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]

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.

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]

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 $\sum_{i=1}^{s} k_i \leq \mathrm{st}(f)$.

Podtělesa

Definice. Nechť T je těleso. Libovolný podokruh R tělesa T takový, že pro každé $a \in R$, $a \neq 0$ platí $a^{-1} \in R$, nazýváme podtělesem tělesa T. Říkáme též, že T je rozšířením tělesa R. Anebo také, že $R \subseteq T$ je rozšířením těles (v literatuře se hojně používá zápis: T/R je rozšířením těles).

Jinými slovy: podokruh R tělesa T je podtělesem, jestliže R je těleso.

Příklad. Každé těleso charakteristiky $p \neq 0$ obsahuje podtěleso izomorfní s $\mathbb{Z}_p$.

Věta. Nechť R je těleso a T netriviální okruh. Pak každý homomorfismus okruhů $\varphi : R \to T$ je injektivní.

Důkaz. Nechť $\varphi : R \to T$ je homomorfismus okruhů, stačí ukázat, že $\ker \varphi = \{0\}$. Kdyby nějaké $\alpha \in \ker \varphi$ bylo nenulové, existoval by v R inverzní prvek α^{-1}. Pak by $1 = \varphi(1) = \varphi(\alpha \cdot \alpha^{-1}) =$
$= \varphi(\alpha) \cdot \varphi(\alpha^{-1}) = 0$, a tedy by T byl triviální okruh, spor.

Podtěleso generované množinou

Věta. *Nechť $I \neq \emptyset$ je libovolná množina taková, že pro každé $i \in I$ je dáno podtěleso R_i tělesa T. Pak $\bigcap_{i \in I} R_i$ je podtěleso tělesa T.*

Definice. Nechť T je těleso. Předchozí věta nám umožňuje definovat podtěleso tělesa T generované množinou $M \subseteq T$ jako průnik všech podtěles tuto množinu obsahujících. Je to tedy nejmenší podtěleso tělesa T obsahující M.
Je-li $M = R \cup \{c_1, \ldots, c_n\}$, kde R je podtěleso tělesa T a $c_1, \ldots, c_n \in T$, pak podtěleso generované množinou $R \cup \{c_1, \ldots, c_n\}$ značíme $R(c_1, \ldots, c_n)$.

Poznámka. Připomeňme, že je-li T okruh, R jeho podokruh a $c_1, \ldots, c_n \in T$, pak podokruh generovaný množinou $R \cup \{c_1, \ldots, c_n\}$ značíme $R[c_1, \ldots, c_n]$. V situaci z definice mají tedy smysl oba zápisy, zřejmě platí $R[c_1, \ldots, c_n] \subseteq R(c_1, \ldots, c_n)$.

Vektorový prostor nad tělesem R

Definice. Nechť R je těleso, $(V, +)$ komutativní grupa. Nechť pro každé $r \in R$ a každé $v \in V$ je definován prvek $r \cdot v \in V$ tak, že pro každé $r_1, r_2 \in R$ a každé $v_1, v_2 \in V$ platí

- $(r_1 + r_2) \cdot v_1 = r_1 \cdot v_1 + r_2 \cdot v_1$,
- $r_1 \cdot (v_1 + v_2) = r_1 \cdot v_1 + r_1 \cdot v_2$,
- $r_1 \cdot (r_2 \cdot v_1) = (r_1 \cdot r_2) \cdot v_1$,
- $1 \cdot v_1 = v_1$,

pak říkáme, že V je **vektorový prostor nad** R, prvky tělesa R v této souvislosti nazýváme **skaláry**, prvky grupy V nazýváme **vektory**. Neutrální prvek grupy V se nazývá nulový vektor, inverzní prvek k libovolnému vektoru u v grupě V nazýváme opačný vektor k u a značíme $-u$.

Poznámka. Přiřazení $(r, v) \mapsto r \cdot v$ z definice vektorového prostoru je zobrazením $R \times V \to V$, nejde tedy o operaci na množině, protože R a V jsou obecně různé množiny. Přesto $r \cdot v$ nazýváme součin skaláru r a vektoru v.

Podprostor vektorového prostoru

Definice. Nechť V je vektorový prostor nad tělesem R a W je podmnožinou V. Řekneme, že W je **podprostor** vektorového prostoru V, jestliže platí

- $W \neq \emptyset$,
- pro každé $u, v \in W$ je $u + v \in W$,
- pro každé $r \in R$ a každé $u \in W$ je $r \cdot u \in W$.

