Konečná tělesa

Alexander „Olin“ Slávik

Abstrakt. Konečná tělesa jsou pozoruhodným zákoutím abstraktní algebry hned ze dvou důvodů – kromě toho, že pro ně platí zajímavé věci, mají i mnohá uplatnění v dalších matematických oborech i praktických aplikacích. Příspěvek přibližuje konstrukci konečných těles a uvádí jejich základní vlastnosti.

Algebraická příprava

Definice. Množinu $\mathbb{F}$ spolu s binárními operacemi $+$ a $\cdot$ a „význačnými“ prvky 0 a 1 nazveme *(komutativním) tělesem*, pokud pro všechna $x, y, z \in \mathbb{F}$ platí následující vztahy:

(i) $x + (y + z) = (x + y) + z$,
(ii) $x + y = y + x$,
(iii) $x + 0 = x$,
(iv) $x \cdot (y \cdot z) = (x \cdot y) \cdot z$,
(v) $x \cdot y = y \cdot x$,
(vi) $x \cdot 1 = x$,
(vii) $x \cdot (y + z) = x \cdot y + x \cdot z$,
(viii) existuje prvek $-x \in \mathbb{F}$ takový, že $x + -x = 0$,
(ix) je-li $x \neq 0$, pak existuje prvek $x^{-1} \in \mathbb{F}$ takový, že $x \cdot x^{-1} = 1$.

Řečeno neformálně, prvky z $\mathbb{F}$ lze sčítat, odčítat, násobit a dělit.

„Každodenními“ příklady těles jsou např. racionální, reálná nebo komplexní čísla. Jiným příkladem jsou tělesa $\mathbb{Z}_p$ pro p prvočíslo, kde se vše počítá modulo p. Jak uvidíme, posledně zmíněné struktury budou výchozím bodem pro konstrukci všech konečných těles.

Definice. *Polynomem* nad tělesem $\mathbb{F}$ (stupně $n \in \mathbb{N}$) nazveme formální výraz $a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$, kde $a_0, \ldots, a_n \in \mathbb{F}$. Množinu všech polynomů nad $\mathbb{F}$ značíme $\mathbb{F}[x]$.

Pozor: polynom pro nás *a priori* nepředstavuje funkci $\mathbb{F} \to \mathbb{F}$, jak jsme typicky zvyklí. Např. v tělese $\mathbb{Z}_2$ se polynomy x a x^2 jakožto funkce shodují, chápeme je však jako různé polynomy.

Polynomy přirozeně umíme sčítat, odčítat, násobit, dělit se zbytkem a hledat jejich největší společné dělitele (pomocí Euklidova algoritmu). Analogicky k celým číslům tedy pro ně můžeme zavést užitečný pojem kongruence.

Definice. Nechť f, r, s jsou polynomy nad tělesem $\mathbb{F}$. Řekneme, že r a s jsou *kongruentní* modulo f, pokud f dělí jejich rozdíl; tuto skutečnost zapisujeme

$$r \equiv s. \pmod{f}$$

Snadno vypozorujeme, že kongruence polynomů má analogické vlastnosti jako kongruence celých čísel. Připomeňme, že u celých čísel měly význačné postavení kongruence modulo prvočíslo, protože se v nich „dalo dělit“. Přirozený protějšek prvočísel ve světě polynomů představuje následující definice.

Definice. Polynom $f \in \mathbb{F}[x]$ nazveme *ireducibilní*, pokud jej nelze zapsat jako součin dvou polynomů stupně alespoň jedna.

Poznámka. Ireducibilitu polynomu vždy chápeme vůči konkrétnímu tělesu. Např. polynom $x^2 + 1$ je v tělese reálných čísel ireducibilní, v komplexních číslech již však nikoli.

Konstrukce nových těles

Argumenty podobnými případu celých čísel dojdeme k závěru, že v kongruencích modulo ireducibilní polynom lze vskutku dělit (nenásobkem onoho polynomu). Vezmeme-li tedy libovolné těleso a ireducibilní polynom f nad ním, získáme nové těleso jednoduše tak, že budeme počítat s polynomy modulo f (postup je analogický k sestrojení těles $\mathbb{Z}_p$).

Pro přehlednost budeme proměnnou „skutečných“ polynomů značit x, zatímco proměnnou polynomů chápaných jako prvky tělesa α.

Příklad. Polynom x^2+x+1 je ireducibilní nad $\mathbb{Z}_2$ (jak se snadno ověří). Jak bude fungovat těleso sestrojené dle výše naznačeného postupu?

Předně si uvědomme, že stejně jako nám v případě $\mathbb{Z}_p$ stačí počítat s čísly $0, \ldots, p-1$ (zbytky modulo p), bude nám v tomto případě stačit s polynomy stupně nejvýše jedna. V souladu s výše uvedenou konvencí tedy půjde o prvky 0, 1, α a $\alpha + 1$.

Pro názornost vynásobme dva prvky – např. α a $\alpha + 1$. Máme

$$\alpha \cdot (\alpha + 1) = \alpha^2 + \alpha = (\alpha^2 + \alpha + 1) + 1 \equiv 1. \pmod{\alpha^2 + \alpha + 1}$$

Takto vytvořené těleso budeme značit $\mathbb{Z}_2[\alpha]/(\alpha^2 + \alpha + 1)$.

Vlastnosti konečných těles

Podívejme se blíže, jaké speciální vlastnosti konečná tělesa mají.

Věta. (Weddenburn) *Všechna konečná tělesa jsou automaticky komutativní, t. j. lze pro ně vynechat bod (v) z definice tělesa.*

Poznámka. Příkladem nekonečného nekomutativního tělesa je např. „těleso“ kvaternionů.

Věta. *Konečné těleso velikosti (počtu prvků) t existuje právě tehdy, když $t = p^n$ pro nějaké prvočíslo p a přirozené číslo n. Navíc jsou všechna konečná tělesa o téže velikosti isomorfní;*[1] *„to jediné“ těleso o velikosti t značíme $\mathrm{GF}(t)$. Každé takové těleso lze navíc sestrojit jako $\mathbb{Z}_p[\alpha]/(f)$, kde $f \in \mathbb{Z}_p[\alpha]$ je libovolný ireducibilní polynom stupně n.*

Věta. *Pro každé konečné těleso existuje primitivní prvek, tedy takový prvek, jehož mocněním získáme všechny nenulové prvky tělesa.*

Příklad. Primitivním prvkem ve výše zmiňovaném tělese $\mathbb{Z}_2[\alpha]/(\alpha^2 + \alpha + 1)$ je např. α, protože $\alpha^2 \equiv \alpha + 1$ a $\alpha^3 \equiv \alpha^2 + \alpha \equiv 1$.

Věta. *Každé těleso $\mathrm{GF}(p^n)$ má jako podtělesa všechna $\mathrm{GF}(p^m)$ pro $m \mid n$.*

[1] Dvě tělesa jsou *isomorfní*, pokud mezi nimi existuje bijekce φ, která splňuje $\varphi(0) = 0$, $\varphi(1) = 1$, $\varphi(x+y) = \varphi(x)+\varphi(y)$ a $\varphi(x \cdot y) = \varphi(x) \cdot \varphi(y)$. Jinak řečeno, jsou „z algebraického pohledu stejná“.