10. Okruhy polynomů

Buď R okruh a ať x je nějaký symbol mimo R. Množinu všech (formálních) mocninných řad $\sum_{i=0} a_i x^i$ značíme $R[[x]]$.

V $R[[x]]$ definujeme součet a součin:
$(\sum a_i x^i) + (\sum b_i x^i) = \sum (a_i + b_i) x^i$,
$(\sum a_i x^i) \cdot (\sum b_j x^j) = \sum c_k x^k$, kde $c_k = \sum_{i+j=k} a_i b_j$.

$R[[x]]$ je vzhledem k těmto binárním operacím, vzhledem k unární operaci $-(\sum a_i x^i) = \sum (-a_i) x^i$ a vzhledem k nulárním operacím $\mathbf{0} = 0 \cdot x^0$ a $\mathbf{1} = 1 \cdot x^0$ okruh.

Ověřme například asociativitu násobení (ostatní axiomy se ověří ještě snadněji):
$((\sum a_i x^i) \cdot (\sum b_j x^j)) \cdot (\sum c_k x^k) = (\sum_r (\sum_{i+j=r} a_i b_j) x^r) \cdot (\sum c_k x^k) =$
$\sum_t (\sum_{r+k=t} (\sum_{i+j=r} a_i b_j) c_k) x^t = \sum_t (\sum_{i+j+k=t} a_i b_j c_k) x^t =$
$\sum_t (\sum_{i+s=t} a_i (\sum_{j+k=s} b_j c_k)) x^t = (\sum a_i x^i) \cdot (\sum_s (\sum_{j+k=s} b_j c_k) x^s) =$
$(\sum a_i x^i) \cdot ((\sum b_j x^j) \cdot (\sum c_k x^k))$.

Ztotožníme-li každý prvek a okruhu R s odpovídajícím prvkem ax^0 okruhu $R[[x]]$, stane se okruh R podokruhem okruhu $R[[x]]$. Z definice je zřejmé, že $R[[x]]$ je komutativní okruh právě když R je komutativní okruh.

10.1 Lemma. *$R[[x]]$ je obor integrity právě když R je obor integrity.*

Důkaz. Ať $a = \sum a_i x^i$ a $b = \sum b_j x^j$ jsou takové mocninné řady, že $a \neq \mathbf{0} \neq b$. Položme $r = \min\{i; a_i \neq 0\}$ a $s = \min\{j; b_j \neq 0\}$. Ať $a \cdot b = \sum c_k x^k$. Pak $c_{r+s} = \sum_{i+j=r+s} a_i b_j = \sum_{i<r} a_i b_{r+s-i} + a_r b_s + \sum_{s>j} a_{r+s-j} b_j = a_r b_s \neq 0$, takže $a \cdot b \neq 0$. $\square$

Pro $a = \sum a_i x^i$ definujeme (formální) derivaci a' tak, že a' je mocninná řada $\sum (i+1) a_{i+1} x^i$. Všimněte si, že rovněž platí $a' = \sum_{i \geq 1} i a_{i-1} x^i$.

10.2 Tvrzení. *Buď $a, b \in R[[x]]$ a $r \in R$. Pak $(a+b)' = a' + b'$, $(ab)' = a'b + ab'$ a $(ra)' = ra'$.*

Důkaz. Ať $a = \sum a_i x^i$, $b = \sum b_i x^i$. Pak $(a+b)' = \sum (i+1)(a_{i+1} + b_{i+1}) x^i = \sum (i+1) a_{i+1} x^i + \sum (i+1) b_{i+1} x^i = a' + b'$. Dále $(ab)' = \sum_k ((k+1)(\sum_{i+j=k+1} a_i b_j)) x^k = \sum_k (\sum_{i+j=k+1} (i+j) a_i b_j) x^k = \sum_k (\sum_{i+j=k+1} (i a_i) b_j) x^k + \sum_k (\sum_{i+j=k+1} a_i (j b_j)) x^k = \sum_k (\sum_{i+j=k} (i+1) a_{i+1} b_j) x^k + \sum_k (\sum_{i+j=k} a_i (j+1) b_{j+1}) x^k = a'b + ab'$. Konečně $(ra') = r'a + ra' = ra'$, neboť $r' = 0$. $\square$

