Konečná tělesa

Konvence

V této přednášce značí $\mathbb{K}$ vždy těleso.
Řekneme-li polynom, myslíme tím polynom nad $\mathbb{K}$.
Symbolem $m(x)$ značíme pevný polynom stupně alespoň 1.

Minule

Každé $\mathbb{K}[x]/m(x)$ je komutativní okruh s jednotkou.

Analogicky jako v $\mathbb{Z}_m$

1. Rozšířený Eukleidův algoritmus.
2. Invertibilita: $a(x) \in \mathbb{K}[x]/m(x)$ má inversi, pokud $\gcd(a(x), m(x))$ je asociován s 1.
3. Lineární rovnice $a(x) \cdot p(x) = b(x)$ v $\mathbb{K}[x]/m(x)$ má řešení $p(x) = a(x)^{-1} \cdot b(x)$, pokud $\gcd(a(x), m(x))$ je asociován s 1.
   Do složitějších analýz se nebudeme v této přednášce pouštět.

Tvrzení

$\mathbb{K}[x]/m(x)$ je těleso iff $m(x)$ je ireducibilní v $\mathbb{K}[x]$.

Důsledek

Ať p je prvočíslo. Pak $\mathbb{Z}_p[x]/m(x)$ je těleso iff $m(x)$ je ireducibilní v $\mathbb{Z}_p[x]$. Takové těleso má přesně p^n prvků, kde $n = \deg(m(x))$. Značíme jej $GF(p^n)$.[a]

[a] Galois field: Evariste Galois (1811–1832) byl francouzský matematik.

Věta

Každé konečné těleso $\mathbb{K}$ je isomorfní nějakému tělesu $GF(p^n)$.

Příklad — těleso $GF(8)$

1. $8 = 2^3$: hledáme ireducibilní polynom $m(x) \in \mathbb{Z}_2[x]$ stupně 3. Hrubá síla (my nemáme jiné prostředky): $m(x) = x^3 + x + 1$.
2. $GF(8) \cong \mathbb{Z}_2[x]/(x^3 + x + 1)$. Prvky: 0, 1, x, $x+1$, x^2, x^2+1, x^2+x, x^2+x+1.
3. Počítáme standardním způsobem. Např.

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

(vynásobení a nahrazení zbytkem po dělení).

Příklad

Těleso $\mathbb{R}$ reálných čísel, $x^2 + 1 \in \mathbb{R}[x]$.
Zbytky po dělení polynomem $x^2 + 1$ mají tvar:

$$ax + b, \quad a, b \in \mathbb{R}$$

Operace:

1. Sčítání: $(ax + b) + (a'x + b') = (a + a')x + (b + b')$.
2. Násobení: $(ax + b) \cdot (a'x + b') =$
   $(aa')x^2 + (ab' + a'b)x + (bb') = (ab' + a'b)x + (bb' - aa')$.
   Nahradili jsme zbytkem po dělení polynomem $x^2 + 1$.

To jsou komplexní čísla!

$$\mathbb{C} \cong \mathbb{R}[x]/(x^2 + 1)$$

Příklad

V minulém příkladě $x \cdot x = -1$ v $\mathbb{R}[x]/(x^2+1)$, tj. x odpovídá komplexní jednotce. Polynom x^2+1 nemá kořen v $\mathbb{R}$, ale má kořen v $\mathbb{R}[x]/(x^2+1)$.

Tvrzení

Ireducibilní polynom $p(x) \in \mathbb{K}[x]$ stupně alespoň 2 nemá kořen v $\mathbb{K}$.

Tvrzení

Ať $\mathbb{K}$ je těleso a ať $p(x)$ je ireducibilní polynom nad $\mathbb{K}$. Potom polynom $p(x)$ má v $\mathbb{K}[x]/p(x)$ kořen.

Příklad

Nenulové prvky $1, x, x+1, x^2, x^2+1, x^2+x, x^2+x+1$ tělesa $\mathbb{Z}_2[x]/(x^3+x+1)$ lze chápat jako mocniny kořene polynomu x^3+x+1. Označme $\alpha = [x]_{x^3+x+1}$. Pak

$$\begin{aligned}
\alpha^1 &= \alpha \\
\alpha^2 &= \alpha^2 \\
\alpha^3 &= \alpha + 1 \\
\alpha^4 &= \alpha^2 + \alpha \\
\alpha^5 &= \alpha^3 + \alpha^2 = \alpha^2 + \alpha + 1 \\
\alpha^6 &= \alpha^3 + \alpha^2 + \alpha = \alpha^2 + 1 \\
\alpha^7 &= \alpha^3 + \alpha = 1
\end{aligned}$$

Tato reprezentace je možná vždy v tělese $\mathbb{Z}_p[x]/m(x)$, když $m(x)$ je primitivní polynom.