Polynomy nad libovolným okruhem R

Poznámka. Abychom nemuseli definovat, co je to výraz, jak se výrazy sčítají a násobí a kdy jsou si dva výrazy rovny, nezavedeme polynom „středoškolsky“ jako výraz určitého tvaru, ale pomocí posloupnosti koeficientů.

Polynomy nad libovolným okruhem R

Poznámka. Abychom nemuseli definovat, co je to výraz, jak se výrazy sčítají a násobí a kdy jsou si dva výrazy rovny, nezavedeme polynom „středoškolsky“ jako výraz určitého tvaru, ale pomocí posloupnosti koeficientů. To lze udělat nad libovolným okruhem R.

Polynomy nad libovolným okruhem R

Poznámka. Abychom nemuseli definovat, co je to výraz, jak se výrazy sčítají a násobí a kdy jsou si dva výrazy rovny, nezavedeme polynom „středoškolsky“ jako výraz určitého tvaru, ale pomocí posloupnosti koeficientů. To lze udělat nad libovolným okruhem R.

Definice. Nechť R je okruh. **Polynom** nad okruhem R je každá nekonečná posloupnost $f = (f_0, f_1, f_2, \dots)$, kde $f_i \in R$ pro každé $i = 0, 1, 2, \dots$, taková, že množina $\{i \in \mathbb{N} \cup \{0\};\ f_i \neq 0\}$ je konečná.

Polynomy nad libovolným okruhem R

Poznámka. Abychom nemuseli definovat, co je to výraz, jak se výrazy sčítají a násobí a kdy jsou si dva výrazy rovny, nezavedeme polynom „středoškolsky“ jako výraz určitého tvaru, ale pomocí posloupnosti koeficientů. To lze udělat nad libovolným okruhem R.

Definice. Nechť R je okruh. **Polynom** nad okruhem R je každá nekonečná posloupnost $f = (f_0, f_1, f_2, \dots)$, kde $f_i \in R$ pro každé $i = 0, 1, 2, \dots$, taková, že množina $\{i \in \mathbb{N} \cup \{0\};\ f_i \neq 0\}$ je konečná. Prvky $f_0, f_1, f_2, \dots$ nazýváme **koeficienty** polynomu f.

Polynomy nad libovolným okruhem R

Poznámka. Abychom nemuseli definovat, co je to výraz, jak se výrazy sčítají a násobí a kdy jsou si dva výrazy rovny, nezavedeme polynom „středoškolsky“ jako výraz určitého tvaru, ale pomocí posloupnosti koeficientů. To lze udělat nad libovolným okruhem R.

Definice. Nechť R je okruh. **Polynom** nad okruhem R je každá nekonečná posloupnost $f = (f_0, f_1, f_2, \dots)$, kde $f_i \in R$ pro každé $i = 0, 1, 2, \dots$, taková, že množina $\{i \in \mathbb{N} \cup \{0\};\ f_i \neq 0\}$ je konečná. Prvky $f_0, f_1, f_2, \dots$ nazýváme **koeficienty** polynomu f.

Dohoda. Polynom $(0, 1, 0, 0, \dots)$ bude hrát významnou roli, označme jej symbolem $x = (0, 1, 0, 0, \dots)$.

Polynomy nad libovolným okruhem R

Poznámka. Abychom nemuseli definovat, co je to výraz, jak se výrazy sčítají a násobí a kdy jsou si dva výrazy rovny, nezavedeme polynom „středoškolsky“ jako výraz určitého tvaru, ale pomocí posloupnosti koeficientů. To lze udělat nad libovolným okruhem R.

Definice. Nechť R je okruh. **Polynom** nad okruhem R je každá nekonečná posloupnost $f = (f_0, f_1, f_2, \dots)$, kde $f_i \in R$ pro každé $i = 0, 1, 2, \dots$, taková, že množina $\{i \in \mathbb{N} \cup \{0\};\ f_i \neq 0\}$ je konečná. Prvky $f_0, f_1, f_2, \dots$ nazýváme **koeficienty** polynomu f.

Dohoda. Polynom $(0, 1, 0, 0, \dots)$ bude hrát významnou roli, označme jej symbolem $x = (0, 1, 0, 0, \dots)$. Množinu všech polynomů nad okruhem R označme symbolem $R[x]$.

Polynomy nad libovolným okruhem R

Poznámka. Abychom nemuseli definovat, co je to výraz, jak se výrazy sčítají a násobí a kdy jsou si dva výrazy rovny, nezavedeme polynom „středoškolsky“ jako výraz určitého tvaru, ale pomocí posloupnosti koeficientů. To lze udělat nad libovolným okruhem R.

Definice. Nechť R je okruh. **Polynom** nad okruhem R je každá nekonečná posloupnost $f = (f_0, f_1, f_2, \dots)$, kde $f_i \in R$ pro každé $i = 0, 1, 2, \dots$, taková, že množina $\{i \in \mathbb{N} \cup \{0\};\ f_i \neq 0\}$ je konečná. Prvky $f_0, f_1, f_2, \dots$ nazýváme **koeficienty** polynomu f.

Dohoda. Polynom $(0, 1, 0, 0, \dots)$ bude hrát významnou roli, označme jej symbolem $x = (0, 1, 0, 0, \dots)$. Množinu všech polynomů nad okruhem R označme symbolem $R[x]$. Koeficienty polynomu f budeme automaticky označovat symboly $f_0, f_1, f_2, \dots$.

Polynomy nad libovolným okruhem R

Poznámka. Abychom nemuseli definovat, co je to výraz, jak se výrazy sčítají a násobí a kdy jsou si dva výrazy rovny, nezavedeme polynom „středoškolsky“ jako výraz určitého tvaru, ale pomocí posloupnosti koeficientů. To lze udělat nad libovolným okruhem R.

Definice. Nechť R je okruh. **Polynom** nad okruhem R je každá nekonečná posloupnost $f = (f_0, f_1, f_2, \dots)$, kde $f_i \in R$ pro každé $i = 0, 1, 2, \dots$, taková, že množina $\{i \in \mathbb{N} \cup \{0\};\ f_i \neq 0\}$ je konečná. Prvky $f_0, f_1, f_2, \dots$ nazýváme **koeficienty** polynomu f.

Dohoda. Polynom $(0, 1, 0, 0, \dots)$ bude hrát významnou roli, označme jej symbolem $x = (0, 1, 0, 0, \dots)$. Množinu všech polynomů nad okruhem R označme symbolem $R[x]$. Koeficienty polynomu f budeme automaticky označovat symboly $f_0, f_1, f_2, \dots$.

Věta. Nechť R je okruh. Na množině $R[x]$ definujeme operace $+$, $\cdot$ vztahy $(f + g)_i = f_i + g_i$, $(f \cdot g)_i = \sum_{k=0}^{i} f_k \cdot g_{i-k}$ *pro každé $f, g \in R[x]$, $i \in \mathbb{Z}$, $i \geq 0$.*

Polynomy nad libovolným okruhem R

Poznámka. Abychom nemuseli definovat, co je to výraz, jak se výrazy sčítají a násobí a kdy jsou si dva výrazy rovny, nezavedeme polynom „středoškolsky“ jako výraz určitého tvaru, ale pomocí posloupnosti koeficientů. To lze udělat nad libovolným okruhem R.

Definice. Nechť R je okruh. **Polynom** nad okruhem R je každá nekonečná posloupnost $f = (f_0, f_1, f_2, \dots)$, kde $f_i \in R$ pro každé $i = 0, 1, 2, \dots$, taková, že množina $\{i \in \mathbb{N} \cup \{0\};\ f_i \neq 0\}$ je konečná. Prvky $f_0, f_1, f_2, \dots$ nazýváme **koeficienty** polynomu f.

Dohoda. Polynom $(0, 1, 0, 0, \dots)$ bude hrát významnou roli, označme jej symbolem $x = (0, 1, 0, 0, \dots)$. Množinu všech polynomů nad okruhem R označme symbolem $R[x]$. Koeficienty polynomu f budeme automaticky označovat symboly $f_0, f_1, f_2, \dots$.

Věta. *Nechť R je okruh. Na množině $R[x]$ definujeme operace $+$, $\cdot$ vztahy* $(f + g)_i = f_i + g_i$, $(f \cdot g)_i = \sum_{k=0}^{i} f_k \cdot g_{i-k}$ *pro každé $f, g \in R[x]$, $i \in \mathbb{Z}$, $i \geq 0$. Pak $(R[x], +, \cdot)$ je okruh.*

Polynomy nad libovolným okruhem R

Poznámka. Abychom nemuseli definovat, co je to výraz, jak se výrazy sčítají a násobí a kdy jsou si dva výrazy rovny, nezavedeme polynom „středoškolsky“ jako výraz určitého tvaru, ale pomocí posloupnosti koeficientů. To lze udělat nad libovolným okruhem R.

