Konečná tělesa

1. Úvod

Definice. *Těleso* $\mathbf{F}$ je množina se dvěma operacemi $+$, $\cdot$, splňující axiomy:

(A1) $a + (b + c) = (a + b) + c$ pro libovolné $a, b, c \in \mathbf{F}$
(A2) $a + b = b + a$ pro libovolné $a, b \in \mathbf{F}$
(A3) existuje $0 \in \mathbf{F}$ tak, že pro všechna $a \in \mathbf{F}$ platí $a + 0 = 0 + a = a$
(A4) pro všechna $a \in \mathbf{F}$ existuje $-a \in \mathbf{F}$ tak, že platí $a + (-a) = (-a) + a = 0$
(M1) $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ pro všechna $a, b, c \in \mathbf{F}$
(M2) $a \cdot b = b \cdot a$ pro všechna $a, b \in \mathbf{F}$
(M3) existuje $1 \in \mathbf{F}$ tak, že pro všechna $a \in \mathbf{F}$ platí $1 \cdot a = a \cdot 1 = a$
(M4) pro všechna $a \neq 0$ existuje $a^{-1} \in \mathbf{F}$ tak, že platí $a \cdot a^{-1} = a^{-1} \cdot a = 1$
(D) $a \cdot (b + c) = a \cdot b + a \cdot c$ pro všechna $a, b, c \in \mathbf{F}$ (distributivita)
(N) $0 \neq 1$ (netrivialita)

Je-li $\mathbf{F}$ konečná množina, pak $\mathbf{F}$ je konečné těleso.

V dalším textu postupně přejdeme od zápisu součinu dvou prvků $a, b \in \mathbf{F}$ ve tvaru $a \cdot b$ ke stručnému ab.

Příklad. Příkladem tělesa je $\mathbb{Z}_p$ s operacemi sčítání a násobení modulo p, kde p je prvočíslo a $\mathbb{Z}_p = \{0, 1, \ldots, p - 1\}$.

Jediné ne zcela zřejmé je dokázat existenci inverzního prvku. Jak se inverzní prvky hledají? Nechť $p = 19997$ a mějme číslo 16. Pak hledáme prvek 16^{-1}.

Pomocí rozšířeného Eukleidova algoritmu najdeme celá čísla a, b tak, že $a \cdot 16 + b \cdot p = 1$. Nalezené číslo a ale nemusí patřit do $\mathbb{Z}_p$ a proto není obecně ještě inverzním prvkem k 16 v $\mathbb{Z}_p$. Najdeme proto dále nezáporný zbytek r při dělení čísla a číslem p. Číslo r je určené jednoznačně podmínkami $a = p \cdot q + r$ pro nějaké celé číslo q a $0 \leq r < p$. Dosazením $a = p \cdot q + r$ do rovnosti $a \cdot 16 + b \cdot p = 1$ pak dostaneme $r \cdot 16 + p \cdot (16 \cdot q + b) = 1$ a tedy $r \cdot 16 \equiv 1 \mod p$. Protože nyní už platí $r \in \mathbb{Z}_p$, je r hledaný inverz k 16.

Použitím Eukleidova algoritmu tedy dostáváme:

$$19997 = 1249 \cdot 16 + 13$$

$$16 = 1 \cdot 13 + 3$$

$$13 = 4 \cdot 3 + 1$$

Teď spočteme vyjádření čísel a a b. Z prvé rovnice dostáváme $13 = 19997 - 1249 \cdot 16$. Z druhé rovnice dostáváme $3 = 16 - 1 \cdot 13$ a po dosazení vyjádření z prvé rovnice dostáváme $3 = 16 - (19997 - 1249 \cdot 16) = 1250 \cdot 16 - 19997$. Z třetí rovnice dostáváme $1 = 13 - 4 \cdot 3$ a po dosazení vyjádření z prvé a druhé rovnice dostáváme $1 = (19997 - 1249 \cdot 16) - 4 \cdot (1250 \cdot 16 - 19997) = -6249 \cdot 16 + 5 \cdot 19997$.

Hledaným číslem je $-6249 + 19997 = 13748$. Inverz k číslu 16 v $\mathbb{Z}_{19997}$ je tedy číslo 13748.

Příklad. Nechť $p(x) = x^3 + x + 1 \in \mathbb{Z}[x]$. Platí, že množina všech polynomů s koeficienty v $\mathbb{Z}_2$ stupně rovného nebo menšího než 2 s operacemi sčítaní a násobení modulo $x^3 + x + 1$ je těleso.

