ALGEBRA

JAN TRLIFAJ

1991 *Mathematics Subject Classification.* General Algebra??????
??????????

Obsah

1. Polynomy

Definice 1.1. Nechť $\mathcal{G} = (G, \odot, e)$ je monoid a $\mathcal{R} = (R, +, -, 0, \cdot, 1)$ je okruh. Pak definujeme *monoidový okruh* $\mathcal{RG} = (RG, +, -, \mathbf{0}, \cdot, \mathbf{1})$, kde $RG = \{f : G \to R \mid f(g) = 0 \text{ pro skoro všechna } g \in G\}$ a příslušné operace jsou definovány následovně:

$+$

$$\begin{aligned} f, f' \in RG,\ f + f' \colon G &\to R \\ g &\mapsto f(g) + f'(g) \end{aligned}$$

$-$

$$\begin{aligned} f \in RG,\ -f \colon G &\to R \\ g &\mapsto -f(g) \end{aligned}$$

$\mathbf{0}$

$$\begin{aligned} \mathbf{0} \colon G &\to R \\ g &\mapsto 0 \end{aligned}$$

$\cdot$

$$\begin{aligned} f, f' \in RG,\ f \cdot f' \colon G &\to R \\ g &\mapsto \sum_{\substack{g = h \odot h' \\ h, h' \in G}} f(h) \cdot f'(h') \end{aligned}$$

$\mathbf{1}$

$$\begin{aligned} \mathbf{1} \colon G &\to R \\ e &\mapsto 1 \\ g \neq e &\mapsto 0 \end{aligned}$$

Poznámka 1.2. Z definice množiny RG je ihned vidět, že v definici $\cdot$ sčítáme jen konečně mnoho nenulových prvků, tedy součet je dobře definován. Dokážeme nyní, že $\cdot$ je asociativní binární operace. Pro $x, y, z \in RG$, $g \in G$ máme $(x \cdot y) \cdot z(g) = \sum_{g = h \odot h'} (x \cdot y)(h) \cdot z(h') = \sum_{g = h \odot h'} \left(\sum_{h = h''' \odot h''} x(h''') \cdot y(h'') \right) \cdot z(h') = \sum_{g = h''' \odot h'' \odot h'} x(h''') \cdot y(h'') \cdot z(h')$ a stejně tak $x \cdot (y \cdot z)(g) = \sum_{g = h''' \odot h} x(h''') \cdot (y \cdot z)(h) = \sum_{g = h''' \odot h} x(h''') \cdot \left(\sum_{h = h'' \odot h'} y(h'') \cdot z(h') \right) = \sum_{g = h''' \odot h'' \odot h'} x(h''') \cdot y(h'') \cdot z(h')$. Čili $\cdot$ je asociativní binární operace. Nyní již není těžké ověřit, že $(RG, \cdot, \mathbf{1})$ je monoid a že $(RG, +, -, \mathbf{0}, \cdot, \mathbf{1})$ je skutečně okruh.

Lemma 1.3. *Nechť $\mathcal{G} = (G, \odot, e)$ je monoid a $\mathcal{R} = (R, +, -, 0, \cdot, 1)$ je okruh. Pak $\mathcal{G}$ je podmonoidem v $(RG, \cdot, \mathbf{1})$ a $\mathcal{R}$ je podokruhem v $\mathcal{RG}$.*

Důkaz. Důkazem prvního tvrzení buď následující prostý monoidový homomorfismus

$$\begin{aligned} G &\to RG \\ g &\mapsto f_g \end{aligned}$$

kde zobrazení f_g je definováno následovně

$$\begin{aligned} f_g\colon G &\to R \\ g &\mapsto 1 \\ h \neq g &\mapsto 0 \end{aligned}$$

Důkazem druhého tvrzení buď následující prostý okruhový homomorfismus

$$\begin{aligned} R &\to RG \\ r &\mapsto f_r \end{aligned}$$

kde zobrazení f_r je definováno následovně

$$\begin{aligned} f_r\colon G &\to R \\ e &\mapsto r \\ g \neq e &\mapsto 0 \end{aligned}$$

□

Příklad 1.4 (Polynomy jedné neurčité nad okruhem $\mathcal{R}$). Uvažme monoid $\mathcal{G} = (\mathbb{N}, +, 0) \simeq (\{x^n \mid n \in \mathbb{N}\}, \cdot, 1)$, kde binární operace $\cdot$ a nulární operace 1 jsou definovány následovně: $x^m \cdot x^n = x^{m+n}$ a $1 = x^0$. Isomorfismem těchto dvou monoidů je zobrazení $\varphi : n \mapsto x^n$. Množina RG pak formálně vypadá následovně: $f \in RG \Leftrightarrow f = \sum_{n\in\mathbb{N}} r_n x^n$, přičemž $f(x^n)$ je definováno jako $r_n \in R$. Okruh $\mathcal{RG}$ značíme $\mathcal{R}[x]$ a říkáme, že je to *okruh polynomů jedné neurčité nad* $\mathcal{R}$. Popišme ještě dvě základní vnoření.

$$\begin{aligned} \psi_{\mathcal{G}}\colon G &\hookrightarrow R[x] \\ n &\mapsto x^n \end{aligned}$$

$$\begin{aligned} \psi_{\mathcal{R}}\colon R &\hookrightarrow R[x] \\ r &\mapsto r \cdot x^n \end{aligned}$$

Příklad 1.5 (Polynomy konečně mnoha komutujících neurčitých nad okruhem $\mathcal{R}$). Buď $1 \leq n \in \mathbb{N}$. Uvažme monoid $\mathcal{G}_n = (\mathbb{N}, +, \bar{0}) \simeq (\{x_1^{k_1}, \dots, x_n^{k_n} \mid (k_1, \dots, k_n) \in \mathbb{N}^n\}, \cdot, 1)$, kde operace $+$, $\bar{0}$, $\cdot$, 1 jsou definovány následovně: $(k_1, \dots, k_n) + (k'_1, \dots, k'_n) = (k_1 + k'_1, \dots, k_n + k'_n)$, $\bar{0} = (0, \dots, 0)$, $(x_1^{k_1}, \dots, x_n^{k_n}) \cdot (x_1^{l_1}, \dots, x_n^{l_n}) = (x_1^{k_1+l_1}, \dots, x_n^{k_n+l_n})$ a $1 = (x_1^0, \dots, x_n^0)$. Množina RG_n formálně vypadá následovně: $f \in RG_n \Leftrightarrow f = \sum\limits_{(k_1,\dots,k_n)\in\mathbb{N}^n} r_{(k_1,\dots,k_n)} x_1^{k_1} \cdots x_n^{k_n}$, přičemž $f(x_1^{k_1} \cdots x_n^{k_n})$ je definováno jako $r_{(k_1,\dots,k_n)} \in R$. Okruh $\mathcal{RG}_n$ značíme $\mathcal{R}[x_1, \dots, x_n]$ a říkáme, že je to *okruh polynomů* n*-neurčitých nad* $\mathcal{R}$. Popišme ještě dvě základní vnoření.

$$\begin{aligned} \psi_{\mathcal{G}_n}\colon G_n &\hookrightarrow R[x_1, \dots, x_n] \\ (k_1, \dots, k_n) &\mapsto x_1^{k_1} \cdots x_n^{k_n} \end{aligned}$$

$$\begin{aligned} \psi_{\mathcal{R}}\colon R &\hookrightarrow R[x_1, \dots, x_n] \\ r &\mapsto r \cdot x_1^0 \cdots x_n^0 \end{aligned}$$

Pro obraz zobrazení $\psi_{\mathcal{G}_n}$ platí $\operatorname{Im} \psi_{\mathcal{G}_n} \simeq \mathcal{G}_n = \{x_1^{k_1} \cdots x_n^{k_n} \mid (k_1, \dots, k_n) \in \mathbb{N}^n\}$, což jsou takzvané *monické monočleny*. Pro zobrazení $\psi_{\mathcal{R}}$ platí $\operatorname{Im} \psi_{\mathcal{R}} \simeq \mathcal{R} = \{r \cdot x_1^0 \cdots x_n^0 = r \cdot 1 \mid r \in \mathcal{R}\}$, což jsou takzvané *konstantní polynomy*.

Příklad 1.6 (Polynomy κ komutujících neurčitých nad $\mathcal{R}$). Buď κ libovolný kardinál. Uvažme monoid $\mathcal{G} = (\mathbb{N}^{(\kappa)}, +, \bar{0}) \simeq (\{\prod_{\alpha\in\kappa} x_\alpha^{k_\alpha} \mid (k_\alpha) \in \mathbb{N}^{(\kappa)}\}, \cdot, 1)$. Analogicky jako v předchozích příkladech dostáváme $\mathcal{R}\mathcal{G}_\kappa$ *okruh polynomů* κ*-neurčitých nad* $\mathcal{R}$.

Příklad 1.7 (Grupové okruhy). Pokud $\mathcal{G}$ je dokonce grupa a $\mathcal{R}$ je okruh, pak okruh $\mathcal{R}\mathcal{G}$ nazýváme *grupovým okruhem grupy* $\mathcal{G}$ *nad okruhem* $\mathcal{R}$.

Věta 1.8. *Nechť $\mathcal{G}$ je grupa, K komutativní těleso a $1 \leq n \in \mathbb{N}$. Pak existuje vzájemně jednoznačná korespondence mezi třídami ekvivalence reprezentací grupy $\mathcal{G}$ stupně n nad K a třídami izomorfismů levých $K\mathcal{G}$-modulů jejichž K-dimenze je n.*

Důkaz. Uvedeme pouze náznak důkazu. Nejdřívě poznamenejme, že díky vnoření $K \hookrightarrow KG$ je každý $K\mathcal{G}$-modul i K-modul, takže skutečně můžeme požadovat, aby K-dimenze $K\mathcal{G}$-modulu byla n. Nyní ke třídě ekvivalentních reprezentací najdeme $K\mathcal{G}$-modul. Mějme tedy T třídu ekvivalentních reprezentací stupně n nad K. Poznamenejme, že se jedná o třídu zobrazení $\varphi\colon G \to GL(n, K)$. Jako nosič modulu $\mathcal{M}$ si vezmeme aritmetický prostor n-tic prvků z K, tedy $M = K^{(n)}$. Definujeme levé násobení prvky z $K\mathcal{G}$ následovně:

$$(\sum_g k_g g) \cdot \begin{pmatrix} k_1 \\ \vdots \\ k_n \end{pmatrix} \overset{def.}{=} \sum_g k_g \cdot \varphi(g) \times \begin{pmatrix} k_1 \\ \vdots \\ k_n \end{pmatrix}$$

A nyní ke $K\mathcal{G}$-modulu, jekož K-dimeze je n najdeme reprezentaci grupy $\mathcal{G}$ stupně n nad K. Nechť tedy $N \in K\mathcal{G}$-Mod, $\dim_K N = n$ a nechť B je báze $\mathcal{N}$ jako K-modulu. Definujme reprezentaci

$$\begin{aligned} \varphi\colon G &\to GL(n, K) \\ g &\mapsto A_g \end{aligned}$$

kde A_g je matice následujícího automorfismu a_g modulu $\mathcal{N}$ vzhledem k bázi B.

$$\begin{aligned} a_g\colon N &\to N \\ n &\mapsto g \cdot n \end{aligned}$$

a_g je tedy násobení zleva prvkem g. □

Příklad 1.9. Buď $\mathcal{G}$ konečná grupa, $|G| = n$, K buď komutativní těleso. Označme φ regulární reprezentaci $\mathcal{G}$ nad k. Užijeme-li značení z věty **??**, má φ následující tvar:

$$\begin{aligned} \varphi\colon G &\to GL(n, K) \\ g &\mapsto \psi(b \circ L_g \circ b^{-1}) \end{aligned}$$

Podívejme se jak vypadá odpovídající levý $K\mathcal{G}$-modul. Jako nosič si vezmeme množinu $M = K^n$, což je lineární aritmetický prostor dimenze n. Nějak nevidim jak to násobení zleva funguje a nechce se mi to koumat.

