ARITMETIKA = věda o číslech, čís. soustavách, operacích s čísly, ...

ALGEBRA = ~~počty s písm~~ disciplína zabývající se řešením rovnic a soustav — KLASICKÁ AL.

= algebra struktur (množin) a operací s nimi — MODERNÍ AL.

DEFINICE zavádí nový pojem, termín, symbol

Celá čísla, která jsou dělitelná dvěma, se nazývají sudá.

VĚTA přináší nový poznatek

- POPIS SITUACE
- PŘEDPOKLAD
- TVRZENÍ

Jestliže je $2^{p}-1$ prvočíslo, potom je p prvočíslo =>

Nechť V_1 a V_2 jsou podprostory prostoru V. Potom platí:

$\dim(V_1 \cap V_2) + \dim(V_1 + V_2) = \dim V_1 + \dim V_2$.

// LINEÁRNÍ ALGEBRA — definice a věty z hlediska jazyka

DŮKAZY

Důkaz věty, která má tvar implikace $(A \Rightarrow B)$ < přímý / sporem ($A=1$, $B=0$ => spor)

Důkazy indukcí

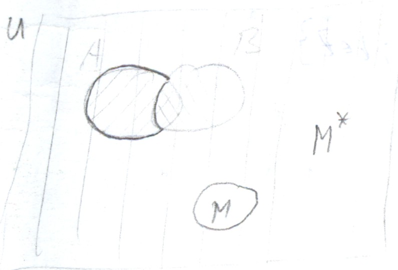
Důkazy existenční a konstruktivní

disjunktní množiny: $A \cap B = \emptyset$

DESCARTES

univerzum

JOHN VENN (1834–1923)



univerzum

M^* ... doplněk M

$\mathbb{P} = \{2,3,5,7,11,13,17,19,23,\dots\}$ ... prvočísla

M – množina

$M = \{a,b,c,d\}$

P(M) – potenční množina = množina všech podmnožin množiny M.

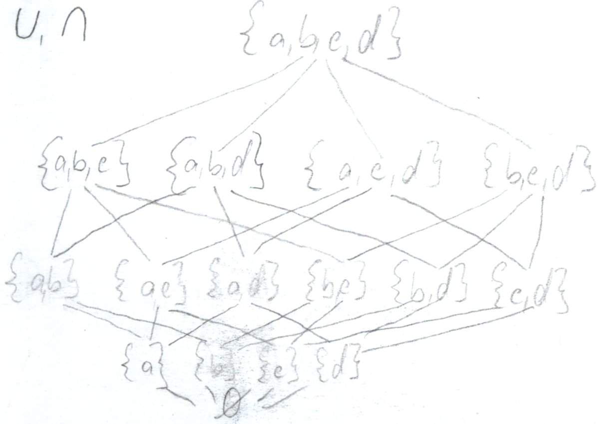
4 6

$P(M) = \{\{a\},\{b\},\{c\},\{d\},\{a,b\},\{a,c\},\{a,d\},\{b,c\},\{b,d\},\{c,d\},\{a,b,c\},\{a,b,d\},\{a,c,d\},\{b,c,d\},\{a,b,c,d\},\{\}\}$

4

svaz podmnožin

$\cup, \cap$



$1+4+6+4+1 = 2^4$

DÚ: $P(\{1,2,3,4,5\})$

M, $A, B, C \in M$

(i) $A \cup A = A$ $\quad A \cap A = A$

(ii) $A \cup B = B \cup A$ $\quad A \cap B = B \cap A$

(iii) $(A \cup B) \cup C = A \cup (B \cup C)$ $\quad (A \cap B) \cap C = A \cap (B \cap C)$

(iv) $(A \cup B) \cap A = A$ $\quad (A \cap B) \cup A = A$

} svaz

(v) $(A \cup B) \cap C = (A \cap C) \cup (B \cap C)$ $\quad (A \cap B) \cup C = (A \cup C) \cap (B \cup C)$

} distributivní svaz

(vi) $(A \cup B)^* = A^* \cap B^*$ $\quad (A \cap B)^* = A^* \cup B^*$

(vii) $(A^*)^* = A$

(viii) Existence největšího a nejmenšího prvku

} Booleovský svaz (algebra)

Disjunktní rozklad množiny

$M = \bigcup_{i=1}^{n} M_i$, $\quad M = \bigcup_{i=1}^{\infty} M_i$, $\quad M = \bigcup_{i \in A} M_i$ — libovolná množina A

množiny M_i jsou navzájem disjunktní.

$\{M_1, M_2, M_3, \dots, M_n\}$, $\quad \{M_i\}_{i=1}^{n}$, $\quad \{M_i\}_{i=1}^{\infty}$, $\quad \{M_i\}_{i \in A}$

Příklady: 1. Triviální rozklady množiny M:

$M = M$, $\quad M = \bigcup_{a \in M} \{a\}$

2. $\mathbb{Z} = \{\dots, -2, -1\} \cup \{0\} \cup \{1, 2, \dots\}$

3. $\mathbb{Z} = \{\dots -2; 0; 2, 4 \dots\} \cup \{\dots, -3, -1, 1, 3, \dots\} = \{2k;\ k \in \mathbb{Z}\} \cup \{2k+1;\ k \in \mathbb{Z}\}$

4. $\mathbb{Z}$, $n \in \mathbb{N}$

$\mathbb{Z} = \{k \cdot n;\ k \in \mathbb{Z}\} \cup \{kn+1;\ k \in \mathbb{Z}\} \cup \{kn+2;\ k \in \mathbb{Z}\} \cup \dots \cup \{kn+(n-1);\ k \in \mathbb{Z}\}$

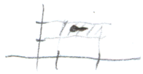
5. $\mathbb{R} = \mathbb{Q} \cup \mathbb{I}$ $\quad$ ($\mathbb{I}$ – množ. všech irac. č.)

6. $\mathbb{C} = \bigcup_{r \in \mathbb{R}_0^+} \{\alpha \in \mathbb{C};\ |\alpha| = r\}$ $\quad$ ($\mathbb{R}_0^+ = \{r \in \mathbb{R};\ r \geq 0\}$)

7. $\mathbb{C} = \bigcup \{\alpha \in \mathbb{C};$ $\quad$?}

stejný argument (? úhel ?)

Relace mezi množinami A, B je podmnožina kartézského součinu $A \times B$.

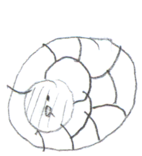


Relace na množině A je podmnožina $A^2 = A \times A$.

Ekvivalence na množině M – relace na M, která je

- reflexivní $\quad (\forall a \in M \quad a \equiv a)$
- symetrická $\quad (\forall a, b \in M \quad a \equiv b \Rightarrow b \equiv a)$
- tranzitivní $\quad (\forall a, b, c \in M \quad a \equiv b \wedge b \equiv c \Rightarrow a \equiv c)$

$M, \equiv$ $\qquad a \in M$ $\qquad \bar{a} = \{x \in M;\ a \equiv x\}$



a, b $\qquad x \in \bar{a} \cap \bar{b}$

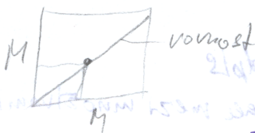
$x \equiv a \quad x \equiv b$

$a \equiv x,\ x \equiv b \Rightarrow a \equiv b$

$\Rightarrow \bar{a} = \bar{b}$

1. $\forall x,y \in M \quad x \equiv y$

$\forall x,y \in M \quad x \equiv y \Rightarrow x = y$ (Rovnost)



sgn ... signum – znaménko

2. $\forall x,y \in \mathbb{Z} \quad x \equiv y \left(\Leftrightarrow \operatorname{sgn} x = \operatorname{sgn} y \quad \Leftrightarrow x \cdot y > 0 \right)$

3., 4. $\forall x,y \in \mathbb{Z} \quad x \equiv y \pmod{n} \Leftrightarrow x - y = k \cdot n$ pro nějaké $k \in \mathbb{Z}$

5. POPIS ?

6. $\forall \alpha,\beta \in \mathbb{C} \quad \alpha \equiv \beta \Leftrightarrow |\alpha| = |\beta|$

7. $\forall \alpha,\beta \in \mathbb{C} \quad \underset{a+bi}{\alpha} \equiv \underset{c+di}{\beta} \Leftrightarrow \frac{a}{\sqrt{a^2+b^2}} = \frac{c}{\sqrt{c^2+d^2}} \ / \ \frac{b}{\sqrt{a^2+b^2}} = \frac{d}{\sqrt{c^2+d^2}}$

Faktorová množina množiny M podle ekvivalence $\equiv$ se značí $M/_{\equiv}$

Uspořádání na množině M – relace, pro níž platí: (ČÁSTEČNÉ)

- reflexivita ($\forall a \in M \quad a \leq a$)
- antisymetrie ($\forall a,b \in M \quad a \leq b, b \leq a \Rightarrow a = b$)
- tranzitivita ($\forall a,b,c \in M \quad a \leq b, b \leq c \Rightarrow a \leq c$)

ÚPLNÉ, LINEÁRNÍ

- dichotomie ($\forall a,b \in M \quad a \leq b \vee b \leq a$)

Př. část. uspoř. množina

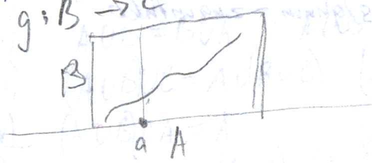
lineární:

ZOBRAZENÍ

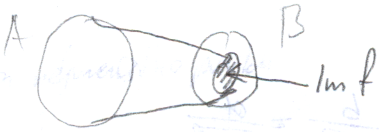
$f: A \to B$ $\quad$ f - předpis

$g: B \to C$ $\quad$ f je relace mezi množinami A, B pro kterou $\forall a \in A\ \exists! b \in B\ \ f(a) = b$

právě jeden



Obraz $\mathrm{Im} f = f(A) = \{b \in B;\ \exists a \in A\ \ b \in f(a)\}$



$\mathbb{Z} \to \mathbb{Z}$

$x \mapsto 2x$

$\mathrm{Im} f = 2\mathbb{Z}$

- prosté: pro každý obraz jenom jeden vzor (injektivní, injekce)
- na (surjektivní, surjekce) - na každý prvek se něco zobrazí [syrjektivní, syrjekce]
- prosté a na (bijektivní, bijekce) (vzájemně jednoznačné)

DÚ: Složení injekcí, surjekcí je opět injekce, surjekce, bijekce

$gf: A \to C$

$(gf)(a) = g(f(a))$

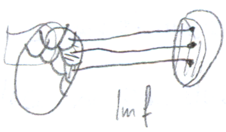
Je-li gf surjekce, potom ... ?

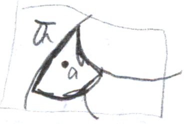
injekce, ... ?

definujme ekvivalenci na A

$\forall x, y \in A \quad x \sim y \iff f(x) = f(y)$

disjunktní rozklad





Kanonické zobrazení surjekce $\quad A \to A/_\sim$

$a \mapsto \bar{a} = \{x \in A;\ f(x) = f(a)\}$

vnoření podmnožiny

$\mathrm{Im} f \to B$

$b \mapsto b$

injekce

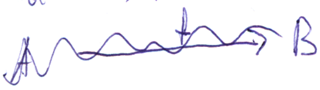
bijekce

$A/_\sim \to \mathrm{Im} f$

$\bar{a} \mapsto f(a)$

$$\begin{tikzcd} A \arrow[rr, "f"] \arrow[d, "s"', "\text{surjekce}"] & & B \\ A/_\sim \arrow[rr, "b", "\text{bijekce}"'] & & \mathrm{Im} f \arrow[u, "i"', "\text{injekce}"] \end{tikzcd}$$

$$\boxed{f = i \cdot b \cdot s}$$



$$\begin{tikzcd}
\mathbb{Z} \arrow[rr, "f"] \arrow[d] & & \mathbb{Z} \\
\mathbb{Z}/_{\equiv} \arrow[r] & \{0,1,\dots,n-1\} \arrow[ru] &
\end{tikzcd}$$

$= \{kn\} \cup \{kn+1\} \cup \dots \cup \{kn+n-1\}$

JAK SE LIŠÍ KONEČNÉ MNOŽINY OD NEKONEČNÝCH

$$\begin{tikzcd}
f: A \arrow[rr] \arrow[d] & & B \\
A/_{\equiv} \arrow[r] & \mathrm{Im} f \arrow[ru] &
\end{tikzcd}$$

$f: \mathbb{R} \longrightarrow \mathbb{R}$

$x \longmapsto x^2$

$f(x) = x^2$

$$\begin{tikzcd}
\mathbb{R} \arrow[rr, "f"] \arrow[d] & & \mathbb{R} \; x^2 \\
\mathbb{R}/_{\equiv} \arrow[r] & \mathbb{R}_0^+ \arrow[ru] &
\end{tikzcd}$$

$x \quad \{x,-x\} \quad x^2$

$\mathbb{R}/_{\equiv} = \{\{x,-x\}; x \in \mathbb{R}\}$

$f: \mathbb{R} \longrightarrow \mathbb{R}$

$x \longmapsto |x|$

$f: \mathbb{R} \longrightarrow \mathbb{R}$

$x \longmapsto [x]$ – celá část x = nejbližší menší celé číslo

$f(x) = [x]$

Př. $\left[\frac{3}{2}\right] = 1$

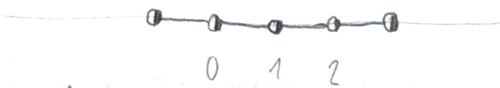
$\left[-\frac{3}{2}\right] = -2$

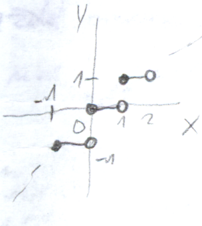
$$\begin{tikzcd}
\mathbb{R} \arrow[rr, "f"] \arrow[d] & & \mathbb{R} \; [x] \\
\mathbb{R}/_{\equiv} \arrow[r] & \mathbb{Z} \arrow[ru] &
\end{tikzcd}$$

$x \quad M_{[x]} \longrightarrow [x]$

$\mathbb{R}/_{\equiv} = \{M_i; i \in \mathbb{Z}\}$

$M_i = \{x \in \mathbb{R}; i \leq x < i+1\}$





$f: \mathbb{R} \to \mathbb{R}$

$f \subset \mathbb{R} \times \mathbb{R}$

$\forall x \in \mathbb{R} \; \exists! y \in \mathbb{R} \; f(x) = y$

$f: \{a,b,c,d\} \longrightarrow \{1,2,3\}$

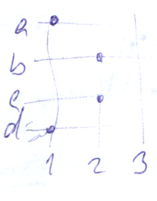
$a \longrightarrow 1$

$b \longrightarrow 2$

$c \longrightarrow 2$

$d \longrightarrow 1$

není bijekce, surjekce ani injekce



TRANSFORMACE MNOŽINY M

$f: M \to M$

bijekce M na M je tzv. permutace

$M = \{1,2,3\}$

Zobrazení $M \to M$ jako trojice : $(f(1), f(2), f(3))$

Permutace:

$\{(1,2,3),(1,3,2),(2,1,3),(2,3,1),(3,1,2),(3,2,1)\}$ GRUPA

Transformace:

$\{(1,1,1),(1,1,2),(1,2,1),(1,2,2),(1,1,3),(1,2,3),(1,3,1),(1,3,2),(1,3,3),$
$(2,1,1),(2,1,2),(2,1,3),(2,2,1),(2,2,2),(2,2,3),(2,3,1),(2,3,2),(2,3,3),$
$(3,1,1),(3,1,2),(3,1,3),(3,2,1),(3,2,2),(3,2,3),(3,3,1),(3,3,2),(3,3,3)\}$

$(\mathcal{T}, \cdot)$
- asociat.
- jednotkový prvek

MONOID

$\{a,b,c\}$ $\{1,2,3\}$

$a \to 2$
$b \to 3$ prosté zobrazení na
$c \to 1$

– KONEČNÁ MNOŽINA: transformace PROSTÁ je NA

$\mathbb{N} \to \mathbb{N}$

$x \mapsto 5x$

$1 \to 2$
$2 \to 4$ prosté zobrazení
$3 \to 6$
$\vdots$

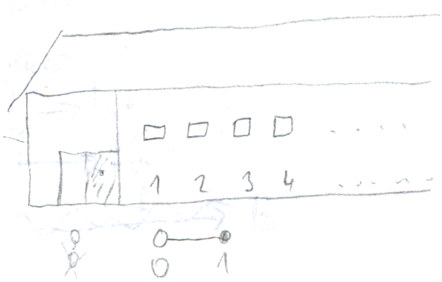
$1 \to 1$
$2 \to 1$
$3 \to 1$ zobrazení na
$4 \to 2$
$5 \to 2$
$\vdots$

$\mathbb{N} = \{1,2,\dots\}$

– spočetná množina (prvky se dají srovnat do posloupnosti)

spočetná množina je každá, která se dá bijekcí zobrazit na $\mathbb{N}$ (srovnat do posloupnosti)

Hilbertův hotel



$\mathbb{N}, 2\mathbb{N}, 3\mathbb{N}, 100\mathbb{N},$ – bijekce

spočetné
$\mathbb{Z}, \mathbb{N}$ $\{0,1,-1,2,-2,3,-3,\dots\}$
$\mathbb{Q}$

$0 \quad \frac{1}{1} \quad \frac{2}{1} \quad \frac{3}{1} \quad \frac{4}{1} \ \dots$

$-\frac{1}{1} \quad -\frac{2}{1} \quad -\frac{3}{1} \quad -\frac{4}{1} \quad -\frac{5}{1} \ \dots$

$\frac{1}{2} \quad \frac{2}{2} \quad \frac{3}{2} \quad \frac{4}{2} \quad \frac{5}{2} \ \dots$

$-\frac{1}{2} \quad -\frac{2}{2} \quad -\frac{3}{2} \ \dots$

$\mathbb{R}, \mathbb{C}$
nespočetné!

$(0,1)$

SPOREM: Předp., že interval $(0,1)$ má spočetně mnoho čísel.

$\bar{c}_1 = 0{,}a_{11}a_{12}a_{13}\ldots$ $\quad x = 0{,}b_1b_2b_3\ldots$ $\quad b_1 \neq a_{11}$ $\quad x \neq \bar{c}_1$

$\bar{c}_2 = 0{,}a_{21}a_{22}a_{23}\ldots$ $\quad b_2 \neq a_{22}$ $\quad x \neq \bar{c}_2$

$\bar{c}_3 = 0{,}a_{31}a_{32}a_{33}\ldots$ $\quad b_3 \neq a_{33}$ $\quad x \neq \bar{c}_3$ $\quad \Rightarrow (0,1)$ NELZE seřadit do posloupnosti

$\vdots$

Leopold KRONECKER (1823–1891) 1886: „Celá čísla vytvořil Bůh, všechno ostatní je lidským dílem."

Richard DEDEKIND (1831–1916) 1888: „Čísla jsou svobodným výtvorem lidského ducha. Slouží jako prostředek pro snadnější pochopení rozmanitějších věcí."

