

Relace uspořádané $\leq$:

Definice: Uspořádané

Relace $\leq$ na množině X je uspořádaná na X , jestliže je:

- ① Reflexivní: $\forall x \in X: x \leq x$
- ② Antisymetrická: $\forall x, y \in X: x \leq y \wedge x \geq y \Rightarrow x = y$
- ③ Transitivní: $\forall x, y, z \in X: x \leq y \wedge y \leq z \Rightarrow x \leq z$

Říkáme, že prvky $x, y \in X$ jsou porovnatelné, pokud $x \leq y \vee x \geq y$.

Definice: Úplné uspořádané

Říkáme, že uspořádané $\leq$ na X je úplné, jestliže všechny prvky jsou navzájem porovnatelné.

Poznámka:

- Antisymetrie v axiomech uspořádané se nazývá někdy tzv.: slabou antisymetrií
- silná antisymetrie: $a \leq b \Rightarrow \neg(b < a)$
příklad: ostrá nerovnost
- Pro úplné uspořádané platí trichotomie:
 $\forall x, y \in X: x \leq y \vee x \geq y \vee x < y$

Platí:

Je-li $Y \subset X$, X je uspořádaná relací $\leq$, pak $\leq|_Y$ je uspořádaná na Y .
Když $\leq$ je úplné na X , pak $\leq|_Y$ je úplné na Y .

Definice: Nejmenší a minimální prvek

Buď X uspořádaná $\leq$, $x \in X$.

Řekneme, že x je minimální $\Leftrightarrow \forall y \in X: x \leq y \Rightarrow x = y$
prvek (nejmenší) $\Leftrightarrow \forall y \in X: x \leq y$

Plat':

1. Nejmenší' prvek je určen' jednoznačně.
2. Nejmenší' prvek je minimální'.

Důkaz:

1. x_1, x_2 ~~nejmenší'~~ nejmenší' prvky: $x_1 \leq x_2 \wedge x_2 \leq x_1 \Rightarrow x_1 = x_2$
2. x nejmenší' $\rightarrow \forall y \in X: x \leq y$
 $\rightarrow$ Kdykoli $y \leq x \rightarrow x = y$

Poznámka:

Jestliže je uspořádané' úplné', pak pojmy minimálního' a nejmenší'ho prvku splývají'.

Definice: Izomorfismus

Bud' X, Y množiny uspořádané' relacemi $\leq_x, \leq_y$.
Řekneme, že zobrazení $f: X \rightarrow Y$ je izomorfismus (podobnost),
když f je bijekce a plat': $\forall a, b \in X: a \leq_x b \Rightarrow f(a) \leq_y f(b)$

Definice: Dobře uspořádané'

Uspořádané' na X je dobré', pokud každá neprázdná'
podmnožina obsahuje nejmenší' prvek.

Plat'

Každé' dobře' uspořádané' je úplné'

Důkaz:

Bud' $x, y \in X$ libovolné': $A := \{x, y\} \subset X \rightarrow$ existuje nejmenší' prvek
BÚNO: $x \leq y$

Definice: Úseč množiny

Bud' $(X, \leq)$ úplné' uspořádaná' množina, $a \in X$.

Množina $M_a := \{y \in X \mid y < a\}$ je úseč množiny X určená' prvkem

Věta: Princip transfinite indukce:

Nechť X je dobře uspořádaná množina, $A \subset X$ taková že:

$$\forall x \in X : M_x \subset A \Rightarrow x \in A.$$

Potom $A = X$.

Důkaz:

Nechť $A \neq X$, tj. $X \setminus A \neq \emptyset$

→ $X \setminus A$ obsahuje nejmenší prvek $a \in X$

→ $M_a \cap (X \setminus A) = \emptyset \rightarrow M_a \subset A \rightarrow a \in A \wedge a \in X \setminus A$, spor.

Definice: Peanovy axiomy

Nechť $\mathbb{N}_0$ je množina, $\sigma: \mathbb{N}_0 \rightarrow \mathbb{N}_0$ zobrazení, $0 \in \mathbb{N}_0$.

Množina nerozporných celých čísel je uspořádaná trajice:

$(\mathbb{N}_0, \sigma, 0)$, kde:

① σ je zobrazení

② $0 \notin \sigma(\mathbb{N}_0)$

③ $\forall M \subset \mathbb{N}_0 : 0 \in M \wedge \sigma(M) \subset M \Rightarrow M = \mathbb{N}_0$ (princip matematické indukce)

Platí:

1. $\sigma(\mathbb{N}_0) = \mathbb{N}_0 \setminus \{0\}$

2. $\forall m \in \mathbb{N}_0 : \sigma(m) \neq m$

Důkaz:

1. $M := \{0\} \cup \sigma(\mathbb{N}_0) : 0 \in M$

$\sigma(M) \subset M : \sigma(\{0\} \cup \sigma(\mathbb{N}_0)) \subset \{0\} \cup \sigma(\mathbb{N}_0)$

→ $M = \mathbb{N}_0 \rightarrow \sigma(\mathbb{N}_0) = \mathbb{N}_0 \setminus \{0\}$

2. $M := \{m \in \mathbb{N}_0 \mid \sigma(m) \neq m\} : 0 \in M$

$\sigma(M) \subset M$

→ $M = \mathbb{N}_0$

Definice: Přirozená čísla:

$(\mathbb{N}_0, \sigma, 0)$ je množina přirozených čísel, $\sigma: \mathbb{N}_0 \rightarrow \mathbb{N}_0$, $0 \in \mathbb{N}_0$, pokud:

- ① σ je prosté
- ② $0 \notin \sigma(\mathbb{N}_0)$
- ③ $\forall M \subset \mathbb{N}_0 : 0 \in M, \sigma(M) \subset M \Rightarrow M = \mathbb{N}_0$

Věta: Princip definice rekursí:

Nechť S je množina, $a \in S$, $g: S \rightarrow S$.

Pak existuje právě jedna $h_0: \mathbb{N}_0 \rightarrow S$ taková, že:

- ① $h_0(0) = a$
- ② $\forall m \in \mathbb{N}_0 : h_0(\sigma(m)) = g(h_0(m))$

Důkaz:

• Jednoznačnost:

Nechť existují h_1, h_2 různé:

$$A := \{m \in \mathbb{N}_0 \mid h_1(m) = h_2(m)\}$$

$$1. h_1(0) = a = h_2(0), 0 \in A \checkmark$$

$$2. \sigma(m) \in A : h_1(\sigma(m)) = g(h_1(m)) = g(h_2(m)) = h_2(\sigma(m)) \checkmark$$

$$\rightarrow A = \mathbb{N}_0 \rightarrow h_1 = h_2$$

Příklad:

• $S = X^X$, $a \in S : a := 1_X$, $g: X^X \rightarrow X^X : g(\varphi) = f \circ \varphi$,
kde $f: X \rightarrow X \in X^X$:

1. $h(0) = f^0 = 1_X$

2. $h(\sigma(m)) = f^{\sigma(m)} = f \circ f^m$

Speciálně: $f := \sigma: \mathbb{N}_0 \rightarrow \mathbb{N}_0$

Platí: $\forall m \in \mathbb{N}_0 : \sigma^m(0) = m$

Důkaz:

indukcí: $A := \{m \in \mathbb{N} \mid \sigma^m(0) = m\}$

1. $0 \in A : \sigma^0(0) = 1_{\mathbb{N}_0}(0) = 0 \checkmark$

2. $\sigma(m) \in A : \sigma^{\sigma(m)} = (\sigma \circ \sigma^m)(0) = \sigma(\sigma^m(0)) = \sigma(m) \checkmark$

$\rightarrow A = \mathbb{N}_0$

Platí:

$\forall m, n \in \mathbb{N}_0, f, g: X \rightarrow X$ složeno, $\checkmark : f \circ g = g \circ f$ platí:

① $f^m \circ g^n = g^n \circ f^m$

② $(f \circ g)^m = f^m \circ g^m$

③ $(f^m)^n = (f^m)^n$

Důkaz:

Jasně: pomocí indukce

Definice: Sčítání a násobení na $\mathbb{N}_0$

Na $\mathbb{N}_0$ definujeme binární operace $+, \cdot : \mathbb{N}_0 \times \mathbb{N}_0 \rightarrow \mathbb{N}_0$ takto:

$\forall m, n \in \mathbb{N}_0 : m + n := \sigma^n(m)$

$m \cdot n := (\sigma^m)^n(0)$

Značíme: $\sigma(0) := 1$

Thesen: Vlastnosti sčítání a násobení

Pro všechna $m, n \in \mathbb{N}_0$ platí:

- ① $n + 0 = n$
- ② $n + \sigma(m) = \sigma(n+m)$
- ③ $n \cdot 0 = 0$
- ④ $n \cdot \sigma(m) = n + n \cdot m$
- ⑤ $\forall f: X \rightarrow X : f^1 = f$
- ⑥ $n + 1 = \sigma(n)$
- ⑦ $n \cdot 1 = n$

Důkaz:

- ① $n + 0 = \sigma^0(n) = 1_{\mathbb{N}_0}(n) = n$
- ② $n + \sigma(m) = \sigma^{\sigma(m)}(n) = \sigma \circ \sigma^m(n) = \sigma(n+m)$
- ③ $n \cdot 0 = (\sigma^n)^0(0) = 1_{\mathbb{N}_0}(0) = 0$
- ④ $n \cdot \sigma(m) = (\sigma^n)^{\sigma(m)}(0) = (\sigma^n \circ (\sigma^m)^m)(0) = \sigma^m(n \cdot m) = n + n \cdot m$
- ⑤ $f^1 = f^{\sigma(0)} = f^0 \circ f^0 = f^0 \circ 1_X = f$
- ⑥ $n + 1 = \sigma^1(n) = \sigma^{\sigma(0)}(n) = \sigma \circ \sigma^0(n) = \sigma \circ 1_{\mathbb{N}_0}(n) = \sigma(n)$
- ⑦ $n \cdot 1 = \sigma^n(0) = n$

Platí:

$$\forall m, n \in \mathbb{N}_0 ; f: X \rightarrow X : f^{m+n} = f^m \circ f^n = f^n \circ f^m$$

Důkaz:

Bud' $m \in \mathbb{N}_0$ libovolně pevně

$$A = \{n \in \mathbb{N}_0 \mid f^{m+n} = f^m \circ f^n = f^n \circ f^m\}$$

$$\bullet 0 \in A : f^{m+0} = f^m = f^m \circ 1_X = 1_X \circ f^m$$

$$\bullet \sigma(m) \in A : f^{m+\sigma(m)} = f^{\sigma(m+m)} = f^0 \circ f^{m+m} = f^0 \circ f^m \circ f^m = f^m \circ f^{\sigma(m)} \circ f^m = f^m \circ f^{\sigma(m)} \circ f^m$$

Věta: Vlastnosti operace +:

Binární operace + na $\mathbb{N}_0$ je asociativní a komutativní s neutrálním prvkem 0 a navíc platí:

- křáček (vzhledem ke sčítání):

$$\forall m, n, k \in \mathbb{N}_0 : m + k = n + k \Rightarrow m = n$$

- pravidlo nuly:

$$\forall m, n \in \mathbb{N}_0 : m + n = 0 \Leftrightarrow m = 0 \wedge n = 0$$

Důkaz:

- Asociativita: $(m+n)+k = \sigma^k(m+n) = \sigma^{(m+n)+k}(0) = (\sigma^m \circ \sigma^n \circ \sigma^k)(0) = \sigma^{m+(n+k)}(0) = m + (n+k)$

- Komutativita: $m+n = \sigma^m(n) = (\sigma^m \circ \sigma^n)(0) = (\sigma^n \circ \sigma^m)(0) = n+m$

- 0 je neutrální prvek: plyne z předchozího tvrzení

- Křáček: indukcí na k : $A := \{k \in \mathbb{N}_0 \mid m+k = m+k\}$

Buď $m, n \in \mathbb{N}_0$ libovolná:

$0 \in A$ ✓, neutralita nuly

$$\sigma(k) \in A : m + \sigma(k) = \sigma(m+k)$$

$$n + \sigma(k) = \sigma(n+k)$$

$$\Rightarrow m + \sigma(k) = n + \sigma(k) \Rightarrow A = \mathbb{N}_0 \Rightarrow m = n$$

- Pravidlo nuly:

$\Leftarrow$ jasno

$\Rightarrow$ necht' BŮNO $m \neq 0$: $\exists k \in \mathbb{N}_0 : \sigma(k) = m$

$$m + n = m + \sigma(k) = \sigma(m+k) \neq 0$$

Věta: Vlastnosti operace σ .

Binární operace σ je na $\mathbb{N}_0$ asociativní a komutativní s neutrálním prvkem 1 a navíc platí:

Distributivní zákon:

$$\forall m, n, k \in \mathbb{N}_0 : (m+n) \cdot k = m \cdot k + n \cdot k$$

Pravidlo nuly:

$$\forall m, n \in \mathbb{N}_0 : m \cdot n = 0 \Leftrightarrow m = 0 \vee n = 0$$

Důkaz

$$\begin{aligned} \text{• Asociativita : } (m \cdot n) \cdot k &= (\sigma^{(m \cdot n)})^k(0) = \sigma^{m \cdot n \cdot k}(0) = (\sigma^m)^{n \cdot k}(0) = \\ &= m \cdot (n \cdot k) \end{aligned}$$

$$\text{• Komutativita : } m \cdot n = \sigma^{m \cdot n}(0) = \sigma^{n \cdot m}(0) = n \cdot m$$

• neutrální prvek 1 : plyne z předchozích tvrzení

$$\begin{aligned} \text{• Distributivní zákon : } (m+n) \cdot k &= (\sigma^{m+n})^k(0) = (\sigma^m \circ \sigma^n)^k(0) = \\ &= ((\sigma^m)^k \circ (\sigma^n)^k)(0) = \sigma^{mk+nk}(0) = \\ &= m \cdot k + n \cdot k \end{aligned}$$

• Pravidlo nuly:

$\Leftarrow$ plyne z předchozích tvrzení

$\Rightarrow$ necht' $m \neq 0, n \neq 0 : \exists k \in \mathbb{N}_0 : n = \sigma(k)$

$$m \cdot n = m \cdot \sigma(k) = \underbrace{m}_{\neq 0} + k \cdot m \neq 0$$

Definicija: Uspoređivanje na $\mathbb{N}_0$

Na $\mathbb{N}_0$ zavedimo relaciju $\leq$:

$$\forall m, n \in \mathbb{N}_0 : m \leq n \Leftrightarrow \exists x \in \mathbb{N}_0 : n = m + x$$

$$m < n \Leftrightarrow \exists x \in \mathbb{N}_0 \setminus \{0\} : n = m + x$$

a nazivamo je usporođivanje na $\mathbb{N}_0$.

Teoremi: Uspoređivanje na $\mathbb{N}_0$ je usporođivanje

Dokaz:

Reflexivita: $\forall m \in \mathbb{N}_0 : m \leq m$, $x = 0$

Antisimetrija: $\forall m, n \in \mathbb{N}_0 : m \leq n \wedge n \leq m \stackrel{?}{\Rightarrow} m = n$

$$m = m + x_1 \wedge n = m + x_2 \Rightarrow m = m + (x_1 + x_2) \rightarrow x_1 = x_2 = 0$$

Tranzitivita: $\forall m, n, k \in \mathbb{N}_0 : m \leq n \wedge n \leq k \stackrel{?}{\Rightarrow} m \leq k$

$$m = m + x_1 \wedge k = n + x_2 \Rightarrow k = m + (x_1 + x_2) \stackrel{!}{=} m + x \quad \text{gdje } x = x_1 + x_2$$

Plati:

- $\forall n \in \mathbb{N}_0 : n \geq 0$

dk: $n = 0 + n$ ✓

- $\forall n \in \mathbb{N}_0 : \sigma(n) > n$

dk: $\sigma(n) = n + 1$

- $\forall n \in \mathbb{N}_0 \setminus \{0\} : n \geq 1$

dk: $A := \{n \in \mathbb{N}_0 \mid n \geq 1\} \cup \{0\} : \left. \begin{array}{l} \text{① } 0 \in A \quad \checkmark \\ \text{② } \sigma(n) > n \geq 1 \quad \checkmark \end{array} \right\} \rightarrow A = \mathbb{N}_0$

- $\forall m, n, k \in \mathbb{N}_0 : m < n \Rightarrow m + k < n + k$

dk: $m < n \Leftrightarrow \exists x \in \mathbb{N}_0 \setminus \{0\} : n = m + x \rightarrow n + k = m + k + x$

- $\forall m, n, k \in \mathbb{N}_0, k \neq 0 : m < n \Rightarrow m \cdot k < n \cdot k$

dk: $m < n \Leftrightarrow \exists x \in \mathbb{N}_0 \setminus \{0\} : n = m + x \rightarrow m \cdot k = (m + x) \cdot k = m \cdot k + x \cdot k$

- $\forall m, n \in \mathbb{N}_0 : m < n \Rightarrow \sigma(m) \leq n$

dk: $m < n \Leftrightarrow \exists x \in \mathbb{N}_0 \setminus \{0\} : n = m + x = m + \sigma(k) = m + 1 + k$
 $\uparrow$
 $\exists k \in \mathbb{N}_0 : \sigma(k) = x$

Věta: Uspořádaná $\mathbb{N}_0$ je dobře!

Důkaz:

Bud' $A \subset \mathbb{N}_0$ libovolná neprázdná:

$M_A := \{k \in \mathbb{N}_0 \mid \forall m \in A : k \leq m\}$, chceme: $M_A \cap A \neq \emptyset$

sporem:

Necht' $M_A \cap A = \emptyset$: ① $0 \in M_A$

② $\sigma(k) \leq m, \forall m \in A$

$k \leq m \wedge M_A \cap A \Rightarrow k < m$

$\rightarrow M_A = \mathbb{N}_0$

$\rightarrow A = \emptyset$, spor

Trvzení:

$\forall m, n, k \in \mathbb{N}_0, k \neq 0 : m \cdot k = n \cdot k \Rightarrow m = n$

Důkaz:

$\mathbb{N}_0$ je úplně uspořádaná $\rightarrow$ platí trichotomie

Necht' $m \neq n$, pak $\exists \mathbb{N}_0 : m < n$

$\rightarrow \exists x \in \mathbb{N}_0 \setminus \{0\} : n = m + x$

$\rightarrow m \cdot k = (m + x) \cdot k = m \cdot k + \underbrace{x \cdot k}_{\neq 0} \rightarrow m \cdot k < m \cdot k$, spor

Mohutnost množin

Definice: Ekvivalence množin

Množiny M, N jsou ekvivalentní (mají stejnou mohutnost), když existuje bijekce $f: M \rightarrow N$.

Píšeme: $\text{card}(M) = \text{card}(N)$, značíme $M \sim N$

Definice: Axiom výběru

Na každé množině M existuje selektor (výběrová funkce),
 $f: \mathcal{P}(M) \setminus \{\emptyset\} \rightarrow M: \forall A \subset M, A \neq \emptyset: f(A) \in A$

Trvzení:

Každá nekonečná množina má spočetnou podmnožinu:

Důkaz:

Nechť A je množina: $|A| = +\infty$:

stačí sestavit posloupnost prvků z A :

volíme: $a_0 \in A$ libovolně

$a_1 \in A \setminus \{a_0\}$ libovolně

$a_2 \in A \setminus \{a_0, a_1\}$ libovolně

$\vdots$

$a_n \in A \setminus \{a_0, \dots, a_{n-1}\}$ libovolně

→ Sestavili jsme posloupnost $(a_n)_{n \geq 0}$, sed spočetnou podmnožinu

Důsledek:

$\text{card}(\aleph_0) =: \aleph_0$ je nejmenší nekonečná kardinalita

Definice: Subvalence

Nechť M, N jsou libovolné množiny.

