Matematika IV – 5. přednáška
Okruhy a tělesa, okruhy polynomů

Michal Bulant

Masarykova univerzita
Fakulta informatiky

22. 3. 2010

Obsah přednášky

Doporučené zdroje

- Martin Panák, Jan Slovák, **Drsná matematika**, *e*-text.
- *Předmětové záložky v IS MU*

Doporučené zdroje

- Martin Panák, Jan Slovák, **Drsná matematika**, *e*-text.
- *Předmětové záložky v IS MU*
- R. B. Ash, Abstract algebra, `http://www.math.uiuc.edu/~r-ash/Algebra.html`.
- Jiří Rosický, *Algebra*, PřF MU, 2002.
- Peter J. Cameron. *Introduction to algebra*, Oxford University Press, 2001, 295 s. (Dostupné v knihovně PřF).
- Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone , *Handbook of Applied Cryptography*, CRC Press, 2001, 780 p., `http://www.cacr.math.uwaterloo.ca/hac/`

Plán přednášky

Okruhy

S grupami se potkáváme nejčastěji jako s množinami transformací. U skalárů ale vystupovalo hned více obdobných struktur zároveň. Jako standardní příklady mějme na mysli **skaláry** (tj. celá čísla $\mathbb{Z}$, racionální čísla $\mathbb{Q}$, reální či komplexní čísla $\mathbb{R}, \mathbb{C}$) a **množiny polynomů nad takovými skaláry** R. Klasickým příkladem konečného okruhu je pak $\mathbb{Z}_m$.

Okruhy

S grupami se potkáváme nejčastěji jako s množinami transformací. U skalárů ale vystupovalo hned více obdobných struktur zároveň. Jako standardní příklady mějme na mysli **skaláry** (tj. celá čísla $\mathbb{Z}$, racionální čísla $\mathbb{Q}$, reální či komplexní čísla $\mathbb{R}, \mathbb{C}$) a **množiny polynomů nad takovými skaláry** R. Klasickým příkladem konečného okruhu je pak $\mathbb{Z}_m$.

Definice

Komutativní grupa $(R, +)$ s neutrálním prvkem $0 \in R$, spolu s operací $\cdot$ se nazývá **komutativní okruh** $(R, +, \cdot)$, pokud splňuje

- $(a \cdot b) \cdot c = a \cdot (b \cdot c)$, pro všechny $a, b, c \in R$ *(asociativita)*;
- $a \cdot b = b \cdot a$, pro všechny $a, b \in R$ *(komutativita)*;
- existuje prvek 1 takový, že pro všechny $a \in R$ platí $1 \cdot a = a$ *(existence jedničky)*;
- $a \cdot (b + c) = a \cdot b + a \cdot c$, pro všechny $a, b, c \in R$ *(distributivita)*.

Definice

Jestliže v komutativním okruhu R platí $c \cdot d = 0$ právě, když je alespoň jeden z prvků c a d nulový, pak okruh R nazýváme **oborem integrity**.

Příklad

- Okruhy $(\mathbb{Z}, +, \cdot), (\mathbb{Q}, +, \cdot)$ jsou obory integrity.
- Okruh Gaussových celých čísel $\mathbb{Z}[i] = \{a + bi; a, b \in \mathbb{Z}\}$ je oborem integrity.
- Okruh $(\mathbb{Z}_4, +, \cdot)$ není obor integrity, narozdíl od $(\mathbb{Z}_5, +, \cdot)$.

Definice

Jestliže v komutativním okruhu R platí $c \cdot d = 0$ právě, když je alespoň jeden z prvků c a d nulový, pak okruh R nazýváme **oborem integrity**.

Příklad

- Okruhy $(\mathbb{Z}, +, \cdot), (\mathbb{Q}, +, \cdot)$ jsou obory integrity.
- Okruh Gaussových celých čísel $\mathbb{Z}[i] = \{a + bi; a, b \in \mathbb{Z}\}$ je oborem integrity.
- Okruh $(\mathbb{Z}_4, +, \cdot)$ není obor integrity, narozdíl od $(\mathbb{Z}_5, +, \cdot)$.

Pokud neplatí vlastnost komutativity operace $\cdot$, hovoříme o nekomutativním okruhu (nebo pouze o okruhu). V dalším se obvykle omezíme pouze na okruhy komutativní.

Definice

Jestliže v komutativním okruhu R platí $c \cdot d = 0$ právě, když je alespoň jeden z prvků c a d nulový, pak okruh R nazýváme **oborem integrity**.

