Učební text k přednášce TEORETICKÁ ARITMETIKA
Michal Marvan
Slezská univerzita v Opavě

Okruh polynomů nad Gaussovým okruhem

Nechť R označuje Gaussův okruh. Ukážeme, že okruh polynomů $R[x]$ je také Gaussův okruh. Protože R je obor integrity, existuje jeho podílové pole, označme je Q. Okruh polynomů $Q[x]$ je pak eukleidovský, a tedy Gaussův.

Abychom mohli ukázat, že i $R[x]$ je Gaussův, musíme nejdříve najít souvislosti mezi teorií dělitelnosti v $R[x]$ a v $Q[x]$. Zaveďme některá pomocná zobrazení. Především, R je podokruh ve svém podílovém poli Q, takže polynomy z $R[x]$ leží i v $Q[x]$. Inkluze $R[x] \longrightarrow Q[x]$ je homomorfismem okruhů, který nám umožňuje snadno přenášet algebraické výsledky z $R[x]$ do $Q[x]$. Musíme ovšem rozlišovat mezi asociovaností v okruzích $R[x]$ a $Q[x]$. Asociovanost v $R[x]$ budeme značit $\|_R$, zatímco asociovanost v $Q[x]$ budeme značit $\|_Q$. Připomeňme, že asiciovanost je určena grupou jednotek. Přitom platí $R[x]^* = R^*$ a $Q[x]^* = Q^* = Q \setminus \{0\}$ (protože Q je pole).

Opačná cesta z $Q[x]$ do $R[x]$ je komplikovanější. Ke každému polynomu z $Q[x]$ existuje s ním asociovaný polynom z $R[x]$:

Tvrzení. *Je-li $f \in Q[x]$ libovolný polynom, pak existuje polynom $g \in R[x]$ takový, že $f \|_Q g$.*

Důkaz. Uvažujme o polynomu $f \in Q[x]$, řekněme

$$f = \frac{a_n}{b_n}x^n + \cdots + \frac{a_1}{b_1}x + \frac{a_0}{b_0}.$$

Jeho koeficienty, v souladu s konstrukcí podílového pole Q, jsou zlomky; přitom $a_0, \ldots, a_n \in R$, $b_0, \ldots, b_n \in R \setminus \{0\}$. Převedeme-li zlomky na společného jmenovatele $b \|_R D(b_0, \ldots, b_n)$, obdržíme vyjádření

$$f = \frac{c_n x^n + \cdots + c_1 x + c_0}{b}, \qquad b \neq 0.$$

Stačí tedy položit $g = c_n x^n + \cdots + c_1 x + c_0$.

1. Primitivní polynomy

Existuje způsob, jak přiřazený polynom z $R[x]$ určit jednoznačně až na asociovanost $\|_R$. Uvažujme o polynomu $g = c_n x^n + \cdots + c_1 x + c_0 \in R[x]$. Po vytknutí největšího společného dělitele c všech koeficientů $c_n, \ldots, c_0$ získáme

$$g = c\,(c'_n x^n + \cdots + c'_1 x + c'_0),$$

kde koeficienty $c'_n, \ldots, c'_0 \in R$ jsou již nesoudělné, tj. $D(c'_n, \ldots, c'_0) \|_R 1$.

Definice. Polynom $g \in R[x]$ se nazývá *primitivní*, jsou-li jeho koeficienty nesoudělné.

Označme $\operatorname{cont} g = c$, $\operatorname{pp} g = c'_n x^n + \cdots c'_1 x + c'_0$. Prvek $\operatorname{cont} g \in R$ se nazývá *obsah* polynomu g, polynom $\operatorname{pp} g \in R[x]$ se nazývá *primitivní část* polynomu g. Platí pak

$$g \|_R \operatorname{cont} g \cdot \operatorname{pp} g.$$

Obě části jsou určeny jednoznačně až na asociovanost:

Tvrzení. *Jsou-li $g_1, g_2 \in R[x]$ primitivní polynomy a $c_1, c_2 \in R$ libovolné prvky, přičemž*

$$c_1 g_1 \parallel_R c_2 g_2,$$

pak $c_1 \parallel_R c_2$ a $g_1 \parallel_R g_2$.

