1. Polynomy

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

$\boldsymbol{+}$

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

$\boldsymbol{-}$

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

$\mathbf{0}$

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

$\boldsymbol{\cdot}$

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

$\mathbf{1}$

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

Poznámka 1.2.
(1) Prvky množiny RG často zapisujeme formálně jako $f = \sum_{g \in G} r_g g$, kde $f(g) = r_g \in R$.
(2) V definici $\boldsymbol{\cdot}$ sčítáme přes všechny rozklady prvku g, tj. přes všechny uspořádané dvojice $[h, h']$ takové, že $g = h \odot h'$. Takových rozkladů může být nekonečně, nicméně z definice množiny RG je ihned vidět, že i tak se jedná o konečný součet prvků z R. (čili $\boldsymbol{\cdot}$ je dobře definovaná operace).
(3) Dokážeme nyní, že $\boldsymbol{\cdot}$ je asociativní binární operace na množině RG. Pro $x, y, z \in RG$, $g \in G$ máme $[(x \boldsymbol{\cdot} y) \boldsymbol{\cdot} z](g) = \sum_{g = h \odot h'} (x \boldsymbol{\cdot} y)(h) \cdot z(h') = \sum_{g = h \odot h'} (\sum_{h = h''' \odot h''} x(h''') \cdot y(h'')) \cdot z(h') = \sum_{g = h''' \odot h'' \odot h'} x(h''') \cdot y(h'') \cdot z(h')$.
Stejně tak $[x \boldsymbol{\cdot} (y \boldsymbol{\cdot} z)](g) = \sum_{g = h''' \odot h} x(h''') \cdot (y \boldsymbol{\cdot} z)(h) = \sum_{g = h''' \odot h} x(h''') \cdot (\sum_{h = h'' \odot h'} y(h'') \cdot z(h')) = \sum_{g = h''' \odot h'' \odot h'} x(h''') \cdot y(h'') \cdot z(h')$. Čili $\boldsymbol{\cdot}$ je asociativní binární operace. Nyní již není těžké ověřit, že $(RG, \boldsymbol{\cdot}, \mathbf{1})$ je monoid a že $(RG, \boldsymbol{+}, \boldsymbol{-}, \mathbf{0}, \boldsymbol{\cdot}, \mathbf{1})$ 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 monoidu $(RG, \boldsymbol{\cdot}, \mathbf{1})$ a $\mathcal{R}$ je podokruhem v okruhu $\mathcal{RG}$.*

Důkaz. Důkazem prvního tvrzení buď následující prostý monoidový homomorfismus

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

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

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

kde zobrazení f_r je definováno následovně

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

Ověřte si jako cvičení, že $\psi_{\mathcal{G}}$ i $\psi_{\mathcal{R}}$ jsou skutečně prosté homomorfismy. □

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.

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

$$\begin{aligned} \psi_{\mathcal{R}}\colon R &\hookrightarrow R[x] \\ r &\mapsto r \cdot x^0 \end{aligned}$$

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

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

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

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

Poznámka 1.7. Nechť $\mathcal{R}, \mathcal{R}_1, \mathcal{R}_2$ jsou okruhy, nechť $\mathcal{G}, \mathcal{G}_1, \mathcal{G}_2$ jsou monoidy, nechť $\varphi\colon R_1 \to R_2$ je okruhový homomorfismus a nechť $\varphi' : G_1 \to G_2$ je monoidový homomorfismus. Krásnou vlastností konstrukce monoidového okruhu je to, že se z φ resp. φ' dá snadno udělat okruhový homomorfismus $\bar{\varphi}\colon R_1G \to R_2G$, resp. $\bar{\varphi'}\colon RG_1 \to RG_2$. A to následovně:

$$\begin{aligned} \bar{\varphi}\colon R_1G &\to R_2G \\ \sum_{g\in G} r_g g &\mapsto \sum_{g\in G} \varphi(r_g) g \end{aligned}$$

a

$$\begin{aligned} \bar{\varphi'}\colon RG_1 &\to RG_2 \\ \sum_{g\in G} r_g g &\mapsto \sum_{g\in G} r_g \varphi'(g) \end{aligned}$$

Ověřte jako cvičení, že se skutečně v obou případech jedná o okruhový homomorfismus.

Pokud si za $\mathcal{G}_2$ zvolíme $\{e\}$ a za φ' zvolíme $\varphi_e : G_1 \to \{e\}, g \mapsto e$, dostaneme okruhový homorfismus z $\mathcal{R}\mathcal{G}_1$ do $\mathcal{R}$:

$$\begin{aligned} \bar{\varphi}_e\colon RG_1 &\to R\{e\} = R \\ \sum_{g\in G} r_g g &\mapsto \sum_{g\in G} r_g \end{aligned}$$

Jeho jádrem je přirozeně ideál a tento ideál má svůj název (protože se s ním často pracuje) a říká se mu *fundamentální ideál*.

Příklad 1.8 (Grupové okruhy). Pokud $\mathcal{G}$ je dokonce grupa a nechť $\mathcal{R}$ je okruh, pak okruh $\mathcal{R}\mathcal{G}$ nazýváme *grupovým okruhem grupy $\mathcal{G}$ nad okruhem $\mathcal{R}$.*

Věta 1.9. *Nechť $\mathcal{G}$ je grupa, K komutativní těleso a $1 \le n \in \mathbb{N}$. 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, jehož 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 1.10. 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 ještě jak vypadá odpovídající levý $K\mathcal{G}$-modul. Jako nosič si vezmeme množinu $M = K^n$, což je lineární aritmetický prostor dimenze n a násobení zleva prvky z $K\mathcal{G}$ je definováno následovně:

$$(\sum_{g\in G} k_g g)\cdot \begin{pmatrix}k_1\\ \vdots\\ k_n\end{pmatrix} = \sum_g k_g\cdot\psi(b\circ L_g\circ b^{-1})\times\begin{pmatrix}k_1\\ \vdots\\ k_n\end{pmatrix}.$$

Definice 1.11. Nechť $\mathcal{R}$ je okruh a nechť $\mathcal{R}[x_1,\dots,x_n]$ značí okruh polynomů n-neurčitých nad $\mathcal{R}$. Z příkladu 1.5 víme, že $f \in RG \Leftrightarrow f = \sum\limits_{(k_1,\dots,k_n)\in\mathbb{N}^n} r_{(k_1,\dots,k_n)} x_1^{k_1}\cdots x_n^{k_n}$. Definujeme *nosič* polynomu f jako $\operatorname{supp}(f) = \{(k_1,\dots,k_n) \mid r_{(k_1,\dots,k_n)} \neq 0\}$. Polynom f se dá tedy zapsat také jako $f = \sum\limits_{(k_1,\dots,k_n)\in\operatorname{supp}(f)} r_{(k_1,\dots,k_n)} x_1^{k_1}\cdots x_n^{k_n}$. Již by mělo být zřejmé, že nosič libovolného polynomu je konečná množina.

Definice 1.12. Na množině $\mathbb{N}^n$ definujeme *lexikografické uspořádání* $<_{LEX}$ klasickým způsobem: pro $(k_1,\dots,k_n) \neq (l_1,\dots,l_n)$ je $(k_1,\dots,k_n) <_{LEX} (l_1,\dots,l_n)$, právě když pro i nejmenší takové, že $k_i \neq l_i$ platí, že $k_i < l_i$. Definujeme též neostrou verzi tohoto uspořádání.

Definice 1.13. Buď $f = \sum\limits_{(k_1,\dots,k_n)\in\mathbb{N}^n} r_{(k_1,\dots,k_n)} x_1^{k_1}\cdots x_n^{k_n}$ nenulový polynom z $\mathcal{R}[x_1,\dots,x_n]$. Každému členu $r_{(k_1,\dots,k_n)} x_1^{k_1}\cdots x_n^{k_n}$ ve formálním zápise polynomu f se říká *monočlen*, pokud navíc $r_{(k_1,\dots,k_n)} = 1$, mluvíme o *monickém monočlenu*. Dále definujeme:

(i) *Stupeň* polynomu f jako $\deg(f) = \max\{\sum_{i=1}^n k_i \mid (k_1,\dots,k_n) \in \operatorname{supp}(f)\} in\mathbb{N}$. Stupeň nulového polynomu definujeme jako -1.
(ii) *Výšku* polynomu f jako $\operatorname{ht}(f) = \max_{LEX}\{(k_1,\dots,k_n) \mid (k_1,\dots,k_n) \in \operatorname{supp}(f)\} \in \mathbb{N}^n$.
(iii) *Vedoucí monočlen* polynomu f jako $\operatorname{lm}(f) = x_1^{k_1}\cdots x_n^{k_n}$, kde $(k_1,\dots,k_n) = \operatorname{ht}(f)$.
(iv) *Vedoucí koeficient* polynomu f jako $\operatorname{lc}(f) = r_{(k_1,\dots,k_n)}$, kde $(k_1,\dots,k_n) = \operatorname{ht}(f)$.

Příklad 1.14. Uvažme okruh $\mathbb{Q}[x_1,\dots,x_n]$ a polynom $f = 3x_1^2x_5 + 10x_2^{12}x_4 + x_3^7$. Pak platí $\deg(f) = 13$, $\operatorname{ht}(f) = (2,0,0,0,1)$, $\operatorname{lm}(f) = x_1^2x_5$ a $\operatorname{lc}(f) = 3$.

Příklad 1.15. Uvažme okruh $\mathcal{R}[x]$ a libovolný nenulový polynom $f = \sum_{n=0}^{k} a_n x^n$, $a_k \neq 0$ z tohoto okruhu. Pak platí $\deg(f) = k$, $\mathrm{ht}(f) = (k)$, $\mathrm{lm}(f) = x^k$, $\mathrm{lc}(f) = a_k$.

2. Mocninné řady

Definice 2.1. 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 2.2. 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.

Definice 2.3. Nechť $\mathcal{G} = (G, \odot, e)$ je finitární monoid a $\mathcal{R} = (R, +, -, 0, \cdot, 1)$ je okruh. Pak definujeme *okruh formálních mocninných řad* $\langle \mathcal{RG} \rangle = (R^G, \mathbf{+}, \mathbf{-}, \mathbf{0}, \boldsymbol{\cdot}, \mathbf{1})$, kde R^G je množina všech zobrazení z G do R a operace na R^G jsou definovány stejně jako v případě monoidového okruhu.

Poznámka 2.4. Zřejmě $\mathcal{RG}$ je podokruhem v $\langle \mathcal{RG} \rangle$.

Příklad 2.5.
1. V případě, kdy $\mathcal{G} = \mathbb{N}$ se $\langle \mathcal{RG} \rangle$ značí $\mathcal{R}\langle x \rangle$ a prvkům tohoto okruhu říkáme *formální mocninné řady* a často je zapisujeme ve tvaru $\sum_0^\infty r_n x^n$.
2. V případě, kdy $\mathcal{G} = \mathbb{N}^n$ se $\langle \mathcal{RG} \rangle$ značí $\mathcal{R}\langle x_1, \ldots, x_n \rangle$ a prvkům tohoto okruhu říkáme *formální mocninné řady neurčitých* $x_1, \ldots, x_n$ a často je zapisujeme ve tvaru $\sum_{(k_1,\ldots,k_n) \in \mathcal{N}^n} r_{(k_1,\ldots,k_n)} x_1^k$
3. Aby grupa $\mathcal{G}$ byla finitárním monoidem, musí být konečná. Pokud ale $\mathcal{G}$ je konečný monoid, pak $\langle \mathcal{RG} \rangle = \mathcal{RG}$. Čili v případě kdy $\mathcal{G}$ je grupa, nepřinese konstrukce okruhu formálních mocninných řad oproti grupovému okruhu nic nového.

3. Obory integrity

Lemma 3.1. *Pokud $\mathcal{R}$ je navíc obor integity, pak 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) $ht(f \cdot g) = ht(f) + ht(g)$
(iv) $deg(f \cdot g) = deg(f) \cdot deg(g)$.

Důkaz. Ověřte jako snadné cvičení. □

Lemma 3.2. *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 3.1. □

Lemma 3.3. *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 $q_1 = q_2$, takže $p_1 = p_2$, čímž je dokázána jednoznačnost polynomů p a q. $\square$

Definice 3.4. 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 3.5. Uveďme pár příkladů oborů integrity hlavních ideálů.

(1) Okruh $\mathcal{Z}$ je oborem integrity hlavních ideálů. Ideály v $\mathcal{Z}$ jsou právě všechny podmnožiny tvaru $n \cdot \mathbb{Z}$, $n \in \mathbb{N}$, tedy vždy generované jedním prvkem n.
(2) Každé komutativní těleso K je jistě oborem integrity hlavních ideálů, neboť K obsahuje právě dva ideály a to $0 = 0 \cdot K$ a $K = 1 \cdot K$.

Věta 3.6. *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 $\{n \in \mathbb{N} \mid \exists f \in I : f \neq 0 \wedge \deg(f) = n\}$ a f_0 příslušný polynom z $\mathcal{I}$. Dokážeme, že $I = Rf_0 = \{g \cdot f_0 \mid g \in R\}$. Zřejmě $Rf_0 \subseteq I$ neboť $\mathcal{I}$ je ideál. Naopak pro libovolný polynom $h \in I$ existují podle lemmatu 3.3 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. $\square$

Příklad 3.7. Následující příklad ukazuje, že důsledek 3.6 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 3.1 dostáváme náledující rovnost:

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

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

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

Z čehož plyne, že $f = x_2$ 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 (důkaz sporem: pokud by se vlastnost být OIHI přenášela z okruhu $\mathcal{R}$ na okruh $\mathcal{R}[x]$, měli bychom, že pokud je $\mathcal{R}$ OIHI, je jím i $\mathcal{R}[x]$ a protože $(\mathcal{R}[x_1])[x_2] \simeq \mathcal{R}[x_1, x_2]$, je OIHI i $\mathcal{R}[x_1, x_2]$, což je ale spor s naším příkladem).

4. Noetherovské okruhy

Definice 4.1. Okruh $\mathcal{R}$ je *noetherovský*, pokud v $\mathcal{R}$ neexistuje nekonečný ostře rostoucí řetězec ideálů (ostře rostoucím řetězcem se myslí posloupnost tvaru $I_1 \subsetneq I_2 \subsetneq I_3 \subsetneq \dots$).