Definice. Nechť R je okruh. **Polynom** nad okruhem R je každá nekonečná posloupnost $f = (f_0, f_1, f_2, \dots)$, kde $f_i \in R$ pro každé $i = 0, 1, 2, \dots$, taková, že množina $\{i \in \mathbb{N} \cup \{0\};\ f_i \neq 0\}$ je konečná. Prvky $f_0, f_1, f_2, \dots$ nazýváme **koeficienty** polynomu f.

Dohoda. Polynom $(0, 1, 0, 0, \dots)$ bude hrát významnou roli, označme jej symbolem $x = (0, 1, 0, 0, \dots)$. Množinu všech polynomů nad okruhem R označme symbolem $R[x]$. Koeficienty polynomu f budeme automaticky označovat symboly $f_0, f_1, f_2, \dots$.

Věta. *Nechť R je okruh. Na množině $R[x]$ definujeme operace $+$, $\cdot$ vztahy* $(f + g)_i = f_i + g_i$, $(f \cdot g)_i = \sum_{k=0}^{i} f_k \cdot g_{i-k}$ *pro každé $f, g \in R[x]$, $i \in \mathbb{Z}$, $i \geq 0$. Pak $(R[x], +, \cdot)$ je okruh. Je-li R komutativní, pak $R[x]$ je také komutativní.* [Věta 5.2, str. 78]

Definice. Okruh $R[x]$ se nazývá **okruh polynomů** nad okruhem R.

Definice. Okruh $R[x]$ se nazývá **okruh polynomů** nad okruhem R.

Věta. *Nechť R je okruh. Zobrazení $k : R \to R[x]$ určené předpisem $k(a) = (a, 0, 0, \dots)$ je injektivní homomorfismus okruhů.*

Definice. Okruh $R[x]$ se nazývá **okruh polynomů** nad okruhem R.

Věta. Nechť R je okruh. Zobrazení $k : R \to R[x]$ určené předpisem $k(a) = (a, 0, 0, \dots)$ je injektivní homomorfismus okruhů. [Věta 5.4, str. 79]

Ztotožnění. Polynomy tvaru $(a, 0, 0, \dots)$ se nazývají **konstatntní**.

Definice. Okruh $R[x]$ se nazývá **okruh polynomů** nad okruhem R.

Věta. Nechť R je okruh. Zobrazení $k : R \to R[x]$ určené předpisem $k(a) = (a, 0, 0, \dots)$ je injektivní homomorfismus okruhů. [Věta 5.4, str. 79]

Ztotožnění. Polynomy tvaru $(a, 0, 0, \dots)$ se nazývají **konstatntní**. Předchozí věta nám umožňuje ztotožnit $a \in R$ s konstantním polynomem $(a, 0, 0, \dots)$.

Definice. Okruh $R[x]$ se nazývá **okruh polynomů** nad okruhem R.

Věta. *Nechť R je okruh. Zobrazení $k : R \to R[x]$ určené předpisem $k(a) = (a, 0, 0, \dots)$ je injektivní homomorfismus okruhů.* [Věta 5.4, str. 79]

Ztotožnění. Polynomy tvaru $(a, 0, 0, \dots)$ se nazývají **konstatntní**. Předchozí věta nám umožňuje ztotožnit $a \in R$ s konstantním polynomem $(a, 0, 0, \dots)$. Tím se okruh R stává podokruhem okruhu $R[x]$.

Definice. Okruh $R[x]$ se nazývá **okruh polynomů** nad okruhem R.

Věta. *Nechť R je okruh. Zobrazení $k : R \to R[x]$ určené předpisem $k(a) = (a, 0, 0, \dots)$ je injektivní homomorfismus okruhů.* [Věta 5.4, str. 79]

Ztotožnění. Polynomy tvaru $(a, 0, 0, \dots)$ se nazývají **konstatntní**. Předchozí věta nám umožňuje ztotožnit $a \in R$ s konstantním polynomem $(a, 0, 0, \dots)$. Tím se okruh R stává podokruhem okruhu $R[x]$. Polynom $0 = (0, 0, 0, \dots)$ se nazývá **nulový**, ostatní polynomy se nazývají **nenulové**.

Definice. Okruh $R[x]$ se nazývá **okruh polynomů** nad okruhem R.

Věta. *Nechť R je okruh. Zobrazení $k : R \to R[x]$ určené předpisem $k(a) = (a, 0, 0, \dots)$ je injektivní homomorfismus okruhů.* [Věta 5.4, str. 79]

Ztotožnění. Polynomy tvaru $(a, 0, 0, \dots)$ se nazývají **konstatntní**. Předchozí věta nám umožňuje ztotožnit $a \in R$ s konstantním polynomem $(a, 0, 0, \dots)$. Tím se okruh R stává podokruhem okruhu $R[x]$. Polynom $0 = (0, 0, 0, \dots)$ se nazývá **nulový**, ostatní polynomy se nazývají **nenulové**.

Definice. Nechť f je nenulový polynom nad okruhem R.

Definice. Okruh $R[x]$ se nazývá **okruh polynomů** nad okruhem R.

Věta. Nechť R je okruh. Zobrazení $k : R \to R[x]$ určené předpisem $k(a) = (a, 0, 0, \dots)$ je injektivní homomorfismus okruhů. [Věta 5.4, str. 79]

Ztotožnění. Polynomy tvaru $(a, 0, 0, \dots)$ se nazývají **konstatntní**. Předchozí věta nám umožňuje ztotožnit $a \in R$ s konstantním polynomem $(a, 0, 0, \dots)$. Tím se okruh R stává podokruhem okruhu $R[x]$. Polynom $0 = (0, 0, 0, \dots)$ se nazývá **nulový**, ostatní polynomy se nazývají **nenulové**.

Definice. Nechť f je nenulový polynom nad okruhem R. Největší $n \geq 0$ takové, že $f_n \neq 0$, se nazývá **stupeň** polynomu f, značíme $\mathrm{st}(f)$. (Takové n existuje, protože množina $\{i \in \mathbb{N} \cup \{0\};\ f_i \neq 0\}$ je konečná.)

Definice. Okruh $R[x]$ se nazývá **okruh polynomů** nad okruhem R.

Věta. Nechť R je okruh. Zobrazení $k : R \to R[x]$ určené předpisem $k(a) = (a, 0, 0, \dots)$ je injektivní homomorfismus okruhů. [Věta 5.4, str. 79]

Ztotožnění. Polynomy tvaru $(a, 0, 0, \dots)$ se nazývají **konstatntní**. Předchozí věta nám umožňuje ztotožnit $a \in R$ s konstantním polynomem $(a, 0, 0, \dots)$. Tím se okruh R stává podokruhem okruhu $R[x]$. Polynom $0 = (0, 0, 0, \dots)$ se nazývá **nulový**, ostatní polynomy se nazývají **nenulové**.

Definice. Nechť f je nenulový polynom nad okruhem R. Největší $n \geq 0$ takové, že $f_n \neq 0$, se nazývá **stupeň** polynomu f, značíme $\mathrm{st}(f)$. (Takové n existuje, protože množina $\{i \in \mathbb{N} \cup \{0\};\ f_i \neq 0\}$ je konečná.) Koeficient f_n se pak nazývá **vedoucí koeficient** polynomu f.

Definice. Okruh $R[x]$ se nazývá **okruh polynomů** nad okruhem R.

Věta. Nechť R je okruh. Zobrazení $k : R \to R[x]$ určené předpisem $k(a) = (a, 0, 0, \dots)$ je injektivní homomorfismus okruhů. [Věta 5.4, str. 79]

Ztotožnění. Polynomy tvaru $(a, 0, 0, \dots)$ se nazývají **konstatntní**. Předchozí věta nám umožňuje ztotožnit $a \in R$ s konstantním polynomem $(a, 0, 0, \dots)$. Tím se okruh R stává podokruhem okruhu $R[x]$. Polynom $0 = (0, 0, 0, \dots)$ se nazývá **nulový**, ostatní polynomy se nazývají **nenulové**.