Řekneme, že M je subvalentní N , když existuje injektivní zobrazení $f: M \rightarrow N$

Poznámka

M je subvalentní N , když je ekvivalentní nějaké podmnožině

Lemma:

Nechť M, N jsou množiny a $\varphi: M \rightarrow M$ zobrazení takové, že:
 $\varphi(M) \subset N \subset M$, φ prosté!

Potom $M \sim N$

Důkaz:

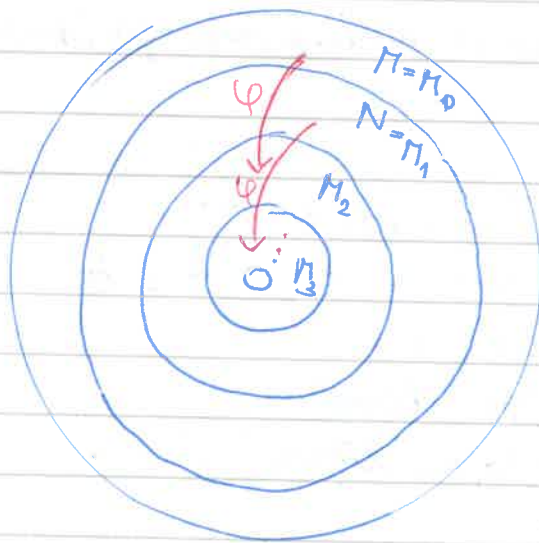
Položme:

$$M_0 := M$$

$$M_1 := N$$

$$M_{2k} := \varphi^k(M_0)$$

$$M_{2k+1} := \varphi^k(M_1)$$



Z předpokladů dále plyne:

$$M_1 = N \subset M_0 = M$$

$$\varphi(M) \subset N$$

$$\varphi(M_1) \subset \varphi(M_0)$$

$$\varphi(M_0) \subset M_1$$

$$\varphi^k(M_1) \subset \varphi^k(M_0)$$

$$\varphi^{k+1}(M_0) \subset \varphi^k(M_1)$$

$$\rightarrow M_{2k+1} \subset M_{2k}$$

$$\rightarrow M_{2k+2} \subset M_{2k+1}$$

$$\rightarrow M = M_0 \supset N = M_1 \supset M_2 \supset M_3 \supset \dots \supset M_{2k} \supset M_{2k+1} \supset M_{2k+2} \supset \dots$$

$$\bullet \varphi(M_{2k} \setminus M_{2k+1}) = M_{2k+2} \setminus M_{2k+3}$$

$$\bullet \varphi(M_{2k+1} \setminus M_{2k+2}) = M_{2k+3} \setminus M_{2k+4}$$

Označme: $P := \bigcap_{n=0}^{+\infty} M_n$

Získali jsme disjunktivní rozklad M na „mezích“ zobrazení:

$$\begin{aligned} M &= P \dot{\cup} \left(\dot{\bigcup}_{k=0}^{+\infty} (M_k \setminus M_{k+1}) \right) = \\ &= P \dot{\cup} \left(\dot{\bigcup}_{k=0}^{+\infty} (M_{2k} \setminus M_{2k+1}) \right) \dot{\cup} \left(\dot{\bigcup}_{k=0}^{+\infty} (M_{2k+1} \setminus M_{2k+2}) \right) \end{aligned}$$

Nyní definujeme bijekci $\psi: M \rightarrow N$:

$$\psi(x) := \begin{cases} \varphi(x), & x \in \dot{\bigcup}_{k=0}^{+\infty} (M_{2k} \setminus M_{2k+1}) \\ x, & \text{jinak} \end{cases}$$

Zbývá ověřit, že se jedná o bijekci:

- ψ je zřejmě prosté
- Ověříme, že ψ je surjektivní, tj: $\forall y \in N: \exists x \in M: \psi(x) = y$

Bud' $y \in N$ libovolné:

- $y \in P \dot{\cup} \left(\dot{\bigcup}_{n=0}^{+\infty} (M_{2n+1} \setminus M_{2n+2}) \right) \rightarrow x = y$
- $y \in \dot{\bigcup}_{n=1}^{+\infty} (M_{2n} \setminus M_{2n+1}) \rightarrow \dot{\bigcup}_{n=1}^{+\infty} (M_{2n} \setminus M_{2n+1}) = \varphi \left(\dot{\bigcup}_{n=0}^{+\infty} (M_{2n} \setminus M_{2n+1}) \right)$

Věta: Cantor - Bernstein - Schröder

Nechť M, N jsou množiny takové, že existují prostá zobrazení

$$f: M \rightarrow N, g: N \rightarrow M.$$

Potom $M \sim N$.

Důkaz:

Položme $\psi := g \circ f: M \rightarrow M$, pak platí:

$$\psi(M) \subset g(N) \subset M \xrightarrow{\text{Lemma}} g(N) \sim M \Rightarrow N \sim M$$

(g je bijekce N na $g(N)$, je prosté)

Důsledek:

Subvalence je uspořádaná třída ekvivalence vůči bijekcím.

Důkaz:

Reflexivita: M subvalentní M

Cantor-Bernstein

Antisymetrie: M subvalentní N , N subvalentní $M \Rightarrow M \sim N$

Tranzitivita: M subvalentní N , N subvalentní $P \Rightarrow M$ subvalentní P

Poznámka:

$\text{card}(M) \leq \text{card}(N) \Leftrightarrow M$ subvalentní N

$\text{card}(M) < \text{card}(N) \Leftrightarrow M$ subvalentní N , M nevsubvalentní M

Věta: Cantor

$$\text{card}(M) < \text{card}(P(M))$$

Důkaz:

• M subvalentní $P(M)$: $f(x) := \{x\}$, $\forall x \in M$

• $P(M)$ nevsubvalentní M :

Nechť $M \sim P(M) \Leftrightarrow \exists g: M \rightarrow P(M)$ bijekce

položme: $D := \{x \in M \mid x \in g(x)\}$

$$d := g^{-1}(D)$$

$\rightarrow d \in D \Leftrightarrow d \in g(d) = D$, spor

Úplně uspořádané množiny

Definice: Podobnost

Necht' $(A, \leq_1), (B, \leq_2)$ jsou úplně uspořádané množiny.

Potom řekneme, že A je podobná B (relace podobnost: $A \cong B$), pokud existuje zobrazení $f: A \rightarrow B$, které je bijektivní a izotomní.

Poznámka:

Izotomie: $\forall x, y \in A: x \leq_1 y \Rightarrow f(x) \leq_2 f(y)$

Lemma:

Podobnost je ekvivalence na třídách úplně uspořádaných množin vůči izotomním bijekcím.

Důkaz:

Reflexivita: $A \cong A, f := \text{id}$

Symetrie: $A \cong B \Rightarrow B \cong A, f: A \rightarrow B$ izotomní bijekce $\Rightarrow g := f^{-1}$ izotomní bijekce

Tranzitivita: $A \cong B \wedge B \cong C \Rightarrow A \cong C, f: A \rightarrow B, g: B \rightarrow C$ izotomní bijekce:
 $\rightarrow h: A \rightarrow C := g \circ f$ izotomní bijekce

Definice: Ordinační typ

Ordinalní typ je charakteristická vlastnost tříd ekvivalence na všech úplně uspořádaných množinách podle $\cong$.

Značí se $\text{ord } A$.

Příklad:

• $\text{ord } \emptyset = 0$

• necht' M je úplně uspořádaná a $|M| = n \in \mathbb{N}$,
pak $\text{ord } M = n$

• $\text{ord } (\mathbb{N}_0, \leq) = \omega$

Definice: Uspořádané' sjednocení'

Pro $(M_1, \leq_1), (M_2, \leq_2)$ dobře uspořádané' množiny zavedíme uspořádané' sjednocení' $M_1 + M_2 := (M_1 \cup M_2, \leq)$:

$$\forall x, y \in M_1: x \leq y \Leftrightarrow x \leq_1 y$$

$$\forall x \in M_1, \forall y \in M_2: x \leq y$$

Definice: Uspořádaný' kartézský' součin

Pro $(M_1, \leq_1), (M_2, \leq_2)$ dobře uspořádané' množiny zavedíme uspořádaný' kartézský' součin $M_1 \cdot M_2 := (M_1 \times M_2, \leq)$

Zpětne' lexikografické' uspořádané' :

$$(x, y) \leq (u, w) \Leftrightarrow y \leq_2 w \vee (y = w \wedge x \leq_1 u)$$

Poznámka:

• $M_1 + M_2, M_1 \cdot M_2$ jsou dobře uspořádané'

• Značení:

$$\alpha = \text{ord}(A), \beta = \text{ord}(B)$$

$$\text{pač: } \text{ord}(A+B) =: \alpha + \beta$$

$$\text{ord}(A \cdot B) =: \alpha \cdot \beta$$

• Operace jsou dobře definované, tj.: nezávisí na volbě A, B vůči

Příklad:

$$\bullet 1 + \omega: \text{ord}(\{b\}) = 1: \{b\} + \mathbb{N}_0: b < 0 < 1 < \dots$$

$$\text{ord}(\mathbb{N}_0) = \omega$$

$$\mathbb{N}_0: 0 < 1 < 2 < \dots$$

$$\rightarrow 1 + \omega = \omega$$

$$\bullet \omega + 1: \text{ord}(\{b\}) = 1: \mathbb{N}_0 + \{b\}: 0 < 1 < 2 < \dots < b$$

$$\text{ord}(\mathbb{N}_0) = \omega$$

$$\rightarrow \omega + 1 \neq 1 + \omega = \omega$$

- $2 \cdot \omega : \text{ord}(\{a, b\}) = 2 : \{a, b\} \cdot \mathbb{N}_0 : \underbrace{\{(x, k) \mid x \in \{a, b\}, k \in \mathbb{N}_0\}}_{x_k}$
 $\text{ord}(\mathbb{N}_0) = \omega$

$$\begin{array}{ccccccc} a_0 & < & b_0 & < & a_1 & < & b_1 & < & \dots & \rightarrow & 2 \cdot \omega = \omega \\ 0 \downarrow & & 1 \downarrow & & 2 \downarrow & & 3 \downarrow & & & & & & \end{array}$$

- $\omega \cdot 2 : \text{ord}(\{a, b\}) = 2 : \mathbb{N}_0 \cdot \{a, b\} : \{(k, x) \mid x \in \{a, b\}, k \in \mathbb{N}_0\}$
 $\text{ord}(\mathbb{N}_0) = \omega$

$$a_0 < a_1 < a_2 < \dots < b_0 < b_1 < b_2 < \dots$$

$$\rightarrow \omega \cdot 2 = \omega + \omega$$

- $\omega \cdot \omega : \text{ord}(\mathbb{N}_0) = \omega : \mathbb{N}_0 \cdot \mathbb{N}_0 : \underbrace{\{(n, k) \mid n \in \mathbb{N}_0, k \in \mathbb{N}_0\}}_{a_{k,n}}$

$$a_{0,0} < a_{1,0} < a_{2,0} < \dots < a_{0,1} < a_{1,1} < a_{2,1} < \dots < a_{0,2} < a_{1,2} < a_{2,2} < \dots$$

$$\rightarrow \omega \cdot \omega = \omega + \omega + \dots$$

Poznámka:

- $n + \omega = \omega$

- $n \cdot \omega = \omega$

- $\omega \cdot n = \underbrace{\omega + \omega + \dots + \omega}_n$

- Značení: $\omega^2 \equiv \omega \cdot \omega$

Definice: Uspořádané ordinály

Pro ordinální čísla α, β dobře uspořádaných množin A, B píšeme $\alpha \leq \beta$, právě když A lze podobně zobrazit na B nebo na nějaký jeho úsek

Tvzení:

Uspořádané ordinály jsou uspořádané

Důkaz:

Reflexivita: $\alpha \leq \alpha \quad \checkmark$

Antisymetrie: $\alpha \leq \beta \wedge \beta \leq \alpha \stackrel{?}{\Rightarrow} \alpha = \beta$

Transitivita: $\alpha \leq \beta \wedge \beta \leq \gamma \Rightarrow \alpha \leq \gamma \quad \checkmark$

Antisymetrie není jasná, proto budeme potřebovat následující lemma:

Lemma

Nechť M je dobře uspořádaná množina, $N \subset M$.
Je-li f podobnost M na N , pak $x \leq f(x)$, $\forall x \in M$.

Důkaz:

položme $A = \{x \in M \mid x \leq f(x)\}$

Transfinitní indukce:

Bud' $a \in M$ libovolné: $M_a \subset A \stackrel{?}{\Rightarrow} a \in A$

nechť $a \in A$, tj. $a > f(a)$:

• $a > f(a) \rightarrow f(a) \in M_a \rightarrow f(a) \leq f(f(a))$

• f podobnost: $a > f(a) \rightarrow f(a) > f(f(a))$, spor

$\rightarrow a \in A \rightarrow A = M$

Důsledek:

Žádná dobře uspořádaná množina není podobná svému úseku.

Důkaz:

Bud' M dobře uspořádaná množina, $a \in M$.

Nechť platí: $M_a \cong M$, tj.: $\exists f: M \rightarrow M_a$ podobnost:

• Lemma $\rightarrow a \leq f(a)$

• f bijekce: $f(a) \in M_a \Leftrightarrow f(a) < a$, spor

Důsledek:

Pro ordinální čísla platí antisymetrie; tj.:

$$\alpha \leq \beta \wedge \beta \leq \alpha \Rightarrow \alpha = \beta$$

Důkaz:

Kdyby $\alpha \neq \beta$: $\alpha < \beta$: $\exists f: A \rightarrow B$ podobnost
 $\alpha \geq \beta$: $\exists g: B \rightarrow A$ podobnost

$\rightarrow h: g \circ f: A \rightarrow A$ podobnost, spor.

Poznámka:

$$(A_a)_c = A_c, c \in A_a$$

Nyní nás zajímá jak porovnat libovolná ordinální čísla:
Neexistuje množina všech ordinálních čísel.

Formální postup:

1. U - "dostatečně velká množina"

2. $\tilde{W} := \{\text{ord } A \mid A \in P(U), A \text{ dobře uspořádaná}\}$

Pro $\gamma \in \tilde{W}$ zavedeme: $W(\gamma) = \{\beta \in \tilde{W} \mid \beta < \gamma\}$

Platí:

Jestliže A je dobře uspořádána, $\alpha = \text{ord } A$,
pak $f: A \rightarrow W(\alpha): a \mapsto \text{ord}(A_a)$ je podobnost.

Důsledek:

$W(\alpha)$ je dobře uspořádána

Trvsemí:

Nechť α, β jsou ordinální čísla, $\gamma := \text{ord}(W(\alpha) \cap W(\beta))$.

Potom platí: ① $W(\alpha) \cap W(\beta) = W(\gamma)$

$\gamma: \gamma \leq \alpha, \gamma \leq \beta$

② Nenastane zároveň $\gamma < \alpha$ a $\gamma < \beta$

Důkaz:

$$\gamma = \alpha, \gamma = \beta \Rightarrow \alpha = \beta$$

$$\gamma < \alpha, \gamma = \beta \Rightarrow \beta < \alpha$$

$$\gamma = \alpha, \gamma < \beta \Rightarrow \alpha < \beta$$

$\gamma < \alpha, \gamma < \beta$ nemůže nastat

Důsledek:

Mohutnost každých dvou dobře uspořádaných množin lze porovnat.

Důkaz:

Budť A, B dobře uspořádány, $\alpha = \text{ord}(A)$
 $\beta = \text{ord}(B)$

Ordinální čísla umíme porovnat $\rightarrow$ BUŇO $\alpha \leq \beta$

$\rightarrow \exists f: A \rightarrow B$ mono

$\rightarrow \text{card}(A) \leq \text{card}(B)$

Poznámka:

Přijmeme-li axiom výběru, resp. větu o dobře uspořádanosti, pak lze porovnávat mohutnosti libovolných množin.

Ordinální číslo	Ordinální typ
0	$\emptyset$
1	$\{\emptyset\} = \{0\}$
2	$\{0, 1\}$
3	$\{0, 1, 2\}$
$\vdots$	$\vdots$
ω	$\{0, 1, \dots\} = W(\omega)$
$\omega+1$	$\{0, 1, \dots, \omega\} = W(\omega+1)$
$\vdots$	$\vdots$
$\omega+\omega$	$\{0, 1, \dots, \omega+\omega+1, \dots\} = W(\omega \cdot 2)$
$\vdots$	$\vdots$

$\left. \begin{matrix} \omega \\ \omega+1 \\ \vdots \\ \omega+\omega \\ \vdots \end{matrix} \right\} \aleph_0$

- Každé ordinální číslo má svého následníka
- Ordinální čísla, která nemají svého předchůdce se nazývají limitní
tj.: jejich ordinální typ nemá poslední prvek

Lemma:

Je-li M množina ordinálních čísel, pak M je dobře uspořádaná.

Důkaz:

Bud' $A \subset M, A \neq \emptyset$ libovolná

Nechť $\alpha, \beta \in A, \beta \neq 0 \Rightarrow \alpha < \beta \Rightarrow \alpha \in (W(\beta) \cap A) \subset W(\beta)$

$\rightarrow$ existuje nejmenší prvek $\gamma \in W(\beta) \cap A$

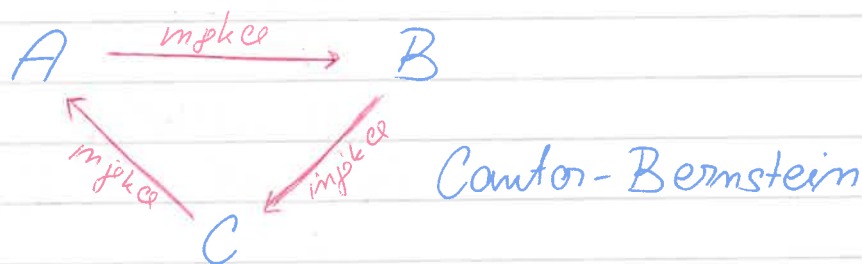
Kdyby existovalo $\delta \in A: \delta < \gamma \leq \alpha < \beta \rightarrow \delta \in (W(\beta) \cap A)$, spor.

Dobře uspořádaná
 $\downarrow$

Poznámka:

Přirázení $\alpha = \text{ord}(A) \mapsto \text{card}(A)$ je zobrazení

- Na konečných množinách bijekce
- Na nekonečných množinách se může stát:
 $\text{ord}(A) < \text{ord}(B)$ ale $\text{card}(A) = \text{card}(B)$
- Jestliže $\alpha < \beta < \gamma$ jsou ordinální čísla množin A, B, C
a $\text{card}(A) = \text{card}(C)$, pak $\text{card}(A) = \text{card}(B)$



- Interval ordinálních čísel se stejnou mohutností nemá největší prvek, ale má nejmenší prvek

Důkaz:

- Minimalita je sjímatelná
- S každým $\alpha \in I$ i $\alpha + 1 \in I$
- Nejmenší prvek $\mu \in I$ je limitou ordinálních čísel, jinak by $\mu \in I$ měl předchozí prvek ν , který je předchůdcem μ .