Lemma 4.2. *Okruh $\mathcal{R}$ je noetherovský právě, když každý ideál v $\mathcal{R}$ je konečně generovaný.*

Důkaz. Předpokládejme, že $\mathcal{R}$ je noetherovský a pro spor předpokládejme dále, že v $\mathcal{R}$ existuje ideál I, který nemá konečnou podmnožinu generátorů. Jelikož I nemá konečnou podmnožinu generátorů, můžeme postupně vybírat prvky $r_1, r_2, \dots \in I$ tak, abychom dostali následující ostře rostoucí řetězec ideálů

$$0 \subsetneq Rr_1 \subsetneq Rr_2 \subsetneq \dots \subsetneq I \subseteq R.$$

Což je ale spor s tím, že $\mathcal{R}$ je noetherovský okruh.

Předpokládejme nyní, že každý ideál v $\mathcal{R}$ je konečně generovaný a pro spor předpokládejme dál, že $\mathcal{R}$ není noetherovský okruh, tedy, že v $\mathcal{R}$ existuje následující nekonečný ostře rostoucí řetězec ideálů

$$I_1 \subsetneq I_2 \subsetneq \dots \subsetneq I_n \subsetneq I_{n+1} \subsetneq \dots \subsetneq R.$$

Položme $I = \bigcup_{n<\infty} I_n$. Je snadné ověřit, že I je ideál (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). Nechť tedy $\{r_1, \dots, r_n\} \subseteq I$ je jeho konečná podmnožina generátorů. Jistě pro každé r_i existuje $j_{r_i} \in \mathbb{N}$ tak, že $r_i \in I_{j_{r_i}}$. Položme $j = \max_{i=1,\dots,k} j_{r_i}$. Pak ale $I \subseteq I_j$, čili $I = I_j$, což je spor s tím, že $I_{j+1} \supsetneq I_j$. □

Věta 4.3 (Hilbertova o bázi)**.** *Nechť $\mathcal{R}$ je noetherovský okruh. Pak okruh $\mathcal{R}[x_1, \dots, x_n]$ je také noetherovský.*

Důkaz. V první řadě si uvědomíme, že tvrzení stačí dokázat jen pro případ $n = 1$, zbytek totiž plyne z isomorfismu okruhů $\mathcal{R}[x_1, x_2] \simeq (\mathcal{R}[x_1])[x_2]$. Dále dle 4.2 stačí ukázat, že každý ideál okruhu $\mathcal{R}[x_1]$ je konečně generovaný. Označme $\mathcal{S} = \mathcal{R}[x_1]$.

Nechť I je ideál v $\mathcal{S}$. Pro každé $n \geq 0$ přirozené definujme množinu $J_n = \{r \in R \mid \exists 0 \neq f_r \in I \colon \mathrm{lc}\,(f_r) = r, \deg\,(f_r) = n\} \cup \{0\}$. Ukážeme, že J_n jsou ideály v $\mathcal{R}$ a že máme následující řetězec ideálů v $\mathcal{R}$

$$J_0 \subseteq J_1 \subseteq \dots \subseteq J_n \subseteq J_{n+1} \subseteq \dots \subseteq R.$$

- Jistě $0 \in J_n$. Pokud $r, r' \in J_n$, pak i $r + r' \in J_n$, neboť $\mathrm{lc}\,(f_r + f'_r) = r + r'$ (pokud $r + r' \neq 0$). Pokud $r \in J_n$, pak i $-r \in J_n$, neboť $\mathrm{lc}\,(-f_r) = -r$. Pokud $0 \neq s \in R$ a zároveň $0 \neq r \in J_n$, pak i $sr \in J_n$, neboť $\mathrm{lc}\,(sf_r) = sr$.
- Pokud $0 \neq r \in J_n$, pak $r \in J_{n+1}$, neboť $\deg\,(xf_r) = n + 1$ a $\mathrm{lc}\,(xf_r) = r$.

Podle předpokladu je $\mathcal{R}$ noetherovský okruh, tedy existuje $m \geq 0$ přirozené takové, že se řetězec u J_m zastaví, tedy takové m, že $J_{m+k} = J_m$ pro každé $k \geq 0$ přirozené. Dále všechny ideály J_n jsou konečně generované dle 4.2. Označme $\{r_{i,0}, \dots, r_{i,k_i}\}$ konečnou generující podmnožinu ideálu J_i. Ukážeme, že konečná množina F polynomů

$$\{f_{r_{0,0}}, \dots, f_{r_{0,k_0}}, f_{r_{1,0}}, \dots, f_{r_{1,k_1}}, \dots, f_{r_{m,0}}, \dots, f_{r_{m,k_m}}\} = F \subseteq I$$

generuje I

Zřejmě $\sum_{f\in F} Sf \subseteq I$, protože $\mathcal{I}$ je ideál. Pro opačnou inkluzi předpokládejme pro spor, že existuje nenulový polynom $g \in I \setminus \sum_{f\in F} Sf$. Vyberme takové g minimálního stupně a označme $n = \deg(g)$, $r = \mathrm{lc}(g)$. Rozlišme dva případy

$n \leq m$: Máme $r \in J_n$, proto $r = r_{n,0}r'_0 + \cdots + r_{n,k_n}r'_{k_n}$ pro nějaké $r'_0, \ldots r'_{k_n} \in R$. Tedy $\mathrm{lc}(g) = \mathrm{lc}(f_{r_{n,0}})r'_0 + \cdots + \mathrm{lc}(f_{r_{n,k_n}})r'_{k_n}$. Pak ale $g' = g - f_{r_{n,0}}r'_0 + \cdots + f_{r_{n,k_n}}r'_{k_n} \in I \setminus \sum_{f\in F} Sf$ a navíc $\deg(g') < \deg(g)$, což je spor s předpokladem, že g je minimálního stupně.

$n > m$: Máme $r \in J_n$, proto $r = r_{n,0}r'_0 + \cdots + r_{n,k_n}r'_{k_n}$ pro nějaké $r'_0, \ldots r'_{k_n} \in R$. Tedy $\mathrm{lc}(g) = \mathrm{lc}(f_{r_{n,0}})r'_0 + \cdots + \mathrm{lc}(f_{r_{n,k_n}})r'_{k_n}$. Pak ale $g' = g - x^{n-m}f_{r_{n,0}}r'_0 + \cdots + x^{n-m}f_{r_{n,k_n}}r'_{k_n} \in I \setminus \sum_{f\in F} Sf$ a navíc $\deg(g') < \deg(g)$, což je spor s předpokladem, že g je minimálního stupně.

Dokákzali jsme že v $\mathcal{R}[x_1]$ je každý ideál konečně generovaný, dle 4.2 je $\mathcal{R}[x_1]$ noetherovský okruh. $\square$

Nyní se opět budeme věnovat výhradně oborům integrity, tedy komutativním okruhům, ve kterých platí $ab = 0 \Rightarrow (a = 0 \vee b = 0)$

Lemma 4.4. *Nechť $\mathcal{R}$ je obor integrity hlavních ideálů, pak $\mathcal{R}$ je noetherovský obor integrity.*

Důkaz. Pro spor předpokládejme, že v $\mathcal{R}$ existuje nekonečný ostře rostoucí řetězec ideálů $I_1 \subsetneq I_2 \ldots I_n \subsetneq I_{n+1} \subsetneq \ldots$. Uvažme množinu $I = \bigcup_{n\in\mathbb{N}} I_n$. Je snadné ověřit, že I je ideál. Protože 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 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. $\square$

5. Gaussovy obory integrity a obory integrity jednoznačných rozkladů (UFD)

Definice 5.1. Nechť $\mathcal{R}$ je obor integrity, $a, b \in R$. Řekneme, že a *dělí* b (a je *dělitelem* b), pokud $\exists\, c \in R$ tak, že $b = ac$ (ekvivalentně $Rb \subseteq Ra$). Značení $a \mid b$. Pokud navíc $Rb \subsetneq Ra$, řekneme, že a je *vlastním dělitelem* b. Dále řekneme, že a je *asociováno s* b, pokud $a \mid b$ a zároveň $b \mid a$ (ekvivalentně $Ra = Rb$). Značení $a \parallel b$. Relace být asociován je relace ekvivalence na množině R.

Příklad 5.2. Nechť $\mathcal{R}$ je obor integrity, $r \in R$. Pak $r \parallel 1$ právě, když r je invertibilní. Důkaz můžeme provést například takto: $r \parallel 1$ právě tehdy, když $R \cdot r = R \cdot 1 = R$, což je právě tehdy, když existuje prvek $s \in R$ takový, že $s \cdot r = 1$, tedy právě tehdy, když r je invertibilní prvek $\mathcal{R}$.

Příklad 5.3. Nechť $\mathcal{R}$ je obor integrity, $r \in R$. Pak $r \parallel 0$ právě když $r = 0$.

Lemma 5.4. *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. $\square$

Definice 5.5. Nechť $\mathcal{R}$ je obor integrity, $r \in R$. Řekneme, že r je *ireducibilní* prvek, pokud $r \neq 0$, $r \nparallel 1$ a kdykoli $s \mid r$, pak buď $s \parallel r$ nebo $s \parallel 1$ (tj. r nemá vlastní dělitele).

Definice 5.6. Nechť $\mathcal{R}$ je obor integrity, $r \in R$. Řekneme, že r je *prvočinitel* , pokud $r \neq 0$, $r \nparallel 1$ a kdykoli $r \mid st$, pak $r \mid s$ nebo $r \mid t$ (tj. Rr je prvoideál v $\mathcal{R}$).

Poznámka 5.7. Nechť $\mathcal{R}$ je obor integrity, nechť $r \in R$ je prvočinitel a nechť $s_1, \ldots, s_n \in R$. Z definice prvočinitele se snadno indukcí dokáže následující implikace: $r \mid (s_1 \cdots s_k) \Rightarrow \exists\, k \in \{1, \ldots, n\} \colon r \mid s_k$.

Lemma 5.8. *Nechť $\mathcal{R}$ je obor integrity. Pak každý prvočinitel je ireducibilní.*

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 $s \parallel 1$. □

Příklad 5.9. Podmnožina $R_5 = \{a + b\sqrt{5} \mid a, b \in \mathbb{Z}\} \subseteq \mathbb{R}$ spolu s operacemi z $\mathbb{R}$ tvoří okruh. Lze ukázat, že prvek 2 je ireducibilní, ale nejedná se o prvočinitel, neboť $2 \mid 4 = (1+\sqrt{5})(-1+\sqrt{5})$, ale 2 nedělí $1 + \sqrt{5}$, ani $-1 + \sqrt{5}$.

Definice 5.10. 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 5.11. Zřejmě každý noetherovský obor integrity splňuje podmínku (K).

Definice 5.12. 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 t značíme $\mathrm{NSD}\,(r, s)$ a říkáme, že je to *největší společný dělitel* r a s.

Definice 5.13. Nechť $\mathcal{R}$ je obor integrity. $\mathcal{R}$ splňuje *podmínku (P)* (prvočíselnou podmínku), pokud každý ireducibilní prvek $\mathcal{R}$ je prvočinitelem.

Definice 5.14. Nechť $\mathcal{R}$ je obor integrity. $\mathcal{R}$ splňuje *podmínku (E)* (podmínku existence ireducibilních rozkladů), pokud pro každý nenulový prvek $a \in \mathcal{R}$, který není asociovaný s 1 platí, že a je součinem ireducibilních prvků (tj. $\exists\, n \in \mathbb{N}, \exists\, a_1, \ldots a_n \in R$, a_i ireducibilní pro každé i: $a = a_1 \cdots a_n$).

Definice 5.15. Nechť $\mathcal{R}$ je obor integrity. $\mathcal{R}$ splňuje *podmínku (J)* (podmínku jednoznačnosti ireducibilních rozkladů), pokud platí následující implikace. Nechť $\{a_1, \ldots, a_m\}$, $\{b_1, \ldots, b_n\}$ jsou dvě neprázdné množiny ireducibilních 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 $i = 1, \ldots, m$.

Definice 5.16. Nechť $\mathcal{R}$ je obor integrity. Pak

(i) $\mathcal{R}$ je *Gaussův*, pokud $\mathcal{R}$ splňuje podmínky (K) a (D),
(ii) $\mathcal{R}$ je *UFD* (*obor integrity jednoznačných rozkladů*), pokud každé nenulové $r \in R$, pro které platí $r \nparallel 1$, lze vyjádřit jako součin prvočinitelů.

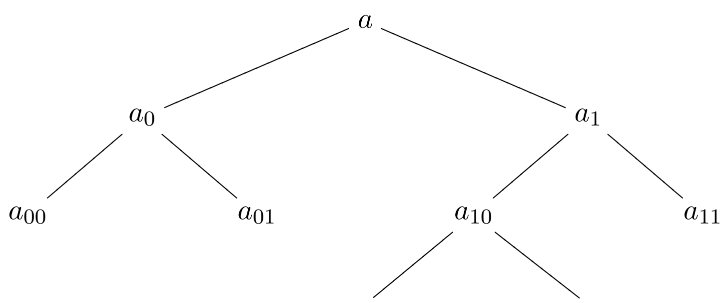
Poznámka 5.17. Nechť $\mathcal{R}$ je UFD. Ukážeme, že z existence plyne jednoznačnost. Vezměme nenulové $r \in R$, pro které platí $r \not\parallel 1$. Máme $r = p_1 \cdot p_2 \cdots p_m$ a předpokládejme dále, že $r = q_1 \cdot q_2 \cdots q_n$. Jistě $p_1 \mid q_1 \cdot q_2 \cdots q_n$, takže existuje index i, že $p_1 \mid q_i$ (BÚNO $i = 1$, jinak můžeme prvočinitele q_i přečíslovat). Z definice prvočinitele máme, že nutně $p_1 \parallel q_1$. Takto můžeme postupovat indukcí dále, až dostaneme, že $m = n$ a $\exists\, \pi \in S_n : p_i \parallel q_{\pi(i)}$ pro každé $i = 1, \ldots, n$.