Důkaz. Vidíme, že $c_1 \mid c_2 g_2$, takže c_1 dělí všechny koeficienty polynomu $c_2 g_2$, a proto i jejich největšího společného dělitele c_2 (polynom g_2 je primitivní). Analogicky se ukáže, že c_2 dělí c_1, načež $c_1 \parallel_R c_2$, a potažmo také $g_1 \parallel_R g_2$.

Z našich úvah pak vyplývá, že i libovolnému polynomu $f \in Q[x]$ lze přiřadit primitivní část jako $\operatorname{pp} f = \operatorname{pp} g$, kde $g \in R[x]$ a $f \parallel_Q g$. Potom platí $\operatorname{pp} f \in R[x]$ a

$$\operatorname{pp} f \parallel_Q f,$$

ale obdoba obsahu $\operatorname{cont} f$ v tomto případě neexistuje.

Tvrzení (Gaussovo lemma). *Je-li R Gaussův okruh, pak součin libovolných primitivních polynomů je primitivní polynom.*

Důkaz. Uvažujme o primitivních polynomech $f = a_n x^n + \cdots + a_1 x + a_0$, $g = b_m x^m + \cdots + b_1 x + b_0$. Připusťme, že jejich součin fg není primitivní. Buď $d \in R$ největší společný dělitel všech koeficientů polynomu fg. Buď $e \in R$ libovolný ireducibilní faktor prvku d. Prvek e jistě nedělí všechny koeficienty polynomu f (ten je primitivní), a proto existuje nejmenší index i takový, že koeficient a_i není dělitelný prvkem e. Máme tedy $e \mid a_0, \ldots, e \mid a_{i-1}$, ale neplatí $e \mid a_i$. Podobně existuje nejmenší index j takový, že $e \mid b_0, \ldots, e \mid b_{j-1}$, ale neplatí $e \mid b_j$. Koeficient c_{i+j} u x^{i+j} v součinu fg je

$$c_{i+j} = a_{i+j} b_0 + \cdots + a_{i+1} b_{j-1} + a_i b_j + a_{i-1} b_{j+1} + \cdots + a_0 b_{i+j}.$$

Zde jsou všechny sčítance dělitelné e, kromě $a_i b_j$, protože e je ireducibilní a nedělí ani a_i ani b_j. Proto e nedělí koeficient c_{i+j}, a to je spor.

Lemma. *Buďte $p_1, p_2 \in R[x]$ primitivní polynomy. Pak $p_1 \parallel_Q p_2$ právě tehdy, když $p_1 \parallel_R p_2$.*

Důkaz. „$\Rightarrow$“: Podle předpokladu $p_1 = (a/b) p_2$ pro nějaké $a/b \in Q^* = Q \setminus \{0\}$, kde můžeme předpokládat $a, b \in R \setminus \{0\}$. Pak máme $b p_1 = a p_2$. Protože p_1, p_2 jsou primitivní, máme $b \parallel_R \operatorname{cont}(b p_1) = \operatorname{cont}(a p_2) \parallel_R a$, tj. $a \parallel_R b$. Potom ale a/b je jednotka a $p_1 \parallel_R p_2$.
„$\Leftarrow$“: Triviální.

Důsledek. *Je-li R Gaussův okruh, pak*

$$\operatorname{pp}(f_1 \cdots f_n) \parallel_R \operatorname{pp} f_1 \cdots \operatorname{pp} f_n$$

pro libovolné polynomy $f_1, \ldots, f_n \in R[x]$.

Nyní již můžeme přistoupit k důkazu hlavní věty:

Věta. *Je-li R Gaussův okruh, pak $R[x]$ je též Gaussův okruh.*

Důkaz. Musíme ukázat, že libovolný nekonstantní polynom $f \in R[x]$ má jednoznačný rozklad na ireducibilní činitele. (Pro konstantní polynomy tvrzení plyne z faktu, že R je Gaussův okruh.)