Věta. *Nechť V je vektorový prostor nad tělesem R, I neprázdná množina taková, že pro každé $i \in I$ je dán podprostor W_i vektorového prostoru V. Pak průnik $\bigcap_{i \in I} W_i$ všech těchto podoprostorů je opět podprostorem vektorového prostoru V.*

Definice. Nechť M je podmnožina vektorového prostoru V nad tělesem R. Pak průnik všech podprostorů vektorového prostoru V, jejichž podmnožinou je množina M, je podle předchozí věty podprostorem vektorového prostoru V obsahujícím množinu M; evidentně je nejmenší s touto vlastností. Tento podprostor nazýváme **podprostor generovaný množinou** M, množinu M nazýváme **množina generátorů podokruhu** $\langle M \rangle$.

Lineární kombinace

Definice. Nechť V je vektorový prostor nad tělesem R a jsou dány $u_1, \ldots, u_k \in V$. Řekneme, že vektor $v \in V$ je **lineární kombinace** vektorů $u_1, \ldots, u_k$, jestliže existují skaláry $r_1, \ldots, r_k \in R$ tak, že

$$v = r_1 \cdot u_1 + \cdots + r_k \cdot u_k.$$

Množinu všech lineárních kombinací vektorů $u_1, \ldots, u_k$ budeme značit $L(u_1, \ldots, u_k)$.

Věta. Nechť V je vektorový prostor nad tělesem R a jsou dány $u_1, \ldots, u_k \in V$. Pak $L(u_1, \ldots, u_k)$ je podprostor vektorového prostoru V generovaný množinou $\{u_1, \ldots, u_k\}$.

Věta. Nechť V je vektorový prostor nad tělesem R a jsou dány $u_1, \ldots, u_k, v_1, \ldots, v_t \in V$ tak, že $v_1, \ldots, v_t \in L(u_1, \ldots, u_k)$. Pak $L(v_1, \ldots, v_t) \subseteq L(u_1, \ldots, u_k)$.

Lineární závislost a nezávislost vektorů

Definice. Nechť V je vektorový prostor nad tělesem R a jsou dány $u_1, \ldots, u_k \in V$. Řekneme, že vektory $u_1, \ldots, u_k$ jsou **lineárně závislé** nad tělesem R, jestliže existují skaláry $r_1, \ldots, r_k \in R$ tak, že

$$r_1 \cdot u_1 + \cdots + r_k \cdot u_k = 0$$

a současně je alespoň jeden ze skalárů $r_1, \ldots, r_k$ nenulový.
V opačném případě řekneme, že vektory $u_1, \ldots, u_k$ jsou **lineárně nezávislé** nad tělesem R.

Poznámka. Vektory $u_1, \ldots, u_k$ jsou tedy lineárně nezávislé nad tělesem R, právě když pro každé skaláry $r_1, \ldots, r_k \in R$ platí

$$r_1 \cdot u_1 + \cdots + r_k \cdot u_k = 0 \qquad \Longleftrightarrow \qquad r_1 = \cdots = r_k = 0.$$

Poznámka. Přesnější než o vektorech $u_1, \ldots, u_k$ by bylo hovořit o posloupnosti těchto vektorů - některý vektor se totiž může mezi těmito vektory zopakovat. V takovém případě jde vždy o lineárně závislé vektory. Stejně tak i v situaci, kdy je některý z vektorů nulový.

Věty o lineární závislosti a nezávislosti vektorů

Věta. Nechť V je vektorový prostor nad tělesem R a jsou dány $u_1, \ldots, u_k \in V$.

- Je-li $k = 1$, pak vektor u_1 je lineárně závislý, právě když $u_1 = 0$.
- Je-li $k \geq 2$, pak vektory $u_1, \ldots, u_k$ jsou lineárně závislé, právě když existuje $i \in \{1, \ldots, k\}$ tak, že u_i je lineární kombinací ostatních vektorů (tj. vektorů $u_1, \ldots, u_{i-1}, u_{i+1}, \ldots, u_k$).

Věta (Steinitz). Nechť V je vektorový prostor nad tělesem R a jsou dány $u_1, \ldots, u_k, v_1, \ldots, v_t \in V$, přičemž vektory $v_1, \ldots, v_t$ jsou lineárně nezávislé a splňují $v_1, \ldots, v_t \in L(u_1, \ldots, u_k)$. Pak platí

- $t \leq k$.
- Při vhodném přečíslování vektorů $u_1, \ldots, u_k$ je $L(u_1, \ldots, u_k) = L(v_1, \ldots, v_t, u_{t+1}, \ldots, u_k)$.