Mocninné řady $\sum a_i x^i$, pro které lze najít takové $k \geq 0$, že $a_i = 0$ pro každé $i \geq k$, se nazývají *polynomy*. Je-li $a = \sum a_i x^i$ polynom, definujeme jeho *stupeň* $\operatorname{st} a$ tak, že $\operatorname{st} \mathbf{0} = -1$ a pro $\mathbf{0} \neq a$ je $\operatorname{st} a = \max\{i; a_i \neq 0\}$.

10.3 Lemma. *Buď $a, b \in R[[x]]$ dva polynomy. Pak, $-a$, $a+b$ a $a \cdot b$ jsou polynomy a platí:*

(i) $\operatorname{st}(-a) = \operatorname{st} a$ a $\operatorname{st}(a+b) \leq \max\{\operatorname{st} a, \operatorname{st} b\}$.
(ii) *Pro $a \neq \mathbf{0} \neq b$ je $\operatorname{st}(a \cdot b) \leq \operatorname{st} a + \operatorname{st} b$. Je-li R obor integrity, tak pro $a \neq \mathbf{0} \neq b$ je $\operatorname{st}(ab) = \operatorname{st} a + \operatorname{st} b$.*

Důkaz. (i) je zřejmé, dokažme (ii). Ať $a = \sum a_i x^i$, $b = \sum b_j x^j$ a $a \cdot b = \sum c_k x^k$. Ať $n = \operatorname{st} a$ a $m = \operatorname{st} b$. Je-li $i + j > n + m$, je $i > n$ nebo $j > m$, takže $\operatorname{st}(a \cdot b) \leq n + m$. Protože $c_{n+m} = a_n b_m$, pro obory integrity platí $\operatorname{st}(a \cdot b) = \operatorname{st} a + \operatorname{st} b$. $\square$

Množina všech polynomů okruhu R se značí $R[x]$.

10.4 Důsledek. *$R[x]$ je podokruh okruhu $R[[x]]$.*

Je-li R obor integrity, je i $R[x]$ obor integrity.

I nadále budeme ztožňovat prvky R a polynomy nultého stupně.

10.5 Tvrzení. *Buď R obor integrity. Polynom $a \in R[x]$ je invertibilní právě když $\operatorname{st} a = 0$ a a je invertibilní v R.*

Důkaz. Ať $a \cdot b = \mathbf{1}$. Pak $\operatorname{st} a + \operatorname{st} b = \operatorname{st} \mathbf{1} = 0$, takže $\operatorname{st} a = \operatorname{st} b = 0$. Zbytek je jasný. $\square$

10.6 Věta. *Buď R obor integrity a $a = \sum a_i x^i$ a $b = \sum b_i x^i$ dva polynomy nad R. Ať $m = \operatorname{st} b \geq 0$ a b_m je invertibilní v R. Pak existují jednoznačně určené polynomy $q, r \in R[x]$ takové, že $a = bq + r$, kde $\operatorname{st} r < m$.*

Důkaz. Dokažme nejprve, že uvedené polynomy skutečně existují. Položme $n = \operatorname{st} a$. Je-li $m > n$, tak stačí položit $q = 0$ a $r = a$. Pro $n \geq m$ budeme postupovat indukcí dle $\delta = n - m$. Je-li $\delta = 0$, položíme $q = a_n b_n^{-1}$ a $r = a - qb$. Ať je $\delta > 0$. Položme $s = a_n b_m^{-1} x^\delta$ a $c = a - sb$. Pak $\operatorname{st} c \leq \operatorname{st} a = n$ a současně koeficient u x^n v c je roven $a_n - a_n b_m^{-1} b_m = 0$, takže $\operatorname{st} c \leq n - 1$. Podle indukčního předpokladu existují polynomy t a r takové, že $c = bt + r$, $\operatorname{st} r < \operatorname{st} b$. Potom $a = c + sb = bt + r + bp = b(t + p) + r$, a stačí položit $q = t + p$.