Poznámka 5.18. Nyní dokážeme, že mezi právě definovanými podmínkami platí následující vztahy:

$$
\begin{array}{ccc}
((\mathrm{K})) & \wedge & (\mathrm{D})) \\
\Downarrow & \Updownarrow & \Downarrow \\
((\mathrm{E}) & \wedge & (\mathrm{P})) \\
 & & \Downarrow \\
 & & (\mathrm{J})
\end{array}
$$

Lemma 5.19. *Nechť $\mathcal{R}$ je obor integrity. Pak platí: (K) $\Rightarrow$ (E).*

Důkaz. Pro spor předpokládejme, že máme nenulové $a \in R$, které není asociováno s 1 takové, že a není součinem ireducibilních 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 Konigovy 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). $\square$

Důsledek 5.20. *Okruh $\mathcal{R} = K[x_1, \ldots, x_n]$ splňuje podmínku (E).*

Lemma 5.21. *Nechť $\mathcal{R}$ je obor integrity splňující podmínku (D) a nechť $a, b \in R$, $0 \neq d \in R$. 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 $f \parallel 1$. $\square$

Lemma 5.22. *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 ireducibilní, 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 ireducibilního 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 5.21 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 $r \mid s_2$. $\square$

Lemma 5.23. *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 ireducibilních 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 ireducibilitou 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 5.7 $j \in \{1, \ldots, n\}$ (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: $\pi(m) = j$. $\square$

Lemma 5.24. *Nechť $\mathcal{R}$ je obor integrity. Pak platí: ((E) $\wedge$ (J)) $\Rightarrow$ (K).*

Důkaz. Pro spor předpokládejme, že existuje 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 ireducibilní 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 ireducibilní rozklad. Každý z těchto rozkladů obsahuje alespoň jeden ireducibilní prvek, čímž jsme dostali ireducibilní rozklad prvku a_1, který má alespoň $n + 1$ členů, což je spor s podmínkou (J). $\square$

Lemma 5.25. *Nechť $\mathcal{R}$ je obor integrity. Pak platí: ((E) $\wedge$ (J)) $\Rightarrow$ (D).*

Důkaz. Mějme dva prvky a, $b \in R$, 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 předpokladů plyne existence následujících rozkladů:

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

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

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

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 $dy = b$. Z předpokladů máme 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 $\pi\colon \{1, \ldots, t\} \to \{1, \ldots, m\}$ takové, že platí $s_i \parallel p_{\pi(i)}$, $i = 1, \ldots, t$ a zároveň dostáváme, že $h_i \leq k_i$, $i = 1, \ldots t$. Ze vztahu $dy = b$ a podmínky (J) plyne, že $t \leq n$ a že existuje zobrazení $\sigma\colon \{1, \ldots, t\} \to \{1, \ldots, n\}$ takové, že platí $s_i \parallel q_{\sigma(i)}$, $i = 1, \ldots, t$ a zároveň dostáváme, že $h_i \leq l_i$, $i = 1, \ldots t$. Z předchozích vzathů 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 $h_i \leq \min(k_i, l_i) = r_i$, $i = 1, \ldots, t$, máme $d \mid c$, čímž je důkaz hotov. □

Věta 5.26. *Nechť $\mathcal{R}$ je obor integrity. Pak následující je ekvivalentní*

1. *$\mathcal{R}$ je Gaussův,*
2. *$\mathcal{R}$ je UFD,*
3. *$\mathcal{R}$ splňuje podmínky (K) a (D),*
4. *$\mathcal{R}$ splňuje podmínky (E) a (J),*
5. *$\mathcal{R}$ splňuje podmínky (E) a (P).*

(všchny tyto podmínky splňuje obor integrity $\mathcal{R} = K[x]$, kde K je komutativní těleso)

Důkaz. (1) ⇔ (3): je přímo definice. (1) ⇒ (4): plyne z 5.19, 5.22, 5.23. (4) ⇒ (1): plyne z 5.24, 5.25. (4) ⇒ (5): plyne z 5.25, 5.22. (5) ⇒ (4): plyne z 5.23. (2) ⇒ (5): lehké cvičení. □

Lemma 5.27. *Nechť $\mathcal{R}$ je obor integrity hlavních ideálů. Pak $\mathcal{R}$ je UFD.*

Důkaz. V první řadě, $\mathcal{R}$ je noetherovský okruh podle 4.4, čili 5.11 implikuje podmínku (K). Zbývá dokázat, že $\mathcal{R}$ splňuje podmínku (D). Vezměme libovolná $a, b \in R$. Víme, že ideál $Ra + Rb$ je hlavní, takže $Ra + Rb = Rc$ pro nějaké $c \in R$. Je snadné cvičení ukázat, že $c = \mathrm{NSD}(a, b)$. □

6. Euklidovské obory integrity

Definice 6.1. 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 6.2. Uveďme pár příkladů Euklidovských oborů integrity.

(1) Buď $R = \mathbb{Z}$ 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 6.1 nemusí být určeny jednoznačně (např. $5 = 3 \cdot 2 - 1$ a $5 = 2 \cdot 2 + 1$).

(2) Buď $R = K[x]$, 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 6.1. 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 $R = \{a + \sqrt{2} \cdot b \mid a, b \in \mathbb{Z}\} \subseteq \mathbb{R}$ a Euklidovskou normu na $\mathcal{R}$ definujeme následovně:

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

Lemma 6.3. *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) $\forall\, r, s \in R \setminus \{0\}\colon r \parallel s \Leftrightarrow \varphi(r) = \varphi(s)$, *speciálně: r je invertibilní právě, když $\varphi(r) = \varphi(1)$*

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

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

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 6.1 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, címž dostáváme $\varphi(0) < \varphi(1)$, což dokazuje první tvrzení. Nechť nyní $r \parallel s$, to implikuje existenci prvku $r' \in R$ takového, že $s = r \cdot r'$ a také vztah $\varphi(r) \leq \varphi(s)$, ale podobně také vztah $\varphi(s) \leq \varphi(r)$, což 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 6.4. *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 6.1 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 6.5. 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 6.6. *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 6.1 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 6.1 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 $b_n = \text{NSD}\,(a, b)$ $(a_n = \text{NSD}\,(a, b))$. K tomu zbývá ukázat, že $\text{NSD}\,(a_n, b_n) = \text{NSD}\,(a_{n+1}, b_{n+1})$ 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}). $\square$

7. Symetrické polynomy

Definice 7.1. Nechť $\mathcal{R}$ je okruh. Polynom $f \in \mathcal{R}[x_1, \ldots, x_n]$ je *homogenní*, pokud všechny monočleny polynomu f mají stejný stupeň.

Poznámka 7.2. Zřejmě součin homogenních polynomů je homogenní polynom. Součet dvou homogenních polynomů obecně nemusí být homogenní polynom.

Definice 7.3. 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 7.4. *Zobrazení π z definice 7.3 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 $g = \sum_{(l_1,\ldots,l_n)\in\mathbb{N}^n} b_{l_1,\ldots,l_n} x_1^{l_1} \cdots x_n^{l_n}$ jsou dva polynomy z $\mathcal{R}[x_1, \ldots, x_n]$, pak:

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

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. $\square$

Definice 7.5. 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 7.6. Uveďme pár příkladů symetrických polynomů. Budeme se držet značení z definice 7.5.

(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) $\mathrm{lm}(\delta_{in}) = x_1 \cdots x_i$
(c) $\mathrm{lc}(\delta_{in}) = 1$
(d) $\mathrm{ht}(\delta_{in}) = (\underbrace{1, \ldots, 1}_{i\times}, \underbrace{0, \ldots, 0}_{(n-i)\times})$
(e) δ_{in} je homogenní polynom

Lemma 7.7. *Nechť $\mathcal{R}$ je okruh a nechť $(\varphi_i \mid i \in I)$ je systém okruhových homomorfismů $\mathcal{R}$ do sebe. Označme $S = \{r \in R \mid \forall i \in I : \varphi_i(r) = r\}$ (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 7.8. *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 7.7 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 7.9. *Nechť $\mathcal{R} \leq \mathcal{S}$ jsou dva obory integrity, $s_1, \ldots, s_n \in S$ a nechť*

$$\varphi \colon R \;\; \to \;\; S$$

je okruhový homomorfismus. Pak existuje právě jeden okruhový homomorfismus

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

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 $0 \neq f = \sum_{(k_1,\dots,k_n)\in\mathbb{N}^n} a_{k_1,\dots,k_n} x_1^{k_1} \cdots x_n^{k_n}$ definujme:

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

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

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

neboť $\varphi(a_{k_1,\dots,k_n} + b_{k_1,\dots,k_n}) = \varphi(k_1, \dots, k_n) + \varphi(b_1, \dots, b_n)$. 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 $\psi' \colon R[x_1, \dots, x_n] \to S$ takový, že $\psi'_{\restriction R} = \varphi$ a zároveň nechť pro každé $i = 1, \dots, n$ platí, že $\psi'(x_i) = s_i$. Pak zřejmě pro libovolné $f = \sum_{(k_1,\dots,k_n)\in\mathbb{N}^n} a_{k_1,\dots,k_n} x_1^{k_1} \cdots x_n^{k_n}$ platí:

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

□

Příklad 7.10. Uveďme pár konkrétních příkladů na předchozí lemma. Budeme se držet značení z lemmatu 7.9, 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 $\mathcal{R} \supseteq \mathcal{S}$ jsou dva obory integrity, $s \in S$ a $\varphi = \mathrm{id} \colon R \hookrightarrow S$. Pak z lemmatu 7.9 plyne existence následujícího zobrazení:

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

(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 7.9 plyne existence následujícího zobrazení:

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

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

Lemma 7.11. *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 7.6 platí:

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

z čehož plyne:

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

Nyní využijeme lemma 3.1 a dostáváme:

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

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

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

což platí, právě když $\mathrm{ht}\,(v)=(l_1,\ldots,l_n)=(k_1,\ldots,k_n)=\mathrm{ht}\,(u)$ (Poslední implikace z leva doprava 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 7.12. Nechť $\mathcal{R}\le\mathcal{S}$ 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 7.13. *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 7.9 zobrazení $\psi: S\to S$ 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:

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

Pro každé $j=1,\ldots,m$ označíme polynom $\psi(g_j)=g_j(\delta_{1n},\ldots,\delta_{nn})$ jako h_j. Z lemmatu 7.11 plyne, že pro každé $j=1,\ldots,m$ platí:

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

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 $\mathrm{ht}\,(h_j) = \mathrm{ht}\,(f(\delta_{1n}, \dots, \delta_{nn}))$, což implikuje $f(\delta_{1n}, \dots, \delta_{nn}) \neq 0$. $\square$

Lemma 7.14. *Nechť $\mathcal{R}$ je obor integrity a nechť f je libovolný nenulový polynom z okruhu symetrických polynomů $\mathcal{S}_R[x_1, \dots, x_n]$ takový, že $ht(f) = (k_1, \dots, k_n)$. Pak $k_1 \geq k_2 \geq \dots \geq k_n$.*

Důkaz. Nechť f má následující tvar:

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

Pro spor předpokládejme, že existuje $i \in \{1, \dots, n\}$ 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:

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

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

Věta 7.15 (O symetrických polynomech)**.** *Nechť $\mathcal{R}$ je obor integrity a nechť f je libovolný polynom z okruhu symetrických polynomů $\mathcal{S}_R[x_1, \dots, x_n]$. Pak existuje jednoznačně určený polynom $f' \in R[x_1, \dots, x_n]$ takový, že $f = f'(\delta_{1n}, \dots, \delta_{nn})$.*

Důkaz. Nejdříve dokážeme existenci polynomu $f' \in R[x_1, \dots, x_n]$. Pokud $f = 0$, stačí jako f' vzít nulový polynom. Nechť tedy $f \neq 0$. Tvrzení dokážeme indukcí podle výšky polynomu f (z lemmatu 7.14 plyne, že tato indukce je na množině všech symetrických polynomů skutečně možná). Pokud $\mathrm{ht}\,(f) = (0, 0, \dots, 0)$, pak $f = a \cdot x_1^0 \cdots x_n^0$, kde $0 \neq a \in R$ a stačí zvolit $f' = a \in R[x_1, \dots, x_n]$. 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 7.14 plyne, že $k_1 \geq k_2 \geq \dots \geq k_n$. 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 7.11 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 7.13 plyne, že $f' = f''$. $\square$

Příklad 7.16. Buď $f = x_1^2x_2 + x_1x_2^2 + x_1x_2 \in S_{\mathbb{C}}[x_1, x_2]$, zřejmě $\mathrm{ht}\,(f) = (2, 1)$ a $\mathrm{lc}\,(f) = 1$. Budeme-li se držet značení z věty 7.15, máme $u = x_1 \cdot x_2$ a $g = \delta_{12} \cdot \delta_{22} = (x_1 + x_2)(x_1x_2) = x_1^2x_2 + x_1x_2^2$, zřejmě $\mathrm{ht}\,(g) = (2, 1)$ a $\mathrm{lc}\,(g) = 1$. A jelikož $f - g = x_1x_2 = \delta_{22}$, máme $h' = x_2$ a tedy $f' = x_1x_2 + x_2 \in \mathbb{C}[x_1, x_2]$.

Příklad 7.17 (Aplikace teorie symetrických polynomů). Nechť $\mathcal{R} \leq \mathcal{S}$ jsou dva obory integrity, mějme polynom $f \in R[x]$, $f = \sum_{i=0}^{n} a_i x^i$ 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 7.15 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:

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

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 7.18. Budeme se držet značení z příkladu 7.17. 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 7.16 plyne, že $g = g'(\delta_{12}, \delta_{22})$, kde $g' = x_1x_2 + x_2$. Máme tedy:

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

8. Derivace a násobnost kořenů

Lemma 8.1 (o dosazovacím homomorfismu)**.** *Nechť $\mathcal{R}, \mathcal{S}$ jsou komutativní okruhy, $\varphi\colon R \to S$ je okruhový homomorfismus a $s \in S$. Pak existuje právě jeden okruhový homomorfismus $\varphi_s\colon R[x] \to S$, takový, že $\varphi_s \restriction R = \varphi$ a $\varphi_s(x) = s$. (φ_s se nazývá dosazovací homomorfismus příslušný φ a s)*

Důkaz.

$$\begin{tikzcd}
R \arrow[d, "\varphi"] & \subseteq & R[x] \arrow[dll, "\bar{\varphi}"] \\
S & &
\end{tikzcd}$$

Homomorfismus $\varphi_s : R[x] \to S$ definujeme následovně: $\varphi_s(0) = 0$ a $\varphi_s(f) = \sum_{n=0}^{m} \varphi(a_n)s^n$, kde $f = \sum_{n=0}^{m} a_n x^n$. Dokážeme, že se jedná o okruhový homomorfismus. Označme $g = \sum_{n=0}^{m'} a'_n x^n$. Snadno ověříte, že $\varphi_s(f+g) = \varphi_s(f) + \varphi_s(g)$. Pro součin máme

$$\varphi_s(f \cdot g) = \varphi_s(\sum_{n=0}^{m+m'} (\sum_{k=0}^{n} a_k a'_{n-k}) x^n) = \sum_{n=0}^{m+m'} \varphi(\sum_{k=0}^{n} a_k a'_{n-k}) s^n = \sum_{m=0}^{m+m'} \sum_{k=0}^{n} \varphi(a_k)\varphi(a'_{n-k}) s^n$$

$$\varphi_s(f) \cdot \varphi_s(g) = (\sum_{n=0}^{m} \varphi(a_n)s^n \cdot \sum_{n=0}^{m'} \varphi(a'_n)s^n = \sum_{m=0}^{m+m'} \sum_{k=0}^{n} \varphi(a_k)\varphi(a'_{n-k}) s^n.$$

A triviálně $\varphi_s(1) = \varphi(1) \cdot a^0 = 1$.

