
n	...	...	...	...	...

Máme dva latinské čtverce



ortogonální - na sebe
kolmý

(i, s) - pro každé souř. i, s dá jinou dvojici

$$n = p^k \quad GF(n) \quad \dots \quad \alpha, \alpha^2, \dots, \alpha^{n-1} = 1, 0$$

+	α	α^2	...	α^{n-1}	0
0	α	α^2	...	α^{n-1}	0
α^i	$\alpha^i + \alpha$	$\alpha^i + \alpha^2$	...	$\alpha^i + \alpha^{n-1}$	α^i
α^{i+1}	$\alpha^{i+1} + \alpha$	$\alpha^{i+1} + \alpha^2$	...	$\alpha^{i+1} + \alpha^{n-1}$	α^{i+1}
α^{i+2}	$\alpha^{i+2} + \alpha$	$\alpha^{i+2} + \alpha^2$	...	$\alpha^{i+2} + \alpha^{n-1}$	α^{i+2}
...	...	...	...	...	...
i	$\alpha^i + \alpha$	$\alpha^i + \alpha^2$	...	$\alpha^i + \alpha^{n-1}$	α^i

nahradiťme

$$\alpha \rightarrow 1$$

$$\alpha^2 \rightarrow 2$$

$$\alpha^i \rightarrow i$$

$$0 \rightarrow n$$

$$\alpha^i + \alpha^j = \alpha^s + \alpha^n \quad s = n$$

$$\alpha^i + \alpha^0 = \alpha^i + \alpha^2 \quad i = j$$

a je to latinský čtverec :-0

$\mathbb{P}_M$ $\mathbb{Z}_5$ $\{0, 1, 2, 3, 4\}$

$$\alpha = 2 \quad \alpha^2 = 4 \quad \alpha^3 = 3 \quad \alpha^4 = 1$$

	α	α^2	α^3	α^4	0
0	α	α^2	α^3	α^4	0
α^3	0	α	α^4	α^2	α^3
$1 = \alpha^4$	α^3	0	α^2	α	α^4
$\alpha = \alpha^5$	α^2	α^4	0	α^3	α
$\alpha^2 = \alpha^6$	α^4	α^3	α	0	α^2

1	2	3	4	5
5	1	4	2	3
3	5	2	1	4
2	4	5	3	1
4	3	1	5	2

Plati: je-li $i \neq j$, jsou L^i a L^j ortogonální
latinské čtverce

(9)

viz slajdy

(10)

nebyl

(11)

$(A, \subseteq)$
uspořádání

reflexivní - vztah sám se sebou

antisym. - $A \subseteq B$ a $B \subseteq A$ pak $A = B$

transitivní $A \subseteq B, B \subseteq C$ pak $A \subseteq C$

$$c = \sup \{a, b\}$$

je 1) horní mez $a \subseteq c, b \subseteq c$

2) nejmenší horní mez

tedy $a \subseteq d, b \subseteq d$, pak $c \subseteq d$

$d = \inf \{a, b\}$ je největší dolní mez

$(A, \subseteq)$ je swaz, jestliže pro každé $a, b \in A$ existuje $\sup \{a, b\}, \inf \{a, b\}$

$$a \vee b = \sup \{a, b\} \quad \text{spojení}$$

$$a \wedge b = \inf \{a, b\} \quad \text{průsečík}$$

$$1) a \vee a = a \quad a \wedge a = a$$

$$2) a \vee b = b \vee a \quad a \wedge b = b \wedge a$$

$$3) a \vee (b \wedge c) = (a \vee b) \wedge c \quad a \wedge (b \vee c) = (a \wedge b) \vee c$$

$$4) a \vee (b \wedge a) = a \quad a \wedge (b \vee a) = a$$

$a \subseteq b$
$a \vee b = b$
$a \wedge b = a$
$a \subseteq a \vee b$
$b \subseteq a \vee b$

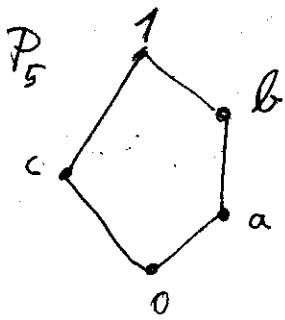
Věta: Jestliže A s dvěma operacemi $\vee, \wedge$ splňujícími 1) - 4),
pak relace $\subseteq$ definovaná $a \subseteq b \text{ iff } a \vee b = b \text{ iff } a \wedge b = a$
je uspořádaná a $\sup_{\subseteq} \{a, b\} = a \vee b, \inf_{\subseteq} \{a, b\} = a \wedge b$
(opravdu důležitá věta)

Platí: V každém swazu ① $a \vee (b \wedge c) \subseteq (a \vee b) \wedge (a \vee c)$

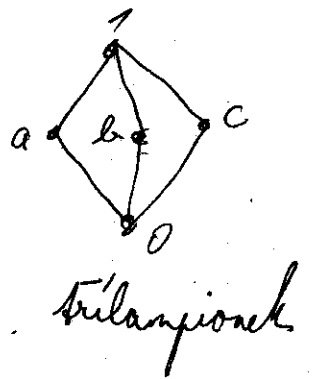
$$② (a \wedge b) \vee (a \wedge c) \subseteq a \wedge (b \vee c)$$

$$\begin{aligned} ① \quad & \left. \begin{aligned} a &\subseteq a \vee b \\ a &\subseteq a \vee c \end{aligned} \right\} a \text{ je dolní mez } (a \vee b), (a \vee c), \\ & \text{tj. } a \subseteq (a \vee b) \wedge (a \vee c) \end{aligned}$$

$$\begin{aligned} b \wedge c &\subseteq b \subseteq a \vee b \text{ tj. } (b \wedge c) \text{ je dolní mez } (a \vee b), (a \vee c), \\ b \wedge c &\subseteq c \subseteq a \vee c \text{ tj. } b \wedge c \subseteq (a \vee b) \wedge (a \vee c) \end{aligned}$$