Ať $a = bq_1 + r_1 = bq_2 + r_2$ a ať platí $\operatorname{st} r_1 < m$ a $\operatorname{st} r_2 < m$. Potom b dělí $r_1 - r_2$ a z $r_1 - r_2 \neq 0$ by podle 10.3(ii) plynulo $\operatorname{st} b \leq \operatorname{st}(r_1 - r_2) < m$. To je spor, takže musí platit $r_1 = r_2$, a tím i $q_1 = q_2$. $\square$

Buď R obor integrity. Zobrazení $\nu : R^\# \to \mathbb{N}_0$ (kde $R^\# = R \setminus \{\mathbf{0}\}$) se nazývá *eukleidovskou funkcí*, jestliže pro libovolné $a, b \in R$ platí:

(1) pokud $a|b$ a $b \neq \mathbf{0}$, tak $\nu(a) \leq \nu(b)$,

(2) pokud $a \neq \mathbf{0} \neq b$, tak existují $q, r \in R$ takové, že $a = bq + r$, kde $r = 0$ nebo $\nu(r) < \nu(b)$.

Obor integrity R, pro který lze definovat alespoň jednu eukleidovskou funkci, se nazývá *eukleidovským oborem integrity.*

10.7 Věta. *Jestliže R je komutativní těleso, tak $R[x]$ je eukleidovský obor integrity, přičemž stupeň polynomu je eukleidovskou funkcí.*

Důkaz. Použij 10.3(ii) a 10.6. $\square$

Obor integrity R se nazývá *oborem integrity hlavních ideálů*, jestliže každý ideál R je hlavní ideál.

10.8 Tvrzení. *Každý eukleidovský obor integrity je oborem integrity hlavních ideálů.*

Důkaz. Buď $\nu : R^\# \to \mathbb{N}_0$ eukleidovská funkce a ať I je nenulový ideál v R. Položme $t = \min\{\nu(b);\ \mathbf{0} \neq b \in I\}$ a zvolme $a \in I$ tak, aby $\nu(a) = t$. Pak $aR \subseteq I$. Naopak, je-li $b \in I$, tak $b = aq + r$, kde $r = \mathbf{0}$ nebo $\nu(r) < \nu(a) = t$. Protože $r \in I$, tak z minimality t dostáváme $r = \mathbf{0}$, takže $b \in aR = I$. $\square$

Obor integrity R se nazývá *Gaussův*, jestliže v $R^\#(\cdot, \mathbf{1})$ má každý neinvertibilní prvek jednoznačný ireducibilní rozklad. (Připomeňme, že ve Větě 5.19 jsou formulovány další podmínky této podmínce ekvivalentní.)

10.9 Tvrzení. *Buď R obor integrity hlavních ideálů a $a_1, \dots, a_n \in R$. Pak existují $u_1, \dots, u_n \in R$ takové, že $\sum u_i a_i = NSD(a_1, \dots, a_n)$.*

Důkaz. Ať I je ideál generovaný prvky $a_1, \dots, a_n$. Pak existuje $d \in R$, že $I = dR$, takže $d = \sum a_i u_i$ dle 7.5. Současně $d | a_i$ pro $1 \le i \le n$. Jestliže $t | a_i$ pro $1 \le i \le n$, tak také $t | \sum a_i u_i = d$. $\square$

10.10 Lemma. *Buď R obor integrity hlavních ideálů. Pak kvaziuspořádání R dělitelností je noetherovské.*

Důkaz. Ať $a_0, a_1, \dots$ je nekonečná posloupnost vlastních dělitelů. Potom pro $i \in \mathbb{N}_0$ je $a_i R \subsetneqq a_{i+1} R$. Snadno ověříme, že $I = \bigcup_i a_i R$ je ideál, a tedy existuje $d \in R$, pro které je $I = dR$. To ovšem znamená, že $d \in a_j R$ pro některé $j \in \mathbb{N}_0$, takže $a_j R = dR = a_{j+1} R$, spor. $\square$

