# 1. Polynomy nad komutativními tělesy

## 1.1. Polynomy

▶ 1.1.1. Poznámka. Budeme značit $T$ komutativní těleso a budeme vyšetřovat okruh polynomů nad tělesem $T$, který značíme $T[x]$. Víme, že $T[x]$ je asociativní, komutativní, bez dělitelů nuly, tedy je oborem integrity s jednotkou $1 \cdot x^0$.

▶ 1.1.2. Věta (o dělení se zbytkem, algoritmus dělení). Buďte $P_1, P_2 \in T[x]$ polynomy, přičemž $P_2 \neq \theta$. Pak existují polynomy $Q, R \in T[x]$ takové, že $P_1 = P_2Q + R$, přičemž $R = \theta$ nebo $\operatorname{st} R < \operatorname{st} P_2$.

◦ *Důkaz.* Pro $P_1 = \theta$ platí $P_1 = P_2 \cdot \theta + \theta$. Pro $\operatorname{st} P_1 < \operatorname{st} P_2$ je $P_1 = P_2 \cdot \theta + P_1$. Tedy nechť $P_1 \neq \theta$ a $\operatorname{st} P_1 \geq \operatorname{st} P_2$. Nechť $P_1 = \sum_{i=0}^{m} a_i x^i$ a $P_2 = \sum_{i=0}^{n} b_i x^i$, kde $a_m \neq 0$, $b_n \neq 0$ a $m \geq n$.
Důkaz provedeme matematickou indukcí podle $m$.

**(1)** $m = 0$, tedy i $n = 0$, tedy $P_1 = a_0x^0$ a $P_2 = b_0x^0$. Pak $P_1 = a_0x^0 = (b_0x^0)(a_0b_0^{-1}x^0) + \theta$.

**(2)** Nechť $m > 0$ a nechť tvrzení platí polynomy $P_1$ stupně menšího než $m$. Definujme $\tilde{P}_1 := P_1 - (a_m b_n^{-1} x^{m-n})\, P_2$. Stupeň $(a_m b_n^{-1} x^{m-n})\, P_2$ je $m$ a jeho člen s nejvyšší mocninu je $a_m x^m$. Tedy člen $\tilde{P}_1$ s mocninou $x^m$ je $a_m - a_m = 0$. Pokud je $\tilde{P}_1 = \theta$, je $P_1 = P_2(a_m b_n^{-1} x^{m-n}) + \theta$. Pokud $\tilde{P}_1 \neq \theta$, je $\operatorname{st} \tilde{P}_1 < \operatorname{st} P_1$ a podle indukčního předpokladu existují $\tilde{Q}, \tilde{R}$ takové, že $\tilde{P}_1 = P_2\tilde{Q} + \tilde{R}$ a $\tilde{R} = \theta$ nebo $\operatorname{st} \tilde{R} < \operatorname{st} P_2$. A konečně $P_1 = \tilde{P}_1 + (a_m b_n^{-1} x^{m-n})\, P_2 = P_2 \left( \tilde{Q} + (a_m b_n^{-1} x^{m-n}) \right) + \tilde{R}$.

□

▶ 1.1.3. Poznámka. $T[x]$ je Eukleidův okruh, tj. každé 2 polynomy mají největšího společného dělitele a ten se dá najít Eukleidovým algoritmem.

▶ 1.1.4. Věta. Okruh $T[x]$ je okruhem hlavních ideálů.

◦ *Důkaz.* Mějme libovolný ideál $I \lhd T[x]$. Pokud $I = E = \{\theta\}$, je $I = I_\theta$. Tedy nechť $I \neq E$. Mějme polynom $P \in I$, $P \neq \theta$ takový, že má nejmenší stupeň ze všech nenulových polynomů v $I$. Ukážeme, že $I = I_P$.

($I \subseteq I_P$) Zvolme libovolný $P_1 \in I$, pak víme, že existují $Q, R$ takové, že $P_1 = PQ + R$, kde $R = \theta$ nebo $\operatorname{st} R < \operatorname{st} P$. Dále $R = P_1 - QP \in I$, tedy pokud by $R \neq \theta$, nutně $\operatorname{st} R < \operatorname{st} P$, což je spor s minimalitou $\operatorname{st} P$. Tedy $R = \theta$ a $P_1 = PQ \in I_P$.

