Okruhy

Definice. Množina R spolu se dvěma operacemi $+$ a $\cdot$ se nazývá **okruh**, jestliže platí:

- $(R, +)$ je komutativní grupa,
- $(R, \cdot)$ je pologrupa s neutrálním prvkem,
- platí distributivní zákony, tj. pro libovolné prvky $a, b, c \in R$ je $a \cdot (b + c) = a \cdot b + a \cdot c, \quad (b + c) \cdot a = b \cdot a + c \cdot a$ (užíváme obvyklou konvenci o tom, že násobení má přednost před sčítáním).

Příklady. $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$ jsou okruhy.
Pro libovolné $m \in \mathbb{N}$ je $(\mathbb{Z}_m, +, \cdot)$ okruh.
Množina všech čtvercových matic $M_{n,n}(R)$, kde R značí $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ nebo $\mathbb{C}$ a $n \in \mathbb{N}$, tvoří okruh $(M_{n,n}(R), +, \cdot)$.
Množina všech polynomů $R[x]$, kde R značí $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ nebo $\mathbb{C}$, tvoří okruh $(R[x], +, \cdot)$.

Příklad. $(\mathbb{N}, +, \cdot)$ okruhem není.

Okruhy

Definice. $(R, +, \cdot)$ je **okruh**, jestliže:

- $(R, +)$ je komutativní grupa,
- $(R, \cdot)$ je pologrupa s neutrálním prvkem,
- platí distributivní zákony, tj. pro libovolné prvky $a, b, c \in R$ je $a \cdot (b + c) = a \cdot b + a \cdot c, \quad (b + c) \cdot a = b \cdot a + c \cdot a$.

Označení. Neutrální prvek grupy $(R, +)$ značíme 0 a nazýváme **nula okruhu** R, zatímco neutrální prvek pologrupy $(R, \cdot)$ značíme 1 a nazýváme **jednička okruhu** R.
Inverzní prvek k prvku $a \in R$ v grupě $(R, +)$ se nazývá **opačný prvek**, značíme $-a$.
Symbolem $a - b$ rozumíme $a + (-b)$.
Mocninu prvku $a \in R$ v grupě $(R, +)$ nazýváme **násobek prvku** a značíme na pro libovolné $n \in \mathbb{Z}$.
Součet $a_1 + \cdots + a_n$ prvků okruhu R lze stručně zapsat $\sum_{i=1}^{n} a_i$.

Základní vlastnosti okruhů

Definice. Okruh $(R, +, \cdot)$ se nazývá **triviální**, má-li R jediný prvek.

Věta. *Nechť R je okruh. Pak platí*

- $\forall a \in R: \ a \cdot 0 = 0 \cdot a = 0$,
- $\forall a, b \in R: \ (-a) \cdot b = a \cdot (-b) = -(a \cdot b)$,
- $\forall a, b, c \in R:$
  $a \cdot (b - c) = a \cdot b - a \cdot c, \quad (b - c) \cdot a = b \cdot a - c \cdot a$,
- $\forall n, m \in \mathbb{N} \ \forall a_1, \ldots, a_n, b_1, \ldots, b_m \in R:$
  $(a_1 + \cdots + a_n) \cdot (b_1 + \cdots + b_m) = \sum_{i=1}^{n} \sum_{j=1}^{m} a_i \cdot b_j$,
- $\forall n, m \in \mathbb{Z} \ \forall a, b \in R: \ (na) \cdot (mb) = (n \cdot m)(a \cdot b)$. [Věta 1.6, str. 58]

Věta. *Okruh R je triviální, právě když v něm platí $1 = 0$.* [Věta 1.7, str. 59]

Definice. Okruh R se nazývá **komutativní**, je-li pologrupa $(R, \cdot)$ komutativní.

Definice. Prvky a, b okruhu R se nazývají **dělitelé nuly**, jestliže $a \neq 0$, $b \neq 0$, avšak $a \cdot b = 0$.

Obory integrity

Definice. Netriviální komutativní okruh R se nazývá **obor integrity**, pokud nemá dělitele nuly.

Označení. Množinu všech nenulových prvků okruhu R značíme R^*. Netriviální komutativní okruh R je tedy obor integrity, právě když $(R^*, \cdot)$ je pologrupa.

Věta. Netriviální komutativní okruh R je obor integrity, právě když v něm platí **zákon o krácení**, *tj. pro každé $a, b, c \in R$ platí*

$$a \neq 0, \ a \cdot b = a \cdot c \quad \Rightarrow \quad b = c.$$ [Věta 1.10, str. 59]

Definice. Nechť R je okruh. Invertibilní prvek pologrupy $(R, \cdot)$ se nazývá **jednotka** okruhu R. Množinu všech jednotek okruhu R značíme $R^\times$.

Poznámka. Nezaměňujte pojmy jednička a jednotka okruhu. Okruh má jedinou jedničku, kdežto jednotek může mít více. Vždy je jednička jednotkou. Okruhy s jedinou jednotkou jsou výjimečné (například okruh $\mathbb{Z}_2$). Nezaměňujte R^* a $R^\times$. Uvědomte si, že nové označení je v souladu s užívaným $\mathbb{Z}_m^\times$.