Báze a dimenze vektorového prostoru

Definice. Konečná posloupnost $u_1, \ldots, u_k$ vektorů vektorového prostoru V nad tělesem R se nazývá bází prostoru V, jestliže

- $u_1, \ldots, u_k$ jsou lineárně nezávislé,
- $V = L(u_1, \ldots, u_k)$, tj. množina $\{u_1, \ldots, u_k\}$ generuje vektorový prostor V.

Poznámka. Ze Steinitzovy věty plyne, že jsou-li $u_1, \ldots, u_k$ a $v_1, \ldots, v_t$ dvě báze téhož prostoru V, pak $k = t$.

Definice. Nechť V je vektorový prostor nad tělesem R.

- Je-li $V = \{0\}$, pak říkáme, že vektorový prostor V má dimenzi nula.
- Jestliže existuje báze $u_1, \ldots, u_k$ prostoru V, řekneme, že vektorový prostor V má dimenzi k.
- Jestliže $V \neq \{0\}$ a současně neexistuje žádná báze prostoru V, řekneme, že vektorový prostor V má dimenzi ∞.

Stupeň rozšíření těles

Je-li R podtělesem tělesa T, pak můžeme aditivní grupu $(T, +)$ chápat jako vektorový prostor nad tělesem R: skalárním násobkem vektoru $t \in T$ skalárem $r \in R$ je součin $r \cdot t$ počítaný v tělese T. Axiomy vektorového prostoru jsou splněny:
pro každé skaláry $r_1, r_2 \in R$ a každé vektory $t_1, t_2 \in T$ platí

- $(r_1 + r_2) \cdot t_1 = r_1 \cdot t_1 + r_2 \cdot t_1$,
- $r_1 \cdot (t_1 + t_2) = r_1 \cdot t_1 + r_1 \cdot t_2$,
- $r_1 \cdot (r_2 \cdot t_1) = (r_1 \cdot r_2) \cdot t_1$,
- $1 \cdot t_1 = t_1$,

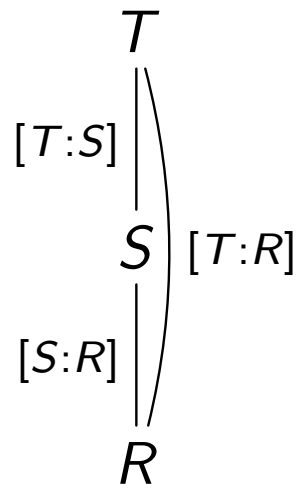
(v T platí distributivní zákony, násobení je asociativní a 1 je jednička). Máme tedy definovánu dimenzi $\dim_R T \in \mathbb{N} \cup \{\infty\}$, zřejmě tato dimenze nemůže být nula.

Definice. Nechť $R \subseteq T$ je rozšířením těles. Jeho stupněm $[T : R]$ rozumíme dimenzi vektorového prostoru T nad tělesem R, tj. $[T : R] = \dim_R T$.

Multiplikativnost stupně rozšíření

Věta. *Nechť $R \subseteq S$, $S \subseteq T$ jsou rozšíření těles. Pak platí*

$$[T : R] = [T : S] \cdot [S : R],$$



kde užíváme konvence $n \cdot \infty = \infty \cdot n = \infty$ pro každé $n \in \mathbb{N} \cup \{\infty\}$.

Důkaz. Je-li $[S : R] = \infty$, pro každé $n \in \mathbb{N}$ v S existuje n lineárně nezávislých prvků nad R, protože $S \subseteq T$, jsou tyto prvky v T a platí $[T : R] = \infty$.

Je-li $[T : S] = \infty$, pro každé $n \in \mathbb{N}$ v T existuje n lineárně nezávislých prvků nad S. Ty jsou lineárně nezávislé i nad R, a proto $[T : R] = \infty$.