($I_P \subseteq I$) Pokud $P \in I$, pak také $I_P \subseteq I$.

□

▶ 1.1.5. Definice. Buďte $P, Q \in T[x]$. Řekneme, že $Q$ dělí $P$, existuje-li $S \in T[x]$ takový, že $P = QS$. Značíme $Q \mid P$.

▶ 1.1.6. Definice. Buďte $T, U$ komutativní tělesa, $T \Subset U$ a buďte $P = \sum_{i=0}^{n} a_i x^i \in T[x]$ a $\alpha \in U$. Pak položíme hodnotu polynomu $P$ na prvku $\alpha$ jako $P(\alpha) := \sum_{i=0}^{n} a_i \alpha^i \in U$.

► 1.1.7. Definice. Buď $P \in T[x]$. Kořenem polynomu $P$ (řešení algebraické rovnice $P(x) = 0$) rozumíme libovolný prvek $\alpha$ z nějakého nadtělesa $U \supseteq T$ takový, že $P(\alpha) = 0$.

► 1.1.8. Věta. Buďte $T \subseteq U$, $P \in T[x]$, $\alpha \in U^\bullet$. Potom

$$P(\alpha) = 0 \iff (x - \alpha) \mid P.$$

◦ *Důkaz.*

(⇒) Nechť $P(\alpha) = 0$ a $P = (x - \alpha)Q + R$. Platí $R = \theta$ nebo $\operatorname{st} R < 1$, tedy $R = r_0 x^0$ pro $r_0 \in T$. Pak $0 = P(\alpha) = 0 + r_0$, tedy $r_0 = 0$ a $P = (x - \alpha)Q$.

(⇐) Platí $P = (x - \alpha)S$ tedy $P(\alpha) = 0 \cdot S(\alpha) = 0$.

□

► 1.1.9. Důsledek. Má-li $P$ navzájem různé kořeny $\alpha_1, \ldots, \alpha_k$, pak $(x - \alpha_1) \cdots (x - \alpha_k) \mid P$.

◦ *Důkaz.* $P(\alpha_1) = 0 \Rightarrow (x - \alpha_1) \mid P \Rightarrow P = (x - \alpha_1)P_1$.
$P(\alpha_2) = 0 \Rightarrow (\alpha_2 - \alpha_1)P_1(\alpha_2) = 0 \Rightarrow P_1 = (x - \alpha_2)P_2 \Rightarrow P = (x - \alpha_1)(x - \alpha_2)P_2$.
Po $k$ krocích dostaneme $P = (x - \alpha_1) \cdots (x - \alpha_k)P_k$. □

► 1.1.10. Důsledek. Polynom stupně $n$ má nejvýše $n$ různých kořenů.

► 1.1.11. Poznámka. Není-li $T$ komutativní těleso, nemusí poslední důsledek platit.

Vezměme např. okruh $Z_{16}$, který není tělesem, a $x^2 \in Z_{16}[x]$. Jeho kořeny jsou 0, 4, 8 a 12, tedy jsou čtyři pro polynom stupně 2.

Mějme $K$ těleso kvaternionů, které je nekomutativní, a polynom stupně dva, $P := x^2 + 1 \in K[x]$. Pak pro $\alpha = \pm i, \pm j, \pm k$ platí $\alpha^2 = -1$, tedy má 6 kořenů.

► 1.1.12. Definice. Derivací polynomu $P = \sum_{i=0}^{n} a_i x^i \in T[x]$ rozumíme polynom $P' \in T[x]$ daný vztahem

$$P' := \sum_{i=1}^{n} i a_i x^{i-1}.$$

► 1.1.13. Poznámka. Ve vztahu $\sum_{i=1}^{m} i a_i x^{i-1}$ není součin $i a_i$ součinem v tělese, ale $i \times a_i$. Pro jednoduchost zápis zkracujeme.