Definice 1.10. Nechť $\mathcal{G} = (G, \odot, e)$ je monoid. Řekneme, že monoid $\mathcal{G}$ je *finitární*, pokud každé $g \in G$ má jen konečně mnoho vyjádření tvaru $g = h \odot h'$, $h, h' \in G$.

Poznámka 1.11. V příkladech 1.4, 1.5 a 1.6 byly monoidy $\mathcal{G}$ (definiční obory zobrazení z RG) finitárními monoidy. Dále zřejmě platí, že grupa $\mathcal{G}$ je finitárním monoidem, právě když je to konečná grupa (poznámka k příkladu 1.7).

Definice 1.12. Nechť $\mathcal{G} = (G, \odot, e)$ je finitární monoid a $\mathcal{R} = (R, +, -, 0, \cdot, 1)$ je okruh. Pak definujeme *okruh formálních mocninných řad* $\langle\mathcal{R}\mathcal{G}\rangle = (R^G, +, -, \mathbf{0}, \cdot, \mathbf{1})$, kde R^G je množina všech zobrazení z G do R a operace na R^G jsou definovány následovně:

$+$

$$\begin{aligned} f, f' \in R^G,\ f + f' \colon G &\to R \\ g &\mapsto f(g) + f'(g) \end{aligned}$$

$-$

$$\begin{aligned} f \in RG,\ -f \colon G &\to R \\ g &\mapsto -f(g) \end{aligned}$$

$\mathbf{0}$

$$\begin{aligned} \mathbf{0} \colon G &\to R \\ g &\mapsto 0 \end{aligned}$$

$\cdot$

$$\begin{aligned} f, f' \in RG,\ f \cdot f' \colon G &\to R \\ g &\mapsto \sum_{\substack{g = h \odot h' \\ h, h' \in G}} f(h) \cdot f'(h') \end{aligned}$$

$\mathbf{1}$

$$\begin{aligned} \mathbf{1} \colon G &\to R \\ e &\mapsto 1 \\ g \neq e &\mapsto 0 \end{aligned}$$

Poznámka 1.13. Zřejmě $\mathcal{R}\mathcal{G}$ je podokruhem v $\langle\mathcal{R}\mathcal{G}\rangle$. V případě, kdy $\mathcal{G} = \mathcal{N}$ se $\langle\mathcal{R}\mathcal{G}\rangle$ značí $\mathcal{R}\langle x\rangle$ a prvkům tohoto okruhu říkáme *formální mocninné řady*, můžeme je totiž zapisovat ve tvaru $\sum_{g \in G} r_g g$. V případě, kdy $\mathcal{G} = \mathcal{N}^n$ se $\langle\mathcal{R}\mathcal{G}\rangle$ značí $\mathcal{R}\langle x_1, \ldots, x_n\rangle$. V případě, kdy $\mathcal{G} = \mathcal{N}^{(\kappa)}$ se $\langle\mathcal{R}\mathcal{G}\rangle$ značí $\mathcal{R}\langle\kappa\rangle$. Pokud $\mathcal{G}$ je konečná grupa, platí, že $\mathcal{R}\mathcal{G} = \langle\mathcal{R}\mathcal{G}\rangle$. Ještě syntaktický monoid nad A, jenže tomu nějak nerozumim.

Definice 1.14. Nechť $\mathcal{R}$ je okruh a nechť $\mathcal{R}[x_1, \ldots, x_n]$ značí okruh polynomů n-neurčitých nad $\mathcal{R}$. Z příkladu 1.5 víme, že $f \in RG \Leftrightarrow f = \sum_{(k_1, \ldots, k_n) \in \mathbb{N}^n} r_{(k_1, \ldots, k_n)} x_1^{k_1} \cdots x_n^{k_n}$. Definujeme *nosič* polynomu f jako $\operatorname{supp}(f) = \{(k_1, \ldots, k_n) \mid r_{(k_1, \ldots, k_n)} \neq 0\}$. Polynom f se dá tedy zapsat také jako $f = \sum_{(k_1, \ldots, k_n) \in \operatorname{supp}(f)} r_{(k_1, \ldots, k_n)} x_1^{k_1} \cdots x_n^{k_n}$.

Definice 1.15. Buď f *nenulový* polynom z $\mathcal{R}[x_1, \ldots, x_n]$. Definujme *stupeň* polynomu f jako $\deg(f) = \max\{\sum_{i=1}^n k_i \mid (k_1, \ldots, k_n) \in \operatorname{supp}(f)\}$.

Definice 1.16. Na množině všech monických monočlenů z $\mathcal{R}[x_1, \ldots, x_n]$ definujeme uspořádání následujícím způsobem: $x_1^{k_1} \cdots x_n^{k_n} < x_1^{l_1} \cdots x_n^{l_n} \overset{def.}{\Leftrightarrow} (k_1, \ldots, k_n) <_{LEX} (l_1, \ldots, l_n)$. Kde $<_{LEX}$ je lexikografické uspořádání na $\mathbb{N}^n$ (čili pro $(k_1, \ldots, k_n) \neq (l_1, \ldots, l_n)$ je $(k_1, \ldots, k_n) <_{LEX} (l_1, \ldots, l_n)$, právě když pro i nejmenší takové, že $k_i \neq l_i$ platí, že $k_i < l_i$). Definujeme též neostrou verzi tohoto uspořádání. Pro dva mnoické monočleny u, v platí $u \leq v \overset{def.}{\Leftrightarrow} (u < v) \vee (u = v)$.

Poznámka 1.17. Poznamenejme některé z vlastností právě definovaného uspořádání.

(1) Pro libovolný monický monočlen u různý od $1 = x_1^0 \cdots x_n^0$ platí, že $1 < u$.
(2) Pro u,v,w monické monočleny platí, že $u < v \Rightarrow u \cdot w < v \cdot w$.
(3) Uspořádání $<$ je artinovské. Čili na množině všech monických monočlenů neexistuje ostře klesající nekonečný řetězec v uspořádání $<$.
(4) Uspořádání $<$ je lineární.

Definice 1.18. Buď f nenulový polynom z $\mathcal{R}[x_1, \ldots, x_n]$. Definujme *výšku* polynomu f jako $\mathrm{ht}\,(f) = \max_{LEX} \{(k_1, \ldots, k_n) \mid (k_1, \ldots, k_n) \in \mathrm{supp}\,(f)\}$.

Definice 1.19. Buď f nenulový polynom z $\mathcal{R}[x_1, \ldots, x_n]$. Definujme *vedoucí monočlen* polynomu f jako $\mathrm{lm}\,(f) = x_1^{k_1} \cdots x_n^{k_n}$, kde $(k_1, \ldots, k_n) = \mathrm{ht}\,(f)$.

Definice 1.20. Buď $f = \sum_{(k_1,\ldots,k_n)\in\mathbb{N}^n} r_{(k_1,\ldots,k_n)} x_1^{k_1} \cdots x_n^{k_n}$ nenulový polynom z $\mathcal{R}[x_1, \ldots, x_n]$. Definujme *vedoucí koeficient* polynomu f jako $\mathrm{lc}\,(f) = r_{(k_1,\ldots,k_n)}$, kde $(k_1, \ldots, k_n) = \mathrm{ht}\,(f)$.

Příklad 1.21. Uvažme okruh $\mathcal{Q}[x_1, \ldots, x_n]$ a polynom $f = 3x_1^2x_5 + 10x_2^{12}x_4 + x_3^7$. Pak platí $\deg(f) = 13$, $\mathrm{ht}\,(f) = (2, 0, 0, 0, 1)$, $\mathrm{lm}\,(f) = x_1^2x_5$ a $\mathrm{lc}\,(f) = 3$.

Příklad 1.22. Uvažme okruh $\mathcal{R}[x]$ a libovolný nenulový polynom $f = \sum_{n=0}^{k} a_n x^n$, $a_0, \ldots, a_k \neq 0$ z tohoto okruhu. Pak platí $\deg(f) = k$, $\mathrm{ht}\,(f) = (k)$, $\mathrm{lm}\,(f) = x^k$, $\mathrm{lc}\,(f) = a_k$.

Lemma 1.23. *Pro libovolné dva nenulové polynomy f, g z $\mathcal{R}[x_1, \ldots, x_n]$ platí:*

(i) $lm(f \cdot g) = lm(f) \cdot lm(g)$
(ii) $lc(f \cdot g) = lc(f) \cdot lc(g)$
(iii) $ht(f \cdot g) = ht(f) + ht(g)$

Důkaz. Monický monočlen $\mathrm{lm}\,(f)$ je jednoznačně charakterizován vlastností $\mathrm{lm}\,(f) > u$ pro libovolný monočlen (znormovaný) u vyskytující se v f. Analogicky platí $\mathrm{lm}\,(g) > v$ pro libovolný monočlen (znormovaný) v vyskytující se v g. Nyní využijeme vlastnost (2) z poznámky 1.17 a dostáváme $\mathrm{lm}\,(f) \cdot \mathrm{lm}\,(g) > \mathrm{lm}\,(f) \cdot v > u \cdot v$, z čehož tvrzení přímo plyne. Druhé a třetí tvrzení jsou snadným důsledkem prvního. □

Lemma 1.24. *Nechť $\mathcal{R}$ je obor integrity. Pak i $\mathcal{R}[x_1, \ldots, x_n]$ je obor integrity.*

Důkaz. Mějme dva nenulové polynomy z $\mathcal{R}[x_1, \ldots, x_n]$. Potřebujeme dokázat, že i jejich součin je nenulový polynom. To je však snadným důsledkem lemmatu 1.23. □

Definice 1.25. Nechť $\mathcal{R}$ je okruh. Potom $\mathcal{R}$ je *obor integrity hlavních ideálů* (OIHI), pokud $\mathcal{R}$ je obor integrity a každý ideál v $\mathcal{R}$ je hlavní (tj. generovaný jedním prvkem).

Příklad 1.26. Uveďme pár příkladů oborů integrity hlavních ideálů.

(1) Okruh $\mathcal{Z}$ je oborem integrity hlavních ideálů. Ideály v $\mathcal{Z}$ jsou právě všechny podgrupy v $\mathcal{Z}$, ty jak víme jsou tvaru $\mathbb{Z} \cdot n$, $n \in \mathbb{N}$.
(2) Každé komutativní těleso K je jistě oborem integrity hlavních ideálů, neboť K obsahuje právě dva ideály I_1, I_2, které jsou tvaru $I_1 = \{0\} = K \cdot 0$ a $I_2 = K = K \cdot 1$.

