Algebraická čísla

Definice. Komplexní číslo α se nazývá algebraické, existuje-li normovaný polynom $f(x) \in \mathbb{Q}[x]$, jehož je α kořenem. V opačném případě se α nazývá transcendentní.

Příklad. Všechna racionální čísla jsou algebraická, pro každé $a \in \mathbb{Q}$, $n \in \mathbb{N}$ je $\sqrt[n]{a}$ kořen polynomu $x^n - a$, a tedy číslo algebraické. Čísla $\pi = 3,14159\ldots$, $e = 2,71828\ldots$ jsou transcendentní (to není vidět na první pohled, naopak je to věta, kterou je docela těžké dokázat).

Definice. Nechť α je algebraické číslo, pak ze všech normovaných polynomů s racionálními koeficienty, jejichž je α kořenem, vyberme polynom $f(x) \in \mathbb{Q}[x]$ co nejmenšího stupně. Tento polynom nazýváme minimální polynom čísla α.

Poznámka. Minimální polynom algebraického čísla α je určen jednoznačně (pokud jsou $g_1(x)$ a $g_2(x)$ dva různé normované polynomy stejného stupně mající kořen α, pak je α kořenem i nenulového rozdílu $g_1(x) - g_2(x)$ majícího menší stupeň, který je možné vydělením vedoucím koeficientem normovat).

Vlastnosti minimálního polynomu

<u>*Věta 1.*</u> *Nechť $f(x)$ je minimální polynom algebraického čísla α. Pak $f(x)$ je ireducibilní nad $\mathbb{Q}$ a pro libovolný polynom $h(x) \in \mathbb{Q}[x]$ platí $h(\alpha) = 0$, právě když $f(x) \mid h(x)$ v $\mathbb{Q}[x]$.*

<u>*Důkaz.*</u> Sporem: je-li $f(x) = g_1(x) \cdot g_2(x)$ rozklad $f(x)$ na součin nekonstantních polynomů s racionálními koeficienty, pak $g_1(\alpha) = 0$ nebo $g_2(\alpha) = 0$. Po vydělení vedoucím koeficientem dostaneme normovaný polynom s racionálními koeficienty s kořenem α menšího stupně než je stupeň $f(x)$, spor.
Vydělme polynom $h(x)$ polynomem $f(x)$ se zbytkem:
$h(x) = q(x)f(x) + r(x)$ pro $q(x), r(x) \in \mathbb{Q}[x]$, $\operatorname{st} r(x) < \operatorname{st} f(x)$.
Dosazením α za x dostaneme $h(\alpha) = r(\alpha)$. Je-li $r(x)$ nulový polynom, pak $f(x) \mid h(x)$ v $\mathbb{Q}[x]$ a současně α je kořenem $h(x)$.
Jestliže $r(x)$ není nulový polynom, pak by $r(\alpha) = 0$ vedlo ke sporu (vydělením vedoucím koeficientem bychom dostali normovaný polynom s racionálními koeficienty s kořenem α menšího stupně než je stupeň $f(x)$), a tedy $h(\alpha) = r(\alpha) \neq 0$ a $f(x) \nmid h(x)$ v $\mathbb{Q}[x]$.

Celá algebraická čísla

Definice. Algebraické číslo α se nazývá celé algebraické, má-li jeho minimální polynom $f(x)$ celočíselné koeficienty.

Příklad. Libovolné $a \in \mathbb{Q}$ má minimální polynom $x - a$, a tedy racionální čísla jsou celá algebraická, právě když jsou celá. Číslo $\sqrt[3]{2}$ je celé algebraické (jeho minimální polynom je $x^3 - 2$), číslo $\sqrt{\frac{2}{3}}$ není celé algebraické (jeho minimální polynom je $x^2 - \frac{2}{3}$).

Definice. Nenulový polynom $f(x) \in \mathbb{Z}[x]$ se nazývá primitivní, je-li největší společný dělitel jeho koeficientů roven 1.