Giuseppe PEANO (1858–1932) 1889 – Peanovy axiomy přirozených čísel

---

Přirozená čísla

$1, 2, 3, 4, 5, \ldots$

Peanovy axiomy

1. 1 je přirozené číslo.
2. Každé přirozené číslo n má následníka $s(n)$.
3. Číslo 1 není následníkem žádného přirozeného čísla.
4. Dvě různá přirozená čísla mají různé následníky ($n_1 \neq n_2 \Rightarrow s(n_1) \neq s(n_2)$)
5. Jestliže pro podmnožinu $X \subset \mathbb{N}$ je $1 \in X$, $n \in X \Rightarrow s(n) \in X$, potom je $X = \mathbb{N}$. (Princip matematické indukce)

DÚ: Následující dva principy jsou ekvivalentní

(i) Princip matematické indukce.

(ii) Princip dobrého uspořádání: Každá neprázdná podmnožina množiny $\mathbb{N}$ má nejmenší prvek.

Každá omezená podmnožina množiny $\mathbb{N}$ má největší prvek.

$11^{n+1} + 12^{2n-1}$ dělitelné číslem 133 pro $n \in \mathbb{N}$.

$n=1$: $11^2 + 12^1 = 133$ O.K.

$n \to n+1$:

$$11^{n+2} + 12^{2n+1} = 11\cdot 11^{n+1} + 12^2\cdot 12^{2n-1} = 11\cdot 11^{n+1} + 144\cdot 12^{2n-1} =$$

$$= 11\cdot 11^{n+1} + (133+11)\cdot 12^{2n-1} = 11\cdot 11^{n+1} + 133\cdot 12^{2n-1} + 11\cdot 12^{2n-1} =$$

$$= 11\cdot(11^{n+1} + 12^{2n-1}) + 133\cdot 12^{2n-1}$$

$$1^2 + 2^2 + \ldots + n^2 = \frac{1}{6}\cdot n\cdot(n+1)\cdot(2n+1)$$

$n \to n+1$

$$\frac{1}{6}\cdot(n+1)\cdot(n+2)\cdot(2n+3) = \frac{1}{6}\cdot n(n+1)(2n+1) + (n+1)^2 = \frac{2n^3+3n^2+n+6n^2+12n+6}{6} = \frac{2n^3+9n^2+13n+6}{6}$$

$$\frac{(n+1)(n+2)(2n+3)}{6} = \frac{2n^3+9n^2+13n+6}{6}$$

$1^3+2^3+\dots+n^3=\frac{n^2\cdot(n+1)^2}{4}$ $\quad n=1:\ \frac{1^2\cdot(1+1)^2}{4}$

$$\frac{(n+1)^2(n+2)^2}{4}=\frac{n^2(n+1)^2}{4}+(n+1)^3$$

$$\frac{(n+1)^2(n+2)^2}{4}=\frac{(n^2+2n+1)(n^2+4n+4)}{4}=\frac{n^4+6n^3+13n^2+12n+4}{4}$$

$$\Updownarrow$$

$$\frac{n^2(n+1)^2}{4}+(n+1)^3=\frac{n^4+2n^3+n^2+4n^3+12n^2+12n+4}{4}=\frac{n^4+6n^3+13n^2+12n+4}{4}$$

$\boxed{1^k+2^k+\dots+n^k=?}$

$n(n+1)(n+2)$ dělitelné 6

$1+3+\dots+(2n-1)=n^2$

$$\frac{1}{1\cdot 2}+\frac{1}{2\cdot 3}+\dots+\frac{1}{n\cdot(n+1)}=\frac{n}{n+1}$$

I $n=1$: $\frac{1}{2}=\frac{1}{1+1}$

II $\frac{n+1}{n+2}=\frac{n}{n+1}+\frac{1}{(n+1)(n+2)}=\frac{n^2+2n+1}{(n+1)(n+2)}=\underline{\underline{\frac{n+1}{n+2}}}$

$$1^2+3^2+\dots+(2n-1)^2=\frac{1}{3}n(2n-1)(2n+1)$$

I $n=1$ $\quad 1^2=\frac{1}{3}\cdot 1\cdot 1\cdot 3$

II. $\frac{1}{3}(n+1)(2n+1)(2n+3)=\frac{1}{3}n(2n-1)(2n+1)+(2n+1)^2=\frac{4n^3-n+12n^2+12n+3}{3}$

$$\frac{4n^3+12n^2+11n+3}{3}$$

$$1^3+3^3+\dots+(2n-1)^3=n^2(2n^2-1)$$

I $n=1$ $\quad 1^3=1^2(2\cdot 1-1)$

II. $(n+1)^2\left[2(n+1)^2-1\right]=(n^2+2n+1)(2n^2+4n+1)=2n^4+8n^3+11n^2+1+6n$

$n^2(2n^2-1)+(2n+1)^3=2n^4-n^2+8n^3+12n^2+6n+1$

Def. Jestliže pro přirozená čísla a, b, c platí $a = bc$, pak říkáme, že a je násobkem čísla b a b je dělitelem čísla a. Píšeme $b \mid a$.

Značení: $N(a_1, a_2, \dots, a_k)$ = množina všech násobků čísel $a_1, \dots, a_k$

$D(a_1, a_2, \dots, a_k)$ = množina všech dělitelů čísel $a_1, \dots, a_k$

Dobré uspořádání $\Rightarrow$ v $N(a_1, \dots a_k)$ ex. nejmenší prvek $n(a_1, \dots, a_k)$ nejmenší společný násobek čísel $a_1, \dots, a_k$

$D(a_1, \dots, a_k)$ je omezená $\Rightarrow$ ex. největší prvek $d(a_1, \dots, a_k)$ největší společný dělitel čísel $a_1, \dots, a_k$

Př. 4, 6, 14 $\quad d(4,6,14) = 2$

$n(4,6,14) = 84$

Def. Přirozené číslo $p > 1$ se nazývá prvočíslo, je-li množina $D(p)$ dvouprvková.

$D(p) = \{1, p\}$

Má-li $D(n)$ více prvků, nazývá se n složené.

1

prvočísla: 2, 3, 5, 7, ...

složená: 4, 6, 8, 9, ...

Věta: Každé přirozené číslo větší než 1 je násobkem nějakého prvočísla.

D. Sporem: Nechť M je množina všech přirozených čísel, která nejsou násobkem nějakého prvočísla a jsou větší než 1.

$2, 3, 4, 5 \notin M$

princip do Dobré uspoř. $\Rightarrow$ M má nejmenší prvek m.

m musí být složené $m = a \cdot b$, $a < m$, $b < m$

Tedy a je násobkem nějakého prvočísla

Tedy i m je násobkem nějakého prvočísla.

$\Downarrow$

Věta: Každé přirozené číslo je součinem prvočísel.

D. 1 je součinem prázdné množiny prvočísel.

sporem: Nechť M je množina všech přiroz. čísel, která nejsou součinem prvočísel.

Dobré uspoř. $\Rightarrow$ nechť m je nejmenší prvek z množiny M. Číslo m nemůže být prvočíslo, tedy $m = a \cdot b$, kde $a < m$, $b < m$. Tedy a, b jsou součiny prvočísel, a tedy i m je součinem prvočísel.

Věta: Prvočísel je nekonečně mnoho.

D. Předp., že $p_1, \dots, p_k$ jsou všechna prvočísla.

Uvažujme číslo $p_1 \cdot p_2 \cdot \dots \cdot p_k + 1$.

Existuje prvočíslo, které číslo n dělí.

Prvočísla $p_1, \dots, p_k$ však číslo n nedělí! SPOR.

Modifikace: Ke každému prvočíslu p existuje prvočíslo které je větší.

$p \quad p! + 1$ musí být dělitelné nějakým prvočíslem, ale není dělitelný čísly $1, 2, \dots, p$

$\Rightarrow$

$F_n = 2^{2^n} + 1$ – Fermatova čísla

<u>DÚ</u>: $F_n = 2^k + 1$ je prvočíslo $\Rightarrow$ k je mocninou dvojky

$F_0 = 3$
$F_1 = 5$
$F_2 = 17$
$F_3 = 257$
$F_4 = 2^{16} + 1 = 65\,537$
prvočísla

F_5 není prvočíslo (Euler)

$a^3 + b^3$

$F_5 = 2^{32} + 1 =$ $\underline{641}$

$$2^{32} = 2^2 \cdot (2^{10})^3 = 4 \cdot (1024)^3 = 4 \cdot (641 + 383)^3 = 4 \cdot (641 \cdot a + 383^3) = 4 \cdot (641 a + \underset{56\,181\,727}{56\,181\,887}) =$$

$$= 4 \cdot (641 a + 641 \cdot 87647 + 160) = 641 b + 640$$

$$F_5 = 641 (b+1)$$

$$F_{n+t} - 1 = (F_n - 1)^{2^t}$$

$$2^{2^{n+t}} = \left(2^{2^n}\right)^{2^t}$$

$$F_{n+t} = F_n \cdot a + 2$$

$\Rightarrow$ kdyż prvočíslo dělí 1 Fermatovo číslo, tak nemůže dělit další

$\Rightarrow$ PRVOČÍSEL JE NEKONEČNĚ MNOHO

Celá čísla

Dělení se zbytkem: $b \in \mathbb{N}$.

Pro každé celé číslo a existují jednoznačně určená celá čísla q, r taková, že $\boxed{a = bq + r, \text{ kde } 0 \le r < b.}$

D. $\dots \{-b, \dots, -1\}, \{0, \dots, b-1\}, \{b, \dots, 2b-1\}, \{2b, \dots, 3b-1\}, \dots$

$$\{qb, \dots, (q+1)b-1\}$$

Euklidův algoritmus $a > b$, $a, b \in \mathbb{N}$. Posloupnost dělení

$$a = bq_0 + r_0 \quad 0 \le r_0 < b$$
$$b = r_0 q_1 + r_1 \quad 0 \le r_1 < r_0$$
$$r_0 = r_1 \cdot q_2 + r_2 \quad 0 \le r_2 < r_1$$
$$\vdots$$
$$r_{k-2} = r_{k-1} \cdot q_k + r_k \quad 0 \le r_k < r_{k-1}$$
$$r_{k-1} = r_k \cdot q_{k+1} \quad (\text{beze zbytku})$$

je konečná! Číslo r_k (poslední nenulový zbytek) je největším společným dělitelem čísel a, b. Navíc je lineární kombinací čísel a, b, tj. $r_k = u \cdot a + v \cdot b$, $u, v \in \mathbb{Z}$.

D. r_k je společným dělitelem čísel a, b (viděno odspodu)
x dělí $a, b \Rightarrow x$ dělí r_k (viděno odshora)
r_k je LK čísel a, b (viděno odshora)

DÚ: Zvolte konkrétní čísla a, b a vypočtěte nejv. spol. dělitele a vyjádřete jej jako LK čísel a, b.

Důsledek. Jsou-li čísla a, b nesoudělná, pak existují celá čísla u, v taková, že $\boxed{1 = u \cdot a + v \cdot b.}$

Euklidovo lemma

Jestliže prvočíslo p dělí součin $a \cdot b$, kde $a, b \in \mathbb{N}$, potom buď p dělí a nebo p dělí b.

D. Pokud p nedělí a, jsou a, p nesoudělná. Tedy $pu + av = 1$, kde $u, v \in \mathbb{Z}$.
Potom $b = \underline{p} \cdot u \cdot b + \underline{a \cdot v \cdot b}$ Nyní p dělí pravou stranu, tedy dělí levou stranu.

Základní věta aritmetiky: Každé přirozené číslo se dá jediným způsobem zapsat ve tvaru $p_1^{k_1} \cdot p_2^{k_2} \cdot \ldots \cdot p_t^{k_t}$, kde $t \in \mathbb{N}_0$, $p_1 < p_2 < \ldots < p_t$ jsou prvočísla a $k_1, \ldots, k_t \in \mathbb{N}$

D. Existence již byla dokázána.
Jednoznačnost plyne z Euklejdova lemmatu.

$\operatorname{sgn} n \cdot p_1^{k_1} \cdot \ldots \cdot p_t^{k_t}$

GAUSOVA CELÁ ČÍSLA

Gaussova celá čísla $\mathbb{Z}[i] = \{a+bi \,;\, a,b \in \mathbb{Z}\}$

$N(a+bi) = a^2+b^2$

norma = „vzdálenost od počátku"$^{(2)}$

VYRUŠÍ
VYKRÁTÍ

Zákon normy: $N(\alpha \cdot \beta) = N(\alpha) \cdot N(\beta)$

D. $N(\alpha \cdot \beta) = \underline{(ac-bd)^2 + (ad+bc)^2} = a^2c^2 - 2abcd + b^2d^2 + a^2d^2 + 2abcd + b^2c^2 = \underline{(a^2+b^2)(c^2+d^2)}$

- $\alpha = a+bi$
  $\beta = c+di$
  $\alpha \cdot \beta = (ac-bd) + (ad+bc)i$

~~$N(\alpha) \cdot N(\beta) = (ac-bc)(ad+bc) = a^2cd + abc^2 - abcd - b^2c$~~

INVERTIBILNÍ PRVKY

$\alpha \cdot \alpha^{-1} = 1$

$1 = N\left(\frac{\alpha \cdot \alpha^{-1}}{1}\right) = \underline{N(\alpha) \cdot N(\alpha^{-1})}$ $\Rightarrow$ $\underline{N(\alpha) = 1}$ $\Rightarrow$ $\alpha \in \underline{\{1; -1; i; -i\}}$

$N(\alpha) = 0; 1;$ ⟶ $a^2 = 0, 1, 4, 9, 16, 25 \ldots$

2 5 10 17 26
8 13 20 29
18 25 34
32 41
50

$\alpha = \beta \cdot \gamma \Rightarrow N(\alpha) = N(\beta) \cdot N(\gamma)$

$N(2) = 4$ $2 = (1+i)(1-i)$ je rozložitelná   ($1+i$, $1-i$ jsou prvočísla)

$N(3) = 9$ 3 je prvočíslo

$N(5) = 25$ $5 = (2+i)(2-i)$
$(1+2i)(1-2i)$ je rozlož.

$2+i$, $2-i$
$1+2i$, $1-2i$ jsou prvočísla

DÚ
$4k+1$ – rozlož.
$4k+3$ – prvočísla

Každé prvočíslo tvaru $4k+1$ je součtem 2 čtverců.

DÚ

$\mathbb{Z}[i\sqrt{5}]$ $N(\alpha) = a^2 + 5b^2$

INV. PRVKY ± 1

Eratosthenovo síto

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

$\mathbb{P}$: 2, lichá $\begin{cases} 4k+1 & \text{- nekonečně mnoho} \\ 4k+3 & \text{- nekonečně mnoho} \end{cases}$

Věta: Prvočísel tvaru $4k+3$ je nekonečně mnoho.

D. Každé číslo tvaru $4k+3$ je dělitelné prvočíslem tohoto tvaru

$4k+3=(4a+1)(4b+1)\dots(4z+1)$

$4k+3=4x+1$ SPOR

$p_1=3,\ p_2=7$ $\quad$ p_2 tvaru $4k+3$ $\quad$ $p_1 \geq 7$

$\boxed{n=p_n!-1}=4k+3$ - musí být dělitelné prvočíslem tvaru $4k+3$, nechť je to $p_{n+1}>p_n$

Malá Fermatova věta $\quad$ stejný zbytek při dělení p

$p\in\mathbb{P}$ $\quad$ $a\in\mathbb{N}$ $\quad$ $a^p\equiv a \pmod p$

$a^p = a$ v $\mathbb{Z}_p$

$p\nmid a \Rightarrow a^{p-1}\equiv 1 \pmod p$

p nedělí a $\quad$ $a^{p-1}=1$ v $\mathbb{Z}_p$

Důkaz: $p\nmid a$ $\quad$ $a, 2a, 3a, \dots, (p-1)a$ - mají různé zbytky při dělení p

$ka=la$ v $\mathbb{Z}_p \Rightarrow (k-l)a=np \Rightarrow p\mid k-l$ SPOR

$a=q_1p+z_1$

$2a=q_2p+z_2$

$\vdots$

$(p-1)a=q_{p-1}p+z_{p-1}$

$(p-1)!\,a^{p-1}=A\cdot p+\underbrace{z_1z_2\dots z_{p-1}}_{(p-1)!}$

$(p-1)!\,(a^{p-1}-1)=A\cdot p$

$p\mid a^{p-1}-1 \Rightarrow a^{p-1}\equiv 1 \pmod p.$

D. $(a+b)^p\equiv a^p+b^p \pmod p$

neboť $(a+b)^p=a^p+\cancel{\binom{p}{1}a^{p-1}b}+\cancel{\binom{p}{2}a^{p-2}b^2}+\dots+\cancel{\binom{p}{p-1}ab^{p-1}}+b^p$

$\binom{p}{k}=\frac{p!}{k!\cdot(p-k)!}$ - násobky p

Indukcí: $a=1$ $\quad$ $1^p\equiv 1 \pmod p$

$a\to a+1$ $\quad$ $(a+1)^p-(a+1)=a^p+1-a-1=a^p-a\equiv 0 \pmod p$

$a^p\equiv a$

$(a+1)^p\equiv a+1 \pmod p$

Věta: Prvočísel tvaru $4k+1$ je nekonečně mnoho.

D. Každé liché prvočíslo, které dělí číslo tvaru n^2+1 je tvaru $4k+1$

$p \mid n^2+1 \Rightarrow n^2 \equiv -1 \pmod p \Rightarrow n^4 \equiv 1 \pmod p$

$\Rightarrow p \nmid n \Rightarrow n^{p-1} \equiv 1 \pmod p$

Kdyby $p=4k+3$, tak $n^{p-1} = n^{4k+2} = (n^4)^k \cdot n^2 \equiv -1 \pmod p$

SPOR

Tedy $p=4k+1$.

$p_1=5 \dots p_n$ tvaru $4k+1$, $p_n \geq 5$ $\qquad p_{n+1} > p_n$!

$m=(p_n!)^2+1 \Rightarrow$ prvočíslo p_{n+1}, které dělí m má tvar $4k+1$

Dokonalá čísla: $6=1+2+3 \quad (2\cdot 6 = 1+2+3+6)$

$28 = 1+2+4+7+14 \quad (2\cdot 28 = 1+2+4+7+14+28)$

Věta (Eukleides): Je-li 2^p-1 prvočíslo, je $2^{p-1}(2^p-1)$ dokonalé (sudé).

$(1+2+\dots+2^{p-1}) + (1+2+\dots+2^{p-2})(2^p-1) = \dots = 2^{p-1}(2^p-1)$

$(2^p-1) + (2^{p-1}-1)(2^p-1) = (2^p-1)\cdot 2^{p-1}$

D. DÚ

MERSENNEOVA ČÍSLA 2^k-1 $k\in\mathbb{N}$

[mersenova]

DÚ: $2^k-1 \in \mathbb{P} \Rightarrow k \in \mathbb{P}$ důk. sporem

$2^2-1=3 \dots\dots \cdot 2^1 \rightarrow 6$

$2^3-1=7 \dots\dots \cdot 2^2 \rightarrow 28$

$2^5-1=31 \dots\dots \cdot 2^4 \Rightarrow 16\cdot 31 = 496$

$2^7-1=127 \dots\dots \cdot 2^6 \rightarrow 8\,128$

$2^{11}-1=2047 =$ NENÍ PRVOČÍSLO

$2^{13}-1=$

1750 Euler $M_{31}=2^{31}-1$ je prvočíslo

1876 LUCAS $M_{127}=2^{127}-1$ (39 cifer) – 12. známé MERSENOVO PRVOČÍSLO

1951

2000 38 MERS. PRVOČÍSEL

dnes 47

2008: $M_{43\,112\,609}$ skoro 13 milionů cifer

Věta (Euler): Každé sudé dokonalé číslo má tvar $2^{p-1}(2^p-1)$, kde 2^p-1 je prvočíslo.