Tělesa

$R^* = R - \{0\}$ ... množina nenulových prvků okruhu R,
$R^\times = \{a \in R;\ \exists b \in R :\ a \cdot b = b \cdot a = 1\}$ ... množina invertibilních prvků pologrupy $(R, \cdot)$.

Věta. *Nechť R je okruh. Pak $(R^\times, \cdot)$ je grupa.* [[Věta 4.7, str. 25] je užita pro pologrupu $(R, \cdot)$.]

Definice. Netriviální komutativní okruh R se nazývá **těleso**, pokud je každý jeho nenulový prvek jednotkou.

Věta. *Netriviální komutativní okruh R je těleso, právě když $R^* = R^\times$, tedy právě když $(R^*, \cdot)$ je grupa.* [Věta 1.14, str. 60]

Důsledek. *Každé těleso je oborem integrity.* [Věta 1.13, str. 60]

Příklad. Okruh celých čísel $\mathbb{Z}$ je oborem integrity, který není tělesem.

Věta. *Každý konečný obor integrity je tělesem.* [Věta 1.17, str. 61]

Věta. *Okruh zbytkových tříd $\mathbb{Z}_m$ je oborem integrity, právě když je tělesem, což nastane právě když m je prvočíslo.* [Věta 1.16, str. 61]

Charakteristika okruhu

Poznámka. Připomeňme, že v okruhu R pro libovolné $a \in R$, $n \in \mathbb{N}$ je $na = \underbrace{a + a + \cdots + a}_{n}$. Protože jedničku a nulu okruhu R značíme 1 a 0, v následující definici je rovností $n1 = 0$ nutno rozumět, že v okruhu R platí $\underbrace{1 + 1 + \cdots + 1}_{n} = 0$.

Definice. Nechť R je okruh. Nejmenší přirozené číslo n takové, že $n1 = 0$, se nazývá **charakteristika** okruhu R. Pokud takové n neexistuje (tedy pro všechna $k \in \mathbb{N}$ platí $k1 \neq 0$), řekneme, že charakteristika okruhu R je nula.

Označení. Charakteristiku okruhu R značíme $\operatorname{char} R$.

Příklady. $\operatorname{char} \mathbb{Z} = \operatorname{char} \mathbb{Q} = \operatorname{char} \mathbb{R} = \operatorname{char} \mathbb{C} = 0$, $\operatorname{char} \mathbb{Z}_m = m$.

Věta. Nechť R je okruh, $m = \operatorname{char} R$. Pak pro každé $a \in R$ platí $ma = 0$. [Věta 2.4, str. 62]

Věta. Nechť R je obor integrity, pak $\operatorname{char} R$ je buď 0, nebo prvočíslo. [Věta 2.5, str. 62]

Charakteristika okruhu

Definice. Nechť R je okruh. Nejmenší přirozené číslo n takové, že $n1 = 0$, se nazývá **charakteristika** okruhu R. Pokud takové n neexistuje (tedy pro všechna $k \in \mathbb{N}$ platí $k1 \neq 0$), řekneme, že charakteristika okruhu R je nula. Charakteristiku okruhu R značíme $\operatorname{char} R$.

Věta. *Nechť R je obor integrity. Pak pro libovolný $a \in R^*$ platí:*

- *pokud* $\operatorname{char} R = 0$, *pak pro každé* $k \in \mathbb{N}$ *je* $ka \neq 0$;
- *pokud* $\operatorname{char} R = p > 0$, *pak řád prvku a v grupě $(R, +)$ je p.*

[Věta 2.6, str. 62]

Důsledek. *Je-li R obor integrity, pak všechny nenulové prvky grupy $(R, +)$ mají stejný řád.*

Důsledek. *Je-li R konečné těleso, $p = \operatorname{char} R$, pak grupa $(R, +)$ je izomorfní s grupou $(\mathbb{Z}_p, +) \times \cdots \times (\mathbb{Z}_p, +)$, počet prvků konečného tělesa R je tedy mocninou jeho prvočíselné charakteristiky p.* [Poznámka 2.8, str. 62]

Homomorfismus okruhů

Definice. Nechť $(R, +, \cdot)$ a $(S, +, \cdot)$ jsou okruhy, $f : R \to S$ zobrazení. Řekneme, že f je **homomorfismus** okruhu R do okruhu S, jestliže

- pro každé $a, b \in R$ platí $f(a + b) = f(a) + f(b)$,
- pro každé $a, b \in R$ platí $f(a \cdot b) = f(a) \cdot f(b)$,
- $f(1) = 1$.

Injektivní homomorfismus se nazývá **vnoření**, bijektivní **izomorfismus**. O okruzích R, S řekneme, že jsou izomorfní, píšeme $R \cong S$, existuje-li alespoň jeden izomorfismus $R \to S$.

Příklad. Pro libovolné $m \in \mathbb{N}$ je zobrazení $\pi : \mathbb{Z} \to \mathbb{Z}_m$, určené předpisem $\pi(a) = [a]_m$ pro libovolné $a \in \mathbb{Z}$, homomorfismus okruhu $(\mathbb{Z}, +, \cdot)$ celých čísel do okruhu $(\mathbb{Z}_m, +, \cdot)$ zbytkových tříd modulo m.