Příklad

- Okruhy $(\mathbb{Z}, +, \cdot), (\mathbb{Q}, +, \cdot)$ jsou obory integrity.
- Okruh Gaussových celých čísel $\mathbb{Z}[i] = \{a + bi; a, b \in \mathbb{Z}\}$ je oborem integrity.
- Okruh $(\mathbb{Z}_4, +, \cdot)$ není obor integrity, narozdíl od $(\mathbb{Z}_5, +, \cdot)$.

Pokud neplatí vlastnost komutativity operace $\cdot$, hovoříme o nekomutativním okruhu (nebo pouze o okruhu). V dalším se obvykle omezíme pouze na okruhy komutativní.
Operaci $+$ budeme říkat **sčítání** a operaci $\cdot$ **násobení**. Navíc budeme vždy předpokládat existenci **jedničky** 1 pro operaci násobení, neutrálnímu prvku pro sčítání říkáme **nula**.

Základní vlastnosti operací v okruhu

V každém komutativním okruhu R s jedničkou platí následující vztahy (které nám jistě připadají samozřejmé u skalárů)

1. $0 \cdot c = c \cdot 0 = 0$ pro všechny $c \in R$,
2. $-c = (-1) \cdot c = c \cdot (-1)$ pro všechny $c \in R$,
3. $-(c \cdot d) = (-c) \cdot d = c \cdot (-d)$ pro všechny $c, d \in R$,
4. $a \cdot (b - c) = a \cdot b - a \cdot c$,

Dělitelnost v okruhu

Obecně říkáme, že $a \in R$ **dělí** $c \in R$, jestliže existuje b tak, že $a \cdot b = c$. Skutečnost že $c \in R$ je dělitelné $a \in R$ zapisujeme $a|c$.

Dělitelnost v okruhu

Obecně říkáme, že $a \in R$ **dělí** $c \in R$, jestliže existuje b tak, že $a \cdot b = c$. Skutečnost že $c \in R$ je dělitelné $a \in R$ zapisujeme $a|c$. Dodatečnou vlastností oboru integrity oproti obecnému okruhu je **neexistence netriviálních dělitelů nuly**. Okamžitě odtud také vyplývá jednoznačnost dělitelů:

Dělitelnost v okruhu

Obecně říkáme, že $a \in R$ **dělí** $c \in R$, jestliže existuje b tak, že $a \cdot b = c$. Skutečnost že $c \in R$ je dělitelné $a \in R$ zapisujeme $a|c$. Dodatečnou vlastností oboru integrity oproti obecnému okruhu je **neexistence netriviálních dělitelů nuly**. Okamžitě odtud také vyplývá jednoznačnost dělitelů:

Věta

Platí-li v oboru integrity $a = b \cdot c$ a $b \neq 0$, pak c je jednoznačně dáno volbou a, b.

Dělitelnost v okruhu

Obecně říkáme, že $a \in R$ **dělí** $c \in R$, jestliže existuje b tak, že $a \cdot b = c$. Skutečnost že $c \in R$ je dělitelné $a \in R$ zapisujeme $a|c$. Dodatečnou vlastností oboru integrity oproti obecnému okruhu je **neexistence netriviálních dělitelů nuly**. Okamžitě odtud také vyplývá jednoznačnost dělitelů:

Věta

Platí-li v oboru integrity $a = b \cdot c$ a $b \neq 0$, pak c je jednoznačně dáno volbou a, b.

Důkaz.

Pro $a = bc = bc'$ totiž platí $0 = b \cdot (c - c')$ a $b \neq 0$, proto $c = c'$. □

Dělitelé jedničky, tj. invertibilní prvky v R, se nazývají **jednotky**. Jednotky v komutativním okruhu vždy tvoří komutativní grupu. Netriviální (komutativní) okruh, ve kterém jsou všechny nenulové prvky invertibilní, se nazývá (komutativní) **těleso**.

Dělitelé jedničky, tj. invertibilní prvky v R, se nazývají **jednotky**.
Jednotky v komutativním okruhu vždy tvoří komutativní grupu.
Netriviální (komutativní) okruh, ve kterém jsou všechny nenulové prvky invertibilní, se nazývá (komutativní) **těleso**.
V české literatuře se někdy v případě komutativního tělesa můžete setkat s pojmenováním **pole** (z angl. *field*).

Typickým příkladem komutativních těles jsou číselné obory $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$. Dále pak všechny okruhy zbytkových tříd $\mathbb{Z}_p$ s prvočíselným p.

