LA 20/11/14

n - PRVOČÍSLO

$\mathbb{Z}_p$ - TĚLESO

TVRZENÍ

n = PRVOČÍSLO

$a \neq 0$, $a \in \mathbb{Z}_p^*$

$$\{0, 1, \dots, n-1\} = \{0a, 1a, \dots, (n-1)a\}$$

DK:

- V TRUZENÍ MÁME 2 SLOŽKY MNOŽINY, TAKŽE SOUČIN JEJICH PRVKŮ JE SLOŽKA

$$1 \cdot 2 \cdot 3 \cdots (n-1) = (1a)(2a)(3a) \cdots ((n-1)(a)) =$$

$$= 1 \cdot 2 \cdot 3 \cdots (p-1) \cdot a^{p-1}$$

$$(n-1)! = (n-1)! \cdot a^{n-1} \quad (a \in \mathbb{Z}_n)$$

$(n-1)! = 0$

JINAK UPRAVÍME: $1 = a^{n-1}$

NEBOŤ PROTOŽE $\mathbb{Z}_n$ JE TĚLESO A $1, 2, \dots (n-1) \neq 0$

DŮSLEDEK

MALÁ FERMATOVA VĚTA

$$a^{p-1} \equiv 1 \quad (v\ \mathbb{Z}_p)$$

p - PRVOČÍSLO, $a \neq 0$

POZN: $x, y \in \mathbb{Z}$

$$x \equiv y \iff n \mid x - y$$

PŘÍKLAD: $p = 5$, $a = 2$

$$2^{n-1} = 2^4 = 16 = 1 \pmod 5$$

$GF(q)$ ... TĚLESO S q PRVKY

- GALOISOVO TĚLESO

FAKT

q ... MOCNINA PRVOČÍSLA $\Rightarrow GF(q)$ EXISTUJE A JE JEDNOZN. URČENO

JINAK $GF(q)$ NEEXISTUJE

$\mathbb{Z}_4$ NENÍ TĚLESO $\Rightarrow GF(4) \neq \mathbb{Z}_4$

4 PRVKY

DF: CHARAKTERISTIKA TĚLESA K

JE MINIMÁLNÍ n, TAK ŽE $\underbrace{1+1+1+1+\dots+1}_{n\text{-KRÁT}} = 0$

$n > 0$

NEBO 0 POKUD TAKOVÉ TĚLESO NEEXISTUJE.

PŘÍKLAD ~~$\mathbb{Z}_n$~~

$\mathrm{char}(\mathbb{Z}_n) = n$

$\mathrm{char}(\mathbb{R}, \mathbb{Q}, \mathbb{C}) = 0$

VĚTA
TVRZENÍ

$\forall$ TĚLESO K JE CHARAKTERISTIKA K 0 NEBO PRVOČÍSLO

DŮKAZ SPOREM

~~$\mathrm{CHAR}\,K = n \neq 0$, n - složené~~

$\mathrm{CHAR}\,K = n \neq 0$, n - složené PRVOČÍSLO.

$1 = \underbrace{1+1+\dots+1}_{k\text{-KRÁT}} \in K$

$\mathbb{Z}_k$

VEKTOROVÉ PROSTORY

ZATÍM: TĚLESO $\mathbb{R}$

VEKTOR $\mathbb{R}^n$

DEF: VEKTOROVÝ PROSTOR NAD TĚLESEM $\mathbb{K}$

JE MNOŽINA V (PRVKY VEKTORY)

S BINÁRNÍ OPERACÍ $+$, A OPERACE $\cdot : \mathbb{K} \times V \to V$

TAK ŽE $(S\mathbb{G})$ $(V, +)$ ABY.... NEUTRÁLNÍ PRVEK $\vec{0} = \mathbb{O}$

....OPAČNÝ PRVEK v JE $-v$

(NA) $a(bv) = (ab)v$ — NÁSOBENÍ $\mathbb{K} \times V$

$\forall a, b \in \mathbb{K}, \forall v \in V$

NÁSOBENÍ V $\mathbb{K}$

(N1) $1 \cdot v = v, \ \forall v \in V$

(NENÍ TOTÉŽ JAKO $1 \cdot a = a, \ a \in \mathbb{K}$)

(D1) $(a+b) \cdot v = av + av, \ a, b \in \mathbb{K}, \ v \in V$

(D2) $a(u+v) = au + av, \ a \in \mathbb{K}, \ u, v \in V$

POZNÁMKA

PRVKY TĚLESA $\mathbb{K}$ SE NAZÝVAJÍ SKALÁRY

$a \cdot v = av$

PŘ

1) $V = \{\vec{0}\}$, $\mathbb{K} = \mathbb{R}$

$\vec{0} + \vec{0} = \vec{0}$; $\alpha \cdot \vec{0} = \vec{0}$

DEFINICE

PODPROSTOR VP V je $W \subseteq V$.

W je JAKÉ VP se "ZDĚDĚNÝMI OPERACEMI"

JE POTŘEBA OVĚŘOVAT JEN? $\vec{0} \in W$

$u, v \in W \Rightarrow$

$\Downarrow$

$u + v \in W$

$\alpha \in \mathbb{K}, v \in W$

$\Rightarrow \alpha \cdot v = a$

PŘÍKLADY

1) $\{\vec{0}\} \subseteq V$

2) v $\mathbb{R}^2$ JSOU PODPROSTORY

- $\{\vec{0}\}$
- PŘÍMKA PROCHÁZEJÍCÍ POČÁTKEM

POZOROVÁNÍ

$(V_\alpha)_{\alpha \in A}$ JE SOUBOR PODPROSTORŮ V

(A ... LIBOVOLNÁ MNOŽINA, PRO $\alpha \in A$ JE DÁNO V_α)

PAK $\bigcap_{\alpha \in A} V_\alpha$ JE TAKÉ PODPROSTOR

DŮKAZ

1) $\vec{0} \in W$? $\forall \alpha \in A : \vec{0} \in V_\alpha \Rightarrow \vec{0} \in \bigcap V_\alpha = W$

2) $u, v \in W$? $\Rightarrow u + v \in W$

$u, v \in \bigcap V_\alpha$ ✓

3) ANALOGICKY JAKO 2

DEF $V \dots VP$

$X \subseteq V$ ... MNOŽINA (NE NUTNĚ PODPROSTOR)

$\mathrm{SPAN}(X) := \bigcap_{\alpha \in A} V_\alpha$ (V_α JSOU VŠECHNY PODPROSTORY V KTERÉ OBSAHUJÍ X)

... LINEÁRNÍ OBAL X

ZNAČENÍ $\langle X \rangle$, $\mathrm{SPAN}(X)$, $L(X)$

VĚTA:

$$\text{SPAN}(X) = \{ \overbrace{\alpha_1 v_1 + \alpha_2 v_2 + \dots + \alpha_m v_m}^{\text{LINEÁRNÍ KOMBINACE VEKTORŮ } v_1 \dots v_m} \}$$

KDE $v_1 \dots v_m \in X$
$\alpha_1 \dots \alpha_m \in K$ }