1. Úvod

Tato práce je věnována studiu počtu tříd divizorů (tento počet bývá standardně označován jako h) tělesa $\mathbb{Q}\left(\sqrt{p}, \sqrt{q}, \sqrt{r}\right)$, vzniklého rozšířením tělesa $\mathbb{Q}$ o odmocniny ze tří prvočísel $p, q, r \equiv 1 \pmod 4$ (takové těleso se nazývá *kompozitum kvadratických těles*). Navazuje na práci [4], ve které je zkoumáno bikvadratické těleso $\mathbb{Q}\left(\sqrt{p}, \sqrt{q}\right)$, kde rovněž $p, q \equiv 1 \pmod 4$. Speciálně se nám jedná o paritu počtu tříd divizorů, případně o zjištění vyšší mocniny čísla 2, která dělí h.

Označení

V celé práci budeme používat následujícího označení: $\zeta_n = e^{2\pi i/n}$ znamená n-tou odmocninu z jedné, $\xi_n = \zeta_n^{(n+1)/2}$ pro n liché je jedna z druhých odmocnin z ζ_n. Dalším běžně používaným pojmem je Legendreův symbol $\left(\frac{a}{b}\right)$, který určuje, zda je a kvadratickým zbytkem modulo b (pak je Legendreův symbol roven 1) nebo kvadratickým nezbytkem (pak je roven -1). Symbolem $[a]$ označujeme celou část reálného čísla a, symbolem $\langle a\rangle$ pak část necelou.

Rovněž budeme používat tzv. exponenciálního zápisu homomorfismů, tj. místo standardního $\sigma(a)$ budeme psát a^σ. Tento zápis má některé výhody, které budou při výpočtech užitečné.

Další označení, která zavedeme v tomto odstavci, se budou vztahovat k libovolnému prvočíslu $l \equiv 1 \pmod 4$. Zvolme tedy pro účely tohoto označení takové l pevně a nechť b_l, c_l jsou přirozená čísla splňující $l - 1 = 2^{b_l} c_l$, kde $b_l \geqslant 2$ a $2 \nmid c_l$. Zvolme pevně Dirichletův charakter ψ_l modulo l řádu 2^{b_l} a položme $R_l = \left\{\rho_l^j \;\middle|\; 0 \leqslant j < 2^{b_l-2}\right\}$ a $R_l' = \zeta_{2^{b_l}} R_l$, kde $\rho_l = e^{4\pi i c_l/(l-1)}$ $(= \zeta_{2^{b_l-1}})$ je primitivní 2^{b_l-1}-tá odmocnina z jedné. Pro počet prvků obou takto definovaných množin zřejmě platí $\#R_l = \#R_l' = (l-1)/(4c_l)$. Dále buď χ_l některý pevně zvolený charakter řádu 4 modulo l. Je-li nyní a přirozené číslo splňující $\left(\frac{a}{l}\right) = 1$, pak je $\chi_l(a)$ určeno jednoznačně již čísly a a l a nezávisí na volbě konkrétního charakteru. To plyne například z následujícího Lemmatu:

Lemma 1.1. *Nechť $\left(\frac{a}{l}\right) = 1$ a nechť $u \in \mathbb{Z}$ je takové, že $u^2 \equiv a \pmod l$. Pak $\chi_l(a) = \left(\frac{u}{l}\right)$.*

Důkaz. Z vlastností charakterů zřejmě plyne

$$\chi_l(a) = \chi_l(u^2) = \chi_l^2(u) = \left(\frac{u}{l}\right),$$

protože χ_l^2 je charakter řádu 2 modulo l a ten je určen jednoznačně (je jím Legendreův symbol modulo l). ◻

Předpoklady

Od tohoto místa zafixujme pevně tři různá prvočísla $p, q, r \equiv 1 \pmod 4$ a jako ψ označme pevně zvolený Dirichletův charakter ψ_p. Podobně klademe $R := R_p$ a $R' := R_p'$. Definujme ještě $M = \left\{ a \in \mathbb{Z} \;\middle|\; 0 < a < pqr, \left(\frac{a}{q}\right) = \left(\frac{a}{r}\right) = 1, \psi(a) \in R \right\}$. Pro počet prvků této množiny platí podle Čínské zbytkové věty $\#M = \frac{p-1}{4}\frac{q-1}{2}\frac{r-1}{2}$, speciálně je tedy $2 \mid \#M$.

Vztah počtu tříd divizorů a grupy jednotek

Cílem této kapitoly je ozřejmit souvislost mezi počtem tříd divizorů kompozita kvadratických těles a vlastnostmi grupy jednotek tohoto tělesa. Buď $J = \{l \in \mathbb{N} \,|\, l \text{ prvočíslo}, l \equiv 1 \pmod 4\}$, potom pro libovolnou konečnou množinu $S \subseteq J$ definujeme (zde i dále klademe součin přes prázdnou množinu roven jedné)

$$n_S = \prod_{l \in S} l, \quad \zeta_S = e^{2\pi i/n_S}, \quad \mathbb{Q}^S = \mathbb{Q}(\zeta_S), \quad K_S = \mathbb{Q}\left(\{\sqrt{l} \,|\, l \in S\}\right).$$

V následující definici zavedeme základní (tzv. *kruhové*) jednotky, se kterými budeme pracovat ($\mathrm{N}_{K/k}(\alpha)$ znamená *normu* prvku α v rozšíření K/k).

Definice 1.1.

$$\varepsilon_{n_S} = \begin{cases} 1 & \text{je-li } S = \emptyset, \\ \frac{1}{\sqrt{l}} \mathrm{N}_{\mathbb{Q}^S/K_S}(1 - \zeta_S) & \text{je-li } S = \{l\}, \\ \mathrm{N}_{\mathbb{Q}^S/K_S}(1 - \zeta_S) & \text{je-li } \#S > 1. \end{cases}$$

Není těžké ukázat, že pro libovolnou konečnou podmnožinu $S \subseteq J$ je ε_{n_S} jednotka tělesa K_S. Platí dokonce (viz [5, Theorem 1.]), že $\{\varepsilon_{n_S} \,|\, \emptyset \neq T \subseteq S\} \cup \{-1\}$ tvoří bázi tzv. *podgrupy kruhových jednotek* tělesa K_S. V našem případě tedy jednotky $\varepsilon_p, \varepsilon_q, \varepsilon_r, \varepsilon_{pq}, \varepsilon_{pr}, \varepsilon_{qr}$ a ε_{pqr} spolu s -1 tvoří bázi podgrupy kruhových jednotek (v dalším ji značíme C) grupy jednotek E tělesa $\mathbb{Q}\left(\sqrt{p}, \sqrt{q}, \sqrt{r}\right)$.

Dalším důležitým pojmem, který budeme využívat, je tzv. *Frobeniův automorfismus* pro prvočíslo l. Ten je definován následovně: je-li $\mathbb{Q}(\zeta_f)$ nejmenší kruhové těleso, obsahující dané abelovské těleso K, pak pro $a \in \mathbb{Z}, (a, f) = 1$ označíme jako τ_a automorfismus tělesa $\mathbb{Q}(\zeta_f)$, který prvku ζ_f přiřadí ζ_f^a. Pokud je nyní l prvočíslo, $l \nmid f$, pak τ_l nazveme Frobeniovým automorfismem pro prvočíslo l v $\mathbb{Q}(\zeta_f)/\mathbb{Q}$. *Frobeniovým automorfismem pro l v $K/\mathbb{Q}$* pak nazveme restrikci τ_l na těleso K a značíme $\mathrm{Frob}(l, K)$. V dalším textu budeme pro $l \in S$ jako σ_l označovat neidentický prvek grupy $\mathrm{Gal}\left(K_S/K_{S\setminus\{l\}}\right)$. Tento automorfismus speciálně prvku $\sqrt{l}$ tělesa K_S přiřadí prvek $-\sqrt{l}$. V případě $\left(\frac{p_1}{p_2}\right) = 1$ je $\mathrm{Frob}(p_1, \mathbb{Q}\left(\sqrt{p_2}\right)) = 1$, zatímco v případě $\left(\frac{p_1}{p_2}\right) = -1$ je $\mathrm{Frob}(p_1, \mathbb{Q}\left(\sqrt{p_2}\right)) = \sigma_{p_2}$. Je tedy vidět, že prvky grupy $\mathrm{Gal}\left(\mathbb{Q}(\zeta_l)/\mathbb{Q}\left(\sqrt{l}\right)\right)$ jsou automorfismy τ_a z $\mathrm{Gal}\left(\mathbb{Q}(\zeta_l)/\mathbb{Q}\right)$ pro ta čísla a, pro která platí $\left(\frac{a}{l}\right) = 1$.

Následující lemma převzaté z [5] nám objasní, jak působí prvky grupy $\mathrm{Gal}\left(K_S/K_{S\setminus\{l\}}\right)$ na jednotky, definované v Definici 1.1.