Definice: Kardinální čísla

Nejmenší prvek κ intervalu ordinálních čísel se stejnou mohutností se nazývá kardinální číslo

Cantorova číselová: $\aleph_0, \aleph_1, \dots, \aleph_\omega, \aleph_{\omega+1}$

Poznámka:

Každé kardinální číslo má svého následníka (Cantor)

Hypotéza kontinua:

$$\text{card}(\mathbb{R}) = \text{card}(\mathcal{P}(\mathbb{N}_0)) = 2^{\aleph_0} \quad \text{Kontinuum}$$

$$\text{Otázka: } 2^{\aleph_0} \stackrel{?}{=} \aleph_1 > \aleph_0$$

$$\text{Zobecněná hypotéza kontinua: } 2^{\aleph_\alpha} \stackrel{?}{=} \aleph_{\alpha+1}$$

Axiom výběru

Následující tvrzení jsou ekvivalentní:

- Axiom výběru
- Zermelova lemma (věta o dobrém uspořádání)
- Zornova lemma

Zornova lemma:

Je-li M uspořádaná množina, ve které má každý řetězec horní záhoru, pak M obsahuje maximální prvek.

Řetězec: nepořádná, úplně uspořádaná podmnožina

Univerzální algebry

Definice: n -ární operace

Bud' M libovolná neprázdná množina, $n \in \mathbb{N}_0$.

Zobrazení $f: M^n \rightarrow M$ nazýváme n -ární operací na M .

$n = 2$ binární

$n = 1$ unární

$n = 0$ nulární (rybář významného polu)

Definice: univerzální algebra

Univerzální algebra je uspořádaná dvojice (A, Ω) , kde

$A \neq \emptyset$ je nosič algebry,

$\Omega \neq \emptyset$ je množina operací na A

Definice: Groupoid

Groupoid je dvojice $(M, *)$.

$M \neq \emptyset$

$*$ je binární operace na M

Definice: Pologrupa

Pologrupa je dvojice $(M, *)$.

$M \neq \emptyset$

$*$ je binární operace na $M: \forall x, y, z \in M: x * (y * z) = (x * y) * z$ (Asociativita)

Pokud je navíc operace $*$ komutativní, pak mluvíme o komutativní pologrupě.

Příklad:

$(\mathbb{Z}, -)$ groupoid: $x - (y - z) \neq (x - y) - z$ (neú pologrupa)

$(\mathbb{Q}, \oplus)$, $x \oplus y := \frac{x+y}{2}$, komutativní, neú asociativní (Groupoid)

$(\mathbb{N}_0, +)$ je pologrupa

Věta:

V pologrupě M nezávisí na pořadí provádění operací, tj.:
 $\forall n \in \mathbb{N} : \forall x_1, \dots, x_n \in M$ platí, že výsledek $x_1 * \dots * x_n$
nezávisí na rozmištnění závorek

Lemma:

$$\forall n, m \in \mathbb{N} : \left(\prod_{k=1}^n a_k \right) * \left(\prod_{k=1}^m a_{k+n} \right) = \prod_{k=1}^{n+m} a_k$$

Důkaz:

Bud' $m \in \mathbb{N}$ libovolně: ~~arbitrárně~~

$m=1$: jasně!

$$\begin{aligned} m \rightarrow m+1 : \left(\prod_{k=1}^n a_k \right) * \left(\prod_{k=1}^{m+1} a_{k+n} \right) &= \left(\prod_{k=1}^n a_k \right) * \left(\prod_{k=1}^m a_{k+n} \right) * a_{n+m+1} = \\ &= \left(\prod_{k=1}^{n+m} a_k \right) * a_{n+m+1} = \prod_{k=1}^{n+m+1} a_k \end{aligned}$$

Důkaz věty:

$n=1, 2$: triviální!

$n=3$: asociativní zákon

$n \geq 4$: Ve výrazu $x_1 * \dots * x_n$ provedu $n-2$ operací,
poslední je tvaru $u * v$, kde:

$$u = \prod_{j=1}^k x_j, \quad v = \prod_{j=1}^{n-k} x_{k+j}, \quad k \in \hat{n}$$

$\rightarrow$ z lemmatu už trváce plyne

Poznámka:

• Multiplikativní zápis: $*$ $\equiv$ $\cdot$

$$\prod_{k=1}^n a_k = a_1 \cdot a_2 \cdot \dots \cdot a_n$$

$$\underbrace{a \cdot a \cdot \dots \cdot a}_{n\text{-krát}} = a^n$$

• Aditivní zápis: $*$ $\equiv$ $+$

$$\prod_{k=1}^n a_k = a_1 + a_2 + \dots + a_n$$

$$\underbrace{a + a + \dots + a}_{n\text{-krát}} = n \times a$$

Definice: Neutra'ni' prvek

Prvek e v pologrupě $(M, *)$ je neutra'ni' prvek, pokud: $\forall x \in M: x * e = e * x = x$

Definice: Monoid

Pologrupa s neutra'nim prvkem $(M, *, e)$ se nazývá monoid

Tvrzení:

Neutra'ni' prvek je v Monoidu právě jeden.

~~Důkaz~~

Důkaz:

Nechť e_1, e_2 jsou neutra'ni' prvky:

$$e_1 * e_2 = e_1 = e_2$$

Poznámka:

V multiplikativním zápise: $e = 1$

V aditivním zápise: $e = 0$

Příklady:

$(\mathbb{N}_0, +, 0)$

$(\mathbb{N}, \cdot, 1)$

Definice: Homomorfismus pologrup

Nechť $(M_1, *_1), (M_2, *_2)$ jsou pologrupy, $f: M_1 \rightarrow M_2$.

Řekneme, že f je homomorfismus pologrup, pokud:

$$\forall x, y \in M_1: x *_1 y = f(x) *_2 f(y)$$

Definice: Homomorfismus monoidů

Nechť $(M_1, *_1, e_1), (M_2, *_2, e_2)$ jsou monoidy, $f: M_1 \rightarrow M_2$.

Řekneme, že f je homomorfismus monoidů, jestliže

f je homomorfismus pologrup a navíc $f(e_1) = e_2$

Průklad:

$A = (\{1\}, \cdot, 1)$ monoid

$B = (D, \cdot, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix})$, $D = \{ \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \}$

$f: A \rightarrow B: f(1) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

f je homomorfismus pologrup, ale není homomorfismus monoidů

Definice:

Nechť f je homomorfismus pologrup (monoidů).

Připome, že f je:

- Epimorfismus $\Leftrightarrow f$ je surjektivní
- Monomorfismus $\Leftrightarrow f$ je injektivní
- Isomorfismus $\Leftrightarrow f$ je bijektivní
- Endomorfismus $\Leftrightarrow f: M \rightarrow M$
- Automorfismus $\Leftrightarrow f: M \rightarrow M$ bijekce

Průklad:

- Monoid konečných slov nad abecedou A :

$A = \{a_1, \dots, a_n\}$ množina písmen (abeceda)

$A^* := \bigcup_{n=0}^{\infty} A^n$, ($A^0 = \{\emptyset\}$), $\emptyset := \varepsilon$

$\circ: A^* \times A^* \rightarrow A^* : (x_1, \dots, x_k) \circ (y_1, \dots, y_\ell) := (x_1, \dots, x_k, y_1, \dots, y_\ell)$

Pak $(A^*, \circ, \varepsilon)$ je monoid

- $M := \{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbb{N}_0^{2,2} \mid \det \begin{pmatrix} a & b \\ c & d \end{pmatrix} = 1 \}$
 $(M, \cdot, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix})$ monoid

$N = (\{0, 1\}^*, \cdot, \varepsilon)$ monoid

M je isomorfní N (SSM1)

Tvrzení:

Každou pologrupu lze rozšířit na monoid.

Důkaz:

Bud' M libovolná pologrupa.

Neu-li už M monoid definujeme monoid jako:

$$(M \cup \{e\}, *, e): e * x := x, x * e := x$$

Definice: Absorbující prvek

Nechť $(M, *)$ je pologrupa, $a \in M$.

Řekneme, že a je absorbující prvek, jestliže: $\forall b \in M: b * a = a * b = a$.

Platí:

V každé pologrupě je nejvýše jeden absorbující prvek.

Důkaz:

Bud' a, b absorbující prvky v pologrupě M : $a * b = a, a * b = b \rightarrow a = b$

Definice: Nuloid

Pologrupa obsahující absorbující prvek je nuloid.

Tvrzení:

Každou pologrupu lze rozšířit na nuloid.

Důkaz:

Bud' $(M, *)$ libovolná pologrupa.

Neu-li již M nuloid, pak definujeme rozšíření následně:

$$(M \cup \{0\}, *): \forall b \in M: 0 * b = b * 0 = 0$$

Příklad:

$(\mathbb{N}_0, \cdot, 1)$ monoid, který je zároveň nuloid

Definice: Invertibilní prvek, inverzní prvek

Necht' $(M, *, e)$ je monoid, $a \in M$.

Prvek a se nazývá 'invertibilní', jestliže existuje $a' \in M$: $a' * a = a * a' = e$.

Prvek a' se nazývá 'inverzní'.

Příklad:

$(\{0, 1, \dots, 5\}, \cdot \text{mod } 6, 1)$ monoid
 $\mathbb{Z}_6$

Definice: Kvarigrupa

Grupoid $(M, *)$ je kvarigrupa, jestliže $*$ je dělení, tj:

$$\forall a, b \in M: \exists x, y \in M: a * x = b$$

$$y * a = b$$

Příčemž x, y jsou vždy jednoznačné

Poznámka:

$$x = a/b \quad \text{levý podíl}$$

$$y = b/a \quad \text{právní podíl}$$

Příklad:

$(\mathbb{Q} \setminus \{0\}, \div)$ je kvarigrupa

$(\mathbb{Z}, -)$ je kvarigrupa

Definice: Lupa

Kvarigrupa s neutrálním prvkem je lupa.

Platí:

V kvarigrupě platí 'krácení'.

Důkaz:

$$\text{Necht' } \underbrace{a * c}_B = b * \underbrace{c}_A \rightarrow \exists! x \in M: x * A = B \rightarrow x * c = a * c \rightarrow b = a$$

Tvrzení:

Jestliže $\sim$ Grupoidu platí 'hočem', pak je to kvazigrupa.

Důkaz:

níže: $a * c = b * c \Rightarrow a = b$

Chceme: $\forall a, b: \exists! x, y: a * x = b$
 $y * a = b$

Bud'že $a, b \in M$ libovolné: $a * x_1 = b \rightarrow x_1 = x_2$ (leví 'hočem')
 $a * x_2 = b$

Existence plyne z Cayleho tabulky:

	a	b	c	...
a	$a * a$	$a * b$	$a * c$	
b	$b * a$	$b * b$	$b * c$	
c	$c * a$	$c * b$	$c * c$	
$\vdots$				$\ddots$

Grupoid

↓ Asociativita

Pologrupa

↓ Neutrotní prvek

Monoid

↓ Inverzní prvek

Grupa

Grupoid

↓ Dělení

Kvazigrupa

↓ Neutrotní prvek

Leva

↓ Asociativita

Grupa

Grupy

Definice: Grupa

Monoid ve kterém jsou všechny prvky invertibilní se nazývá grupa

Poznámka:

Alternativní definice:

binární unární nulární
↓ ↓ ↓
 $*$ $\sim$ e

Uspořádaná čtveřice $(G, *, \sim, e)$ je grupa, jestliže:

- ① $*$ je asociativní
- ② Prvek e je neutrální
- ③ $\sim$ je přirozený inverzního prvku

Pokud je navíc operace $*$ komutativní, říkáme že grupa je komutativní (Abelova, abelovská)

Tvrzení:

Necht' $(G, *)$ je pologrupa.

Jestliže v G existuje levý neutrální prvek a ke každému $x \in G$ existuje levý inverzní prvek.

Pak G je grupa

Důkaz:

Víme: $\forall x \in G: e * x = x$

Chci: $x * e = x$

$\forall x \in G: \exists x' \in G: x' * x = e$

$x * x' = e$

• $x * e = x * x' * x = e * x = x$

• $x * x' = e: \cancel{e * x * x'} = (x')' * x' = (x')' * (e * x') = (x')' * (x' * x) * x' = e * x' * x' = x * x'$

Trvzení:

V grupě platí krácení

Důkaz:

Nechť $a * e = b * e$:

$$a = a * e = a * c * c^{-1} = b * c * c^{-1} = b * e = b$$

Důsledek:

Rovnice $a * x = b$ pro dané $a, b \in G$ má právě jedno řešení
 $x = a^{-1} * b$

Důkaz:

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

Důsledek:

- Neutroloví prvek v grupě je jednoznačný.
- Inverzní prvek je jednoznačný.
- $(a^{-1})^{-1} = a$
- $(ab)^{-1} = b^{-1} * a^{-1}$

Důkaz:

- Každá grupa je monoid $\rightarrow$ v monoidu je e řešený jednoznačně
- $aa_1 = aa_2 = e \xrightarrow{\text{krácení}} a_1 = a_2$
- $(a^{-1})^{-1} * a^{-1} = e = a * a^{-1} \xrightarrow{\text{krácení}} a = (a^{-1})^{-1}$
- $(ab)^{-1} * ab = e = b^{-1} * a^{-1} * ab \xrightarrow{\text{krácení}} b^{-1} * a^{-1} = (ab)^{-1}$

Definice: Homomorfismus grup

Nechť G_1, G_2 jsou grupy, $f: G_1 \rightarrow G_2$.

Řekneme, že f je homomorfismus grup G_1, G_2 , jestliže:

$$\forall a, b \in G_1: f(a * b) = f(a) *_2 f(b)$$

Definice:

Nechť $f: G_1 \rightarrow G_2$ je homomorfismus grup.

Překážme, že f je:

- ① Epimorfismus $\Leftrightarrow f$ je surjektivní
- ② Monomorfismus $\Leftrightarrow f$ je injektivní
- ③ Isomorfismus $\Leftrightarrow f$ je bijektivní
- ④ Endomorfismus $\Leftrightarrow f: G \rightarrow G$
- ⑤ Automorfismus $\Leftrightarrow f: G \rightarrow G$, bijekce

Tworzenie:

Nechť $f: G_1 \rightarrow G_2$ je homomorfismus grup.

Paž platí: ① $f(e_1) = e_2$
② $f(a^{-1}) = (f(a))^{-1}$

Důkaz:

- ① $f(e_1) = f(e_1 * e_1) = f(e_1) * f(e_1)$, $f(e_1) = f(e_1) * e_2$
 $\rightarrow$ zkrácením plyne: $e_2 = f(e_1)$
- ② $(f(a))^{-1} * f(a) = e_2 = f(a^{-1}) * f(a) \xrightarrow{\text{zkrácením}} (f(a))^{-1} = f(a^{-1})$

Příklad:

$f: \mathbb{Z} \rightarrow G$, G libovolná grupa, $a \in G$

$f(n) := a^n, n \in \mathbb{Z}$

$f(n+m) = a^n \cdot a^m = a^{n+m} = f(n) \cdot f(m)$

Věta: $\mathbb{Z}_n^*$

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

$(\mathbb{Z}_n^*, \cdot \text{ mod } n, 1)$ je grupa $\Leftrightarrow n \in \mathbb{P}$

Důkaz:

$\Rightarrow$ Necht n je složené: $\exists a \in \mathbb{Z}_n^*: a \perp n$

$\rightarrow$ vzhledem k tomu, že a má inverzi $b \in \mathbb{Z}_n^*: ab \equiv 1 \text{ mod } n$

$\rightarrow n \mid ab - 1 \rightarrow ab - 1 = kn \rightarrow ab - kn = 1$, což ale neexistuje řešení, spor

$\Leftarrow$: Necht $n \in \mathbb{P}$: Bud $a \in \mathbb{Z}_n^*$ libovolné, pak vždy existuje řešení rovnice $ab - kn = 1 \Leftrightarrow ab \equiv 1 \text{ mod } n$

Definice: Podgrupa

Necht G je grupa, $H \subset G$.

Řekneme, že H je podgrupa G , jestliže:

- ① $e \in H$
- ② $\forall a \in H: a^{-1} \in H$
- ③ $\forall a, b \in H: ab \in H$

Poznámka:

- ① plyne z ② a ③, protože $H \neq \emptyset$

Věta:

Necht G je grupa, $H \subset G$, $H \neq \emptyset$.

Paž H je podgrupa $G \Leftrightarrow \forall a, b \in H: a^{-1}b \in H$

Důkaz:

$\Rightarrow$ jasné

$\Leftarrow$: ① Bud' $a \in H$ libovolně, $b := a \rightarrow a \cdot a^{-1} = e \in H$

② $a := e, b := a^{-1} \rightarrow a^{-1} \in H$

③ $a := a^{-1}, b := b \rightarrow ab \in H$

Poznámka:

Každá podgrupa G má podgrupy $\{e\}$ a G ,
tyto podgrupy se nazývají netriviální.

Definice: Jádru homomorfismu

Necht $f: G \rightarrow H$ je homomorfismus grup.

Paž množinu $\text{Ker } f := \{x \in G \mid f(x) = e_H\}$ se nazývá
jádro homomorfismu f .

Twierdzenie:

Niech $f: G \rightarrow H$ jest homomorfizmem grup.

Podział: ① $\text{Ker } f$ jest podgrupą G

② $\text{Im } f$ jest podgrupą H

Dowód:

① $\forall a, b \in \text{Ker } f \Rightarrow a^{-1}b \in \text{Ker } f, e_G \in \text{Ker } f \Rightarrow \text{Ker } f \neq \emptyset$.

Budźcie $a, b \in \text{Ker } f$ dowolne: $f(a^{-1}b) = (f(a))^{-1}f(b) = e_H \in \text{Ker } f$

② $e_H \in \text{Im } f \Rightarrow \text{Im } f \neq \emptyset$

Budźcie $a, b \in \text{Im } f$ dowolne:

$a, b \in \text{Im } f \Rightarrow \exists x, y \in G: f(x) = a, f(y) = b$

$\Rightarrow a^{-1}b = (f(x))^{-1}f(y) = f(x^{-1}y) \in \text{Im } f$

Twierdzenie:

Niech $f: G \rightarrow H$ jest homomorfizmem grup.

f jest monomorfizmem $\Leftrightarrow \text{Ker } f = \{e_G\}$

Dowód:

$\Rightarrow$ Niech f jest monomorfizmem

Budźcie $a \in \text{Ker } f$ dowolne, $a \neq e_G: f(a) = e_H = f(e_G)$, sprz.

$\Leftarrow$ Niech $\text{Ker } f = \{e_G\}$

Niech $\exists a, b \in G, a \neq b: f(a) = f(b) \rightarrow f(a)(f(b))^{-1} = e_H$

$\rightarrow ab^{-1} \in \text{Ker } f = \{e_G\} \rightarrow a = b$, sprz.

Twresen!:

Necht $f: G \rightarrow H$ je homomorfismus grup.

Paž plat!:

- ① $\tilde{G}$ podgrupa $G \Rightarrow f(\tilde{G})$ podgrupa H
- ② $\tilde{H}$ podgrupa $H \Rightarrow f^{-1}(\tilde{H})$ podgrupa G

Dikaz:

① $e_H \in f(\tilde{G}) \Rightarrow f(\tilde{G}) \neq \emptyset$:

Budte $a, b \in f(\tilde{G})$ libovolno! $\exists x, y \in \tilde{G} : a = f(x), b = f(y)$

$$f(a^{-1}b) = (f(x))^{-1}f(y) = f(\underbrace{x^{-1}y}_{\in \tilde{G}}) \in f(\tilde{G})$$

② $e_G \in f^{-1}(\tilde{H}) \Rightarrow f^{-1}(\tilde{H}) \neq \emptyset$:

Budte $a, b \in f^{-1}(\tilde{H})$ libovolno!

$$f(a^{-1}b) = (f(a))^{-1}f(b) \in \tilde{H} \rightarrow a^{-1}b \in f^{-1}(\tilde{H})$$

Příklad:

$$\bullet f: GL(n, T) \rightarrow T^* = (T \setminus \{0\}, \cdot)$$

$$f(A) := \det(A)$$

$$\text{Ker } f = SL(n, T)$$

$$\bullet f: \mathbb{Z}_n \rightarrow \mathbb{C}^*$$

$$f(k) := e^{i \frac{2\pi}{n} k}$$

$$f(\mathbb{Z}_n) = \mathbb{C}_n = \{\sqrt[n]{1}, \dots, \sqrt[n]{1}\}$$

Věta: Cayleyova

Každou grupu lze izomorfně mapovat do nějaké grupy permutací.

