3.B Okruhy polynomů

V této podkapitole odvodíme některé vlastnosti okruhů polynomů v jedné proměnné nad komutativním tělesem. Znalosti, které zde získáme, budeme používat v další kapitole o komutativních tělesech.

Připomeňme si nejdříve definici tělesa. Komutativní okruh T je *těleso*, pokud pro každé $0 \neq t \in T$ existuje prvek $s \in T$ tak, že $ts = 1$. Značíme $s = t^{-1}$ a mluvíme o inverzním prvku k t. Těleso můžeme také definovat jako komutativní okruh T, ve kterém je *množina nenulových prvků* $T^* = T \setminus \{0\}$ uzavřená na násobení a $T^*(\cdot)$ je grupa. Zdůrazněme, že všechna *tělesa v této přednášce budou komutativní*. Abychom se dále vyhnuli triviálním případům, budeme vždy předpokládat, že v tělese T je $0 \neq 1$. Dosud jsme mluvili o těchto příkladech těles: $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ a $\mathbb{Z}_p$ pro prvočíslo p.

Definice. Ať je T komutativní těleso a $x \notin T$ nový symbol. Součet $p = \Sigma_{i \in \mathbb{N} \cup \{0\}}\ t_i x^i$, kde $x^0 = 1 \in T$ a t_i jsou prvky T až na konečně mnoho indexů $i \in \mathbb{N} \cup \{0\}$ rovné nule, se nazývá *polynom v proměnné x nad tělesem T*. Prvky t_i se nazývají *koeficienty polynomu p*. Největší $n \in \mathbb{N} \cup \{0\}$ takové, že $t_n \neq 0$, se nazývá *stupeň polynomu p*, značíme jej st p, koeficient t_n se pak nazývá *vedoucí koeficient p*. Pro nulový polynom $0 \in T$ definujeme st $0 = -\infty$. Číslo $t_0 = t_0 x^0$ se nazývá *absolutní člen p*.

Je-li $n \in \mathbb{N} \cup \{0\}$ číslo větší nebo rovné stupni polynomu $p = \Sigma_{i \in \mathbb{N} \cup \{0\}}\ t_i x^i$, stačí psát pouze $p = \Sigma_{i=0,\ldots,n}\ t_i x^i = t_0 + t_1 x + t_2 x^2 + \ldots + t_n x^n$. Většinou budeme používat tento zápis.

Polynomy stupně nejvýše nula jsou totožné s prvky T. Polynomy stupně nula jsou právě prvky T^*.

Sčítání a násobení polynomů. Označme $T[x]$ množinu všech polynomů v proměnné x nad tělesem T. Pro $p, q \in T[x]$, $p = \Sigma_{i \in \mathbb{N} \cup \{0\}}\ t_i x^i$, $q = \Sigma_{i \in \mathbb{N} \cup \{0\}}\ s_i x^i$ definujeme součet

$$p + q = \Sigma_{i \in \mathbb{N} \cup \{0\}}\ (t_i + s_i) x^i$$

a součin

$$p \cdot q = \Sigma_{k \in \mathbb{N} \cup \{0\}}\ (\Sigma_{i,j \in \mathbb{N} \cup \{0\},\ i+j=k}\ t_i s_j) x^k.$$

Snadno se ověří, že výsledky jsou opět polynomy. Pro $p \cdot q$ je koeficient u x^k roven 0 kdykoli je $k >$ st $p +$ st q. Definovali jsme dvě operace na množině $T[x]$. Ukážeme, že $T[x]$ je s těmito operacemi komutativní okruh.

Lemma 3.7 *$T[x]$ je vektorový prostor nekonečné dimenze nad tělesem T.*

Důkaz. Stačí si uvědomit, že polynom $p = \Sigma_{i \in \mathbb{N} \cup \{0\}}\ t_i x^i$ si můžeme představit jako posloupnost koeficientů $(t_0, t_1, \ldots)$. Sčítání polynomů je sčítání těchto posloupností po složkách. Násobení skalárem plyne z definice násobení polynomů: $t \cdot p = (tx^0) \cdot p = \Sigma_{i \in \mathbb{N} \cup \{0\}}\ (tt_i) x^i$. Tedy $t \cdot (t_0, t_1, \ldots) = (tt_0, tt_1, \ldots)$ (posloupnost vynásobíme skalárem

tak, že ji vynásobíme v každé složce). $T[x]$ je tedy vektorový prostor až na konečně mnoho míst nulových posloupností prvků T. Tento prostor má nekonečnou bázi tvořenou mocninami x, $B = \{x^i \ ; \ i \in \mathbb{N} \cup \{0\}\}$. □

Z předchozího lemmatu (a z vlastností vektorového prostoru) plyne, že $T[x](+)$ je komutativní grupa. Zbývající vlastnosti okruhu dokážeme v následujícím lemmatu:

Lemma 3.8 *Násobení polynomů je komutativní, asociativní, má neutrální prvek a je distributivní vzhledem ke sčítání polynomů.*

