Kořen polynomu

Definice. Nechť R je okruh, $f = a_n \cdot x^n + \cdots + a_1 \cdot x + a_0 \in R[x]$, $c \in R$. Pak prvek $a_n \cdot c^n + \cdots + a_1 \cdot c + a_0 \in R$ značíme $f(c)$ a nazýváme **hodnota** polynomu f v prvku c.

Kořen polynomu

Definice. Nechť R je okruh, $f = a_n \cdot x^n + \cdots + a_1 \cdot x + a_0 \in R[x]$, $c \in R$. Pak prvek $a_n \cdot c^n + \cdots + a_1 \cdot c + a_0 \in R$ značíme $f(c)$ a nazýváme **hodnota** polynomu f v prvku c.

Věta. Nechť R je komutativní okruh, $f, g \in R[x]$, $c \in R$. Pak platí

- $(f + g)(c) = f(c) + g(c)$,

Kořen polynomu

Definice. Nechť R je okruh, $f = a_n \cdot x^n + \cdots + a_1 \cdot x + a_0 \in R[x]$, $c \in R$. Pak prvek $a_n \cdot c^n + \cdots + a_1 \cdot c + a_0 \in R$ značíme $f(c)$ a nazýváme **hodnota** polynomu f v prvku c.

Věta. *Nechť R je komutativní okruh, $f, g \in R[x]$, $c \in R$. Pak platí*

- $(f + g)(c) = f(c) + g(c)$,
- $(f \cdot g)(c) = f(c) \cdot g(c)$.

Kořen polynomu

Definice. Nechť R je okruh, $f = a_n \cdot x^n + \cdots + a_1 \cdot x + a_0 \in R[x]$, $c \in R$. Pak prvek $a_n \cdot c^n + \cdots + a_1 \cdot c + a_0 \in R$ značíme $f(c)$ a nazýváme **hodnota** polynomu f v prvku c.

Věta. Nechť R je komutativní okruh, $f, g \in R[x]$, $c \in R$. Pak platí

- $(f + g)(c) = f(c) + g(c)$,
- $(f \cdot g)(c) = f(c) \cdot g(c)$. [Věta 6.2, str. 87]

Poznámka. Předpoklad o komutativitě byl podstatný pro násobení: jestliže pro $a, c \in R$ platí $a \cdot c \neq c \cdot a$, pak pro $f = x$, $g = a$ je $(f \cdot g)(c) = (x \cdot a)(c) = (a \cdot x)(c) = a \cdot c \neq c \cdot a = f(c) \cdot g(c)$.

Kořen polynomu

Definice. Nechť R je okruh, $f = a_n \cdot x^n + \cdots + a_1 \cdot x + a_0 \in R[x]$, $c \in R$. Pak prvek $a_n \cdot c^n + \cdots + a_1 \cdot c + a_0 \in R$ značíme $f(c)$ a nazýváme **hodnota** polynomu f v prvku c.

Věta. *Nechť R je komutativní okruh, $f, g \in R[x]$, $c \in R$. Pak platí*

- $(f + g)(c) = f(c) + g(c)$,
- $(f \cdot g)(c) = f(c) \cdot g(c)$. [Věta 6.2, str. 87]

Poznámka. Předpoklad o komutativitě byl podstatný pro násobení: jestliže pro $a, c \in R$ platí $a \cdot c \neq c \cdot a$, pak pro $f = x$, $g = a$ je $(f \cdot g)(c) = (x \cdot a)(c) = (a \cdot x)(c) = a \cdot c \neq c \cdot a = f(c) \cdot g(c)$.

Důsledek. *Nechť R je komutativní okruh, $c \in R$. Pak zobrazení $\alpha : R[x] \to R$ určené předpisem $\alpha(f) = f(c)$ pro každé $f \in R[x]$ je homomorfismus okruhů.*

Kořen polynomu

Definice. Nechť R je okruh, $f = a_n \cdot x^n + \cdots + a_1 \cdot x + a_0 \in R[x]$, $c \in R$. Pak prvek $a_n \cdot c^n + \cdots + a_1 \cdot c + a_0 \in R$ značíme $f(c)$ a nazýváme **hodnota** polynomu f v prvku c.

Věta. *Nechť R je komutativní okruh, $f, g \in R[x]$, $c \in R$. Pak platí*

- $(f + g)(c) = f(c) + g(c)$,
- $(f \cdot g)(c) = f(c) \cdot g(c)$. [Věta 6.2, str. 87]

Poznámka. Předpoklad o komutativitě byl podstatný pro násobení: jestliže pro $a, c \in R$ platí $a \cdot c \neq c \cdot a$, pak pro $f = x$, $g = a$ je $(f \cdot g)(c) = (x \cdot a)(c) = (a \cdot x)(c) = a \cdot c \neq c \cdot a = f(c) \cdot g(c)$.

Důsledek. *Nechť R je komutativní okruh, $c \in R$. Pak zobrazení $\alpha : R[x] \to R$ určené předpisem $\alpha(f) = f(c)$ pro každé $f \in R[x]$ je homomorfismus okruhů.*

Definice. Nechť R je okruh, $f \in R[x]$, $c \in R$. Řekneme, že c je **kořenem** polynomu f, jestliže $f(c) = 0$.

Násobnost kořene polynomu

Věta. *Nechť R je komutativní okruh, $f \in R[x]$, $c \in R$. Pak platí: c je kořenem polynomu f, právě když $(x - c) \mid f$ v okruhu $R[x]$.*

Násobnost kořene polynomu

Věta. *Nechť R je komutativní okruh, $f \in R[x]$, $c \in R$. Pak platí: c je kořenem polynomu f, právě když $(x - c) \mid f$ v okruhu $R[x]$.*

[Věta 6.5, str. 87]

Definice. Nechť R je komutativní okruh, $f \in R[x]$, $f \neq 0$, $c \in R$, $f(c) = 0$. Přirozené číslo k se nazývá **násobnost** kořene c polynomu f, jestliže $(x - c)^k \mid f$ a $(x - c)^{k+1} \nmid f$ v okruhu $R[x]$.

Násobnost kořene polynomu

Věta. *Nechť R je komutativní okruh, $f \in R[x]$, $c \in R$. Pak platí: c je kořenem polynomu f, právě když $(x - c) \mid f$ v okruhu $R[x]$.*

[Věta 6.5, str. 87]

Definice. Nechť R je komutativní okruh, $f \in R[x]$, $f \neq 0$, $c \in R$, $f(c) = 0$. Přirozené číslo k se nazývá **násobnost** kořene c polynomu f, jestliže $(x - c)^k \mid f$ a $(x - c)^{k+1} \nmid f$ v okruhu $R[x]$. Kořeny násobnosti k se také nazývají k-**násobné**.

Násobnost kořene polynomu

Věta. *Nechť R je komutativní okruh, $f \in R[x]$, $c \in R$. Pak platí: c je kořenem polynomu f, právě když $(x - c) \mid f$ v okruhu $R[x]$.*

[Věta 6.5, str. 87]

Definice. Nechť R je komutativní okruh, $f \in R[x]$, $f \neq 0$, $c \in R$, $f(c) = 0$. Přirozené číslo k se nazývá **násobnost** kořene c polynomu f, jestliže $(x - c)^k \mid f$ a $(x - c)^{k+1} \nmid f$ v okruhu $R[x]$. Kořeny násobnosti k se také nazývají k-**násobné**. Kořeny násobnosti 1 nazýváme **jednoduché**.

Násobnost kořene polynomu

Věta. *Nechť R je komutativní okruh, $f \in R[x]$, $c \in R$. Pak platí: c je kořenem polynomu f, právě když $(x - c) \mid f$ v okruhu $R[x]$.*

[Věta 6.5, str. 87]

Definice. Nechť R je komutativní okruh, $f \in R[x]$, $f \neq 0$, $c \in R$, $f(c) = 0$. Přirozené číslo k se nazývá **násobnost** kořene c polynomu f, jestliže $(x - c)^k \mid f$ a $(x - c)^{k+1} \nmid f$ v okruhu $R[x]$. Kořeny násobnosti k se také nazývají k-**násobné**. Kořeny násobnosti 1 nazýváme **jednoduché**.

Poznámka. Podmínka $(x - c)^k \mid f$ znamená, že existuje $g \in R[x]$ tak, že $(x - c)^k \cdot g = f$.

Násobnost kořene polynomu

Věta. *Nechť R je komutativní okruh, $f \in R[x]$, $c \in R$. Pak platí: c je kořenem polynomu f, právě když $(x - c) \mid f$ v okruhu $R[x]$.*

[Věta 6.5, str. 87]

Definice. Nechť R je komutativní okruh, $f \in R[x]$, $f \neq 0$, $c \in R$, $f(c) = 0$. Přirozené číslo k se nazývá **násobnost** kořene c polynomu f, jestliže $(x - c)^k \mid f$ a $(x - c)^{k+1} \nmid f$ v okruhu $R[x]$. Kořeny násobnosti k se také nazývají k-**násobné**. Kořeny násobnosti 1 nazýváme **jednoduché**.

Poznámka. Podmínka $(x - c)^k \mid f$ znamená, že existuje $g \in R[x]$ tak, že $(x - c)^k \cdot g = f$. Protože $(x - c)^k$ je normovaný polynom stupně k, platí $k + \mathrm{st}(g) = \mathrm{st}(f)$.

Násobnost kořene polynomu

Věta. *Nechť R je komutativní okruh, $f \in R[x]$, $c \in R$. Pak platí: c je kořenem polynomu f, právě když $(x - c) \mid f$ v okruhu $R[x]$.*

[Věta 6.5, str. 87]

Definice. Nechť R je komutativní okruh, $f \in R[x]$, $f \neq 0$, $c \in R$, $f(c) = 0$. Přirozené číslo k se nazývá **násobnost** kořene c polynomu f, jestliže $(x - c)^k \mid f$ a $(x - c)^{k+1} \nmid f$ v okruhu $R[x]$. Kořeny násobnosti k se také nazývají k-**násobné**. Kořeny násobnosti 1 nazýváme **jednoduché**.

Poznámka. Podmínka $(x - c)^k \mid f$ znamená, že existuje $g \in R[x]$ tak, že $(x - c)^k \cdot g = f$. Protože $(x - c)^k$ je normovaný polynom stupně k, platí $k + \mathrm{st}(g) = \mathrm{st}(f)$. Přitom $g \neq 0$, tedy $\mathrm{st}(g) \geq 0$, odkud plyne $k \leq \mathrm{st}(f)$.

Násobnost kořene polynomu

Věta. *Nechť R je komutativní okruh, $f \in R[x]$, $c \in R$. Pak platí: c je kořenem polynomu f, právě když $(x - c) \mid f$ v okruhu $R[x]$.*

[Věta 6.5, str. 87]

Definice. Nechť R je komutativní okruh, $f \in R[x]$, $f \neq 0$, $c \in R$, $f(c) = 0$. Přirozené číslo k se nazývá **násobnost** kořene c polynomu f, jestliže $(x - c)^k \mid f$ a $(x - c)^{k+1} \nmid f$ v okruhu $R[x]$. Kořeny násobnosti k se také nazývají k-**násobné**. Kořeny násobnosti 1 nazýváme **jednoduché**.

Poznámka. Podmínka $(x - c)^k \mid f$ znamená, že existuje $g \in R[x]$ tak, že $(x - c)^k \cdot g = f$. Protože $(x - c)^k$ je normovaný polynom stupně k, platí $k + \mathrm{st}(g) = \mathrm{st}(f)$. Přitom $g \neq 0$, tedy $\mathrm{st}(g) \geq 0$, odkud plyne $k \leq \mathrm{st}(f)$. Proto nenulový polynom nemůže být dělitelný každou mocninou polynomu $x - c$ a předchozí definice jednoznačně určuje násobnost každého kořene libovolného nenulového polynomu nad komutativním okruhem.

Počet kořenů polynomu nad tělesem

Věta. *Nechť R je těleso, $f \in R[x]$, $f \neq 0$. Polynom f má nejvýše* $\mathrm{st}(f)$ *kořenů v R, počítáno i s násobností. Přesněji: součet násobností všech kořenů polynomu f v R je menší nebo roven* $\mathrm{st}(f)$.

Počet kořenů polynomu nad tělesem

Věta. *Nechť R je těleso, $f \in R[x]$, $f \neq 0$. Polynom f má nejvýše* $\mathrm{st}(f)$ *kořenů v R, počítáno i s násobností. Přesněji: součet násobností všech kořenů polynomu f v R je menší nebo roven* $\mathrm{st}(f)$.

Důkaz. Nechť $c_1, \ldots, c_s$ jsou různé kořeny polynomu f v R, nechť k_i je násobnost kořene c_i.

Počet kořenů polynomu nad tělesem

Věta. *Nechť R je těleso, $f \in R[x]$, $f \neq 0$. Polynom f má nejvýše* $\mathrm{st}(f)$ *kořenů v R, počítáno i s násobností. Přesněji: součet násobností všech kořenů polynomu f v R je menší nebo roven* $\mathrm{st}(f)$.

Důkaz. Nechť $c_1, \ldots, c_s$ jsou různé kořeny polynomu f v R, nechť k_i je násobnost kořene c_i. Pak $(x - c_i)^{k_i} \mid f$ v $R[x]$.

Počet kořenů polynomu nad tělesem

Věta. *Nechť R je těleso, $f \in R[x]$, $f \neq 0$. Polynom f má nejvýše* $\mathrm{st}(f)$ *kořenů v R, počítáno i s násobností. Přesněji: součet násobností všech kořenů polynomu f v R je menší nebo roven* $\mathrm{st}(f)$.

Důkaz. Nechť $c_1, \ldots, c_s$ jsou různé kořeny polynomu f v R, nechť k_i je násobnost kořene c_i. Pak $(x - c_i)^{k_i} \mid f$ v $R[x]$. Přitom $x - c_1$, $\ldots$, $x - c_s$ jsou různé normované ireducibilní polynomy v $R[x]$.

Počet kořenů polynomu nad tělesem

Věta. *Nechť R je těleso, $f \in R[x]$, $f \neq 0$. Polynom f má nejvýše* $\mathrm{st}(f)$ *kořenů v R, počítáno i s násobností. Přesněji: součet násobností všech kořenů polynomu f v R je menší nebo roven* $\mathrm{st}(f)$.

Důkaz. Nechť $c_1, \ldots, c_s$ jsou různé kořeny polynomu f v R, nechť k_i je násobnost kořene c_i. Pak $(x - c_i)^{k_i} \mid f$ v $R[x]$. Přitom $x - c_1$, $\ldots$, $x - c_s$ jsou různé normované ireducibilní polynomy v $R[x]$. Rozklad f na součin vedoucího koeficientu f a normovaných ireducibilních polynomů nad R je jednoznačný a polynom $x - c_i$ se zde objeví k_i-krát pro každé $i = 1, \ldots, s$.