Lemma 1.2. *Buď $S \subseteq J$ konečná a $l \in S$. Potom*

$$\mathrm{N}_{K_S/K_{S\setminus\{l\}}}(\varepsilon_{n_S}) = \begin{cases} -1 & \text{je-li } S = \{l\}, \\ \left(\frac{l}{k}\right) \cdot \varepsilon_k^{1-\mathrm{Frob}(l, K_{\{k\}})} & \text{je-li } S = \{l, k\}, l \neq k, \\ \varepsilon_{n_{S\setminus\{l\}}}^{1-\mathrm{Frob}(l, K_{S\setminus\{l\}})} & \text{je-li } \#S > 2. \end{cases}$$

Pro index $[E : C]$ podgrupy C v E platí následující tvrzení, plynoucí z tvrzení dokázaného rovněž v [5, Theorem1.]:

Tvrzení 1.1. $[E : C] = 2^4 \cdot h$

Z tohoto tvrzení tedy plyne, že pokud najdeme podgrupu E „dostatečně malého" indexu, budeme schopni diskutovat hodnotu počtu tříd divizorů h. Konkrétní postup bude následující: budeme hledat jednotky η z podgrupy C_1 zatím nejmenšího známého indexu vůči E, které se dají v E odmocnit, tj. pro které existuje v $E \setminus C_1$ jednotka η_1 taková, že

$\eta = \eta_1^2$. Jednotku η_1 pak přidáme ke generátorům podgrupy C_1 a získáme tak novou podgrupu grupy E polovičního indexu. V některých případech bude možné takovou jednotku najít i pro podgrupu C_1 indexu h, pak budeme schopni tvrdit, že h je sudé.

Z výsledků 3. kapitoly v [4] plyne, že takovými jednotkami jsou v tělese $\mathbb{Q}\left(\sqrt{p}, \sqrt{q}, \sqrt{r}\right)$ zejména $\varepsilon_{pq}, \varepsilon_{pr}, \varepsilon_{qr}$. Pro ně vždy existují jednotky (značíme $\beta_{pq}, \beta_{pr}, \beta_{qr}$), které jsou jejich odmocninami. Jednotka β_{pq} je přitom definována jako

$$\beta_{pq} = \prod_{a \in M_{pq}} (\xi^a - \xi^{-a}), \tag{1}$$

kde $M_{pq} = \{a \in \mathbb{Z} \mid 0 < a < pq, \left(\frac{a}{q}\right) = 1, \psi(a) \in R\}$ a jednotky β_{pr} a β_{qr} jsou definovány analogicky.

Poznámka: Je vidět, že definice množiny M_{pq} není symetrická vzhledem k p a q. Dále je možné si povšimnout, že tato definice závisí na zvoleném Dirichletově charakteru ψ. Ani jeden z těchto problémů však není podstatný, protože případná jiná volba charakteru, resp. opačně vzaté pořadí čísel p a q při definici M_{pq}, ovlivní pouze znaménko β_{pq}. V dalších výpočtech však toto znaménko nebudeme zkoumat a ve výpočtech, kde bude důležité zjišťování znaménka některého výrazu, nebude znaménko β_{pq} důležité. Stejná poznámka se pak týká i množiny M a v příštím odstavci definované jednotky β_{pqr}.

Podobnými prostředky jako v článku [4] ukážeme, že generátorem, který lze v E odmocnit, je i jednotka ε_{pqr}.

Protože pro každé $a \in Z$, splňující $0 < a < pqr$ a $\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right) = \left(\frac{a}{r}\right) = 1$ platí buď $a \in M$ nebo $pqr - a \in M$, máme

$$\begin{aligned}\varepsilon_{pqr} &= \prod_{\substack{0<a<pqr \\ \left(\frac{a}{p}\right)=\left(\frac{a}{q}\right)=\left(\frac{a}{r}\right)=1}} (1 - \zeta_{pqr}^a) = \prod_{a \in M} (1 - \zeta_{pqr}^a)(1 - \zeta_{pqr}^{-a}) = \\ &= \prod_{a \in M} (1 - \xi_{pqr}^{2a})(1 - \xi_{pqr}^{-2a}) = \prod_{a \in M} (\xi_{pqr}^{-a} - \xi_{pqr}^a)(\xi_{pqr}^a - \xi_{pqr}^{-a}),\end{aligned}$$

kde $\xi_{pqr} = \zeta_{pqr}^{(1+pqr)/2}$. Protože $2 \mid \#M$, můžeme psát $\varepsilon_{pqr} = \beta_{pqr}^2$, kde

$$\beta_{pqr} = \prod_{a \in M} (\xi_{pqr}^a - \xi_{pqr}^{-a}). \tag{2}$$

Nyní musíme dokázat, že $\beta_{pqr} \in \mathbb{Q}\left(\sqrt{p}, \sqrt{q}, \sqrt{r}\right)$. Ukážeme, že pro libovolný automorfismus σ tělesa $\mathbb{Q}(\zeta_{pqr})$, který nechává na místě prvky tělesa $\mathbb{Q}\left(\sqrt{p}, \sqrt{q}, \sqrt{r}\right)$ platí $\beta_{pqr}^\sigma = \beta_{pqr}$. Uvažujme tedy libovolný automorfismus $\sigma \in \mathrm{Gal}\left(\mathbb{Q}(\zeta_{pqr}) / \mathbb{Q}\left(\sqrt{p}, \sqrt{q}, \sqrt{r}\right)\right)$. Znamená to, že $\sigma = \sigma_k$ pro vhodné k, kde $\left(\frac{k}{p}\right) = \left(\frac{k}{q}\right) = \left(\frac{k}{r}\right) = 1$ a $\sigma_k(\zeta_{pqr}) = \zeta_{pqr}^k$. Ukážeme, že $\beta_{pqr}^\sigma = \beta_{pqr}$.

$$\beta_{pqr}^\sigma = \beta_{pqr}^{\sigma_k} = \prod_{a \in M} (\xi_{pqr}^{ak} - \xi_{pqr}^{-ak}) = \beta_{pqr} \cdot (-1)^{\#\{\, a \in M \mid \psi(ak) \notin R \,\}},$$

zbývá tedy dokázat, že počet prvků množiny $\{\, a \in M \mid \psi(ak) \notin R \,\}$ je sudý. K tomu si ale stačí povšimnout následujícího. Pro $d \in M$ je zřejmě číslo $\#\{\, a \in M \mid \psi(a) = \psi(d) \,\} = \frac{q-1}{2} \frac{r-1}{2} c$ sudé (dokonce je dělitelné 4), tedy i číslo $\#\{\, a \in M \mid \psi(ak) = \psi(dk) \,\}$ je sudé. Je tedy $\beta_{pqr}^\sigma = \beta_{pqr}$, což znamená, že $\beta_{pqr} \in \mathbb{Q}\left(\sqrt{p}, \sqrt{q}, \sqrt{r}\right)$.

V předchozím odstavci jsme nalezli $\beta_{pqr} \in \mathbb{Q}\left(\sqrt{p}, \sqrt{q}, \sqrt{r}\right)$, pro které platí

$$\beta_{pqr}^2 = \varepsilon_{pqr}. \tag{3}$$

Našli jsme tedy podgrupu C_1 grupy jednotek E (s bází $-1, \varepsilon_p, \varepsilon_q, \varepsilon_r, \beta_{pq}, \beta_{pr}, \beta_{qr}, \beta_{pqr}$), která má index h. Pokud se nám v další části podaří najít podgrupu s menším indexem, poskytne nám to již informaci o počtu tříd divizorů tělesa $\mathbb{Q}\left(\sqrt{p}, \sqrt{q}, \sqrt{r}\right)$. To bude také cílem zbývajících částí této práce. Je zřejmé, že stačí hledat jednotku, kterou lze odmocnit, pouze mezi jednotkami tvaru

$$\eta = \pm\varepsilon_p^{x_p}\varepsilon_q^{x_q}\varepsilon_r^{x_r}\beta_{pq}^{x_{pq}}\beta_{pr}^{x_{pr}}\beta_{qr}^{x_{qr}}\beta_{pqr}^{x_{pqr}},$$

kde $x_p, x_q, x_r, x_{pq}, x_{pr}, x_{qr}, x_{pqr} \in \{0,1\}$. Každou jednotku z C_1 lze totiž (jednoznačně) zapsat ve tvaru součinu jednotky uvedeného tvaru a druhé mocniny vhodné jednotky z C_1.

2. Pomocné výpočty

V této kapitole provedeme některé výpočty užitečné ke zjišťování toho, zda je jednotka η kvadrátem v E. Nutnou podmínkou toho, aby η byla druhou mocninou v E, je, že i její norma vzhledem k libovolnému podtělesu k tělesa $\mathbb{Q}\left(\sqrt{p}, \sqrt{q}, \sqrt{r}\right)$ je v tělese k druhou mocninou. Pro formulaci podmínky postačující je nutné definovat pojem *křížového homomorfismu.* Tento pojem a následující tvrzení s ním spjatá jsou odvozena pro obecné kompozitum K_S, kde $S \subseteq J$ konečná, použita pak budou později pro konkrétní těleso $\mathbb{Q}\left(\sqrt{p}, \sqrt{q}, \sqrt{r}\right)$.

Definice 2.1. *Označme $G := \mathrm{Gal}\,(K_S/\mathbb{Q})$. Funkce $f : G \to K_S$ se nazývá* ***křížový homomorfismus****, jestliže pro všechny $\sigma, \tau \in G$ platí*

$$f(\sigma\tau) = f(\sigma)f(\tau)^\sigma.$$

Následující tvrzení, uvedené v [5, Proposition 2.], ukazuje postačující podmínku k tomu, aby jednotka $\varepsilon \in E$ byla v E druhou mocninou.

Tvrzení 2.1. *Buď $\varepsilon \in E$ taková, že existuje funkce $f : G \to K_S$, splňující $\varepsilon^{1-\sigma} = f(\sigma)^2$ pro libovolné $\sigma \in G$, která je křížovým homomorfismem. Potom ε nebo $-\varepsilon$ je druhou mocninou v K_S.*

Důkaz. Důkaz je proveden v 5.kapitole článku [5] □

Obráceně se snadno ukáže, že pokud je $\pm\varepsilon$ druhou mocninou v K_S, takové f vždy existuje. Je-li totiž $\varepsilon = \pm\eta^2$ pro vhodné $\eta \in E$, stačí pro všechna $\sigma \in G$ položit $f(\sigma) = \eta^{1-\sigma}$. Potom pro libovolná $\sigma, \tau \in G$ platí

$$f(\sigma\tau) = \eta^{1-\sigma\tau} = \eta^{1-\sigma} \cdot (\eta^{1-\tau})^\sigma = f(\sigma)f(\tau)^\sigma$$

a f je tedy hledaným křížovým homomorfismem.