Důkaz. Mějme polynomy $p = \Sigma_{i \in \mathbb{N} \cup \{0\}} \ t_i x^i$, $q = \Sigma_{i \in \mathbb{N} \cup \{0\}} \ s_i x^i$ a $h = \Sigma_{i \in \mathbb{N} \cup \{0\}} \ v_i x^i$. V předchozím důkazu jsme násobili skalárem $t \cdot p = \Sigma_{i \in \mathbb{N} \cup \{0\}} \ (tt_i) x^i = p \cdot t$, tedy $1 \in T$ je neutrální prvek $T[x]$. Dále je

$$(p \cdot q) \cdot h = (\Sigma_{k \in \mathbb{N} \cup \{0\}} \ (\Sigma_{i,j \in \mathbb{N} \cup \{0\}, \ i+j=k} \ t_i s_j) x^k) \cdot h =$$

$$\Sigma_{l \in \mathbb{N} \cup \{0\}} \ (\Sigma_{i,j,m \in \mathbb{N} \cup \{0\}, \ i+j+m=l} \ t_i s_j v_m) x^l.$$

Výsledný polynom nezávisí na pořadí ani na uzávorkování součinu, proto je násobení polynomů komutativní i asociativní. Na závěr spočítejme

$$h \cdot (p+q) = h \cdot (\Sigma_{j \in \mathbb{N} \cup \{0\}} \ (t_j + s_j) x^j) = \Sigma_{k \in \mathbb{N} \cup \{0\}} \ (\Sigma_{i,j \in \mathbb{N} \cup \{0\}, \ i+j=k} \ v_i (t_j + s_j)) x^k =$$

$$= (\Sigma_{k \in \mathbb{N} \cup \{0\}} \ (\Sigma_{i,j \in \mathbb{N} \cup \{0\}, \ i+j=k} \ v_i t_j) x^k) + (\Sigma_{k \in \mathbb{N} \cup \{0\}} \ (\Sigma_{i,j \in \mathbb{N} \cup \{0\}, \ i+j=k} \ v_i s_j) x^k) = h \cdot p + h \cdot q.$$

□

Okruh $T[x]$ se nazývá *okruh polynomů v jedné proměnné nad* T. Operaci násobení budeme obvykle vynechávat a místo $p \cdot q$ psát pouze pq.

Úkol. Dokažte, že $\text{st}\ (p+q) \leq \ \max(\text{st}\ p, \text{st}\ q)$. Je-li $\text{st}\ p \neq \text{st}\ q$, pak $\text{st}\ (p+q) = \max(\text{st}\ p, \text{st}\ q)$. Dokažte, že $\text{st}\ (p \cdot q) = \ \text{st}\ p + \text{st}\ q$.

Na $T[x]$ můžeme stejným způsobem jako v $\mathbb{N}$ zavést relaci dělitelnosti. Řekneme, že $p \in T[x]$ *dělí* $q \in T[x]$, pokud existuje $h \in T[x]$ tak, že $q = hp$. Značíme $p|q$. Nejmenší v dělitelnosti polynomů jsou prvky T^*. Nejedná se tedy o uspořádání, ale je to uspořádání až na takzvanou asociovanost. Polynomy $p, q \in T[x]$ se nazývají *asociované*, pokud $p|q$ a zároveň $q|p$. Tento vztah budeme značit $p||q$. Z vlastností stupňů snadno zjistíme, že pro $p||q$ platí $\text{st}\ p = \ \text{st}\ q$ a tedy nutně $p = tq$ pro vhodné $t \in T^*$. Polynomy jsou tudíž asociované *právě když* jeden je nenulový skalární násobek druhého.

Pro dělitelnost polynomů platí řada vlastností analogických dělitelnosti v $\mathbb{N}$. Je to především dělení polynomů se zbytkem, existence největších společných dělitelů a jednoznačné rozklady na součin "prvočísel". Jednoznačnost rozkladů je zde myšlena až na asociovanost.

Lemma 3.9 (dělení polynomů se zbytkem) *Pro* $p, q \in T[x]$, $p \neq 0$, *existují jednoznačně určené polynomy* $h, r \in T[x]$ *tak, že* $q = hp + r$ *a zároveň* $\text{st}\ r < \text{st}\ p$.

Důkaz. V důkazu existence budeme postupovat indukcí podle stupně q. Pro $q = 0$ musí být $h = 0$ a $r = 0$. Ať je nyní st $q \geq 0$ a ať tvrzení platí pro všechny dvojice $p, \overline{q}$, st $\overline{q} <$ st q. Je-li st $q <$ st p musí být opět $h = 0$ a tedy $r = q$. Pro $m =$ st q, $n =$ st p, $m \geq n$, položme $t = s_m/t_n$, kde $q = \Sigma_{i=0,\ldots,m}\ s_i x^i$ a $p = \Sigma_{i=0,\ldots,n}\ t_i x^i$. Stupeň polynomu $tx^{m-n}p$ je m a jeho vedoucí koeficient je s_m, tedy pro $\overline{q} = q - tx^{m-n}p$ je st $\overline{q} <$ st q. Podle indukčního předpokladu existují $\overline{h}, r \in T[x]$ tak, že $\overline{q} = \overline{h}p + r$ a st $r <$ st p. Položíme-li $h = \overline{h} + tx^{m-n}$, pak dostaneme $q = hp + r$.

K jednoznačnosti si stačí uvědomit, že kdykoli je $q = hp + r = h_1 p + r_1$, st $r <$ st p a st $r_1 <$ st p, pak je $r_1 - r = (h - h_1)p$. Protože st $(r_1 - r) <$ st p, musí být $h - h_1 = 0$. Tedy $h = h_1$ a $r = q - hp = q - h_1 p = r_1$. □

Jednoznačně určený zbytek r budeme značit q mod p (q modulo p).

