OKRUH

R - množina $+$ - sčítání - abelova grupa
$\cdot$ - násobení

$\forall x, y, z \in R$

$$x \cdot (y+z) = (x \cdot y) + (x \cdot z)$$

$$(x+y) \cdot z = (x \cdot z) + (y \cdot z)$$

R - okruh. $\cdot$ - asoc. Okruh je asociativní
$\cdot$ - komut. komutativní
$\cdot$ - jednotka má jednotku.

Pokud existují $x, y \neq 0$ takové, že $x \cdot y = 0$
řekneme, že R má dělitele nuly

Příklady:

$\mathbb{R}$ $+ \cdot$ - komut. asoc. okruh s jednotkou

$\mathbb{C}$

$\mathbb{Z}_n$ -

M_n - matice n/n - asoc. okruh s jednotkou
má dělitele nuly.

$P[x]$ - polynomy

POLE

Netriviální komutativ. asoc. okruh s jednotkou jehož každý nenulový prvek má inverzi

$$x + y = y + x$$
$$(x+y)+z = x+(y+z)$$
$$0+x = x+0 = x$$
$$x+(-x) = (-x)+x = 0$$
$$x\cdot(y+z) = (x\cdot y)+(x\cdot z)$$
$$(x+y)\cdot z = (x\cdot z)+(y\cdot z)$$
$$x\cdot y = y\cdot x$$
$$x\cdot(y\cdot z) = (x\cdot y)\cdot z$$
$$x\cdot 1 = 1\cdot x = x$$
$x \neq 0$ $$x\cdot x^{-1} = x^{-1}\cdot x = 1$$

Příklady $\mathbb{R}, +, \cdot$ – pole

$\mathbb{C}, +\ \cdot$ – pole

$\mathbb{Q}\ +\ \cdot$ – pole

$P[x]$ – nejsou pole – nemají inverzi

$\mathcal{M}_n$ – nejsou pole –

$\mathcal{F}$ – reálné funkce – nejsou inverze

$\mathbb{Z}_3$ – pole

$\mathbb{Z}_4$ – není pole – 2 nemá inverzi.

Věta Pole nemá dělitele nuly.

Věta V každém poli platí

1. $0 \cdot x = 0$
2. $(-1) \cdot x = -x$

Důkaz: 1. $\underbrace{0 \cdot x}_{y} = x \cdot (0+0) = \underbrace{x \cdot 0}_{y} + \underbrace{x \cdot 0}_{y}$

$y = y + 0 = y + (y - y) = (y + y) - y = y - y = 0$

2. $(-1)x + x = (-1)x + 1 \cdot x = (-1+1)x = 0 \cdot x = 0$

$f: P \to R$ P, R pole

homomor. polí

$f(x+y) = f(x) + f(y)$

$f(x \cdot y) = f(x) \cdot f(y)$

f - bijektivní - izomorfismus polí

$P \approx R$ - izomorfní

5 VEKTOROVÉ PROSTORY

V - množina + sčítání - Abelova grupa

P - pole + $\cdot$

skalární násobení $P \times V \to V$

$a, b \in P$, $x, y \in V$

$$a\cdot(x+y) = a\cdot x + a\cdot y$$
$$(a+b)\cdot x = a\cdot x + b x$$
$$1\cdot x = x$$
$$(a\cdot b)\cdot x = a\cdot(b\cdot x)$$

$x_1, x_2, \dots, x_n \in V$, $\alpha_1, \alpha_2, \dots, \alpha_n \in P$

$\alpha_1 x_1 + \alpha_2 x_2 + \dots + \alpha_n x_n$ - lineární kombinace $x_1, \dots, x_n$ s koeficienty $\alpha_1, \dots, \alpha_n$

$x_1, \dots, x_n$ - jsou lineárně závislé

$\alpha_1 x_1 + \alpha_2 x_2 + \dots + \alpha_n x_n = 0$

má řešení pro nějaké $\alpha_1, \dots, \alpha_n$ alespoň jedno $\neq 0$

Řekneme že V má dimenzi $n \in \mathbb{N}$ $\dim V = n$ jestliže existuje n-lineárně nezávislých vektorů $e_1, \dots, e_n$ a každých $n+1$ vektorů z V je lineárně závislých $(e_1, \dots, e_n)$ - báze V

Pokud $\forall k \in \mathbb{N}$ existuje k lineárně nezávislých vektorů V - nekonečně rozměrný

$M \subset V$ lineární obal množiny M $[\![M]\!]$ jsou všechny lineární kombinace z M

$$[\![M]\!] = \{\alpha_1 x_1 + \dots + \alpha_n x_n \mid x_i \in M, \alpha_1 \in P\}$$

Příklad: $\mathbb{R}$ nad $\mathbb{R}$ vektor. prostor

$\dim \mathbb{R} = 1$ báze (1)

$\mathbb{R}^n$ nad $\mathbb{R}$ – vektorový prostor $\dim n$

$(e_i) = ((1,0,\dots,0),(0,1,0,\dots,0),\dots,(0,0,\dots,0,1))$

$(x^1,x^2,\dots,x^n) = x^1(1,0,\dots,0) + x^2(0,1,0,\dots,0) + \dots + x^n(0,\dots,0,1)$

(e_i) – přirozená báze $\mathbb{R}^n$.

$P_{[x]}$ – polynomy na $\mathbb{R}$ nekonečně rozměrný

$f_1,\dots,f_n$ $f(x) = x^m$ $m > \deg f_i$

$$f(x) = \underbrace{\alpha_1 f_1(x) + \alpha_2 f_2(x) + \dots + \alpha_n f_n(x)}_{\deg < m}$$

Př. $M = \{(1,0,0),(0,0,1)\}$

$$[\![M]\!] = \{\underbrace{\alpha(1,0,0) + \beta(0,0,1)}_{(\alpha,0,\beta)} \quad \alpha,\beta \in \mathbb{R}\}$$

Věta 5.1 Lineární obal báze V je celý V.

Důkaz (e_i) - báze V $\quad x \neq e_i \quad x \notin [\![(e_i)]\!]$

$(e_1, \ldots, e_n, x)$ - lineárně nezávislý

$$\alpha_1 e_1 + \ldots + \alpha_n e_n + \beta x = 0$$

$$-\frac{\alpha_1}{\beta} e_1 - \ldots - \frac{\alpha_n}{\beta} e_n = x \in [\![e_1, \ldots, e_n]\!]$$

Věta 5.2 (Steinitzova věta o výměně)
Každý lineárně nezávislý systém lze doplnit na bázi.

Důkaz $f_1, \ldots, f_k$ - lineárně nezávislé

$k < n \qquad (e_1, \ldots, e_n)$ báze V

$(f_1, e_1, e_2, \ldots, e_n)$

$(f_1, \ldots, f_m, e_{i_1}, e_{i_2}, \ldots, e_{i_{n-m}})$

$(f_1, \ldots, f_m, f_{m+1}, e_{i_1}, \ldots, e_{i_{n-m}})$

$$\alpha^1 f_1 + \alpha^2 f_2 + \ldots + \alpha^m f_m + \alpha^{m+1} f_{m+1} + \beta^1 e_{i_1} + \ldots + \beta^{n-m} e_{i_{n-m}}$$

$\beta^l \neq 0 \qquad \cancel{e_{i_l}}$

$(f_1, \ldots, f_m, f_{m+1}, e_{i_1}, \ldots, e_{i_{l-1}}, e_{i_{l+1}}, \ldots, e_{i_{n-m}})$ - báze