ÚVOD DO ALGEBRAICKÉ TEORIE ČÍSEL

ANDREW KOZLÍK

Tento text navazuje na skripta k předmětu *Komutativní okruhy* [1] a společně s nimi pokrývá obsah přednášky *Úvod do algebraické teorie čísel* na MFF UK v letním semestru 2011/2012.

Tvrzení 1. *Nechť K je číselné těleso, pak $\Delta(\mathbb{Z}_K) \equiv 0, 1 \pmod 4$.*

Důkaz. Nechť $\{g_1, \dots, g_n\} = \mathrm{Hom}_{\mathbb{Q}}(K, \bar{K})$ a $\{\alpha_1, \dots, \alpha_n\}$ je celistvá báze K nad $\mathbb{Q}$. Pak $\Delta(\mathbb{Z}_K) = \Delta(\alpha_1, \dots, \alpha_n) = (\det(g_i(\alpha_j)))^2 = (a - 2b)^2 = a^2 - 4ab + 4b^2$, kde

$$\det(g_i(\alpha_j)) = \sum_{\pi \in S_n} \operatorname{sgn} \pi \prod_{i=1}^{n} g_{\pi(i)}(\alpha_i) = \underbrace{\sum_{\pi \in S_n} \prod_{i=1}^{n} g_{\pi(i)}(\alpha_i)}_{a} - 2 \underbrace{\sum_{\pi \in S_n \setminus A_n} \prod_{i=1}^{n} g_{\pi(i)}(\alpha_i)}_{b} = a - 2b.$$

Pro každé $g \in \mathrm{Hom}_{\mathbb{Q}}(K, \bar{K})$ je $g(a) = \sum_{\pi \in S_n} \prod_{i=1}^{n} g(g_{\pi(i)}(\alpha_i)) = a$, protože složení $g \circ g_{\pi(i)}$ má akorát za následek, že se změní pořadí součtu. Takže $a \in \mathrm{Fix}(K, \mathrm{Hom}_{\mathbb{Q}}(K, \bar{K})) = \mathbb{Q}$. Pro každé i platí $g_i(\mathbb{Z}_K) \subseteq \mathbb{Z}_K$, takže $a, b \in \mathbb{Z}_K$, a navíc $a \in \mathbb{Z}_K \cap \mathbb{Q} = \mathbb{Z}$. Dále $-ab + b^2 = \frac{1}{4}(\Delta(\mathbb{Z}_K) - a^2) \in \mathbb{Q} \cap \mathbb{Z}_K = \mathbb{Z}$, čili $\Delta(\mathbb{Z}_K) = a^2 + 4(-ab + b^2) \equiv a^2 \equiv 0, 1 \pmod 4$. □

Tvrzení 2. *Pro $\alpha \in \mathbb{Z}_K$ platí, že $\alpha \in \mathbb{Z}_K^*$ právě tehdy, když $\mathrm{N}_{K|\mathbb{Q}}(\alpha) \in \{-1, 1\}$.*

Důkaz. Jestliže $\alpha \in \mathbb{Z}_K^*$, pak i $\alpha^{-1} \in \mathbb{Z}_K^*$, a tedy α i α^{-1} mají celočíselnou normu, přičemž platí $\mathrm{N}_{K|\mathbb{Q}}(\alpha)\,\mathrm{N}_{K|\mathbb{Q}}(\alpha^{-1}) = \mathrm{N}_{K|\mathbb{Q}}(1) = 1$, takže $\mathrm{N}_{K|\mathbb{Q}}(\alpha) \in \{-1, 1\}$.

Nyní naopak předpokládejme, že $\mathrm{N}_{K|\mathbb{Q}}(\alpha) \in \{-1, 1\}$ a označme $\{g_1, \dots, g_n\} = \mathrm{Hom}_{\mathbb{Q}}(K, \bar{K})$, kde g_1 je identický homomorfismus. Pak $\pm 1 = \mathrm{N}_{K|\mathbb{Q}}(\alpha) = \prod_{i=1}^{n} g_i(\alpha) = \alpha \prod_{i=2}^{n} g_i(\alpha)$ a pro každé i je $g_i(\mathbb{Z}_K) \subseteq \mathbb{Z}_K$, takže $\alpha^{-1} = \pm \prod_{i=2}^{n} g_i(\alpha) \in \mathbb{Z}_K$. □

Věta 3. *Třídová grupa číselného tělesa K je konečná.*

Důkaz. Ukážeme, že pro každou třídu $T \in \mathcal{C}l_K$ existuje ideál J v $\mathbb{Z}_K$ takový, že $T = [J]$ a $\mathcal{N}(J) \leq H_K = \prod_{j=1}^{n} \sum_{i=1}^{n} |g_j(\alpha_i)|$, kde $\{\alpha_1, \dots, \alpha_n\}$ je celistvá báze $\mathbb{Z}_K$ a $\{g_1, \dots, g_n\} = \mathrm{Hom}_{\mathbb{Q}}(K, \bar{K})$. Podle tvrzení IV.1.3 [1] je takových J konečně mnoho, a tím pádem i tříd v $\mathcal{C}l_K$ je konečně mnoho.

Nechť tedy $T \in \mathcal{C}l_K$, pak také $T^{-1} \in \mathcal{C}l_K$ a existuje ideál I v $\mathbb{Z}_K$ a $d \in \mathbb{Z}_K$ takové, že $T^{-1} = [d^{-1}I]$. Vzhledem k tomu, že počítáme modulo hlavní lomené ideály, je $[d^{-1}I] = [I]$, neboť $d^{-1}II^{-1} = d^{-1}\mathbb{Z}_K \in \mathcal{P}_K$.

Ať $M = \{ \sum_{i=1}^{n} m_i \alpha_i \mid 0 \leq m_i < \sqrt[n]{\mathcal{N}(I)} + 1, m_i \in \mathbb{Z} \}$, pak existuje $k \in \mathbb{Z}$ takové, že $\sqrt[n]{\mathcal{N}(I)} \leq k < \sqrt[n]{\mathcal{N}(I)} + 1$. Takže $|M| \geq (k+1)^n \geq k^n + 1 \geq \mathcal{N}(I) + 1 = |\mathbb{Z}_K / I| + 1$. To znamená, že alespoň 2 prvky z množiny M leží v téže třídě faktorokruhu $\mathbb{Z}_K / I$. Označme tyto prvky a a b, pak $a - b \in I \setminus \{0\}$, a $a - b = \sum_{i=1}^{n} m_i' \alpha_i$, kde $|m_i'| < \sqrt[n]{\mathcal{N}(I)} + 1$ pro každé i. Vzhledem k tomu, že $a - b \in I$, je $(a-b)\mathbb{Z}_K \subseteq I$, a existuje tedy ideál J v $\mathbb{Z}_K$ takový, že $(a-b)\mathbb{Z}_K = IJ$. Jelikož $(a-b)\mathbb{Z}_K \in \mathcal{P}_K$, je $[J] = [I^{-1}] = T$. Nyní určíme horní odhad pro $\mathcal{N}(J)$:

$$\begin{aligned} \mathcal{N}(I)\,\mathcal{N}(J) = \mathcal{N}((a-b)\mathbb{Z}_K) = \mathrm{N}_{K|\mathbb{Q}}(a-b) &= |\prod_{i=1}^{n} g_i(a-b)| \\ &= |\prod_{i=1}^{n} \sum_{j=1}^{n} m_j' g_i(\alpha_j)| \leq \prod_{i=1}^{n} \sum_{j=1}^{n} |m_j'||g_i(\alpha_j)| \leq (\sqrt[n]{\mathcal{N}(I)} + 1)^n H_K, \end{aligned}$$

Tento text vznikl za podpory SVV-2012-265317.

takže $\mathcal{N}(J) \leq (1+\mathcal{N}(I)^{-1/n})^n H_K$. Umíme zajistit, aby $\mathcal{N}(I)$ byla libovolně velká. Místo I jsme totiž mohli začít s ideálem cI, kde $c \in \mathbb{N}$, potom $\mathcal{N}(cI) = c^n \mathcal{N}(I)$ a přitom $[cI] = [I] = T^{-1}$, protože počítáme modulo hlavní lomené ideály. Takto dostaneme místo ideálu J ideál J_c v $\mathbb{Z}_K$ takový, že $[J_c] = T$ a $\mathcal{N}(J_c)$ je seshora omezena číslem libovolně blízkým k H_K. □

Definice. Řád třídové grupy $\mathcal{C}l_K$ se nazývá *třídové číslo* oboru K a značí se h_K.