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

Důkaz. Sporem: předpokládejme, že každý koeficient součinu primitivních polynomů $f(x)$, $g(x)$ je dělitelný nějakým prvočíslem p. Máme homomorfismus okruhů $\psi : \mathbb{Z}[x] \to \mathbb{Z}_p[x]$ (každý koeficient je nahrazen zbytkovou třídou). Z primitivnosti $\psi(f(x)) \neq 0$, $\psi(g(x)) \neq 0$. Přitom $\psi(f(x)) \cdot \psi(g(x)) = \psi(f(x) \cdot g(x)) = 0$. Ovšem $\mathbb{Z}_p[x]$ je obor integrity, spor.

Celá algebraická čísla

<u>*Věta 2.*</u> *Algebraické číslo α je celé algebraické, právě když existuje normovaný polynom $h(x) \in \mathbb{Z}[x]$, jehož je α kořenem.*

<u>*Důkaz.*</u> Je-li α celé algebraické, je tímto polynomem jeho minimální polynom.
Naopak, předpokládejme, že existuje normovaný polynom $h(x) \in \mathbb{Z}[x]$, $h(\alpha) = 0$. Označme $f(x)$ minimální polynom čísla α. Z věty 1 víme, že existuje $g(x) \in \mathbb{Q}[x]$ tak, že $h(x) = f(x) \cdot g(x)$. Protože $f(x)$, $g(x)$ jsou normované, existují přirozená čísla n, m tak, že $nf(x)$, $mg(x)$ jsou primitivní (n, m jsou nejmenší společné násobky jmenovatelů koeficientů polynomů $f(x)$, $g(x)$). Podle Gaussova lemmatu je $mn \cdot h(x) = (nf(x)) \cdot (mg(x))$ také primitivní. Protože polynom $h(x) \in \mathbb{Z}[x]$, znamená to, že $mn = 1$, tedy $n = 1$, odkud $f(x) \in \mathbb{Z}[x]$, a tedy α je celé algebraické.

Celá algebraická čísla

Věta 3. Nechť $\omega_1, \dots, \omega_n \in \mathbb{C}$. Nechť M je aditivní grupa, generovaná $\omega_1, \dots, \omega_n$, tj.

$$M = \{a_1\omega_1 + \cdots + a_n\omega_n;\ a_1, \dots, a_n \in \mathbb{Z}\}.$$

Jestliže pro každé $\alpha, \beta \in M$ platí $\alpha \cdot \beta \in M$, pak je libovolný prvek M celé algebraické číslo.

Důkaz. Bez újmy na obecnosti můžeme předpokládat, že $\omega_1 \dots \omega_n \neq 0$. Buď $\alpha \in M$ libovolné. Protože pro každé $i = 1, \dots, n$ platí $\alpha\omega_i \in M$, existují celá čísla a_{ij} splňující

$$\alpha\omega_i = \sum_{j=1}^{n} a_{ij}\omega_j$$

pro každé $i = 1, \dots, n$. Odtud plyne, že $\det(\alpha E - (a_{ij})) = 0$, kde E je jednotková matice řádu n. Proto je α kořenem normovaného polynomu $f(x) = \det(xE - (a_{ij})) \in \mathbb{Z}[x]$.

Celá algebraická čísla

Věta 4. Označme A množinu všech celých algebraických čísel. Pak A je obor integrity.

Důkaz. Abychom ověřili, že A je obor integrity, stačí ukázat, že je podokruhem tělesa $\mathbb{C}$. Víme, že $\mathbb{Z} \subseteq A$. Musíme tedy dokázat, že pro libovolná $\alpha, \beta \in A$ jsou $\alpha + \beta$, $\alpha - \beta$ i $\alpha\beta$ celá algebraická čísla. Protože α a β jsou celá algebraická čísla, existují polynomy s celými koeficienty $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$, $g(x) = x^m + b_{m-1}x^{m-1} + \cdots + b_1 x + b_0$ tak, že $f(\alpha) = 0$ a $g(\beta) = 0$. Pak ovšem platí

$$\alpha^n = -a_{n-1}\alpha^{n-1} - \cdots - a_1\alpha - a_0, \; \beta^m = -b_{m-1}\beta^{m-1} - \cdots - b_1\beta - b_0,$$

a tedy podgrupa M aditivní grupy tělesa K generovaná součiny

$$\alpha^i \beta^j, \qquad \text{kde } 0 \le i < n,\ 0 \le j < m, \tag{1}$$

je uzavřená na násobení, neboť libovolný součin $\alpha^u \beta^v$ pro $u \ge 0$, $v \ge 0$ je možné vyjádřit jako $\mathbb{Z}$-lineární kombinaci prvků (1). Podle věty 3 jsou $\alpha + \beta$, $\alpha - \beta$, $\alpha\beta \in M$ celá algebraická čísla.

