ŠTÁTNICE - skúšame len to, čo sa odprednášalo

8. **Rozšírenia polí** [konečné rozšírenie poľa, stupeň rozšírenia, algebraické rozšírenie, minimálny polynóm daného algebraického prvku]
9. **Konečné polia** [charakteristika poľa, možné počty prvkov konečných polí, počítanie v poli $F[x]/(p(x))$ pre ireducibilný polynóm $p(x)$, rozkladové pole polynómu, existencia poľa s p^n prvkami]

POLO

NEBOLO - ale povedali sme si to dnes

NEBOLO - ani dnes

ROZŠÍRENIA POLÍ

- charakteristika, $|F| = p^n$ ← NEBUDEM OPAKOVAŤ
- ALG. ROZŠ., MIN. POLYN.
- ROZKLADOVÉ POLE → existuje (práve 1) p^n - prvkové pole

Rozšírenia + stupeň

Definícia

Ak K, F sú polia a súčasne F je podokruhom K, tak hovoríme, že K je *rozšírením* poľa F.

$F \subseteq K$ ← prirodzené označenie

$\mathbb{R} \subseteq \mathbb{C}$

$$\mathbb{C} = \{a + bi; a, b \in \mathbb{R}\}$$

$$\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2}; a, b \in \mathbb{Q}\}$$

Tieto dva príklady sú podobné:

- K poľu $\mathbb{R}$ sme pridali koreň polynómu $x^2 + 1$. i
- K poľu $\mathbb{Q}$ sme pridali koreň polynómu $x^2 - 2$. $\sqrt{2}$

$x^3 - 2$ $\quad \mathbb{Q}(\sqrt[3]{2}) = \{a + b\sqrt[3]{2} + c\sqrt[3]{4};\ a, b, c \in \mathbb{Q}\}$

PRIDÁVANIE KOREŇ

F - pole, $p(x) \in F[x]$

$\downarrow$

$F[x]/(p(x))$

Veta

Nech F je pole a $p(x)$ je ireducibilný polynóm v $F[x]$. Potom existuje rozšírenie poľa F, v ktorom $p(x)$ má koreň.

$K = F[x]/(p(x))$ ~ FAKT. OKRUH

$\downarrow$

D: K je pole

$K = \{ f(x) + (p(x)); f(x) \in F[x] \}$

$= \{ \overline{f(x)}; f(x) \in F[x] \}$

$\overline{f(x)} + \overline{g(x)} = \overline{f(x)+g(x)}$

$\overline{f(x)} \cdot \overline{g(x)} = \overline{f(x)\cdot g(x)}$

R je kom. 1

R/I je pole $\Leftrightarrow$ I je maximálny

$p(x)$ je ired. $\rightarrow (p(x))$ prvoideál $\underset{\text{OM}}{\Rightarrow}$ max. ideál

K obsahuje (izom. kópiu) F

$c \in F \longmapsto \overline{c}$ ... inj. hom. $F \hookrightarrow K \cong F[x]/(p(x))$

$p(x)$ má koreň v K

$\hookrightarrow u = x + (p(x)) = \overline{x}$

? $p(u) = 0$?

$p(x) = c_n x^n + \dots + c_1 x + c_0$

$c_n u^n + \dots + c_1 u + c_0 = \overline{c_n}\cdot\overline{x}^n + \dots + \overline{c_1}\,\overline{x} + \overline{c_0}$

$= \overline{c_n}\cdot\overline{x^n} + \dots + \overline{c_1}\cdot\overline{x} + \overline{c_0}$

$= \overline{c_n x^n + \dots + c_1 x + c_0}$

$= \overline{c_n x^n + \dots + c_1 x + c_0}$

$= \overline{p(x)} = \overline{0}$ □

$\mathbb{C}$.

$$\mathbb{C} = \{a + bi; a, b \in \mathbb{R}\}$$

$$(a_1 + b_1 i)(a_2 + b_2 i) = (a_1 a_2 - b_1 b_2) + (a_1 b_2 + a_2 b_1) i$$

$$\mathbb{C} \cong \underbrace{\mathbb{R}[x]/(x^2+1)}_{K} \cong F[x]/(p(x))$$

$$K = \{ \overline{f(x)} ; f(x) \in \mathbb{R}[x] \}$$
$$= \{ \overline{a + bx} ; a, b \in \mathbb{R} \}$$