Dělení se zbytkem lze využít v Eukleidově algoritmu i pro polynomy - zcela analogicky jako v $\mathbb{N}$ (stupeň zbytku se nemůže stále zmenšovat). My použijeme k důkazu existence a vyjádření NSD trochu jiný postup.

Definice. Ať je R komutativní okruh a a je prvek R. Snadno zjistíme, že množina $aR = \{ab\ ;\ b \in R\}$ je ideál R. Ideál aR se nazývá *hlavní ideál generovaný prvkem* a. Řekneme-li, že ideál I je hlavní, myslíme tím, že existuje $a \in R$ tak, že $I = aR$.

Lemma 3.10 *Každý ideál okruhu $T[x]$ je hlavní.*

Důkaz. Ať je $I \neq 0$ ideál $T[x]$. Zvolme $0 \neq p \in I$ s nejmenším možným stupněm. Dokážeme, že $I = pT[x]$. Jistě platí $pT[x] \subseteq I$. Naopak zvolme $q \in I$ a vydělme se zbytkem $q = hp + r$, st $r <$ st p. Máme $r = q - hp \in I$, neboť $hp \in I$, a proto musí být $r = 0$ a $q = hp \in pT[x]$. □

Definice. Polynom h, který dělí polynomy p i q se nazývá *společný dělitel* p a q. Platí-li navíc $\overline{h}|h$ kdykoli je $\overline{h}$ společný dělitel p a q, pak se h nazývá *největší společný dělitel* p *a* q. Značíme opět $h =$ NSD(p, q).

Největší společný dělitel je určený jednoznačně až na asociovanost, tedy je-li $h =$ NSD(p, q) a $h||g$, pak je také $g =$ NSD(p, q). Naopak jsou-li $h_1, h_2 =$ NSD(p, q), pak je $h_1||h_2$.

Lemma 3.11 *Každé dva polynomy mají v $T[x]$ největšího společného dělitele. Je-li $h =$ NSD(p, q), pak existují polynomy $\overline{p}, \overline{q} \in T[x]$ takové, že $h = p\overline{p} + q\overline{q}$.*

Důkaz. Zvolme $p, q \in T[x]$. Položme $I = pT[x] + qT[x] = \{ph_1 + qh_2\ ;\ h_1, h_2 \in T[x]\}$. Snadno se ověří, že I je ideál $T[x]$ (součet dvou ideálů). Pak ale existuje $h \in T[x]$ tak, že $I = hT[x]$. Ukážeme, že $h =$ NSD(p, q). Nejdříve $p, q \in I$, tedy $h|p$ a $h|q$. Ať je $\overline{h}$ společný dělitel p a q. Pak $p, q \in \overline{h}T[x]$, tedy $pT[x] + qT[x] \subseteq \overline{h}T[x]$. Ukázali jsme, že $I \subseteq \overline{h}T[x]$, proto $h \in \overline{h}T[x]$ a $\overline{h}|h$.

Existence polynomů $\overline{p}$, $\overline{q}$ plyne z $h \in pT[x] + qT[x]$. □

V důkazu jsme používali fakt, že $hT[x] \subseteq \overline{h}T[x]$ právě když $\overline{h}|h$. Navíc jistě platí $hT[x] = \overline{h}T[x]$ právě když jsou h a $\overline{h}$ asociované. Vidíme, že *uspořádání ideálů inkluzí je obrácené uspořádání polynomů dělitelností až na asociovanost.*

Maximálním ideálům odpovídají takzvané nerozložitelné, ireducibilní, polynomy, které hrají roli prvočísel v $T[x]$.

Definice. Polynom $p \in T[x]$ se nazývá *ireducibilní*, pokud je st $p \geq 1$ a p není součin dvou polynomů nižších stupňů.

Všechny polynomy stupně 1 jsou ireducibilní. Jedinými děliteli ireducibilního polynomu jsou asociované polynomy (mají stejný stupeň) a nenulové skaláry. Prvky T^* jsou nejmenší v dělitelnosti. Ireducibilní polynomy jsou tedy minimální v dělitelnosti a proto odpovídají maximálním ideálům.

Faktor $T[x]/p$. Pro polynom $p \in T[x]$ budeme faktorový okruh $T[x]/pT[x]$ značit $T[x]/p$ a mluvit o polynomech *modulo* p. Pro $p = 0$ platí $T[x]/0 \cong T[x]$. Ať je $p \neq 0$. Polynom $q \in T[x]$ můžeme vydělit se zbytkem $q = hp + r$, st $r <$ st p. Vidíme, že $q + pT[x] = r + pT[x]$. Jsou-li $q_1 \neq q_2$ polynomy stupně ostře menšího než st p, pak p nedělí $q_1 - q_2$ a tedy $q_1 + pT[x] \neq q_2 + pT[x]$. Zjistili jsme, že třídy ve faktoru $T[x]/p$ odpovídají přesně polynomům stupně menšího než st p. Můžeme proto ztotožnit:

$$T[x]/p = \{q \in T[x] \ ; \ \text{st } q < \text{st } p\}.$$

V této reprezentaci $T[x]/p$ sčítáme polynomy běžně po složkách a násobíme tak, že výsledek součinu je *zbytek* po vydělení součinu polynomů polynomem p. Také vidíme, že $T[x]/p$ je vektorový prostor nad T dimenze st p, $\dim_T T[x]/p =$ st p. Báze $T[x]/p$ nad T je například množina $\{1 = x^0, x, x^2, ..., x^{\text{st } p \ -1}\}$ (porovnejte s konstrukcí $\mathbb{Z}_n$!).