Definice. Nechť f je nenulový polynom nad okruhem R. Největší $n \geq 0$ takové, že $f_n \neq 0$, se nazývá **stupeň** polynomu f, značíme $\mathrm{st}(f)$. (Takové n existuje, protože množina $\{i \in \mathbb{N} \cup \{0\};\ f_i \neq 0\}$ je konečná.) Koeficient f_n se pak nazývá **vedoucí koeficient** polynomu f. Stupeň nulového polynomu klademe roven $-\infty$, jeho vedoucí koeficient nedefinujeme.

Definice. Okruh $R[x]$ se nazývá **okruh polynomů** nad okruhem R.

Věta. Nechť R je okruh. Zobrazení $k : R \to R[x]$ určené předpisem $k(a) = (a, 0, 0, \dots)$ je injektivní homomorfismus okruhů. [Věta 5.4, str. 79]

Ztotožnění. Polynomy tvaru $(a, 0, 0, \dots)$ se nazývají **konstatntní**. Předchozí věta nám umožňuje ztotožnit $a \in R$ s konstantním polynomem $(a, 0, 0, \dots)$. Tím se okruh R stává podokruhem okruhu $R[x]$. Polynom $0 = (0, 0, 0, \dots)$ se nazývá **nulový**, ostatní polynomy se nazývají **nenulové**.

Definice. Nechť f je nenulový polynom nad okruhem R. Největší $n \geq 0$ takové, že $f_n \neq 0$, se nazývá **stupeň** polynomu f, značíme $\mathrm{st}(f)$. (Takové n existuje, protože množina $\{i \in \mathbb{N} \cup \{0\};\ f_i \neq 0\}$ je konečná.) Koeficient f_n se pak nazývá **vedoucí koeficient** polynomu f. Stupeň nulového polynomu klademe roven $-\infty$, jeho vedoucí koeficient nedefinujeme.

Příklad. Polynomy stupně 0 jsou právě nenulové konstantní polynomy.

Definice. Polynomy stupně 1 se nazývají **lineární**, polynomy stupně 2 **kvadratické**, polynomy stupně 3 **kubické**.

Definice. Polynomy stupně 1 se nazývají **lineární**, polynomy stupně 2 **kvadratické**, polynomy stupně 3 **kubické**.

Příklad. Polynom $x = (0, 1, 0, 0, \dots)$ je lineární,

Definice. Polynomy stupně 1 se nazývají **lineární**, polynomy stupně 2 **kvadratické**, polynomy stupně 3 **kubické**.

Příklad. Polynom $x = (0, 1, 0, 0, \dots)$ je lineární,
polynom $x^2 = (0, 0, 1, 0, 0, \dots)$ kvadraticky,

Definice. Polynomy stupně 1 se nazývají **lineární**, polynomy stupně 2 **kvadratické**, polynomy stupně 3 **kubické**.

Příklad. Polynom $x = (0, 1, 0, 0, \dots)$ je lineární,
polynom $x^2 = (0, 0, 1, 0, 0, \dots)$ kvadraticky,
polynom $x^3 = (0, 0, 0, 1, 0, \dots)$ kubický.

Definice. Polynomy stupně 1 se nazývají **lineární**, polynomy stupně 2 **kvadratické**, polynomy stupně 3 **kubické**.

Příklad. Polynom $x = (0, 1, 0, 0, \dots)$ je lineární,
polynom $x^2 = (0, 0, 1, 0, 0, \dots)$ kvadraticky,
polynom $x^3 = (0, 0, 0, 1, 0, \dots)$ kubický.

Věta. *Nechť R je okruh a $f \in R[x]$ nenulový polynom stupně n. Pak platí $f = f_n \cdot x^n + \cdots + f_1 \cdot x + f_0$, kde koeficienty f_i polynomu f chápeme jako konstantní polynomy a operace $+$ a $\cdot$ jsou operace v okruhu $R[x]$.*

Definice. Polynomy stupně 1 se nazývají **lineární**, polynomy stupně 2 **kvadratické**, polynomy stupně 3 **kubické**.

Příklad. Polynom $x = (0, 1, 0, 0, \dots)$ je lineární,
polynom $x^2 = (0, 0, 1, 0, 0, \dots)$ kvadraticky,
polynom $x^3 = (0, 0, 0, 1, 0, \dots)$ kubický.

Věta. Nechť R je okruh a $f \in R[x]$ nenulový polynom stupně n. Pak platí $f = f_n \cdot x^n + \cdots + f_1 \cdot x + f_0$, kde koeficienty f_i polynomu f chápeme jako konstantní polynomy a operace $+$ a $\cdot$ jsou operace v okruhu $R[x]$. [Věta 5.8, str. 80]

Poznámka. Okruh všech polynomů je tedy generován sjednocením $R \cup \{x\}$, kde R je ztotožněno s podokruhem konstantních polynomů, je tedy naše označení $R[x]$ v souladu s dříve zavedeným označením podokruhu, který je generován podmnožinou $R \cup \{x\}$.

Definice. Polynomy stupně 1 se nazývají **lineární**, polynomy stupně 2 **kvadratické**, polynomy stupně 3 **kubické**.

Příklad. Polynom $x = (0, 1, 0, 0, \dots)$ je lineární,
polynom $x^2 = (0, 0, 1, 0, 0, \dots)$ kvadraticky,
polynom $x^3 = (0, 0, 0, 1, 0, \dots)$ kubický.

Věta. Nechť R je okruh a $f \in R[x]$ nenulový polynom stupně n. Pak platí $f = f_n \cdot x^n + \cdots + f_1 \cdot x + f_0$, kde koeficienty f_i polynomu f chápeme jako konstantní polynomy a operace $+$ a $\cdot$ jsou operace v okruhu $R[x]$. [Věta 5.8, str. 80]

Poznámka. Okruh všech polynomů je tedy generován sjednocením $R \cup \{x\}$, kde R je ztotožněno s podokruhem konstantních polynomů, je tedy naše označení $R[x]$ v souladu s dříve zavedeným označením podokruhu, který je generován podmnožinou $R \cup \{x\}$.

Poznámka. Přestože jsme polynomy nedefinovali jako výrazy, předchozí věta nám umožňuje s nimi tak pracovat.

Definice. Polynomy stupně 1 se nazývají **lineární**, polynomy stupně 2 **kvadratické**, polynomy stupně 3 **kubické**.

Příklad. Polynom $x = (0, 1, 0, 0, \dots)$ je lineární,
polynom $x^2 = (0, 0, 1, 0, 0, \dots)$ kvadraticky,
polynom $x^3 = (0, 0, 0, 1, 0, \dots)$ kubický.

Věta. Nechť R je okruh a $f \in R[x]$ nenulový polynom stupně n. Pak platí $f = f_n \cdot x^n + \cdots + f_1 \cdot x + f_0$, kde koeficienty f_i polynomu f chápeme jako konstantní polynomy a operace $+$ a $\cdot$ jsou operace v okruhu $R[x]$. [Věta 5.8, str. 80]

Poznámka. Okruh všech polynomů je tedy generován sjednocením $R \cup \{x\}$, kde R je ztotožněno s podokruhem konstantních polynomů, je tedy naše označení $R[x]$ v souladu s dříve zavedeným označením podokruhu, který je generován podmnožinou $R \cup \{x\}$.

Poznámka. Přestože jsme polynomy nedefinovali jako výrazy, předchozí věta nám umožňuje s nimi tak pracovat. Nejedná se však o nějak abstraktně definovaný výraz, ale jde o výpočet v okruhu polynomů.

Definice. Polynomy stupně 1 se nazývají **lineární**, polynomy stupně 2 **kvadratické**, polynomy stupně 3 **kubické**.

Příklad. Polynom $x = (0, 1, 0, 0, \dots)$ je lineární,
polynom $x^2 = (0, 0, 1, 0, 0, \dots)$ kvadraticky,
polynom $x^3 = (0, 0, 0, 1, 0, \dots)$ kubický.

Věta. Nechť R je okruh a $f \in R[x]$ nenulový polynom stupně n. Pak platí $f = f_n \cdot x^n + \cdots + f_1 \cdot x + f_0$, kde koeficienty f_i polynomu f chápeme jako konstantní polynomy a operace $+$ a $\cdot$ jsou operace v okruhu $R[x]$. [Věta 5.8, str. 80]

Poznámka. Okruh všech polynomů je tedy generován sjednocením $R \cup \{x\}$, kde R je ztotožněno s podokruhem konstantních polynomů, je tedy naše označení $R[x]$ v souladu s dříve zavedeným označením podokruhu, který je generován podmnožinou $R \cup \{x\}$.

Poznámka. Přestože jsme polynomy nedefinovali jako výrazy, předchozí věta nám umožňuje s nimi tak pracovat. Nejedná se však o nějak abstraktně definovaný výraz, ale jde o výpočet v okruhu polynomů. Nemusíme tedy vysvětlovat, kdy si jsou dva výrazy rovny a jak se s nimi počítá.