10.11 Důsledek. *Obory integrity hlavních ideálů jsou Gaussovy.*

Důkaz. Použij 5.19, 10.9 a 10.10. $\square$

10.12 Tvrzení. *Buď R obor integrity hlavních ideálů. Potom $a \in R$ je prvočinitel právě když aR je maximální ideál v R.*

Důkaz. Prvek a je prvočinitel právě když je ireducibilní, tj. právě když není invertibilní a nemá vlastní dělitele. Buď I ideál, $R \supsetneqq I \supseteq aR$. Pak existuje $b \in R$, že $I = bR$. Ovšem $bR \supsetneqq aR$ jedině tehdy, jestliže b je vlastní dělitel a. $\square$

Víme, že v eukleidovských oborech integrity existují největší společní dělitelé. Tyto obory integrity dostali svůj název podle prastarého algoritmu, který umožňuje největší společné dělitele účinně nacházet.

10.13 Tvrzení. (Eukleidův algoritmus.) *Buď R obor integrity a $\nu : R^{\#} \to \mathbb{N}_0$ eukleidovská funkce a ať a_0, a_1 jsou prvky $R^{\#}$. Budeme definovat posloupnost $a_0, a_1, \dots$ takovýmto způsobem:*

(i) *Je-li $i \ge 1$ a a_i nedělí a_{i-1}, tak zvolíme a_{i+1} tak, že pro nějaké $q_i \in R$ je $a_{i-1} = a_i q_i + a_{i+1}$ a $\nu(a_{i+1}) < \nu(a_i)$.*

(ii) *Je-li $i \ge 1$ a a_i dělí a_{i-1}, tak položíme $n = i$ a posloupnost ukončíme.*

Takto vytvořená posloupnost je vždy konečná a $a_n = NSD(a_0, a_1)$.

Důkaz. Konečnost posloupnosti plyne z toho, že $\nu(a_i) > \nu(a_{i+1})$. $NSD(a_n, a_{n-1}) = a_n$ dle 4.8, takže stačí ukázat, že pro každé $1 \le i \le n-1$ je $d || t$, kde $d = NSD(a_{i-1}, a_i)$ a $t = NSD(a_i, a_{i+1})$. Vidíme, že d dělí $a_{i+1} = a_{i-1} - a_i q$, takže $d | t$. Naopak, t dělí $a_{i-1} = a_i q + a_{i+1}$, takže $t | d$. $\square$

Aplikujme nyní dosažené výsledky na eukleidovský obor integrity $T[x]$, kde T je komutativní těleso. Přitom na T hledíme jako na podokruh $T[x]$. Multiplikativní grupu tělesa T budeme označovat T^*. (Pro těleso T je tedy T^* rovno $T^{\#}$; obecně pro okruhy tato rovnost však neplatí, neboť R^* označuje množinu (grupu) invertibilních prvků okruhu R.)

Invertibilní prvky $T[x]$ jsou nenulové prvky tělesa T (viz 10.5). Obor integrity $T[x]$ je eukleidovský (10.7), tedy obor integrity hlavních ideálů (10.8), tedy Gaussův (10.11).

Polynom $a = \sum a_i x^i \in T[x]$ nazvu *monický*, jestliže $a_{\mathrm{st}\, a} = 1$ a $a \neq \mathbf{0}$. Každý nenulový polynom je zjevně asociován právě s jedním monickým polynomem. Z 5.18 plyne, že každý polynom $a \in T[x]$ stupně alespoň 1 lze napsat až na pořadí jediným způsobem jako $cp_1^{k_1} \dots p_r^{k_r}$, kde $p_1, \dots, p_r$ jsou navzájem různé monické ireducibilní polynomy, $k_1, \dots, k_r$ jsou přirozená čísla a $c \in T^*$ (přitom $c = a_{\mathrm{st}\, a}$ a $\mathrm{st}\, a = \sum k_i (\mathrm{st}\, p_i)$).