...
rose není distributivní svaz ;



Tvrzení: $\forall$ svazu $(L, \subseteq, \cap, \cup)$

$$a \cup (b \cap c) = (a \cup b) \cap (a \cup c) \quad \text{iff}$$

$$a \cap (b \cup c) = (a \cap b) \cup (a \cap c)$$

D: Předp., že $a \cup (b \cap c) \stackrel{(*)}{=} (a \cup b) \cap (a \cup c) \quad \forall a, b, c \in L$

$$(a \cap b) \cup (a \cap c) = x \cup (a \cap c) \stackrel{(*)}{=} (x \cup a) \cap (x \cup c) =$$

$$\stackrel{(*)}{=} ((a \cap b) \cup a) \cap ((a \cap b) \cup c) = a \cap (c \cup (a \cap b)) \stackrel{(*)}{=}$$

$$= a \cap ((c \cup a) \cap (c \cup b)) = (a \cap (c \cup a)) \cap (c \cup b) =$$

$$= \underline{a \cap (b \cup c)}$$

Svaz je distributivní, platí-li aspoň jeden z distributivních zákonů (pak platí oba)

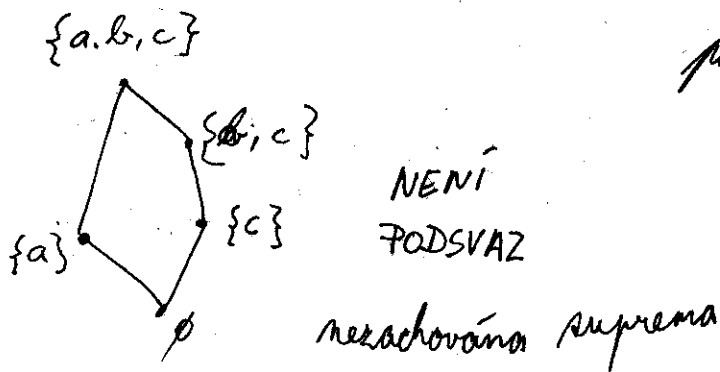
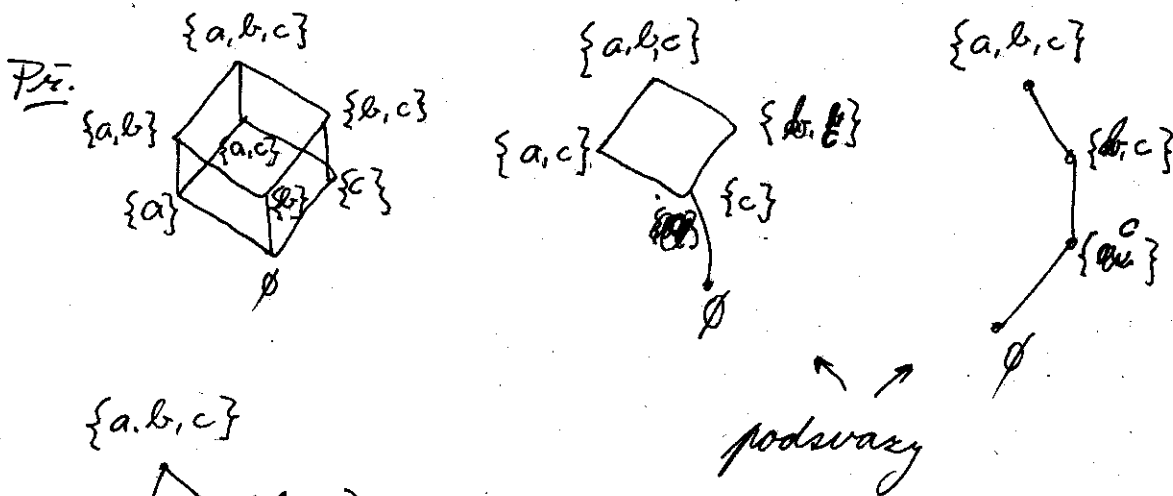
Pr. $L = \mathcal{N}$

$$a \subseteq b \quad \text{iff} \quad b = k \cdot a$$

$$a \cup b = \text{lcm} \{a, b\} \quad \text{least common multiple}$$

$$a \cap b = \text{gcd} \{a, b\}$$

Máme svaz $(L, \sqsubseteq, \vee, \wedge)$. Množina $M \subseteq L$ tvoří
podsvaz pro každé $a, b \in M$, $a \vee b \in M$, $a \wedge b \in M$



Věta: Svaz je distributivní iff neobsahuje $\diamond$ ani $\lozenge$
jako podsvaz.

Máme svaz $(L, \sqsubseteq, \vee, \wedge, 0, 1)$ 0 .. nejmenší
 1 .. největší

Prvek b je doplněk (komplement) prvku a , jestliže
 $a \vee b = 1$ $a \wedge b = 0$

Twicken: jestliže $(L, \sqsubseteq, \vee, \wedge, 0, 1)$ je distributivní svaz
a jestliže prvek a má doplněk, pak doplněk je
jedinný.