Lemma 1.27. *Nechť $\mathcal{R}$ je obor itegrity, $f, g \in \mathcal{R}[x]$, $g \neq 0$ a nechť $lc(g)$ je invertibilní v $\mathcal{R}$. Pak existují jednoznačně určené polynomy $p, q \in R[x]$ takové, že $f = q \cdot g + p$ a $deg(p) < deg(g)$.*

Důkaz. Nejdříve dokážeme existenci polynomů p a q. Pokud je $\deg(f) < \deg(g)$, vezmeme jako p polynom f a jako q nulový polynom. Nechť tedy $\deg(f) = \deg(g)+k$, $k \geq 0$. Polynomy f a g můžeme vyjádřit v následujícím tvaru:

$$f = \sum_{n=0}^{m+k} a_n x^n,\ g = \sum_{n=0}^{m} b_n x^n$$

kde $a_{m+k} \neq 0$ a b_m je invertibilní v $\mathcal{R}$. Důkaz existence p a q provedeme indukcí dle k. Pokud je k rovno nule, zvolíme p a q následovně:

$$\begin{aligned} q &= a_m b_m^{-1} \\ p &= f - q \cdot g = f - a_m b_m^{-1}(\sum_{n=0}^{m} b_m x^m) \end{aligned}$$

Zřejmě platí, že $f = q \cdot g + p$ a $\deg(p) < m = \deg(g)$. Nechť nyní je $k > 0$. Položme $f_1 = f - a_{m+k} b_m^{-1} x^k g$, pak $\deg(f_1) < m + k$. Polynomy f_1 a g splňují indukční předpoklad, takže existují q_1 a $p_1 \in R[x]$ takové, že $f_1 = q_1 \cdot g + p_1$ a $\deg(p_1) < \deg(g)$. Dostáváme:

$$f = f_1 + a_{m+k} b_m^{-1} x^k g = (q_1 + a_{m+k} b_m^{-1} x^k) g + p_1$$

Volbou $q = (q_1 + a_{m+k} b_m^{-1} x^k)$ a $p = p_1$ máme $f = q \cdot g + p$ a $\deg(p) < \deg(g)$. Zbývá ukázat jednoznačnost p a q. Nechť tedy $f = q_1 \cdot g + p_1 = q_2 \cdot g + p_2$, $\deg(p_i) < \deg(g)$ pro $i = 1.2$. Úpravou předchozího dostáváme:

$$(q_1 - q_2) g = p_2 - p_1$$

Předpokládejme pro spor, že $(q_1 - q_2) \neq 0$. Nyní spočítáme stupně polynomů na levé a pravé straně rovnosti: $\deg((q_1 - q_2)g) = \deg((q_1 - q_2)) + \deg(g) \geq \deg(g)$, ale $\deg(p_2 - p_1) < \deg(g)$, z čehož plyne, že $q_1 = q_2$ a to ihned implikuje $p_1 = p_2$, čímž je dokázána jednoznačnost polynomů p a q. □

Důsledek 1.28. *Nechť K je komutativní těleso, pak $\mathcal{R} = K[x]$ je obor integrity hlavních ideálů (OIHI).*

Důkaz. Nechť $\mathcal{I}$ je vlastní ideál v $\mathcal{R}$. Označme n_0 minimální prvek množiny $\{n \in \mathbb{N} \mid \exists\, f \in I\colon f \neq 0 \wedge \deg(f) = n\}$ a f_0 příslušný polynom z I. Dokážeme, že $I = Rf_0 = \{g \cdot f \mid g \in R\}$. Zřejmě $Rf_0 \subseteq I$ neboť $\mathcal{I}$ je ideál. Naopak pro libovolný polynom $h \in I$ existují podle lemmatu 1.27 polynomy p a $q \in R$ takové, že $h = q \cdot f_0 + p$ a $\deg(p) < \deg(f_0)$. Jelikož polynomy h a $q \cdot f_0$ jsou z ideálu $\mathcal{I}$, je i polynom p z $\mathcal{I}$. Stupeň polynomu f_0 byl minimální ze všech nenulových polynomů z $\mathcal{I}$, z čehož plyne, že p je nulový polynom. Takže máme $h = q \cdot f_0$, což dokazuje opačnou inkluzi. □

Příklad 1.29. Následující příklad ukazuje, že důsledek 1.28 nelze zobecnit na okruh polynomů více než jedné proměnné. Nechť $\mathcal{R} = K[x_1, x_2]$, kde K je komutativní těleso. Uvažme vlastní ideál $I = R \cdot x_1 + R \cdot x_2$, ukážeme, že tento ideál není hlavní. Pro spor předpokládejme, že $R \cdot x_1 + R \cdot x_2 = R \cdot f$. Pro polynomy x_1 a x_2 tedy existují polynomy g_1 a g_2 tak, že $x_1 = g_1 \cdot f$ a $x_2 = g_2 \cdot f$. Z 1.23 dostáváme náledující rovnost:

$$x_1 = \mathrm{lm}(x_1) = \mathrm{lm}(g_1) \cdot \mathrm{lm}(f)$$

Ze které plyne, že $f = x_1$ nebo $f = 1$. Obdobně:

$$x_2 = \mathrm{lm}(x_2) = \mathrm{lm}(g_2) \cdot \mathrm{lm}(f)$$

Z čehož plyne, že $f = x_1$ nebo $f = 1$. Takže $f = 1$ a tedy $I = R$, což je spor neboť ideál $\mathcal{I}$ je jistě vlastní. Tento příklad zároveň ukazuje, že vlastnost okruhu být OIHI se nepřenáší na okruh polynomů jedné proměnné (to plyne z toho, že $(K[x_1])[x_2] \simeq K[x_1, x_2]$).

Definice 1.30. Nechť $\mathcal{R}$ je okruh. $\mathcal{R}$ je *noetherovský* okruh, pokud v $\mathcal{R}$ neexistuje nekonečný ostře rostoucí řetězec ideálů.

Věta 1.31 (Hilbertova věta o bázi)**.** *Nechť $\mathcal{R}$ je noetherovský okruh, pak je noetherovský i okruh $\mathcal{R}[x]$.*

Důkaz. Na přednášce sme to nedělali, důkaz, který znám já potřebuje tvrzení, které ještě neznáme. □

Lemma 1.32. *Nechť $\mathcal{R}$ je obor integrity hlavních ideálů, pak $\mathcal{R}$ je noetherovský okruh.*

Důkaz. Pro spor předpokládejme, že v $\mathcal{R}$ existuje nekonečný ostře rostoucí řetězec ideálů $I_1 \subsetneq I_2 \dots I_n \subsetneq I_{n+1} \subsetneq \dots$. Uvažme množinu $I = \bigcup_{n\in\mathbb{N}} I_n$. Pro libovolné dva prvky a, $b \in I$ existuje $n \in \mathbb{N}$ tak, že $a \in I_n$ a $b \in I_n$, takže i $a \pm b \in I_n \subseteq I$ a $r \cdot a \in I_n \subseteq I$, z čehož plyne, že I s restrikcemi operací z $\mathcal{R}$ je ideál. Protože $\mathcal{I}$ je ideál, existuje $r \in R$ takové, že $I = R \cdot r$, ale zároveň musí existovat i $n \in \mathbb{N}$ takové, že $r \in I_n$. Protože $\mathcal{I}_n$ je ideál, platí, že $R \cdot r \subseteq I_n$, což implikuje $I \subseteq I_n \subseteq I$. Takže dostáváme $I = I_n = I_{n+1}$, což je spor s tím, že řetězec ideálů byl ostře rostoucí. □

Definice 1.33. Nechť $\mathcal{R}$ je obor integrity. $\mathcal{R}$ splňuje *podmínku (K)* (podmínku konečnosti řetězců vlastních dělitelů), pokud v $\mathcal{R}$ neexistuje nekonečný ostře rostoucí řetězec hlavních ideálů.

Poznámka 1.34. Zřejmě každý noetherovský obor integrity splňuje podmínku (K).

Poznámka 1.35. Nechť $\mathcal{R}$ je obor integrty. Pokud $R \cdot r_1 \subseteq R \cdot r_2$, pak existuje $r \in R$ takové, že $r_1 = r \cdot r_2$, říkáme, že r_2 *dělí* r_1, značíme $r_2 \mid r_1$. Zřejmě $R \cdot r_1 \subsetneq R \cdot r_2 \Leftrightarrow r_2 \mid r_1 \wedge r_1 \nmid r_2$. Dále říkáme, že r,$s \in R$ jsou *asociované* v $\mathcal{R}$, pokud $r \mid s \wedge s \nmid r$, značíme $r \parallel s$. Relace být asociován je relace ekvivalence na R.

Příklad 1.36. Nechť $\mathcal{R}$ je obor integrity. Pak $r \parallel 1$ právě když $R \cdot r = R$, což je právě tehdy, když existuje prvek $s \in R$ takový, že $s \cdot r = 1$, tedy právě když r je invertibilní prvek $\mathcal{R}$.

Lemma 1.37. *Nechť $\mathcal{R}$ je obor integrity a nechť r a s jsou jeho dva nenulové prvky. Pak r je asociováno s s v $\mathcal{R}$, právě když v $\mathcal{R}$ existuje invertibilní prvek u takový, že $r = u \cdot s$.*

Důkaz. Pokud je r asociováno s s v $\mathcal{R}$, existují r_1, $s_1 \in R$ tak, že $r_1 \cdot r = s$ a $s_1 \cdot s = r$. Dostáváme $(r_1 \cdot s_1) \cdot s = s$, z čehož plyne $s \cdot (1 - r_1 \cdot s_1) = 0$ a jelikož je dle předpokladu s nenulové, máme $r_1 \cdot s_1 = 1$. Hledané u je tedy s_1.

Pokud v $\mathcal{R}$ existuje invertibilní prvek u takový, že $r = u \cdot s$, pak $R \cdot r = R \cdot u \cdot s = R \cdot s$, z čehož plyne, že r a s jsou asociované. □

Definice 1.38. Nechť $\mathcal{R}$ je obor integrity. $\mathcal{R}$ splňuje *podmínku (D)* (podmínku existence *největšího společného dělitele*), pokud pro každé r, $s \in R$ existuje $t \in R$ takové, že

(1) $t \mid r$ a $t \mid s$, čili t je *společný dělitel* r a s, což značíme $t = \mathrm{SD}(r, s)$.
(2) pro každé $t' \in R$ platí následující implikace: $(t' \mid r \wedge t' \mid s) \Rightarrow t' \mid t$, čili t je dělen každým společným dělitelem r a s.

Toto jednoznačně určené t značíme $\mathrm{NSD}(r, s)$ a říkáme, že je to *největší společný dělitel* r a s.

Definice 1.39. Obor integrity $\mathcal{R}$ je *Gaussův*, pokud $\mathcal{R}$ splňuje podmínky (K) a (D).

Poznámka 1.40. Občas budeme Gaussovo obory integrity nazývat obory integrity *splňující podmínku N*.

Lemma 1.41. *Nechť $\mathcal{R}$ je obor integrity hlavních ideálů. Pak $\mathcal{R}$ je Gaussův obor integrity.*

Důkaz. Obor integrity $\mathcal{R}$ splňuje jistě podmínku (K), neboť $\mathcal{R}$ je podle lemmatu 1.32 noetherovský. Pro ověření podmínky (D) mějme libovolné r, $s \in R$. Nechť t je generátor ideálu $I = R \cdot r + R \cdot s$, pak t je zřejmě největším společným dělitelem r a s. Navíc existují prvky r', $s' \in R$ takové, že $t = r' \cdot r + s' \cdot s$. □

Definice 1.42. Nechť $\mathcal{R}$ je obor integrity a nechť r je prvek z R, pro který platí $r \neq 0$ a $r \nparallel 1$. Pak prvek r je *irreducibilní*, pokud pro každý prvek $s \in R$ platí následující implikace: $s \mid r \Rightarrow (s \parallel r \vee s \parallel 1)$. Prvek r je *prvočinitel*, pokud $R \cdot r$ je prvoideál (tj. $\forall\, s_1, s_2 \in R \colon r \mid s_1 \cdot s_2 \Rightarrow (R \mid s_1 \vee r \mid s_2)$).

Poznámka 1.43. Nechť $\mathcal{R}$ je obor integrity, $r \in R$ je prvočinitel a nechť $s_1, \dots, s_n \in R$. Z definice prvočinitele se snadno indukcí dokáže následující implikace: $r \mid (s_1 \cdots s_k) \Rightarrow \exists\, k \in \mathbb{N}$: $r \mid s_k$.