Věta. Jsou-li $f : R \to S$ a $g : S \to T$ homomorfismy okruhů, pak také $g \circ f : R \to T$ je homomorfismem okruhů. [Věta 4.4, str. 73]

Homomorfismus okruhů, jeho jádro

Věta. *Nechť $f : R \to S$ je izomorfismus okruhů. Pak i inverzní zobrazení $f^{-1} : S \to R$ je izomorfismus okruhů.* [Věta 4.5, str. 73]

Důsledek. *Pro libovolné okruhy R, S, T platí: $R \cong R$; z $R \cong S$ plyne $S \cong R$; a konečně z $R \cong S$ a $S \cong T$ plyne $R \cong T$.*

Poznámka. Zapomeneme-li v okruhu R, jak se násobí, zůstane nám aditivní grupa $(R, +)$. Každý homomorfismus okruhů $f : R \to S$ je také homomorfismem aditivních grup, je tedy $f(0) = 0$, pro každé $a \in R$ platí $f(-a) = -f(a)$, a máme jeho jádro:

Definice. Nechť $f : R \to S$ je homomorfismus okruhů. Množina $\ker f = \{a \in R;\ f(a) = 0\}$ se nazývá **jádro homomorfismu** f.

Věta. *Homomorfismus okruhů $f : R \to S$ je injektivní, právě když* $\ker f = \{0\}$. [Věta 4.9, str. 74]

Příklad. Zobrazení $f : \mathbb{C} \to M_{2,2}(\mathbb{R})$, kde $f(a + bi) = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$ pro libovolné $a, b \in \mathbb{R}$, je vnoření tělesa $\mathbb{C}$ komplexních čísel do okruhu $M_{2,2}(\mathbb{R})$ matic typu 2×2.

Binomická věta

Věta (binomická). Nechť R je komutativní okruh, pak pro každé $a, b \in R$ a každé $n \in \mathbb{N}$ platí

$$(a+b)^n = \sum_{i=0}^{n} \binom{n}{i} a^{n-i} \cdot b^i,$$

kde $\binom{n}{i} = \frac{n!}{(n-i)!i!}$ značí obvyklý binomický koeficient.

Důkaz. indukcí vůči n: I. krok: případ $n = 1$ je zřejmý.
II. krok: předpokládejme, že pro nějaké $n \in \mathbb{N}$ už bylo dokázáno, dokážeme tvrzení pro $n+1$. Víme tedy
$(a+b)^n = a^n + \binom{n}{1} a^{n-1} \cdot b + \binom{n}{2} a^{n-2} \cdot b^2 + \cdots + \binom{n}{n-1} a \cdot b^{n-1} + b^n.$
Vynásobením (užíváme komutativitu okruhu)
$(a+b)^n \cdot a = a^{n+1} + \binom{n}{1} a^n \cdot b + \binom{n}{2} a^{n-1} \cdot b^2 + \cdots + \binom{n}{n} a \cdot b^n,$
$(a+b)^n \cdot b = \binom{n}{0} a^n \cdot b + \binom{n}{1} a^{n-1} \cdot b^2 + \cdots + \binom{n}{n-1} a \cdot b^n + b^{n+1}.$
Sečtením a užitím $\binom{n}{i+1} + \binom{n}{i} = \binom{n+1}{i+1}$ dostaneme
$(a+b)^{n+1} =$
$a^{n+1} + \binom{n+1}{1} a^n \cdot b + \binom{n+1}{2} a^{n-1} \cdot b^2 + \cdots + \binom{n+1}{n} a \cdot b^n + b^{n+1},$
což se mělo dokázat.

Umocnění na charakteristiku v oboru integrity

Věta. *Pro libovolné prvočíslo p a libovolné $i \in \{1, 2, \ldots, p-1\}$ platí $p \mid \binom{p}{i}$.*

Důkaz. Platí $p \mid p! = \binom{p}{i} \cdot i! \cdot (p-i)!$. Současně $p \nmid i! \cdot (p-i)!$.

Věta. *Nechť R je obor integrity charakteristiky* $\operatorname{char} R = p > 0$. *Pak pro každé $a, b \in R$ platí*

$$(a+b)^p = a^p + b^p.$$

[Věta 2.9, str. 62]

Důsledek. *Nechť R je obor integrity charakteristiky* $\operatorname{char} R = p > 0$. *Pak zobrazení $f : R \to R$, kde $f(r) = r^p$, je injektivní homomorfismus okruhů.*

Podokruh okruhu

Definice. Nechť $(R, +, \cdot)$ je okruh, H podmnožina množiny R. Řekneme, že H je **podokruh okruhu** R, jestliže

- $0, 1 \in H$,
- pro každé $a \in H$ platí $-a \in H$,
- pro každé $a, b \in H$ platí $a + b$, $a \cdot b \in H$.

Poznámka. Největším podokruhem okruhu R (vzhledem k $\subseteq$) je celý okruh R, nejmenším podokruhem je $\{n1;\ n \in \mathbb{Z}\}$.