D. Mějme sudé dokonalé číslo ve tvaru $2^{m-1}\cdot q$, kde $m>1$, q je liché.

Dokonalé: $2^m \cdot q$ je součet všech dělitelů čísla $2^{m-1} q$

$$2^m \cdot q = \underbrace{(1+2+\dots+2^{m-1})}_{2^m-1} \cdot S$$

S ... součet všech dělitelů čísla q.

$\Rightarrow S = 2^m \cdot x \qquad q=(2^m-1)\cdot x$

kdyby $x \neq 1$:

~~$S=2^m x$~~ $\quad$ ~~$q=(2^m-1)x$~~

$S = 2^m \cdot \cancel{x} = (2^m-1)x + (2^m-1) + x + \dots + 1 = 2^m \cdot x + 2^m > 2^m \cdot x$ SPOR. $\Rightarrow x=1$, $q=2^m-1$

$\boxed{S=2^m} \Rightarrow$

$2^m-1 \in \mathbb{P}$

4200 1980

$4200 / 1980 = 2\ (240)$

240

$1980/240 = 8\ (60)$

$240/60 = 4$

$4200 = 1980\cdot 2 + 240$

$1980 = 240\cdot 8 + \boxed{60}$ NSD(4200, 1980) = 60

$240 = 60\cdot 4$

$60 = 1980 - 8\cdot 240 = 1980 - 8\cdot(4200 - 2\cdot 1980) =$

$= 17\cdot 1980 - 8\cdot 4200$

$\boxed{60 = 17\cdot 1980 - 8\cdot 4200}$ D… LK těch 2 čísel

$4200 = 2^2\cdot 5^2\cdot 2\cdot 3\cdot 7 = 2^3\cdot 3\cdot 5^2\cdot 7$

$1980 = 2^2\cdot 5\cdot 3^2\cdot 11$

$D = 2^2\cdot 3\cdot 5 = \underline{60}$

$n = 2^3\cdot 3^2\cdot 5^2\cdot 7\cdot 11 = \underline{138\,600}$

$60 \times 138\,600 = 4200 \times 1980$

$\boxed{NSD(a,b)\cdot NSN(a,b) = a\cdot b}$

ŘETĚZOVÝ ZLOMEK

$$\frac{4200}{1980} = 2 + \frac{240}{1980} = 2 + \frac{1}{\frac{1980}{240}} = 2 + \frac{1}{8 + \frac{60}{240}} = 2 + \frac{1}{8 + \frac{1}{\frac{240}{60}}} = 2 + \frac{1}{8 + \frac{1}{4}} = [2; 8, 4]$$

$$= 2 + \frac{1}{\frac{33}{4}} = 2 + \frac{4}{33} = \frac{70}{33}$$

8645, 7590

$8645 = 7590\cdot 1 + 1055$

$7590 = 1055\cdot 7 + 205$

$1055 = 205\cdot 5 + 30$

$205 = 30\cdot 6 + 25$

$30 = 25\cdot 1 + \boxed{5}$ NSD(8645, 7590) = 5

$25 = 5\cdot 5$

$5 = 30 - 25 = 30 - (205 - 6\cdot 30) = 7\cdot 30 - 205 = \cancel{7\cdot 30 - (7590 - 7}$

$= 7\cdot(1055 - 5\cdot 205) - 205 = 7\cdot 1055 - 36\cdot 205 = 7\cdot 1055 - 36\cdot(7590 - 7\cdot 1055) =$

$= -36\cdot 7590 + 35\cdot 7\cdot 1055 = -36\cdot 7590 + 257\cdot(8645 - 7590) = \cancel{281}$

$= 259\cdot 8645 - 295\cdot 8645$

$$\frac{8645}{7590} = 1 + \frac{1}{\frac{7590}{1055}} = 1 + \frac{1}{7 + \frac{1}{\frac{1055}{205}}} = 1 + \frac{1}{7 + \frac{1}{5 + \frac{205}{30}}} =$$

$$= 1 + \frac{1}{7 + \frac{1}{5 + \frac{1}{6 + \frac{25}{30}}}} = 1 + \frac{1}{7 + \frac{1}{5 + \frac{1}{6 + \frac{1}{1 + \frac{1}{\frac{25}{5}}}}}} = 1 + \frac{1}{7 + \frac{1}{5 + \frac{1}{6 + \frac{1}{1 + \frac{1}{5}}}}} =$$

$= [1; 7, 5, 6, 1, 5]$

DÚ: $\sqrt{2}$

$8645 = 5 \cdot 1729 = 5 \cdot 7 \cdot 247 = 5 \cdot 7 \cdot 13 \cdot 19$

$7590 = 2 \cdot 3 \cdot 5 \cdot 253 = \cancel{2} \cdot 3 \cdot 5 \cdot 11 \cdot 23$

$8645 \cdot 23 \cdot 33 = 8645 \cdot 759$

$$\begin{array}{r} 8645 \\ \cdot 759 \\ \hline 77805 \\ 43225 \\ 5 \end{array}$$

$NSD(8645, 7590) = 5$

$NSN(8645, 7590) =$

$2282 = 2\cdot 10^3 + 2\cdot 10^2 + 8\cdot 10^1 + 2\cdot 10^0$

$= a_0\cdot 1 + a_1\cdot 12 + a_2\cdot 12^2 + a_3\cdot 12^3$

$$\begin{array}{r} 123 \\ \cdot 12 \\ \hline 246 \\ 123 \\ \hline 1476 \end{array}$$

$2282 = 12\cdot 190 + 2 = 12\cdot(12\cdot 15+10)+2 = 12\cdot(12\cdot(12\cdot 1+3)+10)+2$

$190 = 12\cdot 15 + 10$

$15 = 12\cdot 1 + 3$

$= 1\cdot 12^3 + 3\cdot 12^2 + 10\cdot 12 + 2$

$\cancel{2A3}$

$(2282)_{10} = (13A2)_{12} = (4352)_8 = (10010112)_3 =$

$A = 10$

$= (100011101010)_2$

$2282 = 8\cdot 285 + 2$

$\cancel{387 = 8\cdot 48 + 3}$

$\cancel{48 = 8\cdot 6}$

$285 = 8\cdot 35 + 5$

$35 = 8\cdot 4 + 3$

$2282 = 3\cdot 760 + 2 = 3\cdot(3\cdot 253+1)+2 = 3\cdot(3\cdot(3\cdot 84+1)+1)+2 =$

$= 3\cdot(3\cdot(3\cdot(3\cdot 28+0)+1)+1)+2 = 3\cdot(3\cdot(3\cdot(3\cdot(3\cdot 9+1)+0)+1)+1)+2 =$

$= 3\cdot(3\cdot(3\cdot(3\cdot(3\cdot(3\cdot 3+0)+1)+0)+1)+1)+2 =$

$= 3\cdot(3\cdot(3\cdot(3\cdot(3\cdot(3\cdot(3\cdot 1+0)+0)+1)+0)+1)+1)+2 =$

$= 3\cdot(3\cdot(3\cdot(3\cdot(3\cdot(3\cdot(3\cdot(3\cdot 0+1)+0)+0)+1)+0)+1)+1)+2$

$2282 = 2\cdot 1141 + 0$

$1141 = 2\cdot 570 + 1$

$570 = 2\cdot 285 + 0$

$285 = 2\cdot 142 + 1$

$142 = 2\cdot 71 + 0$

$71 = 2\cdot 35 + 1$

$35 = 2\cdot 17 + 1$

$17 = 2\cdot 8 + 1$

$8 = 2\cdot 4 + 0$

$4 = 2\cdot 2 + 0$

$2 = 2\cdot 1 + 0$

$1 = 2\cdot 0 + 1$

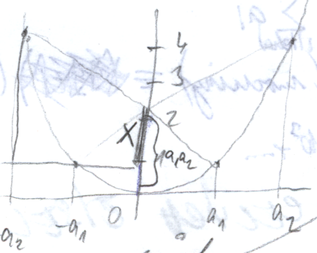
$y=x^2$

(x,x^2) $\quad x\in\mathbb{Z}$

$a_1,a_2\in\mathbb{N}$

$(-a_1,a_1^2)$ $\quad (a_1,a_1^2)$

$(-a_2,a_2^2)$ $\quad (a_2,a_2^2)$ $\Big\}$ body paraboly



$$\frac{a_2^2-a_1^2}{a_1+a_2}=\frac{x}{a_1}$$

Která N na ose y zůstanou nedotčena?

$a_1a_2-a_1^2+a_1^2=a_1a_2$

$x=a_1(a_2-a_1)$

$\Rightarrow$ NEDOTČENÉ BODY NA OSE Y BUDOU PRÁVĚ PRVOČÍSLA !

MATIJASEVIČOVA PARABOLA

$a=a_n\cdot10^n+a_{n-1}\cdot10^{n-1}+\dots+a_1\cdot10+a_0$

Dělitelnost 2, 5, 10: $\iff$ a_0 je dělitelné 2, 5, 10

Dělitelnost 4, 25, 50, 100: $\iff$ $a_1\cdot10+a_0$ je dělitelné 4, 25, 50, 100

Dělitelnost 3, 9 $\iff$ $\sum_{i=0}^{n}a_i$ je dělitelné 3, 9

$$a\equiv\underbrace{a_n+a_{n-1}+\dots+a_1+a_0}_{\text{ciferný součet}}\pmod 9$$

Dělitelnost 6 $\iff$ dělitelnost 2 a 3

Dělitelnost 7

37 790 348 $\qquad 100=7\cdot14+2$

$$a=(7\cdot14+2)\cdot(a_n\cdot10^{n-2}+a_{n-1}\cdot10^{n-3}+\dots+a_2)+a_1\cdot10+a_0$$

$37\,790\,348\equiv2\cdot377\,903+47=755\,853\equiv\cancel{2\cdot7558+47=15163}\equiv2\cdot151+47=349\equiv$

$\cancel{\equiv2\cdot3+47=53}$

$1000=7\cdot143-1$

$$a=(7\cdot143-1)\cdot(a_n\cdot10^{n-3}+\dots+a_3)+a_2\cdot100+a_1\cdot10+a_0$$

$37\,790\,347\equiv-37\,790+347\equiv37-790+347=384-790=-406$

$7\mid406$

Dělitelnost 11 $\iff \sum_{i\,\text{sudé}} a_i - \sum_{i\,\text{liché}} a_i$

$a \equiv$ (sudé mocniny) + (liché mocniny) $\equiv$ ~~...~~ $(a_0+a_2+\dots)+(-a_1-a_3-\dots)$

$a_0+a_2\cdot 10^2+\dots$ $\qquad$ $a_1+a_3\cdot 10^3+\dots$

FORMÁLNÍ KONSTRUKCE CELÝCH ČÍSEL

$\mathbb{N}$ – Peanovy axiomy

Konstrukce $\mathbb{Z}$

$\mathbb{N}\times\mathbb{N}$ ekvivalence $(a,b)\sim(c,d)$ $\qquad$ $a-b=c-d$

právě když $a+d=b+c$ $\qquad$ $a+d=b+c$

$(1,1),(2,2),(3,3),(4,4),\dots$	0
$(2,1),(3,2),(4,3),(5,4),\dots$	1
$(1,2),(2,3),(3,4),(4,5),\dots$	-1
$(2,5),(3,6),(5,8),\dots$	-3
$(1,5),(2,6)$	-4

TŘÍDY EKVIVALENCE

$\mathbb{Z} = \mathbb{N}\times\mathbb{N}/\sim$ $\quad$ faktorová množina podle ekvivalence

$+ \quad \overline{(a,b)} + \overline{(c,d)} = \overline{(a+c,\,b+d)}$

třída, která obsahuje prvek (a,b)

Korektnost:

$$\left.\begin{aligned}(a',b')&\sim(a,b)\\ (c',d')&\sim(c,d)\end{aligned}\right\} \Rightarrow (a'+c',\,b'+d')\sim(a+c,\,b+d)$$

DOKAŽ!

• $\overline{(a,b)}\cdot\overline{(c,d)} = ?$

Korektnost:

$\mathbb{N} \to \mathbb{Z}$

$\mathbb{N}\times\mathbb{N} = \{(a,b);\ a,b\in\mathbb{N}\}$

ekvivalence: $(a,b)\sim(c,d) \overset{df}{\Leftrightarrow} a-b=c-d$

$a+d=b+c$

refl. $(a,b)\sim(a,b)$

sym. $(a,b)\sim(c,d) \Rightarrow (c,d)\sim(a,b)$

tr. $(a,b)\sim(c,d) \sim (e,f) \Rightarrow (a,b)\sim(e,f)$

$a+d=b+c$ $\quad a+f=b+e$

$c+f=d+e$

$a+\cancel{c}+\cancel{d}+f=b+\cancel{c}+\cancel{d}+e$

$a+f=b+e$

faktorová množina

disj. rozklad: $\{(2,1),(3,2),(4,3),\dots\} \to 1$

$\{(3,1),(4,2),(5,3),\dots\} \to 2$

$\{(4,1),(5,2),(6,3),\dots\} \to 3$

$\{(1,1),(2,2),(3,3),\dots\} \to 0$

$\{(1,2),(2,3),(3,4),\dots\} \to -1$

$\{(1,3),(2,4),(3,5),\dots\} \to -2$

$\overline{(a,b)}\cdot\overline{(c,d)} = \overline{(ac+bd, ad+bc)}$

$\overline{(a,b)}+\overline{(c,d)} = \overline{(a+c, b+d)}$

Definujeme operace pomocí reprezentantů ⇒ musíme prověřit korektnost definice.

$(a,b)\sim(a',b')$ $\quad (c,d)\sim(c',d') \Rightarrow (ac+bd, ad+bc)\sim(a'c'+b'd', a'd'+b'c')$

$a+b'=b+a'$ $\quad c+d'=d+c' \Rightarrow ac+bd+a'd'+b'c'=ad+bc+a'c'+b'd'$

$(a+b')\cdot(c+d') = ac+ad'+b'c+b'd'$

$(b+a')\cdot(d+c') = bd+bc'+a'd+a'c'$

$\cdot(c+c')$: $ac+ac'+b'c+b'c' = bc+bc'+a'c+a'c'$

$\cdot(d+d')$: $bd+bd'+a'd+a'd' = ad+ad'+b'd+b'd'$

$\cdot(a+a')$: $ca+ca'+d'a+d'a' = da+da'+c'a+c'a'$

$\cdot(b+b')$: $db+db'+cb+c'b' = cb+cb'+d'b+d'b'$

$2ac+2bd+2b'c'+2a'd'+ac'+bc+bd'+a'd+ca'+da'+db'+c'b =$

$= 2bc+2ad+2a'c'+2b'd'+bc'+a'c+ad'+b'd+da'+ca'+cb'+d'b$

$(a+c, b+d)\sim(a'+c', b'+d') \Rightarrow a+c+b'+d'=b+d+a'+c'$

jsou ekvivalentní

DÚ: zákony PROVĚŘIT

$\mathbb{Z} \longrightarrow \mathbb{Q}$

$\mathbb{Z} \times (\mathbb{Z} \setminus \{0\}) = \{(a,b);\ a,b \in \mathbb{Z},\ b \neq 0\}$

ekvivalence: $(a,b) \sim (c,d) \iff ad = bc$

$\frac{a}{b} = \frac{c}{d}$

$ad = bc$

refl. $(a,b) \sim (a,b) \iff ab = ba$

sym. $(a,b) \sim (c,d) \Rightarrow$ ~~$ad = bc$~~ $(c,d) \sim (a,b)$

tranzitivita $(a,b) \sim (c,d) \sim (e,f) \Rightarrow (a,b) \sim (e,f)$

$ad = bc$ $\qquad af = be$

$cf = de$

$ad\cancel{cf} = b\cancel{cd}e$

$af = be$

$\{(1,2), (2,4), (3,6), (4,8), (-1,-2)\} \longrightarrow 0{,}5$ ⁉ ZLOMEK NENÍ RACIONÁLNÍ ČÍSLO

$\{(1,3), (2,6), (3,9), (4,12), \dots\}$

$\{(-1,2), (-2,4), \dots, (4,-8), \dots\}$

$\{(0,1), (0,-3), (0,156), \dots\} \longrightarrow 0$

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

$ad + bc = bd$

$(a,b) + (c,d) = (ad + bc, bd)$

$(a,b) \cdot (c,d) = (ac, bd)$

Korektnost

$(a,b) \sim (a',b')$ $\qquad (c,d) \sim (c',d')$ $\Rightarrow (ad + cb, bd) \sim (a'd' + c'b', b'd')$

$ab' = a'b \quad / dd'$ $\qquad cd' = c'd \quad / bb'$

$(ad + cb)b'd' = bd(a'd' + c'b')$

$adb'd' + cbb'd' = bda'd' + bdc'b'$

$ab'dd' = a'bdd'$

$cd'bb' = c'dbb'$

$(ac, bd) \sim (a'c', b'd')$

$acb'd' = bda'c'$

$(a,b),\ a \neq 0$

$(a,b) \cdot (b,a) = (ab, ba) = \underline{1}$

$(a,b) + (-a,b) = (ab - ab, bb) = \underline{0}$

$$S_d(n) = 1^d + 2^d + \dots + n^d = \sum_{x=1}^{n} x^d$$

$$S_{d+1}(n+1) = S_{d+1}(n) + (n+1)^{d+1}$$

$$= 1 + \sum_{x=1}^{n} (x+1)^{d+1} = 1 + \sum_{x=1}^{n} \sum_{r=0}^{d+1} \binom{d+1}{r} x^r =$$

$$= 1 + \sum_{x=1}^{n} \left(1 + \sum_{r=1}^{d-1} \binom{d+1}{r} x^r + (d+1) x^d + x^{d+1}\right) =$$

$$= 1 + n + \sum_{r=1}^{d-1} \binom{d+1}{r} S_r(n) + (d+1) \cdot S_d(n) + S_{d+1}(n)$$

$$S_d(n) = \frac{1}{d+1}\left((n+1)^{d+1} - 1 - n - \sum_{r=1}^{d-1} \binom{d+1}{r} S_r(n)\right)$$

$\underline{d=1:}$ $S_1(n) = 1 + 2 + \dots + n = \frac{1}{2}\left(n^2 + 2n + 1 - 1 - n\right) = \frac{1}{2}\left(n^2 + n\right) = \frac{n(n+1)}{2}$

$\underline{d=2:}$ $S_2(n) = 1^2 + 2^2 + \dots + n^2 = \frac{1}{3}\left(n^3 + 3n^2 + 3n + 1 - 1 - n - \binom{3}{1}\frac{n(n+1)}{2}\right) =$

$= \frac{1}{6} \cdot \left(2n^3 + 6n^2 + 4n - 3n^2 - 3n\right) = \frac{1}{6} \cdot \left(2n^3 + 3n^2 + n\right) = \frac{n \cdot (2n^2 + 3n + 1)}{6} =$

$= \frac{1}{6} \cdot n \cdot (n+1)(2n+1)$

LUCASŮV–LEHMERŮV TEST: M_p je prvočíslo $\Leftrightarrow$ M_p dělí S_{p-1}

F.E. LUCAS (1842–1891)
D.H. LEHMER (1905–1991)

$M_p = 2^p - 1$ Mersennovo číslo

$\{S_n\}_{n=1}^{\infty}$: $S_1 = 4$, $S_{n+1} = S_n^2 - 2$

$S_1 = 4$, $S_2 = 14$, $S_3 = 194$, $S_4 = 37\,634$, $S_5 = 1\,416\,317\,954$, ...