Lemma 1.44. *Nechť $\mathcal{R}$ je obor integrity. Pak každý prvočinitel je irreducibilní.*

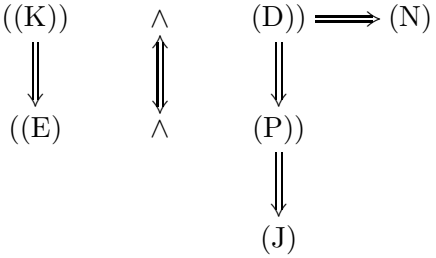
Důkaz. Nechť r je prvočinitel. Pokud prvek s dělí r, pak existuje prvek $s' \in R$ takový, že $r = s \cdot s'$. Jistě $r \mid s \cdot s'$ a protože r je prvočinitel, platí, že $r \mid s$ nebo $r \mid s'$. Pokud nastane první možnost, jsme hotovi. Předpokládejme tedy druhou možnost, tedy $s' = r \cdot r'$, dostáváme $r = s \cdot s' = s \cdot r \cdot r'$, což implikuje $r \cdot (1 - s \cdot r') = 0$ a protože r je jistě nenulové, máme $1 = s \cdot r'$, z čehož plyne, že $s \parallel 1$. □

Definice 1.45. Nechť $\mathcal{R}$ je obor integrity. $\mathcal{R}$ splňuje *podmínku (P)* (prvočíselnou podmínku), pokud každý irreducibilní prvek $\mathcal{R}$ je prvočinitelem.

Definice 1.46. Nechť $\mathcal{R}$ je obor integrity. $\mathcal{R}$ splňuje *podmínku (E)* (podmínku existence irreducibilních rozkladů), pokud pro každý nenulová prvek $\mathcal{R}$, který není asociovaný s 1 platí, že a je součinem irreducibilních prvků (tj. $(\exists\, n \in \mathbb{N})$ $(\exists\, a_1, \dots a_n \in R$, a_i irreducibilní $\forall\, i = 1, \dots, n) \colon a = a_1 \cdots a_n)$.

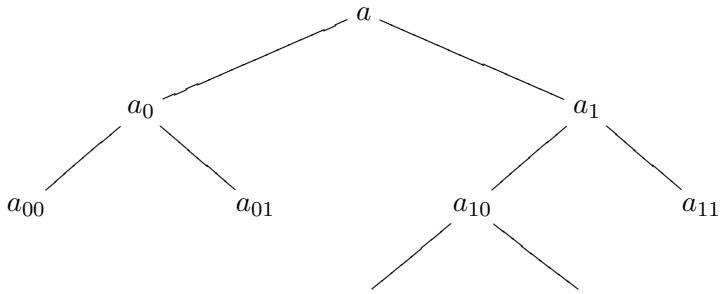
Definice 1.47. Nechť $\mathcal{R}$ je obor integrity. $\mathcal{R}$ splňuje *podmínku (J)* (podmínku jednoznačnosti irreducibilních rozkladů), pokud platí následující tvrzení. Nechť $\{a_1, \dots, a_m\}$, $\{b_1, \dots, b_n\}$ jsou dvě neprázdné množiny irreducibilních prvků z $\mathcal{R}$ takové, že $a_1 \cdots a_m = b_1 \cdots b_n$, pak $n = m$ a existuje permutace $\pi \in S_m$ taková, že $a_i \parallel b_{\pi(i)}$ pro každé $i = 1, \dots, m$.

Poznámka 1.48. Nyní dokážeme, že mezi právě definovanými podmínkami platí následující vztahy:



Lemma 1.49. *Nechť $\mathcal{R}$ je obor integrity. Pak platí: (K) $\Rightarrow$ (E).*

Důkaz. Pro spor předpokládejme, že máme nenulé $a \in R$, které není asociováno s 1 takové, že a není součinem irreducibilních prvků. Pro a tedy platí, že $a = a_0 \cdot a_1$, kde a_0 a a_1 jsou vlastní dělitelé a. Takto můžeme pokračovat dále (např. $a_0 = a_{00} \cdot a_{01}$) a dostaneme následující *nutně nekonečný* strom T:



Tento strom je spočetně nekonečný a 2-větvící, takže z Konigovo věty plyne, že v T existuje nekonečná větev, což znamená, že v $\mathcal{R}$ existuje následující nekonečný ostře rostoucí řetězec hlavních ideálů: $R \cdot a \subsetneq R \cdot a_1 \subsetneq R \cdot a_{10} \subsetneq R \cdot a_{010} \ldots$, čímž jsme dostali spor s podmínkou (K). □

Lemma 1.50. *Nechť $\mathcal{R}$ je obor integrity splňující podmínku (D), a, $b \in R$, $0 \neq d \in R$. Pak platí následující implikace: $c = NSD\,(a, b) \Rightarrow cd = NSD\,(ad, bd)$.*

Důkaz. Označme $e = \mathrm{NSD}\,(ad, bd)$. Protože $c = \mathrm{NSD}\,(a, b)$, existují x, $y \in R$ tak, že $cx = a$ a $cy = b$. Máme tedy $cdx = ad$ a $cdy = bd$, takže cd je společným dělitelem ad a bd. Z definice největšího společného dělitele plyne, že existuje $f \in R$ tak, že $cdf = e$. Našim cílem bude ukázat, že $f \parallel 1$ (pak totiž $cd \parallel e$, z čehož plyne že $cd = \mathrm{NSD}\,(ad, bd)$). Protože $e = \mathrm{NSD}\,(ad, bd)$, existují u, $v \in R$ tak, že $eu = ad$ a $ev = bd$. Dostáváme $cdfu = ad$ a $cdfv = bd$, což implikuje $d(cfu - a) = 0$ a $d(b - cfv) = 0$ a podle předpokladu věty máme $cfu = a$ a $cfv = b$. Takže $cf = \mathrm{SD}\,(a, b)$, z čehož plyne, že $cf \mid c$ a to konečně implikuje $f \parallel 1$. □

Lemma 1.51. *Nechť $\mathcal{R}$ je obor integrity. Pak platí: (D) $\Rightarrow$ (P).*

Důkaz. Uvažme nenulový prvek $r \in \mathcal{R}$, který není asociován s 1 a je irreducibilní, dokážeme, že r je prvočinitel. Předpokládejme, že $r \mid s_1 \cdot s_2$ a že $r \nmid s_1$, naším cílem je tedy ukázat, že $r \mid s_2$. Označme $t = \mathrm{NSD}\,(r, s_1)$. Protože t jistě dělí r, dostáváme z definice irreducibilního prvku, že $t \parallel r$ nebo $t \parallel 1$. Pokud by nastala první možnost, měli bychom $r \mid s_1$, což podle předpokladu není možné. Platí tedy druhá možnost. Z lemmatu 1.50 plyne následující implikace $1 = \mathrm{NSD}\,(r, s_1) \Rightarrow s_2 = \mathrm{NSD}\,(r \cdot s_2, s_1 \cdot s_2)$ a protože $r \mid s_1 \cdot s_2$ máme, že $r = \mathrm{SD}\,(r \cdot s_2, s_1 \cdot s_2)$, z čehož plyne, že $r \mid s_2$. □

Lemma 1.52. *Nechť $\mathcal{R}$ je obor integrity. Pak platí: (P) $\Rightarrow$ (J).*

Důkaz. Dokážeme následující silnější tvrzení. Nechť $\{a_1, \ldots, a_m\}$, $\{b_1, \ldots, b_n\}$ jsou dvě neprázdné množiny irreducibilních prvků z $\mathcal{R}$ takové, že $(a_1 \cdots a_m) \parallel (b_1 \cdots b_n)$, pak $n = m$ a existuje permutace $\pi \in S_m$ taková, že $a_i \parallel b_{\pi(i)}$ pro každé $i = 1, \ldots, m$. Důkaz provedeme indukcí dle $k = m + n$. Pokud $k = 2$, je tvrzení triviálně splněné. Pokud $k = 3$, vypadá část předpokladu silnějšího tvzení následovně: $a_1 \cdot a_2 \parallel b_1$ (popř. $a_1 \parallel b_1 \cdot b_2$), jenže v obou případech dostáváme spor s irreducibilitou prvků z obou množin. Nechť tedy je $m + n = k \geq 4$ a nechť

$(a_1 \cdots a_m) \parallel (b_1 \cdots b_n)$. Máme $a_1 \cdots a_m = u \cdot b_1 \cdots b_n$, kde $u \parallel 1$. Jistě $a_m \mid (u \cdot b_1) \cdot b_2 \cdots b_n$ a protože a_m je prvočinitel, existuje podle poznámky 1.43 $j \in \{1, \ldots, n\}$ (toto j označíme jako $\pi(m)$) tak, že $a_m \mid b_{\pi(m)}$ a protože a_m i $b_{\pi(m)}$ jsou prvočinitelé, platí, že $a_m \parallel b_{\pi(m)}$, z čehož plyne $b_{\pi(m)} = u_m \cdot a_m$, kde $u_m \parallel 1$. Dostáváme:

$$\begin{aligned} a_1 \cdots a_m &= u \cdot b_1 \cdots b_n \\ a_1 \cdots a_m &= u \cdot b_1 \cdots b_{\pi(m)-1} \cdot (u_m \cdot a_m) \cdot b_{\pi(m)+1} \cdots b_n \\ a_1 \cdots a_{m-1} &= (u' \cdot b_1) \cdots b_{\pi(m)-1} \cdot b_{\pi(m)+1} \cdots b_n \end{aligned}$$

kde u' je asociováno s 1 a protože $m-1+n-1 = k-2$, můžeme použít indukční předpoklad, ze kterého plyne $m = n$ a existence $\pi' \in S_{m-1}$ tak, že $a_i \parallel b_{\pi'(i)}$ pro $i = 1, \ldots, m-1$. Hledanou permutaci $\pi \in S_m$ získáme z permutace $\pi' \in S_{m-1}$ dodefinováním na prvku m a to následovně: $\pi(m) = j$. □

Lemma 1.53. *Nechť $\mathcal{R}$ je obor integrity. Pak platí: ((E) ∧ (J)) ⇒ (K).*

Důkaz. Pro spor předpokládejme následující ostře rosoucí řetězec hlavních ideálů:

$$R \cdot a_1 \subsetneq R \cdot a_2 \subsetneq R \cdot a_3 \subsetneq \cdots \subsetneq R \cdot a_n \subsetneq R \cdot a_{n+1} \subsetneq \ldots$$

Prvek a_1 jistě není asociován s 1, neboť pak by $R \cdot a_1 = R$ a můžeme též předpokládat, že $a_1 \neq 0$ (pokud by $a_1 = 0$, začali bychom řetězec prvkem $R \cdot a_2$). Z podmínky (E) plyne, že prvek a_1 má irreducibilní rozklad, tedy $a_1 = b_1 \cdots b_n$, $n \in \mathbb{N}$. Z ostře rostoucího řetězce plyne následující:

$$a_1 = a_2 d_1 = a_3 d_2 d_1 = \ldots = a_{n+1} d_n d_{n-1} \cdots d_1 = \ldots$$

Jak pro prvky a_i, tak pro prvky d_i, $i = 1, 2, \ldots$ platí, že jsou nenulové a nejsou asociované s 1. Z podmínky (E) plyne, že prvek a_{n+1} a každý z prvků d_i, $i = 1, 2, \ldots$ má irreducibilní rozklad. Každý z těchto rozkladů obsahuje alespoň jeden irreducibilní prvek, čímž jsme dostali irreducibilní rozklad prvku a_1, který má alespoň $n+1$ členů, což je spor s podmínkou (J). □

Lemma 1.54. *Nechť $\mathcal{R}$ je obor integrity. Pak platí: ((E) ∧ (J)) ⇒ (D).*

Důkaz. Mějme dva prvky a, b z R, chceme ukázat, že existuje jejich největší společný dělitel c. Bez újmy na obecnosti můžeme předpokládat, že a i b jsou nenulové a nejsou asociovány s 1. Z podmínky (E) plyne existence následujících rozkladů:

$$\begin{aligned} a &\parallel p_1^{k_1} \cdots p_m^{k_m} \\ b &\parallel q_1^{l_1} \cdots q_n^{l_n} \end{aligned}$$

kde prvky $p_i, i = 1, \ldots, m$ a $q_i, i = 1, \ldots, n$, jsou irreducibilní a platí, že $p_i \neq p_j$ pro $i \neq j$, $i, j \leq m$ a $q_i \neq q_j$ pro $i \neq j$, $i, j \leq n$. Zřejmě existuje $j \leq m$ tak, že prvky rozkladů můžeme přeuspořádat tak, aby platilo následující:

$$\begin{aligned} p_i &\parallel q_i && \forall\, i \in \{1, \ldots, j\} \\ p_i &\nparallel q_k && \forall\, i \in \{j+1, \ldots, m\},\ \forall\, k \in \{1, \ldots, n\} \\ q_i &\nparallel p_k && \forall\, i \in \{j+1, \ldots, n\},\ \forall\, k \in \{1, \ldots, m\} \end{aligned}$$