Protože to, jestli je funkce f křížovým homomorfismem, by se podle definice zjišťovalo dosti složitě, uvedeme nyní kritérium, které tuto proceduru zjednoduší. Uvědomme si přitom, že na grupu $G = \mathrm{Gal}\,(K_S/\mathbb{Q})$ se můžeme dívat jako na vektorový prostor nad dvouprvkovým tělesem $\mathbb{F}_2$ s bází $\{\sigma_l \,|\, l \in S\}$.

Tvrzení 2.2. *Nechť funkce $g : \{\sigma_l \,|\, l \in S\} \to K_S$ splňuje podmínky*

$$\forall l \in S: \qquad g(\sigma_l)^{1+\sigma_l} = 1 \tag{4}$$

$$\forall p_1, p_2 \in S: \qquad g(\sigma_{p_1})^{1-\sigma_{p_2}} = g(\sigma_{p_2})^{1-\sigma_{p_1}} \tag{5}$$

Pro libovolné přirozené číslo t označme $S_t = \{k \in S \,|\, k < t\}$. Definujeme-li funkci $f : G \to K_S^\times$ tak, že pro libovolné $V \subseteq S$ položíme

$$f\Big(\prod_{s\in V}\sigma_s\Big) = \prod_{s\in V} g(\sigma_s)^{\prod\limits_{k\in V\cap S_s}\sigma_k},$$

pak f je křížový homomorfismus, tj. pro libovolné $\sigma, \tau \in G$ platí

$$f(\sigma\tau) = f(\sigma)f(\tau)^{\sigma}.$$

Poznámky:

1) Zřejmě platí $f|_{\{\sigma_l \mid l \in S\}} = g$.
2) Snadno je vidět, že pokud existuje funkce g, mající požadované vlastnosti (4),(5), požadované vlastnosti splňuje i libovolná funkce g_1, lišící se od g pouze znaménkem funkční hodnoty v některém z σ_s, kde $s \in S$.

Tvrzení dokážeme pomocí následujících lemmat.

Lemma 2.1. *Splňuje-li g podmínky Tvrzení 2.2 a f je definována týmž předpisem jako v Tvrzení 2.2, pak pro libovolný automorfismus $\tau \in G$ a prvočíslo $l \in S$ platí*

$$f(\tau)^{1-\sigma_l} = f(\sigma_l)^{1-\tau}$$

Důkaz lemmatu: Buď $T \subseteq S$ taková množina, že $\tau = \prod_{t \in T} \sigma_t$. Pak platí

$$f(\tau)^{1-\sigma_l} = \prod_{t \in T} f(\sigma_t)^{(1-\sigma_l) \prod\limits_{s \in T \cap S_t} \sigma_s}.$$

Pak ale podle (5)

$$f(\tau)^{1-\sigma_l} = \prod_{t \in T} f(\sigma_l)^{(1-\sigma_t) \prod\limits_{s \in T \cap S_t} \sigma_s} = f(\sigma_l)^{\sum\limits_{t \in T} (1-\sigma_t) \prod\limits_{s \in T \cap S_t} \sigma_s} = f(\sigma_l)^{1-\tau}.$$

□

Lemma 2.2. *Splňuje-li g podmínky Tvrzení 2.2 a f je definována týmž předpisem jako v Tvrzení 2.2, pak pro libovolný automorfismus $\tau \in G$ a prvočíslo $l \in S$ platí*

$$f(\sigma_l\tau) = f(\sigma_l)f(\tau)^{\sigma_l}$$

Důkaz lemmatu: Buď $T \subseteq S$ množina, pro kterou $\tau = \prod_{t \in T} \sigma_t$. Označme $\rho = \prod_{t \in T \cap S_l} \sigma_t$ a $\omega = \prod_{t \in T \setminus (S_l \cup \{l\})} \sigma_t$. Z definice f plyne

$$f(\rho\sigma_l\omega) = f(\rho)f(\sigma_l)^{\rho}f(\omega)^{\rho\sigma_l} = f(\rho)f(\omega)^{\rho} \cdot \left(f(\sigma_l)f(\omega)^{\sigma_l - 1}\right)^{\rho}.$$

Podle Lemmatu 2.1 pak dále dostáváme

$$f(\rho\sigma_l\omega) = f(\rho\omega) \cdot \left(f(\sigma_l)f(\sigma_l)^{\omega - 1}\right)^{\rho} = f(\rho\omega)f(\sigma_l)^{\rho\omega}.$$

Pokud $l \notin T$, pak je $\tau = \rho\omega$ a z předchozího dostáváme

$$f(\sigma_l\tau) = f(\tau)f(\sigma_l)^{\tau} = f(\tau)f(\sigma_l)f(\sigma_l)^{\tau - 1}$$

a opět podle Lemmatu 2.1

$$f(\sigma_l\tau) = f(\tau)f(\sigma_l)f(\tau)^{\sigma_l - 1} = f(\sigma_l)f(\tau)^{\sigma_l}.$$

Předpokládejme nyní, že $l \in T$, tj. $\tau = \rho\sigma_l\omega$. Máme dokázáno $f(\tau) = f(\tau\sigma_l)f(\sigma_l)^{\tau\sigma_l}$, neboť platí $\rho\omega = \tau\sigma_l$. Podle (4) je $f(\sigma_l)^{-\sigma_l} = f(\sigma_l)$ a tedy

$$f(\sigma_l\tau) = f(\tau)f(\sigma_l)^{-\tau\sigma_l} = f(\tau)f(\sigma_l)^{\tau} = f(\tau)f(\sigma_l)f(\tau)^{\sigma_l - 1} = f(\sigma_l)f(\tau)^{\sigma_l},$$

přičemž jsme opět využili Lemmatu 2.1 $\square$

Důkaz tvrzení 2.2: Nechť $V \subseteq S, \sigma = \prod_{s\in V}\sigma_s$. Je-li $V = \emptyset$, je $\sigma = 1$ a dokazované tvrzení platí triviálně. Budeme postupovat indukcí vzhledem k V, tj. předpokládáme, že pro libovolné $T \subsetneq V$ platí

$$f\Big(\Big(\prod_{s\in T}\sigma_s\Big)\tau\Big) = f\Big(\prod_{s\in T}\sigma_s\Big) \cdot f(\tau)^{\prod\limits_{s\in T}\sigma_s}$$

Označme $m = \min V, \omega = \prod_{s\in V\setminus\{m\}}\sigma_s$. Platí tedy $\sigma = \sigma_m\omega$ a z definice f: $f(\sigma) = f(\sigma_m)f(\omega)^{\sigma_m}$. Dále dostáváme s použitím Lemmatu 2.2

$$f(\sigma\tau) = f(\sigma_m\omega\tau) = f(\sigma_m)f(\omega\tau)^{\sigma_m}$$

Aplikujeme-li nyní indukční předpoklad, tj. vztah $f(\omega\tau) = f(\omega)f(\tau)^{\omega}$, dostaneme

$$f(\sigma\tau) = f(\sigma_m)\big(f(\omega)f(\tau)^{\omega}\big)^{\sigma_m} = f(\sigma)f(\tau)^{\omega\sigma_m} = f(\sigma)f(\tau)^{\sigma}.$$

$\square$

Předchozí dvě tvrzení nyní shrneme do kritéria, které budeme v následující kapitole užívat pro zjišťování toho, zda je jednotka v tělese $\mathbb{Q}\big(\sqrt{p}, \sqrt{q}, \sqrt{r}\big)$ druhou mocninou.

Tvrzení 2.3. *Existuje-li funkce $g : \{\sigma_l \mid l \in S\} \to K_S^{\times}$, splňující $\varepsilon^{1-\sigma_l} = g(\sigma_l)^2$ pro libovolné $l \in S$ a podmínky*

$$\forall l \in S: \qquad g(\sigma_l)^{1+\sigma_l} = 1 \tag{4}$$
$$\forall p_1, p_2 \in S: \qquad g(\sigma_{p_1})^{1-\sigma_{p_2}} = g(\sigma_{p_2})^{1-\sigma_{p_1}}, \tag{5}$$

pak je ε nebo $-\varepsilon$ kvadrátem v K_S.

Důkaz. K důkazu tohoto tvrzení stačí podle Tvrzení 2.2 dokázat pouze fakt, že křížový homomorfismus f indukovaný funkcí g splňuje $\varepsilon^{1-\sigma} = f(\sigma)^2$ pro libovolné $\sigma \in G$. Potom podle Tvrzení 2.1 je ε nebo $-\varepsilon$ v K_J druhou mocninou.