$M_5 = 31$ je prv. $\Leftrightarrow$ 31 dělí 37 634

$M_7 = 127$ je prv. $\Leftrightarrow$ 127 dělí S_6 (19 cifer)

$w = 2 + \sqrt{3}$ $\quad \bar{w} = 2 - \sqrt{3}$

Platí: $w + \bar{w} = 4$, $w \cdot \bar{w} = 1$

$S_n = w^{\cancel{k}^{n-1}} + \bar{w}^{\cancel{k}^{n-1}}$ $\left(w^{2^{n-1}} + \bar{w}^{2^{n-1}}\right)$

D. Indukcí

$n=1$: $S_1 = 4$, $S_1 = w + \bar{w}$

$n \to n+1$: $S_{n+1} = S_n^2 - 2 = \left(w^{2^{n-1}} + \bar{w}^{2^{n-1}}\right)^2 - 2 =$ $\cancel{w^{2^{n-1}} + 2w\bar{w}^{2^{n-1}} + \bar{w}^{2^{n-1}} - 2}$

$w \cdot \bar{w} = 1$

$= w^{2^n} + \bar{w}^{2^n} + 2 - 2 = w^{2^n} + \bar{w}^{2^n}$

D $\Leftarrow$ Předp., že M_p dělí S_{p-1} ($\Rightarrow M_p$ je prvočíslo)

$S_{p-1} = w^{2^{p-2}} + \bar{w}^{2^{p-2}} = A \cdot M_p$ $\quad / \cdot w^{2^{p-2}}$

$w^{2^{p-1}} + 1 = B \cdot M_p$

$w^{2^{p-1}} = B \cdot M_p - 1$ $\quad$ / umocníme na druhou

$w^{2^p} = C \cdot M_p + 1$

Sporem. Předp., že q je nejmenší prvočíslo, které dělí M_p.

a $q^2 \leq M_p$

$X = \{a + b\sqrt{3};\ a, b \in \mathbb{Z}_q\}$ má q^2 prvků

invertibilních může být maximálně $q^2 - 1$

Tvoří grupu. V ní leží w.

$w^{2^{p-1}} = q - 1$ v X $\quad w^{2^{p-1}} \neq 1$

$w^{2^p} = 1$ v X

V uvažované grupě invertibilních prvků leží prvky $w, w^2, w^3, w^4, \ldots\ldots w^{2^p}$ navzájem různé

$2^p \leq q^2 - 1 < M_p = 2^p - 1$ SPOR $\Rightarrow M_p \in \mathbb{P}$

$p \in \mathbb{P}$

~~M_p~~ $\wedge R$

$R_1 = 4 \quad R_{n+1} =$ Zbytek čísla $(R_n^2 - 2)$ při dělení M_p

$p = 5$ $\quad M_5 = 31$

$R_1 = 4 \quad R_2 = 14 \quad R_3 = 8, \quad \underline{R_4 = 0}$ $\Rightarrow$ 31 je prvočíslo

$194 = 31 \cdot 6 + 8 \qquad 62 = 31 \cdot 2 + 0$

$p = 7$ $\quad M_7 = 127$

$R_1 = 4 \quad R_2 = 14 \quad R_3 = 67 \quad R_4 = 42 \quad R_5 = 111 \quad \underline{R_6 = 0}$ $\Rightarrow$ 127 je prvočíslo

$194 = 127 \cdot 1 + 67 \qquad 4487 = 127 \cdot 35 + 42$

$67 \cdot 67$: 469, 402, 4489

$1762 = 127 \cdot 13 + 111$

$42 \cdot 42$: 84, 168, 1764

$111 \cdot 111$: 111, 111, 111, 12321

$12319 = 127 \cdot 97 + 0$

Grupa – množina s jednou binární operací (udsdobení $\cdot$), která je asociativní, existuje jednotkový prvek a ke každému prvku existuje prvek inverzní.

(MULTIPLIKATIVNÍ)

$(G, \cdot)$ $\quad \forall a,b,c \in G \;\; (a \cdot b) \cdot c = a \cdot (b \cdot c)$

$\exists 1 \in G \;\; \forall a \in G \;\; 1 \cdot a = a \cdot 1 = a$

$\forall a \in G \;\; \exists a^{-1} \in G \;\; a \cdot a^{-1} = a^{-1} \cdot a = 1$

(ADITIVNÍ) (sčítání +) nulový prvek, opačný prvek

$(G, +)$ $\quad \forall a,b,c \in G \;\; (a+b)+c = a+(b+c)$

$\exists 0 \in G \;\; \forall a \in G \;\; a+0 = 0+a = a$

$\forall a \in G \;\; \exists -a \in G \;\; a+(-a) = (-a)+a = 0$

$\forall a,b \in G \;\; a+b = b+a$

Komutativní (Abelova, abelovská) $\forall a,b \in G \;\; a \cdot b = b \cdot a$

gaussova celá čísla

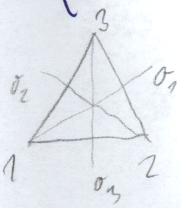
Př: $(\mathbb{Z}, +), (\mathbb{Q}, +), (\mathbb{R}, +), (\mathbb{C}, +), (\mathbb{Z}_{[i]}, +), (\mathbb{H}, +)$

~~$(\mathbb{N}, +)$~~

~~$(\mathbb{Z}, \cdot)$~~, ~~$(\mathbb{Q}, \cdot)$~~

$(\mathbb{Q} \setminus \{0\}, \cdot), (\mathbb{R} \setminus \{0\}, \cdot), (\mathbb{C} \setminus \{0\}, \cdot), (\mathbb{R}^+, \cdot),$ ~~$(\mathbb{R}^-, \cdot)$~~

$(\{z \in \mathbb{C};\ |z| = 1\}, \cdot)$



$r_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \quad o_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$

$r_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \quad o_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$

$r_3 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \quad o_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$

KERYHO TABULKA

$\circ$	r_1	r_2	r_3	o_1	o_2	o_3
r_1	r_1	r_2	r_3	o_1	o_2	o_3
r_2	r_2	r_3	r_1	o_2	o_3	o_1
r_3	r_3	r_1	r_2	o_3	o_1	o_2
o_1	o_1	o_3	o_2	r_1	r_2	r_3
o_2	o_2	o_1	o_3	r_2	r_1	r_3
o_3	o_3	o_2	o_1	r_3	r_3	r_1

$S_3 = \{r_1 = 1, r_2, r_3, o_1, o_2, o_3\}$

$\underline{1} = \{r_1\}$

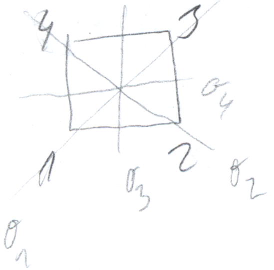
$R = \{r_1, r_2, r_3\}$

$O_1 = \{r_1, o_1\} \quad O_3 = \{r_1, o_3\}$

$O_2 = \{r_1, o_2\}$

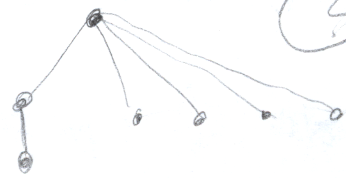
$\{r_2, o_1, r_1, r_3, o_2, o_3\}$

3



$\mu_1, \mu_2, \mu_3, \mu_4$

$\sigma_1, \sigma_2, \sigma_3, \sigma_4$



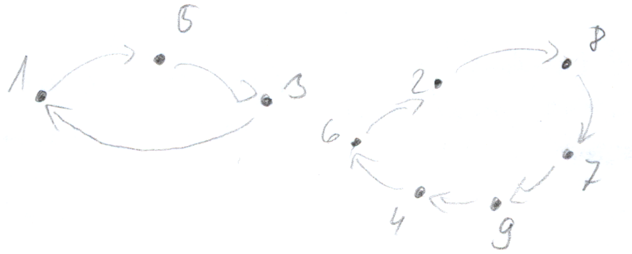
Def. Nechť M je konečná množina.
Permutací množiny M budeme rozumět každé vzájemně jednoznačné zobrazení (bijekci) M na M.

$M = \{1,2,3,\dots,n\}$ – předpokládáme

$P: M \xrightarrow[\text{bijekce}]{} M \qquad P = \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ P(1) & P(2) & P(3) & \dots & P(n) \end{pmatrix}$ – vzory – obrazy

Př. $P = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 5 & 8 & 1 & 6 & 3 & 2 & 9 & 7 & 4 \end{pmatrix}$

graf.



Skládání permutací:

$P, Q \qquad PQ$ nejprve Q, pak P

není komutativní

asociativní
jednotkový prvek – identita
inverzní prvek – ano!

$P^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 6 & 5 & 9 & 1 & 4 & 8 & 2 & 7 \end{pmatrix}$

S_n = grupa permutací n-prvkové množiny
symetrická grupa stupně n — řád grupy = počet prvků

S_n má $n!$ prvků

S_3 = symetrie Δ

Def. Inverzí permutace P budeme rozumět dvojici i,j takovou, že $i<j$ a $P(i)>P(j)$.
Počet inverzí permutace P značíme $\operatorname{in} P$.
Znaménko permutace P definujeme vztahem $\operatorname{sgn} P = (-1)^{\operatorname{in} P}$
Permutace P se nazývá sudá, resp. lichá, je-li $\operatorname{sgn} P = 1$, resp. $\operatorname{sgn} P = -1$.

Př. $P = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 7 & 6 & 9 & 1 & 2 & 4 & 5 & 8 \end{pmatrix}$ inverze $\{1,5\}$ $\{1,6\}$ ~~$\{2,5\}$~~

$\{2,3\}$ $\{2,5\}$ $\{2,6\}$ $\{2,7\}$ $\{2,8\}$
$\{3,5\}$ $\{3,6\}$ $\{3,7\}$ $\{3,8\}$
$\{4,5\}$ $\{4,6\}$ $\{4,7\}$ $\{4,8\}$ $\{4,9\}$

$2+5+4+5 = 16$

$\operatorname{in} P = 16$ $\quad \operatorname{sgn} P = (-1)^{16} = 1 \Rightarrow$ <u>P je sudá</u>

Věta: $\operatorname{sgn} PQ = \operatorname{sgn} P \cdot \operatorname{sgn} Q$

D.

všechny dvojice $i<j$			
$Q(i) < Q(j)$		$Q(i) > Q(j)$	
$PQ(i) < PQ(j)$	$PQ(i) > PQ(j)$	$PQ(i) > PQ(j)$	$PQ(i) < PQ(j)$

inverze P, inverze Q, inverze Q, inverze P, inverze PQ, ×

$\operatorname{in} PQ = \operatorname{in} P + \operatorname{in} Q - 2x$

$\operatorname{sgn} PQ = (-1)^{\operatorname{in} PQ} = (-1)^{\operatorname{in} P + \operatorname{in} Q - 2x} = (-1)^{\operatorname{in} P} \cdot (-1)^{\operatorname{in} Q} =$
$= \operatorname{sgn} P \cdot \operatorname{sgn} Q$

Důsledky: (i) Složení sudých permutací je sudá permutace
(dvou) lichých — sudá
+ složení sudé a liché — lichá

(ii) $S_n \xrightarrow{\text{bijekce}} S_n$, $P \mapsto P \cdot Q$ kde Q je pevně zvolená lichá permutace

$P_1 Q = P_2 Q \;/\cdot Q^{-1}$
$P_1 = P_2 \Rightarrow$ prostá
$PQ^{-1} \to P \in S_n$
$PQ^{-1} \to PQ^{-1}Q = P$ na

Sudých permutací je $\frac{n!}{2}$
lichých permutací je $\frac{n!}{2}$
$n>1$

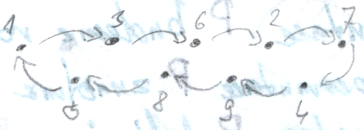
$S_1 = \{\begin{pmatrix} 1 \\ 1 \end{pmatrix}\}$

(iii) $\operatorname{sgn} P^{-1} = \operatorname{sgn} P$ $\quad P \cdot P^{-1} = 1$, $\operatorname{sgn} P \cdot \operatorname{sgn} P^{-1} = 1$ $\Rightarrow$ SUDÉ PERMUTACE TVOŘÍ PODGRUPU

(iv) Sudé permutace tvoří podgrupu v S_n, která má $\frac{n!}{2}$ prvků (pro $n>1$). Značí se obvykle A_n a nazývá se alternující grupa stupně n.

Zobrazení $\operatorname{sgn}: \underset{\text{grupa}}{S_n} \longrightarrow \underset{\text{grupa}}{\{1,-1\}}$
$\operatorname{sgn}(P \cdot Q) = \operatorname{sgn} P \cdot \operatorname{sgn} Q$ homomorfismus grup (epi) ($n>1$)

$$P = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 7 & 6 & 9 & 1 & 2 & 4 & 5 & 8 \end{pmatrix}$$



cyklická permutace
jednoduchý cyklus

rozklad na transpozice

$$P = (1,3,6,2,7,4,9,8,5) = (1,5)(1,8)(1,9)(1,4)(1,7)(1,2)(1,6)$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 5 & 2 & 3 & 4 & 1 & 6 & 7 & 8 & 9 \end{pmatrix} = (1,5)$$

KAŽDÁ TRANSPOZICE JE LICHÁ

Transpozice $\begin{pmatrix} 1 & \dots & i & \dots & j & \dots & n \\ 1 & \dots & j & \dots & i & \dots & n \end{pmatrix}$

je lichá!

$$\left.\begin{matrix} j-i \\ j-i-1 \end{matrix}\right\} \underline{2(j-i)-1} \quad \text{lichá}$$

PODLE POČTU TRANSPOZIC SE POZNÁ ZNAMÉNKO PERMUTACE

ROZKLAD NA NEZÁVISLÉ CYKLY

$$P = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 5 & 8 & 9 & 6 & 4 & 7 & 1 & 2 & 3 \end{pmatrix} = (1,5,4,6,7)(2,8)(3,9) =$$

transpozice

4 6 6 4 3 3 — 26

$sgn\, P = (-1)^{26} = 1$ (sudá)

$$= \underbrace{(1,7)(1,6)(1,4)(1,5)(2,8)(3,9)}_{6} =$$

$$= (4,6,7,1,5)(3,9)(8,2) =$$

$$= (4,5)(4,1)(4,7)(4,6)(3,9)(8,2) =$$

$$= (9,3)(6,7,1,5,4)(2,8) =$$

$$= (9,3)(6,4)(6,5)(6,1)(6,7)(2,8)(1,5)(5,1)$$

$sgn\, P = (-1)^{\text{počet transpozic}} = (-1)^6$

počet permutovaných prvků

$sgn\, P = (-1)^{n - \text{počet cyklů}} = (-1)^{9-3}$

$\to$ = počet transpozic

$$P^{1\,000\,000} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \end{pmatrix} - P$$

$P^{10} = id \Rightarrow$

$$P^{1\,000\,002} = P^2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 4 & 2 & 3 & 7 & 6 & 1 & 5 & 8 & 9 \end{pmatrix}$$

$$P^{1\,000\,002} = (P^{10})^{100\,000} \cdot P^2 = P^2$$

S_9, podgrupa $\langle P \rangle = \{id, P, \dots, P^9\}$ cyklická podgrupa ke grupě S_9

$\{id, P^2, P^4, P^6, P^8\}$
$\{id, P^5\}$
} podgrupy

Trojcyklus: (a,b,c) – cyklus délky 3.

$(a,b,c) = (a,c)(a,b)$ – sudý

trojcykly leží v A_n – alternující grupa

Věta: Trojcykly generují A_n. (Každá sudá permutace se dá složit z trojcyklů.)

D. Sudá permutace je složením sudého počtu transpozic. Ukážeme, že složení ~~dvou transpozic~~ je jeden nebo ~~dva~~ trojcykly.

$(i,j)(j,k) = (j,k,i)$

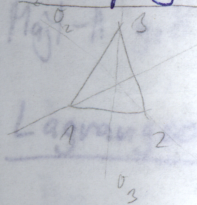
$(i,j)(k,l) = (k,i,j)(j,k,l)$

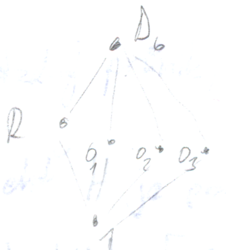
S_3 ... symetrie Δ ..... D_6

symetrie pravidelného n-úhelníku .... D_{2n}

dihedrální grupa

Svaz podgrup $D_6 = S_3$





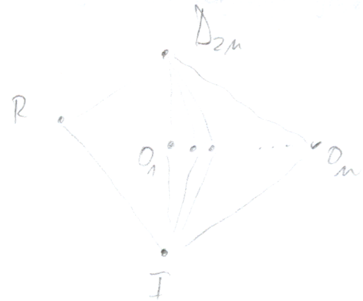
R – podgrupa rotací

O_1, O_2, O_3 – podgrupy z osových souměrností

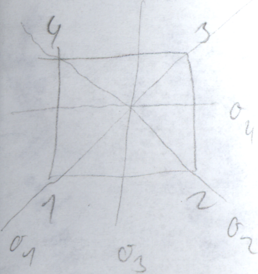
$O_1 = \{id, \sigma_1\}$, $O_2 = \{id, \sigma_2\}$, $O_3 = \{id, \sigma_3\}$

$R = \{id, r, r^2\}$

D_{2n}, $n \in P \setminus \{2\}$:



POČET PODGRUP DĚLÍ POČET PRVKŮ GRUPY



D_8 R – podgrupa rotací

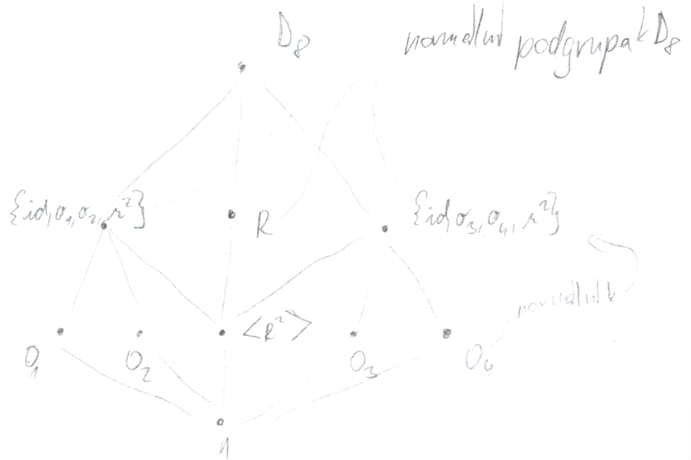
$R = \{id, r, r^2, r^3\}$

$\{id, r^2\}$

$\{id, \sigma_1\}, \{id, \sigma_2\}, \{id, \sigma_3\}, \{id, \sigma_4\}$

$O_1 =$ $O_2 =$

normální podgrupa k D_8



$\sigma_1 r^2 = \sigma_2$

$r^2 \sigma_1 = \sigma_2$

$r^2 \sigma_2 = \sigma_1$

$\sigma_2 r^2 = \sigma_1$

G – grupa, H – podgrupa, $g \in G$

$gH = \{gh ; h \in H\}$ $g \in gH$

Bijekce H na gH — levé třídy (Hg ... pravé třídy)

$h \longmapsto gh$

$gh_1 \overset{?}{=} gh_2$ $| \cdot g^{-1}$

$g^{-1}gh_1 = g^{-1}gh_2$

$h_1 = h_2$

Pokud $gH = Hg \Rightarrow H$ ... normální podgrupa

- všechny podgrupy podgrupy stejně velké

G konečná $\Rightarrow H$ a gH mají stejný počet prvků

$x \in g_1H \cap g_2H \Rightarrow x = g_1h_1 = g_2h_2 \rightarrow g_2^{-1}g_1 = h_2h_1^{-1} \in H$

g_1H a g_2H mají společný prvek $x \Rightarrow g_2^{-1}g_1 \in H$

Potom $g_1H = g_2H$!