Počet kořenů polynomu nad tělesem

Věta. *Nechť R je těleso, $f \in R[x]$, $f \neq 0$. Polynom f má nejvýše* $\mathrm{st}(f)$ *kořenů v R, počítáno i s násobností. Přesněji: součet násobností všech kořenů polynomu f v R je menší nebo roven* $\mathrm{st}(f)$.

Důkaz. Nechť $c_1, \ldots, c_s$ jsou různé kořeny polynomu f v R, nechť k_i je násobnost kořene c_i. Pak $(x - c_i)^{k_i} \mid f$ v $R[x]$. Přitom $x - c_1$, $\ldots$, $x - c_s$ jsou různé normované ireducibilní polynomy v $R[x]$. Rozklad f na součin vedoucího koeficientu f a normovaných ireducibilních polynomů nad R je jednoznačný a polynom $x - c_i$ se zde objeví k_i-krát pro každé $i = 1, \ldots, s$. Označme g součin všech ostatních činitelů tohoto rozkladu, pak $f = g \cdot \prod_{i=1}^{s} (x - c_i)^{k_i}$, a tedy $\mathrm{st}(f) = \mathrm{st}(g) + \sum_{i=1}^{s} k_i$.

Počet kořenů polynomu nad tělesem

Věta. *Nechť R je těleso, $f \in R[x]$, $f \neq 0$. Polynom f má nejvýše* $\mathrm{st}(f)$ *kořenů v R, počítáno i s násobností. Přesněji: součet násobností všech kořenů polynomu f v R je menší nebo roven* $\mathrm{st}(f)$.

Důkaz. Nechť $c_1, \ldots, c_s$ jsou různé kořeny polynomu f v R, nechť k_i je násobnost kořene c_i. Pak $(x - c_i)^{k_i} \mid f$ v $R[x]$. Přitom $x - c_1$, $\ldots$, $x - c_s$ jsou různé normované ireducibilní polynomy v $R[x]$. Rozklad f na součin vedoucího koeficientu f a normovaných ireducibilních polynomů nad R je jednoznačný a polynom $x - c_i$ se zde objeví k_i-krát pro každé $i = 1, \ldots, s$. Označme g součin všech ostatních činitelů tohoto rozkladu, pak $f = g \cdot \prod_{i=1}^{s} (x - c_i)^{k_i}$, a tedy $\mathrm{st}(f) = \mathrm{st}(g) + \sum_{i=1}^{s} k_i$. Odtud $\sum_{i=1}^{s} k_i \leq \mathrm{st}(f)$.

Počet kořenů polynomu nad tělesem

Věta. *Nechť R je těleso, $f \in R[x]$, $f \neq 0$. Polynom f má nejvýše* $\mathrm{st}(f)$ *kořenů v R, počítáno i s násobností. Přesněji: součet násobností všech kořenů polynomu f v R je menší nebo roven* $\mathrm{st}(f)$.

Důkaz. Nechť $c_1, \ldots, c_s$ jsou různé kořeny polynomu f v R, nechť k_i je násobnost kořene c_i. Pak $(x - c_i)^{k_i} \mid f$ v $R[x]$. Přitom $x - c_1$, $\ldots$, $x - c_s$ jsou různé normované ireducibilní polynomy v $R[x]$. Rozklad f na součin vedoucího koeficientu f a normovaných ireducibilních polynomů nad R je jednoznačný a polynom $x - c_i$ se zde objeví k_i-krát pro každé $i = 1, \ldots, s$. Označme g součin všech ostatních činitelů tohoto rozkladu, pak $f = g \cdot \prod_{i=1}^{s} (x - c_i)^{k_i}$, a tedy $\mathrm{st}(f) = \mathrm{st}(g) + \sum_{i=1}^{s} k_i$. Odtud $\sum_{i=1}^{s} k_i \leq \mathrm{st}(f)$.

Poznámka. Předchozí věta platí i za slabšího předpokladu, že R je obor integrity.

Počet kořenů polynomu nad tělesem

Věta. *Nechť R je těleso, $f \in R[x]$, $f \neq 0$. Polynom f má nejvýše* $\mathrm{st}(f)$ *kořenů v R, počítáno i s násobností. Přesněji: součet násobností všech kořenů polynomu f v R je menší nebo roven* $\mathrm{st}(f)$.

Důkaz. Nechť $c_1, \ldots, c_s$ jsou různé kořeny polynomu f v R, nechť k_i je násobnost kořene c_i. Pak $(x - c_i)^{k_i} \mid f$ v $R[x]$. Přitom $x - c_1$, $\ldots$, $x - c_s$ jsou různé normované ireducibilní polynomy v $R[x]$. Rozklad f na součin vedoucího koeficientu f a normovaných ireducibilních polynomů nad R je jednoznačný a polynom $x - c_i$ se zde objeví k_i-krát pro každé $i = 1, \ldots, s$. Označme g součin všech ostatních činitelů tohoto rozkladu, pak $f = g \cdot \prod_{i=1}^{s} (x - c_i)^{k_i}$, a tedy $\mathrm{st}(f) = \mathrm{st}(g) + \sum_{i=1}^{s} k_i$. Odtud $\sum_{i=1}^{s} k_i \leq \mathrm{st}(f)$.

Poznámka. Předchozí věta platí i za slabšího předpokladu, že R je obor integrity. Věta však neplatí obecně pro každý komutativní okruh R, například kvadratický polynom $x^2 - [1]_8 \in \mathbb{Z}_8[x]$ má v $\mathbb{Z}_8$ čtyři jednoduché kořeny $[1]_8$, $[-1]_8$, $[3]_8$, $[-3]_8$.

Počet kořenů polynomu nad tělesem

Věta. *Nechť R je těleso, $f \in R[x]$, $f \neq 0$. Polynom f má nejvýše* $\mathrm{st}(f)$ *kořenů v R, počítáno i s násobností. Přesněji: součet násobností všech kořenů polynomu f v R je menší nebo roven* $\mathrm{st}(f)$.

Důkaz. Nechť $c_1, \ldots, c_s$ jsou různé kořeny polynomu f v R, nechť k_i je násobnost kořene c_i. Pak $(x - c_i)^{k_i} \mid f$ v $R[x]$. Přitom $x - c_1$, $\ldots$, $x - c_s$ jsou různé normované ireducibilní polynomy v $R[x]$. Rozklad f na součin vedoucího koeficientu f a normovaných ireducibilních polynomů nad R je jednoznačný a polynom $x - c_i$ se zde objeví k_i-krát pro každé $i = 1, \ldots, s$. Označme g součin všech ostatních činitelů tohoto rozkladu, pak $f = g \cdot \prod_{i=1}^{s} (x - c_i)^{k_i}$, a tedy $\mathrm{st}(f) = \mathrm{st}(g) + \sum_{i=1}^{s} k_i$. Odtud $\sum_{i=1}^{s} k_i \leq \mathrm{st}(f)$.

Poznámka. Předchozí věta platí i za slabšího předpokladu, že R je obor integrity. Věta však neplatí obecně pro každý komutativní okruh R, například kvadratický polynom $x^2 - [1]_8 \in \mathbb{Z}_8[x]$ má v $\mathbb{Z}_8$ čtyři jednoduché kořeny $[1]_8$, $[-1]_8$, $[3]_8$, $[-3]_8$. V okruhu $\mathbb{Z}_8[x]$ totiž není rozkládání na součin normovaných ireducibilních činitelů jednoznačné: $x^2 - [1]_8 = (x + [1]_8)(x - [1]_8) = (x + [3]_8)(x - [3]_8)$.

Polynomiální funkce

Definice. Nechť R je okruh, pro pevně zvolený polynom $f \in R[x]$ definujme **polynomiální funkci určenou polynomem** f jako zobrazení $\varphi_f : R \to R$ dané předpisem $\varphi_f(c) = f(c)$ pro libovolné $c \in R$.

Polynomiální funkce

Definice. Nechť R je okruh, pro pevně zvolený polynom $f \in R[x]$ definujme **polynomiální funkci určenou polynomem** f jako zobrazení $\varphi_f : R \to R$ dané předpisem $\varphi_f(c) = f(c)$ pro libovolné $c \in R$.

Věta. *Nechť R je nekonečné těleso, $f, g \in R[x]$ libovolné. Jestliže $\varphi_f = \varphi_g$, pak $f = g$.* [Věta 6.12, str. 89]

Polynomiální funkce

Definice. Nechť R je okruh, pro pevně zvolený polynom $f \in R[x]$ definujme **polynomiální funkci určenou polynomem** f jako zobrazení $\varphi_f : R \to R$ dané předpisem $\varphi_f(c) = f(c)$ pro libovolné $c \in R$.

Věta. *Nechť R je nekonečné těleso, $f, g \in R[x]$ libovolné. Jestliže $\varphi_f = \varphi_g$, pak $f = g$.* [Věta 6.12, str. 89]

Důkaz. Předpokládejme $\varphi_f = \varphi_g$ a položme $h = f - g$, odkud $f = h + g$.

Polynomiální funkce

Definice. Nechť R je okruh, pro pevně zvolený polynom $f \in R[x]$ definujme **polynomiální funkci určenou polynomem** f jako zobrazení $\varphi_f : R \to R$ dané předpisem $\varphi_f(c) = f(c)$ pro libovolné $c \in R$.

Věta. *Nechť R je nekonečné těleso, $f, g \in R[x]$ libovolné. Jestliže $\varphi_f = \varphi_g$, pak $f = g$.* [Věta 6.12, str. 89]

Důkaz. Předpokládejme $\varphi_f = \varphi_g$ a položme $h = f - g$, odkud $f = h + g$. Pak pro libovolné $c \in R$ platí $f(c) = h(c) + g(c)$, a tedy $h(c) = f(c) - g(c) = \varphi_f(c) - \varphi_g(c) = 0$.

Polynomiální funkce

Definice. Nechť R je okruh, pro pevně zvolený polynom $f \in R[x]$ definujme **polynomiální funkci určenou polynomem** f jako zobrazení $\varphi_f : R \to R$ dané předpisem $\varphi_f(c) = f(c)$ pro libovolné $c \in R$.

Věta. *Nechť R je nekonečné těleso, $f, g \in R[x]$ libovolné. Jestliže $\varphi_f = \varphi_g$, pak $f = g$.* [Věta 6.12, str. 89]

Důkaz. Předpokládejme $\varphi_f = \varphi_g$ a položme $h = f - g$, odkud $f = h + g$. Pak pro libovolné $c \in R$ platí $f(c) = h(c) + g(c)$, a tedy $h(c) = f(c) - g(c) = \varphi_f(c) - \varphi_g(c) = 0$. Polynom h tedy má nekonečně mnoho kořenů, odkud podle předchozí věty plyne, že h je nulový polynom, tj. $f = g$.

Polynomiální funkce

Definice. Nechť R je okruh, pro pevně zvolený polynom $f \in R[x]$ definujme **polynomiální funkci určenou polynomem** f jako zobrazení $\varphi_f : R \to R$ dané předpisem $\varphi_f(c) = f(c)$ pro libovolné $c \in R$.

Věta. *Nechť R je nekonečné těleso, $f, g \in R[x]$ libovolné. Jestliže $\varphi_f = \varphi_g$, pak $f = g$.* [Věta 6.12, str. 89]

Důkaz. Předpokládejme $\varphi_f = \varphi_g$ a položme $h = f - g$, odkud $f = h + g$. Pak pro libovolné $c \in R$ platí $f(c) = h(c) + g(c)$, a tedy $h(c) = f(c) - g(c) = \varphi_f(c) - \varphi_g(c) = 0$. Polynom h tedy má nekonečně mnoho kořenů, odkud podle předchozí věty plyne, že h je nulový polynom, tj. $f = g$.

Příklad. Nad tělesem reálných čísel $\mathbb{R}$ libovolné dva různé polynomy určují různé polynomiální funkce.

Polynomiální funkce

Definice. Nechť R je okruh, pro pevně zvolený polynom $f \in R[x]$ definujme **polynomiální funkci určenou polynomem** f jako zobrazení $\varphi_f : R \to R$ dané předpisem $\varphi_f(c) = f(c)$ pro libovolné $c \in R$.

Věta. *Nechť R je nekonečné těleso, $f, g \in R[x]$ libovolné. Jestliže $\varphi_f = \varphi_g$, pak $f = g$.* [Věta 6.12, str. 89]

Důkaz. Předpokládejme $\varphi_f = \varphi_g$ a položme $h = f - g$, odkud $f = h + g$. Pak pro libovolné $c \in R$ platí $f(c) = h(c) + g(c)$, a tedy $h(c) = f(c) - g(c) = \varphi_f(c) - \varphi_g(c) = 0$. Polynom h tedy má nekonečně mnoho kořenů, odkud podle předchozí věty plyne, že h je nulový polynom, tj. $f = g$.

Příklad. Nad tělesem reálných čísel $\mathbb{R}$ libovolné dva různé polynomy určují různé polynomiální funkce.

Příklad. Předchozí věta neplatí, je-li R konečné těleso. Například pro $R = \mathbb{Z}_2$ určují polynomy x a x^2 stejnou polynomiální funkci.

Konečná podgrupa multiplikativní grupy tělesa

Definice. Nechť $(G, \cdot)$ je grupa. Existuje-li přirozené číslo e tak, že pro každé $a \in G$ platí $a^e = 1$, pak nejmenší přirozené číslo e s touto vlastností se nazývá **exponent** grupy G.

Věta. Nechť G je konečná komutativní grupa. Pak exponent grupy G je roven největšímu z řádů všech prvků grupy G.

Konečná podgrupa multiplikativní grupy tělesa

Definice. Nechť $(G, \cdot)$ je grupa. Existuje-li přirozené číslo e tak, že pro každé $a \in G$ platí $a^e = 1$, pak nejmenší přirozené číslo e s touto vlastností se nazývá **exponent** grupy G.

Věta. Nechť G je konečná komutativní grupa. Pak exponent grupy G je roven největšímu z řádů všech prvků grupy G.

Věta. Nechť R je těleso, G je konečná podgrupa multiplikativní grupy $(R^\times, \cdot)$. Pak G je cyklická grupa.

Konečná podgrupa multiplikativní grupy tělesa

Definice. Nechť $(G, \cdot)$ je grupa. Existuje-li přirozené číslo e tak, že pro každé $a \in G$ platí $a^e = 1$, pak nejmenší přirozené číslo e s touto vlastností se nazývá **exponent** grupy G.

Věta. Nechť G je konečná komutativní grupa. Pak exponent grupy G je roven největšímu z řádů všech prvků grupy G.

Věta. Nechť R je těleso, G je konečná podgrupa multiplikativní grupy $(R^\times, \cdot)$. Pak G je cyklická grupa.

Důkaz. Označme e exponent grupy G a $n = |G|$ její řád.

Konečná podgrupa multiplikativní grupy tělesa

Definice. Nechť $(G, \cdot)$ je grupa. Existuje-li přirozené číslo e tak, že pro každé $a \in G$ platí $a^e = 1$, pak nejmenší přirozené číslo e s touto vlastností se nazývá **exponent** grupy G.

Věta. Nechť G je konečná komutativní grupa. Pak exponent grupy G je roven největšímu z řádů všech prvků grupy G.