► 1.1.14. Poznámka. Derivace polynomu je formálně stejná jako v analýze, nebudeme tedy znovu dokazovat známá tvrzení, jako $(PQ)' = P'Q + PQ'$ apod.

► 1.1.15. Definice. Buďte $T \subseteq U$, $P \in T[x]$, $\alpha \in U^\bullet$, $m \in \mathbb{N}_0$. Řekneme, že $\alpha$ je $m$-násobný kořen polynomu $P$, platí-li $(x - \alpha)^m \mid P$, ale $(x - \alpha)^{m+1} \nmid P$.

► 1.1.16. Věta. Buď $\alpha$ $m$-násobný kořen polynomu $P$. Potom $\alpha$ je alespoň $(m-1)$-násobným kořenem polynomu $P'$.

◦ *Důkaz.* Máme $P = (x-\alpha)^m Q$, tedy $P' = m(x-\alpha)^{m-1}Q + (x-\alpha)^m Q' = (x-\alpha)^{m-1}(mQ + (x-\alpha)Q')$. □

► 1.1.17. Poznámka. Pokud by $T$ mělo nenulovou charakteristiku $p$ a $m$ bylo násobkem $p$, pak $mQ(\alpha) = 0$ a platí $P' = (x-\alpha)^m Q'$.

► 1.1.18. Definice. Řekneme, že $P \in T[x]$ stupně alespoň 1 je reducibilní nad $T$, existují-li $P_1, P_2 \in T[x]$ takové, že $1 \leq \operatorname{st} P_i < \operatorname{st} P$ a $P = P_1 P_2$.

V opačném případě řekneme, že $P$ je ireducibilní nad $T$.

► 1.1.19. Poznámka. Reducibilita závisí na tělese.

**(1)** Polynom $x^2 - 2 \in Q[x]$ je ireducibilní nad $Q$, ale reducibilní nad $R$, neboť $x^2 - 2 = \left(x + \sqrt{2}\right)\left(x - \sqrt{2}\right)$.

**(2)** Polynom $x^2 + 1 \in Q[x]$ je ireducibilní nad $R$, ale reducibilní nad $C$, neboť $x^2 + 1 = (x+i)(x-i)$.

► 1.1.20. Lemma. Libovolný polynom stupně 1 je ireducibilní nad libovolným tělesem.

► 1.1.21. Věta.

**(1)** Nad $C$ jsou ireducibilní právě jen polynomy 1. stupně.

**(2)** Nad $R$ jsou ireducibilní právě jen polynomy 1. stupně a polynomy 2. stupně se záporným diskriminantem příslušné kvadratické rovnice.

► 1.1.22. Lemma. Má-li polynom $P \in T[x]$ v tělese $T$ kořen, je nad tělesem $T$ reducibilní.

◦ *Důkaz.* Pokud $P(\alpha) = 0$, platí $P = (x-\alpha)Q$, kde $Q \in T[x]$ □

► 1.1.23. Poznámka. Opačná implikace neplatí. Například $P = P_1 P_2$ nad $T$, kde $\operatorname{st} P_i \geq 2$ a nemají kořen v $T$.

► 1.1.24. Lemma. Je-li $\operatorname{st} P \leq 3$ a $P$ je reducibilní nad $T$, pak má $P$ v tělese $T$ kořen.

◦ *Důkaz.* Alespoň jeden z polynomů v rozkladu má stupeň 1. □

► 1.1.25. Poznámka. Každý ideál v okruhu polynomů je hlavní, tj. $(\forall I \lhd T[x])(\exists P \in T[x])(I = I_P)$. Dále $I_P = T[x] \cdot P$.

Mějme třídy ekvivalence $T[x] \,/\, I_P$ pro $P \neq \theta$. Pak do jedné zbytkové třídy patří 2 polynomy právě tehdy, dávají-li stejný zbytek po dělení polynomem $P$

Pro $P = \theta$ jsou polynomy ekvivalentní pouze, když jsou stejné.

Je-li $\operatorname{st} P = n$, pak zbytkové polynomy jsou všechny polynomy stupně nejvýše $n-1$.