$g_1h \in g_1H$

$g_1h = g_2\underbrace{g_2^{-1}g_1h}_{\in H} \in g_2H$

$g_2h \in g_2H$

$g_2h = g_1\underbrace{g_1^{-1}g_2h}_{\in H} \in g_1H$

Mají-li g_1H a g_2H neprázdný průnik, pak se rovnají.

Lagrangeova věta: Nechť H je podgrupa konečné grupy G. Potom

$$\underbrace{|G|}_{\text{řád grupy } G} = \underbrace{|H|}_{\text{řád podgrupy } H} \cdot \underbrace{[G:H]}_{\text{index podgrupy } H \text{ v grupě } G}$$

počet prvků grupy

S_3 – symetrická grupa stupně 3
– grupa permutací množiny $\{1,2,3\}$

$(1, 4, \omega, 2z, 3, \omega, z)$

$(1, 4, 0, 0, 3, 0, 0) + [(1, 4,$

$S_3 = D_6$ – symetrie Δ

~~$S_3 = \{(1,2,3), (2,3,1), (3,1,2), (1,3,2), (3,2,1), (2,1,3)\}$~~

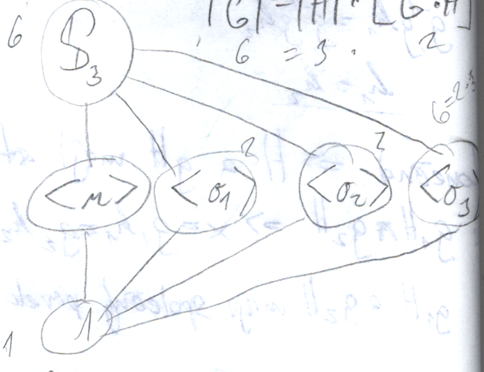
$$\boxed{S_3 = \left\{ \underset{id}{\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}}, \underset{r}{\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}}, \underset{r^2}{\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}}, \underset{\sigma_1}{\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}}, \underset{\sigma_2}{\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}}, \underset{\sigma_3}{\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}} \right\}}$$

G

$\circ$	~~id~~ 1	r	r^2	σ_1	σ_2	σ_3
1	~~id~~ 1	r	r^2	σ_1	σ_2	σ_3
r	r	r^2	~~id~~ 1	σ_3	σ_1	σ_2
r^2	r^2	~~id~~ 1	r	σ_2	σ_3	σ_1
σ_1	σ_1	σ_2	σ_3	1	r	r^2
σ_2	σ_2	σ_3	σ_1	r^2	1	r
σ_3	σ_3	σ_1	σ_2	r	r^2	1

$|G| = |H| \cdot [G:H]$

$6 = 3 \cdot 2$



$G, \; H \subset G$ (podgrupa), $\; g \in G$

$g \cdot H$ levá třída

Levý rozklad S_3 podle $\overset{H}{\langle \sigma_1 \rangle}$:

$g \cdot H$

$S \quad \underbrace{\{1, \sigma_1\}}_{H}, \{\underset{g\cdot 1}{r}, \underset{g\cdot\sigma_1}{\sigma_3}\}, \{r^2, \sigma_2\}, \{\sigma_1, 1\}$

$S_3 = \{1, \sigma_1\} \cup \{r, \sigma_3\} \cup \{r^2, \sigma_2\}$

Pravý rozklad S_3 podle $\langle \sigma_1 \rangle$:

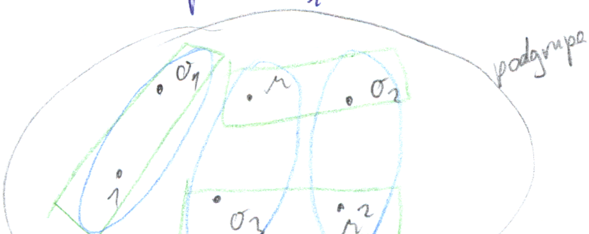
$H \cdot g$

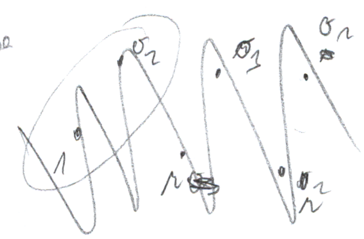
$\{1, \sigma_1\}, \{r, \sigma_2\}, \{r^2, \sigma_3\}$

$S_3 = \{1, \sigma_1\} \cup \{r, \sigma_2\} \cup \{r^2, \sigma_3\}$

Levý rozklad ~~je různý~~ $\neq$ pravý rozklad

$\Rightarrow$ ~~pod~~ $\langle \sigma_1 \rangle$ není normální grupou v S_3





třídy

v komutativní grupě je každá podgrupa normální

H je normální v G, je-li $\forall g \in G \; gH = Hg$

G/H – faktorová množina

$\boxed{g_1 H \cdot g_2 H \overset{def}{=} g_1 g_2 \cdot H}$ Definice operace na faktorové množině

$H = 1 \cdot H$

$g^{-1} \cdot g \cdot H = 1 \cdot H$

$g_1 = g_1' h_1$ protože $\in H$

$g_2 = g_2' h_2$ $\quad h_2 \in H$

$g_1 H = g_1' H$

$g_2 H = g_2' H$

$g_1' H \cdot g_2' H = g_1' \cdot g_2' H = g_1 h_1 g_2 h_2 H = \ldots$

$h_1 g_2 \in H g_2 = g_2 H \Rightarrow h_1 g_2 = \ldots$

$S_3/_N$ ... faktorová grupa S_3

$\langle N \rangle = A$

$\{o_1, o_2, o_3\}$

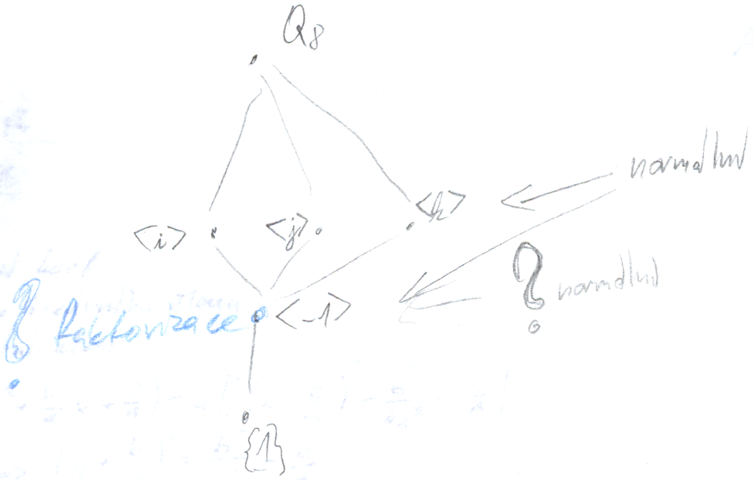
$\Downarrow$

$o_1 < N >$

kvaternionová grupa

$Q_8 = \{1, i, j, k, -1, -i, -j, -k\}$

$\{1\}, \{1,-1\}, \{i,-1,+1,i\}\ \{j,-1,1,-j\}\{k,-1,1,-k\}$



D_8 ... □

D_{10} ... ⬠

ZÁKLADY

Lineární rovnice

$x^3+ax^2+bx+c=0$

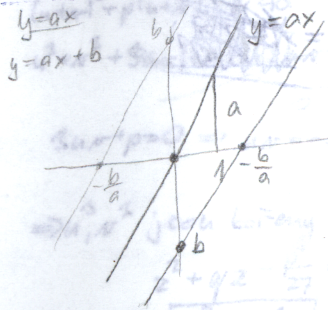
$ax+b=0$

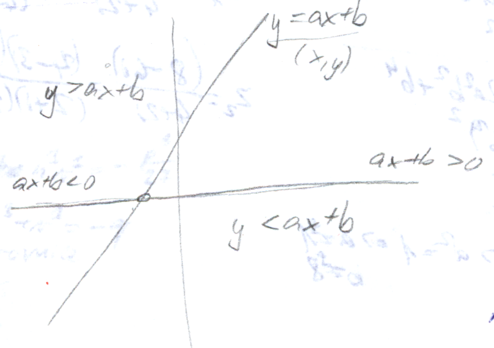
$a\neq 0$ a – vedoucí koeficient

b – absolutní člen

kořen $x=-\frac{b}{a}=a^{-1}\cdot(-b)$

Řešíme nad polem (komutat. tělesem) $\mathbb{Q},\mathbb{R},\mathbb{C}$





nad $\mathbb{Z}$: $3x+2=0$ nemá řešení

$3x+6=0$ má jedno řešení

nad $\mathbb{Z}_6$: $3x+4=0$ nemá

$4x+2=0$ 1,4 má dvě řešení

$\mathbb{Z}$ je obor integrity

NEMÁ NETRIV. DĚLITELE NULY

Každá lin. rovnice má nejvýše jedno řešení!

$ax_1+b=ax_2+b \Rightarrow a(x_1-x_2)=0$

$\Rightarrow x_1-x_2=0$

Matice $T^{n\times n}$

$\underset{n\times n}{A}\underset{n\times n}{X}+\underset{n\times n}{B}=\underset{n\times n}{0}$

$AX=-B$

Lineární nerovnice

Kvadratické rovnice

$ax^2+bx+c=0$

$a\neq 0$ a – vedoucí koef.

b – koef. u lineárního členu

c – absolutní člen

$ax^2+bx+c=a\left(x^2+\frac{b}{a}x+\frac{c}{a}\right)=a\left[\left(x+\frac{b}{2a}\right)^2-\frac{b^2}{4a^2}+\frac{c}{a}\right]$

$ax^2+bx+c=0 \Rightarrow \left(x+\frac{b}{2a}\right)^2=\frac{b^2}{4a^2}-\frac{c}{a}$

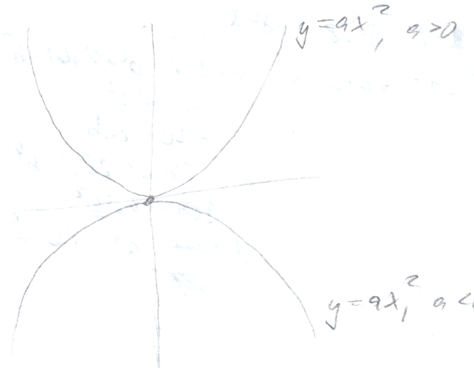
$x+\frac{b}{2a}=\pm\sqrt{\frac{b^2-4ac}{4a^2}} \Rightarrow x_{1,2}=\frac{-b\pm\sqrt{b^2-4ac}}{2a}$

$D=b^2-4ac$ diskriminant

$D>0$ 2 řešení (reálná)

$D=0$ 1 řešení (reálné)

$D<0$ 2 imaginární řešení



$y=ax^2+bx+c$

$y'=2ax+b$

$y'=0 \Rightarrow x_0=-\frac{b}{2a}$ $y_0=\frac{ab^2}{4a^2}-\frac{b^2}{2a}+c=c-\frac{b^2}{4a}$

$y'(0)=b$ $=-\frac{D}{4a}$

Vietovy vzorce

$x^2+bx+c=0$

$x_1+x_2=-b$

$x_1\cdot x_2=c$

$(x-x_1)(x-x_2)=0$

$x^2-x(x_1+x_2)+x_1\cdot x_2$

$x^2+x\underbrace{(-x_1-x_2)}_{b}+\underbrace{x_1x_2}_{c}$

~~$(2+i)z^2-(9+2i)z+5$~~

$x_1^2+2x_1x_2+x_2^2=b^2$

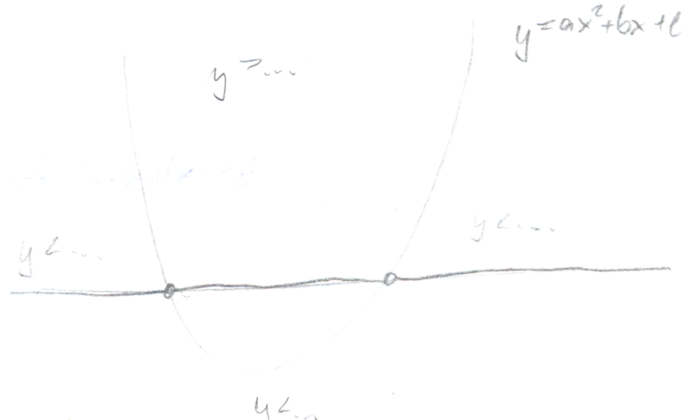
$-4x_1x_2=-4c$

$x_1^2-2x_1x_2+x_2^2=b^2-4c$

$(x_1-x_2)^2=b^2-4c$

$x_1-x_2=\sqrt{b^2-4c}$ $x_{1,2}=\frac{-b\pm\sqrt{b^2-4c}}{2}$

$x_1+x_2=-b$



$ax^2+bx+c>0$

<0

$x+y=10$

$x\cdot y=16$

$x^2+2xy+y^2=100$

$-4xy=-64$

$(x-y)^2=36$

$x-y=\pm 6$

$x+y=10$

$2x=16|4$

$x=8|2 \Rightarrow y=2|8$

$(2+i)z^2-(9+2i)z+5(3-i)=0$

$D = 81+36i-4\cdot\cancel{20}(7+i) = -63+16i$

$\sqrt{-63+16i} = a+bi \Rightarrow -63+16i = a^2+2abi-b^2$

$-63 = a^2-b^2$

$16i = 2abi$

$63^2 = a^4-2a^2b^2+b^4$

$16^2 = 4a^2b^2$

$16^2+63^2 = a^4+2a^2b^2+b^4$

$65^2 = (a^2+b^2)^2$

$65 = a^2+b^2$

$-63 = a^2-b^2$

$2 = 2a^2 \Rightarrow a^2 = 1 \Rightarrow a = \pm 1$

$b = \pm 8$

$z_{1,2} = \frac{9+2i \pm (1+8i)}{4+2i}$

$z_1 = \frac{10+10i}{4+2i} = \frac{10(1+i)(4-2i)}{(4+2i)(4-2i)} = \frac{10(6+2i)}{20} = 3+i$

$z_2 = \frac{(8-6i)}{4+2i} = \frac{(4-3i)(2-i)}{(2+i)(2-i)} = \frac{5-10i}{5} = 1-2i$

$z^2+(1-i)z+4+7i=0$

$D = 1-2i-8-28i = -8-30i$

$\sqrt{-8-30i} = a+bi \Rightarrow -8-30i = a^2+2abi-b^2$

$-8 = a^2-b^2$

$-30 = 2ab$

$64 = a^4-2a^2b^2+b^4$

$900 = 4a^2b^2$

$964 = a^4+2a^2b^2+b^4 = (a^2+b^2)^2$

$964 = 2\cdot 2\cdot 241$

Kubická rovnice $x^3+ax^2+bx+c=0$

jak se y, q dostane z a, b, c?

substituce

$y = x - \frac{a}{3} \Rightarrow \boxed{y^2+py+q=0}$

$x^3+px+q=0$ $\quad (x^2+p)x=-q$

$x=u+v$

$(u+v)^3+p(u+v)+q=0$

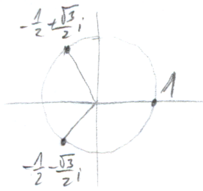
$u^3+v^3+\cancel{3uv}(u+v)\underbrace{(3uv+p)}_{=0}+q=0$

$3uv+p=0 \Rightarrow uv=-\frac{p}{3} \Rightarrow u^3v^3=-\frac{p^3}{27}$

$u^3+v^3=-q$

$\Rightarrow u^3, v^3$ jsou kořeny kvadratické rovnice

$z^2+qz-\frac{p^3}{27}=0$



$u^3=-\frac{q}{2}+\sqrt{\frac{q^2}{4}+\frac{p^3}{27}}$

$v^3=-\frac{q}{2}-\sqrt{\frac{q^2}{4}+\frac{p^3}{27}}$

$u=\sqrt[3]{-\frac{q}{2}+\sqrt{\frac{q^2}{4}+\frac{p^3}{27}}}$ $\quad$ VOLÍME $\sqrt[3]{\ }$ TAK, ABY $u \cdot v = -\frac{p}{3}$

$v=\sqrt[3]{-\frac{q}{2}-\sqrt{\frac{q^2}{4}+\frac{p^3}{27}}}$

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

$f'(x)=3x^2+p$

$f'(x)=0 \Rightarrow x=\pm\sqrt{-\frac{p}{3}}$ pro $p<0$

$p>0 \Rightarrow f$ je rostoucí $\Rightarrow$ jeden reálný kořen

$f''(x)=6x \Rightarrow$ inf. bod pro $x=0$

$x_1=u \cdot v$

$x_2=u\varepsilon+v\varepsilon^2$

$x_3=u\varepsilon^2+v\varepsilon$

$\varepsilon=-\frac{1}{2}+\frac{\sqrt{3}}{2}i$

$x_\alpha=+\sqrt{\frac{-p}{3}}$ $\quad f(x_\alpha)=\sqrt{-\frac{p}{3}}\cdot\left(-\frac{p}{3}+p\right)+q$ $\quad f(x_\alpha)\cdot f(x_\beta)=\frac{p}{3}\cdot\frac{4}{9}p^2+q\sqrt{-\frac{p}{3}}\cdot\frac{2p}{3}-q\sqrt{-\frac{p}{3}}\cdot\frac{2p}{3}+q^2=$

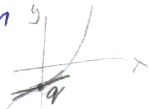
$x_\beta=-\sqrt{\frac{-p}{3}}$ $\quad f(x_\beta)=-\sqrt{-\frac{p}{3}}\cdot\left(-\frac{p}{3}+p\right)+q$ $\quad =q^2+\frac{4p^3}{27}=4\cdot\Delta$ $\quad \Delta$ - diskriminant

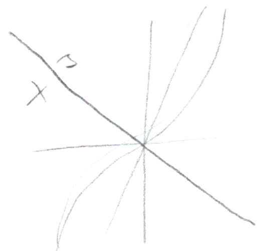
$p<0$

Diskuse: $p>0 \Rightarrow$ Jeden reálný kořen

$q>0 \Rightarrow$ záporný

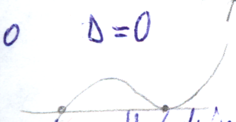
$q<0 \Rightarrow$ kladný





$p<0$ $\quad D>0$

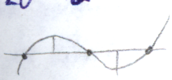
$p<0$ $\quad \Delta=0$



jeden reálný dvojnásobný

jeden reálný jednoduchý

$p<0$ $\quad \Delta<0$ $\quad$ CASUS IRREDUCIBILIS (nerozložitelný případ)



Vietovy vzorce: x_1, x_2, x_3 $\quad x^3+ax^2+bx+c=(x-x_1)(x-x_2)(x-x_3)$

$x_1+x_2+x_3=-a$

$x_1x_2+x_1x_3+x_2x_3=b$

$x_1x_2x_3=-c$

$2z^3-9z^2+18z-7=0$ $\quad 6z^2+18z+18$ změna v 0 je 18

Substituce: $z=\frac{y}{2}$ $\quad 12z-18$

$y^3-9y^2+36y-28=0$

Substituce: $y=x+3$ $\quad x^n+ax^{n-1}+\dots\dots=0$

$x^3+9x+26=0$ $\quad p>1 \Rightarrow 1$ vedl. kořen $\quad x=z-\frac{a}{n}$

$u=1$ $\quad z_1=\frac{1}{2}$

$v=-3$ $\quad z_2=2+\sqrt{3}i$

$2k: u\cdot v=-\frac{p}{3}$ ✓ $\quad z_3=2-\sqrt{3}i$

$x^3-15x-4=0$ $\quad p<0, D<0$

$u=\sqrt[3]{2+\sqrt{4-125}}=\sqrt[3]{2+11i}$ $\quad x=\sqrt[3]{\ }+\sqrt[3]{\ }$

$v=\quad=\sqrt[3]{2-11i}$ $\quad$ CARDANŮV VZOREC

$x^3-3x-52=0$ $\quad p<0, D>0$

Základní věta algebry: Algebraická rovnice (stupně alespoň 1) s komplexními (tedy i reálnými) koeficienty má v poli komplexních čísel alespoň jeden kořen.