Věta. Nechť R je těleso, G je konečná podgrupa multiplikativní grupy $(R^\times, \cdot)$. Pak G je cyklická grupa.

Důkaz. Označme e exponent grupy G a $n = |G|$ její řád. Podle připomenuté věty existuje $g \in G$, jehož řád je e.

Konečná podgrupa multiplikativní grupy tělesa

Definice. Nechť $(G, \cdot)$ je grupa. Existuje-li přirozené číslo e tak, že pro každé $a \in G$ platí $a^e = 1$, pak nejmenší přirozené číslo e s touto vlastností se nazývá **exponent** grupy G.

Věta. Nechť G je konečná komutativní grupa. Pak exponent grupy G je roven největšímu z řádů všech prvků grupy G.

Věta. Nechť R je těleso, G je konečná podgrupa multiplikativní grupy $(R^\times, \cdot)$. Pak G je cyklická grupa.

Důkaz. Označme e exponent grupy G a $n = |G|$ její řád. Podle připomenuté věty existuje $g \in G$, jehož řád je e. Z Lagrangeovy věty pak $e \mid n$. Každý prvek grupy G je kořenem polynomu $x^e - 1$, a podle věty o počtu kořenů $n \leq \mathrm{st}(x^e - 1) = e$, proto $n = e$.

Konečná podgrupa multiplikativní grupy tělesa

Definice. Nechť $(G, \cdot)$ je grupa. Existuje-li přirozené číslo e tak, že pro každé $a \in G$ platí $a^e = 1$, pak nejmenší přirozené číslo e s touto vlastností se nazývá **exponent** grupy G.

Věta. Nechť G je konečná komutativní grupa. Pak exponent grupy G je roven největšímu z řádů všech prvků grupy G.

Věta. Nechť R je těleso, G je konečná podgrupa multiplikativní grupy $(R^\times, \cdot)$. Pak G je cyklická grupa.

Důkaz. Označme e exponent grupy G a $n = |G|$ její řád. Podle připomenuté věty existuje $g \in G$, jehož řád je e. Z Lagrangeovy věty pak $e \mid n$. Každý prvek grupy G je kořenem polynomu $x^e - 1$, a podle věty o počtu kořenů $n \leq \mathrm{st}(x^e - 1) = e$, proto $n = e$. Tedy $\langle g \rangle \subseteq G$ mají obě n prvků, tj. $G = \langle g \rangle$ je cyklická.

Konečná podgrupa multiplikativní grupy tělesa

Definice. Nechť $(G, \cdot)$ je grupa. Existuje-li přirozené číslo e tak, že pro každé $a \in G$ platí $a^e = 1$, pak nejmenší přirozené číslo e s touto vlastností se nazývá **exponent** grupy G.

Věta. Nechť G je konečná komutativní grupa. Pak exponent grupy G je roven největšímu z řádů všech prvků grupy G.

Věta. Nechť R je těleso, G je konečná podgrupa multiplikativní grupy $(R^\times, \cdot)$. Pak G je cyklická grupa.

Důkaz. Označme e exponent grupy G a $n = |G|$ její řád. Podle připomenuté věty existuje $g \in G$, jehož řád je e. Z Lagrangeovy věty pak $e \mid n$. Každý prvek grupy G je kořenem polynomu $x^e - 1$, a podle věty o počtu kořenů $n \leq \mathrm{st}(x^e - 1) = e$, proto $n = e$. Tedy $\langle g \rangle \subseteq G$ mají obě n prvků, tj. $G = \langle g \rangle$ je cyklická.

Důsledek. Nechť R je konečné těleso, pak je jeho multiplikativní grupa $(R^\times, \cdot)$ cyklická.

Konečná podgrupa multiplikativní grupy tělesa

Definice. Nechť $(G, \cdot)$ je grupa. Existuje-li přirozené číslo e tak, že pro každé $a \in G$ platí $a^e = 1$, pak nejmenší přirozené číslo e s touto vlastností se nazývá **exponent** grupy G.

Věta. Nechť G je konečná komutativní grupa. Pak exponent grupy G je roven největšímu z řádů všech prvků grupy G.

Věta. Nechť R je těleso, G je konečná podgrupa multiplikativní grupy $(R^\times, \cdot)$. Pak G je cyklická grupa.

Důkaz. Označme e exponent grupy G a $n = |G|$ její řád. Podle připomenuté věty existuje $g \in G$, jehož řád je e. Z Lagrangeovy věty pak $e \mid n$. Každý prvek grupy G je kořenem polynomu $x^e - 1$, a podle věty o počtu kořenů $n \leq \mathrm{st}(x^e - 1) = e$, proto $n = e$. Tedy $\langle g \rangle \subseteq G$ mají obě n prvků, tj. $G = \langle g \rangle$ je cyklická.

Důsledek. Nechť R je konečné těleso, pak je jeho multiplikativní grupa $(R^\times, \cdot)$ cyklická.

Důsledek. Pro libovolné prvočíslo p je grupa $(\mathbb{Z}_p^\times, \cdot)$ cyklická.

Derivace polynomu

Definice. Nechť R je okruh, $f = a_n \cdot x^n + \cdots + a_2 \cdot x^2 + a_1 \cdot x + a_0$ polynom z $R[x]$. **Derivací** polynomu f rozumíme polynom

$$f' = na_n \cdot x^{n-1} + \cdots + 2a_2 \cdot x + a_1.$$

Derivace polynomu

Definice. Nechť R je okruh, $f = a_n \cdot x^n + \cdots + a_2 \cdot x^2 + a_1 \cdot x + a_0$ polynom z $R[x]$. **Derivací** polynomu f rozumíme polynom

$$f' = na_n \cdot x^{n-1} + \cdots + 2a_2 \cdot x + a_1.$$

Poznámka. V tělese reálných čísel máme pojem limity, který v obecném okruhu není k dispozici.

Derivace polynomu

Definice. Nechť R je okruh, $f = a_n \cdot x^n + \cdots + a_2 \cdot x^2 + a_1 \cdot x + a_0$ polynom z $R[x]$. **Derivací** polynomu f rozumíme polynom

$$f' = na_n \cdot x^{n-1} + \cdots + 2a_2 \cdot x + a_1.$$

Poznámka. V tělese reálných čísel máme pojem limity, který v obecném okruhu není k dispozici. Proto jsme pojem derivace polynomu nemohli definovat limitou, ale jen uvedeným vzorcem, v němž například na_n znamená n-násobek prvku a_n (v grupě $(R, +)$ počítáme součet n sčítanců, z nichž každý je roven prvku a_n).

Derivace polynomu

Definice. Nechť R je okruh, $f = a_n \cdot x^n + \cdots + a_2 \cdot x^2 + a_1 \cdot x + a_0$ polynom z $R[x]$. **Derivací** polynomu f rozumíme polynom

$$f' = na_n \cdot x^{n-1} + \cdots + 2a_2 \cdot x + a_1.$$

Poznámka. V tělese reálných čísel máme pojem limity, který v obecném okruhu není k dispozici. Proto jsme pojem derivace polynomu nemohli definovat limitou, ale jen uvedeným vzorcem, v němž například na_n znamená n-násobek prvku a_n (v grupě $(R, +)$ počítáme součet n sčítanců, z nichž každý je roven prvku a_n).

Věta. Nechť R je okruh, $f, g \in R[x]$, $c \in R$, $n \in \mathbb{N}$. Pak platí

- $(f + g)' = f' + g'$,

Derivace polynomu

Definice. Nechť R je okruh, $f = a_n \cdot x^n + \cdots + a_2 \cdot x^2 + a_1 \cdot x + a_0$ polynom z $R[x]$. **Derivací** polynomu f rozumíme polynom

$$f' = na_n \cdot x^{n-1} + \cdots + 2a_2 \cdot x + a_1.$$

Poznámka. V tělese reálných čísel máme pojem limity, který v obecném okruhu není k dispozici. Proto jsme pojem derivace polynomu nemohli definovat limitou, ale jen uvedeným vzorcem, v němž například na_n znamená n-násobek prvku a_n (v grupě $(R, +)$ počítáme součet n sčítanců, z nichž každý je roven prvku a_n).

Věta. Nechť R je okruh, $f, g \in R[x]$, $c \in R$, $n \in \mathbb{N}$. Pak platí

- $(f + g)' = f' + g'$,
- $(f \cdot g)' = f' \cdot g + f \cdot g'$,

Derivace polynomu

Definice. Nechť R je okruh, $f = a_n \cdot x^n + \cdots + a_2 \cdot x^2 + a_1 \cdot x + a_0$ polynom z $R[x]$. **Derivací** polynomu f rozumíme polynom

$$f' = na_n \cdot x^{n-1} + \cdots + 2a_2 \cdot x + a_1.$$

Poznámka. V tělese reálných čísel máme pojem limity, který v obecném okruhu není k dispozici. Proto jsme pojem derivace polynomu nemohli definovat limitou, ale jen uvedeným vzorcem, v němž například na_n znamená n-násobek prvku a_n (v grupě $(R, +)$ počítáme součet n sčítanců, z nichž každý je roven prvku a_n).

Věta. Nechť R je okruh, $f, g \in R[x]$, $c \in R$, $n \in \mathbb{N}$. Pak platí

- $(f + g)' = f' + g'$,
- $(f \cdot g)' = f' \cdot g + f \cdot g'$,
- $((x - c)^n)' = n(x - c)^{n-1}$.

Derivace polynomu

Definice. Nechť R je okruh, $f = a_n \cdot x^n + \cdots + a_2 \cdot x^2 + a_1 \cdot x + a_0$ polynom z $R[x]$. **Derivací** polynomu f rozumíme polynom

$$f' = na_n \cdot x^{n-1} + \cdots + 2a_2 \cdot x + a_1.$$

Poznámka. V tělese reálných čísel máme pojem limity, který v obecném okruhu není k dispozici. Proto jsme pojem derivace polynomu nemohli definovat limitou, ale jen uvedeným vzorcem, v němž například na_n znamená n-násobek prvku a_n (v grupě $(R, +)$ počítáme součet n sčítanců, z nichž každý je roven prvku a_n).

Věta. Nechť R je okruh, $f, g \in R[x]$, $c \in R$, $n \in \mathbb{N}$. Pak platí

- $(f + g)' = f' + g'$,
- $(f \cdot g)' = f' \cdot g + f \cdot g'$,
- $((x - c)^n)' = n(x - c)^{n-1}$. [Věta 6.15, str. 89]

Označení. Druhou derivaci polynomu f značíme $f'' = (f')'$, třetí $f''' = (f'')'$ atd.

Derivace polynomu

Definice. Nechť R je okruh, $f = a_n \cdot x^n + \cdots + a_2 \cdot x^2 + a_1 \cdot x + a_0$ polynom z $R[x]$. **Derivací** polynomu f rozumíme polynom

$$f' = na_n \cdot x^{n-1} + \cdots + 2a_2 \cdot x + a_1.$$

Poznámka. V tělese reálných čísel máme pojem limity, který v obecném okruhu není k dispozici. Proto jsme pojem derivace polynomu nemohli definovat limitou, ale jen uvedeným vzorcem, v němž například na_n znamená n-násobek prvku a_n (v grupě $(R, +)$ počítáme součet n sčítanců, z nichž každý je roven prvku a_n).

Věta. Nechť R je okruh, $f, g \in R[x]$, $c \in R$, $n \in \mathbb{N}$. Pak platí

- $(f + g)' = f' + g'$,
- $(f \cdot g)' = f' \cdot g + f \cdot g'$,
- $((x - c)^n)' = n(x - c)^{n-1}$. [Věta 6.15, str. 89]

Označení. Druhou derivaci polynomu f značíme $f'' = (f')'$, třetí $f''' = (f'')'$ atd. Obecně pro $k \in \mathbb{N}$ pak k-tou derivaci polynomu f značíme $f^{(k)} = (f^{(k-1)})'$.

Derivace polynomu

Definice. Nechť R je okruh, $f = a_n \cdot x^n + \cdots + a_2 \cdot x^2 + a_1 \cdot x + a_0$ polynom z $R[x]$. **Derivací** polynomu f rozumíme polynom

$$f' = na_n \cdot x^{n-1} + \cdots + 2a_2 \cdot x + a_1.$$

Poznámka. V tělese reálných čísel máme pojem limity, který v obecném okruhu není k dispozici. Proto jsme pojem derivace polynomu nemohli definovat limitou, ale jen uvedeným vzorcem, v němž například na_n znamená n-násobek prvku a_n (v grupě $(R, +)$ počítáme součet n sčítanců, z nichž každý je roven prvku a_n).

Věta. Nechť R je okruh, $f, g \in R[x]$, $c \in R$, $n \in \mathbb{N}$. Pak platí

- $(f + g)' = f' + g'$,
- $(f \cdot g)' = f' \cdot g + f \cdot g'$,
- $((x - c)^n)' = n(x - c)^{n-1}$. [Věta 6.15, str. 89]

Označení. Druhou derivaci polynomu f značíme $f'' = (f')'$, třetí $f''' = (f'')'$ atd. Obecně pro $k \in \mathbb{N}$ pak k-tou derivaci polynomu f značíme $f^{(k)} = (f^{(k-1)})'$. Je tedy $f^{(1)} = f'$, $f^{(2)} = f''$, atd.

Souvislost derivace polynomu s násobností kořenů

Věta. *Nechť R je komutativní okruh, $f \in R[x]$, $c \in R$, $k \in \mathbb{N}$. Jestliže c je alespoň k-násobným kořenem polynomu f, pak je c kořenem polynomů f', f'', $\ldots$, $f^{(k-1)}$.*

Souvislost derivace polynomu s násobností kořenů

Věta. *Nechť R je komutativní okruh, $f \in R[x]$, $c \in R$, $k \in \mathbb{N}$. Jestliže c je alespoň k-násobným kořenem polynomu f, pak je c kořenem polynomů f', f'', $\ldots$, $f^{(k-1)}$.*

Důkaz. Existuje tedy $g \in R[x]$ tak, že $f = (x-c)^k \cdot g$, odkud $f' = k(x-c)^{k-1}g + (x-c)^k g' = (x-c)^{k-1}(kg + (x-c)\cdot g')$.

Souvislost derivace polynomu s násobností kořenů

Věta. *Nechť R je komutativní okruh, $f \in R[x]$, $c \in R$, $k \in \mathbb{N}$. Jestliže c je alespoň k-násobným kořenem polynomu f, pak je c kořenem polynomů f', f'', $\ldots$, $f^{(k-1)}$.*

Důkaz. Existuje tedy $g \in R[x]$ tak, že $f = (x-c)^k \cdot g$, odkud $f' = k(x-c)^{k-1}g + (x-c)^k g' = (x-c)^{k-1}(kg + (x-c)\cdot g')$. Je-li $k > 1$, je c alespoň $(k-1)$-násobným kořenem polynomu f'. Odtud věta plyne indukcí vůči k.