Pro $a, b \in T[x]$ platí $aT[x] = bT[x]$ právě když jsou polynomy a, b v $T[x]$ asociovány (viz 7.6). Protože invertibilní prvky okruhu $T[x]$ se shodují s nenulovými prvky tělesa T (viz 10.5) a protože prvky jsou asociovány tehdy, liší-li se o invertibilní prvek (viz 5.10), vidíme, že $aT[x] = bT[x]$ platí právě když polynom a je roven tb pro nějaké $t \in T$. To znamená, že hlavní ideál $aT[x]$, $a \neq 0$, lze jediným způsobem vyjádřit jako $mT[x]$ tak, aby m byl polynom monický. Tudíž každý monický polynom obsažený v $aT[x]$ je buď roven m, nebo má stupeň vyšší než $\mathrm{st}\, a = \mathrm{st}\, m$. V okruhu $T[x]$ jsou všechny ideály hlavní, takže jsme dokázali, že každý nenulový ideál je jednoznačně charakterizován monickým polynomem, který ho generuje.

Prvek $\alpha \in T$ nazveme *kořenem* polynomu $a \in T[x]$, jestliže polynom $x - \alpha$ dělí a. Přitom $x - \alpha$ je podle 10.3(ii) a 10.5 ireducibilní prvek $T[x]$ pro každé $\alpha \in T$. Je-li $a = cp_1^{k_1} \dots p_r^{k_r}$ rozklad nenulového polynomu a na ireducibilní polynomy, tak ty z nich, které jsou tvaru $x - \alpha$, nazýváme *kořenovými* činiteli a. Jsou-li všechna $p_1, \dots, p_r$ stupně 1, říkáme, že a se *rozkládá na kořenové činitele.* Je-li p_i, $1 \leq i \leq r$, kořenový činitel, $p_i = x - \alpha$, tak číslo k_i nazýváme *násobností* kořenu α. Jestliže se a rozkládá na kořenové činitele, tak $\mathrm{st}\, a = \sum k_i$. Počet kořenů, počítáme-li každý tolikrát, kolik činí jeho násobnost, je tedy menší nebo roven stupni polynomu, přičemž rovnost nastává právě když se polynom rozkládá na kořenové činitele. (Je třeba si uvědomit, že tyto výroky se týkají pouze nenulového polynomu.)

Komutativní těleso T, ve kterém se každý polynom $a \in T[x]$, $\mathrm{st}\, a \geq 1$, rozkládá na kořenové činitele, se nazývá *algebraicky uzavřené.* Příkladem algebraicky uzavřeného tělesa je těleso komplexních čísel $\mathbb{C}$.

10.14 Tvrzení. *Buď T těleso, $0 \neq a \in T[x]$ a ať α je kořen a. Potom α je násobnosti alespoň 2 právě když je také kořenem a'.*

Důkaz. Ať je $a = (x - \alpha)b$ pro vhodné $b \in T[x]$. Máme $a' = b + (x - \alpha)b'$, takže $x - \alpha$ dělí a' právě když $x - \alpha$ dělí b. $\square$

10.15 Důsledek. *Buď T těleso, $a \in T[x]$ a ať $NSD(a, a') = \mathbf{1}$. Potom a nemá vícenásobné kořeny.*

10.16 Tvrzení. *Buď $n \in \mathbb{N}$, T těleso a ať $\mathrm{char}\, T$ nedělí n. Pak polynomy $x^n - \mathbf{1}$ a $x^{n+1} - x$ nemají vícenásobné kořeny.*

Důkaz. Polynom $(x^n - \mathbf{1})' = nx^{n-1} = (n \cdot \mathbf{1})x^{n-1}$ je asociován s polynomem x^{n-1}, neboť z toho, že $\mathrm{char}\, T$ nedělí n, plyne $n \cdot \mathbf{1} \neq 0$. Je $x^n - \mathbf{1} = x \cdot x^{n-1} - \mathbf{1}$, a proto $NSD(x^n - \mathbf{1}, x^{n-1}) = \mathbf{1}$.