Zbytkovou třídu obsahující polynom $R$ označujeme $\overline{R}$.

► 1.1.26. Lemma. Je-li $T$ konečné těleso řádu $q$, pak počet zbytkových tříd podle polynomu $P$ stupně $n$ je $q^n$.

► 1.1.27. Lemma. $T[x] \,/\, I_P$ je asociativní a komutativní okruh s jednotkou. Jednotkou je $\overline{1 \cdot x^0}$.

► 1.1.28. Věta. Je-li $P \in T[x]$ reducibilní nad $T$, potom faktorokruh $T[x] \,/\, I_P$ obsahuje dělitele nuly.

◦ *Důkaz.* Existuje netriviální rozklad $P = P_1 P_2$. Dále $\overline{\theta} \neq \overline{P_i}$ a $\overline{\theta} = \overline{P} = \overline{P_1 P_2}$. □

► 1.1.29. Věta. Je-li $P \in T[x]$ ireducibilní nad $T$, potom je faktorokruh $T[x] \,/\, I_P$ komutativní těleso.

◦ *Důkaz.* Víme, že je komutativní s jednotkou, zbývá ukázat, že každá nenulová třída $\overline{A}$ má třídu inverzní. Důkaz provedeme neúplnou matematickou indukcí podle $m = \operatorname{st} A$, přičemž $0 \leq m < \operatorname{st} P$.

($m = 0$) Platí $A = ax^0$ a $a \neq 0$. Potom $ax^0 \cdot a^{-1}x^0 = 1x^0$, a tedy $\overline{A}\,\overline{a^{-1}x^0} = \overline{1x^0}$.

($m \geq 1$) Nechť každý polynom stupně menšího než $m$ má inverzní. $P = AQ + R$. Pak $R = \theta$ nebo $\operatorname{st} R < \operatorname{st} A = m$. Neboť $P$ je ireducibilní, je $R \neq \theta$, jinak by bylo $P = AQ$, kde $\operatorname{st} A < \operatorname{st} P$.

Tedy podle indukčního předpokladu existuje $\overline{R}^{-1}$ a dále platí: $\overline{\theta} = \overline{P} = \overline{A}\,\overline{Q} + \overline{R}$ a po vynásobení $(\overline{R})^{-1}$ dostáváme $\overline{\theta} = \overline{A}\,\overline{Q}\left(\overline{R}\right)^{-1} + \overline{1x^0}$ a konečně $\left(\overline{A}\right)^{-1} = -\overline{Q}\left(\overline{R}\right)^{-1}$.

□

► 1.1.30. Příklad. Mějme reálný polynom $P := x^2+1 \in R[x]$. Pak $R[x] \,/\, I_P = \left\{\overline{a + bx} \;\middle|\; a, b \in \mathbb{R}\right\}$. Platí

$$\overline{a_1 + b_1 x} + \overline{a_2 + b_2 x} = \overline{(a_1 + a_2) + (b_1 + b_2)x}$$

a

$$\overline{a_1 + b_1 x} \cdot \overline{a_2 + b_2 x} = \overline{(a_1 a_2) + (a_1 b_2 + a_2 b_1)x + (b_1 b_2)x^2}.$$

A neboť $x^2 \equiv_{I_P} -1$, je $\overline{x^2} = \overline{-1}$, a tedy

$$\overline{a_1 + b_1 x} \cdot \overline{a_2 + b_2 x} = \overline{(a_1 a_2 - b_1 b_2) + (a_1 b_2 + a_2 b_1)x}.$$

Víme $R[x] \,/\, I_P$ je komutativní těleso a operace jsou stejné jako v $C$. To nám umožňuje pomocí $R$ definovat komplexní čísla, stačí místo $x$ psát všude $i$.

## • 1.2. Adjunkce

► 1.2.1. Definice. Mějme dvojici těles $T \Subset U$ a $A \subseteq U^\bullet$. Pak definujeme těleso $T(A) := \bigcap \{V \Subset U \mid T^\bullet \cup A^\bullet \subseteq V\}$ a říkame, že vzniká tělesovou adjunkcí $A$ k $T$.