Pro $i \in \{1, \ldots, j\}$ označme $r_i = \min(k_i, l_i)$. Nyní dokážeme, že prvek

$$c = \begin{cases} p_1^{r_1} \cdots p_j^{r_j}, & \text{pokud } j > 0 \\ 1, & \text{pokud } j = 0 \end{cases}$$

je největším společným dělitelem prvků a a b. Zřejmě c je společným dělitelem a a b. Mějme libovolný společný dělitel d prvků a a b, ukážeme, že $d \mid c$. Ze vztahu $d = \mathrm{SD}\,(a,b)$ plyne exitence prvků x, $y \in R$ takových, že $dx = a$ a $dy = b$. Podmínka (E) dává existenci ireducibilního rozkladu $d = s_1^{h_1} \cdots s_t^{h_t}$. Ze vztahu $dx = a$ a podmínky (J) plyne, že $t \leq m$ a že existuje zobrazení $\pi\colon \{1,\dots,t\} \to \{1,\dots,m\}$ takové, že platí $s_i \parallel p_{\pi(i)}$, $i = 1,\dots,t$ a zároveň dostáváme, že $h_i \leq k_i$, $i = 1,\dots t$. Ze vztahu $dy = b$ a podmínky (J) plyne, že $t \leq n$ a že existuje zobrazení $\sigma\colon \{1,\dots,t\} \to \{1,\dots,n\}$ takové, že platí $s_i \parallel q_{\sigma(i)}$, $i = 1,\dots,t$ a zároveň dostáváme, že $h_i \leq l_i$, $i = 1,\dots t$. Z předchozích vztahů plyne, že $q_{\sigma(i)} \parallel p_{\pi(i)}$, což implikuje $\sigma(i) = \pi(i) \leq j$. Dostáváme, že $d \parallel p_{\pi(1)}^{h_1} \cdots p_{\pi(t)}^{h_t}$ a protože $h_i \leq \min\,(k_i, l_i) = r_i$, $i = 1,\dots,t$, máme $d \mid c$, čímž je důkaz hotov. □

Věta 1.55. *Nechť $\mathcal{R}$ je obor integrity. Potom $\mathcal{R}$ je Gaussův (splňuje podmínku (N)) právě když $\mathcal{R}$ splňuje podmínky (E) a (J), což je právě tehdy když $\mathcal{R}$ splňuje podmínky (E) a (P).*

Důkaz. První implikace z leva do prava plyne z lemmat 1.49, 1.51, 1.52 a z prava do leva plyne z lemmat 1.53, 1.54. Druhá implikace z leva do prava plyne z lemmat 1.54, 1.51 a z prava do leva plyne z lemmatu 1.52. □

Věta 1.56. *Nechť K je komutativní těleso. Pak okruh polynomů $K[x]$ je Gaussův.*

Důkaz. Tohle neumim. □

Definice 1.57. Nechť $\mathcal{R}$ je obor integrity. Pak $\mathcal{R}$ je *Euklidovský* obor integrity, pokud existuje zobrazení $\varphi\colon R \to \mathbb{Z}$ mající následující vlastnosti:

(1) $(\forall\, a, b \in R, b \neq 0)\colon a \mid b \Rightarrow \varphi(a) \leq \varphi(b)$.
(2) $(\forall\, a, b \in R, b \neq 0)(\exists\, c, d \in R)\colon a = b \cdot c + d \wedge \varphi(d) < \varphi(b)$

Zobrazení φ se nazývá *Euklidovská* norma na $\mathcal{R}$.

Příklad 1.58. Uveďme pár příkladů Euklidovských oborů integrity.

(1) Buď $\mathcal{R} = \mathcal{Z}$ a Euklidovskou normu na $\mathcal{R}$ definujeme následovně:

$$\begin{aligned} \varphi\colon R &\to \mathbb{Z} \\ z &\mapsto |z| \end{aligned}$$

Tento příklad zároveň ukazuje, že prvky c, $d \in R$ z definice 1.57 nemusí být určeny jednoznačně (např. $5 = 3 \cdot 2 - 1$ a $5 = 2 \cdot 2 + 1$).

(2) Buď $\mathcal{R} = K[x]$, kde K je komutativní těleso a Euklidovskou normu na $\mathcal{R}$ definujeme následovně:

$$\begin{aligned} \varphi\colon R &\to \mathbb{Z} \\ 0 &\mapsto -1 \\ f \neq 0 &\mapsto \deg(f) \end{aligned}$$

(3) Buď $R = \{a + b \cdot i \mid a, b \in \mathbb{Z}\} \subseteq \mathbb{C}$ (této množině říkáme *Gaussova* celá čísla), Euklidovskou normu na $\mathcal{R}$ definujeme následovně:

$$\begin{aligned} \varphi\colon R &\to \mathbb{Z} \\ a + b \cdot i &\mapsto a^2 + b^2 \end{aligned}$$

Dokážeme, že zobrazení φ má vlastnosti (1) a (2) z definice 1.57. Máme $\varphi((a+bi)(c+di)) = (ac - bd)^2 + (ad + cb)^2 = (a^2 + b^2)(c^2 + d^2) = \varphi(a + bi) \cdot \varphi(c + di)$. Nyní pokud $r \mid s \neq 0$, existuje nenulové $r' \in R$ tak, že $s = r \cdot r'$, což implikuje $\varphi(s) = \varphi(r) \cdot \varphi(r')$ a

jelikož $\varphi(r') \geq 1$, máme $\varphi(r) \leq \varphi(s)$, což jsme chtěli dokázat. Mějme nyní $c = a + bi$ a $0 \neq c' = a' + b'i$, pak jistě existuje $d \in \mathbb{C}$, $d = e + fi$, $(e,\ f \in \mathbb{R})$ takové, že $c = c'd$. Označme $d' = e' + f'i$, $(e',\ f' \in \mathbb{Z})$ takový prvek R, že platí: $|e - e'| \leq 1/2$ a $|f - f'| \leq 1/2$. Dále označme $g = c - c'd'$, což je také prvek R. Pak jistě $c = c'd' + g$ a také $\varphi(g) = \varphi(c - c'd') = \varphi(c'd - c'd') = \varphi(c') \cdot \varphi(d - d') \leq \varphi(c')$ neboť $\varphi(c') > 0$ a $\varphi(d - d') \leq 1/2$, čímž je důkaz hotov.

(4) Buď $\mathcal{R} = \{a + \sqrt{2} \cdot b \mid a, b \in \mathbb{Z}\} \subseteq \mathbb{R}$ a Euklidovskou normu na $\mathcal{R}$ definujeme následovně:

$$\begin{array}{rcl} \varphi\colon R & \to & \mathbb{Z} \\ a + \sqrt{2} \cdot b & \mapsto & a^2 + b^2 \end{array}$$

Lemma 1.59. *Nechť $\mathcal{R}$ je Euklidovský obor integrity s Euklidovskou normou φ. Pak platí:*

(i) $\forall\, r \in R \setminus \{0\}\colon \varphi(0) < \varphi(1) \leq \varphi(r)$

(ii) $\forall\, r, s \in R \setminus \{0\}\colon r \mid s \Rightarrow (r \parallel s \Leftrightarrow \varphi(r) = \varphi(s)$, *speciálně: r je invertibilní, právě když* $\varphi(r) = \varphi(1)$

(iii) *Pro každé $z \in \mathbb{Z}$ je následující zobrazení:*

$$\begin{array}{rcl} \varphi_z\colon R & \to & \mathbb{Z} \\ r & \mapsto & \varphi(r) - z \end{array}$$

Euklidovská norma na $\mathcal{R}$.

Důkaz. Pro každé nenulové $r \in R$ platí, že $1 \mid r$, což implikuje $\varphi(1) \leq \varphi(r)$. Uvažme prvky 0, $1 \in R$, pak podle definice 1.57 existují prvky c, $d \in R$ takové, že $0 = 1 \cdot c + d$ a $\varphi(d) < \varphi(1)$. Prvky c, d můžeme oba dva zvolit nulové, čímž dostáváme $\varphi(0) < \varphi(1)$, což dokazuje první tvrzení. Nechť nyní $r \mid s$, to implikuje existenci prvku $r' \in R$ takového, že $s = r \cdot r'$ a také vztah $\varphi(r) \leq \varphi(s)$. Pokud $r \parallel s$, pak $s \mid r$, z čehož plyne $\varphi(s) \leq \varphi(r)$ a to implikuje $\varphi(r) = \varphi(s)$. Pokud naopak $\varphi(r) = \varphi(s)$, existují prvky c, $d \in R$ takové, že $r = s \cdot c + d$ a $\varphi(d) < \varphi(s) = \varphi(r)$. Máme tedy $r = rr'c + d$, pokud by d bylo nenulové, platilo by $r(1 - r'c) = d$ a $\varphi(r) \leq \varphi(d)$, což je spor. Prvek d je tedy nulový, takže dostáváme $1 = r'c$, což implikuje $r' \parallel 1$, z čehož plyne $r \parallel s$, čímž je důkaz druhého tvzení hotov. Třetí tvrzení je snadné a proto ho přenecháme čtenáři jako cvičení. □

Lemma 1.60. *Nechť $\mathcal{R}$ je Euklidovský obor integrity s Euklidovskou normou φ. Pak $\mathcal{R}$ je obor integrity hlavních ideálů.*

Důkaz. Uvažme libovolný vlastní ideál $\mathcal{I}$. Jistě existuje prvek $r \in I$ takový, že $\varphi(r)$ je nejmenším prvkem množiny $\{\varphi(s) \mid 0 \neq s \in I\}$. Ukážeme, že $R \cdot r = \{r' \cdot r \mid r' \in R\} = I$. Inkluze $\subseteq$ je zřejmá. Pro důkaz opačné inkluze mějme libovolný nenulový prvek $s \in I$, z definice 1.57 víme, že existují prvky c, $d \in R$ takové, že $s = r \cdot c + d$ a $\varphi(d) < \varphi(r)$. Jelikož prvky s, $r \cdot c$ patří do $\mathcal{I}$, patří do $\mathcal{I}$ také prvek d, což implikuje $d = 0$ a tím je důkaz hotov. □

Poznámka 1.61. Buď $R = \{a/2 + b/2\sqrt{19} \cdot i \mid a, b \in \mathbb{Z}$, obě sudá nebo obě lichá$\}$. Tento obor integrity je oborem integrity hlavních ideálů, ale není Euklidovským oborem integrity.

Věta 1.62. *Nechť $\mathcal{R}$ je Euklidovský obor integrity s Euklidovskou normou φ. Předpokládejme, že existuje algoritmus, který pro každé a, $b \in R$, $b \neq 0$ dává c, $d \in R$ taková, že $a = b \cdot c + d$ a $\varphi(d) < \varphi(b)$. Pak existuje algoritmus, který pro každé a, $b \in R$ dává NSD(a, b).*

Důkaz. Popíšeme tzv. *Euklidův* algoritmus. Mějme libovolné $a, b \in R$, definujme posloupnost dvojic $(a_n, b_n) \in R^2$ následovně:

(0) $n = 0$, $a_0 = a$, $b_0 = b$
(1) Je-li definováno $(a_n, b_n) \in R^2$ a $a_n \neq 0$ i $b_n \neq 0$, pak:
   (a) Je-li $\varphi(a_n) < \varphi(b_n)$, pak z definice 1.57 plyne existence prvků c_n, $b_{n+1} \in R$ takových, že $b_n = a_n \cdot c_n + b_{n+1}$ a $\varphi(b_{n+1}) < \varphi(a_n)$ (čili $\varphi(b_{n+1}) < \varphi(b_n)$). Dále polož $a_{n+1} = a_n$, $n = n + 1$ a jdi na (1).
   (b) Je-li $\varphi(b_n) \leq \varphi(a_n)$, pak z definice 1.57 plyne existence prvků d_n, $a_{n+1} \in R$ takových, že $a_n = b_n \cdot d_n + a_{n+1}$ a $\varphi(a_{n+1}) < \varphi(b_n)$ (čili $\varphi(a_{n+1}) < \varphi(a_n)$). Dále polož $b_{n+1} = b_n$, $n = n + 1$ a jdi na (1).
(2) Je-li $a_n = 0$ nebo $b_n = 0$, pak KONEC.