↑ každá třída právě na

← stačí stupně < 2

$$f(x) = q(x)(x^2+1) + r(x)$$
$$\overline{f(x)} = \overline{r(x)}$$
$$a + I = b + I \Leftrightarrow a - b \in I$$

$$\overline{a_1 + b_1 x} \cdot \overline{a_2 + b_2 x} = \overline{a_1 a_2 + (a_1 b_2 + a_2 b_1) x + a_2 b_2 x^2}$$
$$= \overline{(a_1 a_2 - a_2 b_2) + (a_1 b_2 + a_2 b_1) x}$$

$$\overline{x^2} = \overline{-1}$$

$$\mathbb{Q}[x]/(x^3-2) \cong \mathbb{Q}(\sqrt[3]{2})$$
$$= \{a + bu + cu^2 ; a, b, c \in \mathbb{Q}\} \cong \{a + b\sqrt[3]{2} + c\sqrt[3]{4} ; a, b, c \in \mathbb{R}\}$$

STUPEŇ ROZŠÍRENIA, KONEČ. ROZŠ.

Definícia

Ak K je rozšírenie poľa F také, že K je konečnorozmerný vektorový priestor nad F, tak K nazývame *konečné rozšírenie* poľa F. Dimenziu $d_F(K)$ poľa K ako vektorového priestoru nad F nazývame *stupeň rozšírenia* a označujeme $[K : F]$.

$$[K : F] = d_F(K)$$

$K \supseteq F$ ... K je VP nad F
? je konečnorozmerný ?
báza (K ako VP nad F)
1, i

$\mathbb{C} \supseteq \mathbb{R}$ $[\mathbb{C} : \mathbb{R}] = 2$
$\mathbb{C} = \{a \cdot 1 + b i ;\ a, b \in \mathbb{R}\}$ ← KONEČNÉ ROZŠ.
$\mathbb{Q}(\sqrt{2}) = \{a \cdot 1 + b\sqrt{2} ;\ a, b \in \mathbb{Q}\}$

$\mathbb{R} \supseteq \mathbb{Q}$ NIE JE konečné rozšírenie
N.P.Ú. $K \supseteq \mathbb{Q}$ $[K : \mathbb{Q}] = n$
? $|K| = \aleph_0$? ⊂ N.D.Ú.

Definícia $K \supseteq F$

Nech K je rozšírenie poľa F. Nech $u \in K$. Hovoríme, že prvok u je *algebraický* nad F, ak existuje nenulový polynóm $f(x) \in F[x]$, ktorého koreňom je u.
Ak každý prvok rozšírenia K je algebraický, hovoríme, že K je *algebraické rozšírenie*.

$x - \sqrt{3} = 0$

$F = \mathbb{Q}$, $K = \mathbb{C}$ $\quad \sqrt{3}$ je alg.: $x^2 - 3$

$\frac{1+\sqrt{5}}{2}$ je alg.: $x^2 - x - 1 = 0$

$\sqrt[3]{2}$ je alg.: $x^3 - 2 = 0$

Čísla, ktoré nie sú algebraické nad $\mathbb{Q}$:

- Napríklad e, π; dôkaz nie je úplne jednoduchý.
- Vieme ukázať, že $|\mathbb{R} \setminus \mathbb{A}| = |\mathbb{C} \setminus \mathbb{A}| = \mathfrak{c}$.

$|A| \leq \aleph_0$ (nekonečný)

MINIMÁLNY POLYNÓM

$I = \{f(x) \in F[x]; f(u) = 0\} \neq (0)$ (je ideál)

Definícia

Ak u je algebraický prvok nad F, tak *minimálny polynóm* prvku u je normovaný polynóm, ktorý generuje ideál $\{f(x) \in F[x]; f(u) = 0\}$. Označujeme ho $m_u(x)$.
Stupeň algebraického prvku definujeme ako stupeň jeho minimálneho polynómu. Označujeme ho $[u : F]$.

$$[u : F] = \operatorname{st} m_u(x)$$

MINIMÁLNY POLYNÓM

$I = \{f(x) \in F[x]; f(u) = 0\} \neq (0)$ ← je ideál

Definícia

Ak u je algebraický prvok nad F, tak *minimálny polynóm* prvku u je normovaný polynóm, ktorý generuje ideál $\{f(x) \in F[x]; f(u) = 0\}$. Označujeme ho $m_u(x)$.

Stupeň algebraického prvku definujeme ako stupeň jeho minimálneho polynómu. Označujeme ho $[u : F]$.

$$[u : F] = \operatorname{st} m_u(x)$$

$F = \mathbb{Q}$

$u = \sqrt{3}$ $\quad m_u(x) = x^2 - 3$ ~~$x - \sqrt{3}$~~

$u = \frac{1+\sqrt{5}}{2}$ $\quad m_u(x) = x^2 - x - 1$

$u = \sqrt[3]{2}$ $\quad m_u(x) = x^3 - 2$ ← ired. nad $\mathbb{Q}$

$F \subseteq K \quad u \in K$

Veta

Ak u je algebraický prvok nad F a $m_u(x) \in F[x]$ je jeho minimálny polynóm. Potom $m_u(x)$ je ireducibilný polynóm nad F,

$$F(u) \cong F[x]/(m_u(x))$$

a $[u : F] = [F(u) : F]$.