Lemma 3.12 *Je-li $p \in T[x]$ ireducibilní polynom, pak $T[x]/p$ je těleso a* $\dim_T T[x]/p =$ st p.

Důkaz. Ideál $pT[x]$ je maximální, tedy podle Věty 3.6 je $T[x]/p$ těleso. □

Příklad. 1) Ať je $p = x^2 - 2 \in \mathbb{Q}[x]$. Pokud má p netriviální rozklad na součin, pak je ve tvaru $p = (x + a)(x + b)$. Přitom musí platit $ab = -2$ a $a + b = 0$, tedy $a^2 = 2$. Tuto vlastnost ale nemá žádné racionální číslo, proto je p nerozložitelný v $\mathbb{Q}[x]$. Těleso $\mathbb{Q}[x]/x^2 - 2$ je vektorový prostor dimenze 2 nad $\mathbb{Q}$ s bází $\{1, x\}$, tedy $\mathbb{Q}[x]/x^2 - 2 = \{c + dx \ ; \ c, d \in \mathbb{Q}\}$. Prvek x má ve faktoru vlastnost $x^2 - 2 = 0$. To znamená (později dokážeme přesněji), že můžeme vyjádřit faktor ve tvaru:

$$\mathbb{Q}[x]/x^2 - 2 = \{c + d\sqrt{2} \ ; \ c, d \in \mathbb{Q}\}.$$

2) Nerozložitelnost polynomu $p = x^2 + 1 \in \mathbb{R}[x]$ můžeme ukázat podobně. Pokud $p = (x + a)(x + b)$, pak $ab = 1$ a $a + b = 0$, tedy $a^2 = -1$. Takové reálné číslo neexistuje a proto je p v $\mathbb{R}[x]$ nerozložitelný. Těleso $\mathbb{R}[x]/x^2 + 1 = \{c + dx \ ; \ c, d \in \mathbb{R}\}$ a pro x platí v tomto tělese vztah $x^2 + 1 = 0$. Můžeme tedy vyjádřit faktor ve tvaru:

$$\mathbb{R}[x]/x^2 + 1 = \{c + di \ ; \ c, d \in \mathbb{R}\} = \mathbb{C}.$$

Úkol. Dokažte bez použití Lemmatu 3.12, že množina $\mathbb{Q}[x]/x^2-2 = \{c+d\sqrt{2}\,;\ c,d \in \mathbb{Q}\}$ z Příkladu je podtěleso $\mathbb{R}$!

Lemma 3.13 *Ať je $p \in T[x]$ ireducibilní polynom a $q, h \in T[x]$. Pokud $p|qh$, pak $p|q$ nebo $p|h$.*

Důkaz. Jedná se o vlastnost analogickou ekvivalentní definici prvočísla. Ideál $pT[x]$ je maximální. Předpokládejme například, že p nedělí q. Pak $q \notin pT[x]$ a ideál $I = pT[x] + qT[x]$ (součet ideálů) je v inkluzi ostře větší než $pT[x]$. Proto $I = R$ a tedy $1 = p\overline{p} + q\overline{q}$ pro vhodné polynomy $\overline{p}, \overline{q} \in T[x]$. Vynásobením dostaneme $h = hp\overline{p} + hq\overline{q}$. Jistě p dělí $hp\overline{p}$ a také $hq\overline{q}$, neboť $p|qh$. Tudíž p dělí h. □

Před vyslovením následující Věty si uvědomíme jednoduchou vlastnost počítání s polynomy. Jsou-li $p, q, h \in T[x]$, $h \neq 0$, takové, že $ph = qh$, pak musí být $p = q$ (lze zkrátit o nenulový polynom). Totiž z $(p-q)h = 0$ plyne $p - q = 0$ nebo $h = 0$ (stupeň součinu je součet stupňů). Totéž platí pro asociovanost: je-li $ph||qh$ a $h \neq 0$, pak je $p||q$. Předpoklad $ph||qh$ lze převést na předchozí případ - existuje $t \in T^*$ tak, že $ph = tqh$, tedy $p = tq$.

Věta 3.14 *Každý polynom stupně alespoň 1 má až na asociovanost jednoznačný rozklad na součin ireducibilních polynomů.*

Důkaz. Ať je $p \in T[x]$. Nejdříve ukážeme existenci rozkladu. Budeme postupovat indukcí podle st p. Polynomy stupně 1 jsou ireducibilní. Předpokládejme, že st $p > 1$ a že p není ireducibilní. Zvolme mezi děliteli p polynom q nejmenšího možného kladného stupně. Polynom q je jistě ireducibilní. Máme $p = q\overline{p}$ pro vhodný $\overline{p} \in T[x]$, $1 \leq \text{st}\ \overline{p} < \text{st}\ p$. Pro $\overline{p}$ můžeme použít indukční předpoklad.

