Matematika IV – 5. přednáška
Polynomy

Michal Bulant

Masarykova univerzita
Fakulta informatiky

17. 3. 2008

Obsah přednášky

Doporučené zdroje

- Martin Panák, Jan Slovák, **Drsná matematika**, *e*-text.
- R. B. Ash, Abstract algebra, `http://www.math.uiuc.edu/~r-ash/Algebra.html`.
- Jiří Rosický, *Algebra*, PřF MU, 2002.
- dále *Předmětové záložky v IS MU*

Směřujeme nyní ke zobecnění rozkladů polynomů nad číselnými obory a k tomu nejprve potřebujeme ujasnit, co je dělitelnost v základním okruhu R samotném. Uvažujme proto nějaký pevně zvolený obor integrity R[1], třeba celá čísla $\mathbb{Z}$ nebo okruh $\mathbb{Z}_p$ s prvočíselným p. V R definujeme dělitelnost analogicky jako to známe ze $\mathbb{Z}$: $b|a \iff \exists c \in R : a = b \cdot c$.

Pak platí:

- je-li $a|b$ a zároveň $b|c$ pak také $a|c$;
- $a|b$ a zároveň $a|c$ pak také $a|(\alpha b + \beta c)$ pro všechny $\alpha, \beta \in R$;
- $a|0$ pro všechny $a \in R$ (je totiž $a \cdot 0 = 0$);
- každý prvek $a \in R$ je dělitelný všemi jednotkami $e \in R$ a jejich násobky $a \cdot e$ (jak přímo plyne z existence e^{-1})

[1] Obor integrity proto, aby bylo jednoznačné dělení!

Řekneme, že prvek $a \in R$ je **nerozložitelný** (*ireducibilní*), jestliže

- je nenulový a není jednotkou (tj. $a \nmid 1$),
- je dělitelný pouze jednotkami $e \in R$ a čísly $a \cdot e$ (tzv. čísla *asociovaná* s a – tj. taková $b \in R$, že $a|b$ a $b|a$).

Řekneme, že okruh R je **obor integrity s jednoznačným rozkladem**, jestliže platí:

- pro každý nenulový prvek $a \in R$, který není jednotkou, existují nerozložitelné $a_1, \dots, a_r \in R$ takové, že $a = a_1 \cdot a_2 \dots a_r$
- jsou-li prvky $a_1, \dots, a_r$ a $b_1, \dots, b_s$ nerozložitelné, nejsou mezi nimi žádné jednotky a $a_1 a_2 \dots a_r = b_1 b_2 \dots b_s$, pak je $r = s$ a ve vhodném přeuspořádání platí $a_j = e_j b_j$ pro vhodné jednotky e_j.

Příklad

1. $\mathbb{Z}, \mathbb{R}[x]$ jsou obory integrity s jednoznačným rozkladem (ireducibilní prvky v $\mathbb{Z}$ jsou prvočísla a čísla k nim opačná).
2. Každé těleso je obor integrity s jednoznačným rozkladem (kde každý nenulový prvek je jednotka).
3. Např. v okruhu $\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5}; a, b \in \mathbb{Z}\}$ existují dva různé rozklady čísla 6 na nerozložitelné prvky:

$$6 = 2 \cdot 3 = (1 - \sqrt{-5})(1 + \sqrt{-5}).$$

Základním nástrojem pro diskusi dělitelnosti, společných dělitelů apod. v okruhu celých čísel $\mathbb{Z}$ je procedura dělení se zbytkem a Euklidův algoritmus pro hledání největších společných dělitelů. Tyto postupy nyní zobecníme.

Lemma (Věta o dělení se zbytkem)

Nechť R je komutativní okruh bez dělitelů nuly a $f, g \in R[x]$ polynomy, $g \neq 0$. Pak existuje $a \in R$, $a \neq 0$, a polynomy q a r splňující $af = qg + r$, kde $r = 0$ nebo $\operatorname{st} r < \operatorname{st} g$. Je-li navíc R těleso nebo je aspoň vedoucí koeficient polynomu g roven jedné, potom lze volit $a = 1$ a polynomy q a r jsou v tomto případě určeny jednoznačně.