Těleso algebraických čísel

Definice. Jsou-li K, L tělesa a je-li K podokruhem L, řekneme, že L je rozšířením tělesa K. Pak je L vektorový prostor nad K (sčítání vektorů i násobení vektorů skaláry je určeno operacemi $+$, $\cdot$ v L). Je-li navíc L konečněrozměrný vektorový prostor nad K, hovoříme o konečném rozšíření, jeho dimenzi značíme $[L : K]$ a nazýváme stupněm rozšíření.

Poznámka. Je-li K podtěleso tělesa $\mathbb{C}$, pak K obsahuje $\mathbb{Q}$, a tedy je rozšířením tělesa $\mathbb{Q}$. Je-li toto rozšíření konečné, říkáme, že K je těleso algebraických čísel stupně $[K : \mathbb{Q}]$.

Varování. Pozor, přestože množina M všech algebraických čísel tvoří podtěleso tělesa $\mathbb{C}$, není M těleso algebraických čísel! Vektorový prostor M nad $\mathbb{Q}$ je totiž nekonečněrozměrný.

Těleso algebraických čísel obsahuje jen algebraická čísla

Věta 5. Nechť K je těleso algebraických čísel, pak každé $\alpha \in K$ je algebraické.

Důkaz. Označme $n = [K : \mathbb{Q}]$. Pak α^n, α^{n-1}, ..., α, 1 je $n+1$ vektorů v n-rozměrném vektorovém prostoru nad $\mathbb{Q}$, proto jsou lineárně závislé, tj. existují a_n, a_{n-1}, ... a_1, $a_0 \in \mathbb{Q}$, ne všechna nulová, tak, že $a_n\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 = 0$, tedy α je kořen nenulového polynomu s racionálními koeficienty $f(x) = a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$.

Okruh R celých algebraických čísel v tělese K

Věta 6. Nechť K je těleso algebraických čísel, pak množina R všech celých algebraických čísel z tělesa K tvoří obor integrity, jehož podílovým tělesem je K.

Důkaz. Stejně jako ve větě 4 označme A množinu všech celých algebraických čísel. Platí $R = K \cap A$, přičemž A i K jsou podokruhy tělesa $\mathbb{C}$. Proto i R je podokruh tělesa $\mathbb{C}$, tedy obor integrity. Zbývá dokázat, že K je podílové těleso okruhu R. Nechť $\beta \in K$ je libovolné. Podle věty 5 existuje normovaný polynom $f(x) = x^k + a_{k-1}x^{k-1} + \cdots + a_1x + a_0 \in \mathbb{Q}[x]$ tak, že $f(\beta) = 0$. Nechť n je nejmenší společný násobek jmenovatelů koeficientů polynomu $f(x)$. Pak polynom $g(x) = x^k + na_{k-1}x^{k-1} + \cdots + n^{k-1}a_1x + n^k a_0 \in \mathbb{Z}[x]$ má kořen $\alpha = n\beta$, neboť $g(\alpha) = g(n\beta) = n^k \cdot f(\beta) = 0$. Je tedy $\alpha \in R$, rovněž $n \in R$. Je tedy $\beta = \frac{\alpha}{n}$ podílem dvou čísel z R. Dokázali jsme, že K je podílové těleso okruhu R.

Opakování z algebry: dělitelnost v oborech integrity

Nechť R je obor integrity, $a, b \in R$.

<u>*Definice.*</u> Řekneme, že a dělí b v R, píšeme $a|b$, jestliže existuje $c \in R$ tak, že $b = a \cdot c$.

<u>*Definice.*</u> Řekneme, že a a b jsou asociované v R, píšeme $a \sim b$, jestliže $a|b$ a současně $b|a$.