[Polynomem stupně alespoň 1 s komplexními (tedy i reálnými) koeficienty má v poli komplexních čísel alespoň jeden kořen.]

Lemma: Jestliže má polynom f v poli T kořen α, potom je $f(x)=(x-\alpha)\cdot g(x)$, kde g je polynom nad T.

D. $f(\alpha)=0$ (tj. α je kořenem polynomu f)

$f(x)=(x-\alpha)\cdot g(x)+r(x)$, kde polynom $r(x)$ má menší stupeň než polynom $(x-\alpha)$, tj. $r(x)$ má stupeň 0, tj. je to konstanta $(r(x)=r\in T)$

$0=f(\alpha)=r \Rightarrow f(x)=(x-\alpha)\cdot g(x)$ (stupeň $g(x)$ je o jedničku menší než stupeň $f(x)$)

Věta Je-li $a_0x^n+a_1x^{n-1}+\dots+a_{n-1}x+a_n$ polynom stupně n s komplexními koeficienty (nad $\mathbb{C}$), potom existují $\alpha_1,\dots,\alpha_n\in\mathbb{C}$ tak, že $a_0x^n+\dots+a_n=a_0(x-\alpha_1)(x-\alpha_2)\dots(x-\alpha_n)$.

Pozn. Polynom s kompl. (reál.) koef. je nad $\mathbb{C}$ rozložitelný až na lineární faktory.

Poznámka Polynom s reálnými koeficienty, který má lichý stupeň, má alespoň jeden reálný kořen.

Lemma: Má-li polynom s reálnými koeficienty kořen α má také kořen $\bar{\alpha}$.

D. $f(x)=a_0x^n+a_1x^{n-1}+\dots+a_n$

α je kořen $\Rightarrow f(\alpha)=0=a_0\alpha^n+\dots+a_n$

$0=\bar{0}=\overline{a_0\alpha^n+\dots+a_n}=\overline{a_0\alpha^n}+\overline{a_1\alpha^{n-1}}+\dots+\overline{a_n}=\underbrace{\bar{a}_0\bar{\alpha}^n+\bar{a}_1\bar{\alpha}^{n-1}+\dots+\bar{a}_n}_{0=f(\bar{\alpha})}$

Pozn. S imaginárními koeficienty NEPLATÍ $(x-i)(x-2i)=x^2-3ix-2$

Věta Je-li $a_0x^n+a_1x^{n-1}+\dots+a_{n-1}x+a_n$ polynom stupně n s reálnými koeficienty (nad $\mathbb{R}$), potom $a_0x^n+\dots+a_n=a_0(x-\alpha_1)\dots(x-\alpha_k)(x^2+\beta_1x+\gamma_1)\dots(x^2+\beta_lx+\gamma_l)$, kde $k\geq0$, $l\geq0$, všechna $\alpha,\beta,\gamma\in\mathbb{R}$.

Polynomem s reálnými koeficienty jde nad $\mathbb{R}$ rozložit na reálné lineární a kvadratické polynomy.

D. $(x-(a+bi))(x-(a-bi))=x^2-2ax+(a^2+b^2)$ – reálný kvadrat. polynom

$D=4a^2-4a^2-4b^2=-4b^2<0$

$x_{1,2}=a\pm bi$

Věta Má-li $a_0x^n+a_1x^{n-1}+\dots+a_{n-1}x+a_n$ s celočíselnými koeficienty kořen $\frac{p}{q}$, kde $p,q\in\mathbb{Z}$, $(p,q)=1$ (nesoudělná), potom $p\mid a_n$, $q\mid a_0$.

D. $a_0\frac{p^n}{q^n}+a_1\frac{p^{n-1}}{q^{n-1}}+\dots+a_{n-1}\frac{p}{q}+a_n=0 \quad /\cdot q^n$

$a_0p^n+a_1p^{n-1}q+\dots+a_{n-1}pq^{n-1}+a_nq^n=0$

dělitelné p $\Rightarrow p\mid a_nq^n\Rightarrow p\mid a_n$

dělitelné q $\Rightarrow q\mid a_0p^n\Rightarrow q\mid a_0$

Důsledek Má-li polynom $x^n+a_1x^{n-1}+\dots+a_n$ celočíselné koeficienty, je každý racionální kořen již celočíselný a je to dělitel koeficientu a_n.

D. $a_0=1 \Rightarrow q=1\Rightarrow$ kořen p dělí a_n.

př. $x^3+2x-7=0$ racion. kořeny? ±1, ±7

nemá žádný racionální kořen!

$x^2-x-12=(x+3)(x-4)$

$(x^3+9x^2+9x+8):(x+8)=x^2+x+1 \qquad x_1=-8$

$-x^3-8x^2$

x^2+9x+8

$-x^2-8x$

$x+8$

$2x^3-9x^2+18x-7=0 \quad \pm1, \pm7, \pm\frac{1}{2}, \pm\frac{7}{2}$

$x_1=\frac{1}{2}$

$(2x^3-9x^2+18x-7):(x-\frac{1}{2})=2x^2-10x+13$

$-2x^3-\cancel{x^2} \qquad +10x^2-5x$

$-10x^2+18x-7 \qquad 13x-7$

$x^3-9x-28=0 \quad \pm1, \pm2, \pm4, \pm7, \pm14, \pm28$

$x_1=4$

$x^3+30x+30=0 \quad \pm1, \pm2, \pm3, \pm5, \pm6, \pm10$

$x^3-15x-4=0 \quad \pm1, \pm2, \pm4$

$x_1=4$

$Z_7 \quad x^2+3x+2=(x+1)(x+2) \quad x_1=5, \; x_2=6$

kvaterniony $\quad x^2+1=0$ – ∞ ŘEŠENÍ

$Z_3 \quad x^2+x+2=0$ NEMÁ ŘEŠENÍ

$x^2+x+1=0$ má kořen $\underline{1}$

$Z_6 \quad x^2+3x+2=(x+1)(x+2)=(x+4)(x+5)$

$Z_9 \quad 6x+1=0$ nemá řeš.

$x^n+a_1x^{n-1}+\ldots\ldots=0$ Vietovy vzorce obecně,

$\boxed{x=z-\frac{a_1}{n}}$

$4x^4-24x^3+57x^2+18x-45=0 \quad ?\,x$

$x_1=3+i\sqrt{6}$

$x_2=3-i\sqrt{6}$

$(4x^4-24x^3+57x^2+18x-45):(x^2-6x+15)=4x^2-3=0$

$(x-3-i\sqrt{6})(x-3+i\sqrt{6})=x^2-6x+15$

$\Rightarrow x_{3,4}=\pm\frac{\sqrt{3}}{2}$

$x^2-xy+y^2=7$

$\cancel{(5-y)^2-(5-y)y+y^2=7}$

$x^3+y^3=35$

$(x+y)(x^2-xy+y^2)=35$

$x+y=\frac{35}{7}=5 \qquad (x+y)^2=25$

$\cancel{x=5-y}$

$x^2+2xy+y^2=25$

$3xy=18$

$xy=6 \qquad 1\cdot4$

$\cancel{x^2y^2=36}$

$x^2-2xy+y^2=1 \qquad x_1=2 \quad x_2=3$

$(x-y)^2=1 \qquad y_1=3 \quad y_2=3$

$x-y=\pm1$

$x^3+y^3=7$

$xy(x+y)=-2$

$(x+y)(x^2-xy+y^2)=7$

$\cancel{(x+y)(x^2+y^2)=5}$

$(x+y)^3=x^3+3x^2y+3xy^2+y^3$

$x^2y+xy^2=-2 \quad / \cdot 3$

$(x+y)^3=1$

$x+y=1 \qquad x+y=-\frac{1}{2}\pm\frac{\sqrt{3}}{2}i$

$xy=-2 \qquad xy\left(-\frac{1}{2}\pm\frac{\sqrt{3}}{2}i\right)=-2$

$xy=-2\cdot\frac{1}{-\frac{1}{2}\pm\frac{\sqrt{3}}{2}i}=-2\cdot\frac{2}{-1\pm\sqrt{3}i}=-\frac{4}{-1\pm\sqrt{3}i}\cdot\frac{(-1\mp\sqrt{3}i)}{(-1\mp\sqrt{3}i)}$ $\frac{-4\pm4\sqrt{3}i}{-4}$, $\frac{-4\mp4\sqrt{3}i}{-4}$ $=1\pm\sqrt{3}i$

$x+y=-\frac{1}{2}+\frac{\sqrt{3}}{2}i \qquad x+y=-\frac{1}{2}-\frac{\sqrt{3}}{2}i$

$xy=1+\sqrt{3}i \quad 1\cdot4 \qquad xy=1-\sqrt{3}i$

$(x-y)^2$

$(x+y)^2=-\frac{1}{4}+\frac{\sqrt{3}}{2}i$

$x^2-2xy+y^2=-\frac{17}{4}-\frac{7\sqrt{3}}{2}i$

$x^2+xy+y^2=84 \qquad xy\geq 0$

$x+\sqrt{xy}+y=14$

$x+y=14-\sqrt{xy}$

$x^2+2xy+y^2=196-28\sqrt{xy}+xy$

$x^2+xy+y^2=196-28\sqrt{xy}$

$196-28\sqrt{xy}=84$

$28\sqrt{xy}=112$

$\sqrt{xy}=\frac{56}{14}=\frac{28}{7}=4 \Rightarrow xy=16$

$(x+y)^2-(\sqrt{xy})^2=84$

$(x+y+\sqrt{xy})(x+y-\sqrt{xy})=84$

$(x+y-\sqrt{xy})=6$

$2\sqrt{xy}=8 \Rightarrow xy=16$

$x^2+2xy+y^2=84+16$

$x+y=\pm10$

$x^2-2xy+y^2=84-48=36$

$x-y=\pm6$

$\boxed{2x=16 \quad x_1=8\Rightarrow y_1=2 \\ 2x=4 \quad x_2=2\Rightarrow y_2=8}$

$\cancel{2x=-4 \quad x_3=-2\Rightarrow y_3=-8}$

$\cancel{2x=-16 \quad x_4=-8\Rightarrow y_4=-2}$

$x^4+x^3+x^2+x=1$

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

$x^4+x^3+x^2+x+1=0$

$(x^4+1)+(x^3+x)+x^2=0 \quad /:x^2$

$\left(x^2+\frac{1}{x^2}\right)+\left(x+\frac{1}{x}\right)+1=0 \qquad y=x+\frac{1}{x}$

$y^2=x^2+2+\frac{1}{x^2}$

$(y^2-2)+y+1=0$

$y^2+y-1=0 \qquad \cancel{\left(y+\frac{1-\sqrt{5}}{2}\right)\left(y+\frac{1+\sqrt{5}}{2}\right)}$

$y_{1,2}=\frac{-1\pm\sqrt{5}}{2}$

$x+\frac{1}{x}=\frac{-1\pm\sqrt{5}}{2}$

$x^2+1=-\frac{x}{2}\pm\frac{\sqrt{5}}{2}x$

$x^2+x\left(\frac{1}{2}\mp\frac{\sqrt{5}}{2}\right)+1=0$

$x_{1,2,3,4}=\frac{-\frac{1\mp\sqrt{5}}{2}\pm\sqrt{\frac{6\mp2\sqrt{5}}{4}-4}}{2}=-\frac{1\mp\sqrt{5}}{4}\pm\frac{\sqrt{\frac{\mp2\sqrt{5}-10}{4}}}{2}$

$x_{1,2,3,4}=\frac{1}{4}\left(1\pm\sqrt{5}\pm i\sqrt{+10\pm2\sqrt{5}}\right)$

$x^5 - 19x^4 + 76x^3 - 76x^2 + 19x - 1 = 0$ $\quad x_1 = 1$

$18 \cdot 18 = 144$, 324 $\quad 192 = 2^2 \cdot 2^2 \cdot 2^2 \cdot 3$

~~$(x^5-1) - 19(x^4 - x) + 76(x^3 - x^2) = 0$~~

$(x^5 - 19x^4 + 76x^3 - 76x^2 + 19x - 1) : (x-1) = x^4 - 18x^3 + 58x^2 - 18x + 1 = 0$

$-18x^4 \quad 58x^3 \quad -18x^2 \quad +x$

$(x^4+1) - 18(x^3+x) + 58x^2 = 0$

$(x^2 + \frac{1}{x^2}) - 18(x+\frac{1}{x}) + 58 = 0$ $\quad x + \frac{1}{x} = y \quad y^2 = x^2 + \frac{1}{x^2} + 2$

$(y^2-2) - 18y + 58 = 0$

$y^2 - 18y + 56 = 0$

$y_{1,2} = \frac{18 \pm \sqrt{100}}{2} \Big< \begin{matrix} 14 \\ 4 \end{matrix}$

14: $x^2 - 14x + 1 = 0$, $x_{2,3} = \frac{14 \pm \sqrt{192}}{2} = \frac{14 \pm 8\sqrt{3}}{2} \Big< \begin{matrix} x_2 = \\ x_3 = \end{matrix}$

4: $x^2 - 4x + 1 = 0$, $x_{4,5} = \frac{4 \pm \sqrt{12}}{2} = \frac{4 \pm 2\sqrt{3}}{2} \Big< \begin{matrix} x_4 = 2 \\ x_5 = 2 \end{matrix}$

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

reciprokí 1. druhu $a_0 = a_n,\ a_1 = a_{n-1}, \dots$

2. druhu $a_0 = -a_n,\ a_1 = -a_{n-1}, \dots$

1. druhu: $x^n f(\frac{1}{x}) = f(x)$ (ekvival. podm.)

2. druhu: $x^n f(\frac{1}{x}) = -f(x)$ — " —

1. druhu, n liché $\Rightarrow$ koren -1. $\quad$ — 2. druhu, n sudé $\Rightarrow$ prostredný koren vypadne

2. druhu, ~~...~~ $\Rightarrow$ koren $+1$.

koren $\alpha \longrightarrow \frac{1}{\alpha}$

$f(x) = (x-1)\cdot g(x) = x^n f(\frac{1}{x}) = -x^n(\frac{1}{x} - 1)\cdot g(\frac{1}{x})$

$(x-1)g(x) = (1-x)(-x^{n-1})g(\frac{1}{x})$

$\boxed{g(x) = x^{n-1} g(\frac{1}{x})}$

2. druh vydelíme $(x-1) \rightarrow$ 1. druh □

$x^6 - x^5 + x^4 - x^2 + x - 1 = 0$ $\quad x_1 = 1$

$(x^6 - x^5 + x^4 - x^2 + x - 1) : (x-1) = x^5 + 2x^4 + 3x^3$

~~$2x^5 \quad 3x^4$~~

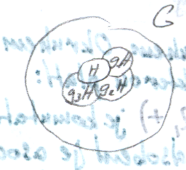
Def. Podgrupa H grupy G se nazývá <u>normální</u>, jestliže platí následující navzájem ekvivalentní podmínky:

(i) $\forall g \in G \quad gH = Hg$ (levý rozklad = pravý rozklad)

(ii) $\forall g \in G \quad g^{-1}Hg = H$

(iii) $\forall g \in G \quad g^{-1}Hg \subset H$ (podgrupa H obsahuje s každým svým prvkem všechny prvky s ním konjugované)

$h \ldots\ldots g^{-1}hg$ – konjugovaný s prvkem h



Je-li $g^{-1}Hg \subset H \quad \forall g \in G$ potom

$g^{-1}Hg = H \quad \forall g \in G.$

D. Musíme dokázat, že $H \subset g^{-1}Hg$ pro $\forall g \in G$

$h \in H \quad h = g^{-1}\underbrace{ghg^{-1}}_{\in H}g = g^{-1}h'g \in g^{-1}Hg$

$H \subset g^{-1}Hg$

$(g^{-1})^{-1}hg^{-1}$

Př. V abelovské grupě je každá podgrupa normální. Podgrupa indexu 2 je normální.

$A_n \subset S_n$ (A_n je podgrupa indexu 2)

D_{2n} ... podgrupa rotací je normální

Grupa kvaternionů (nekomutativní) má zajímavou vlastnost – všechny její podgrupy jsou normální.

Faktorová grupa G/H grupy G podle <u>normální</u> podgrupy H.