Tvrzení 4. *Nechť $\alpha \in K = \mathbb{Q}(\sqrt{m})$, kde $m \in \mathbb{Z}$ je bezčtvercové. Pak $\alpha \in \mathbb{Z}_K$ právě tehdy, když existují $u, v \in \mathbb{Z}$ takové, že $\alpha = \frac{1}{2}(u + v\sqrt{m})$ a $u^2 - mv^2 \equiv 0 \pmod 4$.*

Důkaz. Jestliže $\alpha \in \mathbb{Q}$, pak $u = 2\alpha$ a $v = 0$, a snadno ověříme, že tvrzení platí. Dále tedy předpokládejme, že $\alpha \notin \mathbb{Q}$, potom minimální polynom $m_{\alpha,\mathbb{Q}}$ je stupně 2.

Podle tvrzení III.3.1 [1] je $\alpha \in \mathbb{Z}_K$ právě tehdy, když všechny koeficienty polynomu $m_{\alpha,\mathbb{Q}}$ jsou celočíselné. Podle tvrzení II.5.1 [1], je charakteristický polynom $\lambda^2 - \lambda \operatorname{Tr}_{K|\mathbb{Q}}(\alpha) + \mathrm{N}_{K|\mathbb{Q}}(\alpha)$ prvku α mocninou polynomu $m_{\alpha,\mathbb{Q}}$, a vzhledem k tomu, že tyto polynomy mají stejný stupeň, musejí se rovnat. Odtud vidíme, že $\alpha \in \mathbb{Z}_K$ právě tehdy, když $\operatorname{Tr}_{K|\mathbb{Q}}(\alpha), \mathrm{N}_{K|\mathbb{Q}}(\alpha) \in \mathbb{Z}$.

Nechť $\alpha = \frac{1}{2}(u + v\sqrt{m})$, kde $u, v \in \mathbb{Q}$, pak $\mathrm{N}_{K|\mathbb{Q}}(\alpha) = \left|\begin{smallmatrix} u/2 & mv/2 \\ v/2 & u/2 \end{smallmatrix}\right| = \frac{1}{4}(u^2 - mv^2)$ a $\operatorname{Tr}_{K|\mathbb{Q}}(\alpha) = u$.

Jestliže u a v jsou celá čísla a $u^2 - mv^2$ je dělitelné 4, pak zřejmě $\operatorname{Tr}_{K|\mathbb{Q}}(\alpha)$ i $\mathrm{N}_{K|\mathbb{Q}}(\alpha)$ jsou celá čísla a tedy $\alpha \in \mathbb{Z}_K$.

Obráceně, jestliže $\alpha \in \mathbb{Z}_K$, pak u a $\frac{1}{4}(u^2 - mv^2)$ jsou celá čísla, a tedy $u^2 - mv^2$ je celé číslo dělitelné 4. Odtud vidíme, že i mv^2 je celé. Nechť $v = \frac{p}{q}$, kde $p, q \in \mathbb{Z}$ jsou nesoudělné, pak máme $m\frac{p^2}{q^2} \in \mathbb{Z}$ a vzhledem k tomu, že m je bezčtvercové, q dělí p^2, takže $q = \pm 1$ a v je tedy celé číslo.

□

Důsledek 5. *Nechť $K = \mathbb{Q}(\sqrt{m})$, kde $m \in \mathbb{Z}$ je bezčtvercové. Pro $m \equiv 2, 3 \pmod 4$ je $\mathbb{Z}_K = \mathbb{Z}[\sqrt{m}]$ a $\Delta(\mathbb{Z}_K) = 4m$. Pro $m \equiv 1 \pmod 4$ je $\mathbb{Z}_K = \mathbb{Z}[\frac{1+\sqrt{m}}{2}]$ a $\Delta(\mathbb{Z}_K) = m$.*

Důkaz. Pro libovolné $\alpha \in \mathbb{Z}_K$ existují $u, v \in \mathbb{Z}$ takové, že $\alpha = \frac{1}{2}(u + v\sqrt{m})$ a $u^2 - mv^2 \equiv 0 \pmod 4$.

Pokud $m \equiv 2 \pmod 4$, pak $u^2 + 2v^2 \equiv 0 \pmod 4$ a u i v jsou tedy sudá čísla. Pokud $m \equiv 3 \pmod 4$, pak $u^2 + v^2 \equiv 0 \pmod 4$ a u i v jsou opět sudá čísla. Proto α je celočíselnou kombinací $\{1, \sqrt{m}\}$, což je tedy celistvá báze a $\mathbb{Z}_K = \mathbb{Z}[\sqrt{m}]$. Označme $\{g_1, g_2\} = \operatorname{Hom}_{\mathbb{Q}}(K, \bar{K})$, dejme tomu, že g_2 je neidentický, pak g_2 prohazuje kořeny polynomu $x^2 - m$,

$$\Delta(1, \sqrt{m}) = \det \begin{pmatrix} g_1(1) & g_1(\sqrt{m}) \\ g_2(1) & g_2(\sqrt{m}) \end{pmatrix}^2 = \det \begin{pmatrix} 1 & \sqrt{m} \\ 1 & -\sqrt{m} \end{pmatrix}^2 = 4m.$$

Pokud $m \equiv 1 \pmod 4$, pak $u^2 - v^2 \equiv 0 \pmod 4$ a u i v jsou buď obě sudá nebo obě lichá, tedy $u = v + 2w$, kde $w \in \mathbb{Z}$. Dosazením za u tak dostaneme $\alpha = \frac{1}{2}(v + 2w + v\sqrt{m}) = w + v\frac{1+\sqrt{m}}{2}$, a tedy $\{1, \frac{1+\sqrt{m}}{2}\}$ je celistvá báze.

$$\Delta\left(1, \frac{1+\sqrt{m}}{2}\right) = \det \begin{pmatrix} g_1(1) & g_1(\frac{1+\sqrt{m}}{2}) \\ g_2(1) & g_2(\frac{1+\sqrt{m}}{2}) \end{pmatrix}^2 = \det \begin{pmatrix} 1 & \frac{1+\sqrt{m}}{2} \\ 1 & \frac{1-\sqrt{m}}{2} \end{pmatrix}^2 = m.$$

□

Pozorování 6. Buď K kvadratické těleso a P prvoideál v $\mathbb{Z}_K$, pak existuje prvočíslo p takové, že $P \cap \mathbb{Z} = p\mathbb{Z}$ a podle lemmatu III.6.4 [1] se P vyskytuje v rozkladu $p\mathbb{Z}_K = \prod_{i=1}^k P_i^{e_i}$ na součin kladných mocnin prvoideálů. Podle fundamentální rovnosti $\sum_{i=1}^k e_i f_i = [K : \mathbb{Q}] = 2$, kde $f_i = [\mathbb{Z}_K/P_i : \mathbb{Z}_p]$. Pro každé prvočíslo p tedy nastává jedna z následujících možností:

$$p\mathbb{Z}_K = \begin{cases} P & \text{pokud } k = 1,\ e_1 = 1 \text{ a } f_1 = 2 \text{ (pak } [\mathbb{Z}_K/P : \mathbb{Z}_p] = 2), \\ P^2 & \text{pokud } k = 1,\ e_1 = 2 \text{ a } f_1 = 1 \text{ (pak } \mathbb{Z}_K/P \simeq \mathbb{Z}_p), \\ P\widetilde{P} & \text{pokud } k = 2,\ e_i = f_i = 1 \text{ (pak } \mathbb{Z}_K/P \simeq \mathbb{Z}_p), \text{ kde } \widetilde{P} \neq P \text{ je prvoideál v } \mathbb{Z}_K. \end{cases}$$

Příklad ([2])**.** Ukažte, že třídové číslo $K = \mathbb{Q}(\sqrt{-5})$ je 2.