Předpokládejme, že $\varphi' : R[x] \to S$ je dosazovací homomorfismus příslušný φ a $s \in S$, tedy $\varphi'(x) = s$ a $\varphi'(a) = \varphi(a)$ pro každé $a \in R$. Z vlastností homomorfismů snadno plyne, že $\varphi'(x^n) = s^n$ a dále $\varphi'(a_n x^n) = \varphi(a_n)s^n$. Tedy $\varphi'(\sum_{n=0}^{m} a_n x^n) = \sum_{n=0}^{m} \varphi(a_n)s^n = \varphi_s(\sum_{n=0}^{m} a_n x^n)$, neboli $\varphi' = \varphi_s$. □

Věta 8.2. *Nechť $\mathcal{R}, \mathcal{S}$ jsou komutativní okruhy, $\varphi : R \to S$ je okruhový homomorfismus a $\rho = (s_i \mid i \in I)$ je posloupnost prvků z $\mathcal{S}$. Pak existuje právě jeden okruhový homomorfismus $\varphi_\rho : R[x_i \mid i \in I] \to S$, takový, že $\varphi_\rho \restriction R = \varphi$ a pro každé $i \in I$ platí $\varphi_\rho(x_i) = s_i$. (φ_ρ se nazývá dosazovací homomorfismus příslušný φ a ρ)*

Důkaz. Jedná se o zobecnění důkazu předchozího lemmatu. □

Příklad 8.3.
(1) Pokud $\varphi = \mathrm{id}_R : R \to S$ ($\mathcal{R}$ je podokruhem v $\mathcal{S}$) a $s \in S$. Pak $\varphi_s = \mathrm{id}_s : R[x] \to S$ a $\mathrm{Ker}\ \mathrm{id}_s = \{f \in R[x] \mid f(s) = 0\}$ je ideál v $\mathcal{R}[x]$. Speciálně, je-li $\mathcal{R}$ komutativní těleso, je $\mathrm{Ker}\ \mathrm{id}_s$ hlavní ideál a jeho monický generátor se nazývá *minimální polynom* s nad $\mathcal{R}$.
(2) Pokud $R = S$, $\varphi = \mathrm{id}_R$ a $s \in S$. Pak se $\varphi_s = \mathrm{id}_s$ nazývá *polynomiální funkce* nad $\mathcal{R}$.
(3) Pokud $S = R[x]$ a $s \in S$. Pak dosazovací homomorfismus $\varphi_s = \mathrm{id}_s : R[x] \to R[x]$ dělá to, že do polynomů z $\mathcal{R}[x]$ dosazuje polynom s.

Definice 8.4. Nechť $R \subseteq S$ jsou obory integrity.

(i) Nechť $f \in R[x]$, $s \in S$. Pak s je *kořenem* polynomu f v $\mathcal{S}$, pokud $f(s) = 0$ (neboli $\mathrm{id}_s(f) = 0$, pro $f = 0$ je kořenem každé $s \in S$.
(ii) Prvek $s \in S$ se nazývá *algebraický* nad $\mathcal{R}$, pokud existuje $0 \neq f \in R[x]$ takové,že s je kořenem f ($f(s) = 0$). V opačném případě se s nazývá *transcendentní* nad $\mathcal{R}$.
(iii) $\mathcal{S}$ je *algebraickým rozšířením* $\mathcal{R}$, pokud každé $s \in S$ je algebraickým prvkem nad $\mathcal{R}$.
(iv) $\mathcal{S}$ je *transcendentním rozšířením* $\mathcal{R}$, pokud každý prvkek $s \in S \setminus R$ není algebraickým prvkem nad $\mathcal{R}$.

Příklad 8.5.
(1) Každý prvek $s \in R$ je algebraický nad $\mathcal{R}$, neboť $f(s) = 0$ pro $f = x - s \in R[x]$.
(2) $\mathcal{S} = \mathcal{R}[x]$ je transcendentním rozšířením $\mathcal{R}$, neboť pokud $0 \neq f \in R[x]$, $s \in R[x] \setminus R$, pak $f(s) \neq 0$, neboť když $\deg(f) = 0$ (f je konstantní nenulový polynom), pak jistě $f(s) \neq 0$ a když $\deg(f) \geq 1$, pak $\deg(f(s)) = \deg(f) \cdot \deg(s) \geq 1$, čili opět $f(s) \neq 0$.

Lemma 8.6. *Nechť $R \subseteq S$ jsou obory integrity, $f \in R[x]$, $deg(f) = n \geq 0$. Potom f má v $\mathcal{S}$ nejvýše n různých kořenů.*

Důkaz. Budeme postupovat indukcí dle stupně polynomu f, čili podle n. Pro $n = 0$ je tvrzení triviální. Předpokládejme, že $\deg(f) = n \geq 0$. Pokud f nemá v $\mathcal{S}$ kořen, jsme hotovi. Předpokládejme tedy, že f má v $\mathcal{S}$ kořen s. Z 3.3 víme, že si polynom f můžeme napsat jako $f = (x - s)f' + g$ v oboru integrity $\mathcal{S}[x]$. Ukážeme, že g je nutně nulový polynom. V první řadě máme

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

a dále z 3.3 víme, že $1 = \deg(x - s) > \deg(g)$, takže $\deg(g) = 0$. Takže nezbývá nic jiného, než, že $g = 0$ a tedy $f = (x - s)f'$ v oboru integrity $\mathcal{S}[x]$ a navíc $\deg(f') = n - 1$. Dle indukčního předpokladu má polynom f' v $\mathcal{S}[x]$ nejvýše $n-1$ kořenů a je snadné si rozmyslet, že z toho plyne, že f má v $\mathcal{S}[x]$ nejvýše n kořenů (jediný kořen, který má f navíc je prvek s). □

Definice 8.7. Nechť $\mathcal{R}$ je obor integrity. *Operátorem derivování* v $\mathcal{R}[x]$ rozumíme zobrazení $D(-) : R[x] \to R[x]$, které definujeme následovně:

(i) $D(f) = 0$, je-li $\deg(f) \leq 0$,

(ii) $D(f) = \sum_{n=0}^{m-1}(n+1)a_{n+1}x^n$, kde $f = \sum_{n=0}^{m} a_n x^n$.

Pokud je stupeň polynomu f roven m, je stupeň výsledného polynomu $D(f)$ menší nebo roven $m-1$ a pokud $char R \neq m$, je stupeň polynomu $D(f)$ roven $m-1$. Dále definujeme pro každé přirozené $n \geq 1$ operátor

$$D^n(-) = \underbrace{D(\dots(D}_{n\text{-krát}}(-))\dots)$$

a dále definujeme $D^0(-) = \mathrm{id}(-)$. $D^n(f)$ se nazývá *n-tá (formální) derivace* polynomu f a $D(f) = D^1(f)$ se též nazývá *(formální) derivace* polynomu f. (Pokud si za $\mathcal{R}$ představíte těleso reálných čísel, dostanete přesně ten operátor na který jste zvyklí z matematické analýzy.)

Lemma 8.8. *Nechť $\mathcal{R}$ je obor integrity, $f, g \in R[x]$. Pak pro každé přirozené $n \geq 0$ máme*

(1) $D^n(f + g) = D^n(f) + D^n(g)$

(2) $D^n(f \cdot g) = \sum_{k=0}^{n}\binom{n}{k}D^k(f)D^{n-k}$, *pokud* $char(R) = 0$ *(Leibnitzova formule)*

(3) $D(f^n) = n \cdot f^{n-1} \cdot D(f)$, *pokud* $n \geq 1$.

Důkaz. Vztahy (1) a (2) se dokáží indukcí podle n ze vztahů $D(f + g) = D(f) + D(g)$ a $D(f \cdot g) = f \cdot D(g) + g \cdot D(f)$ (u vztahu (2) využijeme identitu z kombinatoriky $\binom{n+1}{k+1} = \binom{n}{k+1} + \binom{n}{k}$).

Vztah (3) se také dokáže indukcí podle n. Pro $n = 1$ je tvrzení triviální. Pokud $n \geq 2$, máme z indukčního předpokladu

$$D(f^n) = D(f^{n-1} \cdot f) = D(f^{n-1}) \cdot f + f^{n-1} \cdot D(f) = n \cdot f^{n-1} \cdot D(f)$$

. □

Definice 8.9. Nechť $R \subseteq S$ jsou obory integrity, $s \in S$, $f \in R[x]$, $\deg(f) \geq 1$ a $n \geq 0$ nechť je přirozené číslo. Pak s je *n-násobným kořenem* polynomu f v $\mathcal{S}$, pokud existuje polynom $g \in S[x]$ takový, že $f(x) = (x - s)^n \cdot g(x)$ a s není kořenem polynomu g v $\mathcal{S}$. Pokud s je 1-násobným kořenem polynomu f v $\mathcal{S}$, říkáme, že s je *jednoduchý kořen* polynomu f v $\mathcal{S}$.

Poznámka 8.10. V oborech integrity je n určeno jednoznačně. Pro spor předpokládejme, že $f(x) = (x - s)^n \cdot g(x) = (x - s)^m \cdot h(x)$ v $\mathcal{S}[x]$ a BÚNO $n < m$. Pak $(x - s)^n(g(x) - (x - s)^{m-n} \cdot h(x)) = 0$ v $S[x]$. Protože $\mathcal{S}[x]$ je obor integrity a $(x - s)^n$ není nulový polynom, nutně $g(x) = (x-s)^{m-n} \cdot h(x)$. Dosazením $x = s$ získáme $g(s) = 0 \cdot h(s) = 0$, což je spor s předpokladem, že s není kořenem polynomu g.

Věta 8.11. *Nechť $R \subseteq S$ jsou obory integrity, $s \in S$, $f \in R[x]$, $deg(f) \geq 1$. Pak platí:*

(1) *s je kořenem f v $\mathcal{S}$, právě když existuje $1 \leq n \leq deg(f)$ takové, že s je n-násobným kořenem f v S (a toto n je jednoznačně určené, dle 8.10).*

(2) *je-li $char(R) = 0$ nebo $deg(f) < char(R)$, pak s je n-násobným kořenem f v $\mathcal{S}$ právě tehdy, když s je kořenem polynomů $f, D(f), \ldots D^{n-1}(f)$ v $\mathcal{S}$, ale s není kořenem polynomu $D^n(f)$v $\mathcal{S}$.*

Důkaz. (1) Implikace zprava doleva je triviální. Ukážeme obrácenou implikaci. Jelikož $\deg(f) \geq 1$ a $\mathcal{S}[x]$ je Eukleidovský obor integrity, existují polynomy $p, q \in S[x]$ takové, že $f(x) = q(x)(x-s) + p(x)$ v $\mathcal{S}[x]$ a $\deg(p) < \deg(x-s) = 1$. Dosazením kořene s do předchozího vyjádření zjistíme, že $f(x) = q(x)(x-s)$ v $\mathcal{S}[x]$. Dále je buď $q(s) \neq 0$ (s je jednoduchý kořen f v $\mathcal{S}$) a jsme hotovi nebo $q(s) = 0$ a v takovém případě opakujeme předchozí úvahu. Jelikož $\deg(q) = \deg(f) - 1$, zastavíme se po nejvýše $\deg(f)$ krocích.

(2) Nechť $f = (x-s)^n g$, $g(s) \neq 0$. Pak pro $m \geq 1$ máme

$$D^m(f) = D^m((x-s)^n g) = \sum_{k=0}^{m} \binom{m}{k} D^k((x-s)^n) \cdot D^{n-k}(g)$$

a pro každé $k \leq n$ platí

$$D^k((x-s)^n) = D^{k-1}(n \cdot (x-s)^{n-1} \cdot D((x-s)) =$$
$$= D^{k-1}(n \cdot (x-s)^{n-1}) = n \cdot (n-1) \ldots (n-k+1) \cdot (x-s)^{n-k}$$

Tedy, je-li $k \leq m < n$, pak $D^k((x-s)^n)(s) = 0$ a tudíž $D^m(f)(s) = 0$. Pokud $m = n$, pak $D^n(f)(s) = n! g(s) \neq 0$, protože $g(s) \neq 0$ dle předpokladu a $n! \neq 0$ též dle předpokladu, tentokráte ale dle předpokladu o charakteristice oboru integrity $\mathcal{S}$.

Pro implikaci zprava doleva máme v první řadě z části (1), že existuje $m \leq \deg(f)$ takové, že s je m-násobný kořen polynomu f v $\mathcal{S}$. Podle právě dokázané implikace z části (2) máme, že s je kořenem $f, D(f) \ldots D^{m-1}(f)$ v $\mathcal{S}$, ale s není kořenem $D^m(f)$ v $\mathcal{S}$. Z předpokladu víme, že s je kořenem $f, D(f) \ldots D^{n-1}(f)$ v $\mathcal{S}$ a s není kořenem $D^n(f)$ v $\mathcal{S}$, proto musí platit $m = n$.

□

Důsledek 8.12. *Nechť $R \subseteq S$ jsou obory integrity, $f \in R[x]$, $deg(f) \geq 1$, $char(R) = 0$. Potom f má v $\mathcal{S}$ jen jednoduché kořeny právě, když f a $D(f)$ nemají v $\mathcal{S}$ žádné společné kořeny.*

Důkaz. Dle 8.11 je prvek s kořenem f v $\mathcal{S}$ právě, když $f = (x-s)g$ pro nějaké $g \in S[x]$. Dále $D(f) = D((x-s)g) = g + D(g)(x-s)$ v $\mathcal{S}[x]$. Takže s je jednoduchým kořenem polynomu f v $\mathcal{S}$ právě, když $g(s) \neq 0$, což je právě, když $D(f)(s) \neq 0$, což je právě, když s není společným kořenem polynomů f a $D(f)$. □

Definice 8.13. Nechť T je komutativní těleso, $f \in T[x]$. Pak řekneme, že polynom f je *separabilní*, pokud f má jen jednoduché kořeny v každém rozšíření $K \geq T$ (K je taktéž komutativní těleso). Dále řekneme, že těleso T je *perfektní*, pokud každý ireducibilní polynom $f \in T[x]$ je separabilní.