<u>*Poznámka.*</u> Platí, že $a \sim b$, právě když existuje jednotka $c \in R^{\times}$ tak, že $b = a \cdot c$.

<u>*Definice.*</u> Prvek a se nazývá ireducibilní prvek v R, jestliže $a \neq 0$, $a \notin R^{\times}$, a kdykoli $a = c \cdot d$ pro $c, d \in R$, pak $c \in R^{\times}$ nebo $d \in R^{\times}$.

<u>*Příklad.*</u> V $\mathbb{Z}$ jsou ireducibilními prvky právě prvočísla a čísla k nim opačná. Je-li K těleso, ireducibilními prvky v $K[x]$ jsou ireducibilní polynomy (například pro $K = \mathbb{C}$ jsou to právě lineární polynomy, pro $K = \mathbb{R}$ jsou to lineární polynomy a kvadratické polynomy se záporným diskriminantem).

Opakování z algebry: okruh s jednoznačným rozkladem

Definice. Říkáme, že okruh R je okruh s jednoznačným rozkladem, jestliže

- R je obor integrity;
- každý $a \in R$, $a \neq 0$, $a \notin R^\times$, je možné napsat jako součin ireducibilních prvků, a to jednoznačně až na pořadí činitelů a jejich asociovanost.

Poznámka. Jednoznačností až na pořadí činitelů a jejich asociovanost znamená toto: jsou-li $a = p_1 \cdots p_n$ a $a = q_1 \cdots q_m$ rozklady prvku a na součiny ireducibilních prvků v R, pak $n = m$ a případnou změnou pořadí činitelů v součinech lze docílit toho, že platí $p_1 \sim q_1, \dots p_n \sim q_n$.

Příklad. Okruhem s jednoznačným rozkladem je například $\mathbb{Z}$ nebo $K[x]$, kde K je libovolné těleso. Z triviálních důvodů je i každé těleso K okruhem s jednoznačným rozkladem (kromě nuly a jednotek totiž těleso žádné jiné prvky nemá).

Příklad: $K = \mathbb{Q}(i\sqrt{15}) = \{a + bi\sqrt{15};\ a,\ b \in \mathbb{Q}\}$

Snadno se ukáže, že K je těleso algebraických čísel a že $[K : \mathbb{Q}] = 2$. Označme R okruh všech celých algebraických čísel v K. Je-li $a,\ b \in \mathbb{Z}$, pak $\alpha = a + b\frac{1+i\sqrt{15}}{2}$ je kořenem polynomu

$$(x-a-b\tfrac{1+i\sqrt{15}}{2})(x-a-b\tfrac{1-i\sqrt{15}}{2}) = x^2-(2a+b)x+(a^2+ab+4b^2),$$

a tedy $\alpha \in R$.

Předpokládejme naopak, že pro nějaké $a,\ b \in \mathbb{Q}$ platí $\alpha = a + b\frac{1+i\sqrt{15}}{2} \in R$ a dokažme, že $a,\ b \in \mathbb{Z}$. Je-li $b = 0$, je $\alpha = a \in \mathbb{Q}$, jeho minimální polynom je $x - a$, a tedy $a \in \mathbb{Z}$. Nechť dále $b \neq 0$, tj. $\alpha \notin \mathbb{Q}$. Pak je minimálním polynomem čísla α polynom $f(x) = x^2 - (2a + b)x + (a^2 + ab + 4b^2)$, tedy $c = 2a + b \in \mathbb{Z}$, $d = a^2 + ab + 4b^2 \in \mathbb{Z}$. Proto $-15b^2 = c^2 - 4d \in \mathbb{Z}$, tj. $b \in \mathbb{Z}$. Pak ovšem $2a = c - b \in \mathbb{Z}$, a tedy $2a^2 = 2d - (2a)b - 8b^2 \in \mathbb{Z}$, odkud $a \in \mathbb{Z}$. Dokázali jsme, že $a,\ b \in \mathbb{Z}$, tj.