Buď tedy $\sigma \in G$ libovolný automorfismus a pišme jej ve tvaru $\sigma = \prod_{t\in T}\sigma_t$, kde $T \subseteq S$ je množina jednoznačně určená automorfismem σ. Důkaz povedeme indukcí přes mohutnost T. Je-li $T = \emptyset$, je $\sigma = 1$ a tvrzení triviálně platí. V případě $|T| = 1$, neboli $\sigma = \sigma_l$ pro některé $l \in J$, plyne požadovaná vlastnost z předpokladů tvrzení a z poznámky za Tvrzením 2.2. Buďte nyní P a R vlastní podmnožiny T takové, že $P \cap R = \emptyset$ a $\sigma = \prod_{j\in P}\sigma_j \cdot \prod_{k\in R}\sigma_k$. Označme $\tau = \prod_{j\in P}\sigma_j$ a $\omega = \prod_{k\in R}\sigma_k$. Pak $\sigma = \tau\omega$ a podle indukčního předpokladu platí $\varepsilon^{1-\tau} = f(\tau)^2$ a $\varepsilon^{1-\omega} = f(\omega)^2$. Celkem tedy, protože f je křížový homomorfismus, máme

$$\varepsilon^{1-\sigma} = \varepsilon^{1-\tau\omega} = \varepsilon^{1-\tau}\big(\varepsilon^{1-\omega}\big)^{\tau} = f(\tau)^2\big(f(\omega)^2\big)^{\tau} = f(\tau\omega)^2.$$

Tím je tvrzení dokázáno. $\square$

Je vidět, že k aplikaci těchto kritérií na jednotku $\eta \in E$, bude třeba umět spočítat $\eta^{1-\sigma}$ pro $\sigma \in G$. Protože v případě $S = \{p, q, r\}$, tj. pro těleso $K_S = \mathbb{Q}\big(\sqrt{p}, \sqrt{q}, \sqrt{r}\big)$, jsou prvky grupy G generovány automorfismy σ_p, σ_q a σ_r, bude nutné spočítat obrazy jednotek z E po aplikaci těchto automorfismů.

Výpočet hodnoty $\beta_{pqr}^{1+\sigma_q}$

Z definice β_{pqr} (viz (2)) dostáváme, že

$$\beta_{pqr}^{1+\sigma_q} = \prod_{\substack{0<a<pqr \\ \psi(a)\in R \\ q\nmid a,\, \left(\frac{a}{r}\right)=1}} (\xi_{pqr}^{a} - \xi_{pqr}^{-a}) = \xi_{pqr}^{s} \prod_{\substack{0<a<pqr \\ \psi(a)\in R \\ q\nmid a,\, \left(\frac{a}{r}\right)=1}} (1 - \zeta_{pqr}^{-a}),$$

kde $s = \sum_a a$, s a probíhajícím přes stejnou množinu jako v předchozích součinech. Pro další výpočty budeme potřebovat zjistit, do jakých tříd kongruence patří s modulo p, q a r.

Lemma 2.3.

a) $q \mid s$, $r \mid s$,

b) $s \equiv (q-1)\sum_a a \pmod{pr}$, *kde se sčítá přes* a, *splňující* $0 < a < pr$, $\psi(a) \in R$, $\left(\frac{a}{r}\right) = 1$.

Důkaz.

a) Na množině přirozených čísel a, splňujících $0 < a < pqr, \psi(a) \in R, \left(\frac{a}{r}\right) = 1$ a $q \nmid a$, definujme funkci f pomocí kongruencí takto:

$$\begin{aligned} f(a) &\equiv a \pmod{p} \\ f(a) &\equiv -a \pmod{q} \\ f(a) &\equiv -a \pmod{r} \end{aligned}$$

Z Čínské zbytkové věty plyne, že f je bijektivní zobrazení bez pevného bodu (kdyby a byl pevný bod f, tj. $f(a) = a$, pak by podle druhé kongruence platilo $a \equiv -a \pmod{q}$ neboli $q \mid a$, což je spor). Odtud

$$s + s = \sum_{\substack{0<a<pqr \\ \psi(a)\in R \\ q\nmid a,\, \left(\frac{a}{r}\right)=1}} a + \sum_{\substack{0<a<pqr \\ \psi(a)\in R \\ q\nmid a,\, \left(\frac{a}{r}\right)=1}} f(a) = \sum_{\substack{0<a<pqr \\ \psi(a)\in R \\ q\nmid a,\, \left(\frac{a}{r}\right)=1}} (a + f(a)),$$

což je zřejmě dělitelné čísly q i r a tedy i s je dělitelné q i r.

b) Uspořádejme si pro větší přehlednost přirozená čísla mezi 0 a pqr do tabulky následujícím způsobem:

$$\begin{array}{ccc} 1 & \dots & pr \\ pr+1 & \dots & 2pr \\ \vdots & & \vdots \\ (q-1)pr+1 & \dots & qpr \end{array}$$

Uvažujme nyní libovolný sloupec této tabulky. Všechna čísla v tomto sloupci mají stejný zbytek po dělení číslem p, je tedy jasné, že pro všechna čísla a ve sloupci platí buď $\psi(a) \in R$ nebo pro všechna platí $\psi(a) \notin R$. Podobně jsou buď všechna čísla ve sloupci kvadratickými zbytky modulo r nebo jsou všechna čísla ve sloupci kvadratickými nezbytky modulo r. V každém sloupci je navíc právě jedno číslo dělitelné q. Uvažujme nyní pouze sloupce čísel a, kde $\psi(a) \in R$ a $\left(\frac{a}{r}\right) = 1$, neboť čísla z ostatních sloupců v sumě, určující číslo s, nevystupují. Nahradíme-li nyní v takovém sloupci každé z $(q-1)$ čísel nedělitelných q číslem v prvním řádku (které je s ním kongruentní modulo pr), dostaneme tvrzení lemmatu. □

Z předchozího lemmatu a z definice β_{pr} v (1) nyní plyne (ve všech součinech a probíhá celá čísla splňující $0 < a < pr, \psi(a) \in R, \left(\frac{a}{r}\right) = 1$)

$$\beta_{pqr}^{1+\sigma_q} = \Big(\prod_a \xi_{pqr}^{qa}\Big)^{1-\mathrm{Frob}(q,\mathbb{Q}(\zeta_{pr}))^{-1}} \prod_a (1-\zeta_{pr}^{-a})^{1-\mathrm{Frob}(q,\mathbb{Q}(\zeta_{pr}))^{-1}} =$$
$$= \prod_a (\xi_{pqr}^{qa} - \xi_{pqr}^{-qa})^{1-\mathrm{Frob}(q,\mathbb{Q}(\zeta_{pr}))^{-1}} = \beta_{pr}^{1-\mathrm{Frob}(q,\mathbb{Q}(\zeta_{pr}))^{-1}} = \beta_{pr}^{1-\mathrm{Frob}(q,\mathbb{Q}(\zeta_{pr}))}$$

Protože $\beta_{pr} \in \mathbb{Q}\left(\sqrt{p}, \sqrt{r}\right)$, je podle definice Frobeniova automorfismu pro abelovské těleso $\beta_{pr}^{1-\mathrm{Frob}(q,\mathbb{Q}(\zeta_{pr}))} = \beta_{pr}^{1-\mathrm{Frob}(q,\mathbb{Q}(\sqrt{p},\sqrt{r}))}$. Dokázali jsme tedy následující

Tvrzení 2.4. *Buďte $p, q, r \equiv 1 \pmod 4$ prvočísla. Potom*

$$\beta_{pqr}^{1+\sigma_q} = \beta_{pr}^{1-\mathrm{Frob}(q,\mathbb{Q}(\sqrt{p},\sqrt{r}))} \tag{6}$$

Výpočet $\beta_{pq}^{1+\sigma_q}$

V [4] je dokázáno, že jednotka ε_{pq} je druhou mocninou jednotky $\beta_{pq} \in E$. Dále bylo ukázáno, že pokud prvočísla p, q splňují $p \equiv q \equiv 1 \pmod 4$ a $\left(\frac{p}{q}\right) = 1$, potom pro β_{pq} platí následující rovnost:

$$\beta_{pq}^{1+\sigma_q} = \chi_p(q), \tag{7}$$

Na tento výsledek navážeme nyní podobným výsledkem pro případ, že $\left(\frac{p}{q}\right) = -1$. Nejprve dokážeme několik pomocných lemmat.

Lemma 2.4. *Pro všechna $n \in \mathbb{N} : n = (1-\zeta_n)(1-\zeta_n^2)\ldots(1-\zeta_n^{n-1})$.*

Důkaz. Uvažujme polynom $x^n - 1$. Tento polynom má v $\mathbb{C}$ kořeny $1, \zeta_n, \zeta_n^2, \ldots, \zeta_n^{n-1}$, můžeme ho tedy v oboru komplexních čísel rozložit na součin lineárních faktorů takto: $x^n - 1 = (x-1)(x-\zeta_n)(x-\zeta_n^2)\ldots(x-\zeta_n^{n-1})$. Pokud tuto rovnost vydělíme polynomem $x-1$, dostaneme $x^{n-1} + x^{n-2} + \cdots + x + 1 = (x-\zeta_n)(x-\zeta_n^2)\ldots(x-\zeta_n^{n-1})$ a po substituci $x = 1$ dostáváme požadovanou rovnost. □

Lemma 2.5. *Pro libovolné prvočíslo $l \equiv 1 \pmod 4$ platí*

$$\sqrt{l} = \prod_{a=1}^{\frac{l-1}{2}} (\xi_l^{-a} - \xi_l^a). \tag{8}$$

Důkaz. Toto lemma dokážeme ve dvou krocích. Nejprve aplikujeme Lemma 2.4 a po několika jednoduchých úpravách dostaneme jiné vyjádření pro l:

$$l = \prod_{a=1}^{l-1}(1-\zeta_l^a) = \prod_{a=1}^{l-1} \xi_l^a(\xi_l^{-a} - \xi_l^a) = (-1)^{\frac{l-1}{2}} \xi_l^{\frac{l(l-1)}{2}} \prod_{a=1}^{\frac{l-1}{2}} (\xi_l^{-a} - \xi_l^a)^2 =$$
$$= \prod_{a=1}^{\frac{l-1}{2}} (\xi_l^{-a} - \xi_l^a)^2.$$