Důsledek 8.14. *Každé komutativní těleso charakteristiky* 0 *je perfektní.*

Důkaz. Chceme, že každý ireducibilní polynom $f \in T[x]$ stupně alespoň 1 má jen jednoduché kořeny v libovolném nadtělese $K \supseteq T$. Uvažme tedy takový polynom f a libovolné nadtěleso $K \supseteq T$. Jistě $f, D(f) \in T[x]$. Označme $g \in T[x]$ jejich největšího společného dělitele v $T[x]$ (který existuje, protože $T[x]$ je Gaussův obor integrity). Z Eukleidova algoritmu dokonce víme, že g je též NSD $(f, D(f))$ v $K[x]$. Jelikož f je ireducibilní, je buď $g = 1$ a tedy f a $D(f)$ jsou nesoudělné v $K[x]$, nebo $g = f$, což nelze, protože by to znamenalo, že f dělí $D(f)$, ale $\deg(D(f)) < \deg(f)$. $D(f)$ a f tedy jistě nemají žádné společné kořeny v $K[x]$, což podle 8.12 znamená, že f má v K pouze jednoduché kořeny. □

9. Kořenová a rozkladová nadtělesa

Lemma 9.1. *Nechť $T \subseteq K$ jsou komutativní tělesa. Nechť $a \in K$ je algebraický prvek nad T. Potom existuje právě jeden polynom $0 \neq f \in T[x]$ takový, že*

(i) *a je kořenem f*
(ii) *f je monický a ireducibilní v $T[x]$*
(iii) *je-li $g \in T[x]$ a a je kořenem g, pak f dělí g (tj. $Rf \supseteq Rg$)*

Důkaz. Definujeme množinu $M_a = \{h \in T[x] | h(a) = 0, \deg(h) > 0\}$. V této množině existuje $\bar{f}$, jehož stupeň je minimální. Označme $\bar{f} = \sum_{n=0}^{k} a_n x^n$, kde $k \geq 1$ a $a_k \neq 0$. Pak polynom $f = a_k^{-1}\bar{f}$ je monický, $f(a) = 0$ a $\deg(f)$ je minimální (naše hledané f).

Kdyby $f = g \cdot g'$, pak $f(a) = g(a) \cdot g'(a)$, tedy $g(a)$ nebo $g'(a)$ je rovno 0, předpokládejme, že $g(a)$. Stupeň f je minimální, proto $\deg(f) = \deg(g)$. Tedy g' je invertibilní (je to prvek T) a polynom g je tedy asociován s polynomem f v $T[x]$. Polynom f je tedy ireducibilní.

Nechť $g(a) = 0$, pak při dělení se zbytkem v $T[x]$ získáme $g = qf + p$, kde $\deg(p) < \deg(f)$. Dosazením a vyjde $0 = g(a) = q(a)\underbrace{f(a)}_{=0} + p(a)$, tudíž $p = 0$ a f dělí h ($Rf \supseteq Rg$).

(Jednoznačnost f) Nechť f i f' mají požadované vlastnosti. Podle předchozího f dělí f' a naopak f' dělí f. Polynomy f a f' jsou tedy asociované. Zároveň jsou oba monické, takže $f = f'$. □

Definice 9.2. Nechť $T \subseteq K$ jsou komutativní tělesa, $a \in K$ je algebraický prvek nad T. Polynom f z věty 9.1 se nazývá *minimální polynom* prvku a nad T a značí se $m_{a,T}$.

Příklad 9.3. Minimálním polynomem prvku $a \in T$ je $m_{a,T} = x - a \in T[x]$.

Lemma 9.4. *Nechť $T \subseteq K$ jsou komutativní tělesa, $a \in K$. Označme $T(a)$ průnik všech podtěles K, která obsahují T i prvek $\{a\}$ (tj. $T(a) = \bigcap_{T \subseteq T' \subseteq K, a \in T'} T'$). Je-li prvek a algebraický nad T, je $T(a) = \{f(a) | f \in T[x]\} \subseteq K$.*

Důkaz. Označme množinu $S = \{f(a) | f \in T[x]\}$. Ukážeme, že S je nejmenší podtěleso (myšleno s operacemi z K) tělesa K, které obsahuje těleso T a prvek a a tím dokážeme tvrzení. Množina S zřejmě obsahuje prvek a i těleso T (dosazení prvku a do polynomu $f = x$ a do konstantních polynomů $f_t = t$, $t \in T$). Je-li T' podtěleso K obsahující T a a, zřejmě platí, že $T' \supseteq S = \{f(a) | f \in T[x]\}$, neboť pro $b = f(a) = \sum_{n=0}^{m} a_n a^n$ máme všechna a_n i a^n prvky tělesa T', takže i $b \in T'$.

Stačí tedy pouze ověřit, že S je nosičem podtělesa K. Jistě $f(a) + g(a) = (f + g)(a) \in S$ a $f(a) \cdot g(a) = (f \cdot g)(a) \in S$, tedy S je podokruh K. Ukážeme, že každý nenulový prvek S je invertibilní. Vezměme $0 \neq f(a) \in S$. Minimální polynom prvku a, $m_{a,T}$ jistě nedělí f, tedy ($m_{a,T}$ je ireducibilní polynom) NSD $(m_{a,T}, f) = 1 \in T[x]$. Dle 3.6 je $T[x]$ obor integrity hlavních ideálů, takže ideál $Tf + Tm_{a,T}$ musí být tvaru $Tf + Tm_{a,T} = Tg$ pro nějaký polynom

$g \in T[x]$. Protože ale NSD $(m_{a,T}, f) = 1$ je $g \in T$, takže $Tf + Tm_{a,T} = T$. Dostáváme, že existují polynomy $g, h \in T[x]$ takové, že $gf + hm_{a,T} = 1$ v $T[x]$. Po dosazení prvku a dostáváme $1 = g(a)f(a)$. Každý nenulový prvek $f(a)$ z S je tedy invertibilní a S je tedy těleso. □

Definice 9.5. Těleso $T(a)$ z předchozího lemmatu se nazývá *těleso vzniklé adjunkcí* algebraického prvku a k tělesu T.

Definice 9.6. Nechť $T \subseteq K$ jsou komutativní tělesa. Pak řekneme, že K je *rozšíření konečného stupně* nad T (nebo zkráceně K je konečného stupně nad T), pokud $\dim_T(K) < \infty$, kde $\dim_T(K)$ znamená dimenzi vektorového prostoru K na tělesem T, která se též značí i jako $[K : T]$.

Věta 9.7. *Nechť $T \subseteq K$ jsou komutativní tělesa. Je-li K rozšíření konečného stupně nad T, pak K je algebraickým rozšířením tělesa T. (Pozn.: Obrácená implikace neplatí.)*

Důkaz. Vezměme libovolný prvek $a \in K$, ukážeme, že je algebraický nad T. Označme $n = \dim_T(K)$, máme, že $n < \infty$ a proto je množina $\{1, a, a^2, \ldots, a^n\}$ T-lineárně závislá (obsahuje $n+1$ prvků). Tudíž existují prvky $t_0, \ldots, t_n \in T$, takové, že alespoň jeden z nich je nenulový a $t_0 \cdot 1 + t_1 \cdot a + \cdots + t_n \cdot a^n = 0$. Označme $f(x) = \sum_{i=0}^{i=n} t_i x^i \in T[x]$. Máme $f(a) = 0$, a proto je prvek a alegbraický nad tělesem$T$. □

Věta 9.8. *Nechť $T \subseteq K$ jsou komutativní tělesa a nechť je $a \in K$ je algebraický prvek nad T. Pak $T(a)$ je rozšíření konečného stupně nad K a $[T(a) : T] = deg(m_{a,T})$. Speciálně, $T(a)$ je algebraickým rozšířením tělesa T.*

Důkaz. Označme $n = \deg(m_{a,T}) \geq 1$. Ukážeme, že $B = \{1, a, a^2, \ldots a^{n-1}\}$ je T-báze (je T-nezávislá) tělesa $T(a)$.

Nejprve dokážeme lineární nezávislost množiny B. Nechť $\sum_{i=0}^{n-1} t_i a^i = 0$. Pak polynom $f = \sum_{i=0}^{n-1} t_i x^i$ má kořen a, tedy $m_{a,T} | f$. Zároveň je ovšem $\deg(f) \leq n-1 < n = \deg(m_{a,T})$. To je možné pouze pro $f = 0$ a $t_0 = \ldots t_{n-1} = 0$, množina B je tedy lineárně nezávislá.

Ověření, že B je generující podmnožina $T(a)$ znamená ukázat, že $T(a) = \{f(a) | f \in T[x], \deg(f) < n\}$. Zřejmě platí

$$T(a) \overset{9.4}{=} \{f(a) | f \in T[x]\} \supseteq \{f(a) | f \in T[x], \deg(f) < n\}.$$

(Opačná inkluze) Po vydělení libovolného polynomu $f \in T[x]$ polynomem $m_{a,T}$ získáme vyjádření $f = m_{a,T} \cdot q + p$, kde $\deg(p) < n$. Dosazením a zjistíme, že

$$f(a) = \underbrace{m_{a,T}(a)}_{=0} \cdot q(a) + p(a) = p(a).$$

Pro každé $b \in T(a)$ existuje polynom f, pro který $f(a) = b$. Podle předchozí úvahy existuje také p, $\deg(p) < m$, takový, že $p(a) = b$. Tím je dokázána inkluze $T(a) \subseteq \{f(a) | f \in T[x], \deg(f) < n\}$ a zároveň celé tvrzení. □

Lemma 9.9. *Nechť $A \subseteq B \subseteq C$ jsou komutativní tělesa. Potom*

$$[C : A] = [C : B] \cdot [B : A].$$

Důkaz. Nechť $\{b_i | i \in I\}$ je A-báze B a $\{c_j | j \in J\}$ je B-báze C. Stačí, když ukážeme, že $U = \{b_i c_j | i \in I, j \in J\}$ je A-báze C, neboť mohutnost U je pak rovna $[C : B] \cdot [B : A]$.

Pro libovolné $c \in C$ existují taková $b'_j \in B, j \in J$, že $c = \sum_{j \in J} b'_j c_j$, protože $\{c_j | j \in J\}$ je B-báze C. Pro každé b'_j pak existují prvky $a_{ij} \in A$ takové, že $b'_j = \sum_{i \in I} a_{ij} b_i$, tudíž každé

$c \in C$ lze zapsat jako $c = \sum_{j \in J}(\sum_{i \in I} a_{ij} b_i) c_j = \sum_{i \in I} \sum_{j \in J} a_{ij}(b_i c_j)$, tedy U je A-generující množina.

Nechť $a_{ij} \in A$ $(i \in I, j \in J)$ taková, že $\sum_{i \in I} \sum_{j \in J} a_{ij}(b_i c_j) = 0$. Pak $\sum j \in J(\sum_{i \in I} a_{ij} b_i) c_j = 0$. Jelikož je $\{c_j | j \in J\}$ B-nezávislá, musí být $\sum_{i \in I} a_{ij} b_i = 0$ pro každé $j \in J$. Množina $\{b_i | i \in I\}$ je ovšem A-nezávislá, tudíž $a_{ij} = 0$ pro každé $i \in I$. Množina U je tedy A-nezávislá a je to tedy A-báze tělesa C. □

Definice 9.10. Nechť $T \subseteq K$ jsou komutativní tělesa a $a_1, \dots, a_n \in K$ nechť jsou algebraické prvky nad T. Označme $T(a_1, \dots, a_n)$ průnik všech podtěles K obsahujících těleso T a prvky $a_1, \dots, a_n$ (neboli nejmenší takové podtěleso). Toto těleso se nazývá *podtěleso K vzniklé adjunkcí algebraických prvků $a_1, \dots a_n$* k tělesu T.

Poznámka 9.11. Zřejmě platí, že $T(a_1, \dots, a_n) = (\dots(T(a_1))(a_2)\dots)(a_n)$.

Věta 9.12. *Nechť $T \subseteq K$ jsou komutativní tělesa. Potom K je konečného stupně nad T právě tehdy, když existuje konečná množina algebraických prvků $\{a_1, \dots a_n\}$ taková, že $K = T(a_1, \dots a_n)$.*

Důkaz. Nechť $[K : T] = m < \infty$. Indukcí dle m dokážeme tvrzení. Pokud $m = 1$, pak stačí volit $n = 1$ a $a_1 = 0$. Pokud $m > 1$, pak jistě $K \neq T$, takže existuje prvek $a_1 \in K \setminus T$. Dle 9.7 je a_1 algebarický prvek nad tělesem T. Máme

$$T \subseteq T(a) \subseteq K.$$

Dle 9.9 platí $m = [K : T] = [K : T(a_1)][T(a_1) : T]$ a protože $\deg(m_{a_1,T}) > 1$, máme, že $[K : T(a_1)] < m$. Dle indukčního předpokladu existují $a_2, \dots, a_n \in K$ algebraické nad T takové, že $(T(a_1))(a_2, \dots, a_n) = K$. Levá strana rovnosti je ale rovna $T(a_1, \dots, a_n)$, čímž je implikace zleva doprava dokázána.

Nechť $K = T(a_1, \dots a_n)$, kde $a_1, \dots a_n$ jsou algebraické nad T. Indukcí dle n dokážeme, že $[K : T] < \infty$. Pro $n = 1$ je $K = T(a_1)$, tedy $[K : T] = \deg(m_{a_1,T}) < \infty$.

Pro $n > 1$ je $K = T(a_1, \dots, a_n) = (T(a_1, \dots a_{n-1})(a_n)$. Dle lemmatu 9.9 je

$$[K : T] = [T(a_1, \dots, a_{n-1}) : T] \cdot [(K : T(a_1, \dots, a_{n-1})],$$

přičemž stupeň $[T(a_1, \dots, a_{n-1}) : T]$ je konečný dle indukčního předpokladu a

$$[(T(a_1, \dots, a_{n-1}))(a_n) : T(a_1, \dots, a_{n-1})] = \deg(m_{a_n, T(a_1, \dots, a_{n-1})}),$$

takže i stupeň $[K : T]$ je konečný, čímž je dokázána i implikace zprava doleva. □

Definice 9.13. Nechť T je komutativní těleso, $f \in T[x]$ polynom stupně alespoň 1. Nadtěleso (rozšíření) U tělesa T se nazývá *kořenovým nadtělesem* polynomu f nad tělesem T, pokud v U existuje prvek a takový, že $U = T(a)$ a zároveň $f(a) = 0$.

Lemma 9.14. *Nechť T je komutativní těleso a $f \in T[x]$ polynom stupně alespoň 1. Potom existuje komutativní nadtěleso $K \supseteq T$ takové, že f má v K alespoň jeden kořen.*

Důkaz. Protože $R = T[x]$ je Gaussův (dokonce Eukleidův) obor integrity (a tedy každý prvek je součinem ireducibilních), stačí tvrzení dokázat pro ireducibilní polynomy v $R = T[x]$, neboť pro ireducibilní rozklad polynomu $f = f_1 \cdot \dots \cdot f_n$ stačí najít kořen libovolného z ireducibilních činitelů.