<u>Operace násobení:</u> $(g_1H)\cdot(g_2H) \overset{def}{=} g_1g_2H$

Korektnost definice:

$g_1H = g_1'H \iff g_1^{-1}\cdot g_1' \in H$

$g_2H = g_2'H \iff g_2^{-1}\cdot g_2' \in H$

$g_1g_2H = g_1'g_2'H \Leftarrow (g_1g_2)^{-1}\cdot g_1'g_2' \in H$

$(g_1g_2)^{-1}\cdot g_1'g_2' = g_2^{-1}\underbrace{g_1^{-1}g_1'}_{\in H}g_2' = g_2^{-1}hg_2' = \underbrace{g_2^{-1}hg_2}_{\in H}\underbrace{g_2^{-1}g_2'}_{\in H}$

<u>Homomorfismus grup:</u> $\varphi: G \to H$

$\varphi(g_1g_2) = \varphi(g_1)\cdot\varphi(g_2)$

NEBO $\varphi(g_1+g_2) = \varphi(g_1)+\varphi(g_2)$

$\operatorname{Ker}\varphi = \{g \in G;\ \varphi(g)=1\}$ – PRO NÁSOBENÍ – podgrupa NORMÁLNÍ

Př. $S_n \longrightarrow \{\pm 1\}$

$P \longmapsto \operatorname{sgn} P$

$\operatorname{sgn}(P_1\cdot P_2) = \operatorname{sgn} P_1 \cdot \operatorname{sgn} P_2$

Př. $GL(T^{n\times n}) \longrightarrow T$ $\qquad GL(T^{n\times n})$ ... regulární ~~matice~~ matice

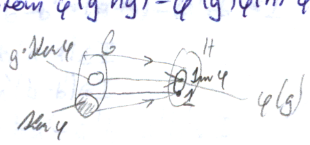
$A \longmapsto \det A$

$\det(A\cdot B) = \det A \cdot \det B$

Je-li $h \in \operatorname{Ker}\varphi$, tj. $\varphi(h)=1$, potom $\varphi(g^{-1}hg) = \varphi(g^{-1})\varphi(h)\cdot\varphi(g) = \varphi(g^{-1})\cdot 1\,\varphi(g) = \varphi(g^{-1}g) = \varphi(1) = \underline{1}$

$$\begin{tikzcd} G \arrow[r, "\varphi"] \arrow[d, "epi"'] & H \\ G/\operatorname{Ker}\varphi \arrow[r, "izo"] & \operatorname{Im}\varphi \arrow[u, "mono"'] \end{tikzcd}$$

$\operatorname{Im}\varphi = \{h \in H \mid \exists g \in G\ \varphi(g)=h\}$



Věta o homomorfismu: $\boxed{G/\operatorname{Ker}\varphi \cong \operatorname{Im}\varphi}$

$$\begin{tikzcd} g \arrow[d] \arrow[r, mapsto] & \varphi(g) \\ g\operatorname{Ker}\varphi \arrow[r] & \varphi(g) \arrow[u] \end{tikzcd}$$

$S_n \xrightarrow{\ \operatorname{sgn}\ } \{\pm 1\}$

$P \longmapsto \operatorname{sgn} P$

$\operatorname{Ker}(\operatorname{sgn}) = A_n$

$h \in A_n$

$g^{-1}hg \in A_n \quad \forall g \in S_n$

$l\ \ s\ \ l$

$\ast\ s$ ... sudá

$\ast\ l$ ... lichá

$S_n/A_n \cong \{\pm 1\}$

$GL_T(n)$ = regulární matice řádu n nad polem T

$GL_T(n) \xrightarrow{\varphi} T\setminus\{0\}$

$A \longmapsto \det A$

$\operatorname{Ker}\varphi = \{A;\ \det A = 1\}$ normální podgrupa v ~~GL~~ $GL_T(n)$

$A \qquad \det A = A$

$\det(B^{-1}AB) = \det B^{-1}\cdot \cancel{\det A}\cdot\det B = 1$

Lagrangeova věta:

$$|G| = |H| \cdot |G/H|$$

řád grupy; řád normální podgrupy; řád faktorové grupy

Def ~~Okruhem~~ Okruhem rozumíme množinu R se dvěma binárními operacemi, sčítáním $+$ a násobením $\cdot$, pro kterou platí:

(i) $(R,+)$ je komutativní grupa
(ii) násobení je asociativní
(iii) násobení je distributivní vzhledem ke sčítání

násobení komutativní $\Rightarrow$ komutativní okruh
má 1 $\Rightarrow$ okruh s 1

Oborem integrity rozumíme komutativní okruh s jednotkovým prvkem bez netriviálních dělitelů nuly, tj. neexistují nenulové prvky, jejichž součin je nula.

Př. $\mathbb{Z}$ = celá čísla – obor int. (invertibilní ± 1)

$\mathbb{Z}[i] = \{a+ib;\ a,b \in \mathbb{Z}\}$ (invertibilní $\pm 1, \pm i$) grupy inv. prvků

$T[x]$ – polynomy s koeficienty z pole T – ob. int. grupa inv. prvků $T \setminus \{0\}$

$\mathbb{Z}_n = \{0,1,\dots,n-1\}$ – okruh, v němž jsou dělitelé nuly ($n \notin \mathbb{P}$)

$\mathbb{Z}_6$: $2 \cdot 3 = 0$

$\mathbb{Q}$ – racion. čísla

$x \oplus y = x+y+1$

$x \odot y = xy+x+y$

$\oplus$ – komutat.

$\odot$ – komutat.

$(\mathbb{Q},\oplus,\odot)$ – ?

$(x\oplus y)\oplus z = (x+y+1)\oplus z = x+y+1+z+1 = x+y+z+2$

$x\oplus(y\oplus z) = x\oplus(y+z+1) = x+y+z+2$

$x \oplus A = x$
$x+A+1 = x \Rightarrow A=-1$

$x \oplus B = -1$
$x+B+1=-1 \Rightarrow (-x) = B = -x-2$

$(x\odot y)\odot z = (xy+x+y)\odot z = xyz+xz+yz+xy+x+y+z$

$x\odot(y\odot z) = x\odot(yz+y+z) = xyz+xy+xz+x+yz+y+z$

$x \odot A = x$
$Ax + \cancel{x} + A = \cancel{x}$
$A(x+1)=0 \Rightarrow A=0$

$x \odot B = 0$
$xB+x+B=0$
$B(x+1)=-x$
$B = -\frac{x}{x+1}$

R-okruh	$I \subset R$	
podokruh		podmnožina uzavřená na +
ideál		„vydrží" násobení, tj. $\forall a \in I \ \forall r \in R \ \ ar \in I, \ ra \in I$

Pr. $\mathbb{Z}$

Všechny ideály jsou $n\mathbb{Z}$, $n = 0, 1, 2, \dots$

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

ideály

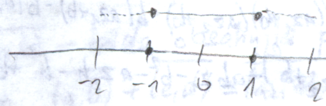
generátor $\langle 1 \rangle = \mathbb{Z}_6 = \langle 5 \rangle$

Funkce na (a,b) okruh

spojité funkce na (a,b) – podokruh, (vynásobením nespojitou fcí nemusí být spojitou)

není ideál

$F_1 \subset F_2 \subset F_3 \subset \dots$



fce mimo kromě intervalu $\langle -1, 1 \rangle$

$\bigcup_{i=1}^{\infty} F_i$ NEMÁ 1, zatímco F_n MÁ 1

Homomorfismus okruhů: $f: R \to S$

$f(r_1 + r_2) = f(r_1) \oplus f(r_2)$

$f(r_1 r_2) = f(r_1) \odot f(r_2)$

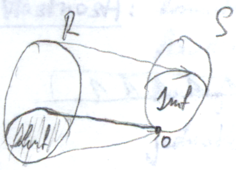
$\operatorname{Ker} f = \{r \in R;\ f(r) = 0\}$

$\operatorname{Im} f = \{s \in S;\ \exists r \in R \ f(r) = s\}$

Ker f = ideál !

$r_1, r_2 \in \operatorname{Ker} f \qquad f(r_1) = f(r_2) = 0$

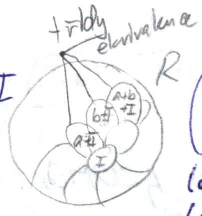
$f(r_1 + r_2) = f(r_1) + f(r_2) = 0 + 0 = 0 \ \to r_1 + r_2 \in \operatorname{Ker} f$



$r_1 \in \operatorname{Ker} f \qquad f(r_1) = 0$

$r_2 \in R \qquad f(r_2 \cdot r_1) = f(r_2) \cdot f(r_1) = f(r_2) \cdot 0 = 0 \Rightarrow r_2 r_1 \in \operatorname{Ker} f$

$r_1 r_2 \in \operatorname{Ker} f$



R-okruh, I-ideál | $a \sim b \iff a - b \in I \iff a + I = b + I$

ekvivalence

faktorová množina $(R/I, +, \cdot)$

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

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

$(a+I) + (-a+I) = I$

$a + I = a' + I \iff a - a' \in I$

$b + I = b' + I \iff b - b' \in I$

$a - a' + b - b' = (a+b) - (a'+b') \in I$

$(a+b) + I \overset{?}{=} (a'+b') + I$

$b(a - a') \in I$

$a'(b - b') \in I$

$ba - ba' + a'b - a'b' \in I$

$ab + I = a'b' + I$

$\mathbb{Z}, n\mathbb{Z} \qquad \mathbb{Z}/n\mathbb{Z} = \{0 + n\mathbb{Z}, 1 + n\mathbb{Z}, 2 + n\mathbb{Z}, \dots, (n-1) + n\mathbb{Z}\} = \{\bar{0}, \bar{1}, \dots, \overline{n-1}\}$

$\Updownarrow$

$\mathbb{Z}_n$

$\mathbb{Z} \xrightarrow{f} \mathbb{Z}_n$

$x = nq + r \to r$

$0 \le r < n$

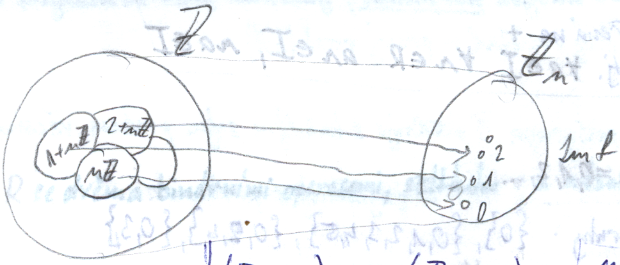
$\mathbb{Z}/\operatorname{Ker} f \qquad x + \operatorname{Ker} f = x + n\mathbb{Z}$

Věta o homomorfismu pro okruhy:

$f: R \to S$

(i) $\mathrm{Ker}\, f$ je ideál

(ii) $\boxed{R/_{\mathrm{Ker}\, f} \cong \mathrm{Im}\, f}$



Př. $(\mathbb{Z}, \oplus, \odot)$ $\quad x \oplus y = x+y-1$ $\quad$ OBOR INTEGRITY?

$x \odot y = x+y-xy$

Př. $(\mathbb{Z}, \oplus, \odot)$ $\quad x \oplus y = x+y-1$ $\quad$ Ob. Int.

$x \odot y = xy-(x+y)+2$

Př. $(\mathbb{Z}, \oplus, \odot)$ $\quad x \oplus y = x+y-b$

$x \odot y = a(xy-bx-by+b^2)+b$

$b \in \mathbb{Z},\ a = \pm 1$

$(\mathbb{Z}, +, \cdot) \longrightarrow (\mathbb{Z}, \oplus, \odot)$ $\quad$ nulový: b, jednotkový: $a+b$

$z \longmapsto az+b$

$\varphi(z_1+z_2) = a(z_1+z_2)+b = az_1+b+az_2+b-b = \varphi(z_1)+\varphi(z_2)-b$

$= \varphi(z_1) \oplus \varphi(z_2)$

$\varphi(z_1 z_2) = a(z_1 z_2)+b$

$\varphi(z_1) \odot \varphi(z_2) = (az_1+b) \odot (az_2+b) = a((az_1+b)(az_2+b)-b(az_1+b)-b(az_2+b)+b^2)+b = a((az_1b+az_2b+z_1z_2+b^2)-abz_1-b^2-az_2b-b^2+b^2)+b$

$= az_1z_2+b$

+	-2	-1	0	1	2	3
-2						
-1						
0						
1	-2	-1	0	1	2	3
2						

b

$\cdot$	-2	-1	0	1	2	3
-2						
-1						
0						
1	1	1	1	1	1	1
2						

P-pole $\quad x \oplus y = x+y-b$ $\quad b \in P,\ a \in P,\ a \neq 0$

$x \odot y = \frac{1}{a}(xy-bx-by+b^2)+b$

$(P, +, \cdot) \xrightarrow{\varphi} (P, \oplus, \odot)$

$z \longmapsto az+b$

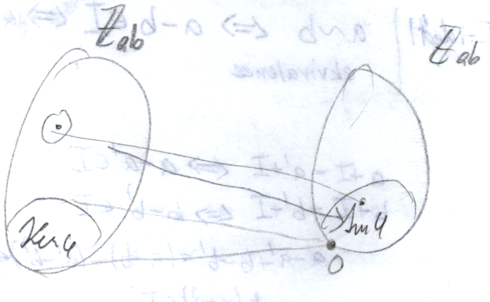
$\mathbb{Z}_{ab} \xrightarrow{\varphi} \mathbb{Z}_{ab}$ $\quad$ EPI/MONO JE TO, IZOMORFNÍ?

$x \longmapsto ax$

epi, mono

$\mathbb{Z}_{ab}/\mathrm{Ker}\, f \xrightarrow[\text{izo}]{\cong} \mathrm{Im}\, \varphi$

$\boxed{\begin{array}{l} \mathrm{Ker}\, f \cong ? \\ \mathrm{Im}\, f \cong ? \end{array}}$



Podílové těleso (pole)

R – obor integrity

zkonstruujeme jeho podílové pole.

$R \times (R \setminus \{0\}) = \{[a,b];\ a,b \in R;\ b \neq 0\}$

$(a,b) \sim (c,d) \overset{def}{\Longleftrightarrow} ad = cb$

$\frac{a}{b} = \frac{c}{d}$ $\boxed{\text{ekvivalence}}$ $(a,b) \sim (a,b)$ ✓

$(a,b) \sim (c,d) \Longleftrightarrow (c,d) \sim (a,b)$ ✓

$(a,b) \sim (c,d),\ (c,d) \sim (e,f) \Longrightarrow (a,b) \sim (e,f)$ ✓

$ad = cb,\ cf = de \overset{?}{\Longrightarrow} af = be$

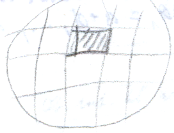
$adcf = cbde$

rozklad na třídy

$\boxed{R \times (R - \{0\}) /_\sim}$

$\overline{(a,b)}$ – třída obsahující prvek (a,b)

$+\quad \overline{(a,b)} + \overline{(c,d)} = \overline{(ad+bc,\ bd)}$ $\qquad \frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$



$\cdot\quad \overline{(a,b)} \cdot \overline{(c,d)} = \overline{(ac,\ bd)}$

Korektnost operací $\quad \overline{(a,b)} = \overline{(a',b')},\ \overline{(c,d)} = \overline{(c',d')}$

$\overline{(a',b')} + \overline{(c',d')} = \overline{(a'd'+c'b',\ b'd')}$

$\left.\begin{array}{l} (a,b) \sim (a',b') \Rightarrow ab' = a'b \quad /\cdot dd' \\ (c,d) \sim (c',d') \Rightarrow cd' = c'd \quad /\cdot bb' \end{array}\right\} \Rightarrow (ad+cb)b'd' = bd(a'd'+c'b')$

$\overline{(a',b')} \cdot \overline{(c',d')} = \overline{(a'c',\ b'd')} \quad \Rightarrow ac b'd' = bd a'c'$

$(a,b) + (c,d) + (e,f)$

Vlastnosti: Komutat.

Asociat. $\quad \overline{(ad+cb,\ bd)} + \overline{(e,f)} = \overline{(f(ad+cb)+bde;\ bdf)}$

$\overline{(a,b)} + \overline{(cf+de;\ df)} = \overline{(b(cf+de)+adf;\ bdf)}$

nulový prvek $\overline{(0,1)}$: $\overline{(c,d)} + \overline{(0,1)} = \overline{(c,d)}$

jednotkový prvek $\overline{(1,1)}$: $\overline{(c,d)} \cdot \overline{(1,1)} = \overline{(c,d)}$

opačný prvek $\overline{(a,b)} + \overline{(-a,b)} = \overline{(ab-ab,\ b)} = \overline{(0,b)} = \overline{(0,1)}$

inverzní prvek $\overline{(a,b)} \cdot \overline{(b,a)} = \overline{(ab,\ ba)} = \overline{(1,1)}$ $\quad (ab)^{*}$ $a \neq 0$

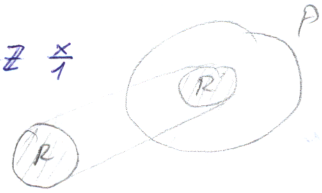
vše. čísla = třídy

navzájem ekvivalent. prvků

izomorfní vnoření ob. int. R do pole T

$R \longrightarrow T$

$x \longmapsto \overline{(x,1)}$ $\qquad x \in \mathbb{Z}\quad \frac{x}{1}$



$\mathbb{Z} \subset \mathbb{Q}$

(z_1, z_2) $\quad z_2 \neq 0$

KVADRATICKÉ NADTĚLESO

– vznikl adjunkcí

$\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2};\ a,b \in \mathbb{Q}\} \subset \mathbb{R}$

$(a+b\sqrt{2})\cdot(c+d\sqrt{2}) = \underbrace{(ac+2bd)}_{\in \mathbb{Q}} + \underbrace{(ad+bc)}_{\in \mathbb{Q}}\sqrt{2}$

$\overline{0}: a=0,\ b=0$

$\overline{1}: a=1,\ b=0$

$-\overline{a}: -(a+b\sqrt{2})$

$\frac{1}{\overline{a}}$: ✓

$\frac{1}{a+b\sqrt{2}} \cdot \frac{a-b\sqrt{2}}{a-b\sqrt{2}} = \underbrace{\frac{a}{a^2-2b^2}}_{\in \mathbb{Q}} - \underbrace{\frac{b}{a^2-2b^2}}_{\in \mathbb{Q}}\sqrt{2}$ $\quad \neq 0$

$(?)\ a^2 - 2b^2 = 0 \Rightarrow a = b = 0$

$\mathbb{Q}[\sqrt{2}] \subset \mathbb{R} \Rightarrow$ komutat., asoc., distr.

$\Rightarrow$ POLE

Rozšíření těles (polí)

$\mathbb{Q} \subset \mathbb{R} \subset \mathbb{C} \subset \mathbb{H}$ „je rozšíření"

Stupeň rozšíření $P \subset P'$

dimenze vekt. prostoru P' nad polem P

stupeň $\mathbb{C}$ nad $\mathbb{R} = 2$

$\mathbb{H}$ nad $\mathbb{R} = 4$

$\mathbb{H}$ nad $\mathbb{C} = 2$

$\mathbb{R}$ nad $\mathbb{Q} = \infty$ ($\mathbb{Q}$ spočet., $\mathbb{R}$ nespočet.)