Nyní dokážeme jednoznačnost. Ať jsou $p_1p_2...p_k||q_1q_2...q_l$ asociované součiny ireducibilních polynomů. Postupujme indukcí podle délky prvního rozkladu, tedy podle k. Je-li $k = 1$, pak je i $l = 1$, neboť p_1 je ireducibilní, a $p_1||q_1$. Předpokládejme, že $k > 1$ a že dva asociované součiny ireducibilních polynomů jsou shodné až na pořadí a asociovanost polynomů, pokud je alespoň jeden ze součinů kratší než k. Jistě $p_k|q_1q_2...q_l$ a tedy opakovanou aplikací Lemmatu 3.13 najdeme $1 \leq i \leq l$ takové, že $p_k|q_i$. Pak musí být $p_k||q_i$ neboť st $p_k \geq 1$. Máme $(p_1p_2...p_{k-1})p_k||(q_1q_2...q_{i-1}q_{i+1}...q_l)p_k$ a můžeme zkrátit $p_1p_2...p_{k-1}||q_1q_2...q_{i-1}q_{i+1}...q_l$. Z indukčního předpokladu je $k-1 = l-1$ a tyto zkrácené součiny jsou až na pořadí a asociovanost shodné. Důsledkem je shodnost původních součinů, tedy $k = l$ a po vhodném přečíslování je $p_1||q_1$, $p_2||q_2$, ..., $p_k||q_k$. □

Před definicí a odvozováním vlastností kořenů polynomů se podíváme na vlastnosti *dosazování*. Tvrzení vyslovíme obecněji pro dosazování prvků komutativního okruhu, který obsahuje těleso T.

Lemma 3.15 (o dosazování) *Ať je T těleso a zároveň podokruh komutativního okruhu R. Ať je a prvek R. Dosazením a do polynomu $p \in T[x]$ myslíme dosazení prvku a za proměnnou x a vyčíslení výrazu $p(a)$ v okruhu R. Příslušné zobrazení $\mathrm{d}_a : T[x] \to R$, $p \mapsto p(a)$, je okruhový homomorfismus.*

Důkaz. Je-li $t \in T$, pak $\mathrm{d}_a(t) = t(a) = t$ (dosazení do skaláru je triviální). Tedy $\mathrm{d}_a(1) = 1$. Dále pro $p, q \in T[x]$, $p = \Sigma_{i \in \mathbb{N} \cup \{0\}}\ t_i x^i$, $q = \Sigma_{i \in \mathbb{N} \cup \{0\}}\ s_i x^i$ platí:

$$(p+q)(a) = (\Sigma_{i \in \mathbb{N} \cup \{0\}}\ (t_i + s_i)x^i)(a) = \Sigma_{i \in \mathbb{N} \cup \{0\}}\ (t_i + s_i)a^i =$$

$$(\Sigma_{i \in \mathbb{N} \cup \{0\}}\ t_i a^i) + (\Sigma_{i \in \mathbb{N} \cup \{0\}}\ s_i a^i) = p(a) + q(a)$$

a také

$$(pq)(a) = (\Sigma_{k \in \mathbb{N} \cup \{0\}}\ (\Sigma_{i,j \in \mathbb{N} \cup \{0\},\ i+j=k}\ t_i s_j)x^k)(a) = \Sigma_{k \in \mathbb{N} \cup \{0\}}\ (\Sigma_{i,j \in \mathbb{N} \cup \{0\},\ i+j=k}\ t_i s_j)a^k =$$

$$(\Sigma_{i \in \mathbb{N} \cup \{0\}}\ t_i a^i) \cdot (\Sigma_{j \in \mathbb{N} \cup \{0\}}\ s_j a^j) = p(a)q(a).$$

□

V definici sčítání a násobení polynomů používáme pouze obecné vlastnosti sčítání a násobení, které platí v každém komutativním okruhu. Konstrukce okruhu polynomů $T[x]$ je tedy vlastně "volné" přidání nového prvku x k tělesu T. Dosazení prvku $a \in R$ lze chápat jako specifikaci prvku x.

Definice. Mějme $T \leq R$, $a \in R$ a $\mathrm{d}_a : T[x] \to R$ jako v předchozím lemmatu. Víme, že $\mathrm{Ker}(\mathrm{d}_a)$ je hlavní ideál okruhu $T[x]$ a obraz $\mathrm{Im}(\mathrm{d}_a)$ je podokruh R. Generátor ideálu $\mathrm{Ker}(\mathrm{d}_a)$ nazýváme *minimální polynom prvku a nad tělesem T* a značíme ho $\mathrm{m}_{T,a}$. Obraz $\mathrm{Im}(\mathrm{d}_a)$ značíme $T[a]$.

Minimální polynom je určený jednoznačně až na asociovanost. Je-li $\mathrm{m}_{T,a} = 0$, znamená to, že prvek a nesplňuje žádný netriviální polynomiální vztah s koeficienty v T.

Každý podokruh okruhu R, který obsahuje T i a, jistě musí obsahovat všechny (nezáporné) mocniny a a také všechny jejich lineární kombinace nad T, což jsou právě prvky tvaru $p(a)$. Z toho plyne, že $T[a]$ je *nejmenší* podokruh R obsahující T i a. Můžeme proto říci, že $T[a]$ je *podokruh generovaný* množinou $T \cup \{a\}$.