Poznámka

Toto tvrzení je možné aplikovat i obecněji (viz *Euklidovské okruhy*), je ale třeba *správně* definovat, jak budeme porovnávat prvky.

Proceduru dělení se zbytkem můžeme okamžitě využít k diskusi kořenů polynomů.
Uvažme polynom $f(x) \in R[x]$, $\operatorname{st} f > 0$, a dělme jej polynomem $x - b$, $b \in R$.
Protože je vedoucí koeficient jednička, algoritmus pro dělení dává jednoznačný výsledek. Dostáváme tedy jednoznačně zadané polynomy q a r splňující $f = q(x - b) + r$, kde $r = 0$ nebo $\operatorname{st} r = 0$, tj. $r \in R$. Tzn., že hodnota polynomu f v $b \in R$ je rovna právě $f(b) = r$.
Proto je prvek $b \in R$ **kořen polynomu** f právě, když $(x - b)|f$.
Protože po vydělení polynomem stupně jedna vždy klesne stupeň výsledku alespoň o jedničku, dokázali jsme následující tvrzení:

Důsledek

Každý nenulový polynom f nad tělesem R má nejvýše $\operatorname{st} f$ kořenů.

Příklad

Polynom x^3 má nad $\mathbb{Z}_8$ 4 kořeny $([0]_8, [2]_8, [4]_8, [6]_8,)$.
Je to tím, že tento okruh není oborem integrity (a tedy ani tělesem).

Důsledkem předchozího tvrzení je následující velmi důležitý fakt.

Důsledek

Libovolná konečná podgrupa multiplikativní grupy $(K^\times, \cdot)$ tělesa $(K, +, \cdot)$ je cyklická. Speciálně existuje prvek $g \in \mathbb{Z}_p^\times$ tak, že jeho mocniny generují celou grupu $\mathbb{Z}_p^\times$.

Platí-li pro $k \geq 1$, že dokonce $(x-b)^k | f$, kde k je největší možné, říkáme, že kořen b je **násobnosti** k.
Dva polynomy nad nekonečným komutativním okruhem, které zadávají stejné zobrazení $R \to R$, mají rozdíl, jehož kořenem je každý prvek v R. Protože rozdíl polynomů má jen konečný stupeň, pokud není nulový, dokázali jsme tak již dříve uvedené tvrzení:

Věta

Jestliže je R nekonečný okruh, pak dva polynomy $f(x)$ a $g(x)$ nad R jsou stejné právě, když jsou stejná příslušná zobrazení f a g.

Polynom h je **největší společný dělitel** dvou polynomů a f a $g \in R[x]$ jestliže:

- $h|f$ a zároveň $h|g$
- jestliže $k|f$ a zároveň $k|g$ pak také $k|h$.

Věta (Bezoutova rovnost)

Nechť R je těleso a nechť $f, g \in R[x]$. Pak existuje největší společný dělitel h polynomů f a g. Polynom h je určený jednoznačně, až na násobek nenulovým skalárem. Přitom existují polynomy $A, B \in R[x]$ takové, že $h = Af + Bg$.

Důkaz.

Euklidův algoritmus. $\square$

Důkaz následujícího tvrzení je poměrně technický a nebudeme jej prezentovat v detailech (i když jsme si vše potřebné pro něj již v podstatě připravili).

Věta

Je-li R obor integrity s jednoznačným rozkladem, pak také okruh polynomů $R[x]$ je obor integrity s jednoznačným rozkladem.

Příklad

$\mathbb{Z}[x], \mathbb{Z}_5[x]$ jsou okruhy s jednoznačným rozkladem.

Důsledkem této věty je skutečnost, že každý polynom nad komutativním okruhem s jednoznačným rozkladem můžeme rozložit tak, jak to známe s polynomy s reálnými nebo komplexními koeficienty. Pokud má polynom tolik kořenů, včetně násobnosti, jako je jeho stupeň st $f = k$, je odpovídající rozklad tvaru

$$f(x) = b \cdot (x - a_1) \cdot (x - a_2) \dots (x - a_k).$$

Zatímco reálné polynomy mohou být i úplně bez kořenů, každý komplexní polynom naopak takovýto rozklad připouští. To je obsahem tzv. základní věty algebry:

Věta (Základní věta algebry)

Pole $\mathbb{C}$ je algebraicky uzavřené, tj. každý polynom stupně alespoň 1 má kořen.