Tímto jsme dokázali, že pravá strana (8) je rovna buď $\sqrt{l}$ nebo $-\sqrt{l}$. Teď už tedy stačí jen dokázat, že tato pravá strana je kladné reálné číslo.

$$\begin{aligned}\prod_{a=1}^{\frac{l-1}{2}}(\xi_l^{-a}-\xi_l^a) &= \prod_{a=1}^{\frac{l-1}{2}}(-2i)\sin\left(\frac{l+1}{l}a\pi\right) = \\ &= (-2i)^{\frac{l-1}{2}}\prod_{a=1}^{\frac{l-1}{2}}(-1)^{\left[\frac{l+1}{l}a\right]}\left|\sin\left(\frac{l+1}{l}a\pi\right)\right| = \\ &= (-2i)^{\frac{l-1}{2}}\cdot(-1)^{\sum_{a=1}^{\frac{l-1}{2}}a}\cdot\prod_{a=1}^{\frac{l-1}{2}}\left|\sin\left(\frac{l+1}{l}a\pi\right)\right| \\ &= (-2i)^{\frac{l-1}{2}}\cdot(-1)^{\frac{l^2-1}{8}}\prod_{a=1}^{\frac{l-1}{2}}\left|\sin\left(\frac{l+1}{l}a\pi\right)\right|\end{aligned}$$

a snadno se ukáže, že toto je pro $l \equiv 1 \pmod 4$ kladné číslo. □

Lemma 2.6. *Buď l prvočíslo, $l > 3$. Potom je součet kvadratických zbytků modulo l mezi 0 a l dělitelný číslem l, t.j.*

$$\sum_{\substack{0<a<l\\ \left(\frac{a}{l}\right)=1}} a \equiv 0 \pmod{l}.$$

Důkaz. Buď g primitivní kořen modulo l. Pak

$$\sum_{\substack{0<a<l\\ \left(\frac{a}{l}\right)=1}} a = g^0+g^2+\cdots+g^{l-3} = \frac{g^{l-1}-g^0}{g^2-1} \equiv 0 \pmod{l},$$

neboť díky předpokladu $l > 3$ je $g^2 \not\equiv 1 \pmod{l}$. Tím je požadované tvrzení dokázáno. □

Pokračujme nyní ve výpočtu $\beta_{pq}^{1+\sigma_q}$ v případě, že $\left(\frac{p}{q}\right) = -1$.

$$\beta_{pq}^{1+\sigma_q} = \prod_{\substack{0<a<pq\\ q\nmid a,\psi(a)\in R}}(\xi_{pq}^a-\xi_{pq}^{-a}) = \xi_{pq}^s \prod_{\substack{0<a<pq\\ q\nmid a,\psi(a)\in R}}(1-\zeta_{pq}^{-a}),$$

kde znovu $s = \sum_a a$ a index a probíhá přes stejnou množinu přirozených čísel jako v předcházejících součinech. V následujícím lemmatu spočítáme třídy kongruence čísla s modulo p a q.

Lemma 2.7.
a) $q \mid s$,
b) $s \equiv (q-1)\sum_a a \pmod{p}$, *kde sčítáme přes a splňující $0 < a < p$, $\psi(a) \in R$.*

Důkaz.
a) Na množině přirozených čísel a, splňujících $0 < a < pq, q \nmid a$ a $\psi(a) \in R$, definujme podobně jako v důkazu Lemmatu 2.3 funkci f pomocí následujících kongruencí:

$$\begin{aligned} f(a) &\equiv a \pmod{p} \\ f(a) &\equiv -a \pmod{q}\end{aligned}$$

Opět z Čínské zbytkové věty plyne, že f je bijektivní zobrazení bez pevného bodu. Odtud

$$s+s=\sum_{\substack{0<a<pq\\ q\nmid a,\psi(a)\in R}} a+\sum_{\substack{0<a<pq\\ q\nmid a,\psi(a)\in R}} f(a)=\sum_{\substack{0<a<pq\\ q\nmid a,\psi(a)\in R}} (a+f(a)),$$

což je zřejmě dělitelné číslem q, protože každý člen součtu je číslem q dělitelný a tedy také číslo s je dělitelné q.

b) Pro větší přehlednost si přirozená čísla $1,\dots,pq$ uspořádejme do řádků a sloupců

$$\begin{array}{ccc} 1 & \dots & p\\ p+1 & \dots & 2p\\ \vdots & & \vdots\\ (q-1)p+1 & \dots & qp \end{array}$$

a uvažujme libovolný sloupec z této tabulky. Protože všechna čísla v tomto sloupci dávají stejný zbytek při dělení číslem p, je zřejmé, že buď pro všechna čísla a ve sloupci platí $\psi(a)\in R$ nebo pro všechna čísla platí $\psi(a)\notin R$. Navíc je v každém sloupci právě jedno číslo dělitelné q. Nyní uvažujme všechny sloupce čísel a, splňujících $\psi(a)\in R$. Každé číslo z takového sloupce, které není dělitelné q, nahraďme číslem v prvním řádku téhož sloupce a dostaneme tvrzení lemmatu. $\square$

Podle Lemmatu 2.7 tedy máme (ve všech následujících součinech probíhá a celá čísla splňující $0<a<p$ a $\psi(a)\in R$).

$$\begin{aligned}\beta_{pq}^{1+\sigma_q} &= \Big(\prod_a \xi_{pq}^{qa}\Big)^{1-\mathrm{Frob}(q,\mathbb{Q}(\zeta_p))^{-1}}\prod_a(1-\zeta_p^{-a})^{1-\mathrm{Frob}(q,\mathbb{Q}(\zeta_p))^{-1}}=\\ &=\prod_a(\xi_p^{a}-\xi_p^{-a})^{1-\mathrm{Frob}(q,\mathbb{Q}(\zeta_p))^{-1}}=\prod_a(\xi_p^{a}-\xi_p^{-a})\prod_a(\xi_p^{aq'}-\xi_p^{-aq'})^{-1}\end{aligned}.$$

kde q' je přirozené číslo splňující $qq'\equiv 1 \pmod p$. Následující krok je alespoň na první pohled poněkud umělý.[1] Obě strany rovnice vynásobíme výrazem

$$\prod_{\substack{0<a<p\\ \left(\frac{a}{p}\right)=-1\\ \psi(a)\notin R'}} (\xi_p^{a}-\xi_p^{-a})^{-1}$$

[1] Ve skutečnosti ale víme (až na znaménko) k čemu chceme dospět. V případě $\left(\frac{p}{q}\right)=-1$ totiž podle Lemmatu 1.2 platí $(\beta_{pq}^{1+\sigma_q})^2=\varepsilon_{pq}^{1+\sigma_q}=\varepsilon_p^2$ a tedy $\beta_{pq}^{1+\sigma_q}=\pm\varepsilon_p$. V tomto odstavci nám jde o přesné určení tohoto znaménka.

a po jednoduché úpravě máme (zde ve všech součinech předpokládáme navíc $0 < a < p$)

$$\begin{aligned}
&\beta_{pq}^{1+\sigma_q} \prod_{\substack{\left(\frac{a}{p}\right)=-1\\ \psi(a)\notin R'}} (\xi_p^a - \xi_p^{-a})^{-1} \prod_{\psi(a)\in R} (\xi_p^{aq'} - \xi_p^{-aq'}) = \\
&= \prod_{\psi(a)\in R} (\xi_p^a - \xi_p^{-a}) \prod_{\substack{\left(\frac{a}{p}\right)=-1\\ \psi(a)\notin R'}} (\xi_p^a - \xi_p^{-a})^{-1} = \\
&= \prod_{\psi(a)\notin R\cup R'} (\xi_p^a - \xi_p^{-a})^{-1} \prod_{\left(\frac{a}{p}\right)=1} (\xi_p^a - \xi_p^{-a}) = \\
&= \prod_{\psi(a)\in R\cup R'} (\xi_p^{-a} - \xi_p^{a})^{-1} \prod_{\left(\frac{a}{p}\right)=1} (\xi_p^{-a} - \xi_p^{a}) = \\
&= \prod_{\psi(a)\in R\cup R'} (\xi_p^{-a} - \xi_p^{a})^{-1} \prod_{\left(\frac{a}{p}\right)=1} \xi_p^{-a}(1 - \zeta_p^{a}) = \\
&= \xi_p^{-\sum_a a} \cdot \prod_{\psi(a)\in R\cup R'} (\xi_p^{-a} - \xi_p^{a})^{-1} \prod_{\left(\frac{a}{p}\right)=1} (1 - \zeta_p^{a}),
\end{aligned}$$

přitom a v součtu probíhá všechny kvadratické zbytky modulo p mezi přirozenými čísly z intervalu $(0, p)$. Z definice množin R a R' a z toho, že násobení číslem q je bijekce modulo p, se snadno ukáže, že

$$\begin{aligned}
&\prod_{\substack{\left(\frac{a}{p}\right)=-1\\ \psi(a)\notin R'}} (\xi_p^a - \xi_p^{-a})^{-1} \prod_{\psi(a)\in R} (\xi_p^{aq'} - \xi_p^{-aq'}) = (-1)^{\#\left\{\, 0<a<p \,\mid\, \psi(a)\in R,\, \psi(aq')\in R' \,\right\}} = \\
&= (-1)^{\#\left\{\, 0<a<p \,\mid\, \psi(aq)\in R,\, \psi(a)\in R' \,\right\}}.
\end{aligned}$$

Z Lemmatu 2.6 nyní plyne, že $\xi_p^{-\sum_a a} = 1$. Dále, z Definice 1.1 plyne, že

$$\varepsilon_p = \frac{1}{\sqrt{p}} \prod_{\substack{0<a<p\\ \left(\frac{a}{p}\right)=1}} (1 - \zeta_p^a).$$

Definujme nyní ještě důležitou funkci α:

Definice 2.2. *Pro libovolné prvočíslo* $l \equiv 1 \pmod 4$ *a libovolné celé číslo* s, *splňující* $\left(\frac{s}{l}\right) = -1$, *definujeme* $\alpha(l,s) := (-1)^{\#\left\{\, 0<a<l \,\mid\, \psi_l(as)\in R_l,\, \psi_l(a)\in R_l' \,\right\}} \cdot (-1)^{\#\left\{\, 0<a\leqslant \frac{l-1}{2} \,\mid\, \psi_l(a)\notin R_l\cup R_l' \,\right\}}$.