Dále platí:

$$T[x]/\mathrm{m}_{T,a} \cong T[a],$$

tedy $T[a]$ *je těleso právě když je polynom* $\mathrm{m}_{T,a}$ *ireducibilní.* Pro $\mathrm{m}_{T,a} \neq 0$ víme, že prvky faktoru $T[x]/\mathrm{m}_{T,a}$ můžeme ztotožnit s polynomy menšího stupně než $\mathrm{st}\ \mathrm{m}_{T,a}$ (v každé třídě faktoru je jediný takový polynom). Proto pro $\mathrm{m}_{T,a} \neq 0$ platí:

$$T[a] = \{q(a)\ ;\ q \in T[x],\ \mathrm{st}\ q < \mathrm{st}\ \mathrm{m}_{T,a}\}.$$

Příklad. Vraťme se ke zmíněným faktorům $\mathbb{Q}[x]/x^2 - 2$ a $\mathbb{R}[x]/x^2 + 1$. V prvním případě uvažme dosazení $\mathrm{d}_{\sqrt{2}} : \mathbb{Q}[x] \to \mathbb{R}$. Již jsme ukázali, že je polynom $x^2 - 2$ ireducibilní nad $\mathbb{Q}$, tedy $I = (x^2 - 2)\mathbb{Q}[x]$ je maximální ideál $\mathbb{Q}[x]$. Jistě je $x^2 - 2 \in \mathrm{Ker}(\mathrm{d}_{\sqrt{2}})$, tedy $I \subseteq \mathrm{Ker}(\mathrm{d}_{\sqrt{2}}) \neq \mathbb{Q}[x]$, neboť dosazení je nenulový homomorfismus (například prvky tělesa se při dosazení nemění). To znamená, že $I = \mathrm{Ker}(\mathrm{d}_{\sqrt{2}})$ a proto $x^2 - 2 = \mathrm{m}_{\mathbb{Q},\sqrt{2}}$. Dostáváme

$$\mathbb{Q}[x]/x^2 - 2 \cong \mathbb{Q}[\sqrt{2}] = \{c + d\sqrt{2}\ ;\ c, d \in \mathbb{Q}\}.$$

V druhém případě zcela analogicky dojdeme při zkoumání dosazení $\mathrm{d}_i : \mathbb{R}[x] \to \mathbb{C}$ k izomorfismu

$$\mathbb{R}[x]/x^2+1 \cong \mathbb{R}[i] = \{c+di \ ; \ c,d \in \mathbb{R}\} = \mathbb{C}.$$

Ve zbytku této podkapitoly budeme mluvit o dosazování prvků tělesa T, tedy o homomorfismech $T[x] \to T$. Vlastnosti homomorfismu budeme velmi často používat.

Definice. Ať je $p \in T[x]$ polynom a $a \in T$. Prvek a se nazývá *kořen polynomu* p, pokud je $p(a) = 0$.

Lemma 3.16 *Ať je $p \in T[x]$ a $a \in T$. Prvek a je kořen p právě když $x - a \mid p$.*

Důkaz. Pokud $x-a \mid p$, pak $p = (x-a)q$ pro nějaké $q \in T[x]$ a tedy $p(a) = (a-a)q(a) = 0 \cdot q(a) = 0$. Předpokládejme, že a je kořen p. Vydělme se zbytkem $p = h(x-a) + r$, st $r < 1$. Z dosazení $0 = p(a) = h(a) \cdot 0 + r(a)$ plyne, že $r(a) = 0$. Ale to znamená, že $r = 0$, neboť $r \in T$ a tudíž $r = r(a)$. Dokázali jsme, že $x - a \mid p$. □

Z lemmatu plyne, že je-li $p \in T[x]$ ireducibilní polynom stupně alespoň 2, pak p nemá v T kořen. Tuto úvahu ale nelze obrátit: například polynom $(x^2+1)^2 \in \mathbb{R}[x]$ má tytéž kořeny jako x^2+1, tedy nemá žádný reálný kořen, ale přesto není ireducibilní!

Polynom z předchozího odstavce byl stupně 4. Polynomy stupně 1 jsou ireducibilní a mají vždy jediný kořen. Ať je $p \in T[x]$ stupně 2 nebo 3. Není-li p ireducibilní, pak má rozklad na součin polynomů nižších stupňů, tedy p má dělitele stupně 1. Máme $tx+s \mid p$ pro vhodné $t \in T^*$ a $s \in T$. Vidíme, že p má kořen $-s/t$. Ukázali jsme, že *polynom stupně 2 nebo 3 je ireducibilní právě když nemá kořen.*

Definice. Ať je $p \in T[x]$ polynom a $a \in T$ kořen p. Je-li $k \in \mathbb{N}$ největší takové, že $(x-a)^k | p$, pak se číslo k nazývá *násobnost kořene* a. Je-li $k \geq 2$, pak říkáme, že a je *vícenásobný kořen* polynomu p.