Dohoda. V následující větě budeme potřebovat tyto vztahy pro počítání s nekonečnem: pro libovolné $n \in \mathbb{Z}$, $n \geq 0$ je $-\infty < n$,

Dohoda. V následující větě budeme potřebovat tyto vztahy pro počítání s nekonečnem: pro libovolné $n \in \mathbb{Z}$, $n \geq 0$ je $-\infty < n$, $(-\infty) + (-\infty) = (-\infty) + n = n + (-\infty) = -\infty$.

Dohoda. V následující větě budeme potřebovat tyto vztahy pro počítání s nekonečnem: pro libovolné $n \in \mathbb{Z}$, $n \geq 0$ je $-\infty < n$, $(-\infty) + (-\infty) = (-\infty) + n = n + (-\infty) = -\infty$.

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

- $\mathrm{st}(f + g) \leq \max\{\mathrm{st}(f), \mathrm{st}(g)\}$,

Dohoda. V následující větě budeme potřebovat tyto vztahy pro počítání s nekonečnem: pro libovolné $n \in \mathbb{Z}$, $n \geq 0$ je $-\infty < n$, $(-\infty) + (-\infty) = (-\infty) + n = n + (-\infty) = -\infty$.

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

- $\mathrm{st}(f + g) \leq \max\{\mathrm{st}(f), \mathrm{st}(g)\}$,
- $\mathrm{st}(f \cdot g) \leq \mathrm{st}(f) + \mathrm{st}(g)$,

Dohoda. V následující větě budeme potřebovat tyto vztahy pro počítání s nekonečnem: pro libovolné $n \in \mathbb{Z}$, $n \geq 0$ je $-\infty < n$, $(-\infty) + (-\infty) = (-\infty) + n = n + (-\infty) = -\infty$.

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

- $\mathrm{st}(f + g) \leq \max\{\mathrm{st}(f), \mathrm{st}(g)\}$,
- $\mathrm{st}(f \cdot g) \leq \mathrm{st}(f) + \mathrm{st}(g)$,
- *jestliže $f \neq 0$, $g \neq 0$ a alespoň jeden z vedoucích koeficientů polynomů f a g není dělitel nuly, pak* $\mathrm{st}(f \cdot g) = \mathrm{st}(f) + \mathrm{st}(g)$. *[Věta 5.10, str. 81]*

Dohoda. V následující větě budeme potřebovat tyto vztahy pro počítání s nekonečnem: pro libovolné $n \in \mathbb{Z}$, $n \geq 0$ je $-\infty < n$, $(-\infty) + (-\infty) = (-\infty) + n = n + (-\infty) = -\infty$.

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

- $\mathrm{st}(f + g) \leq \max\{\mathrm{st}(f), \mathrm{st}(g)\}$,
- $\mathrm{st}(f \cdot g) \leq \mathrm{st}(f) + \mathrm{st}(g)$,
- *jestliže $f \neq 0$, $g \neq 0$ a alespoň jeden z vedoucích koeficientů polynomů f a g není dělitel nuly, pak* $\mathrm{st}(f \cdot g) = \mathrm{st}(f) + \mathrm{st}(g)$. *[Věta 5.10, str. 81]*

Věta. *Je-li R obor integrity, pak také $R[x]$ je obor integrity.*

Dohoda. V následující větě budeme potřebovat tyto vztahy pro počítání s nekonečnem: pro libovolné $n \in \mathbb{Z}$, $n \geq 0$ je $-\infty < n$, $(-\infty) + (-\infty) = (-\infty) + n = n + (-\infty) = -\infty$.

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

- $\mathrm{st}(f + g) \leq \max\{\mathrm{st}(f), \mathrm{st}(g)\}$,
- $\mathrm{st}(f \cdot g) \leq \mathrm{st}(f) + \mathrm{st}(g)$,
- *jestliže $f \neq 0$, $g \neq 0$ a alespoň jeden z vedoucích koeficientů polynomů f a g není dělitel nuly, pak* $\mathrm{st}(f \cdot g) = \mathrm{st}(f) + \mathrm{st}(g)$. *[Věta 5.10, str. 81]*

Věta. *Je-li R obor integrity, pak také $R[x]$ je obor integrity.* [Věta 5.12, str. 81]

Věta. *Nechť R je obor integrity. Pak $(R[x])^\times = R^\times$, tedy polynom f je jednotkou okruhu $R[x]$, právě když je konstantní a současně je jednotkou okruhu R.*

Dohoda. V následující větě budeme potřebovat tyto vztahy pro počítání s nekonečnem: pro libovolné $n \in \mathbb{Z}$, $n \geq 0$ je $-\infty < n$, $(-\infty) + (-\infty) = (-\infty) + n = n + (-\infty) = -\infty$.

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

- $\mathrm{st}(f + g) \leq \max\{\mathrm{st}(f), \mathrm{st}(g)\}$,
- $\mathrm{st}(f \cdot g) \leq \mathrm{st}(f) + \mathrm{st}(g)$,
- *jestliže $f \neq 0$, $g \neq 0$ a alespoň jeden z vedoucích koeficientů polynomů f a g není dělitel nuly, pak* $\mathrm{st}(f \cdot g) = \mathrm{st}(f) + \mathrm{st}(g)$. *[Věta 5.10, str. 81]*

Věta. *Je-li R obor integrity, pak také $R[x]$ je obor integrity.* [Věta 5.12, str. 81]

Věta. *Nechť R je obor integrity. Pak $(R[x])^\times = R^\times$, tedy polynom f je jednotkou okruhu $R[x]$, právě když je konstantní a současně je jednotkou okruhu R.* [Věta 5.13, str. 81]

Důsledek. *Pro žádný okruh R není okruh $R[x]$ těleso.*

Dohoda. V následující větě budeme potřebovat tyto vztahy pro počítání s nekonečnem: pro libovolné $n \in \mathbb{Z}$, $n \geq 0$ je $-\infty < n$, $(-\infty) + (-\infty) = (-\infty) + n = n + (-\infty) = -\infty$.

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

- $\mathrm{st}(f + g) \leq \max\{\mathrm{st}(f), \mathrm{st}(g)\}$,
- $\mathrm{st}(f \cdot g) \leq \mathrm{st}(f) + \mathrm{st}(g)$,
- *jestliže $f \neq 0$, $g \neq 0$ a alespoň jeden z vedoucích koeficientů polynomů f a g není dělitel nuly, pak* $\mathrm{st}(f \cdot g) = \mathrm{st}(f) + \mathrm{st}(g)$. *[Věta 5.10, str. 81]*

Věta. *Je-li R obor integrity, pak také $R[x]$ je obor integrity.* [Věta 5.12, str. 81]

Věta. *Nechť R je obor integrity. Pak $(R[x])^\times = R^\times$, tedy polynom f je jednotkou okruhu $R[x]$, právě když je konstantní a současně je jednotkou okruhu R.* [Věta 5.13, str. 81]

Důsledek. *Pro žádný okruh R není okruh $R[x]$ těleso.*

Příklad. Jestliže R není obor integrity, mohou existovat i nekonstatní jednotky okruhu $R[x]$, například v $\mathbb{Z}_9[x]$ platí $([3]_9 \cdot x + [1]_9) \cdot ([6]_9 \cdot x + [1]_9) = [1]_9$.

Věta o dělení polynomů se zbytkem

Věta. *Nechť R je okruh, $f, g \in R[x]$, přičemž vedoucí koeficient polynomu $g \neq 0$ je jednotka okruhu R. Pak existuje jediná dvojice polynomů $q, r \in R[x]$ taková, že $\mathrm{st}(r) < \mathrm{st}(g)$ a platí $f = g \cdot q + r$.*

Věta o dělení polynomů se zbytkem

Věta. *Nechť R je okruh, $f, g \in R[x]$, přičemž vedoucí koeficient polynomu $g \neq 0$ je jednotka okruhu R. Pak existuje jediná dvojice polynomů $q, r \in R[x]$ taková, že $\mathrm{st}(r) < \mathrm{st}(g)$ a platí $f = g \cdot q + r$.*

Důkaz existence q, r. Pro $f = 0$ zřejmé ($q = r = 0$), dále $f \neq 0$.