Jelikož $\mathcal{R}$ je OIHI a $f_1 = \sum_{i=0}^{n} a_i x^i$ je ireducibilní, Rf_1 je maximální (vlastní) ideál R a faktorový okruh R/Rf_1 je komutativní okruh bez vlastních ideálů, tedy $K' = R/Rf_1$ je těleso.

Definujeme okruhový homomorfismus (projekci) $\pi : R \to K'$ tak, že $r \mapsto r + Rf_1$. Restrikcí $\pi \restriction T$ získáme okruhový homomorfismus z T do K' zobzazující $t \mapsto t + Rf_1$. Tento homomorfismus je prostý, neboť jestliže $t + Rf_1 = t' + Rf_1$, pak $t - t' = rf_1$ pro nějaké $r \in R$. Protože buď $\deg(rf_1) \geq \deg(f_1) \geq 1$ nebo $rf_1 = 0$, zatímco $\deg(t - t') \leq 0$ $(t, t' \in T)$ a stupně obou stran musí být stejné, musí být $t = t'$. T je tedy izomorfní tělesu $\pi(T) \subseteq K'$.

Zbývá dokázat, že $f_1' = \sum_{i=0}^{n} \pi(a_i)x^i$ má v K' alespoň jeden kořen. Označme $\alpha = \pi(x) \in K'$. Pak $f_1'(\alpha) = \sum_{i=0}^{n} \pi(a_i)\pi(x)^i = \sum_{i=0}^{n} \pi(a_i)\pi(x^i) = \pi(f_1) = 0 \in K'$. Prvek $\alpha \in K'$ je tedy kořenem f_1'. $\square$

Věta 9.15. *Nechť T je komutativní těleso a $f \in T[x]$ polynom stupně alespoň 1. Potom existuje kořenové nadtěleso polynomu f nad tělesem T. Je-li f ireducibilní, pak všechna kořenová nadtělesa f nad T jsou T-izomorfní (tj. existuje mezi nimi izomorfismus, který je identita na T).*

Důkaz.

$$\begin{array}{ccccc}
T[x] & \supseteq & T & \subseteq & T(a) \\
\Big\downarrow{\scriptstyle\bar\varphi} & & \Big\downarrow{\scriptstyle\varphi} & & \Big\downarrow{\scriptstyle\psi} \\
T'[x] & \supseteq & T' & \subseteq & T'(a)
\end{array}$$

Z 9.14 víme, že existuje těleso $K \supseteq T$ takové, že f má v K kořen. Položme $U = T(a) \subseteq K$. Pak U je kořenové nadtěleso f nad T.

Abychom ukázali jednoznačnost kořenového rozšíření, dokážeme následující (obecnější) tvrzení. Nechť $T \overset{\varphi}{\simeq} T'$ jsou izomorfní tělesa a $f = \sum a_n x^n \in T[x]$ je ireducibilní a tedy také $\bar\varphi(f) = f' = \sum \varphi(a_n)x^n \in T'[x]$ je ireducibilní (protože $T[x] \overset{\bar\varphi}{\simeq} T'[x]$). Pak jsou-li $T(a)$ a $T'(a')$ kořenová nadtělesa polynomů f nad T a f' nad T', existuje izomorfismus $\psi : T(a) \to T'(a')$ takový, že $\psi|T = \varphi$. Jednoznačnost kořenového nadtělesa je speciálním případem tohoto tvrzení pro $T = T'$ a $\varphi = \mathrm{id}_T$.

Z 9.8 víme, že $[T(a) : T] = \deg(m_{a,T})$, přičemž $\deg(m_{a,T}) = \deg(f)$, protože $f(a) = 0$ a polynom f je ireducibilní. Platí tedy $f = c \cdot m_{a,T}$, kde $0 \neq c \in T$, nebo-li polynom f je asociován s polynomem $m_{a,T}$ v $T[x]$. Analogicky je $[T'(a') : T'] = \deg(m_{a',T'}) = \deg(f')$ a $f' \parallel m_{a',T'}$ v $T[x]$.

Sestrojíme izomorfismus $\psi : T(a) \to T'(a')$ takový, že $\psi|T = \varphi$. Z 9.4 víme, že $T(a) = \{g(a) \mid g \in T[x]\}$ a $T'(a') = \{h(a') \mid h \in T'[x]\}$. Definujme homomorfismus ψ vztahem $\psi(g(a)) = \bar\varphi(g)(a') \in T'(a')$. Ověřme nejprve, že ψ je korektně definované zobrazení. Platí, že $g(a) = h(a)$ právě tehdy, když $(g - h)(a) = 0$, což je právě tehdy, když $m_{a,T} \mid (g - h)$, což už víme, že je právě tehdy, když $f \mid (g - h)$. Aplikací izomorfismu $\bar\varphi$ máme, že předchozí je právě tehdy, když $f' \mid (\bar\varphi(g) - \bar\varphi(h))$. Anaogicky jako před chvílí dostáváme, že $\bar\varphi(g)(a') = \bar\varphi(h)(a')$ a ψ je tedy korektně definované a navíc (díky ekvivalencím) máme rovnou, že ψ je prosté a přímo z definice ψ se snadno ověří, že je též i na. Zobrazení ψ je tedy bijekce.

Zbývá dokázat, že ψ je homomorfismus a že $\psi|T = \varphi$.

$$\psi(g_1(a) + g_2(a)) = \psi(\mathrm{id}_a(g_1) + \mathrm{id}_a(g_2)) = \psi(\mathrm{id}_a(g_1 + g_2)) =$$
$$= \psi((g_1 + g_2)(a)) = \bar\varphi((g_1 + g_2))(a') = \bar\varphi(g_1)(a') + \bar\varphi(g_2)(a') = \psi(g_1(a)) + \psi(g_2(a)).$$

Analogicky lze dokázat, že $\psi(g_1(a) \cdot g_2(a)) = \psi(g_1(a)) \cdot \psi(g_2(a))$.

Pro konstantní polynom $g(a) = t \in T$ je $\psi(t) = \psi(g(a)) = \bar\varphi(g)(a') = \varphi(t)$, tedy $\psi|T = \varphi$ (a navíc $\psi(1_{T(a)} = 1_T) = \varphi(1_T) = 1_{T'} = 1_{T'(a')}$.

Zobrazení ψ je tedy T-izomorfismus mezi $T(a)$ a $T'(a')$. $\square$

Příklad 9.16. Předpoklad ireducibility je v předchozí věte nutný. Platí $[T(a):T] = \deg(m_{a,T})$, tedy je-li $f = f_1 \cdot f_2$, kde f_1, f_2 jsou ireducibilní a $\deg(f_1) \neq \deg(f_2)$, a je-li $T(a_1)$ kořenové nadtěleso f_1 nad T a $T(a_2)$ kořenové nadtěleso f_2 nad T, pak $\deg(f_1) = [T(a_1):T] \neq [T(a_2):T] = \deg(f_2)$, tedy $T(a_1) \not\simeq T(a_2)$.

Definice 9.17. Nechť T je komutativní těleso a $f \in T[x]$ polynom stupně alespoň 1. Nadtěleso (rozšíření) $U \supseteq T$ nazveme *rozkladovým nadtělesem* polynomu f nad tělesem T pokud platí

(i) polynom f se v $U[x]$ rozkládá na součin lineárních (kořenových) činitelů,
(ii) kdykoli $T \subseteq V \subsetneq U$, pak se polynom f nerozkládá ve $V[x]$ na lineární činitele (neboli těleso U je nejmenší těleso vlastnosti (i)).

Věta 9.18. *Nechť T je komutativní těleso a $f \in T[x]$ polynom stupně alespoň 1. Potom existuje rozkladové nadtěleso polynomu f nad tělesem T a navíc všechna rozkladová nadtělesa polynomu f nad tělesem T jsou T-izomorfní.*

Důkaz. Indukcí podle $n = \deg(f)$ nejprve dokážeme existenci tělesa splňujícího (i) z 9.17. Pro $n = 1$ tvrzení zřejmě platí (stačí položit $U = T$). Pro $n > 1$ dle 9.14 existuje $K \supseteq T$ takové, že f má v K kořen a_1, neboli $f(x) = (x - a_1)g(x)$ v $K[x]$. Stupeň g je o jedna menší než stupeň f, takže podle indukčního předpokladu existuje nadtěleso $W \supseteq K$, v němž se g rozkládá na lineární (kořenové) činitele. Nechť $a_2, \dots a_n$ jsou kořeny g ve W. Pak $U = T(a_1, \dots, a_n)$ splňuje (i) z 9.17. Nyní stačí ověřit, že toto těleso splňuje také (ii) z 9.17.

Nechť $T \subseteq V \subsetneq U$. Pak jistě existuje i takové, že $a_i \notin V$. Pro spor předpokládejme, že f lze ve $V[x]$ rozložit na kořenové činitele $f = c \cdot (x - a'_1) \dots (x - a'_n) \in V[x]$. Pak ale pro každé $j = 1, \dots, n$ je $a'_j \neq a_i$. Tedy $f(a_i) = c \cdot \prod_{j=1}^{j=n} (a_i - a'_j) \neq 0$, neboť žádný z činitelů není nulový a $V[x]$ je obor integrity. Dostáváme spor s tím, že a_i je kořenem polynomu f, takže těleso U splňuje i podmínku (ii) z 9.17.

$$
\begin{tikzcd}
T \arrow[d, equal] & \subseteq & U' \arrow[d, "\varphi'"] & \subseteq & U \\
T & \subseteq & V' & \subseteq & V
\end{tikzcd}
$$

(Jednozačnost) Nechť $T \subseteq U, V$ jsou rozkladová nadtělesa polynomu f nad tělesem T. Pak $U = T(a_1, \dots, a_n)$ a $V = T(b_1, \dots, b_n)$, kde $a_1, \dots, a_n$ jsou kořeny polynomu f v U a $b_1, \dots, b_n$ kořeny polynomu f ve V. Definujeme množinu

$$\mathcal{M} = \{(U', \varphi') | T \subseteq U' \subseteq U, \varphi' : U' \to V, \varphi' \text{je prostý } T\text{-homomorfismus}\}$$

a částečné uspořádání $\leq_{\mathcal{M}}$ na této množině tak, že $(U', \varphi') \leq_{\mathcal{M}} (U'', \varphi'')$, pokud $U' \subseteq U''$ a $\varphi' = \varphi'' \restriction U'$. Množina $\mathcal{M}$ je neprázdná, neboť $(T, \mathrm{id}_T) \in \mathcal{M}$. Protože v $[U:T] < \infty$ nemůže v $\mathcal{M}$ existovat nekonečný ostře rostoucí řetězec, tedy podle Zornova lemmatu má $\mathcal{M}$ vzhledem k $\leq_{\mathcal{M}}$ maximální prvek (U', φ').

Sporem dokážeme, že $U' = U$ a že φ' je surjektivní, což bude důkazem, že $U \overset{\varphi}{\simeq} V$. Nechť $U' \subsetneq U = T(a_1, \dots, a_n)$ je maximální prvek $\mathcal{M}$ a BÚNO nechť $a_1 \in U \setminus U'$. Nechť $f = g_1 \dots g_k$ je ireducibilní rozklad f v $U'[x]$ ($U'[x]$ je Gaussův obor integrity) a BÚNO nechť $g_1(a_1) = 0$. Označme $V' = \mathrm{Im}\, \varphi'$. Tedy $U' \overset{\varphi'}{\simeq} V'$, takže také $U'[x] \overset{\bar{\varphi}'}{\simeq} V'[x]$, přičemž

$$g_1 = \sum_{i=0}^{m} t_i x^i \mapsto \bar{\varphi}'(g_1) = \sum_{i=0}^{m} \varphi'(t_i) x^i$$

a

$$f \mapsto f$$

(φ' je T-homomorfismus). Máme $f = g_1 \cdot \cdots \cdot g_n$ v $U'[x]$ a $f = \bar{\varphi}'(g_1) \cdot \cdots \cdot \bar{\varphi}'(g_n)$ ve $V'[x]$ (obojí jsou to ireducibilní rozklady). Polynom $\bar{\varphi}'(g_1)$ má ve V kořen (V je rozkladové nadtěleso polynomu f), označme jej $a_1' \in V$. Podle 9.15 je $U'(a_1) \simeq V'(a_1')$, tudíž $(U'(a_1), \bar{\varphi}') \in \mathcal{M}$, což je ve sporu s maximalitou (U', φ').

Zbývá dokázat, že φ' je na. Pokud není, pak $V' = \operatorname{Im} \varphi'$ je nadtělesem T ve V ($T \subseteq V' \subsetneq V$) takovým, že f se ve $V'[x]$ rozkládá na lineární (kořenové) činitele, což je ve sporu s podmínkou (ii) z 9.17 pro rozkladové nadtěleseo V. □

10. Algebraický uzávěr

Definice 10.1. (i) Nechť K je komutativní těleso. Řekneme, že K je *algebraicky uzavřené* těleso , pokud každý polynom $f \in K[x]$ stupně alespoň 1 má v K alespoň jeden kořen (což je tehdy a jen tehdy, když se f rozkládá na lineární činitele v $K[x]$),

(ii) Nechť $T \subseteq K$ jsou komutativní tělesa. Řekneme, že K je *algebraickým uzávěrem* tělesa T, pokud

a) těleso K je algebraicky uzavřené,

b) K je algebraickým rozšířením tělesa T.

Skutečnost, že K je algebraicky uzavřené těleso symbolicky značíme $K = \bar{K}$ a pro algebraický uzávěr používáme značení $\bar{T}$.

Příklad 10.2. (1) Těleso $\mathbb{C}$ všech komplexních čísel je algebraicky uzavřené (toto je přesně tvrzení věty s názvem *základní věta algebry*).

(2) Těleso $\mathbb{C}$ je algebraickým uzávěrem tělesa $\mathbb{R}$, stupeň toho rozšíření je $[\mathbb{C} : \mathbb{R}] = 2$.

(3) Uzávěrem tělesa $\mathbb{Q}$ všech raiconálních čísel je mezitěleso $\mathbb{Q} \subsetneq \bar{\mathbb{Q}} \subsetneq \mathbb{C}$, kterému se říká *těleso algebraických čísel* a my ho zatím nebudeme blíže specifikovat, jen doplníme, že stupeň rozšíření je v tomto případě nekonečný $[\bar{\mathbb{Q}} : \mathbb{Q}] = \infty$.

(4) Nechť T je konečné těleso (uvidíte později, že každé konečné těleso je komutativní), pak jeho algebraický uzávěr je nekonečné těleso (plyne to z 10.3). Stupeň rozšíření tedy nutně je $[\bar{T} : T] = \infty$.