Řešení. Podle tvrzení 5 je $\mathbb{Z}_K = \mathbb{Z}[\sqrt{-5}]$, takže $\alpha_1 = 1$ a $\alpha_2 = \sqrt{-5}$ tvoří celistvou bázi $\mathbb{Z}_K$, a tedy $H_K = \prod_i \sum_j |g_i(\alpha_j)| = (|1| + |\sqrt{-5}|)(|1| + |-\sqrt{-5}|) = (1+\sqrt{5})^2 \doteq 10{,}5$. Z důkazu věty 3 víme, že pro každou třídu $T \in \mathcal{C}l_K$ existuje ideál I v $\mathbb{Z}_K$ takový, že $T = [I]$ a $\mathcal{N}(I) \leq 10$. Ať $I = \prod_i P_i$ je rozklad ideálu I na prvoideály, pak $\mathcal{N}(I) = \prod_i \mathcal{N}(P_i)$, a tedy $\mathcal{N}(P_i) \leq 10$ pro všechna i. Dále pro každé i existuje prvočíslo p_i takové, že $P_i \cap \mathbb{Z} = p_i\mathbb{Z}$, takže $p_i\mathbb{Z}_K \subseteq P_i$, jinými slovy P_i leží v rozkladu $p_i\mathbb{Z}_K$ na součin prvoideálů. Vidíme, že $\mathcal{N}(P_i) = |\mathbb{Z}_K/P_i| = p_i^k$, pro nějaké $k \in \mathbb{N}$, protože $\mathbb{Z}_K/P_i$ je těleso charakteristiky p_i. Podíváme-li se tedy na rozklady $p\mathbb{Z}_K$ pro $p \in \{2,3,5,7\}$ získáme všechny možné prvoideály v $\mathbb{Z}_K$ modulo hlavní ideály. Vzhledem k tomu, že $(1+\sqrt{-5})(1-\sqrt{-5}) - 2\cdot 2 = 2$, je $\langle 2\rangle \subseteq \langle 2, 1+\sqrt{-5}\rangle\langle 2, 1-\sqrt{-5}\rangle$, takže tento součin ideálů leží v rozkladu $\langle 2\rangle$. Uvážíme-li, že se $\langle 2\rangle$ podle pozorování 6 rozkládá na nejvýše 2 prvoideály, musí se jednat o prvoideály a platí rovnost. Tyto prvoideály jsou navíc totožné, neboť $2 - (1+\sqrt{-5}) = 1 - \sqrt{-5}$. Obdobně postupujeme i v případě ostatních prvočísel a dostáváme tak následující rozklady:

$$\begin{aligned}
\langle 2\rangle &= \langle 2, 1+\sqrt{-5}\rangle\langle 2, 1-\sqrt{-5}\rangle = \langle 2, 1+\sqrt{-5}\rangle^2,\\
\langle 3\rangle &= \langle 3, 1+\sqrt{-5}\rangle\langle 3, 1-\sqrt{-5}\rangle,\\
\langle 7\rangle &= \langle 7, 3+\sqrt{-5}\rangle\langle 7, 3-\sqrt{-5}\rangle,\\
\langle 5\rangle &= \langle \sqrt{-5}\rangle^2.
\end{aligned}$$

Kromě hlavního ideálu $\langle\sqrt{-5}\rangle$ jsou všechny prvoideály, které jsme tímto získali, po dvou ekvivalentní modulo hlavní ideály:

$$\begin{aligned}
\langle 3, 1+\sqrt{-5}\rangle\langle 1-\sqrt{-5}\rangle &= \langle 3\rangle\langle 2, 1-\sqrt{-5}\rangle,\\
\langle 3, 1-\sqrt{-5}\rangle\langle 1+\sqrt{-5}\rangle &= \langle 3\rangle\langle 2, 1+\sqrt{-5}\rangle,\\
\langle 7, 3+\sqrt{-5}\rangle\langle 3-\sqrt{-5}\rangle &= \langle 7\rangle\langle 2, 1-\sqrt{-5}\rangle,\\
\langle 7, 3-\sqrt{-5}\rangle\langle 3+\sqrt{-5}\rangle &= \langle 7\rangle\langle 2, 1+\sqrt{-5}\rangle.
\end{aligned}$$

Grupa $\mathcal{C}l_K$ je tedy generována třídou $[\langle 2, 1+\sqrt{-5}\rangle]$, jejíž řád dělí 2. K tomu, abychom ukázali, že tato třída je řádu 2, zbývá ověřit, že $\langle 2, 1+\sqrt{-5}\rangle$ není hlavní ideál. Předpokládejme, že $\langle 2, 1+\sqrt{-5}\rangle = \langle x+y\sqrt{-5}\rangle$ pro nějaká $x, y \in \mathbb{Z}$, potom $\mathcal{N}(\langle 2, 1+\sqrt{-5}\rangle) = |\mathrm{N}_{K|\mathbb{Q}}(x+y\sqrt{-5})| = |\det(\begin{smallmatrix} x & -5y \\ y & x \end{smallmatrix})| = |x^2+5y^2|$. Dále $\mathcal{N}(\langle 2, 1+\sqrt{-5}\rangle)^2 = \mathcal{N}(\langle 2\rangle) = 4$, takže $\mathcal{N}(\langle 2, 1+\sqrt{-5}\rangle) = 2$, ale $|x^2+5y^2| = 2$ nemá celočíselné řešení.

Příklad ([2])**.** Ukažte, že rovnice $x^2 + 5 = y^3$ nemá celočíselné řešení.

Řešení. Nejdříve si všimněme, že y je liché. Kdyby y bylo sudé, pak by $x^2 + 1 \equiv 0 \pmod 4$, ale takové x neexistuje. Dále si všimněme, že jestliže $d \mid x$ a $d \mid y$, pak $d^2 \mid 5$, a tedy x a y jsou nesoudělné.

V Dedekindově oboru $\mathbb{Z}[\sqrt{-5}]$ máme rozklad $(x+\sqrt{-5})(x-\sqrt{-5}) = y^3$, čili $\langle x+\sqrt{-5}\rangle\langle x-\sqrt{-5}\rangle = \langle y\rangle^3$. Ukážeme, že ideály $\langle x+\sqrt{-5}\rangle$ a $\langle x-\sqrt{-5}\rangle$ neleží ve společném prvoideálu. Postupujeme sporem. Ať oba leží v prvoideálu P, pak $2x = (x+\sqrt{-5}) + (x-\sqrt{-5}) \in P$. Kromě toho vidíme, že $y^3 \in P$, ale y^3 a $2x$ jsou nesoudělné, takže $1 \in P$, což je ve sporu s $P \neq \mathbb{Z}[\sqrt{-5}]$.

Toto nám tedy říká, že rozklady ideálů $\langle x+\sqrt{-5}\rangle$ a $\langle x-\sqrt{-5}\rangle$ na součin prvoideálů mezi sebou nesdílejí žádné prvoideály. Ať $\langle y\rangle^3 = \prod_{i\in S} P_i^{3r_i}$ je rozklad na součin prvoideálů, pak $\langle x+\sqrt{-5}\rangle = \prod_{i\in S_1} P_i^{3r_i}$ a $\langle x-\sqrt{-5}\rangle = \prod_{i\in S_2} P_i^{3r_i}$, kde S je disjunktní sjednocení S_1 a S_2. Máme tedy $\langle x+\sqrt{-5}\rangle = I^3$ pro nějaký ideál I. Podle předchozího příkladu je $h_{\mathbb{Q}(\sqrt{-5})} = 2$, a tak I^2 je hlavní ideál. Jelikož I^3 je hlavní ideál, je i $I = I^3(I^2)^{-1}$ hlavní, a tak existují $a, b \in \mathbb{Z}$ takové, že $I = \langle a+b\sqrt{-5}\rangle$.

Z rovnosti $\langle a+b\sqrt{-5}\rangle^3 = \langle x+\sqrt{-5}\rangle$ plyne, že existuje $u = u_1 + u_2\sqrt{-5} \in \mathbb{Z}[\sqrt{-5}]^*$, kde $u_1, u_2 \in \mathbb{Z}$, takové, že $u(a+b\sqrt{-5})^3 = x+\sqrt{-5}$. Jelikož $u_1^2 + 5u_2^2 = \mathrm{N}_{\mathbb{Q}(\sqrt{-5})|\mathbb{Q}}(u) = \pm 1$, je $u_1 = \pm 1$ a $u_2 = 0$, a tedy $u^3 = \pm 1 = u$. Prvek u se tedy „schová“ do a a b, a můžeme psát $x+\sqrt{-5} = (a+b\sqrt{-5})^3$. To znamená, že $1 = 3a^2b - 5b^3 = b(3a^2 - 5b^2)$, takže $b = \pm 1$, a tak $3a^2 - 5 = \pm 1$, tj. $a^2 \in \{2, \frac{4}{3}\}$, ale takové $a \in \mathbb{Z}$ neexistuje.