Poznámka: Ačkoli je $\alpha(l,s)$ definováno pomocí pevně zvoleného charakteru ψ_l, plyne z následujícího tvrzení, že funkce α na volbě tohoto charakteru nezávisí.

Předchozí definice spolu s Lemmatem 2.5 dohromady dává

$$\begin{aligned}
\beta_{pq}^{1+\sigma_q} &= \varepsilon_p \cdot (-1)^{\#\left\{\, 0<a<p \,\mid\, \psi(aq)\in R,\, \psi(a)\in R' \,\right\}} \cdot (-1)^{\#\left\{\, 0<a\leqslant \frac{p-1}{2} \,\mid\, \psi(a)\notin R\cup R' \,\right\}} = \\
&= \varepsilon_p \cdot \alpha(p,q)
\end{aligned}$$

Tento výsledek zformulujme explicitně jako tvrzení.

Tvrzení 2.5. *Platí-li* $\left(\frac{p}{q}\right) = -1$, *pak*

$$\beta_{pq}^{1+\sigma_q} = \alpha(p,q)\,\varepsilon_p. \tag{9}$$

Nyní zformulujeme a dokážeme užitečné tvrzení o takto definované funkci α, které bude našim hlavním prostředkem ke klasifikaci trojic prvočísel v příští kapitole.

Tvrzení 2.6. *Buďte* m, n *přirozená čísla, která jsou kvadratickými nezbytky modulo* p *Potom platí*

$$\alpha(p,m) \cdot \alpha(p,n) = -\chi_p(mn).$$

Důkaz. Označme kvůli stručnosti $(-1)^{\#\{\,0<a<p\,|\,\psi(am)\in R,\,\psi(a)\in R'\,\}}$ jako $\tau_\psi(p,m)$ (je to jeden z činitelů v $\alpha(p,m)$). Našim cílem bude určit $\tau_\psi(p,m)$ pomocí Dirichletových charakterů. Nechť g je primitivní kořen modulo p takový, že $\psi(g) = \zeta_{2^b}$ (jeho existence plyne z faktu, že ψ je charakter řádu 2^b modulo p). Vyjádřeme nyní m ve formě mocniny g: $m = g^k$, kde $0 \leqslant k < p-1$. Připomeňme navíc, že $p - 1 = c \cdot 2^b$, kde c je liché přirozené číslo a $b \geqslant 2$. Zapišme k jako $k = k_1 \cdot 2^b + k_2$, kde $0 \leqslant k_2 < 2^b$. Protože m je kvadratický nezbytek modulo p, je k_2 liché číslo. Potřebujeme spočítat hodnotu $\tau_\psi(p,m)$, proto nyní vypočteme mohutnost množiny v jeho exponentu.

$$\begin{aligned}
&\#\left\{\, 0 < a < p \;\middle|\; \psi(am) \in R,\, \psi(a) \in R' \,\right\} = \\
&= \#\left\{\, 0 \leqslant j \leqslant p-2 \;\middle|\; \left\langle \frac{j+k}{2^b} \right\rangle < \frac{1}{2}, 2 \mid j, \left\langle \frac{j}{2^b} \right\rangle < \frac{1}{2} \,\right\} = \\
&= \#\left\{\, x \cdot 2^b + y \;\middle|\; 0 \leqslant x < c, 0 \leqslant y < 2^{b-1}, 2 \mid y, \left\langle \frac{y+k}{2^b} \right\rangle < \frac{1}{2} \,\right\} = \\
&= c \cdot \#\left\{\, y \;\middle|\; 0 \leqslant y < 2^{b-1}, 2 \mid y, \left\langle \frac{y+k_2}{2^b} \right\rangle < \frac{1}{2} \,\right\}.
\end{aligned}$$

Rozlišme nyní dva případy:

1) $\underline{0 \leqslant k_2 < 2^{b-1}}$
   Potom máme na y následující podmínky: $0 \leqslant y < 2^{b-1}, y + k_2 < 2^{b-1}, 2 \mid y$. Toto je však zřejmě ekvivalentní podmínkám $0 \leqslant \frac{y}{2} < 2^{b-2} - \frac{k_2-1}{2}$, $\frac{y}{2} \in \mathbb{Z}$. Hledaná kardinalita je tedy v tomto případě rovna $2^{b-2} - \frac{k_2-1}{2}$
2) $\underline{2^{b-1} \leqslant k_2 < 2^b}$
   Podmínky na y jsou v tomto případě: $0 \leqslant y < 2^{b-1}, y + k_2 \geqslant 2^b, 2 \mid y$. To je ekvivalentní podmínkám $2^{b-2} > \frac{y}{2} \geqslant 2^{b-1} - \frac{k_2-1}{2}$, $\frac{y}{2} \in \mathbb{Z}$. Počet prvků množiny je tedy $\frac{k_2-1}{2} - 2^{b-2}$.

V obou případech tedy máme[2]

$$\tau_\psi(p,m) = 1 \iff \begin{cases} k_2 \equiv 1 \pmod 4 & \text{je-li } 8 \mid (p-1) \\ k_2 \equiv 3 \pmod 4 & \text{je-li } 8 \nmid (p-1) \end{cases}$$

Klademe-li nyní $\chi = \psi^{2^{b-2}}$, pak je χ Dirichletův charakter modulo p řádu 4 a pro $a \in \mathbb{Z}$, $\left(\frac{a}{p}\right) = -1$ je $\chi(a) = i$ právě tehdy, když $a = g^k$ a $k \equiv 1 \pmod 4$. Náš výsledek můžeme tedy přepsat ve tvaru

$$\tau_\psi(p,m) = (-1)^{\frac{p-1}{4}} \cdot \frac{\chi(m)}{i}.$$

[2] Poznamenejme, že výsledek stále závisí na zvoleném charakteru ψ.

Dokončeme teď důkaz tvrzení tím, že vypočítáme součin $\alpha(p,m)\cdot\alpha(p,n)$ ($\kappa_\psi(p)$ bude pro zjednodušení znamenat $(-1)^{\#\left\{\,0<a\leqslant\frac{p-1}{2}\,\mid\,\psi(a)\notin R\cup R'\,\right\}}$).

$$\alpha(p,m)\cdot\alpha(p,n)=\left(\kappa_\psi(p)\cdot(-1)^{\frac{p-1}{4}}\cdot\frac{\chi(m)}{i}\right)\left(\kappa_\psi(p)\cdot(-1)^{\frac{p-1}{4}}\cdot\frac{\chi(n)}{i}\right)=-\chi(mn),$$

neboť $p\equiv 1 \pmod 4$ a $\kappa_\psi(p)=(-1)^{\#\left\{\,0<b\leqslant\frac{p-1}{2}\,\mid\,\psi(b)\notin R\cup R'\,\right\}}$ závisí pouze na p a ψ, proto umocněno na druhou je rovno 1. Navíc, protože je mn kvadratický zbytek modulo p, je podle Lemmatu 1.1 $\chi(mn)=\chi_p(mn)$. Tím je naše tvrzení dokázáno. $\square$

3. Hlavní výsledky

Úvod

V práci [4] se R. Kučera zabývá určením parity počtu tříd divizorů bikvadratického tělesa $\mathbb{Q}\left(\sqrt{p},\sqrt{q}\right)$, kde p a q jsou různá prvočísla $p,q\equiv 1 \pmod 4$. Tato charakterizace je závislá především na hodnotě $\left(\frac{p}{q}\right)$. Poznamenejme, že ze zákona kvadratické reciprocity (viz např. [3]) plyne, že pro prvočísla $p,q\equiv 1 \pmod 4$ je $\left(\frac{p}{q}\right)=\left(\frac{q}{p}\right)$. Pro charakterizaci vzájemné „zbytkovosti“ tedy stačí uvažovat číslo $\left(\frac{p}{q}\right)$.

Protože tuto práci využijeme i při charakterizaci těles stupně 8, vzniklých jako rozšíření tělesa $\mathbb{Q}$ o tři různá prvočísla p,q a r, kde $p,q,r\equiv 1 \pmod 4$, uvedeme nyní hlavní větu její 2. kapitoly.