Věta o dělení polynomů se zbytkem

Věta. *Nechť R je okruh, $f, g \in R[x]$, přičemž vedoucí koeficient polynomu $g \neq 0$ je jednotka okruhu R. Pak existuje jediná dvojice polynomů $q, r \in R[x]$ taková, že $\mathrm{st}(r) < \mathrm{st}(g)$ a platí $f = g \cdot q + r$.*

Důkaz existence q, r. Pro $f = 0$ zřejmé ($q = r = 0$), dále $f \neq 0$.
Nechť $g = a_n x^n + \cdots + a_1 x + a_0$, $a_n \in R^\times$, tj. $\mathrm{st}(g) = n$,

Věta o dělení polynomů se zbytkem

Věta. *Nechť R je okruh, $f, g \in R[x]$, přičemž vedoucí koeficient polynomu $g \neq 0$ je jednotka okruhu R. Pak existuje jediná dvojice polynomů $q, r \in R[x]$ taková, že $\mathrm{st}(r) < \mathrm{st}(g)$ a platí $f = g \cdot q + r$.*

Důkaz existence q, r. Pro $f = 0$ zřejmé ($q = r = 0$), dále $f \neq 0$.
Nechť $g = a_n x^n + \cdots + a_1 x + a_0$, $a_n \in R^\times$, tj. $\mathrm{st}(g) = n$,
$f = b_m x^m + \cdots + b_1 x + b_0$, $b_m \neq 0$, tj. $\mathrm{st}(f) = m$.

Věta o dělení polynomů se zbytkem

Věta. *Nechť R je okruh, $f, g \in R[x]$, přičemž vedoucí koeficient polynomu $g \neq 0$ je jednotka okruhu R. Pak existuje jediná dvojice polynomů $q, r \in R[x]$ taková, že $\mathrm{st}(r) < \mathrm{st}(g)$ a platí $f = g \cdot q + r$.*

Důkaz existence q, r. Pro $f = 0$ zřejmé ($q = r = 0$), dále $f \neq 0$.
Nechť $g = a_n x^n + \cdots + a_1 x + a_0$, $a_n \in R^\times$, tj. $\mathrm{st}(g) = n$,
$f = b_m x^m + \cdots + b_1 x + b_0$, $b_m \neq 0$, tj. $\mathrm{st}(f) = m$.
Postupujme indukcí vůči m.
I. krok: Je-li $m < n$, pak označme $q = 0$, $r = f$.

Věta o dělení polynomů se zbytkem

Věta. *Nechť R je okruh, $f, g \in R[x]$, přičemž vedoucí koeficient polynomu $g \neq 0$ je jednotka okruhu R. Pak existuje jediná dvojice polynomů $q, r \in R[x]$ taková, že $\mathrm{st}(r) < \mathrm{st}(g)$ a platí $f = g \cdot q + r$.*

Důkaz existence q, r. Pro $f = 0$ zřejmé ($q = r = 0$), dále $f \neq 0$.
Nechť $g = a_n x^n + \cdots + a_1 x + a_0$, $a_n \in R^\times$, tj. $\mathrm{st}(g) = n$,
$f = b_m x^m + \cdots + b_1 x + b_0$, $b_m \neq 0$, tj. $\mathrm{st}(f) = m$.
Postupujme indukcí vůči m.
I. krok: Je-li $m < n$, pak označme $q = 0$, $r = f$.
II. krok: Předpokládejme, že $m \geq n$ a že pro polynomy stupně menšího než m již bylo dokázáno.

Věta o dělení polynomů se zbytkem

Věta. *Nechť R je okruh, $f, g \in R[x]$, přičemž vedoucí koeficient polynomu $g \neq 0$ je jednotka okruhu R. Pak existuje jediná dvojice polynomů $q, r \in R[x]$ taková, že $\mathrm{st}(r) < \mathrm{st}(g)$ a platí $f = g \cdot q + r$.*

Důkaz existence q, r. Pro $f = 0$ zřejmé ($q = r = 0$), dále $f \neq 0$.
Nechť $g = a_n x^n + \cdots + a_1 x + a_0$, $a_n \in R^\times$, tj. $\mathrm{st}(g) = n$,
$f = b_m x^m + \cdots + b_1 x + b_0$, $b_m \neq 0$, tj. $\mathrm{st}(f) = m$.
Postupujme indukcí vůči m.
I. krok: Je-li $m < n$, pak označme $q = 0$, $r = f$.
II. krok: Předpokládejme, že $m \geq n$ a že pro polynomy stupně menšího než m již bylo dokázáno. Polynom $g \cdot a_n^{-1} \cdot b_m \cdot x^{m-n}$ má stejný stupeň i vedoucí koeficient jako f, proto pro polynom $h = f - g \cdot a_n^{-1} \cdot b_m \cdot x^{m-n}$ platí $\mathrm{st}(h) < m$.

Věta o dělení polynomů se zbytkem

Věta. *Nechť R je okruh, $f, g \in R[x]$, přičemž vedoucí koeficient polynomu $g \neq 0$ je jednotka okruhu R. Pak existuje jediná dvojice polynomů $q, r \in R[x]$ taková, že $\mathrm{st}(r) < \mathrm{st}(g)$ a platí $f = g \cdot q + r$.*

Důkaz existence q, r. Pro $f = 0$ zřejmé ($q = r = 0$), dále $f \neq 0$.
Nechť $g = a_n x^n + \cdots + a_1 x + a_0$, $a_n \in R^\times$, tj. $\mathrm{st}(g) = n$,
$f = b_m x^m + \cdots + b_1 x + b_0$, $b_m \neq 0$, tj. $\mathrm{st}(f) = m$.
Postupujme indukcí vůči m.
I. krok: Je-li $m < n$, pak označme $q = 0$, $r = f$.
II. krok: Předpokládejme, že $m \geq n$ a že pro polynomy stupně menšího než m již bylo dokázáno. Polynom $g \cdot a_n^{-1} \cdot b_m \cdot x^{m-n}$ má stejný stupeň i vedoucí koeficient jako f, proto pro polynom $h = f - g \cdot a_n^{-1} \cdot b_m \cdot x^{m-n}$ platí $\mathrm{st}(h) < m$. Z indukčního předpokladu existují $p, r \in R[x]$ tak, že $\mathrm{st}(r) < \mathrm{st}(g)$ a platí $h = g \cdot p + r$.

Věta o dělení polynomů se zbytkem

Věta. *Nechť R je okruh, $f, g \in R[x]$, přičemž vedoucí koeficient polynomu $g \neq 0$ je jednotka okruhu R. Pak existuje jediná dvojice polynomů $q, r \in R[x]$ taková, že $\mathrm{st}(r) < \mathrm{st}(g)$ a platí $f = g \cdot q + r$.*

Důkaz existence q, r. Pro $f = 0$ zřejmé ($q = r = 0$), dále $f \neq 0$.
Nechť $g = a_n x^n + \cdots + a_1 x + a_0$, $a_n \in R^\times$, tj. $\mathrm{st}(g) = n$,
$f = b_m x^m + \cdots + b_1 x + b_0$, $b_m \neq 0$, tj. $\mathrm{st}(f) = m$.
Postupujme indukcí vůči m.
I. krok: Je-li $m < n$, pak označme $q = 0$, $r = f$.
II. krok: Předpokládejme, že $m \geq n$ a že pro polynomy stupně menšího než m již bylo dokázáno. Polynom $g \cdot a_n^{-1} \cdot b_m \cdot x^{m-n}$ má stejný stupeň i vedoucí koeficient jako f, proto pro polynom $h = f - g \cdot a_n^{-1} \cdot b_m \cdot x^{m-n}$ platí $\mathrm{st}(h) < m$. Z indukčního předpokladu existují $p, r \in R[x]$ tak, že $\mathrm{st}(r) < \mathrm{st}(g)$ a platí $h = g \cdot p + r$. Pak dosazením a úpravou dostaneme
$f = g \cdot a_n^{-1} \cdot b_m \cdot x^{m-n} + h = g \cdot (a_n^{-1} \cdot b_m \cdot x^{m-n} + p) + r$.