Příklad ([2])**.** Nechť $k > 1$ je bezčtvercové celé číslo, které není tvaru $k = 3a^2 \pm 1$, a pro které platí $k \equiv 1, 2 \pmod 4$. Ukažte, že jestliže 3 nedělí třídové číslo tělesa $\mathbb{Q}(\sqrt{-k})$, pak $x^2 + k = y^3$ nemá celočíselné řešení.

Řešení. Postup je stejný jako v předchozím příkladě, podívejme se tedy pouze na hlavní body: Jestliže $d \mid x$ a $d \mid y$, pak $d^2 \mid k$, ale k je bezčtvercové, takže $d = 1$, a tedy x a y jsou nesoudělné. Číslo y je liché. Kdyby totiž y bylo sudé, pak by $x^2 = y^3 - k \equiv -k \equiv 2, 3 \pmod 4$, ale takové x neexistuje. Dále jelikož $-k \equiv 2, 3 \pmod 4$, tak podle tvrzení 5 je $\mathbb{Z}_{\mathbb{Q}(\sqrt{-k})} = \mathbb{Z}[\sqrt{-k}]$. Protože 3 nedělí třídové číslo h tělesa $\mathbb{Q}(\sqrt{-5})$, existují $r, s \in \mathbb{Z}$ takové, že $1 = 3r + hs$. Potom $I = (I^3)^r (I^h)^s \in \mathcal{P}_{\mathbb{Q}(\sqrt{-d})}$, neboť I^3 a I^h jsou hlavní ideály. Vzhledem k tomu, že $k > 1$, dostaneme z $u_1^2 + ku_2^2 = \pm 1$ řešení $u = \pm 1$, a tak opět $u = u^3$. Potom existují $a, b \in \mathbb{Z}$ takové, že $(a + b\sqrt{-k})^3 = x + \sqrt{-k}$. Odtud už snadno dospějeme k tomu, že $k = 3a^2 \pm 1$, což je ve sporu s předpokladem.

Věta 7 (Dirichletova o jednotkách)**.** *Ať K je číselné těleso. Potom $\mathbb{Z}_K^*$ je součinem konečné cyklické grupy $\mu(K)$ a volné abelovské grupy řádu $r+s-1$, kde r značí počet reálných homomorfismů a s počet dvojic komplexně sdružených komplexních homomorfismů v $\mathrm{Hom}_{\mathbb{Q}}(K, \mathbb{C})$.*

Důkaz v kapitole IV.3 [1].

Pozorování 8. Buď $K = \mathbb{Q}(\sqrt{m})$, kde $m \in \mathbb{Z}$ je bezčtvercové. Jestliže $K \subseteq \mathbb{R}$, pak podle Dirichletovy věty o jednotkách je $\mathbb{Z}_K^* \simeq \mathbb{Z} \oplus \mu(K)$, kde $\mu(K) = \{-1, 1\}$. Jestliže $K \not\subseteq \mathbb{R}$, pak $\mathbb{Z}_K^* = \mu(K)$.

Podle tvrzení 4 ve spojení s tvrzením 2 je $\frac{1}{2}(u+v\sqrt{m}) \in \mathbb{Z}_K^*$ právě tehdy, když $u, v \in \mathbb{Z}$ a $u^2 - mv^2 = \pm 4$.

Pro $m = -1$ tak dostaneme podmínku $u^2 + v^2 = 4$, odtud $\mu(K) = \mathbb{Z}_K^* = \{-1, 1, -i, i\}$.
Pro $m = -2$ je $\mu(K) = \mathbb{Z}_K^* = \{-1, 1\}$.
Pro $m = -3$ je $\mu(K) = \mathbb{Z}_K^* = \{-1, 1, \frac{1}{2} + \frac{1}{2}\sqrt{3}, \frac{1}{2} - \frac{1}{2}\sqrt{3}, -\frac{1}{2} + \frac{1}{2}\sqrt{3}, -\frac{1}{2} - \frac{1}{2}\sqrt{3}\}$.
Pro $m < -4$ je $\mu(K) = \mathbb{Z}_K^* = \{-1, 1\}$.

Definice. Buď K reálné kvadratické těleso. Řekneme, že $u \in \mathbb{Z}_K^*$ je *fundamentální jednotka* tělesa K, jestliže $\langle u, -1 \rangle = \mathbb{Z}_K^*$.

Je-li $a \in \mathbb{Z}_K^*$, pak i $a^{-1}, -a, -a^{-1} \in \mathbb{Z}_K$ a do každého z intervalů $(-\infty, -1)$, $(-1, 0)$, $(0, 1)$ a $(1, \infty)$ padne právě jeden z těchto prvků.

Definice. Řekneme, že fundamentální jednotka je *normovaná*, jestliže $u > 1$.

Lemma 9. *Nechť $K = \mathbb{Q}(\sqrt{m})$ a $\alpha = a + b\sqrt{m} \in \mathbb{Z}_K^*$, kde $a, b \in \mathbb{Q}$. Jestliže $\alpha > 1$, pak $a, b > 0$.*

Důkaz. Vzhledem k tomu, že $\alpha^{-1} = \frac{a - b\sqrt{m}}{a^2 - b^2 m}$, kde $a^2 - b^2 m = \mathrm{N}_{K|\mathbb{Q}}(\alpha) \in \{-1, 1\}$, je

$$\{\alpha, \alpha^{-1}, -\alpha, -\alpha^{-1}\} = \{a + b\sqrt{m},\ a - b\sqrt{m},\ -a + b\sqrt{m},\ -a - b\sqrt{m}\}.$$

Jednotka α je z těchto čtyř jednotek největší, proto $a, b > 0$. □

Tvrzení 10. *Jestliže $u = a + b\sqrt{m} > 1$, $a, b \in \mathbb{Q}$, je normovaná fundamentální jednotka tělesa $K = \mathbb{Q}(\sqrt{m})$, pak pro všechny ostatní jednotky $\alpha \in \mathbb{Z}_K^* \setminus \{u\}$, $\alpha = c + d\sqrt{m} > 1$, $c, d \in \mathbb{Q}$, je $a < c$.*

Důkaz. Vzhledem k tomu, že podle tvrzení 4 je $2a \in \mathbb{Z}$ a podle předchozího lemmatu je $a > 0$, můžeme důkaz rozdělit na případy $a = \frac{1}{2}$ a $a \geq 1$.

Předpokládejme, že $a = \frac{1}{2}$. Platí $(\frac{1}{2})^2 - b^2 m = \mathrm{N}_{K|\mathbb{Q}}(u) = \pm 1$, čili $4b^2 m = 1 \pm 4$. Vzhledem k tomu, že $2b \in \mathbb{Z}$, $b > 0$ a uvažujeme $m > 1$, jedinou možností je $m = 5$ a $b = \frac{1}{2}$. Vidíme, že jednotka je těmito vlastnostmi určena jednoznačně, kdyby tedy $c = \frac{1}{2}$, pak $\alpha = u$. Vzhledem k tomu, že $2c \in \mathbb{Z}$, $c > 0$ a $c \neq \frac{1}{2}$, je $c > \frac{1}{2}$.

Předpokládejme, že $a \geq 1$. Všechny ostatní jednotky $c + d\sqrt{m} > 1$ jsou tvaru u^n, kde $n \in \mathbb{N}$. Označme $a_n + b_n\sqrt{m} = u^n$, ukážeme, že $\{a_n\}_{n \in \mathbb{N}}$ je rostoucí posloupnost. Pro každé $n \in \mathbb{N}$ platí $u^{n+1} = u^n u = a_n a + b_n bm + (b_n a + a_n b)\sqrt{m}$, takže $a_{n+1} = a_n a + b_n bm > a_n$, neboť všechny hodnoty v tomto výrazu jsou kladné a $a \geq 1$. □

Příklad. Normovaná fundamentální jednotka tělesa $\mathbb{Q}(\sqrt{2})$ je $1+\sqrt{2}$. Normovaná fundamentální jednotka tělesa $\mathbb{Q}(\sqrt{3})$ je $2+\sqrt{3}$. Normovaná fundamentální jednotka tělesa $\mathbb{Q}(\sqrt{5})$ je $\frac{1}{2}(1+\sqrt{5})$.