Souvislost derivace polynomu s násobností kořenů

Věta. *Nechť R je komutativní okruh, $f \in R[x]$, $c \in R$, $k \in \mathbb{N}$. Jestliže c je alespoň k-násobným kořenem polynomu f, pak je c kořenem polynomů f', f'', $\ldots$, $f^{(k-1)}$.*

Důkaz. Existuje tedy $g \in R[x]$ tak, že $f = (x-c)^k \cdot g$, odkud $f' = k(x-c)^{k-1}g + (x-c)^k g' = (x-c)^{k-1}(kg + (x-c)\cdot g')$. Je-li $k > 1$, je c alespoň $(k-1)$-násobným kořenem polynomu f'. Odtud věta plyne indukcí vůči k.

Poznámka. Každý vícenásobný kořen polynomu $f \in R[x]$, kde R je těleso, je také kořenem největšího společného dělitele (f, f').

Souvislost derivace polynomu s násobností kořenů

Věta. *Nechť R je komutativní okruh, $f \in R[x]$, $c \in R$, $k \in \mathbb{N}$. Jestliže c je alespoň k-násobným kořenem polynomu f, pak je c kořenem polynomů f', f'', $\ldots$, $f^{(k-1)}$.*

Důkaz. Existuje tedy $g \in R[x]$ tak, že $f = (x-c)^k \cdot g$, odkud $f' = k(x-c)^{k-1}g + (x-c)^k g' = (x-c)^{k-1}(kg + (x-c)\cdot g')$. Je-li $k > 1$, je c alespoň $(k-1)$-násobným kořenem polynomu f'. Odtud věta plyne indukcí vůči k.

Poznámka. Každý vícenásobný kořen polynomu $f \in R[x]$, kde R je těleso, je také kořenem největšího společného dělitele (f, f').

Věta. *Nechť R je těleso, $f \in R[x]$, $c \in R$, $k \in \mathbb{N}$. Předpokládejme, že* $\operatorname{char} R = 0$ *nebo* $\operatorname{char} R > k$. *Pak c je k-násobným kořenem polynomu f, právě když je c kořenem polynomů f, f', f'', $\ldots$, $f^{(k-1)}$ a není kořenem polynomu $f^{(k)}$.*

Souvislost derivace polynomu s násobností kořenů

Věta. *Nechť R je komutativní okruh, $f \in R[x]$, $c \in R$, $k \in \mathbb{N}$. Jestliže c je alespoň k-násobným kořenem polynomu f, pak je c kořenem polynomů f', f'', $\ldots$, $f^{(k-1)}$.*

Důkaz. Existuje tedy $g \in R[x]$ tak, že $f = (x-c)^k \cdot g$, odkud $f' = k(x-c)^{k-1}g + (x-c)^k g' = (x-c)^{k-1}(kg + (x-c)\cdot g')$. Je-li $k > 1$, je c alespoň $(k-1)$-násobným kořenem polynomu f'. Odtud věta plyne indukcí vůči k.

Poznámka. Každý vícenásobný kořen polynomu $f \in R[x]$, kde R je těleso, je také kořenem největšího společného dělitele (f, f').

Věta. *Nechť R je těleso, $f \in R[x]$, $c \in R$, $k \in \mathbb{N}$. Předpokládejme, že* char $R = 0$ *nebo* char $R > k$. *Pak c je k-násobným kořenem polynomu f, právě když je c kořenem polynomů f, f', f'', $\ldots$, $f^{(k-1)}$ a není kořenem polynomu $f^{(k)}$.*

Příklad. Předpoklad o charakteristice je nezbytný.

Souvislost derivace polynomu s násobností kořenů

Věta. *Nechť R je komutativní okruh, $f \in R[x]$, $c \in R$, $k \in \mathbb{N}$. Jestliže c je alespoň k-násobným kořenem polynomu f, pak je c kořenem polynomů f', f'', $\ldots$, $f^{(k-1)}$.*

Důkaz. Existuje tedy $g \in R[x]$ tak, že $f = (x-c)^k \cdot g$, odkud $f' = k(x-c)^{k-1}g + (x-c)^k g' = (x-c)^{k-1}(kg + (x-c)\cdot g')$. Je-li $k > 1$, je c alespoň $(k-1)$-násobným kořenem polynomu f'. Odtud věta plyne indukcí vůči k.

Poznámka. Každý vícenásobný kořen polynomu $f \in R[x]$, kde R je těleso, je také kořenem největšího společného dělitele (f, f').

Věta. *Nechť R je těleso, $f \in R[x]$, $c \in R$, $k \in \mathbb{N}$. Předpokládejme, že* char $R = 0$ *nebo* char $R > k$. *Pak c je k-násobným kořenem polynomu f, právě když je c kořenem polynomů f, f', f'', $\ldots$, $f^{(k-1)}$ a není kořenem polynomu $f^{(k)}$.*

Příklad. Předpoklad o charakteristice je nezbytný. Například pro $R = \mathbb{Z}_2$ polynom $f = x^2 \in \mathbb{Z}_2[x]$ má kořen $[0]_2$ násobnosti 2.

Souvislost derivace polynomu s násobností kořenů

Věta. *Nechť R je komutativní okruh, $f \in R[x]$, $c \in R$, $k \in \mathbb{N}$. Jestliže c je alespoň k-násobným kořenem polynomu f, pak je c kořenem polynomů f', f'', $\ldots$, $f^{(k-1)}$.*

Důkaz. Existuje tedy $g \in R[x]$ tak, že $f = (x-c)^k \cdot g$, odkud $f' = k(x-c)^{k-1}g + (x-c)^k g' = (x-c)^{k-1}(kg + (x-c)\cdot g')$. Je-li $k > 1$, je c alespoň $(k-1)$-násobným kořenem polynomu f'. Odtud věta plyne indukcí vůči k.

Poznámka. Každý vícenásobný kořen polynomu $f \in R[x]$, kde R je těleso, je také kořenem největšího společného dělitele (f, f').

Věta. *Nechť R je těleso, $f \in R[x]$, $c \in R$, $k \in \mathbb{N}$. Předpokládejme, že* $\operatorname{char} R = 0$ *nebo* $\operatorname{char} R > k$. *Pak c je k-násobným kořenem polynomu f, právě když je c kořenem polynomů f, f', f'', $\ldots$, $f^{(k-1)}$ a není kořenem polynomu $f^{(k)}$.*

Příklad. Předpoklad o charakteristice je nezbytný. Například pro $R = \mathbb{Z}_2$ polynom $f = x^2 \in \mathbb{Z}_2[x]$ má kořen $[0]_2$ násobnosti 2. Přitom $f' = 2[1]_2 x = 0$, a tedy $f^{(k)}([0]_2) = 0$ pro každé $k \in \mathbb{N}$.

Poznámka. Jev pozorovaný v předchozím příkladě platí obecněji: je-li $\operatorname{char} R = p > 0$, pak pro každé $f \in R[x]$ platí $f^{(p)} = 0$.

Poznámka. Jev pozorovaný v předchozím příkladě platí obecněji: je-li $\operatorname{char} R = p > 0$, pak pro každé $f \in R[x]$ platí $f^{(p)} = 0$.

Věta. *Nechť R je těleso, $f \in R[x]$, $c \in R$, $k \in \mathbb{N}$. Předpokládejme, že* $\operatorname{char} R = 0$ *nebo* $\operatorname{char} R > k$. *Pak c je k-násobným kořenem polynomu f, právě když je c kořenem polynomů f, f', f'', $\ldots$, $f^{(k-1)}$ a není kořenem polynomu $f^{(k)}$.*

Poznámka. Jev pozorovaný v předchozím příkladě platí obecněji: je-li $\operatorname{char} R = p > 0$, pak pro každé $f \in R[x]$ platí $f^{(p)} = 0$.

Věta. Nechť R je těleso, $f \in R[x]$, $c \in R$, $k \in \mathbb{N}$. Předpokládejme, že $\operatorname{char} R = 0$ nebo $\operatorname{char} R > k$. Pak c je k-násobným kořenem polynomu f, právě když je c kořenem polynomů f, f', f'', $\ldots$, $f^{(k-1)}$ a není kořenem polynomu $f^{(k)}$.

Důkaz. „$\Rightarrow$“ Existuje tedy $g \in R[x]$ tak, že $f = (x - c)^k \cdot g$, přičemž $(x - c) \nmid g$.

Poznámka. Jev pozorovaný v předchozím příkladě platí obecněji: je-li $\operatorname{char} R = p > 0$, pak pro každé $f \in R[x]$ platí $f^{(p)} = 0$.

Věta. Nechť R je těleso, $f \in R[x]$, $c \in R$, $k \in \mathbb{N}$. Předpokládejme, že $\operatorname{char} R = 0$ nebo $\operatorname{char} R > k$. Pak c je k-násobným kořenem polynomu f, právě když je c kořenem polynomů f, f', f'', $\ldots$, $f^{(k-1)}$ a není kořenem polynomu $f^{(k)}$.

Důkaz. „$\Rightarrow$“ Existuje tedy $g \in R[x]$ tak, že $f = (x-c)^k \cdot g$, přičemž $(x-c) \nmid g$. Pak $f' = (x-c)^{k-1}(kg + (x-c) \cdot g')$.

Poznámka. Jev pozorovaný v předchozím příkladě platí obecněji: je-li $\operatorname{char} R = p > 0$, pak pro každé $f \in R[x]$ platí $f^{(p)} = 0$.

Věta. Nechť R je těleso, $f \in R[x]$, $c \in R$, $k \in \mathbb{N}$. Předpokládejme, že $\operatorname{char} R = 0$ nebo $\operatorname{char} R > k$. Pak c je k-násobným kořenem polynomu f, právě když je c kořenem polynomů f, f', f'', $\ldots$, $f^{(k-1)}$ a není kořenem polynomu $f^{(k)}$.

Důkaz. „$\Rightarrow$“ Existuje tedy $g \in R[x]$ tak, že $f = (x-c)^k \cdot g$, přičemž $(x-c) \nmid g$. Pak $f' = (x-c)^{k-1}(kg + (x-c) \cdot g')$. Předpokládejme, že $(x-c)^k \mid f'$, pak z jednoznačnosti rozkladu plyne $(x-c) \mid kg$, existuje tedy $h \in R[x]$ tak, že $kg = (x-c) \cdot h$, odkud $g = (x-c) \cdot (k1)^{-1} \cdot h$, kde jsme využili předpokladu o charakteristice R zaručujícího $k1 \neq 0$.

Poznámka. Jev pozorovaný v předchozím příkladě platí obecněji: je-li $\operatorname{char} R = p > 0$, pak pro každé $f \in R[x]$ platí $f^{(p)} = 0$.

Věta. Nechť R je těleso, $f \in R[x]$, $c \in R$, $k \in \mathbb{N}$. Předpokládejme, že $\operatorname{char} R = 0$ nebo $\operatorname{char} R > k$. Pak c je k-násobným kořenem polynomu f, právě když je c kořenem polynomů f, f', f'', $\ldots$, $f^{(k-1)}$ a není kořenem polynomu $f^{(k)}$.

Důkaz. „$\Rightarrow$“ Existuje tedy $g \in R[x]$ tak, že $f = (x-c)^k \cdot g$, přičemž $(x-c) \nmid g$. Pak $f' = (x-c)^{k-1}(kg + (x-c) \cdot g')$. Předpokládejme, že $(x-c)^k \mid f'$, pak z jednoznačnosti rozkladu plyne $(x-c) \mid kg$, existuje tedy $h \in R[x]$ tak, že $kg = (x-c) \cdot h$, odkud $g = (x-c) \cdot (k1)^{-1} \cdot h$, kde jsme využili předpokladu o charakteristice R zaručujícího $k1 \neq 0$. Tedy $(x-c) \mid g$, spor.

Poznámka. Jev pozorovaný v předchozím příkladě platí obecněji: je-li $\operatorname{char} R = p > 0$, pak pro každé $f \in R[x]$ platí $f^{(p)} = 0$.

Věta. Nechť R je těleso, $f \in R[x]$, $c \in R$, $k \in \mathbb{N}$. Předpokládejme, že $\operatorname{char} R = 0$ nebo $\operatorname{char} R > k$. Pak c je k-násobným kořenem polynomu f, právě když je c kořenem polynomů f, f', f'', $\ldots$, $f^{(k-1)}$ a není kořenem polynomu $f^{(k)}$.

Důkaz. „$\Rightarrow$“ Existuje tedy $g \in R[x]$ tak, že $f = (x-c)^k \cdot g$, přičemž $(x-c) \nmid g$. Pak $f' = (x-c)^{k-1}(kg + (x-c) \cdot g')$. Předpokládejme, že $(x-c)^k \mid f'$, pak z jednoznačnosti rozkladu plyne $(x-c) \mid kg$, existuje tedy $h \in R[x]$ tak, že $kg = (x-c) \cdot h$, odkud $g = (x-c) \cdot (k1)^{-1} \cdot h$, kde jsme využili předpokladu o charakteristice R zaručujícího $k1 \neq 0$. Tedy $(x-c) \mid g$, spor. Tedy c je $(k-1)$-násobný kořen f', je-li $k > 1$, resp. c není kořenem f', je-li $k = 1$.

Poznámka. Jev pozorovaný v předchozím příkladě platí obecněji: je-li $\operatorname{char} R = p > 0$, pak pro každé $f \in R[x]$ platí $f^{(p)} = 0$.

Věta. Nechť R je těleso, $f \in R[x]$, $c \in R$, $k \in \mathbb{N}$. Předpokládejme, že $\operatorname{char} R = 0$ nebo $\operatorname{char} R > k$. Pak c je k-násobným kořenem polynomu f, právě když je c kořenem polynomů f, f', f'', $\ldots$, $f^{(k-1)}$ a není kořenem polynomu $f^{(k)}$.

Důkaz. „$\Rightarrow$“ Existuje tedy $g \in R[x]$ tak, že $f = (x-c)^k \cdot g$, přičemž $(x-c) \nmid g$. Pak $f' = (x-c)^{k-1}(kg + (x-c) \cdot g')$. Předpokládejme, že $(x-c)^k \mid f'$, pak z jednoznačnosti rozkladu plyne $(x-c) \mid kg$, existuje tedy $h \in R[x]$ tak, že $kg = (x-c) \cdot h$, odkud $g = (x-c) \cdot (k1)^{-1} \cdot h$, kde jsme využili předpokladu o charakteristice R zaručujícího $k1 \neq 0$. Tedy $(x-c) \mid g$, spor. Tedy c je $(k-1)$-násobný kořen f', je-li $k > 1$, resp. c není kořenem f', je-li $k = 1$. Odtud indukcí vůči k dostáváme, že c je kořenem polynomů f, f', f'', $\ldots$, $f^{(k-1)}$, ale ne polynomu $f^{(k)}$.

Poznámka. Jev pozorovaný v předchozím příkladě platí obecněji: je-li $\operatorname{char} R = p > 0$, pak pro každé $f \in R[x]$ platí $f^{(p)} = 0$.