Je-li $A$ jednoprvková, $A = \{\alpha\}$, pak používáme označení jednoduchá adjunkce, a značíme $T(\alpha) := T(\{\alpha\})$.

► 1.2.2. Příklad.

**(1)** Je-li $A \subseteq T$, je $T(A) = T$.

**(2)** $Q\left(\left\{\sqrt{2}\right\}\right) = \left\{a + b\sqrt{2} \;\middle|\; a, b \in \mathbb{Q}\right\}$.

**(3)** $R(i) = C$.

► 1.2.3. Definice. Pro $T \Subset U$ a $\alpha \in U$ definujeme $T[\alpha] := \{P(\alpha) \mid P \in T[x]\}$.

► 1.2.4. Lemma. $T[\alpha]$ je podokruh $T(\alpha)$.

◦ *Důkaz.* Pro libovolný polynom $P \in T[x]$ je $P(\alpha)$ kombinací $\alpha$ a prvků z $T$, tedy $T[\alpha] \subseteq T(\alpha)$. Snadno se ukáže, že je okruhem. □

► 1.2.5. Lemma. $T[\alpha]$ je obor integrity.

◦ *Důkaz.* $T[\alpha]$ je podokruhem komutativního tělesa $T(\alpha)$, tedy je oborem integrity. □

► 1.2.6. Lemma. Těleso $T(\alpha)$ je izomorfní s podílovým tělesem oboru integrity $T[\alpha]$.

◦ *Důkaz.* Označme $H = T[\alpha]$. Pak těleso zlomků $U_H$ je izomorfní s podílovým tělesem $T_H$.

Definujeme $h : U_H \to T(\alpha)$ jako $h\left(\frac{a}{b}\right) = ab^{-1}$ pro $a, b \in H$ a $b \neq 0$. Tedy existují $P, Q \in T[x]$ takové, že $a = P(\alpha)$ a $b = Q(\alpha)$. Korektnost definice a fakt, že $h$ je monomorfismus jsme ukázali dříve pro obdobný případ, tedy $U_H \cong h(U_H) \overset{\text{těl.}}{\Subset} T(\alpha)$.

Ukážeme, že $T \cup \{\alpha\} \subseteq h(U_H)$, což už stačí pro to, aby $T(\alpha) \Subset h(U_H)$. Zvolíme $Q = 1x^0$, tedy $b = Q(\alpha) = 1$. Volbou $P = x$ dostaneme $a = P(\alpha) = \alpha$ a tedy $h\left(\frac{a}{b}\right) = \alpha$. Volbou $P = tx^0$ pro libovolné $t \in T$ dostaneme $a = P(\alpha) = t$ a tedy $h\left(\frac{a}{b}\right) = t$. □

► 1.2.7. Lemma. Buďte $T \Subset U$ tělesa, $\alpha \in U^\bullet$ a nechť $h : T[x] \to T[\alpha]$ je definované jako $h(P) = P(\alpha)$. Potom $T[\alpha] \overset{\text{okr.}}{\cong} T[x] \,/\, \ker h$, přičemž $\ker h = \{P \in T[x] \mid P(\alpha) = 0\}$.

◦ *Důkaz.* Je $h(P + Q) = (P + Q)(\alpha) = P(\alpha) + Q(\alpha) = h(P) + h(Q)$ a podobně pro $h(PQ)$, tedy $h$ je homomorfismus. Současně $h$ je z definice $T[\alpha]$ na, tedy $h$ je epimorfismus. Tvrzení lemmatu již plyne z věty o homomorfismu. □

► 1.2.8. Definice. Buďte $T \Subset U$ tělesa, $\alpha \in U^\bullet$. Pomocí zobrazení $h$ z předchozího lemmatu dělíme prvky $U$ do 2 skupin.

($\ker h = E = \{\theta\}$) Pak $\alpha$ nazýváme <u>transcendentní prvek</u> nad tělesem $T$.