Věta o dělení polynomů se zbytkem

Věta. *Nechť R je okruh, $f, g \in R[x]$, přičemž vedoucí koeficient polynomu $g \neq 0$ je jednotka okruhu R. Pak existuje jediná dvojice polynomů $q, r \in R[x]$ taková, že $\mathrm{st}(r) < \mathrm{st}(g)$ a platí $f = g \cdot q + r$.*

Důkaz existence q, r. Pro $f = 0$ zřejmé ($q = r = 0$), dále $f \neq 0$.
Nechť $g = a_n x^n + \cdots + a_1 x + a_0$, $a_n \in R^\times$, tj. $\mathrm{st}(g) = n$,
$f = b_m x^m + \cdots + b_1 x + b_0$, $b_m \neq 0$, tj. $\mathrm{st}(f) = m$.
Postupujme indukcí vůči m.
I. krok: Je-li $m < n$, pak označme $q = 0$, $r = f$.
II. krok: Předpokládejme, že $m \geq n$ a že pro polynomy stupně menšího než m již bylo dokázáno. Polynom $g \cdot a_n^{-1} \cdot b_m \cdot x^{m-n}$ má stejný stupeň i vedoucí koeficient jako f, proto pro polynom $h = f - g \cdot a_n^{-1} \cdot b_m \cdot x^{m-n}$ platí $\mathrm{st}(h) < m$. Z indukčního předpokladu existují $p, r \in R[x]$ tak, že $\mathrm{st}(r) < \mathrm{st}(g)$ a platí $h = g \cdot p + r$. Pak dosazením a úpravou dostaneme
$f = g \cdot a_n^{-1} \cdot b_m \cdot x^{m-n} + h = g \cdot (a_n^{-1} \cdot b_m \cdot x^{m-n} + p) + r$.
Stačí označit $q = a_n^{-1} \cdot b_m \cdot x^{m-n} + p$.

Věta o dělení polynomů se zbytkem - dokončení důkazu

Věta. *Nechť R je okruh, $f, g \in R[x]$, přičemž vedoucí koeficient polynomu $g \neq 0$ je jednotka okruhu R. Pak existuje jediná dvojice polynomů $q, r \in R[x]$ taková, že $\mathrm{st}(r) < \mathrm{st}(g)$ a platí $f = g \cdot q + r$.*

Důkaz jednoznačnosti q, r.

Věta o dělení polynomů se zbytkem - dokončení důkazu

Věta. Nechť R je okruh, $f, g \in R[x]$, přičemž vedoucí koeficient polynomu $g \neq 0$ je jednotka okruhu R. Pak existuje jediná dvojice polynomů $q, r \in R[x]$ taková, že $\mathrm{st}(r) < \mathrm{st}(g)$ a platí $f = g \cdot q + r$.

Důkaz jednoznačnosti q, r. Předpokládejme, že polynomy $q, r, \bar{q}, \bar{r} \in R[x]$, přičemž $\mathrm{st}(r) < \mathrm{st}(g)$ a $\mathrm{st}(\bar{r}) < \mathrm{st}(g)$, splňují

$$f = g \cdot \bar{q} + \bar{r} = g \cdot q + r.$$

Věta o dělení polynomů se zbytkem - dokončení důkazu

Věta. Nechť R je okruh, $f, g \in R[x]$, přičemž vedoucí koeficient polynomu $g \neq 0$ je jednotka okruhu R. Pak existuje jediná dvojice polynomů $q, r \in R[x]$ taková, že $\mathrm{st}(r) < \mathrm{st}(g)$ a platí $f = g \cdot q + r$.

Důkaz jednoznačnosti q, r. Předpokládejme, že polynomy $q, r, \bar{q}, \bar{r} \in R[x]$, přičemž $\mathrm{st}(r) < \mathrm{st}(g)$ a $\mathrm{st}(\bar{r}) < \mathrm{st}(g)$, splňují

$$f = g \cdot \bar{q} + \bar{r} = g \cdot q + r.$$

Pak $g \cdot (\bar{q} - q) = g \cdot \bar{q} - g \cdot q = r - \bar{r}$.

Věta o dělení polynomů se zbytkem - dokončení důkazu

Věta. Nechť R je okruh, $f, g \in R[x]$, přičemž vedoucí koeficient polynomu $g \neq 0$ je jednotka okruhu R. Pak existuje jediná dvojice polynomů $q, r \in R[x]$ taková, že $\mathrm{st}(r) < \mathrm{st}(g)$ a platí $f = g \cdot q + r$.

Důkaz jednoznačnosti q, r. Předpokládejme, že polynomy $q, r, \bar{q}, \bar{r} \in R[x]$, přičemž $\mathrm{st}(r) < \mathrm{st}(g)$ a $\mathrm{st}(\bar{r}) < \mathrm{st}(g)$, splňují

$$f = g \cdot \bar{q} + \bar{r} = g \cdot q + r.$$

Pak $g \cdot (\bar{q} - q) = g \cdot \bar{q} - g \cdot q = r - \bar{r}$. Vedoucí koeficient polynomu g není dělitel nuly, tedy podle věty o stupni součtu a součinu polynomů $\mathrm{st}(g) + \mathrm{st}(\bar{q} - q) = \mathrm{st}(g \cdot (\bar{q} - q)) = \mathrm{st}(r - \bar{r}) < \mathrm{st}(g)$.

Věta o dělení polynomů se zbytkem - dokončení důkazu

Věta. Nechť R je okruh, $f, g \in R[x]$, přičemž vedoucí koeficient polynomu $g \neq 0$ je jednotka okruhu R. Pak existuje jediná dvojice polynomů $q, r \in R[x]$ taková, že $\mathrm{st}(r) < \mathrm{st}(g)$ a platí $f = g \cdot q + r$.

Důkaz jednoznačnosti q, r. Předpokládejme, že polynomy $q, r, \bar{q}, \bar{r} \in R[x]$, přičemž $\mathrm{st}(r) < \mathrm{st}(g)$ a $\mathrm{st}(\bar{r}) < \mathrm{st}(g)$, splňují

$$f = g \cdot \bar{q} + \bar{r} = g \cdot q + r.$$

Pak $g \cdot (\bar{q} - q) = g \cdot \bar{q} - g \cdot q = r - \bar{r}$. Vedoucí koeficient polynomu g není dělitel nuly, tedy podle věty o stupni součtu a součinu polynomů $\mathrm{st}(g) + \mathrm{st}(\bar{q} - q) = \mathrm{st}(g \cdot (\bar{q} - q)) = \mathrm{st}(r - \bar{r}) < \mathrm{st}(g)$. Pak tedy $\mathrm{st}(\bar{q} - q) < 0$, a proto $\bar{q} - q = 0$, a tedy také $r - \bar{r} = 0$, tj. $\bar{q} = q$ a $\bar{r} = r$.

Euklidův algoritmus v okruhu polynomů nad tělesem

Poznámka. Je-li R je těleso, je v $R[x]$ vedoucí koeficient každého nenulového polynomu jednotkou.

Euklidův algoritmus v okruhu polynomů nad tělesem

Poznámka. Je-li R je těleso, je v $R[x]$ vedoucí koeficient každého nenulového polynomu jednotkou. Proto pro libovolné nenulové polynomy $f, g \in R[x]$ lze postupovat podle Euklidova algoritmu. Postupně tedy dělíme se zbytkem

$$f = g \cdot q_0 + r_0,$$

Euklidův algoritmus v okruhu polynomů nad tělesem

Poznámka. Je-li R je těleso, je v $R[x]$ vedoucí koeficient každého nenulového polynomu jednotkou. Proto pro libovolné nenulové polynomy $f, g \in R[x]$ lze postupovat podle Euklidova algoritmu. Postupně tedy dělíme se zbytkem

$$\begin{aligned} f &= g \cdot q_0 + r_0, \\ g &= r_0 \cdot q_1 + r_1, \end{aligned}$$

Euklidův algoritmus v okruhu polynomů nad tělesem

Poznámka. Je-li R je těleso, je v $R[x]$ vedoucí koeficient každého nenulového polynomu jednotkou. Proto pro libovolné nenulové polynomy $f, g \in R[x]$ lze postupovat podle Euklidova algoritmu. Postupně tedy dělíme se zbytkem

$$\begin{aligned} f &= g \cdot q_0 + r_0, \\ g &= r_0 \cdot q_1 + r_1, \\ r_0 &= r_1 \cdot q_2 + r_2, \end{aligned}$$

Euklidův algoritmus v okruhu polynomů nad tělesem

Poznámka. Je-li R je těleso, je v $R[x]$ vedoucí koeficient každého nenulového polynomu jednotkou. Proto pro libovolné nenulové polynomy $f, g \in R[x]$ lze postupovat podle Euklidova algoritmu. Postupně tedy dělíme se zbytkem

$$\begin{aligned} f &= g \cdot q_0 + r_0, \\ g &= r_0 \cdot q_1 + r_1, \\ r_0 &= r_1 \cdot q_2 + r_2, \\ r_1 &= r_2 \cdot q_3 + r_3, \end{aligned}$$