Věta. *Nechť H je podokruh okruhu $(R, +, \cdot)$. Pak $+$ a $\cdot$ určují operace na množině H, přičemž H je okruh vzhledem k těmto operacem. Je-li okruh R komutativní, pak je i okruh H komutativní. Je-li R obor integrity, pak je i H obor integrity.* [Věta 3.2, str. 66]

Důsledek. *Každý podokruh tělesa je oborem integrity.*

Příklad. Podokruh tělesa nemusí být těleso: vždyť $\mathbb{Z}$ je podokruhem $\mathbb{Q}$.

Věta. *Jestliže H je podokruh okruhu R a K je podokruh okruhu H, pak je K také podokruh okruhu R.* [Zřejmé, vždyť operace $+$ a $\cdot$ se v okruhu H počítají jako v R.]

Podokruh okruhu generovaný podmnožinou okruhu

Věta. *Nechť R je okruh, I neprázdná množina taková, že pro každé $i \in I$ je dán podokruh H_i okruhu R. Pak průnik $\bigcap_{i \in I} H_i$ všech těchto podokruhů je opět podokruhem okruhu R.*

Definice. Nechť M je podmnožina okruhu R. Symbolem $\langle M \rangle$ označíme průnik všech podokruhů okruhu R, jejichž podmnožinou je množina M. Podle předchozí věty je $\langle M \rangle$ podokruhem okruhu R obsahující množinu M; evidentně je nejmenší s touto vlastností. Podokruh $\langle M \rangle$ nazýváme **podokruh generovaný množinou** M, množinu M nazýváme **množina generátorů podokruhu** $\langle M \rangle$.

Poznámka. Zřejmě $\langle R \rangle = R$, $\langle \emptyset \rangle = \{n1;\ n \in \mathbb{Z}\}$.

Označení. Je-li $M = H \cup \{a\}$, kde H je podokruh okruhu R a $a \in R$, píšeme též $H[a]$ místo $\langle M \rangle$.

Věta. *Nechť H je podokruh komutativního okruhu R a $a \in R$. Pak* $H[a] = \{h_0 + h_1 a + h_2 a^2 + \cdots + h_n a^n;\ n \in \mathbb{N},\ h_0, h_1, \ldots, h_n \in H\}$.

[Věta 3.12, str. 71]

Součin okruhů

Věta. *Nechť $(R, +, \cdot)$ a $(S, +, \cdot)$ jsou okruhy. Definujme na kartézském součinu $R \times S$ nové operace $+$ a $\cdot$ po složkách, tj.*

$$(r_1, s_1) + (r_2, s_2) = (r_1 + r_2, s_1 + s_2),$$
$$(r_1, s_1) \cdot (r_2, s_2) = (r_1 \cdot r_2, s_1 \cdot s_2)$$

pro libovolné $r_1, r_2 \in R$ a $s_1, s_2 \in S$. Pak $(R \times S, +, \cdot)$ je okruh s nulou $(0, 0)$ a jedničkou $(1, 1)$. Navíc platí $(R \times S)^\times = R^\times \times S^\times$.

[Ověření je zdlouhavé, ale snadné: všechny axiomy okruhu jsou v $R \times S$ splněny, protože se operace počítají po složkách a v obou složkách tyto axiomy platí, protože jsou R a S okruhy.]

Definice. Výše popsaný okruh $(R \times S, +, \cdot)$ se nazývá **součin okruhů** $(R, +, \cdot)$ a $(S, +, \cdot)$. Zobrazení $p_1 : R \times S \to R$ a $p_2 : R \times S \to S$ určená předpisy $p_1((r, s)) = r$, $p_2((r, s)) = s$ pro libovolné $(r, s) \in R \times S$ se nazývají **projekce** (ze součinu).

Věta. *Nechť $(R \times S, +, \cdot)$ je součin okruhů $(R, +, \cdot)$ a $(S, +, \cdot)$. Pak obě projekce p_1 a p_2 jsou surjektivní homomorfismy okruhů.*

[Zřejmé, protože se operace počítají po složkách.]

Čínská zbytková věta

Věta (Čínská zbytková). *Nechť $m, n \in \mathbb{N}$ a zobrazení $f : \mathbb{Z}_{mn} \to \mathbb{Z}_m \times \mathbb{Z}_n$ je určeno předpisem $f([a]_{mn}) = ([a]_m, [a]_n)$ pro libovolné $a \in \mathbb{Z}$. Pak f je homomorfismus okruhů. Je-li navíc $(m, n) = 1$, je f izomorfismus, a tedy $\mathbb{Z}_{mn} \cong \mathbb{Z}_m \times \mathbb{Z}_n$.*

Důkaz. Protože $m \mid mn$ a $n \mid mn$, je f definováno korektně. Zřejmě zachovává operace $+$, $\cdot$ i 1. Je-li $(m, n) = 1$, pak je $\ker f = \{[a]_{mn};\ a \in \mathbb{Z},\ m \mid a,\ n \mid a\} = \{[0]_{mn}\}$, a tedy f je injekce. Protože obě množiny mají mn prvků, je f i surjekce.