Dále podle lemmatu je $T[\alpha] \cong T[x] \,/\, E \cong T[x]$ a izomorfní obory integrity mají izomofní podílová tělesa, tedy $T(\alpha) \cong T(x)$, kde symbolem $T(x)$ značíme podílové těleso k $T[x]$, tj. těleso racionálních funkcí.

($\ker h \neq E$) Pak $\alpha$ nazýváme <u>algebraický prvek</u>.

Dále $\ker h$ je ideálem a my jsme v okruhu hlavních ideálů, tedy $\ker h = I_Q$ pro nějaké $Q \in T[x]$, $Q \neq \theta$. Ze všech takových $Q$ vybereme polynom s nejmenším stupněm $n$, který je normovaný (koeficient u $x^n$ je 1), a nazveme jej <u>minimální polynom</u> prvku $\alpha$ nad $T$ a budeme jej značit $M_\alpha^T$. Číslo $n$ nazveme <u>stupněm</u> prvku $\alpha$ a budeme jej značnit $\operatorname{st}\alpha$.

Navíc $T[\alpha] \cong T[x] \,/\, I_{M_\alpha}$, kde pravá strana je těleso, a tedy z izomorfie i $T[\alpha]$ je těleso (pro algebraické $\alpha$). A dále $T(\alpha) \cong T_{T[\alpha]} = T[\alpha] = T[x] \,/\, I_{M_\alpha^T}$.

► 1.2.9. Lemma. Minimální polynom je ireducibilní nad $T$.

► 1.2.10. Věta. Buď $\alpha$ algebraický prvek nad tělesem $T$. Potom $T(\alpha) \cong T[x] \,/\, I_{M_\alpha^T}$.

► 1.2.11. Příklad.

**(1)** Všechny prvky $\alpha \in \mathbb{C}$ jsou algebraické nad $C$ a platí $M_\alpha^C = x - \alpha$.

**(2)** Všechny prvky $\alpha \in \mathbb{C}$ jsou algebraické nad $R$. Pro $\alpha \in \mathbb{R}$ platí $M_\alpha^R = x - \alpha$ a pro $\alpha \notin R$ platí $M_\alpha^{\mathbb{R}} = (x-\alpha)(x-\bar{\alpha}) = x^2 - 2\operatorname{Re}\alpha x + |\alpha|^2$.

**(3)** Algebraické číslo (bez udání tělesa) znamená algebraické nad $\mathbb{Q}$. Totéž pro transcendentní. Příklady transcendentních jsou $\pi$ a $e$.

► 1.2.12. Lemma. Buď $\alpha$ algebraický prvek nad $T$. Potom $T[\alpha] = T(\alpha)$.

◦ *Důkaz.* Pro $\beta \in T$ definujeme $P = \alpha^{-1}\beta x^1$, pak $P(\alpha) = \beta$; položme $P = 1x^1$, pak $P(\alpha) = \alpha$. Tedy $T(\alpha) \subseteq T[\alpha]$. Opačnou inkluzi jsme ukázali dříve. □

► 1.2.13. Věta. Buď $\alpha$ algebraický prvek nad tělesem $T$ a nechť $\operatorname{st}\alpha = n$. Potom $\dim_T T(\alpha) = n$ a jednou z bází $T(\alpha)$ je soubor $(1, \alpha, \alpha^2, \ldots, \alpha^{n-1})$, a tedy libovolný prvek $\beta \in T(\alpha)$ lze psát ve tvaru $\beta = \sum_{i=0}^{n-1} b_i\alpha^i$, kde $b_i \in T^\bullet$.

◦ *Důkaz.* Mějme libovolné $\beta \in T(\alpha) = T[\alpha]$. Tedy $(\exists P \in T[x])(\beta = P(\alpha))$. Pak podle věty o dělení se zbytkem je $P = M_\alpha Q + R$, kde $R = \theta$ nebo $\operatorname{st} R < \operatorname{st} M_\alpha = n$, a platí $R(\alpha) = P(\alpha) = \beta$. Je-li $R = \sum_{i=0}^{n-1} b_i x^i$, pak $\beta = \sum_{i=0}^{n-1} b_i\alpha^i$, a tedy definovaný soubor generuje.