Když $a \wedge b = 0$, $a \wedge c = 0$, $a \vee b = 1$, $a \vee c = 1$
 b doplněk c doplněk

$b = b \wedge (a \vee b) = b \wedge (a \vee c) = (b \wedge a) \vee (b \wedge c) =$
nejak
napravo b

$$= (a \wedge c) \vee (b \wedge c) = (a \vee b) \wedge c = (a \vee c) \wedge c = \underline{\underline{c}}$$

Doplňek a značíme $\bar{a}$, $\bar{0} = 1$, $\bar{1} = 0$

Svaz $(L, \leq, \vee, \wedge, 0, 1)$ se nazývá komplementární, jestliže každý prvek má doplněk.

Booleova algebra je komplementární distributivní svaz

$$L = \{0, 1\}$$

$\vee$	0	1
0	0	1
1	1	1

$\wedge$	0	1
0	0	0
1	0	1

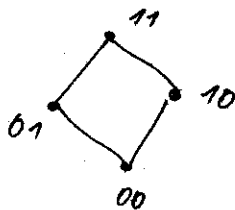
$$\bar{0} = 1$$

$$\bar{1} = 0$$



$$\{0, 1\}^2 = \{00, 01, 10, 11\} = \{0, 1\} \times \{0, 1\}$$

$$ij \leq kl \text{ iff } i \leq k \text{ and } j \leq l$$



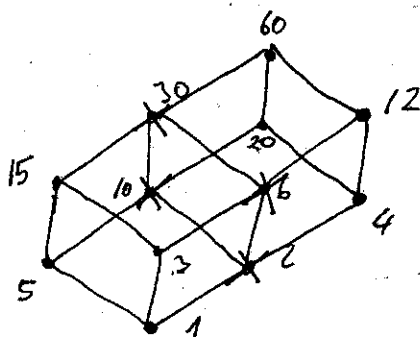
$$ij \vee kl = i \vee k \text{ and } j \vee l$$

$$ij \wedge kl = i \wedge k \text{ and } j \wedge l$$

$$\{0, 1\}^n = \{0, 1\} \times \{0, 1\} \times \dots \times \{0, 1\}$$

$$i_1, i_2, \dots, i_n \leq j_1, j_2, \dots, j_n \text{ iff } i_1 \leq j_1, i_2 \leq j_2, \dots$$

Pr $L = \{1, 2, 3, 4, 5, 6, 10, 12, 15, 20, 30, 60\}$ *delitelé 60*



$$\overline{15} = 4$$

$$\overline{4} = 15$$

$$\overline{3} = 20$$

$$\overline{20} = 3$$

$$\overline{5} = 12$$

$$\overline{12} = 5$$

nemají 2, 6, 10, 30

(12)

zkouška předběrně

5, 12, 21, 26, 11.9.

- grupy a poč. v. $\mathbb{Z}_m$, Euler φ , Čin. věta, RSA, najít prvky řádu ... , řeš. $x^a = 1$
- koneč. tělesa, najít těleso q -prvků,
- lineární a cykl. kódy - gener a kontrol matice ...
- vzory, booleany alg, ...

přesná arpoň polovina správně, 1 nebo bez ústního
příkladů které mohou mít různé bodové hodnocení

BA je komplementární distribuční vzor $(L, \subseteq, \cup, \cap, 0, 1, -)$

Doplň

$$\bar{a}: a \cap \bar{a} = 0$$

$$a \cup \bar{a} = 1$$

Pr $(P(U), \subseteq, \cup, \cap, \emptyset, U, -)$ je BA

$$\bar{x} = U \setminus x$$

Atom ve vzoru L je prvek $a \in L$ takový, že pokrývá 0.

tj. $0 \subseteq a$, $0 \neq a$ a jestliže $0 \subseteq b \subseteq a$, tak $0 = b$ nebo $b = a$

Věta: je-li $(L, \subseteq, \cup, \cap, 0, 1, -)$ BA, která nemá spočetně
tělekce, pak každý prvek $x = \bigvee \{a \mid a \text{ je atom, } a \subseteq x\}$

$$x \mapsto \{a \mid a \text{ je atom, } a \subseteq x\}$$

$$0 \mapsto \emptyset$$

$$1 \mapsto A \text{ množ. atomů}$$

$$\underline{U = A}$$

Kartézský součin BA

$$(L_1, \varepsilon_1, \wedge_1, \vee_1, 0_1, \underline{1}_1, ^{-1}) \quad (L_2, \varepsilon_2, \wedge_2, \vee_2, 0_2, \underline{1}_2, ^{-2})$$

$$\text{Kartézský součin } (L_1 \times L_2, \varepsilon, \wedge, \vee, 0, \underline{1}, ^{-})$$

$$(x_1, y_1) \vee (x_2, y_2) = (x_1 \vee_1 x_2, y_1 \vee_2 y_2)$$

$$(x_1, y_1) \wedge (x_2, y_2) = (x_1 \wedge_1 x_2, y_1 \wedge_2 y_2)$$

$$0 = (0_1, 0_2)$$

$$(\overline{x}, \overline{y}) = (\overline{x^1}, \overline{y^2})$$

$$\underline{1} = (\underline{1}_1, \underline{1}_2)$$

dá se oběcky
napočítat

$$\overline{BA} \quad L = \{0, 1\}$$



$\vee$	0	1
0	0	1
1	1	1

$\wedge$	0	1
0	0	0
1	0	1

$$\overline{0} = 1$$

$$\overline{1} = 0$$

$$L \times L = L^2 \quad \dots \quad L^3 \quad \dots \quad L^4$$

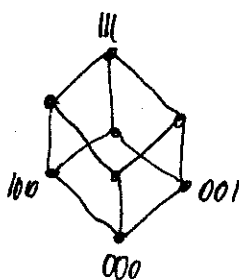
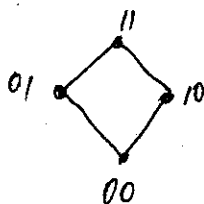
$$\{x_1 \dots x_n \mid x_i \in \{0, 1\}\}$$