Hledání kořenů a ireducibilita

Věta (Gaussovo lemma)

Je-li polynom $f \in \mathbb{Z}[x]$ ireducibilní nad $\mathbb{Z}$, pak je rovněž ireducibilní jakožto polynom nad $\mathbb{Q}$.

Důsledek

$\sqrt{2}$ není racionální číslo.

Věta

Má-li polynom $f(x) = a_n x^n + \cdots + a_0 \in \mathbb{Z}[x]$ racionální kořen $r/s \in \mathbb{Q}$ v základním tvaru, pak $r|a_0$ a $s|a_n$.

Příklad

- Dokažte, že $x^3 - 3x - 1 \in \mathbb{Q}[x]$ je ireducibilní.
- Dokažte, že $x^3 - 3x - 1 \in \mathbb{Z}_2[x]$ je ireducibilní.

Hledání kořenů a ireducibilita, pokr.

Věta (Eisensteinovo kritérium ireducibility)

Je-li $f(x) = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$*, přičemž:*

- $p \mid a_0, \ldots, p_{n-1}, p \nmid a_n$
- $p^2 \nmid a_0$.

Pak je f ireducibilní nad $\mathbb{Z}$ *(a tedy i nad* $\mathbb{Q}$*).*

Důsledek

Nad okruhem $\mathbb{Z}$ *existují ireducibilní polynomy libovolného stupně.*

Důkaz.

Stačí uvážit $f_n = x^n + 2$, který je podle Eisensteinova kritéria (s $p = 2$) ireducibilní stupně n. □

Poznámka

Užitečná je často také tzv. *lokalizace*, tj. redukce koeficientů modulo zvolené prvočíslo p, příp. posunutí proměnné o konstantu. Např., že polynom $x^3 + 27x^2 + 5x + 97$ je ireducibilní, zjistíme díky redukci, ireducibilitu tzv. kruhového polynomu

$$\frac{x^p - 1}{x - 1} = x^{p-1} + \cdots + x + 1$$

díky substituci $x = y + 1$.

Věta

Je-li α kořenem polynomu f nad tělesem násobnosti $k > 1$, je α kořenem f' násobnosti $k - 1$.

Důsledek

Násobné kořeny polynomu f jsou právě kořeny (f, f'). Všechny kořeny polynomu f obdržíme jako (jednoduché) kořeny polynomu $f/(f, f')$.

Polynomy více proměnných

Okruhy polynomů v proměnných $x_1, \dots, x_r$ definujeme induktivně vztahem

$$R[x_1, \dots, x_r] := R[x_1, \dots, x_{r-1}][x_r].$$

Např. $R[x, y] = R[x][y]$, tzn. že uvažujeme polynomy v proměnné y nad okruhem $R[x]$. Snadno se ověří, že polynomy v proměnných $x_1, \dots, x_r$ lze chápat jako výrazy vzniklé z písmen $x_1, \dots, x_n$ a prvků okruhu R konečným počtem (formálního) sčítání a násobení v komutativním okruhu.

Například prvky v $R[x, y]$ jsou tvaru

$$\begin{aligned} f &= a_n(x)y^n + a_{n-1}(x)y^{n-1} + \dots + a_0(x) \\ &= (a_{mn}x^m + \dots + a_{0n})y^n + \dots + (b_{p0}x^p + \dots + b_{00}) \\ &= c_{00} + c_{10}x + c_{01}y + c_{20}x^2 + c_{11}xy + c_{02}y^2 + \dots \end{aligned}$$

Jako důsledek naší definice a předchozích výsledků pro polynomy nad obecnými komutativními okruhy dostáváme:

Důsledek

1. *Jestliže v okruhu R nejsou dělitelé nuly, pak také v okruhu polynomů $R[x_1, \dots, x_r]$ nejsou dělitelé nuly.*
2. *Je-li R obor integrity s jednoznačným rozkladem, pak také okruh polynomů $R[x_1, \dots, x_r]$ je obor integrity s jednoznačným rozkladem.*

Příklad

$\mathbb{Z}[x, y]$ je okruh s jednoznačným rozkladem.