Typickým příkladem komutativních těles jsou číselné obory $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$. Dále pak všechny okruhy zbytkových tříd $\mathbb{Z}_p$ s prvočíselným p. Základním příkladem nekomutativního okruhu s jedničkou je množina $\mathrm{Mat}_k(R)$ všech čtvercových matic nad okruhem R s k řádky a sloupci. Jak jsme viděli dávno, není to ani obor integrity.

Typickým příkladem komutativních těles jsou číselné obory $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$. Dále pak všechny okruhy zbytkových tříd $\mathbb{Z}_p$ s prvočíselným p. Základním příkladem nekomutativního okruhu s jedničkou je množina $\mathrm{Mat}_k(R)$ všech čtvercových matic nad okruhem R s k řádky a sloupci. Jak jsme viděli dávno, není to ani obor integrity. Jako příklad nekomutativního okruhu, kde existují inverze k nenulovým prvkům (tzv. okruh s dělením) uveďme okruh kvaternionů

$$\mathbb{H} = \{a + b \cdot i + c \cdot j + d \cdot k;\ a, b, c, d \in \mathbb{R}\},$$

se sčítáním *po složkách* a násobením odvozeným ze základních relací

$$i^2 = j^2 = k^2 = -1, \quad ij = -ji = k, \quad jk = -kj = i, \quad ki = -ik = j.$$

Obor integrity vs. těleso

Věta

Každý konečný obor integrity je těleso.

Důkaz.

Dokazuje se prostřednictvím homomorfismu $f : R \to R$, $f(x) = ax$ (je to injekce, proto surjekce, proto je R těleso (rozmyslete!). □

Obor integrity vs. těleso

Věta

Každý konečný obor integrity je těleso.

Důkaz.

Dokazuje se prostřednictvím homomorfismu $f : R \to R$, $f(x) = ax$ (je to injekce, proto surjekce, proto je R těleso (rozmyslete!). □

A co obráceně? Samozřejmě je každé těleso oborem integrity.

Obor integrity vs. těleso

Věta

Každý konečný obor integrity je těleso.

Důkaz.

Dokazuje se prostřednictvím homomorfismu $f : R \to R$, $f(x) = ax$ (je to injekce, proto surjekce, proto je R těleso (rozmyslete!). □

A co obráceně? Samozřejmě je každé těleso oborem integrity.

Příklad

Zřejmě je např. $\mathbb{Z}$ obor integrity, který není těleso.

Polynomy

Polynomem rozumíme jakýkoliv konečný výraz, který lze poskládat ze známých konstantních prvků R a jedné neznámé proměnné pomocí operací sčítání a násobení:

Polynomy

Polynomem rozumíme jakýkoliv konečný výraz, který lze poskládat ze známých konstantních prvků R a jedné neznámé proměnné pomocí operací sčítání a násobení:

Definice

Nechť R je jakýkoliv (dále vždy) komutativní okruh skalárů. Polynomem nad R rozumíme konečný výraz

$$f(x) = \sum_{i=0}^{k} a_i x^i$$

kde $a_i \in R$, $i = 0, 1, \ldots, k$, jsou tzv. **koeficienty polynomu**. Je-li $a_k \neq 0$, říkáme, že $f(x)$ má **stupeň** k, píšeme $\operatorname{st} f = k$. Nulový polynom nemá stupeň, polynomy stupně nula jsou právě nenulové prvky v R, kterým říkáme konstantní polynomy.

Polynomy

Polynomem rozumíme jakýkoliv konečný výraz, který lze poskládat ze známých konstantních prvků R a jedné neznámé proměnné pomocí operací sčítání a násobení:

Definice

Nechť R je jakýkoliv (dále vždy) komutativní okruh skalárů.
Polynomem nad R rozumíme konečný výraz

$$f(x) = \sum_{i=0}^{k} a_i x^i$$

kde $a_i \in R$, $i = 0, 1, \ldots, k$, jsou tzv. **koeficienty polynomu**. Je-li $a_k \neq 0$, říkáme, že $f(x)$ má **stupeň** k, píšeme $\operatorname{st} f = k$. Nulový polynom nemá stupeň, polynomy stupně nula jsou právě nenulové prvky v R, kterým říkáme konstantní polynomy.
Polynomy $f(x)$ a $g(x)$ jsou stejné, jestliže mají stejné koeficienty.
Množinu všech polynomů nad okruhem R budeme značit $R[x]$.