Lemma 11. *Nechť $K=\mathbb{Q}(\sqrt{m})$, pak pro každé $\alpha\in\mathbb{Z}_K$ existuje $z\in\mathbb{Z}$ takové, že $\mathrm{N}_{K|\mathbb{Q}}(\alpha)\equiv z^2 \pmod m$.*

Důkaz. Jestliže $m\equiv 2,3 \pmod 4$, pak $\{1,\sqrt{m}\}$ je celistvá báze $\mathbb{Z}_K$, tj. existují $a,b\in\mathbb{Z}$ takové, že $\alpha=a+b\sqrt{m}$. Za z můžeme tedy volit a, neboť $\mathrm{N}_{K|\mathbb{Q}}(\alpha)=a^2-b^2m\equiv a^2 \pmod m$.

Jestliže $m\equiv 1 \pmod 4$, pak $\{1,\frac{1+\sqrt{m}}{2}\}$ je celistvá báze $\mathbb{Z}_K$. Také $\{1,\frac{m+\sqrt{m}}{2}\}$ je celistvá báze $\mathbb{Z}_K$, protože matice přechodu mezi těmito bázemi jsou celočíselné $\left(\begin{smallmatrix}1 & \pm\frac{m-1}{2}\\ 0 & 1\end{smallmatrix}\right)$. Vyjádříme-li $\alpha=a+b\frac{m+\sqrt{m}}{2}$, kde $a,b\in\mathbb{Z}$, pak

$$\mathrm{N}_{K|\mathbb{Q}}(\alpha)=\begin{vmatrix} a & bm\frac{1-m}{4}\\ b & a+bm\end{vmatrix}=a^2+abm-b^2m\frac{1-m}{4}\equiv a^2 \pmod m,$$

neboť $\frac{m+\sqrt{m}}{2}(a+b\frac{m+\sqrt{m}}{2})=a\frac{m+\sqrt{m}}{2}+b\frac{m^2+2m\sqrt{m}+m}{4}=bm\frac{1-m}{4}+(a+bm)\frac{m+\sqrt{m}}{2}$. □

Tvrzení 12. *Nechť $K=\mathbb{Q}(\sqrt{m})$. Jestliže existuje prvočíslo $p\equiv 3 \pmod 4$, které dělí $\Delta(\mathbb{Z}_K)$, pak pro každé $\alpha\in\mathbb{Z}_K^*$ je $\mathrm{N}_{K|\mathbb{Q}}(\alpha)=1$.*

Důkaz. Budeme postupovat sporem. Předpokládejme tedy, že existuje $\alpha\in\mathbb{Z}_K^*$ s normou -1. Podle důsledku 5 je $\Delta(\mathbb{Z}_K)\in\{m,4m\}$, a tedy p dělí m. Podle předchozího lemmatu existuje $z\in\mathbb{Z}$ takové, že $\mathrm{N}_{K|\mathbb{Q}}(\alpha)\equiv z^2 \pmod m$. Takže $-1\equiv z^2 \pmod p$ a tak z je prvek řádu 4 v $\mathbb{Z}_p^*$. To ovšem znamená, že 4 dělí $p-1$, což je ve sporu s předpokladem $p\equiv 3 \pmod 4$. □

Definice. Buď $\sigma: K\to\mathbb{R}$ monomorfismus těles, pro $x\in K$ definujeme *absolutní hodnotu příslušnou* σ jako $|x|_\sigma:=|\sigma(x)|$. Řekneme, že absolutní hodnoty $|\cdot|_{\sigma_1}$ a $|\cdot|_{\sigma_2}$ jsou *ekvivalentní*, jestliže existuje $\beta\in\mathbb{R}^+$ takové, že pro každé $x\in K$ platí $|x|_{\sigma_1}=|x|_{\sigma_2}^\beta$.

Tvrzení 13. *Absolutní hodnoty $|\cdot|_1$ a $|\cdot|_2$ jsou ekvivalentní právě tehdy, když platí inkluze*

$$\{\,x\in K\mid |x|_1>1\,\}\subseteq\{\,x\in K\mid |x|_2>1\,\}.$$

Důkaz. ($\Rightarrow$) Jestliže $|x|_1>1$, pak $|x|_2^\beta>1$ a $|x|_2>1^{1/\beta}=1$.

($\Leftarrow$) Předpokládáme, že pro všechna $x\in K$ platí $|x|_1>1\Rightarrow|x|_2>1$, potom pro všechna $x\in K^*$ platí $|x^{-1}|_1<1\Rightarrow|x^{-1}|_2<1$, a místo x^{-1} můžeme psát x, čili $|x|_1<1\Rightarrow|x|_2<1$.

Zvolme $x\in K$, $|x|_1>1$. Pro každé $y\in K$, $|y|_1>1$, existuje $\alpha\in\mathbb{R}^+$ takové, že $|x|_1^\alpha=|y|_1$. Ukážeme, že $|x|_2^\alpha=|y|_2$. Nechť $\frac{m}{n}>\alpha$, kde $m,n\in\mathbb{Z}^+$, potom z $|y|_1=|x|_1^\alpha<|x|_1^{\frac{m}{n}}$ plyne, že $|y^nx^{-m}|_1<1$, a tak podle předpokladu je $|y^nx^{-m}|_2<1$, a odtud $|y|_2<|x|_2^{\frac{m}{n}}$. Obdobně pro $\frac{m}{n}<\alpha$ získáme $|y|_2>|x|_2^{\frac{m}{n}}$. Limitním přechodem $\frac{m}{n}\to\alpha$ zleva a zprava dostaneme $|x|_2^\alpha\le|y|_2\le|x|_2^\alpha$.

Zvolme $\beta\in\mathbb{R}^+$ takové, že $|x|_1=|x|_2^\beta$. Potom pro libovolné $y\in K$ platí $|y|_1=|x|_1^\alpha=|x|_2^{\alpha\beta}=|y|_2^\beta$. Absolutní hodnoty jsou tedy ekvivalentní. □

Lemma 14. *Nechť g_1 a g_2 jsou dva různé $\mathbb{Q}$-homomorfismy z K do $\mathbb{R}$, pak absolutní hodnoty $|\cdot|_{g_1}$ a $|\cdot|_{g_2}$ nejsou ekvivalentní.*

Důkaz. Zvolme $x\in K$ takové, že $g_1(x)<g_2(x)$. Potom existuje $q\in\mathbb{Q}$ takové, že $0<g_1(x)-q<1<g_2(x)-q$, čili $|x-q|_{g_1}<1<|x-q|_{g_2}$. Odtud vidíme, že neexistuje kladné β takové, že $|x-q|_{g_1}=|x-q|_{g_2}^\beta$. □

Věta 15 (o slabé aproximaci)**.** *Nechť $|\cdot|_1,\dots,|\cdot|_n$ jsou po dvou neekvivalentní absolutní hodnoty, pak pro každé $\varepsilon>0$ a $x_1,\dots,x_n\in K$ existuje $y\in K$ takové, že pro všechna $i=1,\dots,n$ je $|y-x_i|_i<\varepsilon$.*

Důkaz. Nejdříve ukážeme, že existuje $a\in K$ takové, že $|a|_1>1$ a $|a|_i<1$ pro $i=2,\dots,n$. Postupujeme indukcí. Pro dvě absolutní hodnoty toto platí, neboť podle tvrzení 13 jestliže $|\cdot|_1$ a $|\cdot|_1$ nejsou ekvivalentní, pak pro nějaké $a\in K$, $|a|_1>1$, je $|a|_2<1$. Předpokládejme tedy, že to platí pro absolutní

hodnoty $|\cdot|_1, \dots, |\cdot|_{n-1}$, tj. existuje $b \in K$ takové, že $|b|_1 > 1$ a $|b|_i < 1$ pro $i = 2, \dots, n-1$. Zvolme $c \in K$ takové, že $|c|_1 > 1$ a $|c|_n < 1$. Za a zvolíme

$$a = \begin{cases} b & \text{pokud } |b|_n < 1, \\ b^r c & \text{pokud } |b|_n = 1, \\ \frac{b^r}{1+b^r} c & \text{pokud } |b|_n > 1, \end{cases}$$

kde $r \in \mathbb{N}$ je dostatečně velké. To, že takto zvolené a splňuje požadavky lze nahlédnout z chování jednotlivých výrazů pro $r \to \infty$. Konkrétně je-li $|b|_n > 1$, pak $|\frac{b^r}{1+b^r} c|_1 \geq \frac{|b|_1^r}{1+|b|_1^r} |c|_1 \to |c|_1 > 1$, $|\frac{b^r}{1+b^r} c|_i \to \frac{0}{1} |c|_i = 0$, pro $i = 2, \dots, n-1$, a $|\frac{b^r}{1+b^r} c|_n \geq \frac{|b|_n^r}{1+|b|_n^r} |c|_n \to |c|_n < 1$.