Tvrzení 3.1. *Buďte p a q různá prvočísla, taková že $p\equiv q\equiv 1 \pmod 4$ a nechť dále h označuje počet tříd divizorů tělesa $\mathbb{Q}\left(\sqrt{p},\sqrt{r}\right)$. Potom*

1. *je-li $\left(\frac{p}{q}\right)=-1$, je h liché.*
2. *Je-li $\left(\frac{p}{q}\right)=1$, je*
   a) *h liché, jestliže $\chi_q(p)\neq\chi_p(q)$,*
   b) *h sudé, pokud $\chi_q(p)=\chi_p(q)$.*

Poznámky:

1) Výsledky, obsažené v předchozím tvrzení se dokazují stejným postupem jako v tomto článku — v příslušném bikvadratickém tělese se hledají jednotky analogické naší jednotce η, které lze v tomto tělese odmocnit. Ukáže se, že v případě $\left(\frac{p}{q}\right)=-1$ taková jednotka neexistuje, v případě $\left(\frac{p}{q}\right)=1$ pak existuje právě tehdy, když platí $\chi_q(p)=\chi_p(q)$. Tato jednotka je rovna $\pm\beta_{pq}$ v případě, že $\chi_q(p)=\chi_p(q)=1$ a je rovna $\pm\varepsilon_p\varepsilon_q\beta_{pq}$, jestliže $\chi_q(p)=\chi_p(q)=-1$.
2) Označme pro různá $j,k\in\{p,q,r\}$ jako E_{jk} grupu jednotek bikvadratického tělesa $\mathbb{Q}\left(\sqrt{j},\sqrt{k}\right)$. Je-li
$$[\,E_{jk}:\langle -1,\varepsilon_j,\varepsilon_k,\beta_{jk}\rangle\,]=2^{v_{jk}}\cdot l,$$
kde $2\nmid l$, pak z toho, že $\pm\varepsilon_j,\pm\varepsilon_k$ ani $\pm\varepsilon_j\varepsilon_k$ nejsou v E druhými mocninami jednotek, plyne existence jednotky $\lambda_{jk}\in E$ pro kterou platí
$$[\,E_{jk}:\langle -1,\varepsilon_j,\varepsilon_k,\lambda_{jk}\rangle\,]=l,$$
přičemž $\lambda_{jk}^{2^{v_{jk}}}=\pm\beta_{jk}\varepsilon_j^{c_j}\varepsilon_k^{c_k}$, pro vhodná $c_j,c_k\in\mathbb{Z}$.
Potom ale
$$[\,E:\langle -1,\varepsilon_p,\varepsilon_q,\varepsilon_r,\lambda_{pq},\lambda_{pr},\lambda_{qr},\beta_{pqr}\rangle\,]=\frac{h}{2^{v_{pq}+v_{pr}+v_{qr}}}.$$

Dokážeme-li tedy odmocnit nějakou jednotku z podgrupy generované jednotkami -1, ε_p, ε_q, ε_r, λ_{pq}, λ_{pr}, λ_{qr}, β_{pqr}, je zřejmé, že počet tříd divizorů h tělesa $\mathbb{Q}\left(\sqrt{p},\sqrt{q},\sqrt{r}\right)$ je dělitelný číslem $2^{1+v_{pq}+v_{pr}+v_{qr}}$.

Nyní již přejděme k našemu případu tělesa řádu 8. Jak jsme popsali v 1. kapitole, ke zjištění parity počtu tříd divizorů tohoto tělesa nám stačí prověřit, je-li některá jednotka tvaru

$$\eta = \pm\varepsilon_p^{x_p}\varepsilon_q^{x_q}\varepsilon_r^{x_r}\beta_{pq}^{x_{pq}}\beta_{pr}^{x_{pr}}\beta_{qr}^{x_{qr}}\beta_{pqr}^{x_{pqr}},$$

kde $x_p, x_q, x_r, x_{pq}, x_{pr}, x_{qr}, x_{pqr} \in \{0,1\}$, v grupě jednotek E tělesa druhou mocninou jiné jednotky. V následujícím odstavci nejprve ukážeme, že nutnou podmínkou pro to je, že alespoň jeden z koeficientů $x_{pq}, x_{pr}, x_{qr}, x_{pqr}$ je nenulový.

Základní podmínky, kladené na η

Ukážeme, že žádná z jednotek $\pm\varepsilon_p, \pm\varepsilon_q, \pm\varepsilon_r, \pm\varepsilon_p\varepsilon_q, \pm\varepsilon_p\varepsilon_r, \pm\varepsilon_q\varepsilon_r, \pm\varepsilon_p\varepsilon_q\varepsilon_r$ není v E kvadrátem. Z Lemmatu 1.2 plyne:

$$(\pm\varepsilon_p)^{1+\sigma_p} = (\pm\varepsilon_q)^{1+\sigma_q} = (\pm\varepsilon_r)^{1+\sigma_r} = -1,$$

není tedy žádná jednotka z $\pm\varepsilon_p, \pm\varepsilon_q, \pm\varepsilon_r$ v $\mathbb{Q}\left(\sqrt{p},\sqrt{q},\sqrt{r}\right)$ kvadrátem. Dále,

$$(\pm\varepsilon_p\varepsilon_q)^{1+\sigma_p} = -\varepsilon_q^2, \quad (\pm\varepsilon_p\varepsilon_r)^{1+\sigma_p} = -\varepsilon_r^2, \quad (\pm\varepsilon_q\varepsilon_r)^{1+\sigma_q} = -\varepsilon_r^2,$$

tedy ani $\pm\varepsilon_p\varepsilon_q, \pm\varepsilon_p\varepsilon_r, \pm\varepsilon_q\varepsilon_r$ nemohou být druhými mocninami a konečně, protože

$$(\pm\varepsilon_p\varepsilon_q\varepsilon_r)^{1+\sigma_p} = -\varepsilon_q^2\varepsilon_r^2,$$

ani jednotku $\pm\varepsilon_p\varepsilon_q\varepsilon_r$ nelze v E odmocnit. Všechna tato tvrzení plynou z faktu, že norma libovolné druhé mocniny je opět druhou mocninou.

Při přechodu ke konkrétním výpočtům bude nyní nutné rozlišit čtyři případy podle toho, jaké zbytky dávají jednotlivá prvočísla p, q, r modulo prvočísla ostatní.

- $\left(\frac{p}{q}\right) = \left(\frac{p}{r}\right) = \left(\frac{q}{r}\right) = -1$
- $\left(\frac{p}{q}\right) = 1,\ \left(\frac{p}{r}\right) = \left(\frac{q}{r}\right) = -1$
- $\left(\frac{p}{q}\right) = \left(\frac{p}{r}\right) = 1,\ \left(\frac{q}{r}\right) = -1$
- $\left(\frac{p}{q}\right) = \left(\frac{p}{r}\right) = \left(\frac{q}{r}\right) = 1$

Ostatní možné případy jsou pouze symetrickými analogiemi těchto čtyř a výsledky, které uvedeme pro tyto možnosti, se na ně dají snadno převést některou permutací těchto prvočísel (neformálně řečeno, důležité je pouze, kolik ze tří čísel $\left(\frac{p}{q}\right), \left(\frac{p}{r}\right), \left(\frac{q}{r}\right)$ je rovno -1 a kolik 1).

Uveďme nyní hlavní výsledek této práce:

Věta 1. *Buďte p, q, r prvočísla, $p, q, r \equiv 1 \pmod 4$. Označme h počet tříd divizorů tělesa $\mathbb{Q}\left(\sqrt{p},\sqrt{q},\sqrt{r}\right)$. Potom pro paritu čísla h platí:*

1. *Je-li $\left(\frac{p}{q}\right) = \left(\frac{p}{r}\right) = \left(\frac{q}{r}\right) = -1$, položme $u_{pq}, u_{pr}, u_{qr} \in \mathbb{Z}$ pevná taková, že $u_{pq}^2 \equiv pq \pmod r$, $u_{pr}^2 \equiv pr \pmod q$, $u_{qr}^2 \equiv qr \pmod p$. Potom je h sudé právě tehdy, když $\left(\frac{u_{pq}}{r}\right)\left(\frac{u_{pr}}{q}\right)\left(\frac{u_{qr}}{p}\right) = -1$.*
2. *V případě $\left(\frac{p}{q}\right) = 1$, $\left(\frac{p}{r}\right) = \left(\frac{q}{r}\right) = -1$ je parita h rovna paritě počtu tříd divizorů tělesa $\mathbb{Q}\left(\sqrt{p},\sqrt{q}\right)$, speciálně je podle Tvrzení 3.1 číslo h sudé právě tehdy, je-li $\left(\frac{u_p}{q}\right) = \left(\frac{u_q}{p}\right)$. Čísla $u_p, u_q \in \mathbb{Z}$ jsou přitom zvolena pevně tak, že $u_p^2 \equiv p \pmod q$ a $u_q^2 \equiv q \pmod p$.*
3. *Je-li $\left(\frac{p}{q}\right) = \left(\frac{q}{r}\right) = 1$, $\left(\frac{p}{r}\right) = -1$, je h sudé číslo.*

4. *Rovněž v případě* $\left(\frac{p}{q}\right) = \left(\frac{p}{r}\right) = \left(\frac{q}{r}\right) = 1$ *je vždy* h *sudé. (Navíc, označíme-li* v_{pq}, v_{pr}, v_{qr}, v_{pqr} *nejvyšší mocniny 2, dělící počty tříd divizorů těles* $\mathbb{Q}\left(\sqrt{p}, \sqrt{q}\right)$, $\mathbb{Q}\left(\sqrt{p}, \sqrt{r}\right)$, $\mathbb{Q}\left(\sqrt{q}, \sqrt{r}\right)$, $\mathbb{Q}\left(\sqrt{p}, \sqrt{q}, \sqrt{r}\right)$, *platí* $v_{pqr} \geqslant 1 + v_{pq} + v_{pr} + v_{qr}$.*)*

Důkaz. Celá zbývající část této kapitoly je věnována důkazu tohoto tvrzení. Dokážeme jej postupně po jednotlivých případech.