Věta 3.17 *Nenulový polynom stupně n nad komutativním tělesem má nejvýše n kořenů i s násobnostmi.*

Důkaz. Dokazujme indukcí podle stupně. Polynomy stupně 0 nemají žádné kořeny. Ať je $p \in T[x]$ polynom stupně $n \geq 1$ a $a \in T$ kořen p násobnosti k. Existuje rozklad $p = (x-a)^k q$ pro vhodné $q \in T[x]$. Je-li $b \neq a$ nějaký další kořen p, pak $x - b | p$ a tedy $x - b | q$, což plyne z jednoznačnosti rozkladů na ireducibilní polynomy (polynomy stupně 1 jsou ireducibilní a $x - a$ není asociovaný s $x - b$ pro $a \neq b$). Vidíme, že všechny další kořeny p různé od a jsou také kořeny q. Zbývá pro q použít indukční předpoklad spolu s faktem, že st $q = n - k$. □

Multiplikativní grupa konečného tělesa je cyklická. V kapitole o grupách jsme dokazovali, že $\mathbb{Z}_p$ je těleso pro prvočíslo p. Uvědomme si, že již známe konstrukci dalších konečných (= s konečně mnoha prvky) těles. Stačí vzít nějaký ireducibilní polynom $q \in \mathbb{Z}_p[x]$ a faktor

$$\mathbb{Z}_p[x]/q$$

je konečné těleso s p^n prvky, kde n je stupeň q ($\mathbb{Z}_p[x]/q$ můžeme chápat jako množinu polynomů nad $\mathbb{Z}_p$ menšího stupně než n, počet těchto polynomů je p^n). Například 9-prvkové těleso získáme volbou polynomu $x^2+x+2 \in \mathbb{Z}_3[x]$ (dokažte si ireducibilitu!).

Cílem tohoto odstavce je dokázat, že grupa $T^*(\cdot)$ je cyklická pro konečné těleso T. Zvolme $k \in \mathbb{N}$ a uvažme polynom $x^k - 1 \in T[x]$. Je-li H k-prvková podgrupa grupy $T^*(\cdot)$, pak pro $t \in H$ platí $t^k = 1$ (řád prvku dělí řád grupy). Tedy každý prvek H je kořen polynomu $x^k - 1$. Podle Věty 3.17 má polynom $x^k - 1$ v T (tedy v T^*) nejvýše k kořenů (i s násobnostmi). To ale znamená, že grupa $T^*(\cdot)$ má pro každé $k \in \mathbb{N}$ nejvýše jednu k-prvkovou podgrupu, tedy je podle Věty 2.15 cyklická.

Úkol. Najděte nějaký generátor $\mathbb{Z}_{13}^*$.
Vyplňte tabulku násobení v 9-prvkovém tělese. Které prvky jsou generátory jeho multiplikativní grupy?

Úkol. Ať je p prvočíslo. Dokažte, že existují konečná tělesa s p^n prvky pro libovolně velká $n \in \mathbb{N}$.

Definice. Zobrazení $T[x] \to T[x]$, které polynomu $p = \Sigma_{i \in \mathbb{N} \cup \{0\}}\ t_i x^i$ přiřazuje polynom $p' = \Sigma_{i \in \mathbb{N}}\ i t_i x^{i-1}$ se nazývá *derivace na* $T[x]$.

Definice se shoduje s definicí derivace ve spojitém případě, kterou znáte z analýzy. My jsme ji vyslovili nad obecným tělesem (tedy například i nad $\mathbb{Z}_p$), ale i v tomto případě platí základní vlastnosti derivace:

Úkol. Dokažte, že platí:
Derivace $T[x] \to T[x]$ je homomorfismus vektorových prostorů nad T (tedy lineární zobrazení) a $(p \cdot q)' = p' \cdot q + p \cdot q'$ pro každé $p, q \in T[x]$.

Lemma 3.18 *Ať je $a \in T$ kořen polynomu $p \in T[x]$. Pak je a vícenásobný kořen právě když je a kořen p'.*

Důkaz. Je-li a vícenásobný kořen p, pak $(x-a)^2 | p$. Tedy $p = (x-a)^2 q$ pro vhodné $q \in T[x]$ a pro derivaci platí: $p' = ((x-a)^2 q)' = ((x-a)^2)' q + (x-a)^2 q' = 2(x-a)q + (x-a)^2 q' = (x-a)(2q + (x-a)q')$. Vidíme, že a je kořen p'.

Předpokládejme, že a je kořen p i p'. Můžeme psát $p = (x-a)\overline{q}$. Tedy $p' = (x-a)'\overline{q} + (x-a)\overline{q}' = \overline{q} + (x-a)\overline{q}'$. Víme, že $x - a \mid p'$ a z rovnosti $\overline{q} = p' - (x-a)\overline{q}'$ plyne, že $x - a \mid \overline{q}$. Tedy $\overline{q} = (x-a)q$ a máme $p = (x-a)^2 q$. □

Příklad a úkol. 1) Polynom $x^n - 1 \in \mathbb{C}[x]$, $n \geq 1$, nemá vícenásobné kořeny. Totiž $(x^n - 1)' = nx^{n-1}$ nemá žádný nenulový kořen, ale polynom $x^n - 1$ má pouze nenulové kořeny.

2) Polynom $x^p - x \in \mathbb{Z}_p[x]$, p prvočíslo, nemá vícenásobné kořeny. Derivace $(x^p - x)' = px^{p-1} - 1 = -1$ nemá žádný kořen. Najděte všechny kořeny tohoto polynomu v $\mathbb{Z}_p$!

V závěru této podkapitoly budeme studovat polynomy s celočíselnými koeficienty. Položme $\mathbb{Z}[x] = \{p \in \mathbb{Q}[x]$; všechny koeficienty p jsou celá čísla$\}$. Snadno se ukáže, že $\mathbb{Z}[x]$ je podokruh $\mathbb{Q}[x]$.