Věta. Nechť R je těleso, $f \in R[x]$, $c \in R$, $k \in \mathbb{N}$. Předpokládejme, že $\operatorname{char} R = 0$ nebo $\operatorname{char} R > k$. Pak c je k-násobným kořenem polynomu f, právě když je c kořenem polynomů f, f', f'', $\ldots$, $f^{(k-1)}$ a není kořenem polynomu $f^{(k)}$.

Důkaz. „$\Rightarrow$“ Existuje tedy $g \in R[x]$ tak, že $f = (x-c)^k \cdot g$, přičemž $(x-c) \nmid g$. Pak $f' = (x-c)^{k-1}(kg + (x-c) \cdot g')$. Předpokládejme, že $(x-c)^k \mid f'$, pak z jednoznačnosti rozkladu plyne $(x-c) \mid kg$, existuje tedy $h \in R[x]$ tak, že $kg = (x-c) \cdot h$, odkud $g = (x-c) \cdot (k1)^{-1} \cdot h$, kde jsme využili předpokladu o charakteristice R zaručujícího $k1 \neq 0$. Tedy $(x-c) \mid g$, spor. Tedy c je $(k-1)$-násobný kořen f', je-li $k > 1$, resp. c není kořenem f', je-li $k = 1$. Odtud indukcí vůči k dostáváme, že c je kořenem polynomů f, f', f'', $\ldots$, $f^{(k-1)}$, ale ne polynomu $f^{(k)}$.
„$\Leftarrow$“ Označme n násobnost kořene c polynomu f.

Poznámka. Jev pozorovaný v předchozím příkladě platí obecněji: je-li $\operatorname{char} R = p > 0$, pak pro každé $f \in R[x]$ platí $f^{(p)} = 0$.

Věta. Nechť R je těleso, $f \in R[x]$, $c \in R$, $k \in \mathbb{N}$. Předpokládejme, že $\operatorname{char} R = 0$ nebo $\operatorname{char} R > k$. Pak c je k-násobným kořenem polynomu f, právě když je c kořenem polynomů f, f', f'', $\ldots$, $f^{(k-1)}$ a není kořenem polynomu $f^{(k)}$.

Důkaz. „$\Rightarrow$“ Existuje tedy $g \in R[x]$ tak, že $f = (x-c)^k \cdot g$, přičemž $(x-c) \nmid g$. Pak $f' = (x-c)^{k-1}(kg + (x-c) \cdot g')$. Předpokládejme, že $(x-c)^k \mid f'$, pak z jednoznačnosti rozkladu plyne $(x-c) \mid kg$, existuje tedy $h \in R[x]$ tak, že $kg = (x-c) \cdot h$, odkud $g = (x-c) \cdot (k1)^{-1} \cdot h$, kde jsme využili předpokladu o charakteristice R zaručujícího $k1 \neq 0$. Tedy $(x-c) \mid g$, spor. Tedy c je $(k-1)$-násobný kořen f', je-li $k > 1$, resp. c není kořenem f', je-li $k = 1$. Odtud indukcí vůči k dostáváme, že c je kořenem polynomů f, f', f'', $\ldots$, $f^{(k-1)}$, ale ne polynomu $f^{(k)}$.
„$\Leftarrow$“ Označme n násobnost kořene c polynomu f. Podle předchozí věty je c kořenem polynomů f, f', f'', $\ldots$, $f^{(n-1)}$.

Poznámka. Jev pozorovaný v předchozím příkladě platí obecněji: je-li $\operatorname{char} R = p > 0$, pak pro každé $f \in R[x]$ platí $f^{(p)} = 0$.

Věta. Nechť R je těleso, $f \in R[x]$, $c \in R$, $k \in \mathbb{N}$. Předpokládejme, že $\operatorname{char} R = 0$ nebo $\operatorname{char} R > k$. Pak c je k-násobným kořenem polynomu f, právě když je c kořenem polynomů f, f', f'', $\ldots$, $f^{(k-1)}$ a není kořenem polynomu $f^{(k)}$.

Důkaz. „$\Rightarrow$“ Existuje tedy $g \in R[x]$ tak, že $f = (x-c)^k \cdot g$, přičemž $(x-c) \nmid g$. Pak $f' = (x-c)^{k-1}(kg + (x-c) \cdot g')$. Předpokládejme, že $(x-c)^k \mid f'$, pak z jednoznačnosti rozkladu plyne $(x-c) \mid kg$, existuje tedy $h \in R[x]$ tak, že $kg = (x-c) \cdot h$, odkud $g = (x-c) \cdot (k1)^{-1} \cdot h$, kde jsme využili předpokladu o charakteristice R zaručujícího $k1 \neq 0$. Tedy $(x-c) \mid g$, spor. Tedy c je $(k-1)$-násobný kořen f', je-li $k > 1$, resp. c není kořenem f', je-li $k = 1$. Odtud indukcí vůči k dostáváme, že c je kořenem polynomů f, f', f'', $\ldots$, $f^{(k-1)}$, ale ne polynomu $f^{(k)}$. „$\Leftarrow$“ Označme n násobnost kořene c polynomu f. Podle předchozí věty je c kořenem polynomů f, f', f'', $\ldots$, $f^{(n-1)}$. Proto $n \leq k$, odkud v případě $\operatorname{char} R \neq 0$ plyne $\operatorname{char} R > n$.

Poznámka. Jev pozorovaný v předchozím příkladě platí obecněji: je-li $\operatorname{char} R = p > 0$, pak pro každé $f \in R[x]$ platí $f^{(p)} = 0$.

Věta. Nechť R je těleso, $f \in R[x]$, $c \in R$, $k \in \mathbb{N}$. Předpokládejme, že $\operatorname{char} R = 0$ nebo $\operatorname{char} R > k$. Pak c je k-násobným kořenem polynomu f, právě když je c kořenem polynomů f, f', f'', $\ldots$, $f^{(k-1)}$ a není kořenem polynomu $f^{(k)}$.

Důkaz. „$\Rightarrow$“ Existuje tedy $g \in R[x]$ tak, že $f = (x-c)^k \cdot g$, přičemž $(x-c) \nmid g$. Pak $f' = (x-c)^{k-1}(kg + (x-c) \cdot g')$. Předpokládejme, že $(x-c)^k \mid f'$, pak z jednoznačnosti rozkladu plyne $(x-c) \mid kg$, existuje tedy $h \in R[x]$ tak, že $kg = (x-c) \cdot h$, odkud $g = (x-c) \cdot (k1)^{-1} \cdot h$, kde jsme využili předpokladu o charakteristice R zaručujícího $k1 \neq 0$. Tedy $(x-c) \mid g$, spor. Tedy c je $(k-1)$-násobný kořen f', je-li $k > 1$, resp. c není kořenem f', je-li $k = 1$. Odtud indukcí vůči k dostáváme, že c je kořenem polynomů f, f', f'', $\ldots$, $f^{(k-1)}$, ale ne polynomu $f^{(k)}$. „$\Leftarrow$“ Označme n násobnost kořene c polynomu f. Podle předchozí věty je c kořenem polynomů f, f', f'', $\ldots$, $f^{(n-1)}$. Proto $n \leq k$, odkud v případě $\operatorname{char} R \neq 0$ plyne $\operatorname{char} R > n$. Můžeme tedy užít výše dokázaný směr této věty, z něhož porovnáním plyne $n = k$.

Polynomy nad $\mathbb{C}$

Věta (Základní věta algebry). *Každý nekonstantní polynom $f \in \mathbb{C}[x]$ má v $\mathbb{C}$ kořen.*

Polynomy nad $\mathbb{C}$

Věta (Základní věta algebry). *Každý nekonstantní polynom $f \in \mathbb{C}[x]$ má v $\mathbb{C}$ kořen.* [Věta 7.2, str. 93]

Definice. Těleso R se nazývá **algebraicky uzavřené**, jestliže každý nekonstantní polynom $f \in R[x]$ má v R kořen.

Polynomy nad $\mathbb{C}$

Věta (Základní věta algebry). *Každý nekonstantní polynom $f \in \mathbb{C}[x]$ má v $\mathbb{C}$ kořen.* [Věta 7.2, str. 93]

Definice. Těleso R se nazývá **algebraicky uzavřené**, jestliže každý nekonstantní polynom $f \in R[x]$ má v R kořen.

Příklad. Tělesa $\mathbb{R}$ a $\mathbb{Q}$ nejsou algebraicky uzavřená

Polynomy nad $\mathbb{C}$

Věta (Základní věta algebry). Každý nekonstantní polynom $f \in \mathbb{C}[x]$ má v $\mathbb{C}$ kořen. [Věta 7.2, str. 93]

Definice. Těleso R se nazývá **algebraicky uzavřené**, jestliže každý nekonstantní polynom $f \in R[x]$ má v R kořen.

Příklad. Tělesa $\mathbb{R}$ a $\mathbb{Q}$ nejsou algebraicky uzavřená, žádné konečné těleso není algebraicky uzavřené (je-li $R = \{r_1, \ldots, r_n\}$, pak $(x - r_1) \cdot \ \ldots \ \cdot (x - r_n) + 1$ nemá v R kořen).

Polynomy nad $\mathbb{C}$

Věta (Základní věta algebry). *Každý nekonstantní polynom $f \in \mathbb{C}[x]$ má v $\mathbb{C}$ kořen.* [Věta 7.2, str. 93]

Definice. Těleso R se nazývá **algebraicky uzavřené**, jestliže každý nekonstantní polynom $f \in R[x]$ má v R kořen.

Příklad. Tělesa $\mathbb{R}$ a $\mathbb{Q}$ nejsou algebraicky uzavřená, žádné konečné těleso není algebraicky uzavřené (je-li $R = \{r_1, \ldots, r_n\}$, pak $(x - r_1) \cdot \ \ldots \ \cdot (x - r_n) + 1$ nemá v R kořen).

Poznámka. Základní větu algebry lze tedy formulovat takto: $\mathbb{C}$ *je algebraicky uzavřené těleso*.

Polynomy nad $\mathbb{C}$

Věta (Základní věta algebry). *Každý nekonstantní polynom $f \in \mathbb{C}[x]$ má v $\mathbb{C}$ kořen.* [Věta 7.2, str. 93]

Definice. Těleso R se nazývá **algebraicky uzavřené**, jestliže každý nekonstantní polynom $f \in R[x]$ má v R kořen.

Příklad. Tělesa $\mathbb{R}$ a $\mathbb{Q}$ nejsou algebraicky uzavřená, žádné konečné těleso není algebraicky uzavřené (je-li $R = \{r_1, \ldots, r_n\}$, pak $(x - r_1) \cdot \ \ldots \ \cdot (x - r_n) + 1$ nemá v R kořen).

Poznámka. Základní větu algebry lze tedy formulovat takto: $\mathbb{C}$ *je algebraicky uzavřené těleso*.

Důsledek. *Pro libovolný polynom $f \in \mathbb{C}[x]$ platí: f je ireducibilní nad $\mathbb{C}$, právě když je f lineární.*

Polynomy nad $\mathbb{C}$

Věta (Základní věta algebry). *Každý nekonstantní polynom $f \in \mathbb{C}[x]$ má v $\mathbb{C}$ kořen.* [Věta 7.2, str. 93]

Definice. Těleso R se nazývá **algebraicky uzavřené**, jestliže každý nekonstantní polynom $f \in R[x]$ má v R kořen.

Příklad. Tělesa $\mathbb{R}$ a $\mathbb{Q}$ nejsou algebraicky uzavřená, žádné konečné těleso není algebraicky uzavřené (je-li $R = \{r_1, \ldots, r_n\}$, pak $(x - r_1) \cdot \ \ldots \ \cdot (x - r_n) + 1$ nemá v R kořen).

Poznámka. Základní větu algebry lze tedy formulovat takto: *$\mathbb{C}$ je algebraicky uzavřené těleso.*

Důsledek. *Pro libovolný polynom $f \in \mathbb{C}[x]$ platí: f je ireducibilní nad $\mathbb{C}$, právě když je f lineární.*

Důsledek. *Nechť $f \in \mathbb{C}[x]$ je normovaný polynom, $\mathrm{st}(f) = n \geq 1$. Pak existují $c_1, \ldots, c_n \in \mathbb{C}$ tak, že*

$$f = (x - c_1) \cdot \ \ldots \ \cdot (x - c_n).$$

Tento rozklad je navíc jednoznačný až na pořadí činitelů.

Polynomy nad $\mathbb{C}$ - Viètovy vztahy

Důsledek (Viète). *Nechť je dán normovaný polynom* $f = x^n + a_{n-1} \cdot x^{n-1} + \cdots + a_1 \cdot x + a_0 \in \mathbb{C}[x]$, *kde* $n \geq 1$, *nechť* $c_1, \ldots, c_n \in \mathbb{C}$ *jsou jeho kořeny (kde je každý uveden tolikrát, kolik je jeho násobnost). Pak platí*

$$-a_{n-1} = c_1 + \cdots + c_n,$$

Polynomy nad $\mathbb{C}$ - Viètovy vztahy

Důsledek (Viète). *Nechť je dán normovaný polynom* $f = x^n + a_{n-1} \cdot x^{n-1} + \cdots + a_1 \cdot x + a_0 \in \mathbb{C}[x]$, *kde* $n \geq 1$, *nechť* $c_1, \ldots, c_n \in \mathbb{C}$ *jsou jeho kořeny (kde je každý uveden tolikrát, kolik je jeho násobnost). Pak platí*

$$\begin{aligned} -a_{n-1} &= c_1 + \cdots + c_n, \\ a_{n-2} &= c_1c_2 + c_1c_3 + \cdots + c_1c_n + c_2c_3 + \cdots + c_{n-1}c_n, \end{aligned}$$

Polynomy nad $\mathbb{C}$ - Viètovy vztahy

Důsledek (Viète). *Nechť je dán normovaný polynom* $f = x^n + a_{n-1} \cdot x^{n-1} + \cdots + a_1 \cdot x + a_0 \in \mathbb{C}[x]$, *kde* $n \geq 1$, *nechť* $c_1, \ldots, c_n \in \mathbb{C}$ *jsou jeho kořeny (kde je každý uveden tolikrát, kolik je jeho násobnost). Pak platí*

$$\begin{aligned} -a_{n-1} &= c_1 + \cdots + c_n, \\ a_{n-2} &= c_1c_2 + c_1c_3 + \cdots + c_1c_n + c_2c_3 + \cdots + c_{n-1}c_n, \\ &\vdots \\ (-1)^k a_{n-k} &= \sum_{1 \leq i_1 < \cdots < i_k \leq n} c_{i_1} c_{i_2} \ldots c_{i_k}, \end{aligned}$$

Polynomy nad $\mathbb{C}$ - Viètovy vztahy

Důsledek (Viète). *Nechť je dán normovaný polynom* $f = x^n + a_{n-1} \cdot x^{n-1} + \cdots + a_1 \cdot x + a_0 \in \mathbb{C}[x]$, *kde* $n \geq 1$, *nechť* $c_1, \ldots, c_n \in \mathbb{C}$ *jsou jeho kořeny (kde je každý uveden tolikrát, kolik je jeho násobnost). Pak platí*

$$\begin{aligned}
-a_{n-1} &= c_1 + \cdots + c_n, \\
a_{n-2} &= c_1c_2 + c_1c_3 + \cdots + c_1c_n + c_2c_3 + \cdots + c_{n-1}c_n, \\
&\vdots \\
(-1)^k a_{n-k} &= \sum_{1 \leq i_1 < \cdots < i_k \leq n} c_{i_1} c_{i_2} \ldots c_{i_k}, \\
&\vdots \\
(-1)^n a_0 &= c_1 c_2 \ldots c_n.
\end{aligned}$$

Polynomy nad $\mathbb{C}$ - Viètovy vztahy

Důsledek (Viète). *Nechť je dán normovaný polynom* $f = x^n + a_{n-1} \cdot x^{n-1} + \cdots + a_1 \cdot x + a_0 \in \mathbb{C}[x]$, *kde* $n \geq 1$, *nechť* $c_1, \ldots, c_n \in \mathbb{C}$ *jsou jeho kořeny (kde je každý uveden tolikrát, kolik je jeho násobnost). Pak platí*

$$\begin{aligned}
-a_{n-1} &= c_1 + \cdots + c_n, \\
a_{n-2} &= c_1c_2 + c_1c_3 + \cdots + c_1c_n + c_2c_3 + \cdots + c_{n-1}c_n, \\
&\vdots \\
(-1)^k a_{n-k} &= \sum_{1 \leq i_1 < \cdots < i_k \leq n} c_{i_1} c_{i_2} \ldots c_{i_k}, \\
&\vdots \\
(-1)^n a_0 &= c_1 c_2 \ldots c_n.
\end{aligned}$$

[Věta 7.6, str. 94]

Poznámka. Výraz na pravé straně k-tého řádku lze popsat takto: vezmeme všechny k-prvkové podmnožiny množiny indexů $\{1, 2, \ldots, n\}$, pro každou z nich vynásobíme odpovídající kořeny a získané součiny sečteme.