Nyní dokážeme, že tento algoritmus skončí. Z kroku (1) plyne následující vztah $\varphi(a_0)+\varphi(b_0) > \varphi(a_1) + \varphi(b_1) > \cdots > \varphi(a_n) + \varphi(b_n) > \varphi(a_{n+1}) + \varphi(b_{n+1}) \geq 2 \cdot \varphi(0)$ a uvědomíme-li si, že obor hodnot zobrazení φ je množina celých čísel je důkaz konečnosti Euklidova algoritmu hotov. Nyní dokážeme, že když algoritmus skončí dvojicí $(0, b_n)$ ($(a_n, 0)$), pak $b_n = \mathrm{NSD}\,(a, b)$ ($a_n = \mathrm{NSD}\,(a, b)$). K tomu zbývá ukázat, že $\mathrm{NSD}\,(a_n, b_n) = \mathrm{NSD}\,(a_{n+1}, b_{n+1})$ a pro to zřejmě stačí dokázat následující ekvivalenci: $c = \mathrm{SD}\,(a_n, b_n) \Leftrightarrow c = \mathrm{SD}\,(a_{n+1}, b_{n+1})$, ale ta plyne přímo z definice dvojice (a_{n+1}, b_{n+1}). □

1.1. **Symetrické polynomy.**

Definice 1.63. Nechť $\mathcal{R}$ je okruh. Polynom $f \in \mathcal{R}[x_1, \ldots, x_n]$ je *homogenní*, pokud všechny monočleny f mají stejný stupeň.

Poznámka 1.64. Zřejmě součin homogenních polynomů je homogenní polynom. Součet dvou homogenních polynomů obecně nemusí být homogenní polynom.

Definice 1.65. Pro libivolnou permutaci $\pi \in S_n$ definujeme následující zobrazení:

$$\begin{array}{rcl} \pi\colon R[x_1, \ldots, x_n] & \to & R[x_1, \ldots, x_n] \\ 0 & \mapsto & 0 \\ 0 \neq f = \displaystyle\sum_{(k_1,\ldots,k_n)\in\mathbb{N}^n} a_{k_1,\ldots,k_n} x_1^{k_1} \cdots x_n^{k_n} & \mapsto & \pi(f) = \displaystyle\sum_{(k_1,\ldots,k_n)\in\mathbb{N}^n} a_{k_1,\ldots,k_n} x_{\pi(1)}^{k_1} \cdots x_{\pi(n)}^{k_n} \end{array}$$

Poznamenejme ještě, že platí následující rovnost:

$$\pi(f) = \sum_{(k_1,\ldots,k_n)\in\mathbb{N}^n} a_{k_1,\ldots,k_n} x_{\pi(1)}^{k_1} \cdots x_{\pi(n)}^{k_n} = \sum_{(k_1,\ldots,k_n)\in\mathbb{N}^n} a_{k_{\pi(1)},\ldots,k_{\pi(n)}} x_1^{k_{\pi(1)}} \cdots x_n^{k_{\pi(n)}}$$

Lemma 1.66. *Zobrazení π z definice 1.65 je okruhový homomorfismus.*

Důkaz. Zřejmě $\pi(0) = 0$ a $\pi(1) = 1$. Nechť $f = \sum_{(k_1,\ldots,k_n)\in\mathbb{N}^n} a_{k_1,\ldots,k_n} x_1^{k_1} \cdots x_n^{k_n}$ a $g = \sum_{(l_1,\ldots,l_n)\in\mathbb{N}^n} a_{l_1,\ldots,l_n} x_1^{l_1} \cdots x_n^{l_n}$ jsou dva polynomy z $\mathcal{R}[x_1, \ldots, x_n]$, pak:

$$\begin{array}{rcl} \pi(f + g) & = & \pi\Big(\displaystyle\sum_{(k_1,\ldots,k_n)\in\mathbb{N}^n} (a_{k_1,\ldots,k_n} + b_{k_1,\ldots,k_n}) x_1^{k_1} \cdots x_n^{k_n}\Big) = \\ & = & \displaystyle\sum_{(k_1,\ldots,k_n)\in\mathbb{N}^n} (a_{k_1,\ldots,k_n} + b_{k_1,\ldots,k_n}) x_{\pi(1)}^{k_1} \cdots x_{\pi(n)}^{k_n} = \pi(f) + \pi(g) \end{array}$$

Podobně se dokáže, že $\pi(-f) = -\pi(f)$. Protože platí následující rovnosti:

$$\begin{aligned} f \cdot g &= \sum_{(k_1,\ldots,k_n)\in\mathbb{N}^n} \Big(\sum_{\substack{(k_1,\ldots,k_n)= \\ (l_1,\ldots,l_n)+(m_1,\ldots,m_n)}} (a_{l_1,\ldots,l_n} + b_{m_1,\ldots,m_n}) \Big) x_1^{k_1} \cdots x_n^{k_n} \\ \pi(f) &= \sum_{(l_1,\ldots,l_n)\in\mathbb{N}^n} a_{l_1,\ldots,l_n} x_{\pi(1)}^{l_1} \cdots x_{\pi(n)}^{l_n} \\ \pi(g) &= \sum_{(m_1,\ldots,m_n)\in\mathbb{N}^n} a_{m_1,\ldots,m_n} x_{\pi(1)}^{m_1} \cdots x_{\pi(n)}^{m_n} \end{aligned}$$

Dostáváme jednoduchou úpravou i následující vztah:

$$\pi(f \cdot g) = \sum_{(k_1,\ldots,k_n)\in\mathbb{N}^n} \Big(\sum_{\substack{(k_1,\ldots,k_n)= \\ (l_1,\ldots,l_n)+(m_1,\ldots,m_n)}} (a_{l_1,\ldots,l_n} + b_{m_1,\ldots,m_n}) \Big) x_{\pi(1)}^{k_1} \cdots x_{\pi(n)}^{k_n} = \pi(f) \cdot \pi(g)$$

Čímž je důkaz hotov. □

Definice 1.67. Nechť $\mathcal{R}$ je obor integrity a nechť $1 \leq n < \omega$. Polynom $f \in R[x_1, \ldots, x_n]$ se nazývá *symetrický*, pokud $\pi(f) = f$ pro každé $\pi \in S_n$.

Příklad 1.68. Uveďme pár příkladů symetrických polynomů. Budeme se držet značení z definice 1.67.

(1) Pokud $n = 1$, pak každý polynom je symetrický.
(2) Pokud $1 < n < \omega$, označme pro každé $1 \leq i \leq n$:

$$\delta_{in} = \sum_{1\leq j_1<j_2\cdots<j_i\leq n} x_{j_1} \cdots x_{j_i}$$

Polynom δ_{in} se nazývá *i-tý elementární symetrický* polynom. Pro lepší představu uveďme pár i-tých elementárních symetrických polynomů v explicitním tvaru:

$$\begin{aligned} \delta_{1n} &= x_1 + x_2 + \cdots + x_n \\ \delta_{2n} &= x_1x_2 + x_1x_3 + \cdots x_1x_n + x_2x_3 + \cdots x_2x_n + \cdots x_{n-1}x_n \\ \delta_{nn} &= x_1 \cdots x_n \end{aligned}$$

Pro libovolné $1 < n < \omega$ a libovolné $1 \leq i \leq n$ platí:
(a) $\deg(\delta_{in}) = i$
(b) $\operatorname{lm}(\delta_{in}) = x_1 \cdots x_i$
(c) $\operatorname{lc}(\delta_{in}) = 1$
(d) $\operatorname{ht}(\delta_{in}) = (\underbrace{1,\ldots,1}_{i\times},\underbrace{0,\ldots,0}_{(n-i)\times})$
(e) δ_{in} je homogenní polynom

Lemma 1.69. *Nechť $\mathcal{R}$ je okruh a nechť $(\varphi_i \mid i \in I)$ je systém okruhových homomorfismů $\mathcal{R}$ do sebe. Označme $S = \{r \in R \mid \forall\, i \in I\colon \varphi_i(r) = r\}$ (to je právě množina všech pevných bodů systému $(\varphi_i \mid i \in I)$). Pak S je nosičem podokruhu v $\mathcal{R}$.*

Důkaz. Zřejmě pro každé $i \in I$ platí, že $\varphi_i(0) = 0$ a $\varphi_i(1) = 1$. Mějme dále libovolné s_1, $s_2 \in S$, pak pro každé $i \in I$ platí:

$$\begin{aligned} \varphi_i(-s_1) &= -\varphi_i(s_1) = -s_1 \\ \varphi_i(s_1 + s_2) &= \varphi_i(s_1) + \varphi_i(s_2) = s_1 + s_2 \\ \varphi_i(s_1 \cdot s_2) &= \varphi_i(s_1) \cdot \varphi_i(s_2) = s_1 \cdot s_2 \end{aligned}$$

□

Důsledek 1.70. *Množina všech symetrických polynomů v $R[x_1, \ldots, x_n]$ spolu s restrikcemi operací z $\mathcal{R}[x_1, \ldots, x_n]$ je podokruh v $\mathcal{R}[x_1, \ldots, x_n]$. Tento podokruh značíme $\mathcal{S}_R[x_1, \ldots, x_n]$.*

Důkaz. V lemmatu 1.69 stačí položit jako okruh $\mathcal{R}[x_1, \ldots, x_n]$ a jako systém $(\pi \mid \pi \in S_n)$. Pak množina všech pevných bodů tohoto systému má tvar $\{f \in R[x_1, \ldots, x_n] \mid \forall \pi \in S_n : \pi(f) = f\} = S_R[x_1, \ldots, x_n]$. □

Lemma 1.71. *Nechť $\mathcal{R} \leq \mathcal{S}$ jsou dva obory integrity, $s_1, \ldots, s_n \in S$ a nechť*

$$\varphi \colon R \quad \to \quad S$$

je okruhový homomorfismus. Pak existuje právě jeden okruhový homomorfismus

$$\psi \colon R[x_1, \ldots, x_n] \quad \to \quad S$$

takový, že $\psi_{\restriction R} = \varphi$ a zároveň pro každé $i = 1, \ldots, n$ platí, že $\psi(x_i) = s_i$.