Nechť $n = [T : S] \in \mathbb{N}$, $m = [S : R] \in \mathbb{N}$. Nechť $\alpha_1, \ldots, \alpha_n$ je báze T nad S, $\beta_1, \ldots, \beta_m$ báze S nad R. Ukážeme, že $\alpha_i\beta_j$ $(1 \leq i \leq n, 1 \leq j \leq m)$ je bází T nad R. Nechť $\gamma \in T$ je libovolný. Pak existují $\delta_1, \ldots, \delta_n \in S$, že $\gamma = \sum_{i=1}^{n} \delta_i\alpha_i$. Existují tedy $\varepsilon_{ij} \in R$, že $\delta_i = \sum_{j=1}^{m} \varepsilon_{ij}\beta_j$ pro každé i. Dosazením

$$\gamma = \sum_{i=1}^{n} \left(\sum_{j=1}^{m} \varepsilon_{ij}\beta_j \right) \alpha_i = \sum_{i=1}^{n} \sum_{j=1}^{m} \varepsilon_{ij}(\alpha_i\beta_j).$$

Tedy $\alpha_i\beta_j$ $(1 \leq i \leq n, 1 \leq j \leq m)$ je množina generátorů T nad R.

Je-li $\sum_{i=1}^{n} \sum_{j=1}^{m} \varepsilon_{ij}(\alpha_i\beta_j)$ pro nějaké $\varepsilon_{ij} \in R$ nulový vektor, pak z lineární nezávislosti $\alpha_1, \ldots, \alpha_n$ nad S dostaneme, že $\sum_{j=1}^{m} \varepsilon_{ij}\beta_j = 0$ pro každé $i = 1, \ldots, n$ a z lineární nezávislosti $\beta_1, \ldots, \beta_m$ nad R dostaneme, že $\varepsilon_{ij} = 0$ pro každé i, j.

Tedy $\alpha_i\beta_j$ $(1 \leq i \leq n, 1 \leq j \leq m)$ je báze T nad R.

Algebraické a transcendentní prvky

Mějme rozšíření těles $R \subseteq T$ a polynom

$$f = a_n x^n + \cdots + a_1 x + a_0 \in R[x].$$

Pak je také $f \in T[x]$, a proto pro každé $c \in T$ můžeme uvažovat hodnotu $f(c) = a_n \cdot c^n + \cdots + a_1 \cdot c + a_0 \in T$. Připomeňme, že c se nazývá kořenem polynomu f, je-li $f(c) = 0$.

Definice. Nechť $R \subseteq T$ je rozšířením těles, $c \in T$. Řekneme, že prvek c je algebraický nad tělesem R, jestliže existuje nenulový polynom $f \in R[x]$, jehož je c kořenem. V opačném případě říkáme, že prvek c je transcendentní nad tělesem R.

Poznámka. Je-li c kořenem polynomu $f = a_n x^n + \cdots + a_1 x + a_0 \in R[x]$ stupně n, je $a_n \neq 0$, a tedy existuje $a_n^{-1} \in R$, proto c je také kořenem normovaného polynomu $a_n^{-1} \cdot f = x^n + \cdots + a_n^{-1} a_1 x + a_n^{-1} a_0 \in R[x]$.

Poznámka. O komplexním čísle c říkáme, že je algebraické (resp. transcendentní), je-li c algebraické (resp. transcendentní) nad tělesem racionálních čísel $\mathbb{Q}$.

Minimální polynom algebraického prvku

Věta. *Nechť $R \subseteq T$ je rozšířením těles, $c \in T$ algebraický prvek nad R. Pak c je kořenem právě jednoho normovaného ireducibilního polynomu $f \in R[x]$. Navíc platí*

1. *pro libovolný $h \in R[x]$ je $h(c) = 0$, právě když $f \mid h$ v $R[x]$,*
2. *$R(c) = R[c]$ v T,*
3. *$1, c, c^2, \ldots, c^{n-1}$, kde $n = \operatorname{st} f$, je bází vektorového prostoru $R[c]$ nad R,*
4. *stupeň rozšíření $[R(c) : R] = \operatorname{st} f$.*

Důkaz. Protože c je algebraický prvek nad R, můžeme mezi všemi normovanými polynomy z $R[x]$, jejichž je c kořenem, zvolit polynom co možná nejmenšího stupně a označit jej f. Označme $n = \operatorname{st} f$. Zřejmě $n > 0$. Kdyby $f = g \cdot h$ pro nějaké nekonstantní polynomy $g, h \in R[x]$, tak by bylo možné je zvolit oba normované a dostali bychom spor, protože $\operatorname{st} g < n$, $\operatorname{st} h < n$ a přitom c by byl kořenem alespoň jednoho z nich. Je tedy f ireducibilní.