Poznámka:

Jiná formulace:

Nechť G je grupa.

Paž existují monomorfismus $f: G \rightarrow S(G)$,
kde $S(G) := (\{f \in G^G \mid f \text{ bijekce} \}, \circ, ^{-1}, 1_G)$

Důkaz:

Chceme sestavit monomorfismus $f: G \rightarrow S(G): a \mapsto \pi_a$

$$\pi_a(x) := a \cdot x$$

• Ověříme, že π_a je bijekce:

$$\bullet \pi_a(x) = \pi_a(y) \rightarrow ax = ay \xrightarrow{\text{krátím}} x = y \text{ (injektivita)}$$

• Buď $z \in G$ libovolně:

$$\text{Rovnice } ax = z \text{ má řešení } x = a^{-1} \cdot z$$

$\rightarrow \pi_a$ bijekce

• f homomorfismus:

Buď $a, b \in G$ libovolně:

$$f(ab) = \pi_{ab} \stackrel{\uparrow}{=} \pi_a \circ \pi_b = f(a) \circ f(b)$$

$$\pi_{ab}(x) = ab \cdot x = a \cdot \pi_b(x) = \pi_a(\pi_b(x)) = (\pi_a \circ \pi_b)(x)$$

• f prostě:

Buď $a, b \in G$ libovolně:

$$\text{Nechť } f(a) = f(b) \rightarrow \pi_a(x) = \pi_b(x) \quad \forall x \in G \rightarrow ax = bx \xrightarrow{\text{krátím}} a = b$$

Důsledek:

Každá konečná grupa o n prvech je izomorfní nějaké podgrupě grupy S_n

Definice: Grupa automorfismů

Nechť G je grupa.

Paž množinu $\text{Aut } G := \{f: G \rightarrow G \mid f \text{ automorfismus}\}$ společně s operací skládání zobrazení nazýváme grupou automorfismů grupy G .

Poznámka:

Grupa automorfismů je grupa.

Tvoreni:

Nechť G je grupa.

Průnik libovolného systému podgrup grupy G je podgrupa.

Důkaz:

Bud' $I = \{H \subset G \mid H \text{ podgrupa } G\}$

položme $M := \bigcap_{H \in I} H$

$e \in M \rightarrow M \neq \emptyset$

Bud' $a, b \in M$ libovolná

$\rightarrow a, b \in H, \forall H \in I \rightarrow a^{-1}b \in H, \forall H \in I \rightarrow a^{-1}b \in M$

$\rightarrow M$ je podgrupa G

Definice: Grupový obal

Nechť G je grupa, $X \subset G, X \neq \emptyset$.

Nejmenší podgrupa grupy G obsahující X jako podmnožinu se nazývá grupový obal množiny X .

značíme $\langle X \rangle$.

Poznámka:

• Množina X se nazývá množina generátorů podgrupy $\langle X \rangle$

• $\langle X \rangle = \bigcap \{H \subset G \mid H \text{ podgrupa } G, X \subset H\}$

Trvzení:

Nechť G je grupa, $X \subset G$, $X \neq \emptyset$.

Paž: $\langle X \rangle = \{x_1^{k_1} \cdot x_2^{k_2} \cdot \dots \cdot x_m^{k_m} \mid m \in \mathbb{N}, x_i \in X, k_i \in \mathbb{Z}\}$

Důkaz:

Označme $H := \{x_1^{k_1} \cdot \dots \cdot x_m^{k_m} \mid m \in \mathbb{N}, x_i \in X, k_i \in \mathbb{Z}\}$

• $\langle X \rangle \subset H$

Zřejmě $X \subset H$, protože $\langle X \rangle$ je minimální množina obsahující X , paž nutně $\langle X \rangle \subset H$

• $\langle X \rangle \supset H$

Bud' $a \in H$ libovolně

$$a = x_1^{k_1} \cdot \dots \cdot x_m^{k_m}$$

$\langle X \rangle$ grupa $\rightarrow x_1, \dots, x_m \in \langle X \rangle \xrightarrow{\langle X \rangle \text{ grupa}} x_1^{k_1}, \dots, x_m^{k_m} \in \langle X \rangle$
 $\rightarrow x_1^{k_1} \cdot \dots \cdot x_m^{k_m} \in \langle X \rangle$

Definice: Řád grupy

Nechť G je grupa.

Paž řádem grupy rozumíme počet prvků grupy.

Značíme $|G|$

Definice: Řád prvku

Nechť G je grupa, $a \in G$.

Řád prvku značíme $|a|$ a rozumíme jím $|a| = |\langle a \rangle|$

Trvorení:

Nechť G je grupa, $a \in G$.

Pať nastane jedna z možností:

- ① $|a| = +\infty \wedge f: \mathbb{Z} \rightarrow G: f(k) := a^k$ je monomorfismus ($f(\mathbb{Z}) = \langle a \rangle$)
- ② $|a| = m \in \mathbb{N} \wedge f: \mathbb{Z}_m \rightarrow G: f(k) := a^k$ je monomorfismus ($f(\mathbb{Z}_m) = \langle a \rangle$)
nově m je minimální takové, že $a^m = e$

Důkaz:

• $f: \mathbb{Z} \rightarrow G: f(k) = a^k$ je homomorfismus

- ① $\ker f = \{0\} \Leftrightarrow f$ je monomorfismus
 $\rightarrow |\mathbb{Z}| = +\infty \wedge f$ je bijekce $\rightarrow |a| = +\infty$

- ② $\ker f \neq \{0\} \Leftrightarrow \exists k \in \mathbb{Z} \setminus \{0\}: a^k = e$, BUŇO $k \in \mathbb{N}$
Označme $m := \min \{k \in \mathbb{N} \mid a^k = e\}$

Bud' ~~ma~~ $a^m \in \langle a \rangle$:

$$a^m = a^{km+r} = (a^m)^k \cdot a^r = a^r$$

$$\rightarrow \langle a \rangle = \{a^r \mid 0 \leq r < m-1\}$$

Zbylo' ověřit, že $f: \mathbb{Z}_m \rightarrow G$ je monomorfismus:

Bud' $k, l \in \{0, \dots, m-1\}$ libovolná:

$$f(k) = f(l) \rightarrow a^k = a^l \rightarrow a^{k-l} = e, \text{ ~~z čehož plyne~~ }$$

Kdyby $k \neq l$: $1 \leq k-l < m \rightarrow$ spor s minimalitou m

Twoseň:

Necht' G je grupa, $a, b \in G$.

Paž platí:

- ① $|a| = 1 \Leftrightarrow a = e$

- ② $|a| = 2 \Leftrightarrow a = a^{-1}, a \neq e$

- ③ $|a^{-1}| = |a|$

- ④ $|ab| = |ba|$

- ⑤ $|a^{-1}ba| = |b|$

Důkaz:

①, ② jasné

③: $\langle a \rangle = \langle -a \rangle \rightarrow |a| = |-a|$

④ Necht' $|ab| = m \in \mathbb{N}$:

$$(ba)^m = a^{-1}a(ba)^m = a^{-1}ababab \dots ba = a^{-1}(ab)^ma = e$$

$$\rightarrow |ba| \leq m$$

Kdyby $|ba| < m$, tj.: $|ba| = m < m$:

$$(ab)^m = (ab)^m aa^{-1} = a(ba)^m a^{-1} = e \rightarrow |ab| = m < m, \text{ spor}$$

⑤ položíme $A := a^{-1}, B := ba \rightarrow |AB| = |BA| \rightarrow |a^{-1}ba| = |b|$

Definice: Cyklická grupa

Necht' G je grupa.

Řekneme, že G je cyklická, existuje-li $a \in G : \langle a \rangle = G$

Věta: Klasifikace cyklických grup

Necht' G je grupa, která je cyklická.

Paž nastane jedna z následujících možností:

- ① $|G| = +\infty \wedge G \cong \mathbb{Z}$

- ② $|G| = m \in \mathbb{N} \wedge G \cong \mathbb{Z}_m$

Důkaz:

Stačí aplikovat předpoklad cyklické grupy na již doložené Twoseň.

Trvzení:

Každá podgrupa cyklické grupy je cyklická.

Důkaz:

Bud' G cyklická grupa, $H \subset G$ podgrupa.

Nechť $G = \langle a \rangle$:

Dokážeme, že $\exists m \in \mathbb{N} : \langle a^m \rangle = H$

• $\exists b \in H : b = a^m$, určíme $m \in \mathbb{N}$ minimální takové:

• $\langle a^m \rangle \subset H$ ✓

• $\langle a^m \rangle \supset H$:

Bud' $h \in H$ libovolně:

$$\rightarrow \exists n \in \mathbb{N} : h = a^n \rightarrow h = a^{k \cdot m + r} = \underbrace{(a^m)^k}_{\in H} a^r$$

Albo $a^r \in H$, kde $r = 0$, neboť $r \in \{0, 1, \dots, m-1\}$, jindy bychom měli spor s minimalitou m .

Definice: Největší společný dělitel

Bud' $a, b \in \mathbb{Z}$.

Největším společným dělitelem a, b nazýváme libovolné číslo $d \in \mathbb{Z}$ takové, že:

① $d \mid a, d \mid b$
② $\forall d' \in \mathbb{Z} : d' \mid a, d' \mid b \Rightarrow d' \mid d$

Poznámka:

• Největší společný dělitel značíme $\text{nsd}(a, b)$

• Největší společný dělitel není určen jednoznačně:

$$d_1, d_2 : d_1 \mid d_2, d_2 \mid d_1 \rightarrow d_1 = k d_2, d_2 = l d_1 \rightarrow d_1 = k l d_1 \rightarrow k = l = \pm 1$$

Příklad:

Všechny podgrupy $\mathbb{Z}$ jsou tvaru $m\mathbb{Z}$, $m \in \mathbb{N}$

$$m\mathbb{Z} = \{mk \mid k \in \mathbb{Z}\} = \langle m \rangle$$

$$\langle m, n \rangle = \{mx + ny \mid x, y \in \mathbb{Z}\} = \langle \text{nsd}(m, n) \rangle$$

Věta: Bézoutova lemma

Nechť $a, b \in \mathbb{Z}$.

Paž: ① Existuje $\text{nsd}(a, b)$

② Existují $x, y \in \mathbb{Z} : ax + by = \text{nsd}(a, b)$

Důkaz:

Definujeme $M := \{ax + by \mid x, y \in \mathbb{Z}\}$

Nechť $t = ax + by \in M$, pak $-t = a(-x) + b(-y) \in M$

položme $M^+ := \{t \in M \mid t \geq 0\} \subset \mathbb{N}_0$

$\rightarrow \mathbb{N}_0$ je dobře uspořádaná množina $\rightarrow M^+$ obsahuje nejmenší prvek

Označme $d := \min M^+$

Ověříme, že $d = \text{nsd}(a, b)$:

• $d \mid a$ a $d \mid b$:

Nechť $d \nmid a$: $a = k \cdot d + r \rightarrow r = a - k(ax_0 + by_0) = a(1 - kx_0) + b(-ky_0)$
spor s minimalitou d

$\rightarrow d \mid a$ a $d \mid b$

• $\forall d' \in \mathbb{Z} : d' \mid a$ a $d' \mid b \rightarrow d' \mid d$:

Bud' $d' \in \mathbb{Z}$ libovolně zvolíme:

$d' \mid a$ a $d' \mid b \rightarrow d' \mid t, \forall t \in M^+ \rightarrow d' \mid d$

$\rightarrow d = \text{nsd}(a, b) = ax_0 + by_0$

Twreň:

Necht G je cyklická grupa, $\langle a \rangle = G$.

Platí: ① Je-li $|G| = +\infty$, pak jediné generátory G jsou a, a^{-1}
② Je-li $|G| = m \in \mathbb{N}$, pak a^k je generátor $\Leftrightarrow k \perp m$

Důkaz:

① Necht $|G| = +\infty$:

Necht $G = \langle a^m \rangle$ pro nějaké $m \in \mathbb{N}$

$\rightarrow$ pak existuje $k \in \mathbb{Z}$: $a = (a^m)^k \rightarrow e = a^{mk-1} \rightarrow \begin{cases} m=k=\pm 1 \\ |G| \leq mk-1, \text{ spor} \end{cases}$

② Necht $|G| = m \in \mathbb{N}$:

$\Rightarrow$ necht a^k je generátor:

$\rightarrow \exists m \in \mathbb{N}$: $a^{mk} = a \rightarrow mk \equiv 1 \pmod{m} \rightarrow km - ln = 1 \rightarrow k \perp m$

$\Leftarrow$ necht $k \perp m$:

Bezout $\rightarrow \exists x, y \in \mathbb{Z}$: $kx + ym = 1$: $(a^k)^x = (a^k)^x (a^m)^y = a^{kx+my} = a$

Příklad:

$(\mathbb{Z}_7, \cdot)$

$(\mathbb{Z}_m, +)$

Poznámka:

• V cyklické grupě řádu n je prvek b generátorem $\Leftrightarrow |b| = n$

• Cyklická grupa je abelovská

Definice: Direktní součin grup

Necht G_1, G_2 jsou grupy.

Direktním součinem grup G_1, G_2 nazýváme $(G_1 \times G_2, *)$,

kde: $\forall (a_1, a_2), (b_1, b_2) \in G_1 \times G_2$: $(a_1, a_2) * (b_1, b_2) := (a_1 b_1, a_2 b_2)$

Poznámka:

Direktní součin grup je grupa: $e = (e_1, e_2)$, $(x, y)^{-1} = (x^{-1}, y^{-1})$

Poznámka:

• Značení:

Necht' $M, N \subset G$ podgrupy: $M \cdot N := \{xy \mid x \in M, y \in N\}$

$M = \{a\}$, přejme $a \in N$

Věta:

Necht' G je grupa, G_1, G_2 její podgrupy takové, že:

① $\forall u \in G_1: \forall r \in G_2: ur = ru$

② $G_1 \cap G_2 = \{e\}$

③ $G_1 \cdot G_2 = G$

Pak platí: $G \cong G_1 \times G_2$

Důkaz:

Z ③ plyne: $\forall g \in G: \exists u \in G_1: \exists r \in G_2: g = ur$

a tento rozklad je jednoznačný:

Necht' $ur = g = ab$, $a \in G_1, b \in G_2: ur = ab \rightarrow \underbrace{a^{-1}u}_{\in G_1} = \underbrace{br^{-1}}_{\in G_2}$

②
 $\rightarrow a^{-1}u = e, br^{-1} = e \rightarrow a = u, b = r$

Definujme zobrazení $\varphi: G_1 \times G_2 \rightarrow G: (u, r) \mapsto ur$

$\rightarrow$ již víme, že φ je bijekce

• φ homomorfismus:

①
 $\varphi((u, r) \cdot (a, b)) = \varphi(ua, rb) = \overbrace{ua}^{\text{②}} rb = urab = \varphi(u, r) \cdot \varphi(a, b)$

Věta: Čínská věta o zbytcích

Nechť $m_1, \dots, m_k \in \mathbb{N}$ jsou k dvojitě nesoudělná čísla,
Označme $M := m_1 \cdot \dots \cdot m_k$

Potom platí: $\mathbb{Z}_M \cong \mathbb{Z}_{m_1} \times \dots \times \mathbb{Z}_{m_k}$

Důkaz:

Definujme $\varphi: \mathbb{Z}_M \rightarrow \mathbb{Z}_{m_1} \times \dots \times \mathbb{Z}_{m_k}: \varphi(x) := (x \bmod m_1, \dots, x \bmod m_k)$

• φ homomorfismus:

$$(\varphi(x+y))_i = (x+y) \bmod m_i = x \bmod m_i + y \bmod m_i = (\varphi(x) + \varphi(y))_i$$

• φ prostě:

Nechť $x \in \text{Ker } \varphi$ libovolně:

$$\begin{aligned} \varphi(x) = e = (0, \dots, 0) &\rightarrow x \bmod m_i = 0, \forall i \in \{1, \dots, k\} \rightarrow x = \text{mnm}(m_1, \dots, m_k) \cdot l, l \in \mathbb{Z} \\ &\rightarrow x = Ml, l \in \mathbb{Z} \rightarrow x = 0 \rightarrow \text{Ker } \varphi = \{0\} \end{aligned}$$

• φ surjektivní:

Bud' $(u_1, \dots, u_k) \in \mathbb{Z}_{m_1} \times \dots \times \mathbb{Z}_{m_k}$ libovolně, pak

Paž $x \in \mathbb{Z}_M$ zvolíme: $x := \frac{M}{m_1} x_1 u_1 + \dots + \frac{M}{m_k} x_k u_k$,

kde $x_i: \frac{M}{m_i} x_i + m_i y = 1$ je řešení rovnice

Definice: Volná abelovská grupa

Nechť G je grupa.

Řekneme, že G je volná abelovská grupa, pokud $\exists m \in \mathbb{N}: G \cong \mathbb{Z}^m$

Definice: Torsní grupa $Tor G$

Nechť G je grupa.

Paž množinu $G_{TOR} := \{a \in G \mid |a| < \infty\}$ nazýváme torsní grupu G .

Říkáme, že G je torsní grupa, pokud $G = G_{TOR}$.

Lemma:

Necht' G je grupa, $a, b \in G$, $|a|, |b| < \infty$.

Paž plat' $|ab| \mid |a||b|$.

Důkaz:

Označme: $|a| = m \in \mathbb{N}$: $(ab)^{m \cdot m} = (a^m)^m (b^m)^m = e \rightarrow |ab| \leq m \cdot m$
 $|b| = n \in \mathbb{N}$

Označme nyní $|ab| = r \in \mathbb{N}$:

$$(ab)^{m \cdot n} = (ab)^{kr+s} = \underbrace{((ab)^r)^k}_{e} \cdot (ab)^s = (ab)^s = e \rightarrow s=0$$

$$\rightarrow |ab| \mid |a||b|$$

Tvrzení:

G_{TOR} je podgrupa G

Důkaz:

$$1|e|=1 \rightarrow e \in G_{\text{TOR}} \rightarrow G_{\text{TOR}} \neq \emptyset$$

Bud' $a, b \in G_{\text{TOR}}$ libovolně:

$$a^{-1}b \in G_{\text{TOR}} \Leftrightarrow |a^{-1}b| < \infty$$

$$\text{z lemmau plyne: } |a^{-1}b| \mid |a^{-1}||b| \rightarrow |a^{-1}b| \mid |a||b| \rightarrow |a^{-1}b| < \infty$$

Plat':

- G je ~~abelovská~~ $\Leftrightarrow$ ① G je bez torze $\Leftrightarrow G$ je volná abelovská
- ② Každá konečně generovaná abelovská grupa je $G \cong H \times G_{\text{TOR}}$

Definice: Lera' a prava translace

Necht G je grupa, $a \in G$.

~~Přechodem~~ Pak zobrazem' $L_a: G \rightarrow G: x \mapsto ax$, resp. $R_a: G \rightarrow G: x \mapsto xa$ nazýváme levou resp. pravou translace' grupy G .