Symetrické polynomy

Definice

Polynom $f \in R[x_1, \dots, x_n]$, který se nezmění při libovolné permutaci proměnných $x_1, \dots, x_n$, se nazývá *symetrický polynom*. *Elementárními symetrickými polynomy rozumíme polynomy*

$$
\begin{aligned}
s_1 &= x_1 + x_2 + \cdots + x_n, \\
s_2 &= x_1 x_2 + x_1 x_3 + \cdots + x_{n-1} x_n, \\
&\vdots \\
s_n &= x_1 \cdots x_n
\end{aligned}
$$

Věta

Libovolný symetrický polynom lze vyjádřit jako polynom v proměnných $s_1, \dots, s_n$.

RSA

Ron Rivest, Adi Shamir, Leonard Adleman (1977; C. Cocks,GCHQ – 1973)

- každý účastník A potřebuje dvojici klíčů – veřejný V_A a soukromý S_A
- generování klíčů: zvolí dvě velká prvočísla p, q, vypočte $n = pq$, $\varphi(n) = (p-1)(q-1)$ [n je veřejné, ale $\varphi(n)$ nelze snadno spočítat]
- zvolí **veřejný klíč** e a ověří, že $(e, \varphi(n)) = 1$
- např. pomocí Euklidova algoritmu spočítá **tajný klíč** d tak, aby $e \cdot d \equiv 1 \pmod{\varphi(n)}$
- zašifrování numerického *kódu* zprávy M: $C = C_e(M) \equiv M^e \pmod{n}$
- dešifrování šifry C: $OT = D_d(C) \equiv C^d \pmod{n}$

Důkaz.

Fermatova, resp. Eulerova věta. □

Poznámka

- Korektní naprogramování bez postranních kanálů není triviální (viz např. PKCS#1, RFC 3447).
- Analogicky podepisování (hashů) zpráv (viz např. DSA)
- Viz RSA factoring challenge (např. rozklad 212 ciferného čísla RSA-704 vynese 30 000 USD).

Diffie-Hellman key exchange, ElGamal

Whitfield Diffie, Martin Hellman (1976; M. Williamson, GCHQ - 1974)
Výměna klíčů pro symetrickou kryptografii bez předchozího kontaktu (tj. náhrada jednorázových klíčů, kurýru s kufříky, ...).

- Dohoda stran na **cyklické grupě** G a jejím generátoru g (veřejné)
- Alice vybere náhodné a a pošle g^a
- Bob vybere náhodné b a pošle g^b
- Společným klíčem pro komunikaci je g^{ab}.

Poznámka

- Problém diskrétního logaritmu (DLP)
- Nezbytná autentizace (*man in the middle attack*)

Z protokolu DH na výměnu klíčů odvozen šifrovací algoritmus ElGamal:

- Alice zvolí cyklickou grupu G spolu s generátorem g
- Alice zvolí **tajný klíč** x, spočítá $h = g^x$ a zveřejní **veřejný klíč** (G, g, h)
- šifrování zprávy M: Bob zvolí náhodné y a vypočte $C_1 = g^y$ a $C_2 = M \cdot h^y$ a pošle (C_1, C_2)
- dešifrování zprávy: $OT = C_2 / C_1^x$

Poznámka

Opět lze odvodit podepisování.

Eliptické křivky

Eliptické křivky jsou rovinné křivky o rovnici tvaru $y^2 = x^3 + ax + b$ a zajímavé jsou tím, že jejich bodech lze definovat operace tak, že výslednou strukturou bude komutativní grupa.
Přitom uvedené operace lze efektivně provádět a navíc se ukazuje, že mají (nejen) pro kryprografii zajímavé vlastnosti – srovnatelné bezpečnosti jako RSA lze dosáhnout již s podstatně kratšími klíči.
Výhodou je rovněž velké množství použitelných eliptických křivek (a tedy grup různé struktury) podle volby parametru a, b .
Protokoly:

- ECDH - přímá varianta DH na eliptické křívce (jen místo generátoru se vybere *vhodný* bod na křivce)
- ECDSA - digitální podpis pomocí eliptických křivek.

Poznámka

Problém diskrétního logaritmu (ECDLP).
Navíc se ukazuje, že eliptické křivky jsou velmi dobře použitelné při faktorizaci prvočísel.