Důsledek. *Je-li $(m, n) = 1$, pak $\mathbb{Z}_{mn}^\times \cong \mathbb{Z}_m^\times \times \mathbb{Z}_n^\times$, a tedy $\varphi(m \cdot n) = \varphi(m) \cdot \varphi(n)$.*

Důsledek. *Je-li $(m, n) = 1$, pak pro každé $a, b \in \mathbb{Z}$ existuje $c \in \mathbb{Z}$ tak, že*

$$c \equiv a \pmod{n},$$
$$c \equiv b \pmod{m}.$$

Konstrukce podílového tělesa $Q(R)$ oboru integrity R

Motivace. Víme, že každý podokruh tělesa je oborem integrity. Ukažme, že i naopak každý obor integrity je podokruhem vhodného tělesa. Nechť dále R je libovolný, ale pevně zvolený obor integrity.

Věta. Na množině $R \times R^*$ definujeme relaci $\equiv$ předpisem

$$(a, b) \equiv (c, d) \quad \Leftrightarrow \quad a \cdot d = b \cdot c$$

pro libovolné $a, c \in R,\ b, d \in R^*$. Pak $\equiv$ je relace ekvivalence.
[Lemma 4.13, str. 75]

Označení. Označme $Q(R)$ rozklad příslušný ekvivalenci $\equiv$, tedy $Q(R) = (R \times R^*)/\equiv$. Pro libovolné $(a, b) \in R \times R^*$ označme $\frac{a}{b} \in Q(R)$ třídu obsahující (a, b), pro každé $a, c \in R,\ b, d \in R^*$ tedy platí

$$\frac{a}{b} = \frac{c}{d} \quad \Leftrightarrow \quad a \cdot d = b \cdot c.$$

Věta. Na $Q(R)$ lze definovat operace $+$ a $\cdot$ takto: pro každé $a, c \in R,\ b, d \in R^*$ definujeme

$$\frac{a}{b} + \frac{c}{d} = \frac{a \cdot d + c \cdot b}{b \cdot d}, \qquad \frac{a}{b} \cdot \frac{c}{d} = \frac{a \cdot c}{b \cdot d}.$$

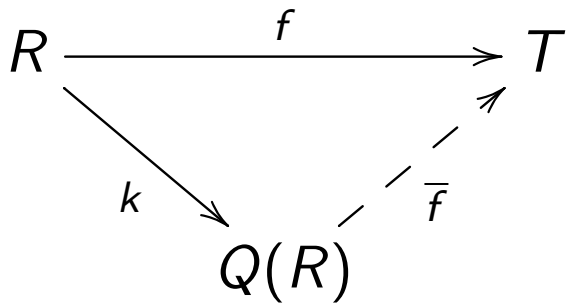
Pak $(Q(R), +, \cdot)$ je těleso a zobrazení $k : R \to Q(R)$, určené předpisem $k(a) = \frac{a}{1}$, je vnoření (tj. injektivní homomorfismus okruhů).
[Věta 4.15, str. 75], [Věta 4.17, str. 76]

Konstrukce podílového tělesa $Q(R)$ oboru integrity R

Máme vnoření $k : R \to Q(R)$, $k(a) = \frac{a}{1}$ pro každé $a \in R$.

Příklad. $Q(\mathbb{Z}) = \mathbb{Q}$.

Věta. *Nechť $f : R \to T$ je vnoření oboru integrity R do tělesa T. Pak předpis $\overline{f}(\frac{a}{b}) = f(a) \cdot f(b)^{-1}$ pro libovolné $a, b \in R$, $b \neq 0$ dává homomorfismus $\overline{f} : Q(R) \to T$ takový, že $\overline{f} \circ k = f$.*



[Věta 4.19, str. 77]

Navíc platí, že $\overline{f}$ je jediný takový homomorfismus a že $\overline{f}$ je také vnoření, a tedy $Q(R)$ je izomorfní se svým obrazem v homomorfismu $\overline{f}$, tj. $Q(R) \cong \{f(a) \cdot f(b)^{-1}; a, b \in R,\ b \neq 0\}$.

Příklad. $\mathbb{Z}[i] = \{x + i \cdot y; x, y \in \mathbb{Z}\}$ je obor integrity, inkluze dává jeho vnoření do $\mathbb{C}$, tj. máme injektivní homomorfismus $f : \mathbb{Z}[i] \to \mathbb{C}$, kde $f(\alpha) = \alpha$ pro $\alpha \in \mathbb{Z}[i]$. Proto $Q(\mathbb{Z}[i]) \cong \{\alpha \cdot \beta^{-1}; \alpha, \beta \in \mathbb{Z}[i],\ \beta \neq 0\} = \{x + i \cdot y; x, y \in \mathbb{Q}\} = \mathbb{Q}[i]$.

Příklad. Podobně $Q(\mathbb{Z}[\sqrt{p}]) \cong \mathbb{Q}[\sqrt{p}]$ pro libovolné prvočíslo p.

Dělitelnost v komutativních okruzích

Definice. Nechť R je komutativní okruh, $a, b \in R$. Řekneme, že prvek b **dělí** prvek a, neboli že prvek a **je dělitelný** prvkem b, píšeme $b \mid a$, jestliže existuje prvek $q \in R$ takový, že $a = q \cdot b$. V opačném případě říkáme, že prvek b **nedělí** prvek a, neboli že prvek a **není dělitelný** prvkem b, píšeme $b \nmid a$.