Definice: Opačná grupa

Necht G je grupa s grupovým násobením $*$.

Opačnou grupou nazýváme grupu G^{op} s operací $\tilde{*}$ definovanou následovně: $\forall a, b \in G^{op}: a \tilde{*} b := b * a$

Trvzení:

- ① L_a, R_a jsou bijekce
- ② Zobrazem' $f: G \rightarrow S(G): a \mapsto L_a, \tilde{f}: G \rightarrow S(G)^{op}: a \mapsto R_a$ jsou monomorfismy

Důkaz:

① Vlastnost: L_a, R_a :

- $L_e = R_e = 1_G$
- $\forall a, b \in G: L_a \circ L_b = L_{ab}: \forall x \in G: L_a L_b x = L_a(L_b x) = abx = L_{ab} x$
 $R_a \circ R_b = R_{ba}: \forall x \in G: R_a R_b x = R_a(R_b x) = xba = R_{ba} x$
- $\forall a \in G: L_a^{-1} = (L_a)^{-1}: \forall x \in G: L_a^{-1} L_a x = a^{-1} a x = 1_G x = L_a L_a^{-1}$
 $R_a^{-1} = (R_a)^{-1}$
 $\rightarrow L_a, R_a$ bijekce

② $f: G \rightarrow S(G):$

$$f(ab) = L_{ab} = L_a \circ L_b = f(a) \circ f(b)$$

$\tilde{f}: G \rightarrow S(G)^{op}$

$$\tilde{f}(ab) = R_{ab} = R_b \circ R_a = R_a \circ R_b = \tilde{f}(a) \circ \tilde{f}(b)$$

$\text{Ker } f:$

Bud' $a \in \text{Ker } f$ libovolně:

$$L_a = 1_G: L_a x = x, \forall x \in G \xrightarrow{\text{volen}} a = e$$

$\text{Ker } \tilde{f}$

Bud' $a \in \text{Ker } \tilde{f}$ libovolně:

$$R_a = 1_G: R_a x = x, \forall x \in G \xrightarrow{\text{volen}} a = e$$

Definice: Relace $\sim_H, \sim_H$

Nechť G je grupa, $H \subseteq G$ její podgrupa, $a, b \in G$.

Řekneme, že a je v relaci $\sim_H$ s b ($a \sim_H b$) $\Leftrightarrow ab^{-1} \in H$

Řekneme, že a je v relaci $\sim_H$ s b ($a \sim_H b$) $\Leftrightarrow b^{-1}a \in H$

Poznámka:

$$a \sim_H b \Leftrightarrow ab^{-1} \in H \Leftrightarrow \exists h \in H : ab^{-1} = h \Leftrightarrow \exists h \in H : a = hb \Leftrightarrow a \in R_b H$$

$$a \sim_H b \Leftrightarrow b^{-1}a \in H \Leftrightarrow \exists h \in H : b^{-1}a = h \Leftrightarrow \exists h \in H : a = bh \Leftrightarrow a \in L_b H$$

Lemma:

$\sim_H, \sim_H$ jsou ekvivalence na G

Důkaz:

$\sim_H$: Reflexivita: $a \sim_H a : aa^{-1} \in H$

Symetrie: $a \sim_H b \Rightarrow b \sim_H a : ab^{-1} \in H \Rightarrow (ab^{-1})^{-1} \in H \Rightarrow ba^{-1} \in H$

Transitivita: $a \sim_H b \wedge b \sim_H c \Rightarrow a \sim_H c : ab^{-1}, bc^{-1} \in H \Rightarrow ab^{-1}bc^{-1} \in H \Rightarrow ac^{-1} \in H$

$\sim_H$: Analogicky

Poznámka:

Rozklad G na třídy ekvivalence podle H :

$$[a]_H = \{x \in G \mid a \sim_H x\} = \{x \in G \mid ax^{-1} \in H\} = Ha, \text{ Prave třídy rozkladu}$$

$${}_H[a] = \{x \in G \mid a \sim_H x\} = \{x \in G \mid x^{-1}a \in H\} = aH, \text{ Leve třídy rozkladu}$$

$$\forall a, b \in G : |[a]_H| = |[b]_H| = |H|$$

$$\text{dč: } |RaH| = |RbH| = |H|$$

$\uparrow$
 Ra je bijekce

Věta: Lagrange

Necht G je grupa, $H \subset G$ její podgrupa, $|G| < \infty$

Paž platí: $\frac{|G|}{|H|} = |G/H| = |H \backslash G|$

Důkaz:

$$G = \bigcup_{a \in G} [a] = \bigcup \{A \mid A \in G/H\}$$

$$\rightarrow |G| = |G/H| |H|$$

Důsledek:

① $\forall a \in G : |a| \mid |G|$

② $|G| = p \in \mathbb{P} \Rightarrow G$ nemá vlastní podgrupy $\Rightarrow G$ je cyklická

Poznámka:

$|G/H|$ nazýváme index podgrupy H v grupě G

Definice: Kongruence

Necht G je grupa, $\equiv$ ekvivalence na G .

Řekneme, že $\equiv$ je kongruence, pokud platí:

$$\forall a, b, c, d \in G : a \equiv b \Rightarrow ac \equiv bd$$

Tvrzení:

Necht G je grupa, $\equiv$ kongruence na G .

Paž $G/\equiv$ s grupovou operací G je grupa

Důkaz:

- Operace je dobře definována, neboť $\equiv$ je kongruence
- G/H je zřejmě uzavřena na grupovou operaci
- $[e] \equiv$ je neutrální prvek G/H
- $([a])^{-1} = [a^{-1}]$

Poznámka:

G je abelovská $\Rightarrow G/H$ je abelovská

Definice: Faktorová grupa (faktorgrupa)
 $G/\equiv$ se nazývá faktorgrupa grupy G

Definice: Norma'lní grupa

Nechť G je grupa, $H \subset G$ její podgrupa.

Řekneme, že H je norma'lní podgrupa G , pokud $\forall a \in G: aH = Ha$.
Značíme $H \triangleleft G$.

Věta: Kongruence a norma'lní podgrupy

Rozklad grupy G je rozkladem podle nějaké kongruence právě když rozkladem podle nějaké norma'lní podgrupy.

Důkaz:

$\Rightarrow$ Bud' $\equiv$ nějaká kongruence na grupě G :

Definujme $H := [e] \equiv$:

Ověříme, že H je norma'lní podgrupa G :

$$a \equiv b \Leftrightarrow a \sim_H b \Leftrightarrow ab^{-1} \in H \Leftrightarrow ab^{-1} = e \Leftrightarrow a \equiv b \Leftrightarrow b^{-1}a = e \Leftrightarrow a_H \sim b$$

$\rightarrow H \triangleleft G$

$\Leftarrow$ Nechť H je norma'lní podgrupa G :

Definujme $\equiv := \sim_H$:

Ověříme, že $\equiv$ je kongruence:

Bud' $a, b, c, d \in G$ libovolná taková, že:

$$\begin{matrix} a \sim_H b \\ c \sim_H d \end{matrix} \Leftrightarrow ab^{-1} \in H, cd^{-1} \in H:$$

$$ac \sim_H bd : \underbrace{acd^{-1}}_{\in H} \underbrace{b^{-1}}_{\in H} = \underbrace{ha}_{\in H} \underbrace{b^{-1}}_{\in H} \in H$$

Poznámka:

- V každé grupě jsou její nevlastní podgrupy norma'lní
- V Abelovské grupě jsou všechny podgrupy norma'lní

Definice: Vnitřní automorfismy

Nechť G je grupa, $a \in G$.

Pak zobrazení $\alpha_a: G \rightarrow G: x \mapsto axa^{-1}$ nazýváme vnitřním automorfismem grupy G .

Množinu všech vnitřních automorfismů značíme $\text{Inn}(G)$

Věta: Vnitřní automorfismy jsou automorfismy

Důkaz:

Bud' G grupa, $a \in G$:

• α_a homomorfismus:

$$\alpha_a(xy) = axya^{-1} = axa^{-1}aya^{-1} = \alpha_a(x)\alpha_a(y)$$

• α_a bijekce:

$$(\alpha_a)^{-1} = \alpha_{a^{-1}}: \forall x \in G: \alpha_{a^{-1}}\alpha_a(x) = \alpha_a\alpha_{a^{-1}}(x) = x = 1_G$$

Lemma:

Nechť G je grupa.

Pak zobrazení $\alpha: G \rightarrow \text{Aut}(G): a \mapsto \alpha_a$ je homomorfismus.

Důkaz:

Bud' $a, b \in G$ libovolně:

$$\alpha(ab) = \alpha_b \circ \alpha_a = \alpha(a) \circ \alpha(b)$$

$$\forall x \in G: \alpha_{ab}(x) = abxb^{-1}a^{-1} = (\alpha_a \circ \alpha_b)(x)$$

Věta:

Nechť G je grupa, $H \leq G$ je její podgrupa.
Pak H je normální podgrupa G právě tehdy když
 H je uzavřeno vůči všem vnitřním automorfismům.

Důkaz:

$\Rightarrow$ Necht' H je normální podgrupa G :

Bud' $a \in G$ libovolně:

$$\alpha_a(H) = aHa^{-1} = Ha a^{-1} = H$$

$\Leftarrow$ Necht' H je uzavřeno vůči všem vnitřním automorfismům:

$$\rightarrow \forall a \in G: aHa^{-1} = H \rightarrow aH = Ha \rightarrow H \trianglelefteq G$$

Platí:

$$\text{Inn}(G) \trianglelefteq \text{Aut}(G)$$

Důkaz:

Ověříme uzavřenost $\text{Inn}(G)$ vůči všem vnitřním automorfismům:

$$\gamma: \forall f \in \text{Aut}(G): \forall a \in G: f \circ \alpha_a \circ f^{-1} \in \text{Inn}(G):$$

$$\forall x \in G: (f \circ \alpha_a \circ f^{-1})(x) = f(a f^{-1}(x) a^{-1}) = f(a) x f(a)^{-1} \in \text{Inn}(G)$$

Důsledek:

$\text{Aut}(G)/\text{Inn}(G)$ je faktorgrupa

Věta:

Nechť G je grupa a $H \leq G$ její podgrupa.

Potom platí, že H je normální podgrupa G právě tehdy, když H je jádrem nějakého homomorfismu.

Důkaz:

$\Rightarrow$ Necht' H je normální podgrupa:

Položme $\varphi := \pi: G \rightarrow G/H: a \mapsto aH$

~~Ker $\varphi = H$~~

$$\text{Ker } \varphi = \{x \in G \mid \varphi(x) = e\} = \{x \in G \mid xH = H\} = H$$

$\Leftarrow$ Necht' $\varphi: G \rightarrow H$ je homomorfismus:

$\text{Ker } \varphi$ je normální podgrupa $G \Leftrightarrow \text{Ker } \varphi$ je uzavřená vůči $\text{Inn}(G)$

Bud' $a \in G$ libovolně; $x \in \text{Ker } \varphi$ libovolně:

$$\varphi(axa^{-1}) = \varphi(a)\varphi(x)\varphi(a)^{-1} = \varphi(a)e\varphi(a)^{-1} = e \rightarrow axa^{-1} \in \text{Ker } \varphi$$

Lemma:

Nechť G je grupa, $H \leq G$, $\varphi: G \rightarrow \tilde{G}$ homomorfismus takový, že $H \leq \text{Ker } \varphi$.

Paž zobrazí $\psi: G/H \rightarrow \tilde{G}: \tilde{\varphi}([a]) := \varphi(a)$ je dobře definovaný homomorfismus grup a platí:

- ① $\text{Im } \tilde{\varphi} = \text{Im } \varphi$
- ② $\text{Ker } \tilde{\varphi} = \text{Ker } \varphi / H$



Důkaz:

• Zobrazí ψ je dobře definováno:

1. Chceme: $[a] = [b] \Rightarrow \varphi(a) = \varphi(b)$

$h \in H \leq \text{Ker } \varphi$

$$[a] = [b] \Leftrightarrow \exists h \in H: b = ah \rightarrow \varphi(b) = \varphi(a)\varphi(h) = \varphi(a)$$

• $\tilde{\varphi}$ je homomorfismus:
 $\varphi([a][b]) = \tilde{\varphi}([ab]) = \varphi(a)\varphi(b) = \tilde{\varphi}([a])\tilde{\varphi}([b])$

• $\text{Im } \tilde{\varphi} = \text{Im } \varphi$:

$\text{Im } \tilde{\varphi} \subset \text{Im } \varphi$: $y \in \text{Im } \tilde{\varphi} \Leftrightarrow \exists [x] \in G/H: \tilde{\varphi}([x]) = \varphi(x) = y \in \text{Im } \varphi$
 $\text{Im } \varphi \subset \text{Im } \tilde{\varphi}$: $y \in \text{Im } \varphi \Leftrightarrow \exists x \in G: \varphi(x) = \tilde{\varphi}([x]) = y \in \text{Im } \tilde{\varphi}$

• $\text{Ker } \tilde{\varphi} = \text{Ker } \varphi/H$

$$\text{Ker } \varphi = \{a \in G \mid \varphi(a) = e_G\}$$

$$\rightarrow \text{Ker } \varphi/H = \{aH \mid \varphi(a) = e_G\}$$

||

$$\text{Ker } \tilde{\varphi} = \{aH \mid \tilde{\varphi}(aH) = \varphi(a) = e_G\}$$

Věta: 1. věta o izomorfismu

Nechť $G, \tilde{G}$ jsou grupy, $f: G \rightarrow \tilde{G}$ homomorfismus grup.

Pak platí: $G/\text{Ker } f \cong \text{Im } f$

Je-li f epimorfismus, pak $G/\text{Ker } f \cong \tilde{G}$

Důkaz:

Označme $H := \text{Ker } f$:

pak z předchozího lemmatu plyne, že: ① $\psi: G/\text{Ker } f \rightarrow \tilde{G}$ je homomorfismus
 ② ψ je bijekce $G/\text{Ker } f$ a $\psi(G/\text{Ker } f)$

• ψ je prostý: •

$$\text{Ker } \psi = \text{Ker } f/H = \{e\}$$

$$\rightarrow G/\text{Ker } f \cong \text{Im } \psi$$

Věta: 2 věta o izomorfismu

Nechť G je grupa, $N, H \subseteq G$ její podgrupy takové, že $N \triangleleft G$.

Potom platí: ① $N \cap H \triangleleft H$

$$② H / (N \cap H) \cong (NH) / N$$

Důkaz:

$$① NH = HN \rightarrow \forall a \in H \cap N : a(N \cap H) = (N \cap H)a$$

$$② NH = HN \rightarrow \forall a \in NH : aN = Na \rightarrow N \triangleleft HN$$

$$\pi : G \rightarrow G/N : \ker \pi = N$$

Označme $\tilde{\pi} := \pi|_H$:

$$\ker \tilde{\pi} = N \cap H \xrightarrow{\text{I. V. I.}} H / (N \cap H) \cong NH / N = \{aN \mid a \in NH\} = \{aN \mid a \in H\}$$

Věta: 3 věta o izomorfismu

Nechť G je grupa, $K \subseteq H \subseteq G$, $K, H \triangleleft G$.

Pak platí: ① $H/K \triangleleft G/K$

$$② (G/K) / (H/K) \cong G/H$$

Důkaz:

① $H/K \triangleleft G/K \Leftrightarrow H/K$ je uzavřena vůči všem vnitřním automorfismům:

Bud' $a \in \text{Inn}(G/K)$ libovolně, $b \in H$ libovolně!

$$\text{důkaz} \quad \text{da} (bK) = a b K a^{-1} \stackrel{H \triangleleft G}{=} \tilde{b} a K a^{-1} = \tilde{b} K \in H/K$$

② Definujme $f : G/K \rightarrow G/H : Ka \mapsto Ha$

Akce grupy na množině

Definice: Akce grupy na množině

Nechť G je grupa, M libovolná množina.

Řekneme, že zobrazení $\Phi: G \times M \rightarrow M$ je akce grupy G na M , pokud:

- ① $\forall m \in M, \forall g_1, g_2 \in G: \Phi(g_1, \Phi(g_2, m)) = \Phi(g_1 g_2, m)$
- ② $\forall m \in M: \Phi(e, m) = m$

Definice: Permy bod

Nechť $\Phi: G \times M \rightarrow M: (g, m) \mapsto g \cdot m$ je akce grupy G na M .

Řekneme, že prvek $m \in M$ je permy bodem vůči G , pokud $g \cdot m = m$

Definice: Stabilizátor

Nechť $\Phi: G \times M \rightarrow M: (g, m) \mapsto g \cdot m$ je akce grupy G na $M, m \in M$

Množina $G_m := \{g \in G / g \cdot m = m\}$ nazýváme stabilizátor prvku m v grupě G .

Definice: Orbita

Nechť $\Phi: G \times M \rightarrow M: (g, m) \mapsto g \cdot m$ je akce grupy G na $M, m \in M$.

Množina $O_m := \{g \cdot m / g \in G\}$ nazýváme Orbita prvku m při akci grupy G .

Platí:

G_m je podgrupa G .

Důkaz:

• $e \in G_m \rightarrow G_m \neq \emptyset$

• Bud' $a, b \in G_m$ libovolně:

$$a^{-1}b \cdot m = a^{-1}(b \cdot m) = a^{-1} \cdot m = a^{-1}(a \cdot m) = a^{-1}a \cdot m = m$$

Věta: Orbita a stabilizátor

Nechť $\Phi: G \times M \rightarrow M$ je akce grupy G na M , $m \in M$, $|G| < \infty$.

Potom platí: $|O_m| = \frac{|G|}{|G_m|}$

Důkaz:

• Označme: $\Phi(g, m) =: g \cdot m$

• G_m je podgrupa $G \rightarrow$ ^{Lagrange} $|G/G_m| = \frac{|G|}{|G_m|}$

• Najdeme bijekci $f: G/G_m \rightarrow O_m$:

Položme $f: G/G_m \rightarrow O_m: [g]_{G_m} \mapsto g \cdot m$:

• f dobře definováno:

Nechť $[g] = [\tilde{g}] \Leftrightarrow g \sim_m \tilde{g} \Leftrightarrow g\tilde{g}^{-1} \in G_m$

$\Rightarrow f([g]) = g \cdot m = g \cdot (g^{-1}\tilde{g}) \cdot m = \tilde{g} \cdot m = f([\tilde{g}])$

• f surjektivní:

Bud' $y \in O_m$ libovolné:

$\exists g \in G: y = g \cdot m \rightarrow [g] \in G/G_m \rightarrow f([g]) = y$

• f prostě:

Nechť $f([g]) = f([\tilde{g}])$:

$g \cdot m = \tilde{g} \cdot m \rightarrow g^{-1}\tilde{g} \cdot m = m \rightarrow g^{-1}\tilde{g} \in G_m \rightarrow \tilde{g} \sim_m g \rightarrow [y] = [\tilde{g}]$

Okruby

Definice: Okruh

Nechť R je množina, $+$, $\cdot$, dvě binární operace s neutro'livními prvky $0, 1 \in R$.
Řekneme, že R je okruh, pokud:

- ① $(R, +, -, 0)$ je abelovská grupa
- ② $(R, \cdot, 1)$ je monoid
- ③ Platí 'distributivní' zákony

Poznámka:

$\forall a, b, c \in R: a + c = b + c \Rightarrow a = b$ (Kra'cení v grupě)

$\forall a \in R: -(-a) = a$

$\forall a, b \in R: -(a+b) = -a + (-b)$

Platí:

Nechť R je okruh.