$$x_1 \dots x_n \vee y_1 \dots y_n = (x_1 \vee y_1) \dots (x_n \vee y_n)$$

$$x_1 \dots x_n \wedge y_1 \dots y_n = (x_1 \wedge y_1) \dots (x_n \wedge y_n)$$

$$\overline{x_1 \dots x_n} = \overline{x_1} \overline{x_2} \dots \overline{x_n}$$

n-rozměrná krychle



↑ kardinál BA platí:

$$1) \quad \overline{\overline{a}} = a \quad a \wedge (\overline{a}) = 0 \quad a \vee (\overline{a}) = 1$$

$$2) \quad \overline{a \vee b} = \overline{a} \wedge \overline{b} \quad \overline{a \wedge b} = \overline{a} \vee \overline{b}$$

$$\begin{aligned} c \vee \overline{c} = 1: & \text{ dle } (a \vee b) \vee (\overline{a} \wedge \overline{b}) = x \vee (\overline{a} \wedge \overline{b}) = (x \vee \overline{a}) \wedge (x \vee \overline{b}) = \\ & = (\overline{a \vee b \vee \overline{a}}) \wedge (\overline{a \vee b \vee \overline{b}}) = 1 \end{aligned}$$

$$\begin{aligned} c \wedge \overline{c} = 0: & (a \vee b) \wedge (\overline{a} \wedge \overline{b}) = (a \vee b) \wedge y = (a \wedge y) \vee (b \wedge y) = \\ & \uparrow \\ & = (\underbrace{a \wedge \overline{a} \wedge \overline{b}}_0) \vee (\underbrace{b \wedge \overline{a} \wedge \overline{b}}_0) = 0 \end{aligned}$$

$$\begin{aligned} 3) \quad & \text{if } a \subseteq b, \text{ then } \overline{b} \subseteq \overline{a} \rightarrow a \wedge b = a \quad \overline{a \wedge b} = \overline{a} \\ & (a \subseteq b \text{ iff } \overline{b} \subseteq \overline{a}) \quad \overline{a \vee b} = \overline{a} \\ & \quad \quad \quad \boxed{\overline{b} \subseteq \overline{a}} \end{aligned}$$

$$a \subseteq b \text{ iff } a \wedge b = a \text{ iff } a \vee b = b$$

$$4) \quad \text{if } \overline{a} = \overline{b} \text{ then } a = b$$

Každý konečný svaz má největší a nejmenší prvek.

$$L_a = \{x_1, \dots, x_m\}$$

$$(\dots(((x_1 \vee x_2) \vee x_3) \vee x_4) \dots x_m = \text{největší prvek}$$

$$(\dots(((x_1 \wedge x_2) \wedge x_3) \wedge x_4) \dots x_m = \text{nejmenší prvek}$$

Aplikace svazů

Kontext $K = (G, M, I)$

G .. konečná množ. objektů
 M .. atributů

$$I \subseteq G \times M$$

	m_1	m_2	...	m_k
g_1	.	.		
g_2	.	x		
$\vdots$				
g_m				

$$g I m$$

$$A \subseteq G$$

$$A^+ = \{m \mid g I m \text{ pro každé } g \in A\} \subseteq M$$

množ atrib, které mají vš. objekty

	m_1	...	m_k
g_1	x		x
$\vdots$	x		x
g	x		x
$\vdots$	x		x
g	x		x

↑ ↑

$$B \subseteq M$$

$$B^+ = \{g \mid g I m \text{ pro každé } m \in B\} \subseteq G$$

extend
intend

Koncept v K je (A, B) taková, že $A^\uparrow = B$, $B^\downarrow = A$

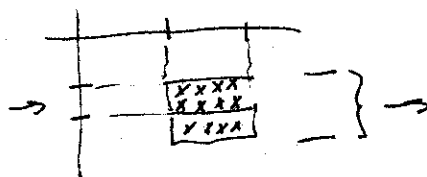
Platí: $K = (G, M, I)$, $A_1, A_2, A_3 \subseteq G$, $B_1, B_2, B_3 \subseteq M$. Pak

1) if $A_1 \subseteq A_2$, then $A_2^\uparrow \subseteq A_1^\uparrow$

více objektů může mít méně společných atributů
 $m \in A_2^\uparrow$ pro každé $g \in A_2$, $g I m$
 když $g \in A_1 = A_2$ ↗

if $B_1 \subseteq B_2$, then $B_2^\downarrow \subseteq B_1^\downarrow$

2) $A \subseteq A^{\uparrow\downarrow}$



3) $A^\uparrow \subseteq A^{\uparrow\downarrow\uparrow}$
 $B^\downarrow \subseteq B^{\downarrow\uparrow\downarrow}$