Důkaz. Nejříve dokážeme existenci okruhového homomorfismu ψ. Definujme $\psi(0) = 0$ a pro $0 \neq f = \sum_{(k_1,\ldots,k_n)\in\mathbb{N}^n} a_{k_1,\ldots,k_n} x_1^{k_1} \cdots x_n^{k_n}$ definujme:

$$\psi(f) = \sum_{(k_1,\ldots,k_n)\in\mathbb{N}^n} \psi(a_{k_1,\ldots,k_n}) s_1^{k_1} \cdots s_n^{k_n} \in S$$

Zřejmě $\psi_{\restriction R} = \varphi$ a zároveň pro každé $i = 1, \ldots, n$ platí, že $\psi(x_i) = s_i$. Dokážeme, že ψ je okruhový homomorfismus. Pro libovolné $0 \neq g = \sum_{(k_1,\ldots,k_n)\in\mathbb{N}^n} b_{k_1,\ldots,k_n} x_1^{k_1} \cdots x_n^{k_n}$ platí:

$$\begin{aligned} \psi(f+g) &= \psi\Big(\sum_{(k_1,\ldots,k_n)\in\mathbb{N}^n} (a_{k_1,\ldots,k_n} + b_{k_1,\ldots,k_n}) x_1^{k_1} \cdots x_n^{k_n}\Big) = \\ &= \sum_{(k_1,\ldots,k_n)\in\mathbb{N}^n} \psi(a_{k_1,\ldots,k_n} + b_{k_1,\ldots,k_n}) s_1^{k_1} \cdots s_n^{k_n} = \psi(f) + \psi(g) \end{aligned}$$

neboť $\psi(a_{k_1,\ldots,k_n} + b_{k_1,\ldots,k_n}) = \psi(k_1, \ldots, k_n) + \psi(b_1, \ldots, b_n)$. Podobně se dokže, že $\psi(-f) = -\psi(f)$ a $\psi(f \cdot g) = \psi(f) \cdot \psi(g)$. Nyní dokážeme jednznačnost ψ. Mějme okruhový homomorfismus $\psi' \colon R[x_1, \ldots, x_n] \to S$ takový, že $\psi'_{\restriction R} = \varphi$ a zároveň nechť pro každé $i = 1, \ldots, n$ platí, že $\psi'(x_i) = s_i$. Pak zřejmě pro libovolné $f = \sum_{(k_1,\ldots,k_n)\in\mathbb{N}^n} a_{k_1,\ldots,k_n} x_1^{k_1} \cdots x_n^{k_n}$ platí:

$$\begin{aligned} \psi'(f) &= \sum_{(k_1,\ldots,k_n)\in\mathbb{N}^n} \underbrace{\psi'(a_{k_1,\ldots,k_n})}_{\varphi(a_{k_1,\ldots,k_n})} \cdot \underbrace{\psi'(x_1^{k_1} \cdots x_n^{k_n})}_{\psi'(x_1)^{k_1} \cdots \psi'(x_n)^{k_n}} = \\ &= \sum_{(k_1,\ldots,k_n)\in\mathbb{N}^n} \varphi(a_{k_1,\ldots,k_n}) s_1^{k_1} \cdots s_n^{k_n} = \psi(f) \end{aligned}$$

□

Příklad 1.72. Uveďme pár konkrétních příkladů na předchozí lemma. Budeme se držet značení z lemmatu 1.71, až na jednu vyjímku, zobrazení ψ (tzv. *dosazovací homomorfismus*) budeme značit jako $\varphi_{s_1,\dots,s_n}$ abychom zdůraznili jeho závislost na zobrazení φ a n-tici $s_1,\dots,s_n$.

(1) Nechť $\mathcal{R} \leq \mathcal{S}$ jsou dva obory integrity, $s \in S$ a $\varphi = \mathrm{id}: R \hookrightarrow S$. Pak z lemmatu 1.71 plyne existence následujícího zobrazení:

$$\begin{aligned} \mathrm{id}_s: R[x] &\to S \\ f &\mapsto f(s) \end{aligned}$$

(2) Nechť $\mathcal{R}$ je obor integrity, $S = R[x] \geq R$, $p \in R[x]$ a $\varphi = \mathrm{id} : R \hookrightarrow R[x]$. Pak z lemmatu 1.71 plyne existence následujícího zobrazení:

$$\begin{aligned} \mathrm{id}_p: R[x] &\to R[x] \\ f &\mapsto f(p) \end{aligned}$$

Zřejmě pokud $\deg(f) = m$ a $\deg(p) = n$, pak $\deg(f(p)) = m \cdot n$.

Lemma 1.73. *Nechť $\mathcal{R}$ je obor integrity a nechť $u = a \cdot x_1^{k_1} \cdots x_n^{k_n}$, $v = b \cdot x_1^{l_1} \cdots x_n^{l_n}$, kde a, b jsou libovolné nenulové prvky z $\mathcal{R}$. Pak platí:*

(i) *Nechť $f = a \cdot \delta_{1n}^{k_1} \cdots \delta_{nn}^{k_n}$. Pak $ht(f) = (\sum_{i=1}^n k_i, \sum_{i=2}^n k_i, \dots, k_{n-1} + k_n, k_n)$*

(ii) *Nechť $g = b \cdot \delta_{in}^{l_1} \cdots \delta_{nn}^{l_n}$. Pak $ht(g) = ht(f)$ právě když $ht(u) = ht(v)$.*

Důkaz. Podle poznámky 1.68 platí:

$$\mathrm{ht}(\delta_{in}) = (\underbrace{1,\dots,1}_{i\times},0,\dots,0)$$

z čehož plyne:

$$\mathrm{ht}(\delta_{in}^{k_i}) = k_i \cdot \mathrm{ht}(\delta_{in}) = (\underbrace{k_i,\dots,k_i}_{i\times},0,\dots,0)$$

Nyní využijeme lemma 1.23 a dostáváme:

$$\begin{aligned} \mathrm{ht}(\delta_{in}^{k_1}) &= (k_1,0,0,\dots,0) \\ \mathrm{ht}(\delta_{2n}^{k_2}) &= (k_2,k_2,0,\dots,0) \\ &\vdots \\ \mathrm{ht}(\delta_{nn}^{k_n}) &= (k_n,k_n,k_n,\dots,k_n) \\ \mathrm{ht}(f) &= (\sum_{i=1}^n k_i, \sum_{i=2}^n k_i, \dots, k_{n-1}+k_n, k_n) \end{aligned}$$

Dále zřejmě pltí, že $\mathrm{ht}(g) = \mathrm{ht}(g)$, právě když:

$$(\sum_{i=1}^n l_i, \sum_{i=2}^n l_i, \dots, l_{n-1}+l_n, l_n) = (\sum_{i=1}^n k_i, \sum_{i=2}^n k_i, \dots, k_{n-1}+k_n, k_n)$$

což platí, právě když $\mathrm{ht}(v) = (l_1,\dots,l_n) = (k_1,\dots,k_n) = \mathrm{ht}(u)$ (Poslední implikace z leva do prava se snadno dokáže zpětnou indukcí. Nejdříve si uvědomíme, že z členů nejvíce vpravo obou n-tic plyne, že $l_n = k_n$, dále postupujeme směrem vlevo, až dostaneme požadované tvrzení). □

Definice 1.74. Nechť $\mathcal{R} \leq \mathcal{S}$ jsou dva obory integrity, $s_1, \ldots, s_n \in S$. Prvky $s_1, \ldots, s_n$ nazveme *algebraicky nezávislé* nad $\mathcal{R}$, pokud $f(s_1, \ldots, s_n) \neq 0$ pro každý nenulový polynom $f \in R[x_1, \ldots, x_n]$. V opačném případě nazveme prvky $s_1, \ldots, s_n$ *algebraicky závislé* nad $\mathcal{R}$.

Lemma 1.75. *Nechť $\mathcal{R}$ je obor integrity, dále buď $\mathcal{S} = \mathcal{R}[x_1, \ldots, x_n]$ a nechť $\delta_{1n}, \ldots, \delta_{nn} \in S$ jsou elementární symetrické polynomy. Pak $\delta_{1n}, \ldots, \delta_{nn}$ jsou algebraicky nezávislé nad $\mathcal{R}$.*

Důkaz. Volbou $\mathcal{R}$, $\mathcal{S} = \mathcal{R}[x_1, \ldots, x_n]$, $s_1 = \delta_{1n}, \ldots, s_n = \delta_{nn} \in S = R[x_1, \ldots, x_n]$ a $\varphi = \mathrm{id}_R$ dostáváme z lemmatu 1.71 zobrazení $\psi \colon S \to S$ takové, že $\psi_{\restriction R} = \mathrm{id}_R$ a zároveň pro každé $i = 1, \ldots, n$ platí, že $\psi(x_i) = \delta_{in}$. Buď f libovolný nenulový polynom z $\mathcal{R}[x_1, \ldots, x_n]$, $f = \sum_{(k_1,\ldots,k_n)\in\mathbb{N}^n} a_{k_1,\ldots,k_n} x_1^{k_1} \cdots x_n^{k_n}$, pak $f = g_1 + \cdots + g_m$, kde g_j jsou monočleny f. Každé g_j, $j = 1, \ldots, m$ je tvaru $g_j = a_j \cdot x_1^{l_{1j}} \cdots x_n^{l_{nj}}$, kde a_j je nenulový prvek z $\mathcal{R}$. Dostáváme:

$$f(\delta_{1n}, \ldots, \delta_{nn}) \quad = \quad \psi(f) = \psi(g_1) + \cdots + \psi(g_m)$$

Pro každé $j = 1, \ldots, m$ označíme polynom $\psi(g_j) = g_j(\delta_{1n}, \ldots, \delta_{nn})$ jako h_j. Z lemmatu 1.73 plyne, že pro každé $j = 1, \ldots, m$ platí:

$$\mathrm{ht}\,(h_j) \quad = \quad (\sum_{i=1}^{n} l_{ij}, \sum_{i=2}^{n} l_{ij}, \ldots, l_{n-1,j} + l_{nj}, l_{nj})$$

Jistě existuje $j \in \{1, \ldots, m\}$ takové, že pro každé $j' \neq j$, $j' \in \{1, \ldots, m\}$ platí:

$$\mathrm{ht}\,(h_j) >_{LEX} \mathrm{ht}\,(h_{j'})$$

Zřejmě tedy platí, že $\mathrm{ht}\,(h_j) = \mathrm{ht}\,(f(\delta_{1n}, \ldots, \delta_{nn}))$, což implikuje $f(\delta_{1n}, \ldots, \delta_{nn}) \neq 0$. □

Lemma 1.76. *Nechť $\mathcal{R}$ je obor integrity a nechť f je libovolný nenulový polynom z okruhu symetrických polynomů $\mathcal{S}_R[x_1, \ldots, x_n]$ takový, že $ht(f) = (k_1, \ldots, k_n)$. Pak $k_1 \geq k_2 \geq \cdots \geq k_n$.*

Důkaz. Nechť f má následující tvar:

$$f = \sum_{(l_1,\ldots,l_n)\in\mathbb{N}^n} a_{l_1,\ldots,l_n} x_1^{l_1} \cdots x_n^{l_n}$$

Pro spor předpokládejme, že existuje $i \in \{1, \ldots, n\}$ takové, že $k_i < k_{i+1}$. Uvažme $\pi \in S_n$ transpozici prvků na pozicích i a $i + 1$. Zřejmě $\pi(f) = f$ a platí následující vztahy:

$$\begin{aligned} \mathrm{lm}\,(f) &= a_{k_1,\ldots,k_n} x_1^{k_1} \cdots x_i^{k_i} \cdot x_{i+1}^{k_{i+1}} \cdots x_n^{k_n} \\ \pi(\mathrm{lm}\,(f)) &= a_{k_1,\ldots,k_n} x_1^{k_1} \cdots x_{i+1}^{k_{i+1}} \cdot x_i^{k_i} \cdots x_n^{k_n} \\ \mathrm{ht}\,(\pi(\mathrm{lm}\,(f))) &= (k_1, \ldots, k_{i-1}, k_{i+1}, k_i, k_{i+2}, \ldots, k_n) >_{LEX} \mathrm{ht}\,(f) \end{aligned}$$

Poslední vztah je ovšem spor s tím, že $(k_1, \ldots, k_n)$ je výškou polynomu f. □

Věta 1.77 (O symetrických polynomech)**.** *Nechť $\mathcal{R}$ je obor integrity a nechť f je libovolný polynom z okruhu symetrických polynomů $\mathcal{S}_R[x_1, \ldots, x_n]$. Pak existuje jednoznačně určený polynom $f' \in R[x_1, \ldots, x_n]$ takový, že $f = f'(\delta_{1n}, \ldots, \delta_{nn})$.*