Každý polynom zadává zobrazení $f : R \to R$, jehož hodnota vznikne dosazením hodnoty c za nezávislou proměnnou x, tj.

$$f(c) = a_0 + a_1 c + \cdots + a_k c^k.$$

Všimněme si, že konstantní polynomy odpovídají právě konstantním zobrazením.

Každý polynom zadává zobrazení $f : R \to R$, jehož hodnota vznikne dosazením hodnoty c za nezávislou proměnnou x, tj.

$$f(c) = a_0 + a_1 c + \cdots + a_k c^k.$$

Všimněme si, že konstantní polynomy odpovídají právě konstantním zobrazením.

Kořen polynomu $f(x)$ je takový prvek $c \in R$, pro který je $f(c) = 0 \in R$.

Každý polynom zadává zobrazení $f : R \to R$, jehož hodnota vznikne dosazením hodnoty c za nezávislou proměnnou x, tj.

$$f(c) = a_0 + a_1 c + \cdots + a_k c^k.$$

Všimněme si, že konstantní polynomy odpovídají právě konstantním zobrazením.

Kořen polynomu $f(x)$ je takový prvek $c \in R$, pro který je $f(c) = 0 \in R$.

Obecně se může stát, že různé polynomy definují stejná zobrazení. Např. polynom $x^2 + x \in \mathbb{Z}_2[x]$ zadává identicky nulové zobrazení. Obecněji, pro každý konečný okruh $R = \{a_0, a_1, \ldots, a_k\}$ zadává polynom $f(x) = (x - a_0)(x - a_1)\ldots(x - a_k)$ identicky nulové zobrazení. Zároveň ale platí tvrzení, které dokážeme zanedlouho:

Věta

Jestliže je R nekonečný okruh, pak dva polynomy $f(x)$ a $g(x)$ nad R jsou stejné právě tehdy, když jsou stejná příslušná zobrazení f a g.

Dva polynomy $f(x) = \sum_i a_i x^i$ a $g(x) = \sum_i b_i x^i$ umíme přirozeně také sčítat i násobit:

$$(f + g)(x) = (a_0 + b_0) + (a_1 + b_1)x + \cdots + (a_k + b_k)x^k$$
$$(f \cdot g)(x) = (a_0 b_0) + \cdots + (a_0 b_\ell + + \cdots + a_\ell b_0)x^\ell + \ldots$$

kde uvažujeme nulové koeficienty všude, kde v původním výrazu pro polynomy nenulové koeficienty nejsou a u sčítání nechť je k maximální ze stupňů f a g.

Tato definice vskutku odpovídá příslušným operacím sčítání a násobení hodnot zobrazení f, $g : R \to R$, díky vlastnostem *skalárů* v původním okruhu R.

Tato definice vskutku odpovídá příslušným operacím sčítání a násobení hodnot zobrazení $f, g : R \to R$, díky vlastnostem *skalárů* v původním okruhu R.
Přímo z definice vyplývá, že množina polynomů $R[x]$ nad komutativním okruhem s jedničkou je opět komutativním okruhem s jedničkou, přičemž jedničkou v $R[x]$ je opět jednička 1 v okruhu R vnímaná jako polynom stupně nula.

Lemma

Okruh polynomů nad oborem integrity je opět obor integrity.

Tato definice vskutku odpovídá příslušným operacím sčítání a násobení hodnot zobrazení $f, g : R \to R$, díky vlastnostem *skalárů* v původním okruhu R.
Přímo z definice vyplývá, že množina polynomů $R[x]$ nad komutativním okruhem s jedničkou je opět komutativním okruhem s jedničkou, přičemž jedničkou v $R[x]$ je opět jednička 1 v okruhu R vnímaná jako polynom stupně nula.

Lemma

Okruh polynomů nad oborem integrity je opět obor integrity.

Důkaz.