$\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2};\ a,b \in \mathbb{Z}\} \subset \mathbb{R}$

– nebudou inverzní prvky $\Rightarrow$ OBOR INTEGRITY

$\mathbb{Q}[i] = \{a + bi;\ a,b \in \mathbb{Q}\} \subset \mathbb{C}$

$a+bi \neq 0 \quad \frac{1}{a+bi} = \underbrace{\frac{a}{a^2+b^2}}_{\in \mathbb{Q}} - \underbrace{\frac{b}{a^2+b^2}}_{\in \mathbb{Q}} i$

~~Rozšíření těles (polí)~~

~~$\mathbb{Q} \subset \mathbb{R} \subset \mathbb{C} \subset \mathbb{H}$~~ „je rozšířením"

Průměry $a, b > 0$

Aritmetický $\frac{a+b}{2}$

Geometrický $\sqrt{ab}$

Harmonický $\frac{2ab}{a+b}$ $\left(= \left(\frac{\frac{1}{a}+\frac{1}{b}}{2}\right)^{-1}\right)$

obecně: $\frac{a+b}{2} \geq \sqrt{ab} \geq \frac{2ab}{a+b}$

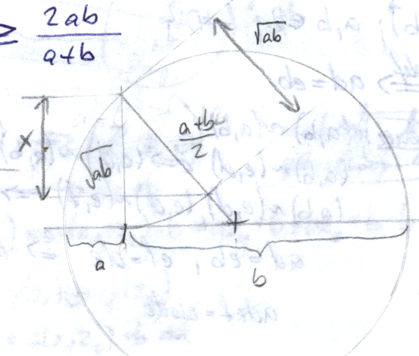
$(\sqrt{a}-\sqrt{b})^2 \geq 0$

$a+b-2\sqrt{ab} \geq 0$

$\boxed{\frac{a+b}{2} \geq \sqrt{ab}}$ $/ \cdot \sqrt{ab}$

$\frac{(a+b)\sqrt{ab}}{2} \geq ab$

$\boxed{\sqrt{ab} \geq \frac{2ab}{a+b}}$



$x = \frac{2ab}{a+b}$

$\frac{a+b}{2} = \frac{2ab}{x}$

$\frac{\frac{a+b}{2}}{\sqrt{ab}} = \frac{\sqrt{ab}}{x}$

Aritmetická posloupnost: $a_0 = a,\ a_1 = a+d, \dots, a_n = a+nd$ – ar. posloupnost 1. stupně

$d=0 \Rightarrow$ ar. posl. 0. stupně

$$S_n = \sum_{i=1}^{n} a_i = \frac{n+1}{2}(a_0+a_n)$$

$a + (a+d) + (a+2d) + \dots\dots + (a+nd)$

$(a+nd) + (a+(n-1)d) + (a+(n-2)d) + \dots\dots + a$

$\big[\underbrace{a}_{a_0} + \underbrace{(a+nd)}_{a_n}\big] \cdot \frac{n+1}{2}$

Diferenční schéma

$a_1 \quad a_2 \quad a_3 \quad a_4 \quad a_5 \quad \dots$

$a_2-a_1 \quad a_3-a_2 \quad a_4-a_3 \quad \dots$

v 1. řádku rozdíly

1	4	9	16	25	36	49	…
3	5	7	9	11	13	…	
2	2	2	2	2	…		
0	0	0	0	…			

$\Rightarrow$ ar. posloupnost 2. stupně

~~$\Rightarrow$ ar. posl.~~

1	8	27	64	125	216	…
7	19	37	61	91	…	
12	18	24	30	…		
6	6	6	…			
0	0	…				

$\Rightarrow$ ar. posloupnost 3. stupně

Geometrická posloupnost: $a_0 = a \quad a_1 = aq \quad \dots\dots \quad a_n = aq^n$

$a + aq + aq^2 + \dots + aq^n + aq^{n+1} = S_{n+1}$

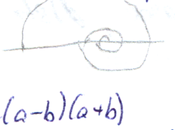
$S_{n+1} = S_n + aq^{n+1}$ $\quad / - S_n$

$a + aq + aq^2 + \dots + aq^{n-1} + aq^n = S_n$

$a(q-1) + aq(q-1) + \dots + aq^n(q-1) = aq^{n+1} - a$

$$S_n = a + aq + \dots + aq^n = a \cdot \frac{q^{n+1}-1}{q-1} = a \cdot \frac{1-q^{n+1}}{1-q}$$

$$S_\infty = \frac{a}{1-q} \quad \text{pro } |q|<1$$



$a^2 - b^2 = (a-b)(a+b)$

$a^3 - b^3 = (a-b)(a^2+ab+b^2)$

$a^{n+1} - b^{n+1} = (a-b)(a^n + a^{n-1}b + a^{n-2}b^2 + \dots + ab^{n-1} + b^n)$

$q^{n+1} - 1 = (q-1)(q^n + q^{n-1} + \dots + q + 1)$

$a \cdot \frac{q^{n+1}-1}{q-1} = (1 + q + \dots + q^n)a$

$a^3 + b^3 = (a+b)(a^2 - ab + b^2)$

$a^n + b^n = (a+b)(a^{n-1} - a^{n-2}b + \dots)$ (n liché)

$$S = 1 + \frac{1}{2} + \underbrace{\frac{1}{3} + \frac{1}{4}}_{>\frac{1}{2}} + \underbrace{\frac{1}{5} + \frac{1}{6} + \frac{1}{7} + \frac{1}{8}}_{>\frac{1}{2}} + \underbrace{\frac{1}{9} + \frac{1}{10} + \frac{1}{11} + \dots + \frac{1}{16}}_{>\frac{1}{2}} + \dots$$

Obory integrity

Euklidovský ob. int. R

norma $\nu : R \setminus \{0\} \to \mathbb{N}^0 = \{0, 1, 2, \dots\}$

(i) $\forall x, y \in R \setminus \{0\}$ $\nu(x) \le \nu(x \cdot y)$

(ii) $\forall x, y \in R, y \neq 0$ $\exists q, r \in R$

$x = yq + r$, kde $r = 0$ nebo $\nu(r) < \nu(q)$

Př.: $\mathbb{Z}$ $\nu(x) = |x|$

$T[x]$ $\nu(f) =$ stupeň f

$\mathbb{Z}[i]$ $\nu(a+bi) = a^2 + b^2$

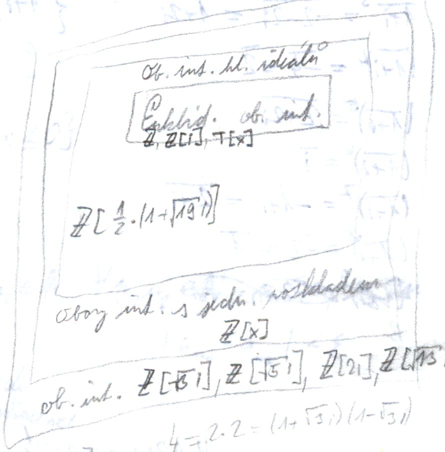
Euklidův algor.

ex. nejv. ~~sol d~~ spol. dělitel

$d(a,b) = (a,b)$

$d = ua + vb$ BEZUTOVA VĚTA

Věta: Každý eukleidovský obor integrity je oborem integrity hlavních ideálů. – hlavní ideál je generován jediným prvkem



~~ireduc~~

ireducibilní prvek (nerozložitelný) $\Uparrow \vee \Downarrow$?

prvočinitel $p | ab \to p | a$ nebo $p | b$

$\mathbb{Z}[\sqrt{3}\, i]$ $4 = 2 \cdot 2 = (1 + \sqrt{3}\, i)(1 - \sqrt{3}\, i)$

$\mathbb{Z}[2i]$ $4 = 2 \cdot 2 = 2i \cdot (-2i)$ – jednotky ± 1, $\nu = a^2 + 4b^2$

různý rozklad

$4 = 2 \cdot 2 = (2i)(-2i)$ v $\mathbb{Z}[i]$ stejný rozklad (jednotky $\pm 1, \pm i$) $\nu = a^2 + b^2$

$|\alpha||\beta| = |\alpha \cdot \beta| \Rightarrow |\alpha| \cdot |\alpha|^{-1} = |1| = 1$

$a^2 + b^2 = 1$

$a^2 + 4b^2 = 1$

6, 9

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

x	1	2	3	4	5	6	7
$f(x)$	0	1	10	33	76	145	246
$f(x+1)-f(x)$	1	9	23	43	69	101	
:	8	14	30	26	32		
	6	6	6	6			
	0	0	0	.....			

3, 2, 1, 0

ar. post. 3. stupně

$\mathbb{Z}[i]$ $\quad I_n = \{a+bi;\ a,b \in n\mathbb{Z}\}$ IDEÁL

třída obsahující nulu $\quad \overline{3} = \overline{0}$

$\mathbb{Z}[i]/I_3 = \{\overline{0}, \overline{1}, \overline{2}, \overline{i}, \overline{2i}, \overline{1+i}, \overline{2+i}, \overline{1+2i}, \overline{2+2i}\}$ faktorový okruh

faktorizace $\mathbb{Z}[i]$ podle I_3 $\quad \overline{0} = I_3$

$\overline{1+i}^2 = \overline{(1+i)(1+i)} = \overline{2i}$

$\overline{1+i}^3 = \overline{-2+2i} = \overline{1+2i}$

$(\overline{1+i})^4 = \overline{-4} = \overline{2}$

$(\overline{1+i})^5 = \overline{2+2i}$

$(\overline{1+i})^6 = \overline{i}$

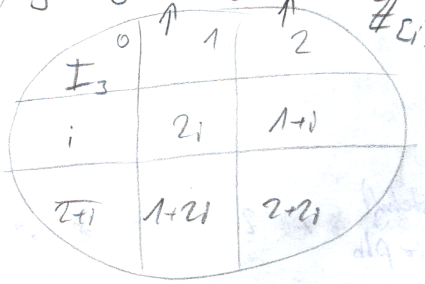
$(\overline{1+i})^7 = \overline{-1+i} = \overline{2+i}$

$(\overline{1+i})^8 = \overline{-2} = \overline{1}$

$\cancel{(\overline{1+i})^9 = \overline{-2+2i} = \overline{1+i}}$

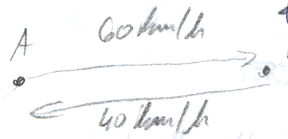
$\{\overline{1+i}, \overline{2i}, \overline{1+2i}, \overline{2}, \overline{2+2i}, \overline{i}, \overline{2+i}, \overline{1}\} = \langle \overline{1+i} \rangle$

$g \quad g^2 \quad g^3 \quad g^4 \quad g^5 \quad g^6 \quad g^7 \quad g^8$



$x - y \in I$

$x + I = y + I$



$\dfrac{2(60 \cdot 40)}{(60+40)}$ km/h $= 48$ km/h — HARMONICKÝ PRŮMĚR

$\sqrt{2} = \frac{p}{q} \quad (p,q) = 1 \qquad 2 = \frac{p^2}{q^2} \Rightarrow 2q^2 = p^2 \Rightarrow p = 2r,\ 2q^2 = 4r^2 \Rightarrow q^2 = 2r^2 \Rightarrow q = 2s$

$\sqrt{2}$ $\quad \sqrt{a^2+1} = a + \sqrt{a^2+1} - a = a + \dfrac{1}{\frac{1}{\sqrt{a^2+1}-a}} x = a + \dfrac{1}{2a + \frac{1}{2a + \frac{1}{2a + \dots}}} = [a; 2a, 2a, 2a, 2a, \dots] = [a; \overline{2a}]$

$x = \dfrac{1}{\sqrt{a^2+1}-a} = \dfrac{\sqrt{a^2+1}+2a-a}{1} = 2a + \dfrac{1}{\frac{1}{\sqrt{a^2+1}-a}} x$

$\sqrt{2} = [1; \overline{2}]$

Číselná osa (19. století)

$-1 \quad 0 \quad \frac{1}{2} \quad 1 \quad \sqrt{2} \quad 2$

Dedekindova teorie řezů   4. stol. př. n. l.

Cantorova teorie fundamentálních posloupností   ~~4. stol. př. n. l.~~

$\mathbb{Q}$ – racionální čísla

řez $\emptyset \neq A \subsetneq \mathbb{Q}$

$a \in A,\ b < a \Rightarrow b \in A$

$\forall a \in A\ \exists a' \in A\ \ a' > a$ (v A není největší prvek)

Př. $A_q = \{x < q;\ x \in \mathbb{Q}\}$

Př. $\{x \in \mathbb{Q};\ x^2 < 2\} \cup \{x \leq 0\}$

$\mathbb{R}$ = množina všech řezů

$A_1 \leq A_2 \Rightarrow A_1 \subseteq A_2$

$A_1 + A_2 = \{a_1 + a_2;\ a_1 \in A_1, a_2 \in A_2\}$

$A_1 \cdot A_2 = \{a_1 \cdot a_2;\ a_1 \in A_1, a_2 \in A_2, a_1 > 0, a_2 > 0\} \cup \{x;\ x \leq 0\}$

2

Fundamentální (cauchyovské) posloupnosti: $\{a_i\}_{i=1}^{\infty},\ a_i \in \mathbb{Q}$

$\forall \varepsilon > 0\ \exists n \in \mathbb{N}\ \forall m_1, m_2 \in \mathbb{N}\ \forall m_1, m_2 \in \mathbb{N},\ m_1 > n,\ m_2 > n$

$|a_{m_1} - a_{m_2}| < \varepsilon$

$$\boxed{\{a_i\} \sim \{b_i\} \quad \lim_{n\to\infty}(a_i - b_i) = 0}$$

$\sim$ ekvivalence $\Rightarrow$ disj. rozklad na třídy ekvivalence

$A \quad 0 \quad \mathbb{Q} - A$

$0 \quad 1 \quad 2 \quad 3 \quad 4$

$\mathbb{R}$ = množina všech těchto tříd

$\mathbb{C} = \mathbb{R} \times \mathbb{R} = \{(a,b);\ a, b \in \mathbb{R}\}$

$(a,b) \leftrightarrow a + bi \leftrightarrow |z|(\cos\varphi + i\sin\varphi) \leftrightarrow |z| \cdot e^{i\varphi}$

$b \quad \varphi \quad a$

$(a,b) = a + bi = z$

$|z| = \sqrt{a^2 + b^2}$

$\cos\varphi = \frac{a}{|z|}$

$\sin\varphi = \frac{b}{|z|}$

$a + bi = |z|(\cos\varphi + i\sin\varphi)$

Moivre: $|z_1|(\cos\varphi_1 + i\sin\varphi_1) \cdot |z_2|(\cos\varphi_2 + i\sin\varphi_2) =$

$= |z_1| \cdot |z_2| (\cos(\varphi_1 + \varphi_2) + i\sin(\varphi_1 + \varphi_2))$

$\cos 3\varphi \quad (\cos\varphi + i\sin\varphi)^3 = \cos 3\varphi + i\sin 3\varphi = \cos^3\varphi + 3i\cos^2\varphi\sin\varphi - 3\cos\varphi\sin^2\varphi - i\sin^3\varphi$

$\cos 3\varphi = \cos^3\varphi - 3\cos\varphi\sin^2\varphi = \cos^3\varphi - 3\cos(1 - \cos^2\varphi)$

$\cos 3\varphi = 4\cos^3\varphi - 3\cos\varphi$

$\sin 3\varphi = 3\cos^2\varphi\sin\varphi = 3(1 - \sin^2\varphi)\sin\varphi$

$\sin 3\varphi = -4\sin^3\varphi + 3\sin\varphi$

$0 \quad 1 \quad 2$

Algebraické rovnice s celočíselnými koeficienty – jejich kořeny jsou tzv. algebraická čísla
(racionální)

SPOČETNÁ MN.

Všechna racionální jsou algebraická $qx-p=0$ $p,q\in\mathbb{Z}$

$\sqrt{2},\sqrt{3},\ldots$

$x^2-2=0$

$x^2-3=0$

$x^3-2=0$

TRANSCENDENTNÍCH ČÍSEL JE NESPOČETNĚ MNOHO

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

$\mathbb{R}$ – úplně uspořádané

$x\le y \Rightarrow x+a\le y+a$

$x\le y,\ a\ge 0 \Rightarrow x\cdot a\le y\cdot a$

$\mathbb{C}$ $\cancel{i>0}$ $\cancel{i<0}$

$\cancel{i^2>0}$ $\cancel{i^2>0}$

$\cancel{-1>0}$ $\cancel{-1>0}$ – není možné uspořádat

$ax+by=c$ v $\mathbb{Z}$ DIOFANTICKÉ ROVNICE

DIOFANT (3. st.)

Řešitelnost

řešitelná $\Leftrightarrow d(a,b) \mid c$

$d = d(a,b)$

$a'x+b'y=c' \Leftarrow$ $a=a'd$, $b=b'd$, $c=c'd$

$a'uc'+b'vc'=c'$

$a'x+b'y=c$

$d(a',b')=1 \Rightarrow \exists u,v \in \mathbb{Z}$

$a'u+b'v=\underline{1}$ $\mid \cdot c'$

$a'(uc')+b'(vc')=c'$

x_0 y_0

Všechna řešení:

$x = uc' + b' \cdot t$

$y = vc' - a' \cdot t$

Př. $5x+7y=64$ $3\cdot 5+(-2)\cdot 7)=1$

$x=64\cdot 3 + 7t = 192+7t = 3+7k$

$y=64\cdot(-2)-5t = -128-5t = 7-5k$

$t = -27+k$

Kladná řeš. $(3,7)$

$(10,2)$

$20\,221x + 5\,183y = 4\,453$

$20\,221 = 5\,183 \cdot 3 + 4\,672$

$5\,183 = 4\,672 + 511$

$4\,672 = 511 \cdot 9 + 73$

$511 = 73 \cdot 7$ $D=73$

$73 = 4672 - 9\cdot 511 = 4672 - 9\cdot(5183-4672) =$

$= 4672 \cdot 10 - 9 \cdot 5183 = -9\cdot 5183 + 10\cdot(20\,221 - 3\cdot 5183) =$

$= 10 \cdot 20\,221 - 39 \cdot 5183$

$277x + 71y = 61$

$277\cdot 10 + 71\cdot(-39) = \underline{1}$

$x = 61\cdot 10 + 71t = 610+71t = 42+71k$

$y = 61(-39) - 277t = -2379 - 277t = -2379 + 2216 - 277k = -163 - 277k$

$(t=-8+k)$

$x_1+4x_2-x_3+x_4=4$

$3x_2+3x_3-2x_4=7$

$20x_3-10x_4=30$

$2x_3-3=x_4$

$x_3=t,\ x_4=2t-3$

$3x_2-t+6=7$

$3x_2=t+1$

$x_2=k$

$t=3k-1$

$x_3=3k-1$

$x_4=6k-5$

$x_1+4k-3k+1+6k-5=4$

$x_1+7k-4=4$

$x_1=-7k+8$

$6x \equiv 21 \pmod{33}$

$ax \equiv c \pmod{n}$

$ax + bn = c$

Řešitelné

$\exists\, d(a,n) \mid c$

$6x \equiv 21 \pmod{33}$

$6x + 33y = 21$

$2x + 11y = 7$

$x = (-5) \cdot 7 + 11t = -35 + 11t = -2 + 11k = \underline{9 + 11l}$

$y = 1 \cdot 7 - 2t$

zk. $6(9 + 11l) \overset{3}{\equiv} 21 \pmod{33}$

Všechna řešení: 9, 20, 31

$d(6,33) = 3$

$33 = 3 \cdot 11$ … 3 řešení

$6x \equiv 21 \pmod{31}$ $\quad 31 = 1 \cdot 31$ … 1 řešení

$6x + 31y = 21$ $\quad (-5) \cdot 6 + 1 \cdot 31 = 1$

$x = -5 \cdot 21 + 31t = -105 + 31t = \underline{19 + 31k}$

$t = 4 + k$

v $\mathbb{Z}_{31}$ $\quad 6x = 21$ $\quad \boxed{x = 19}$

$3x \equiv 1 \pmod{5}$

$2x \equiv 1 \pmod{3}$

$3x + 5k = 1$ $\quad (-3) \cdot 3 + 2 \cdot 5 = 1$ $\quad \underline{x} = (-3) \cdot 1 + 5t = -3 + 5t = \underline{2 + 5m}$

$2x + 3l = 1$

$2 \cdot (2 + 5m) \equiv 1 \pmod{3}$

$10m + 4 \equiv 1$

$m + \cancel{1} \equiv \cancel{1}$

$m \equiv 0$

$m = 3n$ $\quad \underline{x = 2 + 15n}$

$6x_1 + 6x_2 + 25x_3 = -1 \quad / \cdot -2$

$4x_1 + 9x_2 + 10x_3 = 11 \quad / \cdot 3$

$15x_2 - 20x_3 = 35$

$3x_2 - 4x = 7$ $\quad (-1)3 + (-1)(-4) = 1$

$x_2 = (-1) \cdot 7 - 4t$

$x_3 = (-1) \cdot 7 - 3t$

$x_2 = -7 - 4t = 1 - 4k$

$x_3 = -7 - 3t = -1 - 3k$

$t = -2 + k$

$6x_1 + 6 - 24k - 25 - 75k = -1$

$6x_1 - 99k = 18$

$2x_1 - 33k = 6$ $\quad 17 \cdot 2 + (1)(-33) = 1$

$x_1 = 17\cancel{6} - 33m = 102 - 33m$

$k = 6 - 2m = 6 - 2m$

$x_2 = 1 - 24 + 8m = -23 + 8m$

$x_3 = -1 - 18 + 6m = -19 + 6m$