Polynomy nad $\mathbb{R}$

Věta. *Zobrazení* $\alpha : \mathbb{C} \to \mathbb{C}$, *které každému komplexnímu číslu přiřadí číslo komplexně združené, tj.* $\alpha(c) = \overline{c}$ *pro každé* $c \in \mathbb{C}$, *je izomorfismus okruhů.*

Polynomy nad $\mathbb{R}$

Věta. *Zobrazení $\alpha : \mathbb{C} \to \mathbb{C}$, které každému komplexnímu číslu přiřadí číslo komplexně združené, tj. $\alpha(c) = \overline{c}$ pro každé $c \in \mathbb{C}$, je izomorfismus okruhů.*

Důsledek. *Je-li komplexní číslo c kořenem polynomu $f \in \mathbb{R}[x]$, pak i číslo $\overline{c}$ komplexně sdružené s číslem c je kořenem polynomu f.*

Polynomy nad $\mathbb{R}$

Věta. *Zobrazení $\alpha : \mathbb{C} \to \mathbb{C}$, které každému komplexnímu číslu přiřadí číslo komplexně združené, tj. $\alpha(c) = \overline{c}$ pro každé $c \in \mathbb{C}$, je izomorfismus okruhů.*

Důsledek. *Je-li komplexní číslo c kořenem polynomu $f \in \mathbb{R}[x]$, pak i číslo $\overline{c}$ komplexně sdružené s číslem c je kořenem polynomu f.*

[Věta 8.1, str. 97]

Věta. *Pro libovolný polynom $f \in \mathbb{R}[x]$ platí: f je ireducibilní nad $\mathbb{R}$, právě když je f lineární anebo je $f = ax^2 + bx + c$ kvadratický se záporným diskriminantem $b^2 - 4ac < 0$.*

Polynomy nad $\mathbb{R}$

Věta. *Zobrazení $\alpha : \mathbb{C} \to \mathbb{C}$, které každému komplexnímu číslu přiřadí číslo komplexně združené, tj. $\alpha(c) = \overline{c}$ pro každé $c \in \mathbb{C}$, je izomorfismus okruhů.*

Důsledek. *Je-li komplexní číslo c kořenem polynomu $f \in \mathbb{R}[x]$, pak i číslo $\overline{c}$ komplexně sdružené s číslem c je kořenem polynomu f.*

[Věta 8.1, str. 97]

Věta. *Pro libovolný polynom $f \in \mathbb{R}[x]$ platí: f je ireducibilní nad $\mathbb{R}$, právě když je f lineární anebo je $f = ax^2 + bx + c$ kvadratický se záporným diskriminantem $b^2 - 4ac < 0$.* [Věta 8.2, str. 97]

Důsledek. *Každý nekonstantní normovaný polynom $f \in \mathbb{R}[x]$ lze psát jako součin normovaných polynomů, které jsou lineární anebo kvadratické se záporným diskriminantem. Tento zápis je jednoznačný až na pořadí činitelů.*

Polynomy nad $\mathbb{Z}$

Věta. *Nechť* $f = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$ *je nekonstantní polynom stupně* n, *nechť* $r \in \mathbb{Z}$, $s \in \mathbb{N}$ *jsou čísla taková, že* $(r, s) = 1$ *a že* $\frac{r}{s} \in \mathbb{Q}$ *je kořen polynomu* f.

Polynomy nad $\mathbb{Z}$

Věta. *Nechť* $f = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$ *je nekonstantní polynom stupně* n, *nechť* $r \in \mathbb{Z}$, $s \in \mathbb{N}$ *jsou čísla taková, že* $(r, s) = 1$ *a že* $\frac{r}{s} \in \mathbb{Q}$ *je kořen polynomu* f. *Pak platí*

- $r \mid a_0$,

Polynomy nad $\mathbb{Z}$

Věta. *Nechť* $f = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$ *je nekonstantní polynom stupně* n, *nechť* $r \in \mathbb{Z}$, $s \in \mathbb{N}$ *jsou čísla taková, že* $(r, s) = 1$ *a že* $\frac{r}{s} \in \mathbb{Q}$ *je kořen polynomu* f. *Pak platí*

- $r \mid a_0$,
- $s \mid a_n$,

Polynomy nad $\mathbb{Z}$

Věta. *Nechť* $f = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$ *je nekonstantní polynom stupně* n, *nechť* $r \in \mathbb{Z}$, $s \in \mathbb{N}$ *jsou čísla taková, že* $(r, s) = 1$ *a že* $\frac{r}{s} \in \mathbb{Q}$ *je kořen polynomu* f. *Pak platí*

- $r \mid a_0$,
- $s \mid a_n$,
- *pro každé* $m \in \mathbb{Z}$ *platí* $(sm - r) \mid f(m)$.

Polynomy nad $\mathbb{Z}$

Věta. *Nechť* $f = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$ *je nekonstantní polynom stupně* n, *nechť* $r \in \mathbb{Z}$, $s \in \mathbb{N}$ *jsou čísla taková, že* $(r, s) = 1$ *a že* $\frac{r}{s} \in \mathbb{Q}$ *je kořen polynomu* f. *Pak platí*

- $r \mid a_0$,
- $s \mid a_n$,
- *pro každé* $m \in \mathbb{Z}$ *platí* $(sm - r) \mid f(m)$.

Důkaz. $0 = s^n \cdot f\left(\frac{r}{s}\right) = a_n r^n + a_{n-1} r^{n-1} s + \cdots + a_1 r s^{n-1} + a_0 s^n$.

Polynomy nad $\mathbb{Z}$

Věta. *Nechť* $f = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$ *je nekonstantní polynom stupně* n, *nechť* $r \in \mathbb{Z}$, $s \in \mathbb{N}$ *jsou čísla taková, že* $(r, s) = 1$ *a že* $\frac{r}{s} \in \mathbb{Q}$ *je kořen polynomu* f. *Pak platí*

- $r \mid a_0$,
- $s \mid a_n$,
- *pro každé* $m \in \mathbb{Z}$ *platí* $(sm - r) \mid f(m)$.

Důkaz. $0 = s^n \cdot f(\frac{r}{s}) = a_n r^n + a_{n-1} r^{n-1} s + \cdots + a_1 r s^{n-1} + a_0 s^n$.
Proto $r \mid a_0 s^n$, což díky $(r, s) = 1$ dává $r \mid a_0$.

Polynomy nad $\mathbb{Z}$

Věta. *Nechť* $f = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$ *je nekonstantní polynom stupně* n, *nechť* $r \in \mathbb{Z}$, $s \in \mathbb{N}$ *jsou čísla taková, že* $(r, s) = 1$ *a že* $\frac{r}{s} \in \mathbb{Q}$ *je kořen polynomu* f. *Pak platí*

- $r \mid a_0$,
- $s \mid a_n$,
- *pro každé* $m \in \mathbb{Z}$ *platí* $(sm - r) \mid f(m)$.

Důkaz. $0 = s^n \cdot f(\frac{r}{s}) = a_n r^n + a_{n-1} r^{n-1} s + \cdots + a_1 r s^{n-1} + a_0 s^n$.
Proto $r \mid a_0 s^n$, což díky $(r, s) = 1$ dává $r \mid a_0$.
Podobně $s \mid a_n r^n$, což díky $(r, s) = 1$ dává $s \mid a_n$.

Polynomy nad $\mathbb{Z}$

Věta. *Nechť* $f = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$ *je nekonstantní polynom stupně* n, *nechť* $r \in \mathbb{Z}$, $s \in \mathbb{N}$ *jsou čísla taková, že* $(r, s) = 1$ *a že* $\frac{r}{s} \in \mathbb{Q}$ *je kořen polynomu* f. *Pak platí*

- $r \mid a_0$,
- $s \mid a_n$,
- *pro každé* $m \in \mathbb{Z}$ *platí* $(sm - r) \mid f(m)$.

Důkaz. $0 = s^n \cdot f(\frac{r}{s}) = a_n r^n + a_{n-1} r^{n-1} s + \cdots + a_1 r s^{n-1} + a_0 s^n$.
Proto $r \mid a_0 s^n$, což díky $(r, s) = 1$ dává $r \mid a_0$.
Podobně $s \mid a_n r^n$, což díky $(r, s) = 1$ dává $s \mid a_n$.
Označme $d = sm - r$, pak $r = sm - d$, dosazením
$a_n(sm-d)^n + a_{n-1}(sm-d)^{n-1}s + \cdots + a_1(sm-d)s^{n-1} + a_0 s^n = 0$.

Polynomy nad $\mathbb{Z}$

Věta. *Nechť* $f = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$ *je nekonstantní polynom stupně* n, *nechť* $r \in \mathbb{Z}$, $s \in \mathbb{N}$ *jsou čísla taková, že* $(r,s) = 1$ *a že* $\frac{r}{s} \in \mathbb{Q}$ *je kořen polynomu* f. *Pak platí*

- $r \mid a_0$,
- $s \mid a_n$,
- *pro každé* $m \in \mathbb{Z}$ *platí* $(sm - r) \mid f(m)$.

Důkaz. $0 = s^n \cdot f(\frac{r}{s}) = a_n r^n + a_{n-1} r^{n-1} s + \cdots + a_1 r s^{n-1} + a_0 s^n$.
Proto $r \mid a_0 s^n$, což díky $(r,s) = 1$ dává $r \mid a_0$.
Podobně $s \mid a_n r^n$, což díky $(r,s) = 1$ dává $s \mid a_n$.
Označme $d = sm - r$, pak $r = sm - d$, dosazením
$a_n(sm-d)^n + a_{n-1}(sm-d)^{n-1}s + \cdots + a_1(sm-d)s^{n-1} + a_0 s^n = 0$.
Užitím binomické věty a vynecháním všech sčítanců dělitelných d dostaneme
$d \mid a_n(sm)^n + a_{n-1}(sm)^{n-1}s + \cdots + a_1(sm)s^{n-1} + a_0 s^n = f(m) \cdot s^n$.

Polynomy nad $\mathbb{Z}$

Věta. *Nechť* $f = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$ *je nekonstantní polynom stupně* n, *nechť* $r \in \mathbb{Z}$, $s \in \mathbb{N}$ *jsou čísla taková, že* $(r,s) = 1$ *a že* $\frac{r}{s} \in \mathbb{Q}$ *je kořen polynomu* f. *Pak platí*

- $r \mid a_0$,
- $s \mid a_n$,
- *pro každé* $m \in \mathbb{Z}$ *platí* $(sm - r) \mid f(m)$.

Důkaz. $0 = s^n \cdot f(\frac{r}{s}) = a_n r^n + a_{n-1} r^{n-1} s + \cdots + a_1 r s^{n-1} + a_0 s^n$.
Proto $r \mid a_0 s^n$, což díky $(r,s) = 1$ dává $r \mid a_0$.
Podobně $s \mid a_n r^n$, což díky $(r,s) = 1$ dává $s \mid a_n$.
Označme $d = sm - r$, pak $r = sm - d$, dosazením
$a_n(sm-d)^n + a_{n-1}(sm-d)^{n-1}s + \cdots + a_1(sm-d)s^{n-1} + a_0 s^n = 0$.
Užitím binomické věty a vynecháním všech sčítanců dělitelných d dostaneme
$d \mid a_n(sm)^n + a_{n-1}(sm)^{n-1}s + \cdots + a_1(sm)s^{n-1} + a_0 s^n = f(m) \cdot s^n$.
Každé prvočíslo dělící současně d i s musí dělit také r.

Polynomy nad $\mathbb{Z}$

Věta. *Nechť* $f = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$ *je nekonstantní polynom stupně* n, *nechť* $r \in \mathbb{Z}$, $s \in \mathbb{N}$ *jsou čísla taková, že* $(r,s) = 1$ *a že* $\frac{r}{s} \in \mathbb{Q}$ *je kořen polynomu* f. *Pak platí*

- $r \mid a_0$,
- $s \mid a_n$,
- *pro každé* $m \in \mathbb{Z}$ *platí* $(sm - r) \mid f(m)$.

Důkaz. $0 = s^n \cdot f(\frac{r}{s}) = a_n r^n + a_{n-1} r^{n-1} s + \cdots + a_1 r s^{n-1} + a_0 s^n$.
Proto $r \mid a_0 s^n$, což díky $(r,s) = 1$ dává $r \mid a_0$.
Podobně $s \mid a_n r^n$, což díky $(r,s) = 1$ dává $s \mid a_n$.
Označme $d = sm - r$, pak $r = sm - d$, dosazením
$a_n(sm-d)^n + a_{n-1}(sm-d)^{n-1}s + \cdots + a_1(sm-d)s^{n-1} + a_0 s^n = 0$.
Užitím binomické věty a vynecháním všech sčítanců dělitelných d dostaneme
$d \mid a_n(sm)^n + a_{n-1}(sm)^{n-1}s + \cdots + a_1(sm)s^{n-1} + a_0 s^n = f(m) \cdot s^n$.
Každé prvočíslo dělící současně d i s musí dělit také r. Ovšem takové prvočíslo neexistuje, tedy $(d,s) = 1$.