D: IRED. $m_u(x) = f(x) \cdot g(x)$

$m_u(u) = f(u) \cdot g(u) = 0 \Rightarrow f(u) = 0 \vee g(u) = 0$

↑ spor s minimalitou

$F(u)$ ... najm. podpole K obsahujúce $F \cup \{u\}$

$\deg m(x) = n \qquad m(x) = x^n + c_{n-1}x^{n-1} + \dots + c_1 x + c_0$

$F[x]/(m(x)) = \{ a_{n-1}x^{n-1} + \dots + a_1 x + a_0 ; a_0, \dots, a_{n-1} \in F \}$

$\downarrow \qquad \parallel$

$F(u) \overset{2.}{=} \{ a_n u^{n-1} + \dots + a_1 u + a_0 ; a_0, \dots, a_{n-1} \in F \}$

je to HOM A ≠ 0 + INJ + BIJ

je to POLE A ≠ 0

báza $F(u)$: $1, u, \dots, u^{n-1}$ $\Rightarrow [F(u) : F] = n$

(nad F)

$a_n u^{n-1} + \dots + a_1 u + a_0 \cdot 1$

$\in F \qquad \in F \qquad \in F$

---

1. 4-prvkové pole
2. rozširovať o char.
2. rozkl. pole
2. D ak ex. $|F| = p^n$

4 - PRVKOVÉ POLE

BOLO: $\mathrm{char}(F) = p \Rightarrow |F| = p^m$

$\mathrm{char}(F) = 2 \Rightarrow |F| = 2^m$

$F[x]/(p(x))$

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

$F = \mathbb{Z}_2$

$p(x) = ?$ ired., st. 2

$p(x) = x^2 + x + 1$ $\quad \{0,1\} = \mathbb{Z}_2$

↑ ired. lebo nemá koreň v $\mathbb{Z}_2$

(Teleso rozkl. ak. polynómu x^2+x+1 je $\mathbb{Z}_2$, $\mathbb{Z}_3$.)

$\begin{cases} u = 0 & 0^2+0+1 = 1 \\ u = 1 & 1^2+1+1 = 1 \end{cases}$

pole

$\mathbb{Z}_2[x]/(x^2+x+1) = \{\overline{ax+b};\ a,b \in \mathbb{Z}_2\}$ ← KAŽDÁ TRIEDA PRÍVE RAZ

$= \{au+b;\ a,b \in \mathbb{Z}_2\}$

$= \{0, 1, u, u+1\}$ ← 4 prvky

$u = \overline{x}$

$u + (u+1) = 1$

$\overline{x} + \overline{x+1} = \overline{1}$

$u^2+u+1 = 0$

$u^2 = -u-1$

$u^2 = u+1$

$u \cdot (u+1) = u^2 + u = (u+1) + u = 1$

$\overline{x} \cdot \overline{x+1} = \overline{x^2+x} = \overline{1}$

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

·	0	1	u	$u+1$
0	0	0	0	0
1	0	1	u	$u+1$
u	0	u	$u+1$	1
$u+1$	0	$u+1$	1	u

u je koren x^2+x+1

$u^2+u+1 = \overline{x}^2+\overline{x}+\overline{1} = \overline{x^2+x+1} = \overline{0}$