Paž platí: ① $\forall a \in R: a \cdot 0 = 0 \cdot a = 0$

② $\forall a, b \in R: -(a \cdot b) = (-a) \cdot b = a \cdot (-b)$

③ $\forall m \in \mathbb{Z}: m \times (a \cdot b) = (m \times a) \cdot b = a \cdot (m \times b)$

Důkaz:

① $a = a + 0$

$\xrightarrow{\text{kra'cení}} a \cdot 0 = 0$

$a = a \cdot 1 = a \cdot (1 + 0) = a + a \cdot 0$

② $ab + (-a)b = (a + (-a))b = 0 \cdot b = 0 \Rightarrow -(a \cdot b) = (-a) \cdot b$

③ $m=0: 0 = 0 \times a \cdot b = 0 \cdot b = (0 \times a) \cdot b = a \cdot 0 = a(0 \times b)$

$m > 0: m \times ab = (m-1) \times ab + ab = ((m-1) \times a + a) \cdot b = (m \times a) \cdot b$

$m \times ab = (m-1) \times ab + ab = a((m-1) \times b + b) = a \cdot (m \times b)$

Poznámka:

Nechť G je abelovská grupa (aditivní zápis):

$\text{End}(G) = \{f: G \rightarrow G \mid f \text{ homomorfismus},$

definujeme: $f+g: (f+g)(a) = f(a) + g(a)$

$f \cdot g: (f \cdot g)(a) = f(g(a))$

$0: 0(a) = e_G, \forall a \in G$

$1: 1 = 1_G$

Pak $R := \text{End}(G)$ je okruh

Obecně: R okruh $\Rightarrow R^* \text{ je okruh, } x \neq 0$

Příklad:

$(\mathbb{Z}, +, \cdot)$

$(\mathbb{Z}_n, +_{\text{mod } n}, \cdot_{\text{mod } n})$

$\mathbb{R}, \mathbb{Q}, \mathbb{C}$

Definice: Podokruh

Nechť R je okruh, $S \subseteq R$.

Řekneme, že S je podokruh R pokud:

① $S - S \subseteq S$

② $S \cdot S \subseteq S$

③ $1 \in S$

Poznámka:

• ②, ③ $\Leftrightarrow (S, \cdot)$ podmonoid $(R, \cdot)$

• ① $\Leftrightarrow (S, +)$ podgrupa $(R, +)$

• Podokruh okruhu je okruh

Okruch polynomů

Definice: Okruh polynomů

Nechť $\mathcal{R}$ je okruh, x formální proměnná.

Paž množinu $\mathcal{R}[x] := \left\{ \sum_{k=0}^n f_k x^k \mid n \in \mathbb{N}_0, f_k \in \mathcal{R} \right\}$ s operacemi $+$, $\cdot$:

$$\forall f, g \in \mathcal{R}[x], f = \sum_{k=0}^n f_k x^k, g = \sum_{k=0}^m g_k x^k:$$

$$f + g := \sum_{k=0}^{\max(n,m)} (f_k + g_k) x^k, \text{ necht' } \exists \in \mathbb{N}_0 \text{ } n \geq m$$

$$f \cdot g := \sum_{k=0}^{n+m} h_k x^k, h_k := \sum_{j=0}^k f_j g_{k-j}$$

nazveme okruh polynomů nad $\mathcal{R}$.

Definice: Okruh mocninových řad

Nechť $\mathcal{R}$ je okruh, x formální proměnná.

Paž $\mathcal{R}[[x]] := \left\{ \sum_{n=0}^{+\infty} f_n x^n \mid f_n \in \mathcal{R} \right\}$ společně s operacemi $+$, $\cdot$:

$$\forall f, g \in \mathcal{R}[[x]], f = \sum_{n=0}^{+\infty} f_n x^n, g = \sum_{n=0}^{+\infty} g_n x^n:$$

$$f + g := \sum_{n=0}^{+\infty} (f_n + g_n) x^n$$

$$f \cdot g := \sum_{n=0}^{+\infty} h_n x^n, h_n := \sum_{k=0}^n f_k g_{n-k}$$

nazveme okruh mocninových řad nad $\mathcal{R}$.

Poznámka:

$$\cdot x^0 = 1, x^{k+l} = x^k \cdot x^l$$

$$\cdot \mathcal{R} \subset \mathcal{R}[x] \subset \mathcal{R}[[x]] \text{ vzájemně' podokruhy}$$

Definice: Stupeň polynomu

Nechť $\mathcal{R}[x]$ je okruh polynomů nad $\mathcal{R}$, $f \in \mathcal{R}[x], f \neq 0$

Paž stupněm polynomu f rozumíme číslo $\deg f := \max \{ n \in \mathbb{N} \mid f_n \neq 0 \}$.

Speciálně pro $f = 0$ definujeme $\deg f := -1$

Poznámky:

Polynomy a mocninné řady ve více proměnných
Nechť R je okruh, $m \in \mathbb{N}$, $x_1, \dots, x_m$ formální proměnné

$$\alpha \in \mathbb{N}_0^m: \alpha = (\alpha_1, \dots, \alpha_m)$$

$$x := (x_1, \dots, x_m)$$

$$x^\alpha := x_1^{\alpha_1} \cdots x_m^{\alpha_m}$$

$$R[x_1, \dots, x_m] := \left\{ \sum_{\alpha \in \mathbb{N}_0^m} f_\alpha x^\alpha \mid f_\alpha \in R \right\}$$

$$f = \sum_{\alpha \in \mathbb{N}_0^m} f_\alpha x^\alpha, g = \sum_{\alpha \in \mathbb{N}_0^m} g_\alpha x^\alpha$$

$$f + g := \sum_{\alpha \in \mathbb{N}_0^m} (f_\alpha + g_\alpha) x^\alpha$$

$$f \cdot g := \sum_{\alpha \in \mathbb{N}_0^m} h_\alpha x^\alpha, h_\alpha = \sum_{\substack{\beta, \gamma \in \mathbb{N}_0^m \\ \beta + \gamma = \alpha}} f_\beta g_\gamma$$

Definice: Homomorfismus okruhů

Nechť $R, \tilde{R}$ jsou okruhy, $f: R \rightarrow \tilde{R}$.

Řekneme, že f je homomorfismus okruhů, pokud:

- ① $\forall x, y \in R: f(x+y) = f(x) + f(y)$
- ② $\forall x, y \in R: f(x \cdot y) = f(x) \cdot f(y)$
- ③ $f(1) = \tilde{1}$

Poznámka:

$f: R \rightarrow \tilde{R}$ je homomorfismus okruhů, právě když:

f je homomorfismus grup $(R, +)$, $(\tilde{R}, \tilde{+})$ ①
 f je homomorfismus monoidů $(R \setminus \{0\}, \cdot)$, $(\tilde{R} \setminus \{0\}, \tilde{\cdot})$ ②, ③

Tvrzení:

$$R[x_1, \dots, x_m] \simeq R[x_1, \dots, x_{m-1}][x_m]$$

Obory integrity

Definice: Dělitel nuly

Nechť R je okruh, $a \in R$, $a \neq 0$.

Řekneme, že a je dělitel nuly, pokud existuje $b \in R$: $a \cdot b = 0$, $b \neq 0$.

Definice: Obor integrity

Nechť R je nenulový okruh, který nemá žádné dělitele nuly.

Potom R nazveme oborem integrity.

Lemma:

Nechť R je obor integrity, $f, g \in R[x]$, $f, g \neq 0$.

Paž $\deg(fg) = \deg f + \deg g$.

Důkaz:

Označme $f := \sum_{k=0}^n f_k x^k$, $g := \sum_{k=0}^m g_k x^k$, $f_n, g_m \neq 0$

$$f \cdot g = \sum_{k=0}^{n+m} h_k x^k, \quad h_k = \sum_{i=0}^k f_i g_{k-i}$$

R obor integrity

$$h_{n+m} = \sum_{k=0}^{n+m} f_k g_{n+m-k} = f_n g_m \neq 0$$

Tvrzení:

Nechť R je obor integrity,

Paž $R[x]$, $R[[x]]$ jsou obory integrity.

Důkaz:

• $R[x]$:

Bud' $f, g \in R[x]$ libovolné nenulové polynomy:

$$\deg f \neq 0, \deg g \neq 0 \Rightarrow \deg(fg) \neq 0$$

• $R[[x]]$:

Bud' $f, g \in R[[x]]$ libovolné nenulové mocninné řady

Označme $\alpha := \min \{n \in \mathbb{N}_0 \mid f_n \neq 0\}$, $\beta := \min \{m \in \mathbb{N}_0 \mid g_m \neq 0\}$

$$f \cdot g = \sum_{k=0}^{+\infty} h_k x^k, \quad h_k = \sum_{i=0}^k f_i g_{k-i}$$

$$h_{\alpha+\beta} = \sum_{k=0}^{\alpha+\beta} f_k g_{\alpha+\beta-k} = \underbrace{f_\alpha g_\beta}_{\neq 0} + \sum_{\substack{k=0 \\ k \neq \alpha}}^{\alpha+\beta} f_k g_{\alpha+\beta-k} \neq 0$$

Tělesa

Definice: Těleso

Nechť R je okruh s nulou, je $(R \setminus \{0\}, \cdot)$ je grupa.
Pak R nazýváme tělesem.

Věta: Každé těleso je obor integrity

Důkaz:

stačí ukázat, že těleso T nemá dělitele nuly:

Bud' $a \in T$ libovolně, $a \neq 0$:

necht' $ab = 0$ pro nějaké $b \in T$:

$$ab = 0 \rightarrow b = 0$$

Poznámka:

nejmenší těleso: $\mathbb{Z}_2$

Věta: Podílové těleso

Každý obor integrity lze rozšířit na těleso.

Důkaz:

Bud' R libovolný obor integrity:

- Zavedeme ekvivalenci na $R \times R \setminus \{0\}$ ($\sim$):

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

- Faktorizace $R \times R \setminus \{0\} / \sim$:

$$R \times R \setminus \{0\} / \sim = \{[a, b] \mid a, b \in R, b \neq 0\}$$

Označme: $[a, b] =: \frac{a}{b}$, $\Theta(R) := \{\frac{a}{b} \mid a, b \in R, b \neq 0\}$

definujeme operace na $\Theta(R)$:

$$\forall \frac{a}{b}, \frac{c}{d} \in \Theta(R): \frac{a}{b} + \frac{c}{d} =: \frac{ad+bc}{bd}, \quad \frac{a}{b} \cdot \frac{c}{d} =: \frac{ac}{bd}$$

• operace jsou dobře definované:

$$\frac{a}{b} \sim \frac{\tilde{a}}{\tilde{b}}, \frac{c}{d} \sim \frac{\tilde{c}}{\tilde{d}} \Rightarrow a\tilde{b} = b\tilde{a} \wedge c\tilde{d} = d\tilde{c}$$

$$\frac{\tilde{a}}{\tilde{b}} \cdot \frac{\tilde{c}}{\tilde{d}} = \frac{\tilde{a}\tilde{c}}{\tilde{b}\tilde{d}} \rightarrow [\tilde{a}, \tilde{b}] [\tilde{c}, \tilde{d}] = [\tilde{ac}, \tilde{bd}] = [\tilde{a\tilde{c}}, \tilde{b\tilde{d}}]$$

$$\frac{ad+bc}{bd} \stackrel{?}{=} \frac{\tilde{a}\tilde{d}+\tilde{b}\tilde{c}}{\tilde{b}\tilde{d}}$$

$$(ad+bc)\tilde{b}\tilde{d} = (\tilde{a}\tilde{d}+\tilde{b}\tilde{c})bd \rightarrow ad\tilde{b}\tilde{d} + bc\tilde{b}\tilde{d} = \tilde{a}\tilde{d}bd + \tilde{b}\tilde{c}bd$$

Předpokládáme navíc komutativitu:

$$ab\tilde{d}\tilde{d} + cd\tilde{b}\tilde{b} = \tilde{a}b\tilde{d}\tilde{d} + d\tilde{c}\tilde{b}\tilde{b} \quad \checkmark$$

• + asociativní

$$0 := \frac{0}{1}$$

$$1 := \frac{1}{1}$$

• + komutativní

$$\text{• Opacit' pr'el: } \frac{a}{b} \mapsto \frac{-a}{b}$$

$$\text{• Inverze' pr'el: } \left(\frac{a}{b}\right)^{-1} = \frac{b}{a}$$

Definice: Podělové těleso

$\mathcal{Q}(\tilde{R})$ se nazývá podělové těleso ^{oboru} integrity

Lemma:

Nechť $R, \tilde{R}$ jsou obory integrity, takové že $R \simeq \tilde{R}$.

Pak $\mathcal{Q}(R) \simeq \mathcal{Q}(\tilde{R})$

Důkaz:

Bud' $\varphi: R \rightarrow \tilde{R}$ izomorfismus.

Položme $\psi: \mathcal{Q}(R) \rightarrow \mathcal{Q}(\tilde{R}): \frac{a}{b} \mapsto \frac{\varphi(a)}{\varphi(b)}$

Tvrzení:

Necht $R, \tilde{R}$ jsou okruhy, $R \cong \tilde{R}$.

Je-li R obor integrity (tělesa), pak $\tilde{R}$ je obor integrity (tělesa).

Důkaz:

Izomorfismus zachovává dělitele nuly

Definice: Podtělesa

Necht T je tělesa, $S \subset T$.

Řekneme, že S je podtělesa T , pokud: ① $(S, +)$ je podgrupa $(T, +)$
② $(S \setminus \{0\}, \cdot)$ je podgrupa $(T \setminus \{0\}, \cdot)$

Tvrzení:

- ① Průnik libovolného systému podokruhů okruhu R je podokruh R .
- ② Průnik libovolného systému podtělís tělesa T je podtělesa T .

Důkaz:

Tvrzení získaáme aplikací věty o průniku systémů grup

Definice: Okruhový obal

Necht R je okruh, $X \subset R$, $X \neq \emptyset$.

Minimální podokruh okruhu R obsahující X je jeho svou podmnožinou nazýváme okruhový obal X , značíme $\langle X \rangle$

Platí:

$$\begin{aligned} \langle X \rangle &= \bigcap \{ S \subset R \mid S \text{ podokruh } R, X \subset S \} = \\ &= \{ k_1 x_{n_1} \dots a_{m_1} + k_2 x_{n_2} \dots a_{m_2} + \dots + k_m x_{n_m} \dots a_{m_m} \mid m \in \mathbb{N}, n_1, \dots, n_m \in \mathbb{N}, k_i \in \mathbb{Z}, a_j \in X \} \end{aligned}$$

Důkaz:

Stejně jako pro grupový obal

Definice: Direktní součin okruhů

Nechť $R, \tilde{R}$ jsou okruhy.

Paž direktním součinem grup rozumíme množinu $R \times \tilde{R}$ společně s operacemi $+, \cdot$:

$$\forall (a, \tilde{a}), (b, \tilde{b}) \in R \times \tilde{R}: \textcircled{1} (a, \tilde{a}) + (b, \tilde{b}) := (a+b, \tilde{a}+\tilde{b})$$

$$\textcircled{2} (a, \tilde{a}) \cdot (b, \tilde{b}) := (ab, \tilde{a}\tilde{b})$$

Platí:

Direktní součin okruhů je okruh

Důkaz:

Zřejmý

Poznámka:

Jsou-li $R, \tilde{R}$ obory integrity, paž $R \times \tilde{R}$ neu' obor integrity:
 $(0,0) = (a,0) \cdot (0,b)$

Ideally

Definice: Ideal

Necht R je okruh, $I \subset R$.

Rekne me, že I je ideal, pokud:

- ① I je aditivní podgrupa R
- ② $\forall r \in R: \forall a \in I: ar, ra \in I$

Poznámky:

- $I \subset R$ je ideal $\Leftrightarrow I + I \subset I, RI \subset I, IR \subset I$
- ideal obecně není podokruh, nemusí obsahovat 1
 $1 \in I \Rightarrow I = R$
- Každý okruh má své netriviální idealy $I = R, I = \{0\}$

Věta: Faktorizace podle ideálu

Necht R je okruh, I ideal $\subset R$

Potom lze jedním způsobem na R/I zavést $+, \cdot$ tak, aby R/I byl okruh a $\pi: R \rightarrow R/I$ byl okruhový homomorfismus.

Důkaz:

• I je ideal $\Rightarrow I \triangleleft R$ jako aditivní podgrupa:

$\rightarrow R/I$ s sčítáním: $(a+I) + (b+I) = (a+b)+I$ je grupa

$\rightarrow \pi: R \rightarrow R/I: a \mapsto a+I$ je homomorfismus

Operace $\cdot$: položíme pro $a, b \in R: (a+I) \cdot (b+I) := (ab)+I$

$\rightarrow$ dobře definovaná:

Necht $a \sim \tilde{a}, b \sim \tilde{b} \Leftrightarrow a+I = \tilde{a}+I, b+I = \tilde{b}+I$

$ab \stackrel{?}{\sim} \tilde{a}\tilde{b}$:

$$ab - \tilde{a}\tilde{b} = ab - \tilde{a}b + \tilde{a}b - \tilde{a}\tilde{b} = \underbrace{(a - \tilde{a})b}_{\in I} + \underbrace{\tilde{a}(b - \tilde{b})}_{\in I} \in I$$

Projekce $\pi: \pi(ab) \stackrel{?}{=} \pi(a)\pi(b): ab + I = (a+I)(b+I)$

Důsledek:

Nechť R je okruh, $I \subset R$ podgrupa.

Pak I je ideál právě tehdy když I je jádrem okruhového homomorfismu.

Důkaz:

$\Rightarrow$ hledaný homomorfismus je projekce $\pi: R \rightarrow R/I$

$\Leftarrow$ nechť $f: R \rightarrow \tilde{R}$ je okruhový homomorfismus:

f je grupový homomorfismus $\Rightarrow \ker f = f^{-1}(\{0\})$ je podgrupa R

• bylo by ověřit, že: $\forall x \in R, \forall a \in \ker f: xa, ax \in \ker f$,

Buďte $x \in R, a \in \ker f$ libovolně:

$$f(xa) = f(x)f(a) = f(x) \cdot 0 = 0 = 0 \cdot f(x) = f(a)f(x) = f(ax)$$

$\Rightarrow xa, ax \in \ker f$

Věta: 1. věta o izomorfismu

Nechť $f: R \rightarrow \tilde{R}$ je homomorfismus okruhů.

Potom $R/\ker f \cong \operatorname{Im} f$.

Důkaz:

Definujme izomorfismus $\varphi: R/\ker f \rightarrow \operatorname{Im} f: (a + \ker f) \mapsto f(a)$:

• φ dobře definované:

nechť $a \sim b \Leftrightarrow a - b \in \ker f \Rightarrow a = b + h$

$$a - b = h \in \ker f \Rightarrow a = b + h \Rightarrow f(a) = f(b + h) = f(b) + f(h) = f(b)$$

• φ ~~homomorfismus~~ ^{grupa} 1. věta o izomorfismu pro grupy

• φ homomorfismus okruhů:

$$\varphi((a+I)(b+I)) = \varphi(ab+I) = f(ab) = f(a)f(b) = \varphi(a+I) \cdot \varphi(b+I)$$

Věta: 2. věta o izomorfismu

Necht R je okruh, $I \subset J \subset R$ ideally v R .

Potom platí: ① I je podgrupa J

② J/I je ideál v R/I

$$\textcircled{3} R/I / J/I \cong R/J$$

Věta: 3. věta o izomorfismu

Necht R je okruh, I ideál v R , J podokruh R .