Věta. Nechť R je komutativní okruh, pak platí

- $\forall a \in R : \ 1 \mid a, \ a \mid a;$
- $\forall a, b, c \in R : \ a \mid b, \ b \mid c \ \Rightarrow \ a \mid c;$
- $\forall a, b, c \in R : \ a \mid b, \ a \mid c \ \Rightarrow \ a \mid b + c;$
- $\forall a \in R : \ a \in R^\times \ \Leftrightarrow \ a \mid 1;$
- $\forall a, b \in R : \ a \in R^\times, \ b \mid a \ \Rightarrow \ b \in R^\times;$
- $\forall a, b \in R : \ a \in R^\times \ \Rightarrow \ a \mid b.$

[Věta 2.11, str. 63]

Důsledek. Nechť R je komutativní okruh, $a_1, \ldots, a_n, b \in R$, $u_1, \ldots, u_n \in R$ libovolné. Jestliže $b \mid a_i$ pro každé $i = 1, \ldots, n$, pak $b \mid \sum_{i=1}^{n} u_i \cdot a_i$.

Dělitelnost v komutativních okruzích

Definice. Nechť R je komutativní okruh, $a, b \in R$. Řekneme, že prvky a, b jsou **asociované**, píšeme $a \sim b$, jestliže $a \mid b$ a současně $b \mid a$.

Věta. *Nechť R je komutativní okruh. Relace asociovanosti $\sim$ je relací ekvivalence na množině R.* [Věta 2.13, str. 63]

Věta. *Nechť R je obor integrity, $a, b \in R$. Pak platí $a \sim b$, právě když existuje jednotka $c \in R^\times$ tak, že $a = c \cdot b$.* [Věta 2.15, str. 64]

Definice. Nechť R je komutativní okruh, $a, b \in R$. Libovolný prvek $c \in R$ splňující $c \mid a$, $c \mid b$, se nazývá **společný dělitel** prvků a, b. Libovolný prvek $d \in R$ se nazývá **největší společný dělitel** prvků a, b, jestliže

- $d \mid a$, $d \mid b$,
- $\forall c \in R: \ c \mid a, c \mid b \ \Rightarrow \ c \mid d$.

Tedy největší společný dělitel prvků a, b je takový jejich společný dělitel, který je dělitelný každým jejich společným dělitelem.

Dělitelnost v komutativních okruzích

Definice. Nechť R je komutativní okruh, $a, b \in R$. Libovolný prvek $c \in R$ splňující $a \mid c$, $b \mid c$, se nazývá **společný násobek** prvků a, b. Libovolný prvek $d \in R$ se nazývá **nejmenší společný násobek** prvků a, b, jestliže

- $a \mid d$, $b \mid d$,
- $\forall c \in R: \ a \mid c, b \mid c \ \Rightarrow \ d \mid c$.

Tedy nejmenší společný násobek prvků a, b je takový jejich společný násobek, který dělí každý jejich společný násobek.

Poznámka. Předchozí definice mírně pozměňují dříve definované pojmy „největší společný dělitel“ a „nejmenší společný násobek“ v $\mathbb{Z}$. Definovali jsme je totiž pomocí uspořádání podle velikosti, které v obecném okruhu nemáme k dispozici. Dále budeme tyto pojmy používat podle nové definice, avšak zavedené označení (m, n) a $[m, n]$ ponecháme. Tedy (m, n) značí *nezáporný* největší společný dělitel čísel $m, n \in \mathbb{Z}$. Podobně $[m, n]$ značí jejich *nezáporný* nejmenší společný násobek.

Dělitelnost v komutativních okruzích

Věta. *Nechť R je komutativní okruh, $a, b \in R$. Největší společný dělitel prvků a, b, pokud existuje, je určen jednoznačně až na asociovanost. Také nejmenší společný násobek prvků a, b, pokud existuje, je určen jednoznačně až na asociovanost.* [Věta 2.17, str. 64]

Definice. Nechť R je obor integrity, $a \in R$. Řekneme, že a je **ireducibilní** prvek okruhu R, jestliže $a \neq 0$, $a \notin R^\times$ a pro každé $b, c \in R$ takové, že $a = b \cdot c$, platí $b \in R^\times$ a $c \sim a$ anebo $c \in R^\times$ a $b \sim a$.

Příklad. Ireducibilními prvky okruhu $\mathbb{Z}$ jsou právě prvočísla a čísla k nim opačná.

Příklad. Je-li T těleso, pak v T neexistují žádné ireducibilní prvky.

Věta. *Nechť R je obor integrity, $a, b \in R$. Je-li a ireducibilní prvek okruhu R a $b \sim a$, pak je také b ireducibilní.*

Důkaz. Víme, že existuje jednotka $e \in R^\times$, že $a = e \cdot b$. Zřejmě $b \neq 0$, $b \notin R^\times$. Pro každé $x, y \in R$, $b = x \cdot y$, je $a = (e \cdot x) \cdot y$.