Polynomy nad $\mathbb{Z}$

Věta. *Nechť* $f = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$ *je nekonstantní polynom stupně* n, *nechť* $r \in \mathbb{Z}$, $s \in \mathbb{N}$ *jsou čísla taková, že* $(r,s) = 1$ *a že* $\frac{r}{s} \in \mathbb{Q}$ *je kořen polynomu* f. *Pak platí*

- $r \mid a_0$,
- $s \mid a_n$,
- *pro každé* $m \in \mathbb{Z}$ *platí* $(sm - r) \mid f(m)$.

Důkaz. $0 = s^n \cdot f(\frac{r}{s}) = a_n r^n + a_{n-1} r^{n-1} s + \cdots + a_1 r s^{n-1} + a_0 s^n$.
Proto $r \mid a_0 s^n$, což díky $(r,s) = 1$ dává $r \mid a_0$.
Podobně $s \mid a_n r^n$, což díky $(r,s) = 1$ dává $s \mid a_n$.
Označme $d = sm - r$, pak $r = sm - d$, dosazením
$a_n(sm-d)^n + a_{n-1}(sm-d)^{n-1}s + \cdots + a_1(sm-d)s^{n-1} + a_0 s^n = 0$.
Užitím binomické věty a vynecháním všech sčítanců dělitelných d dostaneme
$d \mid a_n(sm)^n + a_{n-1}(sm)^{n-1}s + \cdots + a_1(sm)s^{n-1} + a_0 s^n = f(m) \cdot s^n$.
Každé prvočíslo dělící současně d i s musí dělit také r. Ovšem takové prvočíslo neexistuje, tedy $(d,s) = 1$. Proto $d \mid f(m)$.

Polynomy nad $\mathbb{Z}$ - hledání racionálních kořenů

Poznámka. Předchozí větu používáme pro nalezení všech racionálních kořenů daného polynomu s celočíselnými koeficienty a nenulovým absolutním členem: první dvě podmínky totiž dávají jen konečně mnoho možných hodnot pro r, s.

Polynomy nad $\mathbb{Z}$ - hledání racionálních kořenů

Poznámka. Předchozí větu používáme pro nalezení všech racionálních kořenů daného polynomu s celočíselnými koeficienty a nenulovým absolutním členem: první dvě podmínky totiž dávají jen konečně mnoho možných hodnot pro r, s. Pro každou z možných dvojic r, s lze zjistit dosazením, zda $\frac{r}{s}$ je kořenem f.

Polynomy nad $\mathbb{Z}$ - hledání racionálních kořenů

Poznámka. Předchozí větu používáme pro nalezení všech racionálních kořenů daného polynomu s celočíselnými koeficienty a nenulovým absolutním členem: první dvě podmínky totiž dávají jen konečně mnoho možných hodnot pro r, s. Pro každou z možných dvojic r, s lze zjistit dosazením, zda $\frac{r}{s}$ je kořenem f. V případě velkého počtu dvojic je možné některé dvojice eliminovat třetí podmínkou, například testovat, zda platí $(s + r) \mid f(-1)$ a $(s - r) \mid f(1)$.

Polynomy nad $\mathbb{Z}$ - hledání racionálních kořenů

Poznámka. Předchozí větu používáme pro nalezení všech racionálních kořenů daného polynomu s celočíselnými koeficienty a nenulovým absolutním členem: první dvě podmínky totiž dávají jen konečně mnoho možných hodnot pro r, s. Pro každou z možných dvojic r, s lze zjistit dosazením, zda $\frac{r}{s}$ je kořenem f. V případě velkého počtu dvojic je možné některé dvojice eliminovat třetí podmínkou, například testovat, zda platí $(s + r) \mid f(-1)$ a $(s - r) \mid f(1)$.

Zmíněná podmínka nenulovosti absolutního členu není nijak omezující: libovolný nenulový polynom lze rozložit na součin mocniny x a polynomu s nenulovým absolutním členem.

Polynomy nad $\mathbb{Z}$

Definice. Nechť $f = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$ je nenulový. Řekneme, že f je **primitivní**, jestliže jeho koeficienty jsou nesoudělné, tj. $(a_0, a_1, \ldots, a_n) = 1$.

Polynomy nad $\mathbb{Z}$

Definice. Nechť $f = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$ je nenulový. Řekneme, že f je **primitivní**, jestliže jeho koeficienty jsou nesoudělné, tj. $(a_0, a_1, \ldots, a_n) = 1$.

Věta (Gaussovo lemma). Součin libovolných dvou primitivních polynomů je primitivní polynom.

Polynomy nad $\mathbb{Z}$

Definice. Nechť $f = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$ je nenulový. Řekneme, že f je **primitivní**, jestliže jeho koeficienty jsou nesoudělné, tj. $(a_0, a_1, \ldots, a_n) = 1$.

Věta (Gaussovo lemma). Součin libovolných dvou primitivních polynomů je primitivní polynom.

Důkaz sporem. Přepokládejme, že $f, g \in \mathbb{Z}[x]$ jsou primitivní polynomy takové, že jejich součin $f \cdot g$ primitivní není.

Polynomy nad $\mathbb{Z}$

Definice. Nechť $f = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$ je nenulový. Řekneme, že f je **primitivní**, jestliže jeho koeficienty jsou nesoudělné, tj. $(a_0, a_1, \ldots, a_n) = 1$.

Věta (Gaussovo lemma). Součin libovolných dvou primitivních polynomů je primitivní polynom.

Důkaz sporem. Přepokládejme, že $f, g \in \mathbb{Z}[x]$ jsou primitivní polynomy takové, že jejich součin $f \cdot g$ primitivní není. Pak existuje prvočíslo p, které dělí všechny koeficienty polynomu $f \cdot g$.

Polynomy nad $\mathbb{Z}$

Definice. Nechť $f = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$ je nenulový. Řekneme, že f je **primitivní**, jestliže jeho koeficienty jsou nesoudělné, tj. $(a_0, a_1, \ldots, a_n) = 1$.

Věta (Gaussovo lemma). Součin libovolných dvou primitivních polynomů je primitivní polynom.

Důkaz sporem. Přepokládejme, že $f, g \in \mathbb{Z}[x]$ jsou primitivní polynomy takové, že jejich součin $f \cdot g$ primitivní není. Pak existuje prvočíslo p, které dělí všechny koeficienty polynomu $f \cdot g$.
Zobrazení $\alpha : \mathbb{Z}[x] \to \mathbb{Z}_p[x]$ určené předpisem

$$\alpha(a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0) = \\ = [a_n]_p x^n + [a_{n-1}]_p x^{n-1} + \cdots + [a_1]_p x + [a_0]_p$$

pro libovolné $a_0, a_1, \ldots, a_n \in \mathbb{Z}$ (tedy každý koeficient je nahrazen odpovídající zbytkovou třídou) je homomorfismus okruhů.

Polynomy nad $\mathbb{Z}$

Definice. Nechť $f = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$ je nenulový. Řekneme, že f je **primitivní**, jestliže jeho koeficienty jsou nesoudělné, tj. $(a_0, a_1, \ldots, a_n) = 1$.

Věta (Gaussovo lemma). Součin libovolných dvou primitivních polynomů je primitivní polynom.

Důkaz sporem. Přepokládejme, že $f, g \in \mathbb{Z}[x]$ jsou primitivní polynomy takové, že jejich součin $f \cdot g$ primitivní není. Pak existuje prvočíslo p, které dělí všechny koeficienty polynomu $f \cdot g$.
Zobrazení $\alpha : \mathbb{Z}[x] \to \mathbb{Z}_p[x]$ určené předpisem

$$\alpha(a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0) = \\ = [a_n]_p x^n + [a_{n-1}]_p x^{n-1} + \cdots + [a_1]_p x + [a_0]_p$$

pro libovolné $a_0, a_1, \ldots, a_n \in \mathbb{Z}$ (tedy každý koeficient je nahrazen odpovídající zbytkovou třídou) je homomorfismus okruhů. Pak $\alpha(f) \neq 0$, $\alpha(g) \neq 0$, $\alpha(f) \cdot \alpha(g) = \alpha(f \cdot g) = 0$, což je spor s tím, že $\mathbb{Z}_p$ je těleso, a tedy $\mathbb{Z}_p[x]$ je obor integrity.

Polynomy nad $\mathbb{Z}$ - ireducibilita

Věta (Gauss). Libovolný polynom $f \in \mathbb{Z}[x]$ je ireducibilní nad $\mathbb{Z}$, právě když je ireducibilní nad $\mathbb{Q}$.

Polynomy nad $\mathbb{Z}$ - ireducibilita

Věta (Gauss). Libovolný polynom $f \in \mathbb{Z}[x]$ je ireducibilní nad $\mathbb{Z}$, právě když je ireducibilní nad $\mathbb{Q}$.

Důkaz. Tvrzení je zřejmé pro konstantní polynom f, který není ireducibilní ani nad $\mathbb{Z}$ ani nad $\mathbb{Q}$.

Polynomy nad $\mathbb{Z}$ - ireducibilita

Věta (Gauss). Libovolný polynom $f \in \mathbb{Z}[x]$ je ireducibilní nad $\mathbb{Z}$, právě když je ireducibilní nad $\mathbb{Q}$.

Důkaz. Tvrzení je zřejmé pro konstantní polynom f, který není ireducibilní ani nad $\mathbb{Z}$ ani nad $\mathbb{Q}$. Nechť je tedy f nekonstantní.

Polynomy nad $\mathbb{Z}$ - ireducibilita

Věta (Gauss). Libovolný polynom $f \in \mathbb{Z}[x]$ je ireducibilní nad $\mathbb{Z}$, právě když je ireducibilní nad $\mathbb{Q}$.

Důkaz. Tvrzení je zřejmé pro konstantní polynom f, který není ireducibilní ani nad $\mathbb{Z}$ ani nad $\mathbb{Q}$. Nechť je tedy f nekonstantní. Jestliže f není ireducibilní nad $\mathbb{Z}$, je možné jej psát jako součin dvou nekonstantních polynomů v $\mathbb{Z}[x]$.

Polynomy nad $\mathbb{Z}$ - ireducibilita

Věta (Gauss). Libovolný polynom $f \in \mathbb{Z}[x]$ je ireducibilní nad $\mathbb{Z}$, právě když je ireducibilní nad $\mathbb{Q}$.

Důkaz. Tvrzení je zřejmé pro konstantní polynom f, který není ireducibilní ani nad $\mathbb{Z}$ ani nad $\mathbb{Q}$. Nechť je tedy f nekonstantní. Jestliže f není ireducibilní nad $\mathbb{Z}$, je možné jej psát jako součin dvou nekonstantních polynomů v $\mathbb{Z}[x]$. Tyto polynomy jsou i z $\mathbb{Q}[x]$, a tedy f není ireducibilní nad $\mathbb{Q}$.

Polynomy nad $\mathbb{Z}$ - ireducibilita

Věta (Gauss). Libovolný polynom $f \in \mathbb{Z}[x]$ je ireducibilní nad $\mathbb{Z}$, právě když je ireducibilní nad $\mathbb{Q}$.

Důkaz. Tvrzení je zřejmé pro konstantní polynom f, který není ireducibilní ani nad $\mathbb{Z}$ ani nad $\mathbb{Q}$. Nechť je tedy f nekonstantní. Jestliže f není ireducibilní nad $\mathbb{Z}$, je možné jej psát jako součin dvou nekonstantních polynomů v $\mathbb{Z}[x]$. Tyto polynomy jsou i z $\mathbb{Q}[x]$, a tedy f není ireducibilní nad $\mathbb{Q}$.
Předpokládejme tedy naopak, že f není ireducibilní nad $\mathbb{Q}$.

Polynomy nad $\mathbb{Z}$ - ireducibilita

Věta (Gauss). *Libovolný polynom $f \in \mathbb{Z}[x]$ je ireducibilní nad $\mathbb{Z}$, právě když je ireducibilní nad $\mathbb{Q}$.*

Důkaz. Tvrzení je zřejmé pro konstantní polynom f, který není ireducibilní ani nad $\mathbb{Z}$ ani nad $\mathbb{Q}$. Nechť je tedy f nekonstantní. Jestliže f není ireducibilní nad $\mathbb{Z}$, je možné jej psát jako součin dvou nekonstantních polynomů v $\mathbb{Z}[x]$. Tyto polynomy jsou i z $\mathbb{Q}[x]$, a tedy f není ireducibilní nad $\mathbb{Q}$.
Předpokládejme tedy naopak, že f není ireducibilní nad $\mathbb{Q}$. Pak tedy $f = g \cdot h$ pro vhodné nekonstantní polynomy $f, g \in \mathbb{Q}[x]$.

Polynomy nad $\mathbb{Z}$ - ireducibilita

Věta (Gauss). *Libovolný polynom $f \in \mathbb{Z}[x]$ je ireducibilní nad $\mathbb{Z}$, právě když je ireducibilní nad $\mathbb{Q}$.*

Důkaz. Tvrzení je zřejmé pro konstantní polynom f, který není ireducibilní ani nad $\mathbb{Z}$ ani nad $\mathbb{Q}$. Nechť je tedy f nekonstantní. Jestliže f není ireducibilní nad $\mathbb{Z}$, je možné jej psát jako součin dvou nekonstantních polynomů v $\mathbb{Z}[x]$. Tyto polynomy jsou i z $\mathbb{Q}[x]$, a tedy f není ireducibilní nad $\mathbb{Q}$.
Předpokládejme tedy naopak, že f není ireducibilní nad $\mathbb{Q}$. Pak tedy $f = g \cdot h$ pro vhodné nekonstantní polynomy $f, g \in \mathbb{Q}[x]$. Existují nenulová racionální čísla b, c tak, že $b \cdot g$ a $c \cdot h$ jsou primitivní.

Polynomy nad $\mathbb{Z}$ - ireducibilita

Věta (Gauss). *Libovolný polynom $f \in \mathbb{Z}[x]$ je ireducibilní nad $\mathbb{Z}$, právě když je ireducibilní nad $\mathbb{Q}$.*

Důkaz. Tvrzení je zřejmé pro konstantní polynom f, který není ireducibilní ani nad $\mathbb{Z}$ ani nad $\mathbb{Q}$. Nechť je tedy f nekonstantní. Jestliže f není ireducibilní nad $\mathbb{Z}$, je možné jej psát jako součin dvou nekonstantních polynomů v $\mathbb{Z}[x]$. Tyto polynomy jsou i z $\mathbb{Q}[x]$, a tedy f není ireducibilní nad $\mathbb{Q}$.
Předpokládejme tedy naopak, že f není ireducibilní nad $\mathbb{Q}$. Pak tedy $f = g \cdot h$ pro vhodné nekonstantní polynomy $f, g \in \mathbb{Q}[x]$. Existují nenulová racionální čísla b, c tak, že $b \cdot g$ a $c \cdot h$ jsou primitivní. Podle Gaussova lemmatu je i $(b \cdot g)(c \cdot h) = (bc) \cdot f$ primitivní.

Polynomy nad $\mathbb{Z}$ - ireducibilita

Věta (Gauss). Libovolný polynom $f \in \mathbb{Z}[x]$ je ireducibilní nad $\mathbb{Z}$, právě když je ireducibilní nad $\mathbb{Q}$.