Potom platí: ① $I \cap J$ je ideál v J

② $I+J$ je podokruh R , I je ideál v $I+J$

$$\textcircled{3} (I+J)/I \cong J/(I \cap J)$$

Důkaz:

Analogicky jako u grup

Věta: Zobecněná čínská věta o zbytcích

Necht R je okruh, $I_1, \dots, I_m$ ideally v R takové, že:

① $\forall j, k \in \hat{m}, j \neq k: I_j + I_k = R$

② Označme $I = \bigcap_{k=1}^m I_k$

Potom platí: $R/I \cong R/I_1 \times \dots \times R/I_m$

Lemma:

Necht R je okruh, $I_1, \dots, I_m, K$ ideally v R , takové, že $I_j + K = R$.

Pak platí: $J + K = R$, kde $J = \bigcap_{k=1}^m I_k$

Důkaz:

$I_k + K = R \rightarrow \exists a_k \in I_k, b_k \in K: a_k + b_k = 1$

Chci: $\exists a \in I, b \in K: a + b = 1$

víme, že $I+K$ je ideál $\rightarrow 1 \in I+K \Leftrightarrow I+K = R$:

$$1 = (a_1 + b_1) \dots (a_m + b_m) = \underbrace{a_1 \dots a_m}_{\in I} + \underbrace{(b_1 a_2 \dots a_m + \dots + b_1 \dots b_m)}_{\in K}$$

Důkaz věty a zbytků:

Pomocí 1. věty o izomorfismu:

J.: Chceme: $\varphi: R \rightarrow R/I_1 \times \dots \times R/I_n$ epimorfismus, $\ker \varphi = I$

Položme $\varphi(x) := (\pi_1(x), \dots, \pi_n(x)) \quad \forall x \in R$,

kde $\pi_k: R \rightarrow R/I_k: a \mapsto a + I_k$ je k -ta projekce

• φ homomorfismus:

$$\begin{aligned}\varphi(x+y) &= (\pi_1(x+y), \dots, \pi_n(x+y)) = (\pi_1(x) + \pi_1(y), \dots, \pi_n(x) + \pi_n(y)) = \\ &= (\pi_1(x), \dots, \pi_n(x)) + (\pi_1(y), \dots, \pi_n(y)) = \varphi(x) + \varphi(y)\end{aligned}$$

• $\ker \varphi = I$:

$$\begin{aligned}x \in \ker \varphi &\Leftrightarrow \varphi(x) = 0 \Leftrightarrow \pi_k(x) = 0, \forall k \in \hat{n} \Leftrightarrow x \in \underbrace{\ker \pi_k}_{I_k}, \forall k \in \hat{n} \Leftrightarrow \\ &\Leftrightarrow x \in \bigcap_{k=1}^n I_k = I\end{aligned}$$

• φ epimorfismus:

Bud' $y \in R/I_1 \times \dots \times R/I_n$ libovolné!

Chceme $x \in R: \varphi(x) = y = (\pi_1(u_1), \dots, \pi_n(u_n))$ (π_k epimorfismus)

definujeme $x := a_1 u_1 + \dots + a_n u_n$ tak, že: $\pi_k(a_k) = 1 \wedge \pi_k(a_\ell) = 0, \forall \ell \neq k$

Pro Bud' $k \in \hat{n}$ libovolné!

$$J_k := \bigcap_{\substack{i=1 \\ i \neq k}}^n I_i \xrightarrow{\text{Lemma}} J_k + I_k = R \rightarrow \exists a_k \in J_k, b_k \in I_k: a_k + b_k = 1$$

$$\rightarrow \pi_k(1) = 1 = \pi_k(a_k) \wedge \pi_\ell(a_k) = 0, \forall \ell \neq k$$

Tworemí:

Necht $f: R \rightarrow R$ je homomorfismus okruhů.

Je-li R komutativní těleso, pak $\ker f$ je nulový okruh nebo těleso.

Lemma:

① Těleso nemá vlastních ideálů.

② Komutativní okruh, který nemá vlastních ideálů, je těleso.

Důkaz:

① Bud' T těleso, $I \neq \{0\}$ jeho ideál:

necht $a \in I, a \neq 0$ je libovolný, přez $I: \underbrace{a^{-1}}_{\in T} \underbrace{a}_{\in I} = 1 \in I \rightarrow I = T$

② Bud' T komutativní okruh, který nemá vlastních ideálů, $a \in T$ libovolně, $a \neq 0$

$I := aT$ je ideál $\cap T: I = \{0\} \vee T = T$

$a \neq 0 \Rightarrow I = T \rightarrow \exists 1 \in I: \exists b \in T: ab = 1 \rightarrow b = a^{-1}$

Důkaz Tworemí:

$\ker f$ je ideál $\cap$ těleso $R \rightarrow \ker f = \{0\} \vee \ker f = T$

$\rightarrow T/\ker f = \{0\} \vee T/\ker f = T$

Definice: Maximální ideál

Necht R je okruh, $I \subset R$ ideál.

Řekneme, že I je maximální ideál, jestliže pro každý ideál $J \subset R$,
takový, že $I \subset J$ platí $I = J \vee J = R$.

Věta:

Necht R je nenulový komutativní okruh, $I \subset R$ ideál.

Pak R/I je těleso právě tehdy když I je maximální ideál.

Důkaz:

Poznámka:

Nechť $\varphi: \tilde{R} \rightarrow \tilde{R}$ je homomorfismus okružů, I ideál $\tilde{R}$ J ideál $\tilde{R}$.
Pak $\varphi(I)$ je ideál $\tilde{R}$ a $\varphi^{-1}(J)$ je ideál $\tilde{R}$.

Věta:

Díkat věty:

$\Rightarrow$ Nechť R/I je těleso

$\rightarrow R/I$ má jen nerostnou ideály

Bud' $J \subset R$ libovolný ideál takový, že $I \subset J$:

Pak J/I je ideál $R/I \rightarrow J/I = R/I \vee J/I = \{0\}$

2. věta o izomorfismu:

$$R/I/J/I = R/I/J/I = \{0\} \simeq R/J \rightarrow J = R$$

$$R/I/J/I = R/I/J/I = R/I \simeq R/J \rightarrow I = J$$

$\Leftarrow$ Nechť I je maximální ideál:

R/I je těleso $\Leftrightarrow R/I$ má jen nerostnou ideály

Bud' $J \subset R/I$ libovolný ideál:

Pak $\pi^{-1}(J)$ je ideál R a platí: $I \subset \pi^{-1}(J)$, neboli $I = \pi^{-1}(J)$

$$\rightarrow \pi^{-1}(J) = I \vee \pi^{-1}(J) = R$$

$$\rightarrow J = \{0_{R/I}\} \vee J = R/I \rightarrow R/I \text{ je těleso}$$

Trvzení:

Nechť R je komutativní okruh, $a_1, \dots, a_n \in R$

Pak nejmenší ideál obsahující $a_1, \dots, a_n$ je tvaru $I = a_1 R + \dots + a_n R$

Díkat:

$$\cdot a_i \in I$$

$$\cdot RI, IR \subset I$$

Definice: Hlavní ideál

Necht R je komutativní okruh, $a \in R$.

Ideály tvaru aR značíme (a) a nazýváme hlavní ideály.

Definice: Obor hlavních ideálů

Necht R je komutativní okruh ve kterém jsou všechny ideály hlavní.

Je-li R navíc obor integrity, pak jej nazýváme obor hlavních ideálů.

Věta:

Okruh polynomů nad komutativním tělesem je obor hlavních ideálů.

Důkaz:

• $T[x]$ je obor integrity, neboť T je obor integrity

• Bud' $I \subset T[x]$ libovolný ideál:

Označme $n := \min \{ \deg f \mid f \in I, f \neq 0 \}$

Bud' $f \in I$ libovolný polynom, že $\deg f = n$:

necht' $g \in I$ je libovolný polynom z I :

$$g = fh + r, \quad \deg r < n$$

$$\rightarrow r = g - fh \rightarrow r \in I \rightarrow r = 0$$

$g \in I, f \in I$

Poznámka:

Dělení polynomů:

Necht' T je komutativní těleso.

Pro $\forall f, g \in T[x] \exists q, r \in T[x] : f = qg + r, \deg r < \deg g$

Důkaz:

Existence: $f = \sum_{k=0}^n f_k x^k, g = \sum_{k=0}^m g_k x^k, n \geq m$

indukcí na n :

$$n=0: f = f_0 g_0^{-1} \cdot g_0 + 0$$

$n \rightarrow n+1$: položíme $\tilde{f} := f - (f_n g_{m-1}^{-1} x^{n-m})g \rightarrow \deg \tilde{f} < \deg f$

• buď $\tilde{f} = 0 \rightarrow f = (f_n g_{m-1}^{-1} x^{n-m})g$

• nebo $\tilde{f} \neq 0 \rightarrow \exists \text{ IP: } \exists \tilde{h}, \tilde{r}: \tilde{f} = \tilde{h}g + \tilde{r} \rightarrow f = (\tilde{h} + (f_n g_{m-1}^{-1} x^{n-m}))g + \tilde{r}$

Jednoznačnost:

$$f = q_1 g + r_1 = q_2 g + r_2 : q_1 = q_2 \rightarrow r_1 = r_2$$

$$q_1 \neq q_2 : \underbrace{(q_1 - q_2)}_{\deg > \deg g} g = \underbrace{r_2 - r_1}_{\deg < \deg g} \quad , \text{ spor.}$$

Definice: Irreducibilní polynom

Nechť T je těleso, $f' \in T[x]$.

Řekneme, že f' je irreducibilní nad T , jestliže platí:

$$f = gh \Rightarrow \deg g = 0 \vee \deg h = 0$$

Důsledek věty:

Nechť T je komutativní těleso, $(f) \subset T[x]$ ideál.

Paž (f) je maximální právě když f je irreducibilní!

Důkaz:

$$\Rightarrow \text{necht } f \text{ je reducibilní} \rightarrow f = gh \neq 0 < \deg g < \deg f$$

$$\rightarrow (f) \subsetneq (g) \rightarrow (f) = (g) \rightarrow \deg g = \deg f$$

$\Leftarrow$ necht f je irreducibilní:

$$f \in g T[x] \rightarrow \exists h \in T[x] : f = gh \rightarrow \deg g = 0 \vee \deg g = \deg f \rightarrow (g) = T[x] \vee (g) = (f)$$

Důsledek:

Nechť T je komutativní těleso, $f \in T[x]$.

Paž $T[x]/(f)$ je těleso právě tehdy když f je irreducibilní

Příklad:

$\mathbb{R}[x]/(x^2+1)\mathbb{R}[x]$ je těleso, x^2+1 je ireducibilní nad $\mathbb{R}$

$$\mathbb{R}[x]/(x^2+1)\mathbb{R}[x] = \{g + (x^2+1)\mathbb{R}[x] \mid g \in \mathbb{R}[x]\} = \{g + (x^2+1)\mathbb{R}[x] \mid g \in \mathbb{R}[x], \deg g < 2\}$$

$$\rightarrow \mathbb{R}[x]/(x^2+1) = \{a+bx \mid a, b \in \mathbb{R}\} \cong \mathbb{C}:$$

$$\begin{aligned}(a+bx)(c+dx) &= ac + x(bc+ad) + x^2 ad = \\ &= ac + x(bc+ad) + x^2 bd + bd - bd = \\ &= ac - bd + x(bc+ad)\end{aligned}$$

Kongruence nad polynomy:

$$g \sim h \Leftrightarrow g-h \in (f) \Leftrightarrow f \mid g-h : g \oplus h := g+h \bmod f$$
$$g \odot h := g \cdot h \bmod f$$

Definice: Dávkovací homomorfismus

Necht $\mathcal{R}$ je okruh, $a \in \mathcal{R}$.

$$\text{Pak zobrazení } \varphi_a: \mathbb{R}[x] \rightarrow \mathcal{R} : \sum_{k=0}^m f_k x^k \mapsto \sum_{k=0}^m f_k a^k =: f(a)$$

je naryba' dávkovací homomorfismus.

Poznámka:

$$\text{K } f \in \mathbb{R}[x] \text{ máme zobrazení } \tilde{f}: \mathcal{R} \rightarrow \mathcal{R} : a \mapsto \sum_{k=0}^m f_k a^k$$

Definice: Kořen polynomu

Necht $\mathcal{R}$ je okruh, $f \in \mathbb{R}[x]$, $a \in \mathcal{R}$.

Řekneme, že a je kořen polynomu f , k $\tilde{f}(a) = f(a) = 0$.

Platí:

Necht $\mathcal{R}$ je okruh, $f \in \mathbb{R}[x]$, $a \in \mathcal{R}$

Ponež a je kořen f právě když existuje $g \in \mathbb{R}[x]$, tak že $f = (x-a)g$.

Důkaz:

$$\Leftrightarrow f(a) = (a-a)g(a) = 0$$

$$\Rightarrow f = f - f(a) = \sum_{k=0}^m f_k (x^k - a^k) = \sum_{k=0}^m f_k (x-a) \sum_{i=0}^{k-1} x^i a^{k-1-i} = (x-a) \sum_{k=0}^m f_k \underbrace{\sum_{i=0}^{k-1} x^i a^{k-1-i}}_{a \in \mathcal{D} \mathbb{R}[x]}$$

Platí:

Nechť $a_1, \dots, a_n \in R$ jsou různé kořeny $f \in R[x]$, R okruh.

Pakud R je obor integrity, pak $f = (x-a_1) \dots (x-a_n)g$, po němž $g \in R[x]$.

Důkaz:

R obor integrity

$$\begin{aligned} f &= (x-a_1)g; \\ 0 &= f(a_2) = (a_2-a_1)\tilde{g}(a_2) \xrightarrow{\downarrow} \tilde{g}(a_2) = 0 \rightarrow \tilde{g} = (x-a_2)h \rightarrow \\ &\rightarrow f' = (x-a_1) \dots (x-a_n)g \end{aligned}$$

Důsledek:

Polynom stupně n má v oboru integrity nejvýše n kořenů.

Definice: k -násobný kořen

Nechť R je okruh, $a \in R$, $f \in R[x]$, $k \in \mathbb{N}$.

Řekneme, že f má k -násobný kořen a , jestliže: (počítá k -násobný kořen)
 $(x-a)^k \mid f$ ale $(x-a)^{k+1} \nmid f$

Definice: Derivace

Nechť R je okruh, $f = \sum_{k=0}^n f_k x^k \in R[x]$.

Derivací polynomu f rozumíme polynom $f' := \sum_{k=0}^n k \cdot f_k x^{k-1}$

Věta: Leibnitzovo pravidlo

Nechť R je okruh, $f, g \in R[x]$.

Pak platí: $(fg)' = f'g + fg'$

Důkaz:

stačí ukázat, že $(x^k x^l)' = (x^k)' x^l + x^k (x^l)'$:

$$(x^k x^l)' = (x^{k+l})' = (k+l)x^{k+l-1}$$

$$(x^k)' x^l + x^k (x^l)' = k \cdot x^{k-1} x^l + x^k \cdot l x^{l-1} = (k+l)x^{k+l-1}$$

Tvzení:

Nechť R je okruh, $a \in R$, $f \in R[x]$, $k \in \mathbb{N}$.

Pakud a je k -násobný kořen f , pak a je nejmenší $(k-1)$ -násobný kořen f' .

Důkaz:

$$f = (x-a)^k g \rightarrow f' = (x-a)^k g' + k(x-a)^{k-1} g = (x-a)^{k-1} [(x-a)g' + kg]$$

Poznámka:

J pro R obor integrality se můžeme stát, že a je k -násobný kořen f' .

$$f := (x-2)^6(x-1) \in \mathbb{Z}_3[x]$$

$$f' = \underbrace{6(x-2)^5(x-1)}_{0 \text{ v } \mathbb{Z}_3} + (x-2)^6 = (x-2)^6$$

Tvzení:

Nechť T je komutativní těleso.

Pak každý polynom $f \in T[x]$ lze rozložit na součin ireducibilních polynomů mod T .

Důkaz:

• f ireducibilní, hotovo

• f není ireducibilní: $\exists g, h \in T[x]$, $\deg g, \deg h < \deg f$: $f = gh$

↓ lze rozložit
bezobzvl.

Definice:

Nechť R je komutativní okruh, $S \subset R$ jeho podokruh, $a_1, \dots, a_n \in R$.

Pak nejmenší podokruh R obsahující S a $a_1, \dots, a_n$ značíme:

$$S[a_1, \dots, a_n] := \langle S \cup \{a_1, \dots, a_n\} \rangle$$

Platí:

$$S[a_1, \dots, a_n] = \{f(a_1, \dots, a_n) \mid f \in S[x_1, \dots, x_n]\}$$

Příklad:

$$\mathbb{R}[i] = \left\{ \sum_{k=0}^{\infty} f_k x^k \mid m \in \mathbb{N}_0, f_k \in \mathbb{R} \right\} = \{x + iy \mid x, y \in \mathbb{R}\}$$

$$\mathbb{Q}[\sqrt[3]{2}] = \{a + b\sqrt[3]{2} + c\sqrt[3]{4} \mid a, b, c \in \mathbb{Q}\}$$

$$\mathbb{Q}[\pi] = \left\{ \sum_{k=0}^{\infty} c_k \pi^k \mid c_k \in \mathbb{Q}, m \in \mathbb{N} \right\}$$

Definice:

Nechť T je komutativní těleso, $S \subset T$ jeho podtěleso, $a_1, \dots, a_n \in T$.

Paž zavedeme znočení $S(a_1, \dots, a_n)$:

$$S(a_1, \dots, a_n) := \bigcap \{F \mid F \text{ podtěleso } T, S \subset F, a_i \in F\}$$

nejmenší podtěleso T obsahující $S, a_1, \dots, a_n$

Poznámka:

K danému $a \in T$ a podtělesu S definujeme I_a :

$$I_a := \{f \in S[x] \mid f(a) = 0\}$$

Platí:

I_a je ideál

Důkaz:

I_a je jádro obrazovacího homomorfismu

Poznámka:

Z 1. věty a izomorfismu obalů: $S[x] / I_a \simeq S[a]$

Definice: Algebraický a transcendentní prvek

Nechť T je komutativní těleso, $S \subset T$ jeho podtěleso, $a \in T$.

Řekneme, že a je algebraický nad S , pokud $I_a \neq \{0\}$.

V opačném případě a nazýváme transcendentní nad S .

Tvrzení:

Necht T je komutativní těleso, $S \subset T$ jeho podtěleso, $a \in T$.
Pak a je algebraický nad S , právě když I_a je maximální ideál v $S[X]$.

Důkaz:

Víme, že S je obor hlavních děliteľů:

g: Chceme: $\exists g \in S[X]$ ireducibilní: $I_a = (g)$.

Bud' $g \in T[X]$ takový, že $I_a = (g)$.

Necht' $g = hk \rightarrow g(a) = 0 = h(a)k(a)$:

BUNO $h(a) = 0 \rightarrow h \in I_a : \exists P \in T[X] : h = gP$

$\rightarrow g = gkP \rightarrow \deg k = 0$

Poznámka:

Polynom g je daný jednoznačně až na násobení konstantou $\in S$.

Definice: Minimální polynom prvku (nad S)

Necht' T je komutativní těleso, $S \subset T$ podtěleso, $a \in T$ algebraický nad S .

Polynom g nazýváme minimálním polynomem prvku a , právě když:

$(g) = I_a$ a $\deg g$ je minimální možný a je normovaný a nejvyšší mocniny.

Věta:

Necht' T je komutativní těleso, $S \subset T$ jeho podtěleso, $a \in T$ algebraický nad S .

Pak $S[a] \cong S[X]/(f)$, kde f je minimální polynom prvku a .