Zvolme libovolný $h \in R[x]$ takový, že $h(c) = 0$. Vydělíme-li polynom h polynomem f se zbytkem, dostaneme polynomy $q, r \in R[x]$ takové, že $h = q \cdot f + r$, přičemž $\operatorname{st} r < n$. Protože $0 = h(c) = q(c) \cdot f(c) + r(c) = r(c)$, kdyby r nebyl nulový polynom, existoval by v $R[x]$ normovaný polynom stupně $\operatorname{st} r$ mající kořen c, což by byl spor s naší volbou polynomu f. Proto $f \mid h$ v $R[x]$. Protože opačná implikace je zřejmá, dokázali jsme bod 1.

Je jasné, že normovaný polynom s kořenem c splňující bod 1 je jediný (kdybychom měli takové polynomy dva, každý z nich by dělil toho druhého).

Podle věty o podokruzích generovaných množinou platí, že libovolný prvek $\alpha \in R[c]$ je tvaru $\alpha = h(c)$ pro nějaký polynom $h \in R[x]$. Dělením se zbytkem opět dostaneme polynomy $q, r \in R[x]$ takové, že $h = q \cdot f + r$, přičemž $\operatorname{st} r < n$. Opět $\alpha = h(c) = q(c) \cdot f(c) + r(c) = r(c)$. Proto $1, c, c^2, \ldots, c^{n-1}$ generují vektorový prostor $R[c]$ nad R; kdyby tyto vektory byly lineárně závislé, existoval by v $R[x]$ nenulový polynom stupně menšíno než n, který by měl c za kořen, a to by byl spor. Dokázali jsme bod 3.

Zbývá ukázat, že $R(c) = R[c]$, jinými slovy, že $R[c]$ je těleso.

Víme, že libovolný nenulový prvek $\alpha \in R[c]$ je tvaru $\alpha = h(c)$. Protože $h(c) = \alpha \neq 0$, tak $f \nmid h$, a protože f je ireducibilní, tak jsou f a h nesoudělné. Proto jejich největší společný dělitel 1 lze vyjádřit Bezoutovou rovností, tedy existují polynomy $a, b \in R[x]$ tak, že $1 = a \cdot f + b \cdot h$. Dosazením c odtud dostaneme

$$1 = a(c) \cdot f(c) + b(c) \cdot h(c) = b(c) \cdot h(c) = b(c) \cdot \alpha$$

Je tedy $b(c) \in R[c]$ inverzní prvek k prvku α v okruhu $R[c]$. Dokázali jsme bod 2, díky níž z bodu 3 plyne bod 4.

Definice. Polynom $f \in R[x]$ z předchozí věty nazýváme minimální polynom algebraického prvku $c \in T$ nad R.

(Ne)řešitelnost geometrických úloh pravítkem a kružítkem

Z antiky pocházejí tři problémy, jejichž řešení pravítkem a kružítkem nebylo známo:

- *trisekce úhlu* (rozdělit daný úhel na třetiny),
- *zdvojení krychle* (k dané krychli sestrojit krychli dvojnásobného objemu, tj. k úsečce dané délky najít úsečku $\sqrt[3]{2}$-krát delší),
- *kvadratura kruhu* (k danému kruhu sestrojit čtverec o stejném obsahu).

Abychom mohli dokázat, že žádné řešení těchto úloh neexistuje, musíme přesně specifikovat, co to znamená řešit úlohu pravítkem a kružítkem.

Předpokládejme, že v rovině je zadáno konečně mnoho bodů popisujících zadání úlohy. Těmto bodům budeme říkat význačné. Smíme sestrojit libovolnou přímku procházející dvěma význačnými body a libovolnou kružnici, jejímž středem je význačný bod a poloměrem vzdálenost některých dvou význačných bodů. Libovolný průsečík sestrojených kružnic či přímek můžeme přidat k význačným bodům. Jde o to, jestli po konečně mnoha krocích lze docílit toho, že mezi význačnými body je bod, který popisuje řešení dané úlohy.

Zavedeme v této rovině soustavu souřadnic, rovinu tedy ztotožňujeme s kartézským součinem $\mathbb{R} \times \mathbb{R}$. Označme T_0 podtěleso tělesa $\mathbb{R}$ generované x-ovými a y-ovými souřadnicemi všech zadaných bodů. Pokud bylo přidáno celkem n význačných bodů, definujeme tělesa $T_1, \ldots, T_n$ takto: těleso T_i je generováno tělesem T_{i-1} a souřadnicemi i-tého význačného bodu.