Euklidův algoritmus v okruhu polynomů nad tělesem

Poznámka. Je-li R je těleso, je v $R[x]$ vedoucí koeficient každého nenulového polynomu jednotkou. Proto pro libovolné nenulové polynomy $f, g \in R[x]$ lze postupovat podle Euklidova algoritmu. Postupně tedy dělíme se zbytkem

$$\begin{aligned} f &= g \cdot q_0 + r_0, \\ g &= r_0 \cdot q_1 + r_1, \\ r_0 &= r_1 \cdot q_2 + r_2, \\ r_1 &= r_2 \cdot q_3 + r_3, \\ &\vdots \\ r_{n-2} &= r_{n-1} \cdot q_n + r_n, \end{aligned}$$

Euklidův algoritmus v okruhu polynomů nad tělesem

Poznámka. Je-li R je těleso, je v $R[x]$ vedoucí koeficient každého nenulového polynomu jednotkou. Proto pro libovolné nenulové polynomy $f, g \in R[x]$ lze postupovat podle Euklidova algoritmu. Postupně tedy dělíme se zbytkem

$$\begin{aligned} f &= g \cdot q_0 + r_0, \\ g &= r_0 \cdot q_1 + r_1, \\ r_0 &= r_1 \cdot q_2 + r_2, \\ r_1 &= r_2 \cdot q_3 + r_3, \\ &\vdots \\ r_{n-2} &= r_{n-1} \cdot q_n + r_n, \\ r_{n-1} &= r_n \cdot q_{n+1} + 0. \end{aligned}$$

Přitom $\mathrm{st}(g) > \mathrm{st}(r_0) > \mathrm{st}(r_1) > \mathrm{st}(r_2) > \ldots$, proto skutečně po několika děleních nastane $r_{n+1} = 0$.

Největší společný dělitel v okruhu polynomů nad tělesem

Věta. *Nechť R je těleso. Pak libovolné dva nenulové polynomy $f, g \in R[x]$ mají v $R[x]$ největší společný dělitel $d \in R[x]$, který je možné spočítat pomocí Euklidova algoritmu (jako poslední nenulový zbytek v prováděných děleních) a vyjádřit jej Bezoutovou rovností, tj. existují $a, b \in R[x]$ tak, že $d = a \cdot f + b \cdot g$.*

Největší společný dělitel v okruhu polynomů nad tělesem

Věta. *Nechť R je těleso. Pak libovolné dva nenulové polynomy $f, g \in R[x]$ mají v $R[x]$ největší společný dělitel $d \in R[x]$, který je možné spočítat pomocí Euklidova algoritmu (jako poslední nenulový zbytek v prováděných děleních) a vyjádřit jej Bezoutovou rovností, tj. existují $a, b \in R[x]$ tak, že $d = a \cdot f + b \cdot g$.*

[Věta 5.18, str. 83], [Věta 5.20, str. 84]

Definice. Nenulový polynom se nazývá **normovaný**, je-li jeho vedoucí koeficient roven 1.

Největší společný dělitel v okruhu polynomů nad tělesem

Věta. *Nechť R je těleso. Pak libovolné dva nenulové polynomy $f, g \in R[x]$ mají v $R[x]$ největší společný dělitel $d \in R[x]$, který je možné spočítat pomocí Euklidova algoritmu (jako poslední nenulový zbytek v prováděných děleních) a vyjádřit jej Bezoutovou rovností, tj. existují $a, b \in R[x]$ tak, že $d = a \cdot f + b \cdot g$.*

[Věta 5.18, str. 83], [Věta 5.20, str. 84]

Definice. Nenulový polynom se nazývá **normovaný**, je-li jeho vedoucí koeficient roven 1.

Poznámka. Je-li R těleso, je $R[x]$ obor integrity a platí $(R[x])^\times = R^\times = R^*$. Je tedy každý nenulový polynom z $R[x]$ asociovaný s právě jedním normovaným polynomem.

Největší společný dělitel v okruhu polynomů nad tělesem

Věta. *Nechť R je těleso. Pak libovolné dva nenulové polynomy $f, g \in R[x]$ mají v $R[x]$ největší společný dělitel $d \in R[x]$, který je možné spočítat pomocí Euklidova algoritmu (jako poslední nenulový zbytek v prováděných děleních) a vyjádřit jej Bezoutovou rovností, tj. existují $a, b \in R[x]$ tak, že $d = a \cdot f + b \cdot g$.*

[Věta 5.18, str. 83], [Věta 5.20, str. 84]

Definice. Nenulový polynom se nazývá **normovaný**, je-li jeho vedoucí koeficient roven 1.

Poznámka. Je-li R těleso, je $R[x]$ obor integrity a platí $(R[x])^\times = R^\times = R^*$. Je tedy každý nenulový polynom z $R[x]$ asociovaný s právě jedním normovaným polynomem.

Definice. Nechť R je těleso, $f, g \in R[x]$ nenulové polynomy. Označme (f, g) normovaný největší společný dělitel polynomů f a g.

Největší společný dělitel v okruhu polynomů nad tělesem

Věta. *Nechť R je těleso. Pak libovolné dva nenulové polynomy $f, g \in R[x]$ mají v $R[x]$ největší společný dělitel $d \in R[x]$, který je možné spočítat pomocí Euklidova algoritmu (jako poslední nenulový zbytek v prováděných děleních) a vyjádřit jej Bezoutovou rovností, tj. existují $a, b \in R[x]$ tak, že $d = a \cdot f + b \cdot g$.*

[Věta 5.18, str. 83], [Věta 5.20, str. 84]

Definice. Nenulový polynom se nazývá **normovaný**, je-li jeho vedoucí koeficient roven 1.

Poznámka. Je-li R těleso, je $R[x]$ obor integrity a platí $(R[x])^\times = R^\times = R^*$. Je tedy každý nenulový polynom z $R[x]$ asociovaný s právě jedním normovaným polynomem.

Definice. Nechť R je těleso, $f, g \in R[x]$ nenulové polynomy. Označme (f, g) normovaný největší společný dělitel polynomů f a g. O polynomech f a g řekneme, že jsou **nesoudělné**, je-li $(f, g) = 1$.

Největší společný dělitel v okruhu polynomů nad tělesem

Věta. *Nechť R je těleso. Pak libovolné dva nenulové polynomy $f, g \in R[x]$ mají v $R[x]$ největší společný dělitel $d \in R[x]$, který je možné spočítat pomocí Euklidova algoritmu (jako poslední nenulový zbytek v prováděných děleních) a vyjádřit jej Bezoutovou rovností, tj. existují $a, b \in R[x]$ tak, že $d = a \cdot f + b \cdot g$.*

[Věta 5.18, str. 83], [Věta 5.20, str. 84]

Definice. Nenulový polynom se nazývá **normovaný**, je-li jeho vedoucí koeficient roven 1.

Poznámka. Je-li R těleso, je $R[x]$ obor integrity a platí $(R[x])^\times = R^\times = R^*$. Je tedy každý nenulový polynom z $R[x]$ asociovaný s právě jedním normovaným polynomem.

Definice. Nechť R je těleso, $f, g \in R[x]$ nenulové polynomy. Označme (f, g) normovaný největší společný dělitel polynomů f a g. O polynomech f a g řekneme, že jsou **nesoudělné**, je-li $(f, g) = 1$.

Věta. *Nechť R je těleso, $f, g, h \in R[x]$ nenulové polynomy. Jestliže $f \mid g \cdot h$ a současně $(f, g) = 1$, pak $f \mid h$.* [Věta 5.23, str. 85]

Ireducibilní polynomy

Věta. *Nechť R je těleso, $f \in R[x]$. Polynom f je ireducibilní prvek okruhu $R[x]$, právě když f není konstantní a nelze jej rozložit na součin dvou nekonstantních polynomů z okruhu $R[x]$.*

Ireducibilní polynomy

Věta. *Nechť R je těleso, $f \in R[x]$. Polynom f je ireducibilní prvek okruhu $R[x]$, právě když f není konstantní a nelze jej rozložit na součin dvou nekonstantních polynomů z okruhu $R[x]$.* [Věta 5.24, str. 85]

Definice. Nechť R je okruh, $f \in R[x]$ se nazývá **ireducibilní polynom nad** R, jestliže f není konstantní a nelze jej rozložit na součin dvou nekonstantních polynomů z okruhu $R[x]$.

Ireducibilní polynomy

Věta. *Nechť R je těleso, $f \in R[x]$. Polynom f je ireducibilní prvek okruhu $R[x]$, právě když f není konstantní a nelze jej rozložit na součin dvou nekonstantních polynomů z okruhu $R[x]$.* [Věta 5.24, str. 85]

Definice. Nechť R je okruh, $f \in R[x]$ se nazývá **ireducibilní polynom nad** R, jestliže f není konstantní a nelze jej rozložit na součin dvou nekonstantních polynomů z okruhu $R[x]$.