$(A^{\uparrow\downarrow}, A^\uparrow)$... je koncept

Svat konceptů

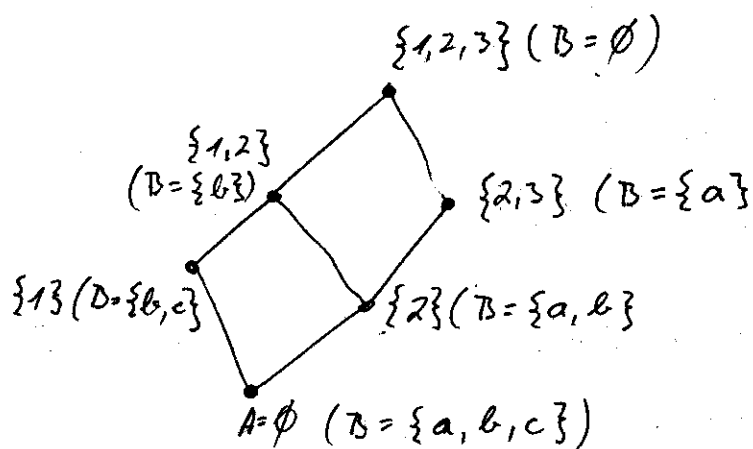
$\{(A, B) \mid (A, B) \text{ je koncept}\}$

$(A, B) \subseteq (C, D)$ iff $A \subseteq C$ iff $B \supseteq D$

Pr $G = \{1, 2, 3\}$, $M = \{a, b, c\}$

I	a	b	c
1		x	x
2	x	x	
3	x		

$A = \emptyset$	$A^\uparrow = \{a, b, c\}$	$A^{\uparrow\downarrow} = \emptyset$
$A = \{1\}$	$A^\uparrow = \{b, c\}$	$A^{\uparrow\downarrow} = \{1\}$
$A = \{2\}$	$A^\uparrow = \{a, b\}$	$A^{\uparrow\downarrow} = \{2\}$
$A = \{3\}$	$A^\uparrow = \{a\}$	$A^{\uparrow\downarrow} = \{2, 3\}$



Twreži: Je-li T indexová množina a pro každé $t \in T$ máme daný koncept (A_t, B_t) , pak

$$\left(\bigcup_{t \in T} A_t \right)^{\uparrow} = \bigcap_{t \in T} A_t^{\uparrow} \quad \left(\bigcup_{t \in T} B_t \right)^{\downarrow} = \bigcap_{t \in T} B_t^{\downarrow}$$

$$\begin{aligned} m \in \left(\bigcup_{t \in T} A_t \right)^{\uparrow} &\Leftrightarrow \text{pro každé } g \in \bigcup_{t \in T} A_t, g I m \\ &\Leftrightarrow \text{pro každé } t \text{ a } g \in A_t, g I m \\ &\Leftrightarrow \text{pro každé } t \text{ je } m \in (A_t)^{\uparrow} \\ &\Leftrightarrow \bigcap_{t \in T} (A_t)^{\uparrow} \end{aligned}$$

?
rychle
zmačala

Množina všech konceptů v K tvoří úplný svaz, kde

$$\bigvee_{t \in T} (A_t, B_t) = \left(\left(\bigcup_{t \in T} A_t \right)^{\uparrow}, \bigcap_{t \in T} B_t \right)$$

$$\bigwedge_{t \in T} (A_t, B_t) = \left(\bigcap_{t \in T} A_t, \left(\bigcup_{t \in T} B_t \right)^{\downarrow} \right)$$

Homomorfismy

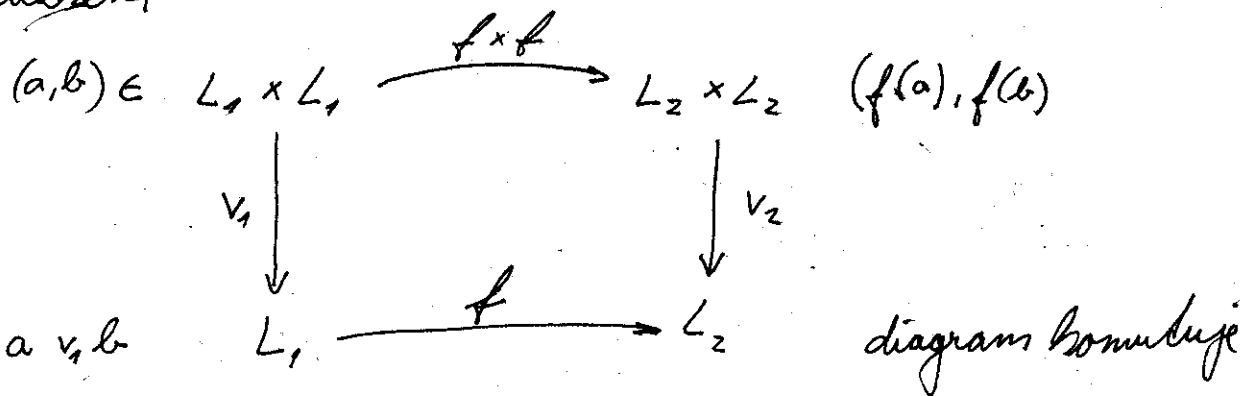
$$(L_1, v_1, \wedge_1, \vee_1) \quad (L_2, v_2, \wedge_2, \vee_2)$$

homomorfismus je zobrazení $f: L_1 \rightarrow L_2$ takové, že
pro každé $a, b \in L_1$