Speciálně $S[a] = S(a)$ je těleso.

Důkaz:

Definujeme $\psi: S[X] \rightarrow S[a]$ obvyklým homomorfismem

z 1. věty o izomorfismu okruhu plyne:

$$S[x] / \ker \psi \simeq \operatorname{Im} \psi$$

$$\cdot \operatorname{Im} \psi = S[a]$$

$$\cdot \ker \psi = (f)$$

(f) je maximální $\rightarrow S[x]/(f)$ je těleso $\rightarrow S[a]$ je těleso

Nauč $S[a]$ je minimální těleso, které obsahuje S , $a \rightarrow S[a] = S(a)$

Definice: Rozšíření tělesa

Nechť T je podtěleso S .

Paž T nazýváme rozšířením tělesa S .

Dále zavedeme značení $\dim_S T =: [T:S]$.

Pomůcka:

Je-li T komutativní těleso, paž T je vektorový prostor nad S

Příklad:

$$[\mathbb{C}:\mathbb{R}] = 2$$

$$[\mathbb{R}:\mathbb{Q}] = +\infty$$

Definice: Stupeň rozšíření

Nechť T je komutativní těleso, $S \subset T$ jeho podtěleso.

Paž číslo $[T:S]$ nazýváme stupeň rozšíření tělesa S .

Tvrzení:

Necht $S(a)$ je rozšíření tělesa S .

Paž $[S(a):S] = \deg f$.

Kde f je minimální polynom pro a .

Důkaz:

$$\begin{aligned} S[x]/(f) &\cong \{g \in S[x] \mid \deg g < \deg f\} \cong \{g(a) \mid g \in S[x], \deg g < \underbrace{\deg f}_{=n}\} = \\ &= \{g_0 + g_1 a + \dots + g_{n-1} a^{n-1} \mid g_i \in S\} \end{aligned}$$

$1, a, \dots, a^{n-1} \in N \bmod S$:

Když $\mathbb{Z}$: paž $\exists g_0, \dots, g_{n-1} : \sum_{k=0}^{n-1} g_k a^k = 0 \rightarrow$ spor s minimalitou f

$\rightarrow \dim S(a) \bmod S = n$

Příklad:

$$\mathbb{Q}(\sqrt{2}) \cong \mathbb{Q}[x]/(x^2-2)$$

$$\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$$

Definice: Rozkladové těleso

Necht S je komutativní těleso, $f \in S[x]$

Rozkladovým tělesem polynomu f nazveme těleso T ,
rozšíření S takové, že:

- ① $f = c(x-a_1) \dots (x-a_r)$, $c, a_i \in T$
- ② $T = S(a_1, \dots, a_r)$

Příklad:

$$f = x^2 - 2 \in \mathbb{Q}[x] : \mathbb{Q}(\sqrt{2}) = T$$

Twresen!

Necht S je komutativní těleso, $f \in S[x]$ irreducibilní mod S .
Pak existuje T , rozšíření $S: T = S(a)$, a kořen f .

Důkaz:

• f irreducibilní: $S[x]/(f)$ je těleso

• Uvažujme projekci $\pi: S[x] \rightarrow S[x]/(f): h \mapsto h \bmod f$

Označme $a := \pi(x)$, $a \in T = S[x]/(f)$

$$f(a) = f(\pi(x)) = f([x]) = [f(x)] = 0$$

$$\pi(S) \subset S[x]/(f)$$

Poznámka:

Pro $T = S(a)$ $\tilde{T} = S(\tilde{a})$, $a, \tilde{a}$ kořeny $f: S(\tilde{a}) \cong S(a)$

$$C_0 + C_1 a + \dots + C_{n-1} a^{n-1} \mapsto C_0 + C_1 \tilde{a} + \dots + C_{n-1} \tilde{a}^{n-1}$$

Věta: O rozkladovém tělese

Necht S je komutativní těleso, $f \in S[x]$.

Pak existuje rozkladové těleso polynomu f , které je rozšířením S .

Důkaz:

indukcí na $n := \deg f$

$n = 0, n = 1: S =: T$

$n > 1: f$ rozložíme na irreducibilní polynomy nad $S: f = f_1 \dots f_m$

Na každý z irreducibilních polynomů f_i aplikujeme předchozí twresen:

$$f_i \rightarrow a_{i,1}^{(i)}, \dots, a_{i,n_i}^{(i)}$$

$$\rightarrow T := S(a_{1,1}^{(1)}, a_{1,n_1}^{(1)}, \dots, a_{m,1}^{(m)}, a_{m,n_m}^{(m)})$$

Necht' $B \cup \mathbb{N} \cap \mathbb{Q}$ je ireducibilní nad S :

$\exists a$: kořen f : $a \in S(a)$: $f = (x-a)g$, $g \in (S(a))[x]$

Kořeny g jsou kořeny f a navíc (kromě a)
 $\deg g < \deg f$

→ existuje rozkladové těleso $g : S(a)(b_1, \dots, b_{n-1}) = S(a, b_1, \dots, b_{n-1})$

→ $f = C(x-a)(x-b_1)\dots(x-b_{n-1})$

Definice: Charakteristika

Necht' R je okruh.

Pak charakteristikou okruhu R nazýváme $n \in \mathbb{N}$, minimální
takové, že : $n \cdot 1_R = 0$, značíme $\text{char } R := n$

Pokud takové n neexistuje, kládeme $\text{char } R := 0$.

Poznámka:

Alternativní definice:

- $\text{char } R$ je řád prvku 1 v aditivní grupě R .
- $\text{char } R = n \in \mathbb{N}$: $n\mathbb{Z} = \ker \varphi$, $\varphi : \mathbb{Z} \rightarrow R$ okružový homomorfismus

Definice: Prvokruh

Prvokruhem okruhu R rozumíme $\langle 1_R \rangle$.

Platí:

Prvokruh okruhu R je izomorfní $\mathbb{Z}$ nebo $\mathbb{Z}_n$, podle toho zda
 $\text{char } R = 0$ nebo $\text{char } R = n$.

Důkaz:

Uvažujeme homomorfismus $\varphi : \mathbb{Z} \rightarrow R : k \mapsto k \cdot 1_R$:

- $\ker \varphi = \{0\}$: $\mathbb{Z}/\{0\} \cong \mathbb{Z} = \text{Im } \varphi$
- $\ker \varphi = n\mathbb{Z}$: $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n = \text{Im } \varphi$

Trvzení:

Charakteristika každého oboru integrity je 0 nebo prvočíslo.

Důkaz:

Nechť R je obor integrity, $\text{Char } R \in \mathbb{N}$ jeho charakteristika:

Buďť $l, s \in \mathbb{N} : n = l \cdot s$ libovolná:

$$0 = n + 1 = \underbrace{(l+1)}_{\neq 0} \underbrace{(s+1)}_{\neq 0} \rightarrow \text{spo, že } R \text{ je obor integrity}$$

$\rightarrow$ Prvočíslo tělesa je $\mathbb{Z}$ nebo $\mathbb{Z}_p, p \in \mathbb{P}$

Definice: Prvotěleso

Nechť T je těleso.

Prvotěleso tělesa T je nejmenší podtěleso, tj.: průnik všech podtěl

Platí:

① Je-li $\text{Char } T = 0$, pak prvotěleso je izomorfní $\mathbb{Z}$ a prvotěleso je izomorfní podlomenému tělesu $\mathbb{Z}, \text{ tj.: } \mathbb{Q}$.

② Je-li $\text{Char } T = p \in \mathbb{P}$, pak prvotěleso je izomorfní $\mathbb{Z}_p$.

Trvzení:

Konečná tělesa mají charakteristiku $p \in \mathbb{P}$

Věta:

Každé konečné těleso je komutativní

Důkaz:

Těžké

Věta:

Konečné těleso o n prvcích existuje právě když
 $n = p^k$, $p \in \mathbb{P}$, $k \in \mathbb{N}$ a je právě jedno až na izomorfismus.

Turner:

Nechť T je těleso $|T| = m \in \mathbb{N}$,

Paž $m = p^k$, $p = \text{char } T$, $k \in \mathbb{N}$

Důkaz:

T je konečné: ~~$\mathbb{P}$~~ $\text{char } T = p \in \mathbb{P}$

→ Hmotěleso $\mathbb{Z}_p \rightarrow T$ je rozšíření $\mathbb{Z}_p \rightarrow T$ je vektorový prostor nad $\mathbb{Z}_p$

→ $[T : \mathbb{Z}_p] = k \in \mathbb{N}$

→ $T = \underbrace{\{a_1 e_1 + \dots + a_k e_k\}}_{\text{báze je } p^k} \mid a_i \in \mathbb{Z}_p$

Turner:

Rozkladové těleso polynomu $x^{p^k} - x$ má p^k prvků.

Důkaz:

Polynom $f := x^{p^k} - x$ má nejvýše p^k kořenů.

Buďte a, b libovolné dva kořeny f : $a^{p^k} - a = 0$
 $b^{p^k} - b = 0$

$$\therefore (ab)^{p^k} - ab = a^{p^k} b^{p^k} - ab = ab - ab = 0 \quad \checkmark$$

$$\therefore (a^{-1})^{p^k} = (a^{p^k})^{-1} = a^{-1} \quad \checkmark$$

Mala Fermatova věta:

$$+ : (a+b)^p = \sum_{k=0}^p \binom{p}{k} a^k b^{p-k} = a^p + b^p + \sum_{k=1}^{p-1} \binom{p}{k} a^k b^{p-k} = a^p + b^p$$

$$\binom{p}{k} = \frac{p(p-1)\dots(p-k+1)}{k!} \in \mathbb{Z} \xrightarrow{p \nmid k} p \mid \binom{p}{k}$$

indukce na k :

$$(a+b)^{p^k} = ((a+b)^{p^{k-1}})^p = (a^{p^{k-1}} + b^{p^{k-1}})^p = a^{p^k} + b^{p^k} = a + b$$

T je minimální min těleso obsahující všechny kořeny f' ,
přítom množina kořenů je těleso: $T = \{ \text{kořeny } f' \} \rightarrow |T| \leq p^k$

Kdyby f' měl násobný kořen a , pak f' má kořen a :

$$f' = x^{p^k} - x = 1 - 1 = 0 \text{ nemá kořen}$$

$$\rightarrow f' \text{ má právě } p^k \text{ kořenů} \rightarrow |T| = p^k$$

Trvzení:

Nechť T je těleso o p^k prvcích.

Pak T je rozkladové těleso polynomu $f' = x^{p^k} - x$

Důkaz:

Ukažeme, že každý prvek $a \in T$ je kořen polynomu f' :

$(T \setminus \{0\}, \cdot)$ je multiplikační grupa

$$\rightarrow |T \setminus \{0\}| = p^k - 1$$

Bud' $a \in T \setminus \{0\}$ libovolný prvek:

$$|a| \mid p^k - 1 \rightarrow a^{|a|} = 1 \rightarrow a^{p^k-1} = 1 \rightarrow a^{p^k} = a \rightarrow a \text{ je kořen } f'$$

Značení: $\mathbb{F}_{p^k}$, $GF(p^k)$ Galois Field

Pozor: $\mathbb{Z}_{p^k}$, $(\mathbb{Z})^k \neq \mathbb{F}_{p^k}$!

Věta:

Multiplikační grupa konečného tělesa je cyklická

Důstředek:

$$\exists a: \{a, a^2, \dots, a^{p^k-1} = 1\}, \mathbb{Z}_p(a) \cong T$$

a je kořen $x^{p^k} - x \in \mathbb{Z}_p[x]$, a je algebraické nad $\mathbb{Z}_p$
Proto $\mathbb{Z}_p(a) \cong \mathbb{Z}_p[x]/(f)$

kde f je minimální polynom přes a nad $\mathbb{Z}_p$:

$$\mathbb{Z}_p[x]/(f) \text{ je těleso velikosti } p^{\deg f} = p^k$$

$$\forall p \in \mathbb{P}: \forall k \in \mathbb{N}: \exists f \in \mathbb{Z}_p[x], \deg f = k \text{ ireducibilní mod } \mathbb{Z}_p.$$

Definice: Exponent grupy

Necht G je grupa, $m \in \mathbb{N}$.

Řekneme, že m je exponent grupy G , pokud: $\forall a \in G: a^m = 1$.
(Poukud existuje)

Lemmy:

Necht G je cyklická grupa, m exponent grupy.

Pak existuje $a \in G: |a|$ je exponent grupy G m .

Dělitelnost

Definice: Dělitel

Nechť R je obor integrity.

Řekneme, že $a \in R$ je dělitel $b \in R$, pokud $\exists c \in R : b = ac$.

Značíme $a|b$, ($b \in aR$)

Definice: Jednotka

Nechť R je obor integrity, $a \in R$.

Řekneme, že a je jednotka, pokud $a|1$

Množinu všech jednotek značíme $U(R)$

Definice: Asociované prvky

Nechť R je obor integrity, $a, b \in R$.

Řekneme, že prvky a, b jsou asociované, pokud $a|b \wedge b|a$,

Značíme $a \sim b$.

Platí:

Množina jednotek $U(R)$ je multiplikační grupou.

Důkaz:

$$1 \in U(R) \rightarrow U(R) \neq \emptyset$$

$$\text{Buďte } a, b \in U(R) \text{ libovolná: } a\tilde{a} = 1, b\tilde{b} = 1$$

$$\tilde{a}b \in U(R): \tilde{a}b(\tilde{b}a) = 1 \checkmark$$

Platí:

Nechť R je obor integrity, $a, b \in R$ l.s.o.?

Paž platí: $a \sim b \Leftrightarrow \exists u \in U(R): a = bu$

Důkaz:

$$\Rightarrow a|b \wedge b|a \rightarrow a = bc \wedge b = ad \rightarrow a = adc \rightarrow c, d \in U(R)$$

$$\Leftarrow a = bu \rightarrow b|a$$

$$u \in U(R) \rightarrow \exists r \in R: ur = 1 \rightarrow ar = bur = b \rightarrow a|b$$

Tvrzení

Relace $\sim$ je ekvivalence na R .

Důkaz:

Reflexivita: $a = 1 \cdot a = a \cdot 1$

Symetrie: $a \sim b \Rightarrow b \sim a$, viz předchozí tvrzení

Tranzitivita: $a \sim b, b \sim c \Rightarrow a \sim c \checkmark$

Příklad:

$$\mathbb{Z}[i] = \{a+bi \mid a, b \in \mathbb{Z}\}, U(\mathbb{Z}[i]) = \{\pm 1, \pm i\}$$

$$\mathbb{Z}[\sqrt{2}] = \{a+b\sqrt{2} \mid a, b \in \mathbb{Z}\}, U(\mathbb{Z}[\sqrt{2}]) = \{\pm (1+\sqrt{2})^n \mid n \in \mathbb{Z}\}$$

Definice: Irreducibilní prvek

Necht' R je obor integrity, $a \in R \setminus U(R)$, $a \neq 0$.

Řekneme, že a je irreducibilní, pokud platí:

$$\forall b, c \in R: a = bc \Rightarrow a \sim b \vee a \sim c$$

Příklad:

Irreducibilní ^{prvky} ~~polynomy~~ $\sim \mathbb{Z}$: prvočísla

$\mathbb{Z}[x]$: irreducibilní polynomy

Definice: Noetherovský obor integrity

Necht' R je obor integrity.

Řekneme, že R je noetherovský, pokud pro každou neklesající posloupnost ideálů $(I_k)_{k=1} \subset R$, tj.:

$I_1 \subset I_2 \subset \dots \subset I_k \subset I_{k+1} \subset \dots$ platí, že $\exists m \in \mathbb{N}$ tak že:

$$\forall k > m: I_k = I_m.$$

Twierdzenie:

Niech R jest noetherowskim pierścieniem całkowitości.

Wtedy dla $a \in R \setminus \{0\}$ istnieje iloczyn iloczynowy $a = b_1 \cdots b_r$, gdzie $b_1, \dots, b_r \in R$ są elementami niepodzielnymi.

Dokaz: (sketch)

Wskazujemy, że dla $a \in R \setminus \{0\}$ istnieje iloczyn iloczynowy.

• a jest elementem niepodzielnym: $r=1, b_1=a$,

• a jest elementem dzielnym:

$\exists b, c \in R \setminus \{0\} : a = bc$ i $b \nmid a$ i $c \nmid a$

$\rightarrow c \mid a$ i $b \mid a$ albo $a \nmid b$ i $a \nmid c$

Z konstruujemy ciąg $(a_k) : a_{k+1} \mid a_k$ i $a_k \nmid a_{k+1}$

$a_1 = a$, niech $b_1 \nmid a$ i $a_2 = b_1$

$a_2 = c_1$ i $a_3 = c_1$

$\vdots$

a_k

niech a_k będzie elementem niepodzielnym.

niech a_k jest elementem dzielnym $\rightarrow a_k = b_k c_k$ i $a_{k+1} = b_k$ i $a_{k+1} \nmid a_k$

$a_{k+1} \mid a_k$ i $a_k \nmid a_{k+1} \rightarrow a_k R \subsetneq a_{k+1} R$

$\rightarrow a_1 R \subset a_2 R \subset \dots \subset a_m R = a_{m+1} R = \dots$ (noetherowskość)

Przykład:

Rozkład na iloczyny.

$R = \{x \in \mathbb{C} \mid \exists f \in \mathbb{C}[x] : f(x) = 0\}$

$$2 = \sqrt{2} \cdot \sqrt{2} = (\sqrt{2})^2 = (\sqrt{2})^2$$

Definice: Gaussovsky' obor integrity

Necht' R je obor integrity.

Řekneme, že R je Gaussovsky', jestliže každý prvek $a \in R \setminus U(R)$, $a \neq 0$ lze rozložit na součin ireducibilních prvků jednoznačně až na asociovanost.

Definice: Prvočinnitel (Prvočíslo)

Necht' R je obor integrity, $a \in R \setminus U(R)$, $a \neq 0$.

Řekneme, že a je prvočíslo, jestliže:

$$\forall b, c \in R : a | bc \Rightarrow a | b \vee a | c$$

Platí:

Každé prvočíslo je ireducibilní.

Důkaz:

Necht' $p \in R$ je prvočíslo.

Buďte $b, c \in R$ taková, že $a = bc$:

$$\begin{aligned} a = bc &\rightarrow a | bc \xrightarrow{\text{B110}} a | b \rightarrow b = ad \\ &\rightarrow a = a \cdot d \cdot c \rightarrow dc = 1 \rightarrow c \in U(R) \rightarrow a \sim b \end{aligned}$$

Věta:

Necht' R je noetherovsky' obor integrity

Pak R je Gaussovsky' $\Leftrightarrow$ Každý ireducibilní prvek je prvočíslo

Tvzení:

Necht' R je obor hlavních ideálů.

Pak R je noetherovsky', dokonce gaussovsky'.

Oprava:

Thorem:

Necht R je noetherovský obor integrity, $a \in R \setminus U(R)$, $a \neq 0$.
Pak existují $b_1, \dots, b_m \in R$ ireducibilní: $a = b_1 \cdot b_2 \cdot \dots \cdot b_m$.

Důkaz

Sporem:

Necht $a \in R \setminus U(R)$, $a \neq 0$ je takové, že jej nelze rozložit
a není ireducibilní:

Pak $\exists b, c \in R \setminus U(R): a = bc$

a alespoň jedno, BÚNO b , je nerozložitelné

$\rightarrow b = ef \rightarrow e$ je nerozložitelné

!

$a_k = d \cdot b$, BÚNO d nerozložitelné: $d := a_{k+1}$

a platí: $a_k \nmid a_{k+1} \wedge a_{k+1} \nmid a_k$