$$R = \{a + b\tfrac{1+i\sqrt{15}}{2};\ a,\ b \in \mathbb{Z}\}.$$

Aritmetika okruhu $R = \{a + b\frac{1+i\sqrt{15}}{2};\ a,\ b \in \mathbb{Z}\}$

Definujme zobrazení (tzv. normu) $\mathcal{N}: R \to \mathbb{Z}$ předpisem $\mathcal{N}(\alpha) = \alpha \cdot \overline{\alpha} = |\alpha|^2$ pro libovolné $\alpha \in R$. Pro $a, b \in \mathbb{Z}$ tedy $\mathcal{N}(a + b\frac{1+i\sqrt{15}}{2}) = a^2 + ab + 4b^2$. Pak platí, že $\mathcal{N}(\alpha\beta) = |\alpha\beta|^2 = |\alpha|^2 \cdot |\beta|^2 = \mathcal{N}(\alpha) \cdot \mathcal{N}(\beta)$ pro každé $\alpha,\ \beta \in R$. Ukažme, že grupa $R^\times$ všech jednotek okruhu R je rovna $R^\times = \{\alpha \in R; \mathcal{N}(\alpha) = \pm 1\}$. Skutečně, je-li $\alpha \in R^\times$, existuje $\beta \in R$ tak, že $\alpha\beta = 1$, odkud plyne $1 = \mathcal{N}(\alpha\beta) = \mathcal{N}(\alpha)\mathcal{N}(\beta)$, a tedy $\mathcal{N}(\alpha) = \pm 1$. Naopak, je-li $\mathcal{N}(\alpha) = \pm 1$, pak $\alpha \cdot (\pm\overline{\alpha}) = 1$, a tedy $\alpha \in R^\times$. Protože $a^2 + ab + 4b^2 = \frac{1}{4}(2a + b)^2 + \frac{15}{4}b^2$, platí pro $a, b \in \mathbb{Z}$, že $\mathcal{N}(a + b\frac{1+i\sqrt{15}}{2}) = \pm 1$, právě když $(2a + b)^2 + 15b^2 = \pm 4$, což nastává právě když $b = 0$ a $a = \pm 1$. Je tedy $R^\times = \{1, -1\}$. Rozložme $4 = 2 \cdot 2 = \frac{1+i\sqrt{15}}{2} \cdot \frac{1-i\sqrt{15}}{2}$ na součin ireducibilních prvků. Kdyby totiž některý z těchto činitelů nebyl ireducibilní, z $\mathcal{N}(2) = \mathcal{N}(\frac{1+i\sqrt{15}}{2}) = \mathcal{N}(\frac{1-i\sqrt{15}}{2}) = 4$ by plynula existence $\alpha \in R$ tak, že $\mathcal{N}(\alpha) = \pm 2$, tedy existence $a, b \in \mathbb{Z}$ tak, že $(2a + b)^2 + 15b^2 = \pm 8$. Tato rovnice však nemá řešení v $\mathbb{Z}$. Proto R **není okruh s jednoznačným rozkladem**.

Další příklad: $K = \mathbb{Q}(\sqrt{10}) = \{a + b\sqrt{10};\ a,\ b \in \mathbb{Q}\}$

Opět je snadné ukázat, že K je těleso algebraických čísel a že $[K : \mathbb{Q}] = 2$. Označme R okruh všech celých algebraických čísel v K. Je-li $a,\ b \in \mathbb{Z}$, pak $\alpha = a + b\sqrt{10}$ je kořenem polynomu

$$(x - a - b\sqrt{10})(x - a + b\sqrt{10}) = x^2 - 2ax + (a^2 - 10b^2),$$

a tedy $a + b\sqrt{10} \in R$. Předpokládejme naopak, že pro nějaké $a,\ b \in \mathbb{Q}$ platí $\alpha = a + b\sqrt{10} \in R$ a dokažme, že $a,\ b \in \mathbb{Z}$. Je-li $b = 0$, je $\alpha = a \in \mathbb{Q}$, jeho minimální polynom je $x - a$, a tedy $a \in \mathbb{Z}$. Nechť dále $b \neq 0$, tj. $\alpha \notin \mathbb{Q}$. Pak je minimálním polynomem čísla α polynom $f(x) = x^2 - 2ax + (a^2 - 10b^2)$, tedy $c = 2a \in \mathbb{Z}$, $a^2 - 10b^2 \in \mathbb{Z}$. Proto $40b^2 = c^2 - 4(a^2 - 10b^2) \in \mathbb{Z}$, odkud $d = 2b \in \mathbb{Z}$. Pak ovšem $4 \mid 4(a^2 - 10b^2) = c^2 - 10d^2$ a tedy c^2 je sudé číslo. Je tedy sudé i samo c a proto je sudé i d^2 a tedy i d. Dokázali jsme, že $a,\ b \in \mathbb{Z}$, tj.