Máme ukázat, že v $R[x]$ mohou být netriviální dělitelé nuly pouze tehdy, jestliže jsou už v R. To je ale zřejmé z definice násobení polynomů. Jsou-li $f(x)$ a $g(x)$ polynomy stupně k a ℓ jako výše, pak koeficient u $x^{k+\ell}$ v součinu $f(x) \cdot g(x)$ je součin $a_k \cdot b_\ell$ a ten musí být nenulový, pokud nejsou dělitelé nuly v R. □

Formální mocninné řady

V Matematice III jsme pracovali s formálními mocninnými řadami a neformálně jsme prohlásili, že *s nimi můžeme provádět analogické operace jako s polynomy*. Nyní toto tvrzení můžeme zasadit do formálního algebraického kontextu:

Formální mocninné řady

V Matematice III jsme pracovali s formálními mocninnými řadami a neformálně jsme prohlásili, že *s nimi můžeme provádět analogické operace jako s polynomy*. Nyní toto tvrzení můžeme zasadit do formálního algebraického kontextu:

Definice

Nechť R je okruh skalárů. *Formální mocninou řadou* nad R rozumíme (obecně nekonečný) **formální** výraz $f(x) = \sum_{i=0}^{\infty} a_i x^i$, kde $a_i \in R$, $i = 0, 1, \ldots$, jsou tzv. **koeficienty řady**.

Formální mocninné řady

V Matematice III jsme pracovali s formálními mocninnými řadami a neformálně jsme prohlásili, že *s nimi můžeme provádět analogické operace jako s polynomy*. Nyní toto tvrzení můžeme zasadit do formálního algebraického kontextu:

Definice

Nechť R je okruh skalárů. *Formální mocninou řadou* nad R rozumíme (obecně nekonečný) **formální** výraz $f(x) = \sum_{i=0}^{\infty} a_i x^i$, kde $a_i \in R$, $i = 0, 1, \ldots$, jsou tzv. **koeficienty řady**.

Snadno se ukáže, že s dříve definovanými operacemi sčítání a násobení tvoří formální mocniné řady okruh, který značíme $R[[x]]$ (a jehož je $R[x]$ podokruhem). Sami si zkuste rozmyslet, které prvky tohoto okruhu jsou invertibilní.

Plán přednášky

Směřujeme nyní ke zobecnění rozkladů polynomů nad číselnými obory a k tomu nejprve potřebujeme ujasnit, co je dělitelnost v základním okruhu R samotném. Uvažujme proto nějaký pevně zvolený obor integrity R[1], třeba celá čísla $\mathbb{Z}$ nebo okruh $\mathbb{Z}_p$ s prvočíselným p. V R definujeme dělitelnost analogicky jako to známe ze $\mathbb{Z}$: $b|a \iff \exists c \in R : a = b \cdot c$.

[1] Obor integrity proto, aby bylo jednoznačné dělení!

Směřujeme nyní ke zobecnění rozkladů polynomů nad číselnými obory a k tomu nejprve potřebujeme ujasnit, co je dělitelnost v základním okruhu R samotném. Uvažujme proto nějaký pevně zvolený obor integrity R[1], třeba celá čísla $\mathbb{Z}$ nebo okruh $\mathbb{Z}_p$ s prvočíselným p. V R definujeme dělitelnost analogicky jako to známe ze $\mathbb{Z}$: $b|a \iff \exists c \in R : a = b \cdot c$.

Pak platí:

- je-li $a|b$ a zároveň $b|c$ pak také $a|c$;
- $a|b$ a zároveň $a|c$ pak také $a|(\alpha b + \beta c)$ pro všechny $\alpha, \beta \in R$;
- $a|0$ pro všechny $a \in R$ (je totiž $a \cdot 0 = 0$);
- každý prvek $a \in R$ je dělitelný všemi jednotkami $e \in R$ a jejich násobky $a \cdot e$ (jak přímo plyne z existence e^{-1})

[1] Obor integrity proto, aby bylo jednoznačné dělení!

Řekneme, že prvek $a \in R$ je **nerozložitelný** (*ireducibilní*), jestliže

- je nenulový a není jednotkou (tj. $a \nmid 1$),

Řekneme, že prvek $a \in R$ je **nerozložitelný** (*ireducibilní*), jestliže

- je nenulový a není jednotkou (tj. $a \nmid 1$),
- je dělitelný pouze jednotkami $e \in R$ a čísly $a \cdot e$ (tzv. čísla *asociovaná* s a – tj. taková $b \in R$, že $a|b$ a $b|a$).

Řekneme, že prvek $a \in R$ je **nerozložitelný** (*ireducibilní*), jestliže

- je nenulový a není jednotkou (tj. $a \nmid 1$),
- je dělitelný pouze jednotkami $e \in R$ a čísly $a \cdot e$ (tzv. čísla *asociovaná* s a – tj. taková $b \in R$, že $a|b$ a $b|a$).