Důkaz. Nejdříve dokážeme existenci polynomu $f' \in R[x_1, \ldots, x_n]$. Pokud $f = 0$, stačí jako f' vzít nulový polynom. Nechť tedy $f \neq 0$. Tvrzení dokážeme indukcí podle výšky polynomu f (z lemmatu 1.76 plyne, že tato indukce je na množině všech symetrických polynomů skutečně možná). Pokud $\mathrm{ht}\,(f) = (0, 0, \ldots, 0)$, pak $f = a \cdot x_1^0 \cdots x_n^0$, kde $0 \neq a \in R$ a stačí zvolit $f' = a \in R[x_1, \ldots, x_n]$. Nechť tvrzení platí pro všechny symetrické polynomy

jejichž výška je ostře menší (v lexikografickém uspořádání) než $(k_1, \dots, k_n) = \mathrm{ht}\,(f)$, dále označme $a = \mathrm{lc}\,(f) \neq 0$. Z lemmatu 1.76 plyne, že $k_1 \geq k_2 \geq \cdots \geq k_n$. Uvažme monočlen $u = a \cdot x_1^{k_1-k_2} x_2^{k_2-k_3} \cdots x_{n-1}^{k_{n-1}-k_n} \cdot x^{k_n}$, pokud do u dosadíme $\delta_{1n}, \dots, \delta_{nn}$, dostaneme polynom $g = a \cdot \delta_{1n}^{k_1-k_2} \delta_{2n}^{k_2-k3} \cdots \delta_{n-1,1}^{k_{n-1}-k_n} \cdot \delta_{nn}^{k_n} \in S_R[x_1, \dots, x_n]$. Podle lemmatu 1.73 platí:

$$\begin{aligned} \mathrm{ht}\,(g) &= (k_1, \dots, k_n) = \mathrm{ht}\,(f) \\ \mathrm{lc}\,(g) &= a = \mathrm{lc}\,(f) \end{aligned}$$

Položme $h = f - g \in S_R[x_1, \dots, x_n]$, zřejmě platí, že $\mathrm{ht}\,(h) < \mathrm{ht}\,(f)$. Podle indukčního předpokladu existuje $h' \in R[x_1, \dots, x_n]$ takový, že $h = h'(\delta_{1n}, \dots, \delta_{nn})$. Položme $f' = u + h' \in R[x_1, \dots, x_n]$. Pak platí:

$$f'(\delta_{1n}, \dots, \delta_{nn}) = \psi(f) = \psi(u) + \psi(h') = \underbrace{u(\delta_{1n}, \dots, \delta_{nn})}_{g} + \underbrace{h'(\delta_{1n}, \dots, \delta_{nn})}_{h} = f$$

Nyní dokážeme jednoznačnost. Mějme f', $f'' \in R[x_1, \dots, x_n]$ takové, že platí:

$$\psi(f') = f'(\delta_{1n}, \dots, \delta_{nn}) = f = f''(\delta_{1n}, \dots, \delta_{nn}) = \psi(f'')$$

Máme tedy $\psi(f') = \psi(f'')$, což implikuje $\psi(f' - f'') = 0 = (f' - f'')(\delta_{1n}, \dots, \delta_{nn})$, z čehož podle lemmatu 1.75 plyne, že $f' = f''$. □

Příklad 1.78. Buď $f = x_1^2 x_2 + x_1 x_2^2 + x_1 x_2 \in S_{\mathbb{C}}[x_1, x_2]$, zřejmě $\mathrm{ht}\,(f) = (2, 1)$ a $\mathrm{lc}\,(f) = 1$. Budeme-li se držet značení z věty 1.77, máme $u = x_1 \cdot x_2$ a $g = \delta_{12} \cdot \delta_{22} = (x_1 + x_2)(x_1 x_2) = x_1^2 x_2 + x_1 x_2^2$, zřejmě $\mathrm{ht}\,(g) = (2, 1)$ a $\mathrm{lc}\,(g) = 1$. A jelikož $f - g = x_1 x_2 = \delta_{22}$, máme $h' = x_2$ a tedy $f' = x_1 x_2 + x_2 \in \mathbb{C}[x_1, x_2]$.

Příklad 1.79 (Aplikace teorie symetrických polynomů). Nechť $\mathcal{R} \leq \mathcal{S}$ jsou dva obory integrity, mějme polynom $f \in R[x_1, \dots, x_n]$, $f = \sum_{i=0}^{n} a_i x_i$ takový, že prvek a_n je invertibilní v $\mathcal{R}$ a pro $s_1, \dots, s_n \in S$ platí:

$$f = a_n(x - s_1) \dots (x - s_n)$$

Tedy polynom f se v $\mathcal{S}_R[x_1, \dots, x_n]$ rozkládá na součin lineárních činitelů. Dále mějme symetrický polynom $g \in S_R[x_1, \dots, x_n]$. Naším cílem bude spočítat hodnotu $g(s_1, \dots, s_n) \in S$ pouze na základě znalosti prvků $a_1, \dots, a_n$ a polynomu g. Z věty 1.77 plyne existence polynomu $g' \in R[x_1, \dots]$ takového, že platí:

$$g = g'(\delta_{1n}, \dots, \delta_{nn})$$

Dále využijeme dobře známých Vietových vztahů, které vypadají následovně:

$$\begin{aligned} a_{n-1} &= a_n(-1)(s_1 + \cdots + s_n) = a_n(-1)\delta_{1n}(s_1, \dots, s_n) \\ a_{n-2} &= a_n \delta_{2n}(s_1, \dots, s_n) \\ &\vdots \\ a_0 &= a_n(-1)^n \delta_{nn}(s_1, \dots, s_n) \end{aligned}$$

Nyní je již velmi snadné spočítat hodnotu $g(s_1, \dots, s_n)$, máme totiž:

$$g(s_1, \dots, s_n) = g'(\underbrace{\delta_{1n}(s_1, \dots, s_n)}_{-\frac{a_{n-1}}{a_n}}, \dots, \underbrace{\delta_{nn}(s_1, \dots, s_n)}_{(-1)^n \frac{a_0}{a_n}}) = g'(-\frac{a_{n-1}}{a_n}, \dots, (-1)^n \frac{a_0}{a_n}) \in S$$

Příklad 1.80. Budeme se držet značení z příkladu 1.79. Buď $R = S = \mathbb{C}$, $f = x^2+ax+b \in \mathbb{C}[x]$ a $g = x_1^2x_2 + x_1x_2^2 + x_1x_2 \in S_{\mathbb{C}}[x_1, x_2]$. Nechť s_1, $s_2 \in \mathbb{C}$ jsou kořeny rovnice $f(x) = 0$ v $\mathbb{C}$. Spočtěme hodnotu $g(s_1, s_2)$. Z příkladu 1.78 plyne, že $g = g'(\delta_{12}, \delta_{22})$, kde $g' = x_1x_2 + x_2$. Máme tedy:

$$g(s_1, s_2) \quad = \quad g'(-a, b) = -ab + b \in \mathbb{C}$$

1.2. **Formální derivace a násobnost kořenů polynomů.**

Definice 1.81. Nechť $\mathcal{R} \leq \mathcal{S}$ jsou dva obory integrity a nechť $f \in R[x]$. Pak řekneme, že:

(i) Prvek $s \in S$ je *kořenem* polynomu f v $\mathcal{S}$, pokud $f(s) = 0$ (tj. $\mathrm{id}_s(f) = 0$ dle příkladu 1.72).
(ii) Prvek $s \in S$ je *algebraický* nad $\mathcal{R}$, pokud existuje $g \in R[x]$, $\deg(g) \geq 1$ takový, že $g(s) = 0$. V opačném případě je prvek s *transcendetní* nad $\mathcal{R}$.
(iii) Obor integrity $\mathcal{S}$ je *algebraickým rošířením* $\mathcal{R}$, pokud každý prvek $s \in S$ je algebraický nad $\mathcal{R}$.

Příklad 1.82. Uveďme pár příkladů na pojmy z definice 1.81:

(1) Nechť $\mathcal{R}$ je obor integity. Prvek $0 \in R$ je kořenem polynomu $f \in R[x]$, právě když absolutní člen polynomu f je nulový.
(2) Nechť $\mathcal{R}$ je obor integity. Prvek $s \in R$ je algebraický nad $\mathcal{R}$ (neboť je kořenem polynomu $x - s \in R[x]$).
(3) Nechť $T \leq K$ dvě jsou komutativní tělesa taková, že $\dim_T K < \infty$. Pak těleso K je algebraickým rozšířením tělesa T (důkaz uvedeme později).
(4) Nechť $\mathcal{R}$ je obor integity, označme $S = R[x] \supseteq R$. Pak libovolný prvek $s \in R[x] \setminus R$ je transcendentní nad $\mathcal{R}$, protože pro libovolný polynom $g \in R[x]$, $\deg(g) \geq 1$ platí následující: $\deg(g(s)) = \deg(g) \cdot \deg(s) \geq 1$, z čehož plyne, že $g(s) \neq 0$.

Lemma 1.83. *Nechť $\mathcal{R} \leq \mathcal{S}$ jsou dva obory integrity a nechť $f \in R[x]$, $n = deg(f) \geq 1$. Pak f má nejvýše n kořenů.*

Důkaz. Důkaz provedeme matematickou indikcí a to dle $n = \deg(f)$. Buď $n = 1$, pak libovolný polynom f z tvrzení lemmatu má tvar $f = r \cdot x + r'$, kde $r, r' \in R[x]$. Tento polynom zřejmě má v $\mathcal{S}$ nejvýše 1 kořen. Nyní předpokládejme, že máme tvrzení dokázané pro všechny polynomy stupně menšího než n (a většího než 0), dokážeme, že tvrzení platí i pro polynomy stupně právě n. Pokud polynom f, $\deg(f) = n$ nemá v $\mathcal{S}$ kořen, jsme hotovi. Nechť je tedy prvek $s \in S$ kořenem polynomu f, vydělíme v $\mathcal{S}[x]$ se zbytkem tento polynom polynomem $(x - s)$. Dostáváme:

$$f \quad = \quad (x - s) \cdot g + h, \ \deg(h) \leq 0$$

Dále zřejmě platí následující (viz. 1.72):

$$\begin{aligned} 0 \quad &= \quad f(s) = \mathrm{id}_s(f) = \mathrm{id}_s((x - s) \cdot g + h) = \mathrm{id}_s(x - s) \cdot \mathrm{id}_s(g) + \mathrm{id}_s(h) = \\ &= \quad \underbrace{(s - s)}_{0} \cdot g(s) + h(s) \end{aligned}$$

Z čehož plyne, že $h = 0$, tj. $f = (x - s) \cdot g$ v $\mathcal{S}[x]$. Stupeň polynomu g je $n - 1$, takže z indukčního předpokladu plyne, že g má v $\mathcal{S}$ nejvýše $n - 1$ kořenů. Nyní dokážeme následující tvrzení, čímž bude důkaz hotov. Nechť $\{s_1, \ldots, s_i\}$, $i \leq n - 1$ jsou kořeny polynomu g v $\mathcal{S}$,

pak množina všech kořenů polynomu f v $\mathcal{S}$ je podmnožinou množiny $\{s_1, \ldots, s_i\} \cup \{s\}$. Buď $s' \in S$ kořen polynomu f, pak platí následující:

$$0 \quad = \quad f(s') = \mathrm{id}_{s'}(f) = \mathrm{id}_{s'}(x - s) \cdot \mathrm{id}_{s'}(g) = (s' - s) \cdot g(s')$$

Z čehož plyne, že $s' = s$ nebo $g(s') = 0$, čímž je tvrzení a zároveň i celé lemma dokázáno. □

Literatura

[1] Ladislav Procházka – Algebra (Academia), 1990
[2] Mac Lane-Birkhoff – Algebra (Alfa), 1973
[3] Hungerford – Algerbra (Springer), 2003
[4] Ladislav Bican– Algebra (pro učitelské studium) (Academia), 2001

Katedra algebry MFF UK, Sokolovská 83, 186 75 Praha 8
E-mail address: Jan.Trlifaj@mff.cuni.cz