Existence: Víme, že $Q[x]$ je Gaussův okruh (je eukleidovský), a proto $f \in Q[x]$ má rozklad na ireducibilní činitele v $Q[x]$, dejme tomu

$$f \parallel_Q q_1 \cdots q_n,$$

kde $q_1, \dots, q_n \in Q[x]$ jsou ireducibilní v $Q[x]$. Položme $p_i = \operatorname{pp} q_i$, pak $\operatorname{pp} f \parallel_Q p_1 \cdots p_n$ (protože $\operatorname{pp} f \parallel_Q f \parallel_Q q_1 \cdots q_n \parallel_Q p_1 \cdots p_n$). Odtud

$$\operatorname{pp} f \parallel_R p_1 \cdots p_n.$$

Ukažme, že p_i jsou ireducibilní v $R[x]$. Připusťme, že p_i má netriviální rozklad v $R[x]$, např. $p_i = uv$. Pak u, v jsou nekonstantní (jakýkoliv konstantní součinitel by byl společným dělitelem všech koeficientů), a proto $q_i \parallel_Q uv$ představuje netriviální rozklad nad Q v rozporu s tím, že q_i je ireducibilní nad Q. Tudíž,

$$\operatorname{pp} f \parallel_R p_1 \cdots p_n$$

je rozklad polynomu $\operatorname{pp} f$ na ireducibilní činitele v $R[x]$.

Dále, $c = \operatorname{cont} f$ je prvek okruhu R. Buď $c \parallel_R s_1 \cdots s_m$ jeho rozklad na ireducibilní činitele v R. Pak z $f \parallel_R \operatorname{cont} f \operatorname{pp} f$ plyne

$$f \parallel_R s_1 \cdots s_m p_1 \cdots p_n.$$

Tento vztah představuje rozklad polynomu f na ireducibilní činitele nad R.

Jednoznačnost: Nechť

$$s_1 \cdots s_m p_1 \cdots p_n \parallel_R s'_1 \cdots s'_{m'} p'_1 \cdots p'_{n'},$$

jsou dva rozklady na ireducibilní prvky v $R[x]$, přičemž na obou stranách jsou rozlišeny konstantní a nekonstantní polynomy: $p_i, p'_i \in R[x]$ jsou nekonstantní ireducibilní polynomy a s_i, s'_i jsou ireducibilní prvky z R. Pak jsou p_i, p'_i primitivní (jakýkoliv netriviální společný dělitel koeficientů je zahrnut mezi konstantní součinitele). Potom však $p_1 \cdots p_n \parallel_Q p'_1 \cdots p'_{n'}$. Polynomy p_i, p'_i jsou ale ireducibilní i nad Q (jsou nekonstantní a kdyby existoval netriviální rozklad $p_i = uv$ nad Q, pak $p_i = \operatorname{pp} p_i = \operatorname{pp} u \cdot \operatorname{pp} v$ je netriviální rozklad nad R). Z jednoznačnosti rozkladu v $Q[x]$ pak plyne, že $n = n'$ a existuje bijekce ϕ taková, že $p_i \parallel_Q p'_{\phi(i)}$, načež i $p_i \parallel_R p'_{\phi(i)}$, protože jde o primitivní polynomy. Nakonec tedy $s_1 \cdots s_m \parallel_R s'_1 \cdots s'_{m'}$ a z jednoznačnosti rozkladu v R dostáváme $m = m'$ a existuje bijekce ψ taková, že $s_i \parallel_R s'_{\psi(i)}$.

Z našich tvrzení vyplývá, že $\mathbf{Z}[x]$ a $(P[x])[y] \cong P[x, y]$ jsou Gaussovy okruhy, přestože nejsou eukleidovské. Indukcí se snadno dokáže, že Gaussovy jsou i okruhy $P[x_1, \dots, x_n]$ a $\mathbf{Z}[x_1, \dots, x_n]$ polynomů n neurčitých.

2. Největší společný dělitel

Věnujme se otázce výpočtu největšího společného dělitele v okruhu $R[x]$. Okruh $R[x]$ nemusí být eukleidovský, a proto nemůžeme obecně použít Eukleidův algoritmus. Nicméně, existuje vztah mezi největším společným dělitelem $D_{R[x]}$ v $R[x]$ a $D_{Q[x]}$ v $Q[x]$, který se hodí i k praktickému počítání.

Tvrzení. *Nechť $f, g \in R[x]$, kde R je Gaussův okruh. Pak*

$$D_{R[x]}(f, g) \parallel_R D_R(\operatorname{cont} f, \operatorname{cont} g) \cdot \operatorname{pp} D_{Q[x]}(\operatorname{pp} f, \operatorname{pp} g).$$