Lemma 10.3. *Nechť T je komutativní algebraicky uzavřené těleso, pak T není konečné.*

Důkaz. Předpokládejme pro spor, že $T = \{t_1, \dots, t_n\}$. Uvažme polynom $f = (x - t_1)(x - t_2) \cdot \cdot \cdot (x - t_n) + 1 \in T[x]$. Tento polynom nemá v T kořen, což je spor s předpokladem, že T je algebraicky uzavřené. Těleso T tedy nemůže být konečné. □

Věta 10.4. *Nechť T je komutativní těleso. Potom existuje nadtěleso $K \supseteq T$ takové, že každý polynom $f \in T[x]$ stupně alespoň 1 má v K alespoň jeden kořen a navíc platí $card(K) \leq \max(\aleph_0, card(T))$.*

Důkaz. □

Lemma 10.5. *Nechť $T \subseteq K$ jsou komutativní tělesa a nechť K je algebraicky uzavřené. Označme $T \subseteq T' = \{a \in K \mid a \text{ je algebraické nad} T\} \subseteq K$. Potom T' je algebraický uzávěr tělesa T ($T' = \bar{T}$).*

Důkaz. Nejdříve dokážeme, že T' je podtělesem K obsahující těleso T. Inkluze $T' \subseteq K$ plyne přímo z definice T'. Jistě libovolný prvek $t \in T$ je algebraický nad T, takže platí i inkluze $T \subseteq T'$. Mějme libovolná $a, b \in T'$. Pak $a, b \in T(a, b) \subseteq K$ a $[T(a, b) : T] < \infty$. Z posledního plyne (9.7), že všechny prvky tělesa $T(a,b)$ jsou algebraické, čili $T(a,b) \subseteq T'$ a speciálně $a+b, a \cdot b \in T'$.

Nyní dokážeme, že každý polynom $f \in T'[x]$ stupně alespoň 1 má v T' alespoň jeden kořen. Mějme polynom $f = \sum_{n=0}^{m} t_n x^n$, $t_0, \dots, t_m \in T'$ stupně alespoň 1. Těleso K je algebraicky uzavřené, takže polynom f má v K alespoň jeden kořen $a \in K$, ukážeme, že a je algebraické nad T, čili $a \in T'$. Máme následující tři komutativní tělesa

$$T \subseteq T(t_0, \dots, t_n) \subseteq T(t_0, \dots, t_n, a).$$

Stupeň rozšíření $[T(t_0, \dots, t_n) : T]$ je konečný podle 9.8. Stupeň rozšíření $[T(t_0, \dots, t_n, a) : T(t_0, \dots, t_n)] = \deg(m_{a, T(t_0, \dots, t_n)})$ je nutně také konečný. Z 9.9 máme, že i stupeň rozšíření $[T(t_0, \dots, t_n, a) : T]$ je konečný. Takže všechny prvky tělesa $T(t_0, \dots, t_n, a)$ jsou algebraické nad T, speciálně tedy i prvek a.

□

Věta 10.6. *Nechť T je komutativní těleso. Pak existuje nadtěleso $K \supseteq T$, které je algebraickým uzávěrem tělesa T ($K = \bar{T}$). Toto těleso je určeno jednoznačně až na T-izomorfismus. Navíc $card(K) = \max(\aleph_0, card(T))$ (pokud T je konečné těleso, pak $card(\bar{T}) = \aleph_0$, jinak $card(\bar{T}) = card(T)$).*

Důkaz. Označme $K_0 = T$, K_1 nadtěleso T (existuje dle 10.4), ve kterém má každý polynom z $K_0[x]$ stupně alespoň 1 kořen, K_2 natěleso K_1, ve kterém má každý polynom z $K_1[x]$ stupně alespoň 1 kořen atd. Pak $K = \bigcup_{0<i<\aleph_0} K_i \supseteq T$ je těleso. Každý polynom z $K[x]$ stupně alespoň 1 má koeficienty v některém K_i a tedy má kořen v K_{i+1}, $K \supseteq T$ je tedy algebraicky uzavřené těleso. Nyní si stačí uvědomit, že $K = \{a \in K \mid a \text{ je algebraické nad } T\} \subseteq K$ a použít 10.5. Máme tedy, že K je algebraickým uzávěrem tělesa T. Tvrzení o mohutnosti plyne z 10.4.

$$\begin{tikzcd}
T \arrow[r, phantom, "\subseteq"] \arrow[d, equal] & T' \arrow[r, phantom, "\subseteq"] \arrow[d, "\varphi'"] & K \\
T \arrow[r, phantom, "\subseteq"] & \operatorname{Ker} \varphi' \arrow[r, phantom, "\subseteq"] & K'
\end{tikzcd}$$

(Jednoznačnost) Mějme K, K' dva algebraické uzávěry tělesa T. Uvažme částečně uspořádanou množinu $\mathcal{M} = ((T', \varphi'), \leq_M)$, kde $T \subseteq T' \subseteq K$, $\varphi' : T' \to K'$ je prostý T-homomorfismus a $(T', \varphi') \leq_M (T'', \varphi'')$, pokud $T' \subseteq T''$ a $\varphi'' | T' = \varphi'$. Tato množina není prázdná, protože obsahuje prvek (T, id_T). Pokud

$$\dots \leq_M (U_\alpha, \varphi_\alpha) \leq_M \dots \leq_M (U_\beta, \varphi_\beta) \leq_M \dots$$

je řetězec v $\mathcal{M}$, pak $(\bigcup_\alpha U_\alpha, \bigcup_\alpha \varphi_\alpha) \in M$, můžeme tedy použít Zornovo lemma. Plyne z něj existence $\leq_M$-maximálního prvku (T', φ'). Předpokládejme pro spor, že $T' \neq K$. Pak existuje prvek $k \in K \setminus T'$ algebraický nad T a tedy i nad T'. Označme $f = m_{k,T'}$ minimální polynom prvku k nad tělesem T'. Definujme $\bar{\varphi}' : T'[x] \to \varphi'(T')[x]$. Pak $f \mapsto \bar{\varphi}'(f)$ a jelikož f je ireducibilní polynom nad T', je také polynom $\bar{\varphi}'(f)$ ireducibilní nad $\varphi'(T')$. Pro kořen k polynomu f můžeme homomorfismus φ' rozšířit na $T'(k) \subseteq K$, za obraz k vezmeme kořen polynomu $\bar{\varphi}'(f)$, který označíme k'. Máme tedy T-izomorfismus $\varphi : T'(k) \to \varphi(T')(k')$ (stejně jako v důkazu věty 9.15), což je spor s maximalitou (T', φ'), a tedy $T' = K$.

Víme, že $T \subseteq \varphi'(K) \subseteq K'$ a $\varphi'(K)$ je algebraicky uzavřené rozšíření T (protože $\varphi'(K) \simeq K$). Je-li $k' \in K'$, pak existuje $f \in T[x]\colon f(k') = 0$, ale f se v $\varphi'(K)$ rozkládá na kořenové činitele a tedy $k' \in \varphi'(K)$, takže $\varphi'(K) = K'$. □

11. Struktura konečných těles

Věta 11.1 (Weddenburn). *Každé konečné těleso je komutativní.*

Věta 11.2 (struktura konečných těles). (i) *Nechť a je přirozené číslo. Potom existuje konečné těleso řádu a, právě tehdy, když $a = p^n$, kde p je prvočíslo a $n \geq 1$. Je-li $a = p^n$, pak existuje (až na izomorfismus) právě jedno konečné těleso řádu a, značí se $GF(p^n)$ (Galois field) a má následující vlastnosti:*
- *jeho charakteristika je p*
- *jeho aditivní grupa je izomorfní $\mathbb{Z}_p^n$*
- *jeho multiplikativní grupa je cyklická*
- *je rozkladovým nadtělesem polynomu $x^a - x \in \mathbb{Z}_p[x]$*

(ii) *Nechť $T = GF(p^n)$. Pak existuje ireducibilní polynom $f \in \mathbb{Z}_p[x]$ stupně n, že $T \simeq \mathbb{Z}_p[x]/f\mathbb{Z}_p[x]$. Naopak pro každý ireducibilní polynom $g \in \mathbb{Z}_p[x]$ stupně n je $\mathbb{Z}_p[x]/g\mathbb{Z}_p[x]$ konečným tělesem izomorfním $GF(p^n)$.*

Důkaz. (Část (i)) Nechť T je konečné komutativní těleso řádu a. Potom $\operatorname{char}(T)$ je prvočíslo p (toto tvrzení je hezkým cvičením). Označme P prvotěleso tělesa T:

$$P = \{1, 1+1, 1+1+1, \dots, \underbrace{1+1+\dots+1}_{p\text{-krát}} = 0\} \simeq \mathbb{Z}_p.$$

Označme $n = \dim_{\mathbb{P}}(T) = [T : P]$. Pak T má právě p^n prvků, a tedy $a = p^n$. T je navíc n-dimenzionální vektorový prostor nad P, tedy aditivní grupa $(T, +, -, 0) \simeq P^n \simeq \mathbb{Z}_p^n$ (to byste si měli pamatovat z lineární algebry).

Zaměřme se nyní na multiplikativní grupu $\mathcal{G} = (G = T \setminus \{0\}, \cdot, ^{-1}, 1)$ Řád této grupy je $|G| = a-1 = p^n-1 = p_1^{n_1} p_2^{n_2} \dots p_k^{n_k}$. Podle Frobeniovy-Stickelbergerovy věty **??** se $\mathcal{G}$ rozkládá na součin p_i-primárních komponent: $G = G_1 \times \dots \times G_k$, takových, že $|G_i| = p_i^{m_i}$. Ukážeme, že každá $\mathcal{G}_i$ je cyklická grupa řádu $p_i^{m_i}$ (což bude důkaz toho, že i $\mathcal{G}$ je cyklická). Pro spor předpokládejme, že grupa $\mathcal{G}_j$ není cyklická. Pro každé $g \in G_j$ platí, že $\mathrm{o}(g) < p_j^{m_j}$. Označme $p_i^{l_i} = \max\{\mathrm{o}(g) \mid g \in G_i\}$ a definujme $b = p_1^{l_1} \dots p_k^{l_k}$, b tedy dělí a, ale není s ním asociováno (speciálně $a \geq b+2$). Uvažme polynom $F = x^b - 1 \in P[x]$. Podle předpokladu je každý prvek grupy $\mathcal{G}$ kořenem polynomu $F(x) \in P[x]$. Grupa $\mathcal{G}$ má ale $a-1$ prvků a stupeň polynomu f je jen $b < a-1$, což je spor s předpokladem, že grupa $\mathcal{G}_j$ není cyklická.

Nyní dokážeme, že T je rozkladovým nadtělesem polynomu $f = x^a - x \in \mathbb{Z}_p[x]$. Protože $P \simeq \mathbb{Z}_p$ můžeme BÚNO předpokládat, že $\mathbb{Z}_p \subseteq T$. Máme $D(f) = -1$, polynomy f a $D(f)$ tedy nemají žádné společné kořeny, z toho plyne, že f má pouze jednoduché kořeny v libovolném nadtělese $T \supseteq \mathbb{Z}_p$. Na druhé straně každé $g \in T \setminus \{0\}$ je kořenem f v T ($g^a = g$ a tedy $f(g) = 0$). Prvek $0 \in T$ je zřejmě také kořenem polynomu f.

Polynom f má stupeň a a má v T a různých kořenů, tedy těleso T je rozkladovým nadtělesem polynomu f nad $\mathbb{Z}_p$:

$$f = (x - t_1)(x - t_2) \dots (x - t_p^n) \qquad \{t_1, \dots, t_{p^n}\} = T$$

Jednoznačnost plyne z jednoznačnosti rozkladového nadtělesa.

(Část (ii)) Mějme těleso T, takové, že $|T| = p^n$. Víme, že jeho multiplikativní grupa $G = T \setminus \{0\}$ je cyklická. Nechť $t \in G$ je její generátor. Potom nutně $\mathbb{Z}_p(t) = T$, tedy T vznikne adjunkcí prvku t k prvotělesu $\mathbb{Z}_p$, tudíž $[T : \mathbb{Z}_p] = n = \deg(m_{t,\mathbb{Z}_p})$, kde $m_{t,\mathbb{Z}_p}$ je minimální polynom prvku t nad prvotělesem $\mathbb{Z}_p$. Navíc zobrazení $\psi \colon \mathbb{Z}_p[x] \to \mathbb{Z}_p(t)$ přiřazující $g \mapsto g(t)$, je surjektivní okruhový homomorfismus (9.4) a Ker $\psi = m_{t,\mathbb{Z}_p} \cdot \mathbb{Z}_p[x]$. Tedy $T = \mathbb{Z}_p(t) \simeq \mathbb{Z}_p[x]/\mathrm{Ker}\ \psi = \mathbb{Z}_p[x]/m_{t,\mathbb{Z}_p} \cdot \mathbb{Z}_p[x]$. Zbytek tvrzení je snadným cvičením. $\square$

12. Svazy

Definice 12.1. Částečně uspořádaná množina $(L, \leq)$ (tj. binární operace $\leq$ je tranzitivní, reflexivní a antisymetrická) se nazývá *svazově uspořádanou*, pokud pro každé dva prvky $x, y \in L$ existuje $\inf(x, y) \in L$ (největší dolní závora, tj. prvek $i \in L\colon (i \leq x, y \wedge (i' \leq x, y \Rightarrow i' \leq i)))$ a $\sup(x, y) \in L$ (nejmenší horní závora, tj. prvek $s \in L\colon (s \geq x, y \wedge (s' \geq x, y \Rightarrow s' \geq s)))$. Navíc $(L, \leq)$ se nazývá *úplně svazově uspořádaná*, pokud pro každou podmnožinu $X \subseteq L$ existuje $\inf(X) \in L$ a $\sup(X) \in L$.

Definice 12.2. Trojice $\mathcal{L} = (L, \wedge, \vee)$, kde L je množina a $\wedge$ a $\vee$ jsou binární operace na L se nazývá *svazem*, pokud pro každé dva prvky $x, y \in L$ platí

(i) $x \wedge x = x = x \vee x$ (reflexivita),
(ii) $x \wedge y = y \wedge x$, $x \vee y = y \vee x$ (komutativita),
(iii) $x \wedge (y \wedge z) = (x \wedge y) \wedge z$, $x \vee (y \vee z) = (x \vee y) \vee z$ (asociativita),
(iv) $x \wedge (y \vee x) = x = x \vee (y \wedge x)$ (absorbce).

Je-li $\mathcal{L} = (L, \wedge, \vee)$ svaz, je $\mathcal{L}^\star = (L, \vee, \wedge)$ (tedy například operace $\vee$ v $\mathcal{L}*$ je definována jako $a \vee b = a \wedge b$, kde $\wedge$ je původní operace z $\mathcal{L}$) také svaz, tzv. *svaz duální* ke svazu $\mathcal{L}$.