Naším cílem je dokážat, že rozšíření těles $T_0 \subseteq T_n$ je konečné a jeho stupeň $[T_n : T_0] \mid 2^n$.

Označme $[x_i, y_i]$ souřadnice i-tého význačného bodu. Tento bod byl získán jako průsečík sestrojených přímek či kružnic, rovnice takové přímky je tvaru $ax + by = c$, kde $a, b, c \in T_{i-1}$, rovnice takové kružnice tvaru $(x - m)^2 + (y - n)^2 = u$, kde $m, n, u \in T_{i-1}$. Proto $[x_i, y_i]$ je řešením soustavy dvou lineárních rovnic anebo soustavy jedné lineární a jedné kvadratické rovnice s koeficienty v T_{i-1} (případ dvou kružnic vede sice na soustavu dvou kvadratických rovnic, jejich odečtením však dostaneme rovnici lineární).

Dosazením z lineární rovnice do druhé rovnice získáme rovnici lineární nebo kvadratickou pro jednu ze souřadnic $[x_i, y_i]$ s koeficienty v T_{i-1}. Minimální polynom získaného řešení nad tělesem T_{i-1} má stupeň 1 nebo 2, druhou ze souřadnic dopočítáme z lineární rovnice. Proto $[T_i : T_{i-1}] \leq 2$.

Z věty o násobení stupňů rozšíření dostáváme $[T_n : T_0] \mid 2^n$.

Neřešitelnost úlohy zdvojení krychle

Jsou dány dva body o souřadnicích $[0,0]$ a $[0,1]$, cílem je získat bod $[0,\sqrt[3]{2}]$.

Je tedy $T_0 = \mathbb{Q}$.

Protože $x^3 - 2$ je minimální polynom čísla $\sqrt[3]{2}$ nad $\mathbb{Q}$, platí $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$.

Jestliže tedy $\sqrt[3]{2} \in T_n$, pak $3 \mid [T_n : T_0]$.

$$\begin{array}{c} T_n \\ | \\ \mathbb{Q}(\sqrt[3]{2}) \\ | \\ T_0 = \mathbb{Q} \end{array}$$

To spolu s odvozenou dělitelností $[T_n : T_0] \mid 2^n$ dává spor $3 \mid 2^n$.

Neřešitelnost úlohy trisekce úhlu

Ukážeme, že nemůžeme sestrojit pravítkem a kružítkem úhel $\frac{\pi}{9}$. Vzhledem k tomu, že umíme sestrojit úhel $\frac{\pi}{3}$ jako vnitřní úhel rovnostranného trojúhelníka, bude to znamenat, že nelze rozdělit na třetiny libovolný zadaný úhel.

Jsou dány dva body o souřadnicích $[0, 0]$ a $[0, 1]$, cílem je získat bod $[\cos\frac{\pi}{9}, \sin\frac{\pi}{9}]$. Opět máme $T_0 = \mathbb{Q}$.

K nalezení minimálního polynomu čísla $\cos\frac{\pi}{9}$ využijeme vzorec $\cos 3\alpha = \cos^3\alpha - 3\cos\alpha\sin^2\alpha = 4\cos^3\alpha - 3\cos\alpha$.

Pro $\alpha = \frac{\pi}{9}$ dostáváme, že $c = 2\cos\frac{\pi}{9}$ je kořenem polynomu $x^3 - 3x - 1$. Tento kubický polynom nemá racionální kořen (± 1 kořen není), a tedy je ireducibilní nad $\mathbb{Q}$.

Odtud $[\mathbb{Q}(\cos\frac{\pi}{9}) : \mathbb{Q}] = 3$ a stejně jako v předchozím případě dostáváme spor.

Neřešitelnost úlohy kvadratury kruhu

V tomto případě využijeme toho, že π je transcendentní číslo (tento fakt zde nebudeme dokazovat).

Jsou dány dva body o souřadnicích $[0, 0]$ a $[0, 1]$. Kruh jednotkového poloměru má obsah π. Cílem je získat bod $[0, \sqrt{\pi}]$. Opět máme $T_0 = \mathbb{Q}$.

Předpokládejme, že $\sqrt{\pi} \in T_n$, pak $\pi \in T_n$.

Protože π je transcendentní nad $\mathbb{Q}$, plyne odtud $[T_n : \mathbb{Q}] = \infty$, což je spor s tím, že $\mathbb{Q} \subseteq T_n$ je konečné rozšíření.