Důkaz. Nechť $f \parallel_R s_1^{u_1} \cdots s_m^{u_m} \cdot p_1^{k_1} \cdots p_n^{k_n}$ resp. $g \parallel_R s_1^{v_1} \cdots s_m^{v_m} \cdot p_1^{l_1} \cdots p_n^{l_n}$ jsou rozklady polynomů f, g na ireducibilní činitele v $R[x]$. Jako obvykle předpokládáme, že $u_i, v_i, k_i, l_i \geq 0$, členy jsou po dvou nesoudělné, s_i jsou konstantní a p_i jsou nekonstantní a navíc primitivní. Pak

$$D_{R[x]}(f, g) \parallel_R s_1^{\min\{u_1,v_1\}} \cdots s_m^{\min\{u_m,v_m\}} \cdot p_1^{\min\{k_1,l_1\}} \cdots p_n^{\min\{k_n,l_n\}},$$

kdežto

$$\begin{aligned} D_R(\operatorname{cont} f, \operatorname{cont} g) &\parallel_R D_R(s_1^{u_1} \cdots s_m^{u_m}, s_1^{v_1} \cdots s_m^{v_m}) \\ &\parallel_R s_1^{\min\{u_1,v_1\}} \cdots s_m^{\min\{u_m,v_m\}} \end{aligned}$$

a

$$\begin{aligned} \operatorname{pp} D_{Q[x]}(\operatorname{pp} f, \operatorname{pp} g) &\parallel_R \operatorname{pp} D_{Q[x]}(p_1^{k_1} \cdots p_n^{k_n}, p_1^{l_1} \cdots p_n^{l_n}) \\ &\parallel_R \operatorname{pp}(p_1^{\min\{k_1,l_1\}} \cdots p_n^{\min\{k_n,l_n\}}) \\ &\parallel_R p_1^{\min\{k_1,l_1\}} \cdots p_n^{\min\{k_n,l_n\}}. \end{aligned}$$

Odtud tvrzení.

Příklad. Spočtěme největšího společného dělitele polynomů

$$f = x^2y^2 - x^2y - xy^2 + x + y - 1,$$
$$g = x^2y + xy^2 - x^2 - 2xy - y^2 + x + y.$$

Jde o polynomy z okruhu $\mathbf{R}[x, y] \cong \mathbf{R}[x][y] = R[y]$, kde $R = \mathbf{R}[x]$. V $R[y]$ máme

$$f = (x^2 - x)y^2 + (-x^2 + 1)y + x - 1,$$
$$g = (x - 1)y^2 + (x^2 - 2x + 1)y - x^2 + x,$$

načež

$$\operatorname{cont} f \parallel_R D(x^2 - x, -x^2 + 1, x - 1) \parallel_R x - 1,$$
$$\operatorname{cont} g \parallel_R D(x - 1, x^2 - 2x + 1, -x^2 + x) \parallel_R x - 1.$$

Tudíž,

$$D_R(\operatorname{cont} f, \operatorname{cont} g) \parallel_R x - 1.$$

Dále potřebujeme najít největšího společného dělitele $D_{Q[y]}(\operatorname{pp} f, \operatorname{pp} g)$, kde Q je podílové pole okruhu R, čili pole $\mathbf{R}(x)$ racionálních lomených funkcí. Máme

$$\operatorname{pp} f \parallel_R f/\operatorname{cont} f \parallel_R xy^2 + (-x - 1)y + 1,$$
$$\operatorname{pp} g \parallel_R g/\operatorname{cont} g \parallel_R y^2 + (x - 1)y - x.$$

Použijme Eukleidův algoritmus v $Q[y]$: V prvním kroku dostáváme $\operatorname{pp} f = q_1 \operatorname{pp} g + r_1$, kde

$$q_1 = x, \qquad r_1 = (-x^2 - 1)y + x^2 + 1,$$

načež v druhém kroku $\operatorname{pp} g = q_2 r_1 + r_2$, kde

$$q_2 = -\frac{y}{x^2 + 1} - \frac{x}{x^2 + 1}, \qquad r_2 = 0.$$

Druhé dělení je beze zbytku a hledaným největším společným dělitelem je $r_1 = -(x^2+1)(y-1)$. Primitivní část je $\operatorname{pp} r_1 \parallel_R y - 1$, načež

$$D_{R[x,y]}(f, g) \parallel D_R(\operatorname{cont} f, \operatorname{cont} g) \cdot \operatorname{pp} D_{Q[y]}(\operatorname{pp} f, \operatorname{pp} g) \parallel (x - 1)(y - 1).$$

Tudíž, největším společným dělitelem polynomů f, g je polynom

$$(x - 1)(y - 1) = xy - x - y + 1.$$