Důkaz. Tvrzení je zřejmé pro konstantní polynom f, který není ireducibilní ani nad $\mathbb{Z}$ ani nad $\mathbb{Q}$. Nechť je tedy f nekonstantní. Jestliže f není ireducibilní nad $\mathbb{Z}$, je možné jej psát jako součin dvou nekonstantních polynomů v $\mathbb{Z}[x]$. Tyto polynomy jsou i z $\mathbb{Q}[x]$, a tedy f není ireducibilní nad $\mathbb{Q}$.
Předpokládejme tedy naopak, že f není ireducibilní nad $\mathbb{Q}$. Pak tedy $f = g \cdot h$ pro vhodné nekonstantní polynomy $f, g \in \mathbb{Q}[x]$. Existují nenulová racionální čísla b, c tak, že $b \cdot g$ a $c \cdot h$ jsou primitivní. Podle Gaussova lemmatu je i $(b \cdot g)(c \cdot h) = (bc) \cdot f$ primitivní. Existují nesoudělná $u, v \in \mathbb{N}$ tak, že $bc = \pm\frac{u}{v}$.

Polynomy nad $\mathbb{Z}$ - ireducibilita

Věta (Gauss). Libovolný polynom $f \in \mathbb{Z}[x]$ je ireducibilní nad $\mathbb{Z}$, právě když je ireducibilní nad $\mathbb{Q}$.

Důkaz. Tvrzení je zřejmé pro konstantní polynom f, který není ireducibilní ani nad $\mathbb{Z}$ ani nad $\mathbb{Q}$. Nechť je tedy f nekonstantní. Jestliže f není ireducibilní nad $\mathbb{Z}$, je možné jej psát jako součin dvou nekonstantních polynomů v $\mathbb{Z}[x]$. Tyto polynomy jsou i z $\mathbb{Q}[x]$, a tedy f není ireducibilní nad $\mathbb{Q}$.
Předpokládejme tedy naopak, že f není ireducibilní nad $\mathbb{Q}$. Pak tedy $f = g \cdot h$ pro vhodné nekonstantní polynomy $f, g \in \mathbb{Q}[x]$. Existují nenulová racionální čísla b, c tak, že $b \cdot g$ a $c \cdot h$ jsou primitivní. Podle Gaussova lemmatu je i $(b \cdot g)(c \cdot h) = (bc) \cdot f$ primitivní. Existují nesoudělná $u, v \in \mathbb{N}$ tak, že $bc = \pm\frac{u}{v}$. Kdyby $u \neq 1$, bylo by u dělitelné nějakým prvočíslem p, které by pak dělilo všechny koeficienty polynomu uf a z $p \nmid v$ bychom dostali, že $(bc) \cdot f$ není primitivní.

Polynomy nad $\mathbb{Z}$ - ireducibilita

Věta (Gauss). Libovolný polynom $f \in \mathbb{Z}[x]$ je ireducibilní nad $\mathbb{Z}$, právě když je ireducibilní nad $\mathbb{Q}$.

Důkaz. Tvrzení je zřejmé pro konstantní polynom f, který není ireducibilní ani nad $\mathbb{Z}$ ani nad $\mathbb{Q}$. Nechť je tedy f nekonstantní. Jestliže f není ireducibilní nad $\mathbb{Z}$, je možné jej psát jako součin dvou nekonstantních polynomů v $\mathbb{Z}[x]$. Tyto polynomy jsou i z $\mathbb{Q}[x]$, a tedy f není ireducibilní nad $\mathbb{Q}$.
Předpokládejme tedy naopak, že f není ireducibilní nad $\mathbb{Q}$. Pak tedy $f = g \cdot h$ pro vhodné nekonstantní polynomy $f, g \in \mathbb{Q}[x]$. Existují nenulová racionální čísla b, c tak, že $b \cdot g$ a $c \cdot h$ jsou primitivní. Podle Gaussova lemmatu je i $(b \cdot g)(c \cdot h) = (bc) \cdot f$ primitivní. Existují nesoudělná $u, v \in \mathbb{N}$ tak, že $bc = \pm\frac{u}{v}$. Kdyby $u \neq 1$, bylo by u dělitelné nějakým prvočíslem p, které by pak dělilo všechny koeficienty polynomu uf a z $p \nmid v$ bychom dostali, že $(bc) \cdot f$ není primitivní. Proto $u = 1$ a $f = (\pm v \cdot (b \cdot g)) \cdot (c \cdot h)$ je rozklad f na součin dvou nekonstantních polynomů v $\mathbb{Z}[x]$, a tedy f není ireducibilní nad $\mathbb{Z}$.

Polynomy nad $\mathbb{Z}$ - ireducibilita

Věta (Eisensteinovo kriterium). *Nechť* $f = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$ *je nekonstantní polynom stupně* n.

Polynomy nad $\mathbb{Z}$ - ireducibilita

Věta (Eisensteinovo kriterium). *Nechť* $f = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$ *je nekonstantní polynom stupně* n. *Jestliže existuje prvočíslo* p *takové, že*

- $p \mid a_{n-1}$, $p \mid a_{n-2}$, $\ldots$, $p \mid a_1$, $p \mid a_0$,

Polynomy nad $\mathbb{Z}$ - ireducibilita

Věta (Eisensteinovo kriterium). *Nechť* $f = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$ *je nekonstantní polynom stupně* n. *Jestliže existuje prvočíslo* p *takové, že*

- $p \mid a_{n-1}$, $p \mid a_{n-2}$, $\ldots$, $p \mid a_1$, $p \mid a_0$,
- $p \nmid a_n$,

Polynomy nad $\mathbb{Z}$ - ireducibilita

Věta (Eisensteinovo kriterium). *Nechť* $f = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$ *je nekonstantní polynom stupně* n. *Jestliže existuje prvočíslo* p *takové, že*

- $p \mid a_{n-1}$, $p \mid a_{n-2}$, $\ldots$, $p \mid a_1$, $p \mid a_0$,
- $p \nmid a_n$,
- $p^2 \nmid a_0$,

Polynomy nad $\mathbb{Z}$ - ireducibilita

Věta (Eisensteinovo kriterium). *Nechť* $f = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$ *je nekonstantní polynom stupně* n. *Jestliže existuje prvočíslo* p *takové, že*

- $p \mid a_{n-1}$, $p \mid a_{n-2}$, $\ldots$, $p \mid a_1$, $p \mid a_0$,
- $p \nmid a_n$,
- $p^2 \nmid a_0$,

pak je f *ireducibilní nad* $\mathbb{Q}$.

Polynomy nad $\mathbb{Z}$ - ireducibilita

Věta (Eisensteinovo kriterium). *Nechť* $f = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$ *je nekonstantní polynom stupně* n. *Jestliže existuje prvočíslo* p *takové, že*

- $p \mid a_{n-1}$, $p \mid a_{n-2}$, $\ldots$, $p \mid a_1$, $p \mid a_0$,
- $p \nmid a_n$,
- $p^2 \nmid a_0$,

pak je f *ireducibilní nad* $\mathbb{Q}$.

Poznámka. Pokud prvočíslo daných vlastností neexistuje, neříká Eisensteinovo kriterium o ireducibilitě f zhola nic.

Polynomy nad $\mathbb{Z}$ - důkaz Eisensteinova kriteria

Důkaz sporem. Předpokládejme, že naopak f není ireducibilní nad $\mathbb{Q}$, podle Gaussovy věty není ireducibilní ani nad $\mathbb{Z}$.

Polynomy nad $\mathbb{Z}$ - důkaz Eisensteinova kriteria

Důkaz sporem. Předpokládejme, že naopak f není ireducibilní nad $\mathbb{Q}$, podle Gaussovy věty není ireducibilní ani nad $\mathbb{Z}$. Z předpokladů $\mathrm{st}(f) = n > 0$ a f je nekonstantní.

Polynomy nad $\mathbb{Z}$ - důkaz Eisensteinova kriteria

Důkaz sporem. Předpokládejme, že naopak f není ireducibilní nad $\mathbb{Q}$, podle Gaussovy věty není ireducibilní ani nad $\mathbb{Z}$. Z předpokladů $\mathrm{st}(f) = n > 0$ a f je nekonstantní. Existují tedy nekonstantní polynomy $g, h \in \mathbb{Z}[x]$ tak, že $f = g \cdot h$.

Polynomy nad $\mathbb{Z}$ - důkaz Eisensteinova kriteria

Důkaz sporem. Předpokládejme, že naopak f není ireducibilní nad $\mathbb{Q}$, podle Gaussovy věty není ireducibilní ani nad $\mathbb{Z}$. Z předpokladů $\mathrm{st}(f) = n > 0$ a f je nekonstantní. Existují tedy nekonstantní polynomy $g, h \in \mathbb{Z}[x]$ tak, že $f = g \cdot h$. Opět užijme homomorfismus okruhů $\alpha : \mathbb{Z}[x] \to \mathbb{Z}_p[x]$ určený předpisem

$$\alpha(b_n x^n + b_{n-1} x^{n-1} + \cdots + b_1 x + b_0) = \\ = [b_n]_p x^n + [b_{n-1}]_p x^{n-1} + \cdots + [b_1]_p x + [b_0]_p$$

pro libovolné $b_0, b_1, \ldots, b_n \in \mathbb{Z}$.

Polynomy nad $\mathbb{Z}$ - důkaz Eisensteinova kriteria

Důkaz sporem. Předpokládejme, že naopak f není ireducibilní nad $\mathbb{Q}$, podle Gaussovy věty není ireducibilní ani nad $\mathbb{Z}$. Z předpokladů $\mathrm{st}(f) = n > 0$ a f je nekonstantní. Existují tedy nekonstantní polynomy $g, h \in \mathbb{Z}[x]$ tak, že $f = g \cdot h$. Opět užijme homomorfismus okruhů $\alpha : \mathbb{Z}[x] \to \mathbb{Z}_p[x]$ určený předpisem

$$\alpha(b_n x^n + b_{n-1} x^{n-1} + \cdots + b_1 x + b_0) = \\ = [b_n]_p x^n + [b_{n-1}]_p x^{n-1} + \cdots + [b_1]_p x + [b_0]_p$$

pro libovolné $b_0, b_1, \ldots, b_n \in \mathbb{Z}$. Pak z prvního předpokladu plyne, že

$$\alpha(g) \cdot \alpha(h) = \alpha(g \cdot h) = \alpha(f) = [a_n]_p x^n$$

je asociované s polynomem x^n, neboť $p \nmid a_n$.

Polynomy nad $\mathbb{Z}$ - důkaz Eisensteinova kriteria

Důkaz sporem. Předpokládejme, že naopak f není ireducibilní nad $\mathbb{Q}$, podle Gaussovy věty není ireducibilní ani nad $\mathbb{Z}$. Z předpokladů $\mathrm{st}(f) = n > 0$ a f je nekonstantní. Existují tedy nekonstantní polynomy $g, h \in \mathbb{Z}[x]$ tak, že $f = g \cdot h$. Opět užijme homomorfismus okruhů $\alpha : \mathbb{Z}[x] \to \mathbb{Z}_p[x]$ určený předpisem

$$\alpha(b_n x^n + b_{n-1} x^{n-1} + \cdots + b_1 x + b_0) = \\ = [b_n]_p x^n + [b_{n-1}]_p x^{n-1} + \cdots + [b_1]_p x + [b_0]_p$$

pro libovolné $b_0, b_1, \ldots, b_n \in \mathbb{Z}$. Pak z prvního předpokladu plyne, že

$$\alpha(g) \cdot \alpha(h) = \alpha(g \cdot h) = \alpha(f) = [a_n]_p x^n$$

je asociované s polynomem x^n, neboť $p \nmid a_n$. Přitom $\mathbb{Z}_p[x]$ je okruh s jednoznačným rozkladem, proto $\alpha(g)$ i $\alpha(h)$ jsou asociované s mocninami polynomu x.

Polynomy nad $\mathbb{Z}$ - důkaz Eisensteinova kriteria

Důkaz sporem. Předpokládejme, že naopak f není ireducibilní nad $\mathbb{Q}$, podle Gaussovy věty není ireducibilní ani nad $\mathbb{Z}$. Z předpokladů $\mathrm{st}(f) = n > 0$ a f je nekonstantní. Existují tedy nekonstantní polynomy $g, h \in \mathbb{Z}[x]$ tak, že $f = g \cdot h$. Opět užijme homomorfismus okruhů $\alpha : \mathbb{Z}[x] \to \mathbb{Z}_p[x]$ určený předpisem

$$\alpha(b_n x^n + b_{n-1} x^{n-1} + \cdots + b_1 x + b_0) = \\ = [b_n]_p x^n + [b_{n-1}]_p x^{n-1} + \cdots + [b_1]_p x + [b_0]_p$$

pro libovolné $b_0, b_1, \ldots, b_n \in \mathbb{Z}$. Pak z prvního předpokladu plyne, že

$$\alpha(g) \cdot \alpha(h) = \alpha(g \cdot h) = \alpha(f) = [a_n]_p x^n$$

je asociované s polynomem x^n, neboť $p \nmid a_n$. Přitom $\mathbb{Z}_p[x]$ je okruh s jednoznačným rozkladem, proto $\alpha(g)$ i $\alpha(h)$ jsou asociované s mocninami polynomu x. A protože jsou nekonstantní, musí být absolutní členy obou polynomů g i h dělitelné p.

Polynomy nad $\mathbb{Z}$ - důkaz Eisensteinova kriteria

Důkaz sporem. Předpokládejme, že naopak f není ireducibilní nad $\mathbb{Q}$, podle Gaussovy věty není ireducibilní ani nad $\mathbb{Z}$. Z předpokladů $\mathrm{st}(f) = n > 0$ a f je nekonstantní. Existují tedy nekonstantní polynomy $g, h \in \mathbb{Z}[x]$ tak, že $f = g \cdot h$. Opět užijme homomorfismus okruhů $\alpha : \mathbb{Z}[x] \to \mathbb{Z}_p[x]$ určený předpisem

$$\alpha(b_n x^n + b_{n-1} x^{n-1} + \cdots + b_1 x + b_0) = \\ = [b_n]_p x^n + [b_{n-1}]_p x^{n-1} + \cdots + [b_1]_p x + [b_0]_p$$

pro libovolné $b_0, b_1, \ldots, b_n \in \mathbb{Z}$. Pak z prvního předpokladu plyne, že

$$\alpha(g) \cdot \alpha(h) = \alpha(g \cdot h) = \alpha(f) = [a_n]_p x^n$$

je asociované s polynomem x^n, neboť $p \nmid a_n$. Přitom $\mathbb{Z}_p[x]$ je okruh s jednoznačným rozkladem, proto $\alpha(g)$ i $\alpha(h)$ jsou asociované s mocninami polynomu x. A protože jsou nekonstantní, musí být absolutní členy obou polynomů g i h dělitelné p. Jejich součin a_0 je tedy dělitelný p^2, což je spor.