$$f(a \vee_1 b) = f(a) \vee_2 f(b)$$

$$f(a \wedge_1 b) = f(a) \wedge_2 f(b)$$

obrážkem



je-li $f: (L_1, v_1, \wedge_1) \rightarrow (L_2, v_2, \wedge_2)$ homomorfismus,
pak $f(L_1) = \{f(s) \mid s \in L_1\} \subseteq L_2$ je podvar $(L_2, v_2, \wedge_2)$

$$f(s), f(t) \in f(L_1) \rightarrow \text{Im}(f) \text{ (obraz } f)$$

$$f(s) \vee_2 f(t) = f(\underbrace{s \vee_1 t}_{\in L_1}) \in f(L_1)$$

$$f(s) \wedge_2 f(t) = f(s \wedge_1 t) \in f(L_1)$$

... je to podalgebra

Jestliže 1 je nejvyšší prvek $(L_1, v_1, \wedge_1)$, pak

$f(1)$ je nejvyšší prvek podvaru $(f(L_1), v_2, \wedge_2)$

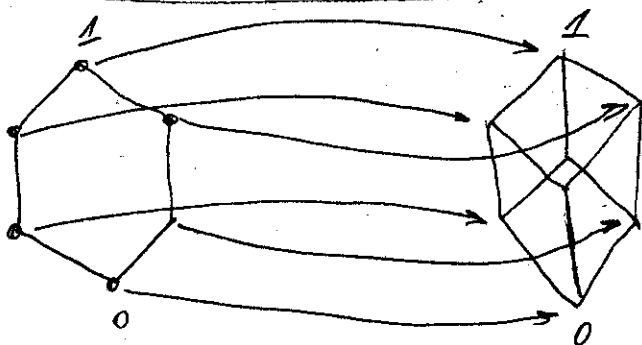
$$s \vee_1 1 = 1 \quad f(s) \vee_2 f(1) = f(s \vee_1 1) = f(1)$$

$$\text{if } s \leq_1 t \text{ then } f(s) \leq_2 f(t)$$

$$s \leq_1 t \quad \text{iff} \quad s \vee_1 t = t$$

$$f(s) \vee_2 f(t) = f(s \vee_1 t) = f(t)$$

$$\text{tj. } f(s) \leq_2 f(t)$$



pravdašně zobrazení.
zachováno $\leq$, ale
není homomorfismus

Jestliže $(L_1, \vee_1, \wedge_1)$ je distributivní svaz a f je homomorfismus,
pak $(f(L_1), \vee_2, \wedge_2)$ je distributivní svaz.

$$\begin{aligned} f(a) \vee_2 (f(b) \wedge_2 f(c)) &= f(a) \vee_2 f(b \wedge_1 c) = \\ &= f(a \vee_1 (b \wedge_1 c)) = f((a \vee_1 b) \wedge_1 (a \vee_1 c)) = \\ &= f(a \vee_1 b) \wedge_2 f(a \vee_1 c) = (f(a) \vee_2 f(b)) \wedge_2 (f(a) \vee_2 f(c)) \end{aligned}$$

Pologrupy $(S, *)$, (T, Δ)

homomorfismus $f: (S, *) \rightarrow (T, \Delta)$ je katrové zobrazení

$f: S \rightarrow T$, že pro každé $x, y \in S$ platí $f(x * y) = f(x) \Delta f(y)$

Platí $(f(S), \Delta)$ je podpologrupa.

Monoid a grupa obdoložně.

Když S je monoid s jednoškovým prvkem e , pak

$(f(S), \Delta)$ je monoid s jednoškovým prvkem $f(e)$.

Je-li x^{-1} inverzní k x v $(S, *)$, pak $f(x^{-1})$ je inverzní k $f(x)$ v $(f(S), \Delta)$

Pr. $(\mathbb{Z}, +, 0)$, $(\mathbb{Z}_m, \oplus, [0]_m)$

$$f: \mathbb{Z} \rightarrow \mathbb{Z}_m \quad f(i) \rightarrow [i]_m \text{ je homomorfismus} \\ \text{na } (\mathbb{Z}_m, \oplus, [0]_m)$$

$$[i]_m \oplus [j]_m = [i+j]_m \iff \begin{cases} k \equiv i \pmod{m} \\ k \equiv j \pmod{m} \end{cases} \begin{matrix} [k]_m = [i]_m \\ [k]_m = [j]_m \end{matrix} \\ f(i) \oplus f(j) = f(i+j)$$

Je-li $f: S \rightarrow T$ zobrazení, pak relace $\sim$ na S definovaná
 $x \sim y \iff f(x) = f(y)$ je ekvivalence na S .

Je-li $f: (S, *) \rightarrow (T, \Delta)$ homomorfismus, pak $\sim$ na S má navíc
 sůlu vlastnost: if $\begin{matrix} x \sim y \\ a \sim b \end{matrix}$ then $x * a \sim y * b$

$$f(x) = f(y) \quad f(a) = f(b)$$

$$f(x * a) = f(x) \Delta f(a) = f(y) \Delta f(b) = f(y * b)$$

Máme danou pologrupu $(S, *)$, ekvivalence $\sim$ na S se nazývá
 kongruence, if platí

$$x \sim y, a \sim b \Rightarrow (x * a) \sim (y * b)$$

Když $\sim$ je kongruence na $(S, *)$, tak můžeme definovat
 kv. faktorovou pologrupu

$$(S, *) / \sim = (S / \sim, \otimes), \text{ kde } S / \sim = \{[s]_n \mid s \in S\}$$