Nyní pro každé $j = 1, \dots, n$ zvolme $a_j \in K$ takové, že $|a_j|_j > 1$ a $|a_j|_i < 1$ pro $i \neq j$. Potom pro dostatečně velké r můžeme zvolit $y = \sum_{j=1}^n \frac{a_j^r}{1+a_j^r} x_j$, neboť pro každé $i = 1, \dots, n$ a pro $r \to \infty$

$$|y - x_i|_i \leq |\frac{a_i^r}{1+a_i^r} x_i - x_i|_i + \sum_{\substack{j=1 \\ i \neq j}}^n |\frac{a_j^r}{1+a_j^r} x_j|_i = |\frac{1}{1+a_i^r} x_i|_i + \sum_{\substack{j=1 \\ j \neq i}}^n |\frac{a_j^r}{1+a_j^r} x_j|_i \to 0.$$

□

Důsledek 16. *Zobrazení $\sigma : K^* \to \{-1, 1\}^n$, $\sigma(k) = (\operatorname{sgn} g_1(k), \dots, \operatorname{sgn} g_n(k))$, kde $\{g_1, \dots, g_n\} = \operatorname{Hom}_{\mathbb{Q}}(K, \mathbb{R})$, je epimorfismus grup.*

Důkaz. Pro libovolné $(x_1, \dots, x_n) \in \{-1, 1\}^n$ najdeme vzor v σ: Podle věty o slabé aproximaci existuje $y \in K$ takové, že pro všechna $i = 1, \dots, n$ je $|y - x_i|_{g_i} < \frac{1}{2}$, neboli $|g_i(y) - x_i| < \frac{1}{2}$. Takže $\operatorname{sgn} g_i(y) = x_i$ pro všechna $i = 1, \dots, n$. □

Definice. Řekneme, že $k \in K^*$ je *totálně pozitivní* jestliže $g(k) > 0$ pro všechna $g \in \operatorname{Hom}_{\mathbb{Q}}(K, \mathbb{R})$. Množinu všech totálně pozitivních prvků z K^* značíme K^+. Dále značíme $\mathbb{Z}_K^+ = \mathbb{Z}_K^* \cap K^+$.

Všimněme si, že jádro epimorfismu σ z důsledku 16 je právě K^+. Odtud vidíme, že $K^*/K^+ \simeq \mathbb{Z}_2^n$.

Definice. Řekneme, že hlavní lomený ideál je *totálně pozitivní*, jestliže je tvaru $k\mathbb{Z}_K$, kde $k \in K^+$. Množinu všech totálně pozitivních hlavních lomených ideálů značíme $\mathcal{P}_K^+$ a definujeme $\mathcal{C}l_K^+ = \mathcal{I}_K / \mathcal{P}_K^+$.

Tvrzení 17. *Definujeme-li zobrazení $\pi_K : \mathcal{C}l_K^+ \to \mathcal{C}l_K$ předpisem $\pi_K(I \cdot \mathcal{P}_K^+) = I \cdot \mathcal{P}_K$, pak posloupnost*

$$1 \ \to \ \mathbb{Z}_K^*/\mathbb{Z}_K^+ \ \to \ \mathbb{Z}_2^n \ \to \ \ker \pi_K \ \to \ 1 \tag{1}$$

je exaktní.

Důkaz. Zobrazení $\nu : \mathbb{Z}_K^*/\mathbb{Z}_K^+ \to K^*/K^+$ definované předpisem $\nu(\alpha \mathbb{Z}_K^+) = \alpha K^+$ je monomorfismus, neboť $\ker \nu = (\mathbb{Z}_K^* \cap K^+)/\mathbb{Z}_K^+ = \mathbb{Z}_K^+/\mathbb{Z}_K^+$. Zobrazení $\mu : K^*/K^+ \to \mathcal{P}_K/\mathcal{P}_K^+$ definované předpisem $\mu(\alpha K^+) = \alpha \mathbb{Z}_K \cdot \mathcal{P}_K^+$ je zřejmě epimorfismus. Dále $\operatorname{Im} \nu = \mathbb{Z}_K^*/K^+ = (K^+ \mathbb{Z}_K^*)/K^+ = \ker \mu$. Posloupnost

$$1 \ \to \ \mathbb{Z}_K^*/\mathbb{Z}_K^+ \ \xrightarrow{\nu} \ K^*/K^+ \ \xrightarrow{\mu} \ \mathcal{P}_K/\mathcal{P}_K^+ \ \to \ 1$$

je tedy exaktní. Nyní stačí uvážit, že $\ker \pi_K = \{ I \cdot \mathcal{P}_K^+ \mid I \in \mathcal{P}_K \} = \mathcal{P}_K/\mathcal{P}_K^+$, a dosadit $K^*/K^+ \simeq \mathbb{Z}_2^n$. □

Lemma 18. *Každý prvek jádra π_K je řádu 1 nebo 2 a $|\ker \pi_K|$ dělí 2^{n-1}.*

Důkaz. Z krátké exaktní posloupnosti (1) vidíme, že $\ker \pi_K$ je izomorfní nějakému faktoru $\mathbb{Z}_2^n$, proto každý prvek je řádu 1 nebo 2. Zřejmě $-1 \in \mathbb{Z}_K^*$, ale $-1 \notin \mathbb{Z}_K^+$, takže $\mathbb{Z}_K^*/\mathbb{Z}_K^+$ je řádu alespoň 2, a tedy $|\ker \pi_K|$ dělí 2^{n-1}. □

Tvrzení 19. *Nechť K je reálné kvadratické těleso, pak $|\ker \pi_K| = 1$ právě tehdy, když existuje fundamentální jednotka tělesa K, která má normu -1.*

Důkaz. Podle předchozího lemmatu řád $\ker \pi_K$ dělí 2. Z krátké exaktní posloupnosti (1) vidíme, že $\ker \pi_K$ je triviální právě tehdy, když $\mathbb{Z}_K^*/\mathbb{Z}_K^+ \simeq \mathbb{Z}_2^2$. Toto nastává právě tehdy, když restrikce $\sigma|_{\mathbb{Z}_K^*}$ je epimorfismus grup, kde σ je zobrazení, které jsme zavedli v důsledku 16. Jestliže $\sigma|_{\mathbb{Z}_K^*}$ je na, pak existuje $u \in \mathbb{Z}_K$ takové, že $\sigma(u) = (1,-1)$. Norma $\mathrm{N}_{K|\mathbb{Q}}(u) = g_1(u)g_2(u)$ je záporná, a tedy $\mathrm{N}_{K|\mathbb{Q}}(u) = -1$. Obráceně, existuje-li $u \in \mathbb{Z}_K$ s normou -1, pak $g_1(u)$ a $g_2(u)$ mají opačné znaménko a $\sigma(1)$, $\sigma(-1)$, $\sigma(u)$ a $\sigma(-u)$ jsou po dvou různé. □

Tvrzení 20. *Nechť $K = \mathbb{Q}(\sqrt{m})$, kde $m \in \mathbb{Z}$ je bezčtvercové, g je neidentický $\mathbb{Q}$-automorfismus tělesa K a p je prvočíslo.*

1. *Jestliže $p\mathbb{Z}_K = P$ nebo $p\mathbb{Z}_K = P^2$, kde P je prvoideál v $\mathbb{Z}_K$, pak $g(P) = P$.*
2. *Jestliže $p\mathbb{Z}_K = P\widetilde{P}$, kde $P \neq \widetilde{P}$, pak $g(P) = \widetilde{P}$.*

Důkaz. Vzhledem k tomu, že $g(\mathbb{Z}_K) \subseteq \mathbb{Z}_K$ a $g^2 = \mathrm{id}$, je $g(\mathbb{Z}_K) = \mathbb{Z}_K$. Podle předpokladů je $p\mathbb{Z}_K \subseteq P$, takže $p\mathbb{Z}_K = pg(\mathbb{Z}_K) = g(p\mathbb{Z}_K) \subseteq g(P)$, jinými slovy $g(P)$ leží v rozkladu $p\mathbb{Z}_K$. Tímto je dokázán bod 1. a v případě, že $p\mathbb{Z}_K = P\widetilde{P}$ vidíme, že $g(P) \in \{P, \widetilde{P}\}$.