Ukážeme, že je nezávislý. Nechť existuje nenulová lineární kombinace souboru, pak je tato kombinace polynomem s nižším stupněm než $n$, který má v bodě $\alpha$ hodnotu 0, což je spor s minimalitou stupně $M_\alpha$. Tedy daný soubor je bází a dimenze je $n$. □

► 1.2.14. Věta. Libovolný ireducibilní polynom má kořen (obecně v nadtělese).

◦ *Důkaz.* Máme ireducibilní $P \in T[x]$. Je-li $\operatorname{st} P = 1$, je $P = a_0 + a_1 x$ a má kořen v $T$. Tedy nechť $\operatorname{st} P \geq 2$.

Označme $U := T[x] \,/\, I_P$ a neboť $P$ je ireducibilní, je $U$ komutativní těleso. Definujeme zobrazení $h : T \to U$ jako $h(a) := \overline{ax^0}$. Snadno se ukáže, že $h$ je okruhový monomorfismus, tedy $T \cong h(T) \Subset U$. Známým postupem najdeme k tělesu $T$ nadtěleso $V$ tak, že z $U$ vyjmeme $h(T)$ a nahradíme jej $T$, tedy $V = (U \setminus h(T)) \cup T \cong U$. Definujeme izomorfismus $g : V \to U$ jako

$$g(\beta) := \begin{cases} h(\beta) \mid \beta \in T \\ \beta \quad\quad \mid \beta \in V \setminus T. \end{cases}$$

Ukážeme, že kořenem $P$ je prvek $\alpha \in V$, $\alpha = g^{-1}(\overline{x})$. Platí

$$P(\alpha) = \sum_{i=0}^{n} a_i\alpha^i = g^{-1}\left(\sum_{i=0}^{n} g(a_i)\, g(\alpha^i)\right) = g^{-1}\left(\sum_{i=0}^{n} \overline{a_i x^0}\,\overline{x^i}\right) = g^{-1}\left(\overline{\sum_{i=0}^{n} a_i x^i}\right) = g^{-1}\big(\overline{P}\big) = g^{-1}\big(\overline{\theta}\big) = 0.$$

□

► 1.2.15. Důsledek. Libovolný polynom stupně většího než nula má kořen.

► 1.2.16. Poznámka. V předchozí větě je $\alpha$ algebraický nad $T$ a navíc $P$ je jeho minimálním polynomem.

◦ *Důkaz.* Máme $P(\alpha) = 0$, tedy $M_\alpha^T \mid P$ (z věty o dělení). Navíc $P$ je ireducibilní, tedy $P$ nemá netriviální dělitele, a je tedy minimálnímu polynomu roven až na normování koeficientu u nejvyšší mocniny na 1. □

► 1.2.17. Definice. Buďte $T$ těleso a $P \in T[x]$. Rozkladové těleso polynomu $P$ je nejmenší nadtěleso $U \supseteq T$ takové, že v něm lze $P$ rozložit na součin lineárních polynomů, tj. že v něm leží všechny kořeny $P$.

► 1.2.18. Věta. Libovolný polynom stupně alespoň 1 má rozkladové těleso.

◦ *Důkaz.* Mějme $P \in T[x]$ a nechť $P = P_1 \cdots P_k$ pro $P_i \in T[x]$ je rozklad na ireducibilní polynomy. Jsou-li všechny $P_i$ stupně jedna, je $T$ samo rozkladovým tělesem. Tedy nechť např. $P_1$ má stupeň alespoň 2. Pak existuje $V \supseteq T$ takové, že $P_1$ má ve $V$ kořen $\alpha$, tedy lze rozložit na polynom a lineární polynom.

Tedy máme $P = Q_1 \cdots Q_\ell$ rozklad v tělese $V$, kde jistě $\ell > k$, neboť jsme $P_1$ rozložili. Je možné, že jsme rozložili víc, než jen $P_1$. Pokud opět zbydou nějaké stupně alespoň 2, proces opakujeme. □