Okruhy s jednoznačným rozkladem

Definice. Řekneme, že R je **okruh s jednoznačným rozkladem**, jestliže

- R je obor integrity,
- každé $a \in R$, $a \neq 0$, $a \notin R^\times$, lze rozložit na součin několika ireducibilních prvků, přičemž tento součin je jednoznačný až na pořadí a asociovanost.

Příklad. Víme, že $\mathbb{Z}$ je okruh s jednoznačným rozkladem (například rozklady $6 = 2 \cdot 3 = 3 \cdot 2 = (-2) \cdot (-3) = (-3) \cdot (-2)$ se liší jen pořadím a asociovaností).

Příklad. Každé těleso je okruh s jednoznačným rozkladem, neboť neobsahuje žádný prvek, který by byl nenulový a nebyl jednotka.

Příklad. V okruhu $\mathbb{Z}[i]$ je možné dokázat větu o dělení se zbytkem (aby se dalo říct, že zbytek je „menší“ než číslo, kterým se dělilo, je třeba nějak měřit velikost zbytku; v tomto případě to lze udělat pomocí absolutní hodnoty). [Věta 3.4, str. 67] Stejnou úvahou jako v $\mathbb{Z}$, tedy pomocí Euklidova algoritmu a Bezoutovy rovnosti lze pak ukázat, že $\mathbb{Z}[i]$ je okruh s jednoznačným rozkladem.

Příklad

Nechť $R = \mathbb{Z}[i\sqrt{5}] = \{a + bi\sqrt{5};\ a, b \in \mathbb{Z}\}$. Pak R je obor integrity, protože je podokruhem $\mathbb{C}$. Definujme zobrazení $N : R \to \mathbb{Z}$ takto: pro libovolné $\alpha = a + bi\sqrt{5}$ klademe $N(\alpha) = |\alpha|^2 = a^2 + 5b^2$.

Jestliže $\beta \mid \alpha$ v R, existuje $\gamma \in R$ tak, že $\alpha = \beta \cdot \gamma$, a tedy $N(\alpha) = |\beta \cdot \gamma|^2 = |\beta|^2 \cdot |\gamma|^2 = N(\beta) \cdot N(\gamma)$, tudíž $N(\beta) \mid N(\alpha)$ v $\mathbb{Z}$.

Je-li $\alpha = a + bi\sqrt{5} \in R^\times$, pak $\alpha \mid 1$ v R, a proto $N(\alpha) \mid N(1) = 1$. Odtud $a^2 + 5b^2 = 1$, proto $b = 0$, $a = \pm 1$. Je tedy $R^\times = \{1, -1\}$.

Platí $6 = 2 \cdot 3 = (1 + i\sqrt{5})(1 - i\sqrt{5})$, přitom tito všichni čtyři činitelé jsou ireducibilními prvky okruhu R. Je totiž $N(2) = 4$, $N(3) = 9$, $N(1 + i\sqrt{5}) = N(1 - i\sqrt{5}) = 6$. Kdyby například $1 + i\sqrt{5} = \gamma \cdot \delta$ pro nějaké $\gamma, \delta \in R - R^\times$, platilo by $N(\gamma) > 1$, $N(\delta) > 1$, $N(\gamma) \cdot N(\delta) = 6$. Proto $N(\gamma) \in \{2, 3\}$, což je spor, protože rovnice $x^2 + 5y^2 = 2$ a $x^2 + 5y^2 = 3$ nemají řešení v $\mathbb{Z}$.

Jsou tedy $2 \cdot 3 = (1 + i\sqrt{5})(1 - i\sqrt{5})$ součiny ireducibilních prvků lišící se více než pořadím a asociovaností, proto R **není okruh s jednoznačným rozkladem.**

Pokračování příkladu

Označme $\alpha = (1 + i\sqrt{5})^2 = 2(-2 + i\sqrt{5})$, $\beta = 2(1 + i\sqrt{5})$ a ukažme sporem, že α, β **nemají největší společný dělitel v** R.

Předpokládejme tedy, že $\gamma = x + yi\sqrt{5}$ je největší společný dělitel čísel α, β. Pak platí $\gamma \mid \alpha$, $\gamma \mid \beta$ v R, a tedy $N(\gamma) \mid N(\alpha) = 36$, $N(\gamma) \mid N(\beta) = 24$ v $\mathbb{Z}$, tedy $N(\gamma) \mid 12$.

Na druhou stranu 2 a $1 + i\sqrt{5}$ jsou společní dělitelé čísel α, β, a tedy $2 \mid \gamma$ a $1 + i\sqrt{5} \mid \gamma$ v R, a tedy $4 = N(2) \mid N(\gamma)$ a $6 = N(1 + i\sqrt{5}) \mid N(\gamma)$ v $\mathbb{Z}$, tedy $12 \mid N(\gamma)$.

Dohromady $12 = N(\gamma) = x^2 + 5y^2$. Taková $x, y \in \mathbb{Z}$ však neexistují. Proto α, β nemají největší společný dělitel v R.

Polynomy nad libovolným okruhem R

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

Definice. Nechť R je okruh. **Polynomem** nad okruhem R rozumíme nekonečnou posloupnost $f = (f_0, f_1, f_2, \dots)$, kde $f_i \in R$ pro každé $i = 0, 1, 2, \dots$ a platí, 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. Množinu všech polynomů nad okruhem R označujeme symbolem $R[x]$.