$$[s]_n \otimes [t]_n = [s * t]_n$$

Př Σ^* je množina ^{všech} slov nad abecedou Σ

• zřetězení, pak $(\Sigma^*, \cdot)$ je monoid

$$\Sigma = \{0, 1\} \quad (\{0, 1\}^*, \cdot) \quad u \cdot (v \cdot w) = uvw = (u \cdot v) \cdot w$$

$$f: \begin{array}{l} 0 \mapsto 3 \\ 1 \mapsto 7 \end{array} \quad (\mathbb{Z}, +, 0) \quad f^*: (\{0, 1\}^*, \cdot) \rightarrow (\mathbb{Z}, +)$$

$$01 \mapsto 3+7$$

$$0110001 \mapsto 4 \cdot 3 + 3 \cdot 7$$

$$00 \mapsto 2 \cdot 3$$

$$w \mapsto p_0 \cdot 3 + p_1 \cdot 7$$

p_0 je počet 0 v w

p_1 — " — 1 — " —

Př $(\{0, 1\}^+, \cdot)$ $(S, *)$... pologrupa

$$f: 0 \rightarrow a \in S$$

$$u = x_1 x_2 \dots x_n \quad x_i \in \{0, 1\}$$

$$1 \mapsto b \in S$$

$$f(0) = a$$

$$f^*(u) = f(x_1) * f(x_2) * \dots * f(x_n)$$

$$f(1) = b$$

f^* je homomorfismus

Př $(\mathbb{Z}_6, +, 0)$ $(\mathbb{Z}_4, +, 0)$

Kolik je homomorfismů $f: (\mathbb{Z}_6, +, 0) \rightarrow (\mathbb{Z}_4, +, 0)$

$$\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$$

$$\mathbb{Z}_4 = \{0, 1, 2, 3\}$$

řešení

generátor 4^6 rozbor

$$(\{0\}_1, +), (\{0, 2\}_2, +)$$

$$1 \quad 2 = 1+1 \quad 3 = 1+1+1 \quad 4 = 1+1+1+1 \quad 5 = 1+1+1+1+1$$

$$\downarrow \quad 0 = 1+1+1+1+1+1$$

a

$a+a$

$a+a+a$

→ redukuje se na 4 možnosti,
kam obraz 1

$$f: \{0, 1, 2, 3, 4, 5\} \rightarrow \{0\} \quad f(i) = 0$$

$$g: g(0) = 0, g(1) = g(3) = g(5) = 2, g(2) = g(4) = 0$$

(14)

$(\mathbb{Z}_p, \cdot)$ Najděte všechna $x \in \mathbb{Z}_p$ taková, že $x^k = 1, k \geq 1$

Nabíráme $x \in \mathbb{Z}_p^*$, protože $x^{k-1} \cdot x = 1$, tj. x^{k-1} je inverzní ke x

$x^k = 1$ znamená řád x dělí k .

$|\mathbb{Z}_p^*| = \varphi(p)$... umíme najít generátor $\mathbb{Z}_p^*$

a je generátor $\mathbb{Z}_p^*$, řád a je $\varphi(p)$

řád a^i je $\frac{\varphi(p)}{\gcd(\varphi(p), i)}$

Pří $(\mathbb{Z}_{13}, \cdot)$ Najděte všechna $x \in \mathbb{Z}$ taková, že $x^3 = 1$

$$|\mathbb{Z}_{13}^*| = 12$$

$$\text{zkusíme } 2, 2^2 = 4, 2^3 = 8, 2^4 = 3, 2^5 = 6, 2^6 = -1$$

$$2^7 = 11, 2^8 = 9, 2^9 = 5, 2^{10} = 10, 2^{11} = 7, 2^{12} = 1$$

je to generátor

$$\text{potřebujeme } \frac{12}{\gcd(12, i)} = 3$$

proto $2^4 = 3$ má řád 3 tj. je řešení $x^3 = 1$

$$2^8 = 9 \quad 9^3 = 27 = 1$$

řešení $1, 2^4, 2^8$ (1, 3, 9)

$\mathbb{P}_{105}$

$\text{v } \mathbb{Z}_{105}$

$$x^3 = 1$$

$$\varphi(105) = \varphi(3 \cdot 5 \cdot 7) = \varphi(3) \cdot \varphi(5) \cdot \varphi(7) = 2 \cdot 4 \cdot 6 = 48$$

mám čím v-0 xlv.

$$\mathbb{Z}_{105} \cong \mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_7$$

$$(i, j, k)$$

$$i^3 = 1 \text{ v } \mathbb{Z}_3, \quad j^3 = 1 \text{ v } \mathbb{Z}_5, \quad k^3 = 1 \text{ v } \mathbb{Z}_7$$

hľadám a keďže je cyklická

$$\mathbb{Z}_{105}^* = \mathbb{Z}_3^* \times \mathbb{Z}_5^* \times \mathbb{Z}_7^*$$

$$\{1, 2\} \quad \{1, \cancel{2}, \cancel{3}, \cancel{4}\} \quad \{1, 2, \cancel{3}, 4, \cancel{5}, \cancel{6}\}$$

$$2^3 = 2 \neq 2$$

je 1

hady ~~po~~ pohľadom, jinak Eukleid

$1 \leftarrow$	$(1, 1, 1)$	$3, 35$	$1 = 3 \cdot 12 - 35$	$q_1 = -35$
$-35 + 21 + 2 \cdot 15 = 16$	$(1, 1, 2)$	$5, 21$	$1 = 21 - 4 \cdot 5$	$q_2 = 21$
$-35 + 21 + 4 \cdot 15 = 46$	$(1, 1, 4)$	$7, 15$	$1 = 15 - 2 \cdot 7$	$q_3 = 15$