$x^2+x+1 \to$ KOREINE $\begin{cases} u \\ u+1 \end{cases}$

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

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

$= x^2 + x + 1$

$(x-0)(x-1)(x-u)(x-u-1) =$

$x(x+1)(x+u)(x+u+1) =$

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

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

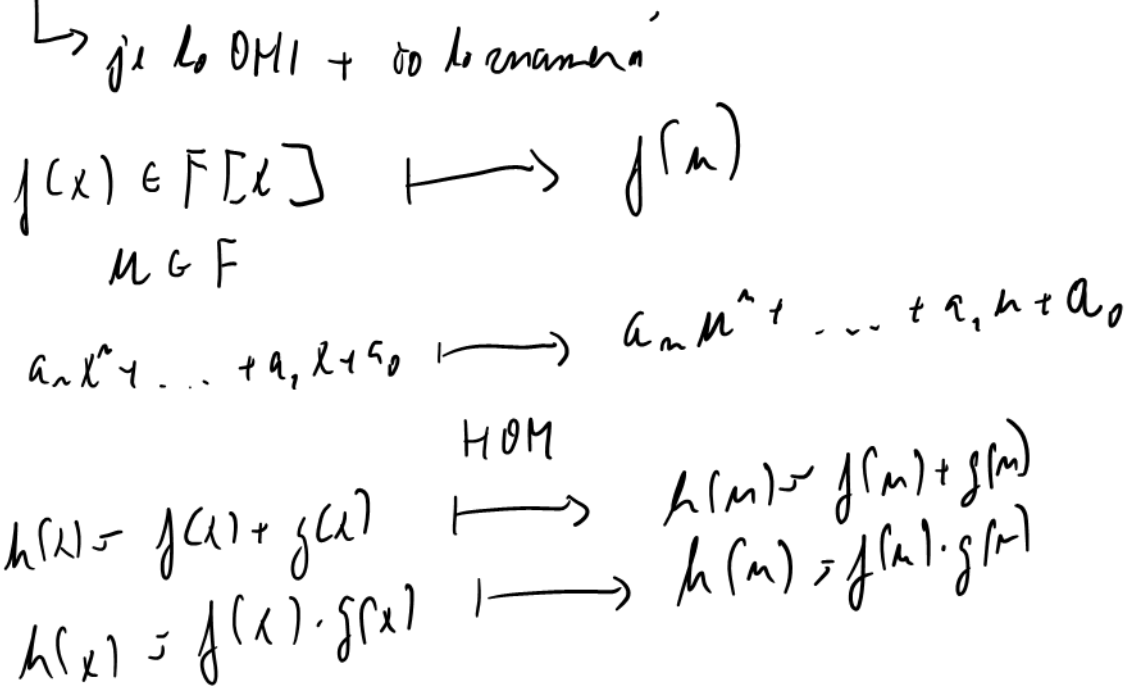
$x(x^3+1) = x^4+x = \underline{x^4-x}$

$p^n = 2^2$

Veta 5.5.5. *Nech $q = p^n$, kde p je prvočíslo a $n > 0$ je prirodzené číslo. Potom existuje (až na izomorfizmus jediné) q-prvkové pole. Je to rozkladové pole polynómu $x^q - x$ nad $\mathbb{Z}_p$.*

$q = p^n$

7. **Okruhy polynómov** [pojem algebraického a transcendentného prvku pre daný okruh, okruh polynómov *R[x]*, okruh polynómov *F[x]* nad poľom *F* ako okruh hlavných ideálov, veta o jednoznačnom rozklade polynómov nad daným poľom, substitučný homomorfizmus (veta o substitúcii), korene, viacnásobné korene, Hornerova schéma]



Príklad 4.3.14. Homomorfizmus $\varphi\colon \mathbb{Z}_2[x] \to \mathbb{Z}_2\langle x\rangle$, ktorý polynómu priraďuje zodpovedajúcu polynomickú funkciu, nie je injektívny.

Stačí si všimnúť, že pre každé $x \in \mathbb{Z}_2$ platí $x^2 + x = 0$, teda polynomická funkcia $x^2 + x$ je nulová a

$$x^2 + x \in \operatorname{Ker}\varphi.$$

Homomorfizmus $\varphi\colon R[x] \to R\langle x\rangle$ nám súčasne dáva možnosť „dosadzovať" do polynómov. Ak totiž máme daný prvok $b \in R$ a nejaký polynóm $f = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in R[x]$, tak mu vieme priradiť funkciu $\varphi(f)\colon R \to R$. Potom môžeme b dosadiť do tejto funkcie, čiže dostaneme

$$\varphi(f)(b) = a_n b^n + a_{n-1}b^{n-1} + \cdots + a_0.$$

Navyše, zobrazenie $f_b\colon R[x] \to R$ určené predpisom

$$f_b\colon f \mapsto a_n b^n + a_{n-1}b^{n-1} + \cdots + a_0$$

je okruhový homomorfizmus taký, že $f(x) = b$ (t.j. polynóm x sa zobrazí na prvok b.)

To, že f_b je skutočne homomorfizmus možno vidieť napríklad z toho, že $f_b = g_b \circ \varphi$, kde $g_b\colon R^R \to R$ je homomorfizmus daný predpisom $g_b(f) = f(b)$ (úloha 4.2.5).

Definícia 4.3.15. Ak R je komutatívny okruh a $b \in R$, tak homomorfizmus $f_b\colon R[x] \to R$ daný predpisom

$$f_b\colon f \mapsto a_n b^n + a_{n-1}b^{n-1} + \cdots + a_0$$

voláme *dosadzovací homomorfizmus*.