Dále postupujeme sporem. Předpokládejme, že $g(P^r) = P^r$ a $g(\widetilde{P}^r) = \widetilde{P}^r$, kde $r \in \mathbb{N}$. Automorfismus g oboru $\mathbb{Z}_K$ můžeme přenést na $\mathbb{Z}_K/p^r\mathbb{Z}_K$ a na $\mathbb{Z}_K/P^r \times \mathbb{Z}_K/\widetilde{P}^r$. Podle čínské věty o zbytcích existuje mezi těmito dvěma okruhy izomorfizmus φ.

$$\begin{array}{ccccc} \mathbb{Z}_K & \to & \mathbb{Z}_K/p^r\mathbb{Z}_K & \overset{\varphi}{\to} & \mathbb{Z}_K/P^r \times \mathbb{Z}_K/\widetilde{P}^r \\ \downarrow g & & \downarrow g' & & \downarrow g'' \\ \mathbb{Z}_K & \to & \mathbb{Z}_K/p^r\mathbb{Z}_K & \overset{\varphi}{\to} & \mathbb{Z}_K/P^r \times \mathbb{Z}_K/\widetilde{P}^r \end{array}$$

Jelikož $\widetilde{P}^r + P^r = \mathbb{Z}_K$, existují $e_1 \in \widetilde{P}^r$ a $e_2 \in P^r$ takové, že $e_1 + e_2 = 1$, a platí

$$g''(1+P^r, 0+\widetilde{P}^r) = g''(e_1+P^r, e_1+\widetilde{P}^r) = (g(e_1)+P^r, g(e_1)+\widetilde{P}^r) = (1+P^r, 0+\widetilde{P}^r);$$

využíváme zde zejména toho, že $1-e_1 = e_2 \in P^r$ a $1-g(e_1) = g(1-e_1) = g(e_2) \in g(P^r) = P^r$. Obdobně pro e_2 dostaneme $g''(0+P^r, 1+\widetilde{P}^r) = (0+P^r, 1+\widetilde{P}^r)$, a g'' je tedy identické zobrazení. Potom i $g' = \varphi^{-1} \circ g'' \circ \varphi$ je identické zobrazení, zároveň však $g'(\sqrt{m}+p^r\mathbb{Z}_K) = -\sqrt{m}+p^r\mathbb{Z}_K$, takže $2\sqrt{m} = \sqrt{m} - (-\sqrt{m}) \in p^r\mathbb{Z}_K$. Podle tvrzení 4 tedy existuje $v \in \mathbb{Z}$ takové, že $2 = p^r\frac{1}{2}v$, ale zvolíme-li např. $r = 3$, pak $\frac{4}{p^r} = v \in \mathbb{Z}$ neplatí pro žádné prvočíslo p. □

Definice. Prvoideál $P \subset \mathbb{Z}_K$ nazveme *ramifikovaný*, jestliže $P^2 = (P \cap \mathbb{Z})\mathbb{Z}_K$. Množinu všech ramifikovaných prvoideálů v $\mathbb{Z}_K$ značíme $\mathcal{R}$.

Tvrzení 21. *Buď $I \subset \mathbb{Z}_K$ ideál takový, že $g(I) = I$. Pak existuje $q \in \mathbb{Q}^+$ takové, že qI je součinem po dvou různých ramifikovaných prvoideálů.*

Důkaz. V následujícím značíme P a $\widetilde{P}$ prvoideály, r_P mocninu prvoideálu P v rozkladu ideálu I a $\mathbb{P}$ množinu všech prvočísel. Prvoideály v rozkladu I rozdělíme do tří skupin:

$$I = \prod_{\substack{p\in\mathbb{P} \\ P=p\mathbb{Z}_K}} P^{r_P} \prod_{\substack{p\in\mathbb{P} \\ P^2=p\mathbb{Z}_K}} P^{r_P} \prod_{\substack{p\in\mathbb{P} \\ P\widetilde{P}=p\mathbb{Z}_K}} P^{r_P}\widetilde{P}^{r_{\widetilde{P}}}.$$

Nyní podle tvrzení 20

$$I = g(I) = \prod_{\substack{p\in\mathbb{P} \\ P=p\mathbb{Z}_K}} P^{r_P} \prod_{\substack{p\in\mathbb{P} \\ P^2=p\mathbb{Z}_K}} P^{r_P} \prod_{\substack{p\in\mathbb{P} \\ P\widetilde{P}=p\mathbb{Z}_K}} g(P)^{r_P} g(\widetilde{P})^{r_{\widetilde{P}}} = \prod_{\substack{p\in\mathbb{P} \\ P=p\mathbb{Z}_K}} P^{r_P} \prod_{\substack{p\in\mathbb{P} \\ P^2=p\mathbb{Z}_K}} P^{r_P} \prod_{\substack{p\in\mathbb{P} \\ P\widetilde{P}=p\mathbb{Z}_K}} \widetilde{P}^{r_P} P^{r_{\widetilde{P}}},$$

a tedy $r_P = r_{\widetilde{P}}$ pro všechna $p \in \mathbb{P}$, kde $P\widetilde{P} = p\mathbb{Z}_K$. Z následujícího již plyne platnost tvrzení:

$$I = \prod_{\substack{p\in\mathbb{P} \\ P=p\mathbb{Z}_K}} p^{r_P}\mathbb{Z}_K \prod_{\substack{p\in\mathbb{P} \\ P^2=p\mathbb{Z}_K}} p^{r_P \operatorname{div} 2} P^{r_P \bmod 2} \prod_{\substack{p\in\mathbb{P} \\ P\widetilde{P}=p\mathbb{Z}_K}} p^{r_P}\mathbb{Z}_K = q^{-1} \prod_{\substack{p\in\mathbb{P} \\ P^2=p\mathbb{Z}_K}} P^{r_P \bmod 2}.$$

□

Věta 22. *Nechť A je algebra nad perfektním tělesem F, která je konečně generovaná jako vektorový prostor nad F. Pak následující jsou ekvivalentní:*

(1) $\mathrm{Rad}(A) = \{\, a \in A \mid a^n = 0$ *pro nějaké* $n \in \mathbb{N} \,\} = \{0\}$*, tj. A neobsahuje nilpotentní prvky.*
(2) *A je izomorfní součinu těles.*
(3) *Existuje báze A nad F, která má nenulový diskriminant.*
(4) *Každá báze A nad F má nenulový diskriminant.*

Důkaz. (1 $\Rightarrow$ 2) Nechť $A = \prod_i A_i$, kde A_i jsou nerozložitelné jakožto okruhy. Ukážeme, že každé A_i je těleso. Nechť $a \in A_i \setminus \{0\}$, najdeme inverzní prvek k a. Pro každé $n \in \mathbb{N}$ platí $a^n A_i \subseteq a^{n+1} A_i$, a tak $\dim_F a^n A_i \leq \dim_F a^{n+1} A_i$. Vzhledem k tomu, že A má konečnou dimenzi nad F, existuje $n \in \mathbb{N}$ takové, že $\dim_F a^n A_i = \dim_F a^{n+1} A_i$, potom ovšem $a^n A_i = a^{n+1} A_i$, a také $a^n A_i = a^{2n} A_i$. Existuje tedy $b \in A_i$ takové, že $a^n = a^{2n} b$. Potom $a^n b = a^{2n} b^2 = (a^n b)^2$, čili $a^n b$ je idempotentní prvek, a vzhledem k tomu, že A_i je nerozložitelné, je $a^n b \in \{0, 1\}$. Kdyby však platilo $a^n b = 0$, pak $a^n = a^{2n} b = 0 \cdot a^n = 0$, tj. a by musel být nilpotentní prvek, což je ve sporu s předpokladem $\mathrm{Rad}(A) = \{0\}$. Zbývá tedy jedině možnost $a^n b = 1$, a tak $a^{-1} = a^{n-1} b$.