$$\textcircled{1} (S, *) \xrightarrow{f} (T, \Delta) \xrightarrow{g} (M, \bullet) \quad f, g \text{ homomorfizmy}$$

pak $g \circ f$ je homomorfizmus $(S, *) \rightarrow (M, \bullet)$

$$\text{Dk } g \circ f(a * b) = g(f(a * b)) = g(\underbrace{f(a)}_{\in T} \Delta \underbrace{f(b)}_{\in T}) =$$

$$= g(f(a)) \bullet g(f(b)) = g \circ f(a) \bullet g \circ f(b)$$

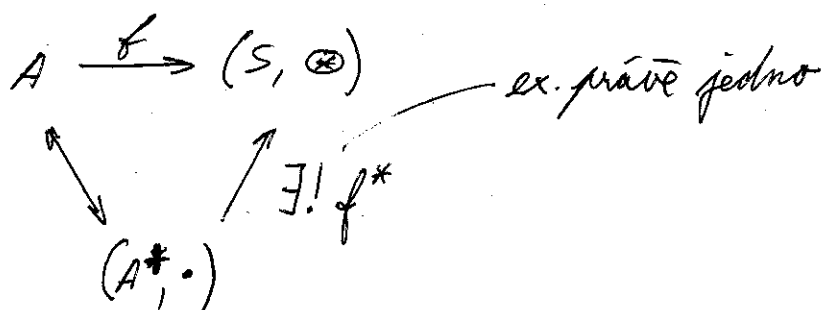
Volná pologrupa (s množinou generátorů A) nad A
je latová pologrupa $(A^+, \cdot)$

kdykoliv $f: A \rightarrow (S, \otimes)$

$(S, \otimes)$ je pologrupa

pak existuje právě jeden homomorfismus

$f^*: (A^+, \cdot) \rightarrow (S, \otimes)$, že $f^*(a) = f(a)$, $a \in A$



$$A = \{a, b\}$$

$$a \mapsto s$$

$$b \mapsto t$$

$$a \cdot b \mapsto s \otimes t$$

$$a \cdot b \cdot a \mapsto s \otimes t \otimes s$$

A^+ je množina všech reprezentujících slov nad A

$\cdot$ je zřetězení

$(A^+, \cdot)$ je volný monoid nad A

Přklady k písemky

② a) $GF(5^2)$?

veveme $\mathbb{Z}_5[x]/m(x)$

$m(x)$ je stupně 2
a je ireducibil (aby
ke každému pol. byl inverzní)

$x^2, x^2+1, \boxed{x^2+2}$
proč 2

$$\begin{aligned} 0^2+2 &= 2 \\ 1^2+2 &= 3 \\ 2^2+2 &= 4 \\ 3^2+2 &= 1 \\ 4^2+2 &= 3 \end{aligned}$$

$$GF(5^2) \cong \mathbb{Z}_5[x]/x^2+2$$

seil
már

$$\begin{aligned} (ax+b) + (cx+d) &= (a+c)x + (b+d) \\ (ax+b) \cdot (cx+d) &= (ad+bc)x + (bd+3ac) \end{aligned}$$

b) $(2x+3)^{-1}$?

$$f(x) \cdot (2x+3) \equiv 1 \pmod{(x^2+2)}$$

$$(x^2+2) : (2x+3) = 3x+3$$

$$\begin{array}{r} -(x^2+4x) \\ \hline x+2 \\ -(x+4) \\ \hline -2 \end{array}$$

$$f(x) \cdot (2x+3) + h(x)(x^2+2) = 1$$

$$x^2+2 = (3x+3) \cdot (2x+3) - 2$$

$$2 = (3x+3) \cdot (2x+3) - (x^2+2) \quad | : 3$$

$$1 = \boxed{3(3x+3)} \cdot (2x+3) - 3(x^2+2)$$

$\downarrow f(x)$

$$(2x+3)^{-1} = 4x+4$$

c)

$(GF(5^2) \setminus \{0\}, \cdot, 1)$ je grupa

má 24 prvků

st. nejvýše 1

1, 2, 3, 4 nemá smysl

$$x, x^2 = -2 = 3, x^4 = -1, x^8 = 1 \quad \text{není}$$

$$\varphi(24) = \varphi(8) \cdot \varphi(3) = (2^3 - 2^2) \cdot 2 = 8$$

bude 8 generátorů

zkusíme

$$x+1 \quad (x+1)^2 = x^2 + 2x + 1 = 3 + 2x + 1 = 2x + 4 = 2 \cdot (x+2)$$

$$(x+1)^4 = 4(x^2 + 4x + 4) = 4(3 + 4x + 4) = \cancel{4} x + 3$$

$$(x+1)^8 = x^2 + x + 4 = 3 + x + 4 = x + 2$$

$$\underline{(x+1)^{12}} = (x+2)(x+3) = x^2 + 1 = 3 + 1 = 4 = -1$$

$x+1$ je generátor

potvrzeno $\frac{24}{\gcd(24, i)} = 24 \quad i=5$ a další nesoustředě

$$\underline{(x+1)^5} = (x+1)^4 \cdot (x+1) = (x+3)(x+1) = x^2 + 4x + 3 = \underline{\underline{4x+1}}$$

draký generátor

není alg., jak najít primitivní prvek