Lemma 12.3. *Zobrazení*

$$\varphi : (L, \leq) \to (L, \wedge, \vee),$$

kde $a \wedge b$ *je definováno jako* $\inf(a, b)$ *a* $a \vee b$ *je definováno jako* $\sup(a, b)$ *a zobrazení*

$$\psi : (L, \wedge, \vee) \to (L, \leq),$$

kde definujeme $x \leq y$*, pokud* $x \wedge y = x$ *(nebo ekvivalentně:* $(x \vee y) = y$*) jsou navzájem inverzní bijekce třídy všech svazově uspořádaných množin a třídy všech svazů. Proto mezi svazově uspořádanou množinou a svazem nerozlišujeme.*

Důkaz. Ověřit, že zobrazení φ a ψ jsou korektně definována je velice užitečné cvičení, a proto ho přenecháme čtenáři. Ukážeme, že $\psi \circ \varphi = \mathrm{id}$. Uvažme svazově uspořádanou množinu $(L, \leq)$, zobrazíme jí zobrazením φ a dostaneme svaz $(L, \wedge, \vee)$, ten zobrazíme zobrazením ψ a dostaneme svazově uspořádanou množinu $(L, \leq')$. Musíme ukázat, že pro každé $x, y \in L$ platí $x \leq' y \Leftrightarrow x \leq y$. Máme, že $x \leq' y$ právě, když $x \wedge y = x$, což je právě tehdy, když $\inf(x, y) = x$, což je právě tehdy, když $x \leq y$.

Ukážeme, že i $\varphi \circ \psi = \mathrm{id}$. Uvažme svaz $(L, \wedge, \vee)$, ten zobrazíme zobrazením ψ a dostaneme svazově uspořádanou množinu $(L, \leq)$, tu zobrazíme zobrazením φ a dostaneme svaz $(L, \wedge', \vee')$. Musíme ukázat, že pro každé $x, y \in L$ platí $x \wedge' y = x \wedge y$ a $x \vee' y = x \vee y$. Ukážeme jen první rovnost, druhou přenecháme čtenáři jako cvičení. Máme, že $x \wedge' y = \inf(x, y)$, ukážeme, že $\inf(x, y) = x \wedge y$. Jistě $\inf(x, y) \geq x \wedge y$. Dále, protože $\inf(x, y) \leq x$ a zároveň $\inf(x, y) \leq y$ máme, že $\inf(x, y) \wedge (x \wedge y) = (\inf(x, y) \wedge x) \wedge y = \inf(x, y) \wedge y = \inf(x, y)$, tedy $\inf(x, y) \leq x \wedge y$, tedy $\inf(x, y) = x \wedge y$. Dokázali jsme, že φ i ψ jsou bijekce a jsou navzájem inverzní. $\square$

Příklad 12.4. (1) Je-li M množina, pak částečně uspořádaná množina $\mathcal{P} = (P(M), \subseteq)$ všech podmnožin množiny M je úplně svazově uspořádaná množina. Dále platí, že $\inf(x, y) = x \cap y$ a $\sup(x, y) = x \cup y$. Tedy $\mathcal{P} = (P(M), \cap, \cup)$ je úplný svaz (svaz nazýváme *úplným*, pokud je jeho odpovídající svazově uspořádaná množina úplně svazově uspořádaná).

(2) Je-li $M \in$ Mod-$\mathcal{R}$ modul (nad libovolným okruhem), pak částečně uspořádaná množina $\mathcal{L} = (\mathcal{L}(M), \subseteq)$ všech podmodulů modulu $\mathcal{M}$ je úplně svazově uspořádaná množina. Dále platí, že $\inf(x, y) = x \cap y$ a $\sup(x, y) = x + y$ (podmodul generovaný podmoduly x a y). Tedy $\mathcal{L} = (\mathcal{L}(M), \cap, +)$ je úplný svaz.

(3) Je-li $\mathcal{G}$ grupa (ne nutně komutativní), pak částečně uspořádaná množina $\mathcal{L} = (\mathcal{L}(G), \subseteq)$ všech podgrup grupy $\mathcal{G}$ je úplně svazově uspořádaná množina. Dále platí, že $\inf(x, y) = x \cap y$ a $\sup(x, y) = x + y$ (podgrupa generovaná podgrupami x a y). Tedy $\mathcal{L} = (\mathcal{L}(G), \cap, +)$ je úplný svaz.

(4) Nechť částečne uspořádaná množina $\mathcal{S} = (\{x_1, x_2, \dots\}, \leq)$ je nekonečný ostře rostoucí řetězec (tedy platí $x_1 \lneq x_2 \lneq x_3 \lneq \cdots \lneq x_n \lneq x_{n+1} \lneq \dots$). Pak $\mathcal{S}$ je svazově uspořádaná množina, ale $\mathcal{S}$ není úplně svazově uspořádaná množina, protože $\sup(\{x_1, x_2, \dots\})$ neexistuje.

Definice 12.5. Nechť $\mathcal{L}, \mathcal{L}'$ jsou svazy. Zobrazení $\varphi : L \to L'$ je *svazový homomorfismus*, pokud pro každé $x, y \in L$ platí, že $\varphi(x \wedge y) = \varphi(x) \wedge' \varphi(y)$ a $\varphi(x \vee y) = \varphi(x) \vee' \varphi(y)$. Je-li φ prosté zobrazení, řekneme, že φ je *svazový monomorfismus*, je-li φ zobrazení na, řekneme, že φ je *svazový epimorfismus* a je-li φ zobrazení bijektivní, řekneme, že φ je *svazový izomorfismus*.

Příklad 12.6. Je-li M množina, pak již víme, že $\mathcal{P} = (P(M), \cap, \cup)$ je svaz. Zobrazení

$$\begin{array}{rcl} \varphi\colon \mathcal{P} & \to & \mathcal{P}^\star \\ N & \mapsto & M \setminus N \end{array}$$

je svazový izomorfismus svazu $\mathcal{P}$ a duálního svaz $\mathcal{P}^\star$ a dále platí, že $\varphi \circ \varphi = \mathrm{id}_M$.

Definice 12.7. Nechť $\mathcal{L}$ je svaz a nechť $L' \subseteq L$. Řekneme, že podmnožina L' spolu s restrikcemi operací z L na L' je *podsvaz* svazu $\mathcal{L}$, pokud je L' uzavřená na operace $\wedge$ a $\vee$, tedy pokud pro každé $x, y \in L'$ platí, že $x \wedge y \in L'$ a $x \vee y \in L'$.

Příklad 12.8. Nechť $\mathcal{L}$ je svaz a nechť $x, y \in L$ jsou takové, že $x \leq y$. Pak množina $[x, y] = \{z \in L | x \leq z \leq y\}$ (spolu s operacemi z $\mathcal{L}$) je podsvaz svazu $\mathcal{L}$. Tento speciální tvar podsvazu se nazývá *interval* ve svazu $\mathcal{L}$ určený prvky x a y.

Definice 12.9. Nechť $\mathcal{L}$ je svaz. Řekneme, že svaz $\mathcal{L}$ je *modulární*, pokud pro každé dva prvky $x, y \in L$ platí, že je-li $z \in L$, $z \leq x$, pak $x \wedge (y \vee z) = (x \wedge y) \vee z$ (této implikaci se často říká *slabá distributivita*).

Poznámka 12.10. Svaz $\mathcal{L}$ je modulární právě tehdy, když je duální svaz $\mathcal{L}^\star$ modulární.

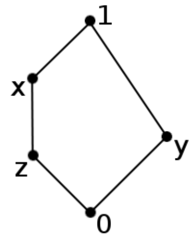
Příklad 12.11. (1) Všechny svazy z 12.4, kromě svazu všech podgrup, jsou vždy modulární, v případech (1) a (4) jsou operace dokonce distributivní ($x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$). V případech (2) a (3) vždy platí, že $x \wedge (y \vee z) \geq (x \wedge y) \vee z$: pro $Z \subseteq X$ máme $X \cap (Y + Z) \subseteq (X \cap Y) + Z$, neboť pokud $x \in X$ a $x \in Y + Z$, tedy $x = y + z$, pak jistě $y \in X$. Takže $x = y + z \in (X \cap Y) + Z$.

(2) Svaz $\mathcal{N}_5$ (viz. obrázek 1, tomuto svazu se říká *pentagon*) není modulární. Např. $x \wedge (y \vee z) = x \neq z = (x \wedge y) \vee z$.

Věta 12.12. *Svaz $\mathcal{L}$ je modulární, právě tehdy, když neobsahuje podsvaz izomorfní se svazem $\mathcal{N}_5$.*

Důkaz. Když $\mathcal{L}$ obsahuje podsvaz izomofní se svazem $\mathcal{N}_5$, pak svaz $\mathcal{L}$ není modulární podle 12.11 části (2). Opačnou implikaci dokážeme nepřímo. Nechť svaz $\mathcal{L}$ není modulární. Pak

OBRÁZEK 1. Svaz $\mathcal{N}_5$



existují prvky x, y, z takové, že $z \leq x$ a $x \wedge (y \vee z) \gneq (x \wedge y) \vee z$ (podívejte se na 12.11 část (1)). Nyní najdeme podsvaz $\mathcal{L}$ izomorfní se svazem $\mathcal{N}_5$. Definujme $a = x \wedge (y \vee z)$, $b = y$ a $c = (x \wedge y) \vee z$. Pak $a \vee b = (x \wedge (y \vee z)) \vee y \leq (y \vee z) \vee y = z \vee y$ a zároveň $a \vee b = (x \wedge (y \vee z)) \vee y \geq (z \wedge (y \vee z)) \vee y \overset{absorbce}{=} z \vee y$, takže

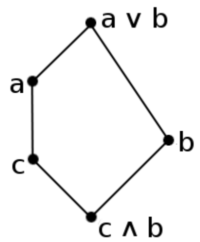
$$a \vee b = z \vee y.$$

Dále $c \wedge b = ((x \wedge y) \vee z) \wedge y \leq ((x \wedge y) \vee x) \wedge y = x \wedge y$ a zároveň $c \wedge b = ((x \wedge y) \vee z) \wedge y \geq ((x \wedge y) \vee z) \wedge (x \wedge y) \overset{absorbce}{=} x \wedge y$, takže

$$c \wedge b = x \wedge y.$$

Dále ještě $c \vee b = (x \wedge (y \vee z) \vee y = z \vee y$ a $a \wedge b = x \wedge (y \vee z) \wedge y = x \wedge y$.

Nyní stačí ukázat, že $b \not\leq c$,$c \not\leq b$, $b \not\leq a$ a $a \not\leq b$. Kdyby $b \leq c$, neboli $b \wedge c = b$, pak by podle již dokázaných vztahů platilo $x \wedge y = y$, tedy $y \leq x$. Dále z předpokladů máme $z \leq x$. Pak ovšem $x \wedge (y \vee z) = y \vee z = (x \wedge y) \vee z$, což je ve sporu s volbou x, y a z. Platnost dalších vztahů dokážeme analogicky. Našli jsme tedy podsvaz $\mathcal{L}$ izomorfní se svazem $\mathcal{N}_5$. $\square$



OBRÁZEK 2. Uspořádání a, b, c

Definice 12.13. Nechť $\mathcal{L}$ je svaz. Řekneme, že svaz $\mathcal{L}$ je *distributivní*, pokud pro každé $x, y, z \in L$ platí $x \wedge (y \vee z) = (x \vee y) \wedge (x \wedge z)$. Dále řekneme, že svaz $\mathcal{L}$ je *komplementární*, pokud existují prvky $0, 1 \in L$ takové, že pro každé $x \in L$ je $0 \leq x \leq 1$ a existuje $x' \in L$ takové, že $x \wedge x' = 0$ a $x \vee x' = 1$. Svaz, který je distributivní a zároveň komplementární se nazývá *booleovský* svaz.

Poznámka 12.14. Zřejmě každý distributivní svaz je modulární.

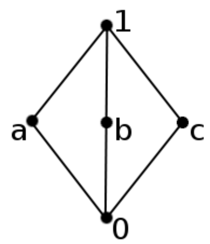
Příklad 12.15. (1) Svaz $\mathcal{P}(M) = (P(M), \cap, \cup)$ je booleovský svaz. Máme $0 = \emptyset$, $1 = M$ a $X' = M \setminus X$. Tento booleovský svaz je krásným příkladem, neboť platí, že každý konečný booleovský svaz je izomorfní svazu $\mathcal{P}(M)$ pro nějakou množinu M.

(2) Nekonečný ostře rostoucí řetězec $\mathcal{S} = (\{x_1, x_2, \dots\}, \leq)$ je zřejmě distributivní svaz, ale pokud obsahuje alespoň tři prvky, pak tento svaz není komplementární.

(3) Svaz $\mathcal{M}_5$ (viz. obrázek 3, tomuto svazu se říká *diamant*) je komplementární, ale není disributivní $(a \wedge (b \vee c = a \neq 0 = (a \wedge b) \vee (a \wedge c))$ a podle 12.12 je modulární.

(4) Svaz $\mathcal{N}_5$ není distributivní ani komplementární ani modulární.

Obrázek 3. Svaz $\mathcal{M}_5$



Věta 12.16. *Svaz $\mathcal{L}$ je distributivní právě tehdy, když svaz $\mathcal{L}^\star$ je distributivní, tj. pro každé $x, y, z \in L^\star$ platí $x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)$.*

Důkaz. Je-li svaz $\mathcal{L}$ distributivní, pak

$$(x \vee y) \wedge (x \vee z) \overset{distr.}{=} ((x \vee y) \wedge x) \vee ((x \vee y) \wedge z) \overset{absorbce}{=} x \vee ((x \vee y) \wedge z) \overset{distr.}{=}$$

$$= x \vee (x(x \wedge z) \vee (y \wedge z)) \overset{absorbce}{=} x \vee (y \wedge z).$$

Dokázali jsme, že je-li svaz $\mathcal{L}$ distributivní, je i svaz $\mathcal{L}^\star$ distibutivní. Naopak, jestliže je svaz $\mathcal{L}^\star$ distributivní, je distributivní i svaz $\mathcal{L}^{\star\star}$. Jelikož ale $\mathcal{L}^{\star\star} = \mathcal{L}$, dokázali jsme také opačnou implikaci. $\square$

Poznámka 12.17. Svaz $\mathcal{L}$ je distributivní právě tehdy, když neobsahuje podsvaz izomorfní svazu $\mathcal{N}_5$ nebo svazu $\mathcal{M}_5$.

Rejstřík