Varování. Pozor, rozlišujte pojmy „ireducibilní polynom nad okruhem R“ a „ireducibilní prvek okruhu $R[x]$.“

Ireducibilní polynomy

Věta. *Nechť R je těleso, $f \in R[x]$. Polynom f je ireducibilní prvek okruhu $R[x]$, právě když f není konstantní a nelze jej rozložit na součin dvou nekonstantních polynomů z okruhu $R[x]$.* [Věta 5.24, str. 85]

Definice. Nechť R je okruh, $f \in R[x]$ se nazývá **ireducibilní polynom nad** R, jestliže f není konstantní a nelze jej rozložit na součin dvou nekonstantních polynomů z okruhu $R[x]$.

Varování. Pozor, rozlišujte pojmy „ireducibilní polynom nad okruhem R“ a „ireducibilní prvek okruhu $R[x]$.“

Příklad. Je-li R těleso, jsou ireducibilní polynomy nad R právě ireducibilními prvky okruhu $R[x]$.

Ireducibilní polynomy

Věta. *Nechť R je těleso, $f \in R[x]$. Polynom f je ireducibilní prvek okruhu $R[x]$, právě když f není konstantní a nelze jej rozložit na součin dvou nekonstantních polynomů z okruhu $R[x]$.* [Věta 5.24, str. 85]

Definice. Nechť R je okruh, $f \in R[x]$ se nazývá **ireducibilní polynom nad** R, jestliže f není konstantní a nelze jej rozložit na součin dvou nekonstantních polynomů z okruhu $R[x]$.

Varování. Pozor, rozlišujte pojmy „ireducibilní polynom nad okruhem R“ a „ireducibilní prvek okruhu $R[x]$.“

Příklad. Je-li R těleso, jsou ireducibilní polynomy nad R právě ireducibilními prvky okruhu $R[x]$.

Příklad. Konstantní polynom 2 je ireducibilním prvkem okruhu $\mathbb{Z}[x]$, ale není ireducibilním polynomem nad $\mathbb{Z}$.

Ireducibilní polynomy

Věta. *Nechť R je těleso, $f \in R[x]$. Polynom f je ireducibilní prvek okruhu $R[x]$, právě když f není konstantní a nelze jej rozložit na součin dvou nekonstantních polynomů z okruhu $R[x]$.* [Věta 5.24, str. 85]

Definice. Nechť R je okruh, $f \in R[x]$ se nazývá **ireducibilní polynom nad** R, jestliže f není konstantní a nelze jej rozložit na součin dvou nekonstantních polynomů z okruhu $R[x]$.

Varování. Pozor, rozlišujte pojmy „ireducibilní polynom nad okruhem R“ a „ireducibilní prvek okruhu $R[x]$.“

Příklad. Je-li R těleso, jsou ireducibilní polynomy nad R právě ireducibilními prvky okruhu $R[x]$.

Příklad. Konstantní polynom 2 je ireducibilním prvkem okruhu $\mathbb{Z}[x]$, ale není ireducibilním polynomem nad $\mathbb{Z}$. Polynom $2x$ je ireducibilní polynom nad $\mathbb{Z}$, ale není ireducibilním prvkem okruhu $\mathbb{Z}[x]$.

Ireducibilní polynomy

Věta. *Nechť R je těleso, $f \in R[x]$. Polynom f je ireducibilní prvek okruhu $R[x]$, právě když f není konstantní a nelze jej rozložit na součin dvou nekonstantních polynomů z okruhu $R[x]$.* [Věta 5.24, str. 85]

Definice. Nechť R je okruh, $f \in R[x]$ se nazývá **ireducibilní polynom nad** R, jestliže f není konstantní a nelze jej rozložit na součin dvou nekonstantních polynomů z okruhu $R[x]$.

Varování. Pozor, rozlišujte pojmy „ireducibilní polynom nad okruhem R“ a „ireducibilní prvek okruhu $R[x]$.“

Příklad. Je-li R těleso, jsou ireducibilní polynomy nad R právě ireducibilními prvky okruhu $R[x]$.

Příklad. Konstantní polynom 2 je ireducibilním prvkem okruhu $\mathbb{Z}[x]$, ale není ireducibilním polynomem nad $\mathbb{Z}$. Polynom $2x$ je ireducibilní polynom nad $\mathbb{Z}$, ale není ireducibilním prvkem okruhu $\mathbb{Z}[x]$.

Věta. *Nechť R je těleso, $f, g, h \in R[x]$ polynomy, přičemž f je ireducibilní nad R. Jestliže $f \mid g \cdot h$, pak $f \mid g$ nebo $f \mid h$.*

Okruh polynomů nad libovolným tělesem je okruhem s jednoznačným rozkladem

Věta. *Nechť R je těleso, $f \in R[x]$ nenulový polynom. Pak existují $k \in \mathbb{Z}$, $k \geq 0$, $a \in R^*$ a polynomy $p_1, \ldots, p_k \in R[x]$, které jsou normované a ireducibilní nad R, tak, že*

$$f = a \cdot p_1 \cdot \ \ldots \ \cdot p_k.$$

Okruh polynomů nad libovolným tělesem je okruhem s jednoznačným rozkladem

Věta. *Nechť R je těleso, $f \in R[x]$ nenulový polynom. Pak existují $k \in \mathbb{Z}$, $k \geq 0$, $a \in R^*$ a polynomy $p_1, \ldots, p_k \in R[x]$, které jsou normované a ireducibilní nad R, tak, že*

$$f = a \cdot p_1 \cdot \ \ldots \ \cdot p_k.$$

Tento rozklad je navíc jednoznačný až na pořadí činitelů. [Věta 5.27, str. 86]

Okruh polynomů nad libovolným tělesem je okruhem s jednoznačným rozkladem

Věta. *Nechť R je těleso, $f \in R[x]$ nenulový polynom. Pak existují $k \in \mathbb{Z}$, $k \geq 0$, $a \in R^*$ a polynomy $p_1, \ldots, p_k \in R[x]$, které jsou normované a ireducibilní nad R, tak, že*

$$f = a \cdot p_1 \cdot \ \ldots \ \cdot p_k.$$

Tento rozklad je navíc jednoznačný až na pořadí činitelů. [Věta 5.27, str. 86]

Důsledek. *Jestliže R je těleso, je $R[x]$ okruh s jednoznačným rozkladem.*

Okruh polynomů nad libovolným tělesem je okruhem s jednoznačným rozkladem

Věta. *Nechť R je těleso, $f \in R[x]$ nenulový polynom. Pak existují $k \in \mathbb{Z}$, $k \geq 0$, $a \in R^*$ a polynomy $p_1, \ldots, p_k \in R[x]$, které jsou normované a ireducibilní nad R, tak, že*

$$f = a \cdot p_1 \cdot \ \ldots \ \cdot p_k.$$

Tento rozklad je navíc jednoznačný až na pořadí činitelů. [Věta 5.27, str. 86]

Důsledek. *Jestliže R je těleso, je $R[x]$ okruh s jednoznačným rozkladem.*

Poznámka. Předchozí důsledek lze značně zesílit, platí totiž následující věta:

Věta. *Nechť R je okruh. Pak okruh polynomů $R[x]$ je okruhem s jednoznačným rozkladem, právě když okruh R je okruhem s jednoznačným rozkladem.*

Okruh polynomů nad libovolným tělesem je okruhem s jednoznačným rozkladem

Věta. *Nechť R je těleso, $f \in R[x]$ nenulový polynom. Pak existují $k \in \mathbb{Z}$, $k \geq 0$, $a \in R^*$ a polynomy $p_1, \ldots, p_k \in R[x]$, které jsou normované a ireducibilní nad R, tak, že*

$$f = a \cdot p_1 \cdot \ \ldots \ \cdot p_k.$$

Tento rozklad je navíc jednoznačný až na pořadí činitelů. [Věta 5.27, str. 86]

Důsledek. *Jestliže R je těleso, je $R[x]$ okruh s jednoznačným rozkladem.*

Poznámka. Předchozí důsledek lze značně zesílit, platí totiž následující věta:

Věta. *Nechť R je okruh. Pak okruh polynomů $R[x]$ je okruhem s jednoznačným rozkladem, právě když okruh R je okruhem s jednoznačným rozkladem.* [Větu uvádíme bez důkazu.]

Důsledek. *Okruh $\mathbb{Z}[x]$ je okruhem s jednoznačným rozkladem.*