Polynom $x^{n+1} - x = x \cdot (x^n - \mathbf{1})$ má za kořeny nulu a všechny kořeny polynomu $x^n - \mathbf{1}$. Protože nula není kořenem polynomu $x^n - \mathbf{1}$, nemůže mít ani polynom $x^{n+1} - x$ jakýkoliv vícenásobný kořen. $\square$

Jsou-li $S \supseteq R$ do sebe vřazené komutativní okruhy a α je prvek S, definujeme *dosazovací homomorfismus* $j_\alpha : R[x] \to S$ tak, že $j_\alpha(\sum a_i x^i) = \sum a_i \alpha^i$ pro každé $a = \sum a_i x^i \in R[x]$.

10.17 Lemma. *$j_\alpha : R[x] \to S$ je homomorfismus okruhů.*

Důkaz. Pro polynomy $a = \sum a_i x^i$ a $b = \sum b_j x^j$ jistě platí $j_\alpha(a+b) = j_\alpha(a)+j_\alpha(b)$. Podobně pro $a\cdot b = c = \sum c_k x^k$ je $j_\alpha(c) = \sum_k (\sum_{i+j=k} a_i b_j)\alpha^k = (\sum a_i \alpha^i)(\sum b_j \alpha^j)$ $= j_\alpha(a) j_\alpha(b)$. □

Místo $j_\alpha(a)$ se většinou píše $a(\alpha)$. Ale označení j_α budeme pro dosazovací homomorfismus dále používat také.

10.18 Tvrzení. *Buď T komutativní těleso, $a \in T[x]$ a $\alpha \in T$. Pak α je kořen polynomu a právě když $a(\alpha) = 0$.*

Důkaz. Ať $a = (x-\alpha)b$ pro $b \in T[x]$. Podle 10.17 je $f_\alpha(a) = a(\alpha) = (\alpha-\alpha)b(\alpha) = 0$. Naopak, ať $a(\alpha) = 0$ a $a = (x-\alpha)q + r$, kde $\operatorname{st} r \leq 0$ (čili $r \in T$). Potom $0 = a(\alpha) = (\alpha-\alpha)q(\alpha) + r(\alpha) = r$. □

10.19 Tvrzení. *Buď T komutativní těleso a $G \subseteq T^*$ nějaká podgrupa (tj. G je množina uzavřená na násobení a inverzní prvky). Je-li G konečná, tak je cyklická.*

Důkaz. Položme $n = |G|$ a připomeňme, že řád každého prvku G dělí n (Lagrangeova věta). Pro dělitel k čísla n označme t_k počet prvků řádu k. Protože každý prvek má nějaký řád, musí platit $n = \sum t_k$. Grupa G bude cyklická, je-li $t_n \geq 1$ (a pak je $t_n = \varphi(n)$, kde φ označuje Eulerovu funkci). Podle 8.14 máme $n = \sum \varphi(k)$. Není-li G cyklická, je $0 = t_n < \varphi(n)$, takže pro nějaký vlastní dělitel k čísla n musí platit $t_k > \varphi(k)$. Předpokládejme, že tomu tak je, zvolme prvek $a \in G$ řádu k, a označme A podgrupu tímto prvkem generovanou. Ta má k prvků, z nichž $\varphi(k)$ má řád k. Z $t_k > \varphi(k)$ plyne, že musí existovat alespoň jeden prvek $b \in G$, jenž je řádu k, ale neleží v A. Každý prvek A je kořenem polynomu $x^k - 1$. Ale i prvek b je kořenem tohoto polynomu. To znamená, že polynom $x^k - 1$ má přinejmenším $|A| + 1 = k + 1$ různých kořenů. To je ovšem spor, takže grupa G skutečně musí být cyklická. □

Je-li R nějaký okruh, S jeho podokruh a $a_1, \ldots, a_n \in R$, budeme podokruh R generovaný množinou $S \cup \{a_1, \ldots, a_n\}$ značit $S[a_1, \ldots, a_n]$. (Protože okruh polynomů $R[x]$ je generovaný $R \cup \{x\}$, není zde žádný konflikt s již zavedeným značením.)