Úkol. Ukažte na příkladu, že v $\mathbb{Z}[x]$ *neplatí* Lemma o dělení polynomů se zbytkem. Najděte ideál $\mathbb{Z}[x]$, který není hlavní.

Definice. Polynom $p \in \mathbb{Z}[x]$ se nazývá *primitivní*, pokud je největší společný dělitel jeho koeficientů roven 1.

Například každý polynom v $\mathbb{Z}[x]$ s vedoucím koeficientem 1 je primitivní. Nyní dokážeme základní tvrzení o primitivních polynomech.

Lemma 3.19 (Gaussovo lemma) *Součin dvou primitivních polynomů je opět primitivní polynom.*

Důkaz. Mějme $p, q \in \mathbb{Z}[x]$ primitivní, $p = \Sigma_{i \in \mathbb{N} \cup \{0\}} t_i x^i$, $q = \Sigma_{j \in \mathbb{N} \cup \{0\}} s_j x^j$. Stačí ukázat, že žádné prvočíslo nedělí všechny koeficienty pq. Zvolme prvočíslo $m \in \mathbb{N}$. Víme, že m nedělí všechny koeficienty p. Ať je $i_m \in \mathbb{N} \cup \{0\}$ nejmenší takové, že m nedělí t_{i_m}. Podobně ať je $j_m \in \mathbb{N} \cup \{0\}$ nejmenší takové, že m nedělí s_{j_m}. Podívejme se na koeficient s indexem $k_m = i_m + j_m$ součinu pq :

$$v_{k_m} = t_{i_m} s_{j_m} + (\Sigma_{i \neq i_m,\ j \neq j_m,\ i+j=k_m}\ t_i s_j).$$

Označme $c = \Sigma_{i \neq i_m,\ j \neq j_m,\ i+j=k_m}\ t_i s_j)$. Ve výrazu c je vždy buď $i < i_m$ nebo $j < j_m$, tudíž vždy buď $m | t_i$ nebo $m | s_j$. Proto $m | c$. Přitom ale m nedělí $t_{i_m} s_{j_m}$, neboť m je prvočíslo a nedělí ani jednoho z činitelů. Dohromady dostaneme, že m nedělí v_{k_m}. □

Každý nenulový polynom $p \in \mathbb{Q}[x]$ je asociovaný s nějakým primitivním polynomem. Nejdříve zvolíme $0 \neq m \in \mathbb{Z}$ tak, aby $mp \in \mathbb{Z}[x]$. Označme $c \in \mathbb{Z}$ největšího společného dělitele koeficientů polynomu mp. Pak dostaneme $p = (c/m) \cdot (mp/c)$, kde $\overline{p} = mp/c \in \mathbb{Z}[x]$ je primitivní polynom.

Dále platí, že dva asociované primitivní polynomy se mohou lišit pouze ve znaménku. Jsou-li $p, q \in \mathbb{Z}[x]$ primitivní a $b \in \mathbb{Q}^*$ takové, že $p = bq$, pak musí jmenovatel zkráceného tvaru čísla b dělit všechny koeficienty q, jinak by totiž bq nebyl polynom s celočíselnými koeficienty. Tedy nutně musí být $b \in \mathbb{Z}$ a to znamená, že $b = \pm 1$, jinak by p nebyl primitivní. Vidíme, že primitivní polynom $\overline{p}$ z předchozího odstavce je až na znaménko jednoznačně určený.

Věta 3.20 *Ať je $p \in \mathbb{Z}[x]$ polynom s vedoucím koeficientem 1. Je-li $a \in \mathbb{Q}$ kořen p, pak je a celé číslo.*

Důkaz. Máme $x - a \mid p$, tedy $p = (x - a)q$ pro vhodné $q \in \mathbb{Q}[x]$. Předpokládejme, že $a = n/m$, $n \in \mathbb{Z}$, $0 \neq m \in \mathbb{Z}$, je zkrácený tvar čísla a. Pak $x - a = (mx - n)/m$, kde $mx - n$ je primitivní polynom. Podobně $q = \overline{q} \cdot l$, kde $\overline{q} \in \mathbb{Z}[x]$ je primitivní a $l \in \mathbb{Q}^*$ vhodné číslo. Máme $p = (mx - n)\overline{q} \cdot (l/m)$. Z Gaussova lemmatu víme, že $\overline{p} = (mx - n)\overline{q}$

je primitivní polynom. Polynom p má vedoucí koeficient 1, tedy je také primitivní, a proto musí být $l/m = \pm 1$.

Vedoucí koeficient p je tedy až na znaménko součin vedoucích koeficientů polynomů $mx - n$ a $\overline{q}$. Oba polynomy mají celočíselné koeficienty, proto je $m = \pm 1$ a $a \in \mathbb{Z}$. □

Důsledek 3.21 *Je-li p polynom s celočíselnými koeficienty a vedoucím koeficientem* 1 *a $a \in \mathbb{R}$ reálný kořen p, pak je a buď celé nebo iracionální.*

Důkaz. Plyne přímo z předchozí Věty. Není-li a celé, pak není ani racionální. □

Příklad. Polynomy tvaru $x^n - b$, kde $n \in \mathbb{N}$ a $b \in \mathbb{Z}$, jsou primitivní a jejich reálné kořeny jsou tedy buď celá nebo iracionální čísla. Čísla $\sqrt{2}$, třetí odmocnina ze 2 a podobně jsou proto iracionální.