$$R = \{a + b\sqrt{10};\ a,\ b \in \mathbb{Z}\}.$$

Aritmetika okruhu $R = \{a + b\sqrt{10};\ a,\ b \in \mathbb{Z}\}$

Definujme normu $\mathcal{N} :\ R \to \mathbb{Z}$, pro libovolné $a, b \in \mathbb{Z}$ položme $\mathcal{N}(a + b\sqrt{10}) = (a + b\sqrt{10}) \cdot (a - b\sqrt{10}) = a^2 - 10b^2$. Opět platí $\mathcal{N}(\alpha\beta) = \mathcal{N}(\alpha) \cdot \mathcal{N}(\beta)$ pro každé $\alpha,\ \beta \in R$. Odtud plyne, že grupa všech jednotek okruhu R je $R^\times = \{\alpha \in R;\ \mathcal{N}(\alpha) = \pm 1\}$.
Zřejmě $3 + \sqrt{10} \in R^\times$. Odtud $R^\times \supseteq \{\pm(3 + \sqrt{10})^n;\ n \in \mathbb{Z}\}$.
Dokažme, že platí rovnost: budeme předpokládat existenci nějaké jednotky $\eta \in R^\times$, pro kterou $\pm\eta$ není mocninou $3 + \sqrt{10}$ a dojdeme ke sporu. Můžeme předpokládat, že $\eta > 0$ (jinak vezmeme $-\eta$), dokonce že $\eta > 1$ (jinak vezmeme $\frac{1}{\eta}$). Navíc můžeme předpokládat $\eta < 3 + \sqrt{10}$ (jinak vydělíme η největší mocninou čísla $3 + \sqrt{10}$ menší než η). Je tedy $\eta = a + b\sqrt{10}$ pro nějaké $a,\ b \in \mathbb{Z}$ a platí $1 < a + b\sqrt{10} < 3 + \sqrt{10}$,
$\mathcal{N}(a + b\sqrt{10}) = (a + b\sqrt{10})(a - b\sqrt{10}) = \pm 1$. Tudíž $a - b\sqrt{10} = \frac{\pm 1}{\eta}$, a proto $-1 < a - b\sqrt{10} < 1$. Sečtením odtud plyne $0 < 2a < 4 + \sqrt{10}$, což vzhledem k tomu, že a je celé číslo, znamená $a \in \{1, 2, 3\}$. Protože b je rovněž celé číslo a platí $b^2 = \frac{1}{10}(a^2 \mp 1)$, dostali jsme, že $\eta = 1$ nebo $\eta = 3 \pm \sqrt{10}$, spor.

Aritmetika okruhu $R = \{a + b\sqrt{10};\ a,\ b \in \mathbb{Z}\}$

Rozložme
$$9 = 3 \cdot 3 = (1 + \sqrt{10})(-1 + \sqrt{10}).$$
Přitom $\mathcal{N}(3) = 9$ a $\mathcal{N}(1 + \sqrt{10}) = \mathcal{N}(-1 + \sqrt{10}) = -9$.
Dokážeme-li, že v R neexistují čísla s normou ± 3, budeme vědět, že všechna čtyři čísla uvedená v rozkladu čísla 9 jsou ireducibilní, tj. není možné je zapsat ve tvaru součinu dvou čísel z R, které nejsou jednotkami. To je ale snadné: z $a^2 - 10b^2 = \pm 3$ plyne $a^2 \equiv \pm 3 \pmod 5$, spor.
Zbývá vysvětlit, že činitelé nejsou asociovaní: kdyby platilo $3 \sim 1 + \sqrt{10}$ v R, bylo by $\frac{1}{3} + \frac{1}{3}\sqrt{10} \in R$, spor.
Proto R **není okruh s jednoznačným rozkladem**.