Dohoda. 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*

$$(f + g)_i = f_i + g_i, \qquad (f \cdot g)_i = \sum_{k=0}^{i} f_k g_{i-k}$$

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]

Polynomy nad libovolným 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 vnoření. [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, vždyť 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.

Polynomy nad libovolným okruhem R

Definice. Polynomy stupně 1 se nazývají **lineární**, polynomy stupně 2 **kvadratické**, polynomy stupně 3 **kubické**. Lineární polynom $(0, 1, 0, 0, \dots)$ budeme označovat symbolem x.

Příklad. Zřejmě $x^2 = (0, 0, 1, 0, 0, \dots)$, $x^3 = (0, 0, 0, 1, 0, \dots)$ atd.

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

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

Polynomy nad libovolným okruhem R

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 $R[x]$ 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 $f = g \cdot q + r$.*

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

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 $q, r, \bar{q}, \bar{r} \in R[x]$, 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 $g \cdot (\bar{q} - q) = r - \bar{r}$. Vedoucí koeficient polynomu g není dělitel nuly, tedy $\mathrm{st}(g) + \mathrm{st}(\bar{q} - q) = \mathrm{st}(g \cdot (\bar{q} - q)) = \mathrm{st}(r - \bar{r}) < \mathrm{st}(g)$. Pak tedy $\mathrm{st}(\bar{q} - q) < 0$, tj. $\bar{q} = q$, odkud $\bar{r} = r$.

Euklidův algoritmus v okruhu polynomů nad tělesem

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

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

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 $d = a \cdot f + b \cdot g$.*

[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 $R[x]$.* [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 existuje $k \in \mathbb{Z}$, $k \geq 0$, $a \in R^*$ a normované ireducibilní polynomy $p_1, \ldots, p_k \in R[x]$ 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.*

Kořen polynomu

Definice. Nechť R je okruh, $f = a_n x^n + \cdots + a_1 x + a_0 \in R[x]$, $c \in R$. 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 $(f \cdot g)(c) = (x \cdot a)(c) = (ax)(c) = a \cdot c \neq c \cdot a = f(c) \cdot g(c)$.

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 $R[x]$.*

[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 1 se nazývají **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.

Příklad. Kvadratický polynom $x^2 - [1]_8 \in \mathbb{Z}_8[x]$ má čtyři jednoduché kořeny $[1]_8$, $[-1]_8$, $[3]_8$, $[-3]_8$.

Počet kořenů polynomu nad oborem integrity

Věta. *Nechť R je obor integrity, $f \in R[x]$, $f \neq 0$. 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 $R[x]$. Označme K podílové těleso oboru integrity R, tedy R je podokruhem tělesa K. Pak $(x - c_i)^{k_i} \mid f$ v $K[x]$. Přitom $x - c_1, \ldots, x - c_s$ jsou různé normované ireducibilní polynomy v $K[x]$. Rozložíme-li f na součin vedoucího koeficientu f a normovaných ireducibilních polynomů v $K[x]$, z jednoznačnosti rozkladu plyne, že se mezi nimi polynom $x - c_i$ objeví alespoň k_i-krát pro každé $i = 1, \ldots, s$. Proto $\prod_{i=1}^{s} (x - c_i)^{k_i} \mid f$. Protože K je těleso, platí $\sum_{i=1}^{s} k_i \leq \mathrm{st}(f)$.

Konečná podgrupa multiplikativní grupy tělesa

Známe následující pojem a větu z teorie grup:

Definice. Nechť G je konečná grupa. Nejmenší $e \in \mathbb{N}$ takové, že pro každé $a \in G$ platí $a^e = 1$, 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 K je těleso, G je konečná podgrupa multiplikativní grupy $(K^*, \cdot)$. 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.
Pak z Lagrangeovy věty $e \mid n$. Každý prvek grupy G je kořenem polynomu $x^e - 1$, a tedy $n \leq \mathrm{st}(x^e - 1) = e$, 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 $(R^*, \cdot)$ cyklická.

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

Derivace polynomu

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

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

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 $n a_n$ znamená n-násobek prvku a_n (tedy součet n kopií prvku a_n v grupě $(R, +)$).

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 k-násobným kořenem polynomu f, pak je c kořenem polynomů f', f'', $\ldots$, $f^{(k-1)}$.* [Věta 6.16, str. 90]

Poznámka. Předchozí věta se používá při hledání vícenásobných kořenů daného polynomu $f \in R[x]$, kde R je těleso. Takový kořen je také kořenem derivace f', a tedy i 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 $f^{(k)}$.* [Věta 6.17, str. 90]

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 $f^{(p)} = 0$.

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* $f = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{C}[x]$ *je normovaný polynom,* $n \geq 1$, $c_1, \ldots, c_n \in \mathbb{C}$ *jeho kořeny (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. *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, $r \in \mathbb{Z}$, $s \in \mathbb{N}$, $(r,s) = 1$, *taková, že* $\frac{r}{s}$ *je kořen polynomu. 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. 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 $\mathbb{Z}$

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 $\mathbb{Q}$.*

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 nekonstantníchch 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. *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 $\mathbb{Z}$. 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.