Vezměme polynom $(x + 1)$. Chceme najít polynom $(x + 1)^{-1}$ inverzní k $(x + 1)$. Budeme postupovat podobně jako v předchozím příkladě. Pomocí Eukleidova

algoritmu najdeme polynomy $a(x), b(x) \in \mathbb{Z}_2[x]$ takové, aby platilo $a(x) \cdot (x+1) + b(x) \cdot p(x) = 1$.

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

Tedy $(x+1)^{-1} = x^2 + x$.

Tento postup funguje vždy, kdykoliv největší společný dělitel $p(x) \in \mathbf{F}[x]$ a libovolného nenulového polynomu z $\mathbf{F}[x]$ stupně menšího než je stupeň $p(x)$, je roven 1.

Postup neplatí například pro polynom $p(x) = x^3 + x = x \cdot (x^2 + 1)$.

Definice. Polynom $p(x) \in \mathbf{F}[x]$, kde $\mathbf{F}$ je těleso, se nazývá *ireducibilní* nad $\mathbf{F}$, pokud $\deg p(x) \geq 1$ a kdykoliv $p(x) = a(x).b(x)$ v $\mathbf{F}[x]$, pak buď $a(x)$ nebo $b(x)$ je konstanta.

Věta 1.1 (o existenci kořenového rozšíření tělesa $\mathbf{F}$ určeného ireducibilním polynomem $p(x) \in \mathbf{F}[x]$)**.** *Nechť $p(x) \in \mathbf{F}[x]$ je polynom stupně n ireducibilní nad $\mathbf{F}$. Pak množina všech polynomů z $\mathbf{F}[x]$ stupně menšího než n se sčítáním a násobením modulo n je těleso.*

Důkaz. Všechny vlastnosti tělesa jsou zřejmé, až na vlastnost (M4). Pro ověření vlastnosti (M4) potřebujeme předpoklad, že $p(x)$ je ireducibilní v $\mathbf{F}[x]$. Pro každý polynom $0 \neq f(x) \in \mathbf{F}[x]$ stupně menšího než n platí, že $\mathrm{NSD}(f(x), p) = 1$, tedy existují polynomy $a(x), b(x) \in \mathbf{F}[x]$ takové, že $a(x)f(x) + b(x)p(x) = 1$. Po úpravě a vydělení polynomu $a(x)$ polynomem $f(x)$ se zbytkem dostáváme $a(x) = p(x)q(x) + r(x)$, kde $\deg r(x) < n$ a dosazení do rovnosti $a(x)f(x) + b(x)p(x) = 1$ dostaneme $r(x)f(x) + p(x)(f(x)q(x) + b(x)) = 1$. Polynom $r(x)$ je tedy inverzní polynom k $f(x)$. □

Definice. Je-li $\mathbf{F}$ těleso, pak nejmenší číslo $n > 0$, pro které platí $\underbrace{1 + 1 + \ldots + 1}_{n} = 0$, se nazývá *charakteristika* $\mathbf{F}$.

Pokud žádné takové n neexistuje, pak říkáme, že $\mathbf{F}$ má charakteristiku 0.

Poznámka (opakování)**.** Charakteristika libovolného tělesa je buď 0 nebo prvočíslo. Konečné těleso má vždy nenulovou charakteristiku.

Definice. Je-li $\mathbf{F}$ těleso, pak nejmenší podtěleso $\mathbf{K}$ tělesa $\mathbf{F}$ se nazývá *prvotěleso* tělesa $\mathbf{F}$.

Poznámka. Jak prvotěleso v tělese $\mathbf{F}$ vypadá, závisí na charakteristike $\mathbf{F}$.

(1) Je-li charakteristika $\mathbf{F}$ rovna prvočíslu $p \geq 2$, musí v prvotělese ležet prvky $0, 1, 1+1, 1+1+1, \ldots, \underbrace{1 + 1 + \ldots + 1}_{p-1}$, které jsou navzájem různé.

Značení:

$\underbrace{1 + 1 + \ldots + 1}_{k} = k.1$

$k.1 + l.1 = (k+l).1 = r.1$, kde r je zbytek po dělení $k + l$ prvočíslem p

$(k.1) \cdot (l.1) = (kl).1 = s.1$, kde s je zbytek po dělení $k + l$ prvočíslem p

Prvotěleso v $\mathbf{F}$ je izomorfní se $\mathbb{Z}_p$.

(2) Je-li charakteristika $\mathbf{F}$ rovna 0, pak prvotěleso v $\mathbf{F}$ je izomorfní s tělesem $\mathbb{Q}$.