Opakování z algebry: ideály v komutativních okruzích

Nechť R je komutativní okruh (jako vždy s jedničkou).

Definice. Řekneme, že $I \subseteq R$ je ideál okruhu R, jestliže $I \neq \emptyset$, pro každé $a, b \in I$ a každé $r \in R$ platí $a + b \in I$, $r \cdot a \in I$.

Příklad. Pro libovolné $a \in R$ je $aR = \{r \cdot a;\ r \in R\}$ ideál okruhu R. Ideál $\{0\}$ se nazývá nulový.

Definice. Ideály aR pro $a \in R$ se nazývají hlavní.

Poznámka. Je-li R obor integrity, pak pro $a, b \in R$ platí $aR = bR$, právě když $a \sim b$, tj. právě když existuje jednotka $c \in R^\times$ tak, že $b = a \cdot c$.

Definice. Jsou-li I, J ideály okruhu R, definujeme
$I + J = \{a + b;\ a \in I,\ b \in J\}$ jejich součet a
$I \cdot J = \{\sum_{i=1}^{n} a_i b_i;\ n \in \mathbb{N},\ a_1, \ldots, a_n \in I,\ b_1, \ldots, b_n \in J\}$ jejich součin.

Příklad. Pro libovolné $a, b \in R$ platí $aR \cdot bR = (a \cdot b)R$. Pozor, nic podobného pro sčítání hlavních ideálů neplatí!

Opakování z algebry: ideály v komutativních okruzích

Stále R je komutativní okruh.

Poznámka. Součet a součin libovolných ideálů okruhu R je ideálem okruhu R. Součet $I + J$ je nejmenší ze všech ideálů obsahujících $I \cup J$. Operace $+$ a $\cdot$ jsou asociativní a komutativní, pro libovolné ideály I_1, I_2, J platí $(I_1 + I_2) \cdot J = I_1 \cdot J + I_2 \cdot J$.

Definice. Ideál I okruhu R se nazývá prvoideál, jestliže $I \neq R$ a pro každé $a, b \in R$ z $ab \in I$ plyne $a \in I$ nebo $b \in I$.

Příklad. Nulový ideál $\{0\}$ je prvoideál, právě když R je obor integrity.

Definice. Ideál I okruhu R se nazývá maximální ideál, jestliže $I \neq R$ a neexistuje žádný ideál J okruhu R splňující $I \subsetneq J \subsetneq R$.

Příklad. V okruhu $\mathbb{Z}$ jsou všechny ideály hlavní, maximální ideály jsou právě ideály $p\mathbb{Z}$, kde p je prvočíslo. Prvoideály okruhu $\mathbb{Z}$ jsou právě tyto maximální ideály a také nulový ideál.

Opakování z algebry: faktorokruh komutativního okruhu

Věta 7. Nechť R je komutativní okruh, I jeho ideál. Pro libovolné $a \in R$ označme $a + I = \{a + j; j \in I\}$. Pak $R/I = \{a + I; a \in R\}$ tvoří rozklad na množině R, na kterém lze definovat operace $+$ a $\cdot$ „pomocí reprezentantů", tj. předpisem

$$\begin{aligned}(a+I)+(b+I) &= (a+b)+I,\\ (a+I)\cdot(b+I) &= (a\cdot b)+I.\end{aligned}$$

Pak R/I s těmito operacemi tvoří komutativní okruh (tzv. faktorokruh okruhu R podle ideálu I).

Věta 8. Nechť R je komutativní okruh, I jeho ideál. Pak I je prvoideál okruhu R, právě když R/I je obor integrity. Podobně I je maximální ideál okruhu R, právě když R/I je těleso.

Důkazy obou vět lze najít ve skriptech J. Rosický: Algebra.

Důsledek. Každý maximální ideál okruhu R je prvoideálem okruhu R.

Aritmetika okruhů R celých algebraických čísel

Nechť K je těleso algebraických čísel (tj. $K \subseteq \mathbb{C}$, $[K : \mathbb{Q}] < \infty$), nechť R je okruh celých algebraických čísel v tělese K.