(2 $\Rightarrow$ 3) Nechť tedy $A \simeq \prod_i F_i$, kde F_i jsou tělesa. Pro $x \in F_i$ Označme $\widetilde{x}$ ten prvek A, který se zobrazuje na $(0, \ldots, 0, \overset{i}{x}, 0, \ldots, 0)$. Pro $x \in F_i$ a $y \in F_j$, kde $i \neq j$, je $\widetilde{x}\widetilde{y} = 0$, neboť násobení v $\prod_i F_i$ probíhá po složkách. Pro každé i označme B_i nějakou bázi F_i nad F, potom $\{a_1, \ldots, a_n\} = \{\, \widetilde{b} \mid b \in \bigcup_i B_i \,\}$ je báze A nad F. Matice $(\mathrm{Tr}(a_i a_j))$ je diagonální bloková, a její determinant je tedy roven součinu determinantů jednotlivých bloků. Odtud $\Delta(a_1, \ldots, a_n) = \prod_i \Delta(B_i) \neq 0$.

(3 $\Rightarrow$ 4) Označme $\{u_1, \ldots, u_n\}$ bázi A nad F, která má nenulový diskriminant. Pro libovolnou bázi $\{v_1, \ldots, v_n\}$ vektorového prostoru A nad F má matice přechodu $(p_{ij}) \in F^{n \times n}$, definovaná vztahem $u_i = \sum p_{ij} v_j$, nenulový determinant a platí $\Delta(u_1, \ldots, u_n) = \det(p_{ij})^2 \Delta(v_1, \ldots, v_n) \neq 0$.

(4 $\Rightarrow$ 1) Budeme postupovat sporem. Předpokládejme, že existuje nenulový nilpotentní prvek $a_1 \in A$, a doplňme jej na bázi $\{a_1, \ldots, a_n\}$ prostoru A nad F. Potom pro každé i je $a_1 a_i$ nilpotentní, a tedy $\mathrm{Tr}(a_1 a_i) = 0$. Matice $(\mathrm{Tr}(a_i a_j))$ obsahuje nulový řádek, a tak $\Delta(a_1, \ldots, a_n) = \det(\mathrm{Tr}(a_i a_j)) = 0$. □

Věta 23. *Nechť $\mathbb{Q} \subseteq K$ je rozšíření konečného stupně a p je prvočíslo. Pak p se větví (tj. $p\mathbb{Z}_K = \prod_i P_i^{r_i}$, kde $r_i > 1$ pro nějaké i) právě tehdy, když p dělí $\Delta(\mathbb{Z}_K)$.*

Důkaz. Mějme rozklad $p\mathbb{Z}_K = \prod_i P_i^{r_i}$ na součin prvoideálů, pak podle čínské věty o zbytcích $\mathbb{Z}_K / p\mathbb{Z}_K \simeq \prod_i \mathbb{Z}_K / P_i^{r_i}$. Odtud plyne, že p se nevětví (tj. $r_i = 1$ pro všechna i) právě tehdy, když $\mathbb{Z}_K / p\mathbb{Z}_K$ je součinem těles. To podle předchozí věty nastává právě tehdy, když diskriminant každé báze (resp. libovolné báze) $\mathbb{Z}_K / p\mathbb{Z}_K$ nad $\mathbb{Z}_p$ je nenulový. Nechť $\{\alpha_1, \ldots, \alpha_n\}$ je celistvá báze $\mathbb{Z}_K$, pak $\{\alpha_1 + p\mathbb{Z}_K, \ldots, \alpha_n + p\mathbb{Z}_K\}$ je báze $\mathbb{Z}_K / p\mathbb{Z}_K$ a $\Delta(\mathbb{Z}_K) = \Delta(\alpha_1, \ldots, \alpha_n) \equiv \Delta(\alpha_1 + p\mathbb{Z}_K, \ldots, \alpha_n + p\mathbb{Z}_K) \pmod{p}$. Čili $\Delta(\mathbb{Z}_K) \not\equiv 0 \pmod{p}$ právě tehdy, když se p nevětví. □

Lemma 24. *Nechť $K = \mathbb{Q}(\sqrt{m})$, d je bezčtvercové a g je neidentický $\mathbb{Q}$-automorfismus tělesa K. Pak pro každé $a \in K$, $\mathrm{N}_{K|Q}(a) = 1$, existuje $b \in K$ takové, že $a = \frac{g(b)}{b}$. Je-li navíc $a \in K^+$, pak lze volit $b \in K^+$.*

Důkaz. Jestliže $a = -1$, zvolíme $b = \sqrt{m}$. Potom $\frac{g(b)}{b} = \frac{g(\sqrt{m})}{\sqrt{m}} = \frac{-\sqrt{m}}{\sqrt{m}} = -1 = a$.

Jestliže $a \neq -1$, zvolíme $b = (1 + a)^{-1}$. Potom $\frac{g(b)}{b} = \frac{1+a}{1+g(a)} = \frac{a(1+a)}{a+ag(a)} = \frac{a(1+a)}{a+1} = a$, neboť $ag(a) = \mathrm{N}_{K|Q}(a) = 1$. Pokud $a \in K^+$, pak i $(1 + a)^{-1} \in K^+$. □

Věta 25. *Označme $S = \{\, \prod_i P_i^{r_i} \mid P_i \in \mathcal{R}, r_i \in \mathbb{Z} \,\}$ a $\nu : S \to \mathcal{C}l_K^+$, $\nu(I) = [I]$. Pak*

(1) *$\mathrm{Im}\,\nu = (\mathcal{C}l_K^+)_2$, kde $(\mathcal{C}l_K^+)_2$ je množina prvků z $\mathcal{C}l_K^+$ řádu 1 nebo 2,*
(2) *$S^2 \subseteq \ker \nu$ a $[\ker \nu : S^2] = 2$.*

Podle věty 23 je $|\mathcal{R}|$ rovno počtu prvočísel, která dělí $\Delta(\mathbb{Z}_K)$. Označíme-li tento počet k, pak $S/S^2 \simeq \mathbb{Z}_2^k$. Podle věty 25 je $\nu' : S/S^2 \to (\mathcal{C}l_K^+)_2$ epimorfismus, který má jádro řádu 2, a tedy $(\mathcal{C}l_K^+)_2 \simeq \mathbb{Z}_2^{k-1}$. Z tvrzení 19 tak získáme následující důsledek.

Důsledek 26. *Nechť K je kvadratické těleso.*

(1) *Je-li* $K \not\subseteq \mathbb{R}$ *anebo je-li* $K \subset \mathbb{R}$ *takové, že existuje fundamentální jednotka tělesa* K *s normou* -1*, pak* $(\mathcal{C}l_K)_2$ *je grupa řádu* 2^{k-1}*.*
(2) *Je-li* $K \subseteq \mathbb{R}$ *takové, že každá fundamentální jednotka tělesa* K *má normu* 1*, pak* $(\mathcal{C}l_K)_2$ *je řádu* 2^{k-2}*.*

Důsledek 27. *Jestliže* K *je kvadratické těleso a* $\Delta(\mathbb{Z}_K)$ *je dělitelné pouze jedním prvočíslem, pak* $|\mathcal{C}l_K|$ *je liché číslo. Jestliže* K *je navíc reálné, pak existuje fundamentální jednotka tělesa* K *s normou* -1*.*

Reference

[1] Drápal, A. *Komutativní okruhy.* Praha, 2006. Dostupné z: `http://www.karlin.mff.cuni.cz/~drapal/komalg.ps`
[2] Esmonde, J. a Murty M. R. *Problems in algebraic number theory.* New York: Springer, 1999, xiv, 314 s. ISBN 0-387-98617-0.
[3] Fröhlich, A. a Taylor, M. J. *Algebraic number theory.* Cambridge: Cambridge University Press, 1991, xiv, 355 s. ISBN 0-521-36664-X.

Matematicko-fyzikální fakulta, Univerzita Karlova v Praze, Sokolovská 83, 186 75 Praha 8