Řekneme, že prvek $a \in R$ je **nerozložitelný** (*ireducibilní*), jestliže

- je nenulový a není jednotkou (tj. $a \nmid 1$),
- je dělitelný pouze jednotkami $e \in R$ a čísly $a \cdot e$ (tzv. čísla *asociovaná* s a – tj. taková $b \in R$, že $a|b$ a $b|a$).

Řekneme, že okruh R je **obor integrity s jednoznačným rozkladem**, jestliže platí:

- pro každý nenulový prvek $a \in R$, který není jednotkou, existují nerozložitelné $a_1, \ldots, a_r \in R$ takové, že $a = a_1 \cdot a_2 \ldots a_r$
- jsou-li prvky $a_1, \ldots, a_r$ a $b_1, \ldots, b_s$ nerozložitelné, nejsou mezi nimi žádné jednotky a $a_1 a_2 \ldots a_r = b_1 b_2 \ldots b_s$, pak je $r = s$ a ve vhodném přeuspořádání platí $a_j = e_j b_j$ pro vhodné jednotky e_j.

Příklad

1. $\mathbb{Z}, \mathbb{R}[x]$ jsou obory integrity s jednoznačným rozkladem (ireducibilní prvky v $\mathbb{Z}$ jsou prvočísla a čísla k nim opačná).

Příklad

1. $\mathbb{Z}, \mathbb{R}[x]$ jsou obory integrity s jednoznačným rozkladem (ireducibilní prvky v $\mathbb{Z}$ jsou prvočísla a čísla k nim opačná).
2. Každé těleso je obor integrity s jednoznačným rozkladem (kde každý nenulový prvek je jednotka).

Příklad

1. $\mathbb{Z}, \mathbb{R}[x]$ jsou obory integrity s jednoznačným rozkladem (ireducibilní prvky v $\mathbb{Z}$ jsou prvočísla a čísla k nim opačná).
2. Každé těleso je obor integrity s jednoznačným rozkladem (kde každý nenulový prvek je jednotka).
3. Např. v okruhu $\mathbb{R}[\sqrt{-5}] = \{a + b\sqrt{-5}; a, b \in \mathbb{R}\}$ existují dva různé rozklady čísla 6 na nerozložitelné prvky:

$$6 = 2 \cdot 3 = (1 - \sqrt{-5})(1 + \sqrt{-5}).^a$$

[a] To, že uvedené prvky jsou ireducibilní a že nejsou asociované, je ale třeba trochu "odpracovat".

Základním nástrojem pro diskusi dělitelnosti, společných dělitelů apod. v okruhu celých čísel $\mathbb{Z}$ je procedura dělení se zbytkem a Euklidův algoritmus pro hledání největších společných dělitelů. Tyto postupy nyní zobecníme.

Základním nástrojem pro diskusi dělitelnosti, společných dělitelů apod. v okruhu celých čísel $\mathbb{Z}$ je procedura dělení se zbytkem a Euklidův algoritmus pro hledání největších společných dělitelů. Tyto postupy nyní zobecníme.

Lemma (Věta o dělení se zbytkem pro polynomy)

Nechť R je komutativní okruh bez dělitelů nuly a $f, g \in R[x]$ polynomy, $g \neq 0$. Pak existuje $a \in R$, $a \neq 0$, a polynomy q a r splňující $af = qg + r$, kde $r = 0$ nebo $\operatorname{st} r < \operatorname{st} g$. Je-li navíc R těleso nebo je aspoň vedoucí koeficient polynomu g roven jedné, potom lze volit $a = 1$ a polynomy q a r jsou v tomto případě určeny jednoznačně.

Základním nástrojem pro diskusi dělitelnosti, společných dělitelů apod. v okruhu celých čísel $\mathbb{Z}$ je procedura dělení se zbytkem a Euklidův algoritmus pro hledání největších společných dělitelů. Tyto postupy nyní zobecníme.

Lemma (Věta o dělení se zbytkem pro polynomy)

Nechť R je komutativní okruh bez dělitelů nuly a $f, g \in R[x]$ polynomy, $g \neq 0$. Pak existuje $a \in R$, $a \neq 0$, a polynomy q a r splňující $af = qg + r$, kde $r = 0$ nebo $\operatorname{st} r < \operatorname{st} g$. Je-li navíc R těleso nebo je aspoň vedoucí koeficient polynomu g roven jedné, potom lze volit $a = 1$ a polynomy q a r jsou v tomto případě určeny jednoznačně.

Poznámka

Toto tvrzení je možné aplikovat i obecněji (viz *Euklidovské okruhy*), je ale třeba *správně* definovat, jak budeme porovnávat prvky.