Poznámka. Je-li $K = \mathbb{Q}$, pak $R = \mathbb{Z}$ je okruh s jednoznačným rozkladem. Viděli jsme však, že pro $K = \mathbb{Q}(\sqrt{10})$ dostaneme $R = \{a + b\sqrt{10};\ a,\ b \in \mathbb{Z}\}$ a pro $K = \mathbb{Q}(i\sqrt{15})$ máme $R = \{a + b\frac{1+i\sqrt{15}}{2};\ a,\ b \in \mathbb{Z}\}$, což nejsou okruhy s jednoznačným rozkladem. Kummer v polovině 19. století objevil způsob, jak jednoznačné rozkládání v okruzích celých algebraických čísel zachránit: platí zde následující věta o jednoznačném rozkladu ideálů (takto Kummerovy výsledky přeformulovat Dedekind).

Věta 9. *Nechť R je okruh celých algebraických čísel v nějakém tělese algebraických čísel K. Nechť I je ideál R, $I \neq R$, $I \neq \{0\}$. Pak existuje jednoznačně určené $n \in \mathbb{N}$ a jednoznačně (až na pořadí) určené prvoideály $P_1, \dots, P_n$ takové, že platí*

$$I = P_1 \dots P_n.$$

Důkaz je mimo možnosti této přednášky.

Aritmetika okruhů R celých algebraických čísel

<u>*Věta 10.*</u> *Nechť R je okruh celých algebraických čísel v nějakém tělese algebraických čísel K. Je-li každý ideál okruhu R hlavní, pak R je okruh s jednoznačným rozkladem.*

<u>*Náznak důkazu.*</u> Protože je každý ideál okruhu R hlavní, pro každý ideál A existuje prvek $a \in R$ tak, že $A = aR$. Přitom je prvek a určen ideálem A jednoznačně až na asociovanost a platí, že $A \neq \{0\}$ je prvoideál, právě když a je ireducibilní.
Nechť $a \in R$, $a \neq 0$, $a \notin R^\times$. Pak existence a jednoznačnost rozkladu prvku a na součin ireducibilních prvků plyne z existence a jednoznačnosti rozkladu ideálu aR na součin prvoideálů.

<u>*Poznámka.*</u> Míru toho, nakolik se okruh celých algebraických čísel R nějakého tělesa algebraických čísel K liší od okruhu s jednoznačným rozkladem, nám vlastně udává to, kolik ze všech ideálů okruhu R je hlavních. Ovšem všech ideálů je spočetně mnoho, hlavních ideálů je také spočetně mnoho, proto slovu „kolik" v předchozí větě je nutno rozumět správně.

Grupa tříd ideálů okruhu R celých algebraických čísel

Nechť K je těleso algebraických čísel (tj. $K \subseteq \mathbb{C}$, $[K : \mathbb{Q}] < \infty$), nechť R je okruh celých algebraických čísel v tělese K. Uvažme pologrupu $(\mathcal{I}, \cdot)$ všech nenulových ideálů okruhu R a jeho podpologrupu všech nenulových hlavních ideálů. Můžeme uvážit faktorizaci této pologrupy podle zmíněné podpologrupy, což odpovídá následující ekvivalenci mezi ideály: položíme $I \approx J$, právě když existují nenulová $a, b \in R$ splňující $aR \cdot I = bR \cdot J$. Pro libovolný nenulový ideál I označme $[I] = \{J \in \mathcal{I};\, J \approx I\}$ třídu všech ideálů ekvivalentních s I.
Nechť $\mathcal{I}/\!\approx\, = \{[I]; I \in \mathcal{I}\}$ je rozklad příslušný této ekvivalenci.
Na $\mathcal{I}/\!\approx$ lze zavést operaci pomocí reprezentantů: $[I] \cdot [J] = [I \cdot J]$.

Věta 11. $(\mathcal{I}/\!\approx, \cdot)$ *je konečná komutativní grupa.*
Důkaz je mimo možnosti této přednášky.

Definice. Grupa z věty 11 se nazývá grupa tříd ideálů okruhu R (nebo také tělesa K) a je jednou z nejdůležitějších charakteristik aritmetiky v okruhu R. Počet jejích prvků se nazývá počet tříd ideálů okruhu R (též tělesa K).