Zbytky

Mějme opět $\eta = \pm\varepsilon_p^{x_p}\varepsilon_q^{x_q}\varepsilon_r^{x_r}\beta_{pq}^{x_{pq}}\beta_{pr}^{x_{pr}}\beta_{qr}^{x_{qr}}\beta_{pqr}^{x_{pqr}}$. K tomu, aby jednotka η byla kvadrátem, potřebujeme nalézt podle Tvrzení 2.3 křížový homomorfismus f, splňující $f(\sigma)^2 = \eta^{1-\sigma}$ pro všechna σ z množiny $\{\sigma_p, \sigma_q, \sigma_r\}$. Spočítejme tedy nejprve požadované výrazy $\eta^{1-\sigma}$. Využijeme přitom toho, že podle (6) platí $\beta_{pqr}^{1+\sigma_p} = \beta_{qr}^{1-1} = 1$, neboť v případě kvadratických zbytků je $\mathrm{Frob}(p, \mathbb{Q}\left(\sqrt{q}, \sqrt{r}\right)) = 1$. Podobně i $\beta_{pqr}^{1+\sigma_q} = \beta_{pqr}^{1+\sigma_r} = 1$. S použitím rovnosti (7) tedy dostáváme

$$\begin{aligned}
\eta^{1-\sigma_p} &= (-\varepsilon_p^2)^{x_p} \cdot \left(\beta_{pq}^2 \cdot \chi_q(p)\right)^{x_{pq}} \cdot \left(\beta_{pr}^2 \cdot \chi_r(p)\right)^{x_{pr}} \cdot \left(\beta_{pqr}^2\right)^{x_{pqr}} \\
\eta^{1-\sigma_q} &= (-\varepsilon_q^2)^{x_q} \cdot \left(\beta_{pq}^2 \cdot \chi_p(q)\right)^{x_{pq}} \cdot \left(\beta_{qr}^2 \cdot \chi_r(q)\right)^{x_{qr}} \cdot \left(\beta_{pqr}^2\right)^{x_{pqr}} \\
\eta^{1-\sigma_r} &= (-\varepsilon_r^2)^{x_r} \cdot \left(\beta_{pr}^2 \cdot \chi_p(r)\right)^{x_{pr}} \cdot \left(\beta_{qr}^2 \cdot \chi_q(r)\right)^{x_{qr}} \cdot \left(\beta_{pqr}^2\right)^{x_{pqr}}
\end{aligned}$$

Rozeberme nejprve případ $x_{pqr} = 0$. Z předchozích výpočtů je vidět, že jedinou možností (až na znaménko — viz poznámka za Tvrzením 2.2) jak definovat funkci g, je

$$\begin{aligned}
g(\sigma_p) &= \varepsilon_p^{x_p} \cdot \beta_{pq}^{x_{pq}} \cdot \beta_{pr}^{x_{pr}} \\
g(\sigma_q) &= \varepsilon_q^{x_q} \cdot \beta_{pq}^{x_{pq}} \cdot \beta_{qr}^{x_{qr}} \\
g(\sigma_r) &= \varepsilon_r^{x_r} \cdot \beta_{pr}^{x_{pr}} \cdot \beta_{qr}^{x_{qr}}
\end{aligned}$$

Nyní ze vztahů (4) a (5) v Tvrzení 2.3 odvodíme nutné i postačující podmínky pro to, aby byla η druhou mocninou v E:

$$\begin{aligned}
1 = g(\sigma_p)^{1+\sigma_p} &= (-1)^{x_p} \cdot \chi_q(p)^{x_{pq}} \cdot \chi_r(p)^{x_{pr}} \\
1 = g(\sigma_q)^{1+\sigma_q} &= (-1)^{x_q} \cdot \chi_p(q)^{x_{pq}} \cdot \chi_r(q)^{x_{qr}} \\
1 = g(\sigma_r)^{1+\sigma_r} &= (-1)^{x_r} \cdot \chi_p(r)^{x_{pr}} \cdot \chi_q(r)^{x_{qr}}
\end{aligned} \tag{10}$$

a dále, protože

$$\begin{aligned}
g(\sigma_p)^{1-\sigma_q} &= \chi_p(q)^{x_{pq}}(\beta_{pq}^2)^{x_{pq}} \\
g(\sigma_q)^{1-\sigma_p} &= \chi_q(p)^{x_{pq}}(\beta_{pq}^2)^{x_{pq}},
\end{aligned}$$

máme podmínku

$$\chi_q(p)^{x_{pq}} = \chi_p(q)^{x_{pq}}$$

a pro zbylé dvojice díky symetrii dostáváme analogicky podmínky

$$\begin{aligned}
\chi_r(p)^{x_{pr}} &= \chi_p(r)^{x_{pr}} \\
\chi_r(q)^{x_{qr}} &= \chi_q(r)^{x_{qr}}
\end{aligned} \tag{11}$$

Platí-li $x_{kj} = 1$ pro některá $k, j \in \{p, q, r\}$, pak podle (11) platí $\chi_j(k) = \chi_k(j)$ a podle poznámky za Tvrzením 3.1 je $\pm\beta_{kj}$ nebo $\pm\varepsilon_k\varepsilon_j\beta_{kj}$ odmocnitelná jednotka. Označme tuto jednotku η_{kj}. Ze vztahů (10) je ale vidět, že pak platí

$$\eta = \gamma^2 \prod_{(k,j)} \eta_{kj},$$

kde γ je vhodná jednotka z C a násobí se přes $(k,j) \in \{(p,q),(p,r),(q,r)\}$ taková, že platí $x_{kj} = 1$. Pomocí jednotky η splňující $x_{pqr} = 0$ tedy podgrupu grupy jednotek E s vyšším indexem nedostaneme.

Věnujme se proto případu $x_{pqr} = 1$. Potom je

$$g(\sigma_p) = \varepsilon_p^{x_p} \cdot \beta_{pq}^{x_{pq}} \cdot \beta_{pr}^{x_{pr}} \cdot \beta_{pqr}$$
$$g(\sigma_q) = \varepsilon_q^{x_q} \cdot \beta_{pq}^{x_{pq}} \cdot \beta_{qr}^{x_{qr}} \cdot \beta_{pqr}$$
$$g(\sigma_r) = \varepsilon_r^{x_r} \cdot \beta_{pr}^{x_{pr}} \cdot \beta_{qr}^{x_{qr}} \cdot \beta_{pqr}$$

Tentýž výpočet jako v případě $x_{pqr} = 0$ (protože $\beta_{pqr}^{1+\sigma_p} = \beta_{pqr}^{1+\sigma_q} = \beta_{pqr}^{1+\sigma_r} = 1$) ukazuje, že podmínky pro to, aby funkce f definovaná na základě funkce g podle Tvrzení 2.2 byla křížovým homomorfismem, jsou stejné jako výše uvedené podmínky (10),(11). Odtud plyne, že jednotka $\eta = \pm\beta_{pqr}$ je hledanou odmocnitelnou jednotkou. Libovolná jiná jednotka s $x_{pqr} = 1$, kterou lze v E odmocnit, je již součinem jednotky β_{pqr} s jednotkou, kterou lze odmocnit a která splňuje $x_{pqr} = 0$. Ukázali jsme ale dříve, že mezi jednotkami s $x_{pqr} = 0$ neexistuje odmocnitelná jednotka, která byla nebyla kombinací odmocnitelných jednotek z podtěles tělesa $\mathbb{Q}\big(\sqrt{p}, \sqrt{q}, \sqrt{r}\big)$.

Podle poznámky za Tvrzením 3.1 platí (v označení z formulace věty) $v_{pqr} \geqslant 1 + v_{pq} + v_{pr} + v_{qr}$. Speciálně je vždy $v_{pqr} \geqslant 1$, a tudíž je počet tříd divizorů tělesa $\mathbb{Q}\big(\sqrt{p}, \sqrt{q}, \sqrt{r}\big)$ sudý.

Jeden nezbytek

V tomto případě předpokládáme $\left(\frac{p}{q}\right) = \left(\frac{q}{r}\right) = 1$, $\left(\frac{p}{r}\right) = -1$. Podobně jako v předchozím případě budeme při výpočtech $\eta^{1-\sigma_k}$, kde $k \in \{p,q,r\}$, potřebovat vypočtené hodnoty výrazů $\beta_{pqr}^{1+\sigma_k}$ a $\beta_{kj}^{1+\sigma_k}$, kde $k,j \in \{p,q,r\}$. Je tedy podle (6),(7) a (9)

$$\beta_{pqr}^{1+\sigma_p} = \beta_{qr}^{1-\sigma_r} = \chi_q(r) \cdot \beta_{qr}^2$$
$$\beta_{pqr}^{1+\sigma_q} = \beta_{pr}^{1-1} = 1$$
$$\beta_{pqr}^{1+\sigma_r} = \beta_{pq}^{1-\sigma_p} = \chi_q(p) \cdot \beta_{pq}^2$$

Nyní můžeme spočítat jednotlivá $\eta^{1-\sigma_k}$:

$$\eta^{1-\sigma_p} = (-\varepsilon_p^2)^{x_p} \cdot \Big(\beta_{pq}^2 \cdot \chi_q(p)\Big)^{x_{pq}} \cdot \Big(\alpha(r,p)\,\varepsilon_r^{-1}\beta_{pr}^2\Big)^{x_{pr}} \cdot \Big(\chi_q(r) \cdot \beta_{qr}^{-2}\beta_{pqr}^2\Big)^{x_{pqr}}$$
$$\eta^{1-\sigma_q} = (-\varepsilon_q^2)^{x_q} \cdot \Big(\beta_{pq}^2 \cdot \chi_p(q)\Big)^{x_{pq}} \cdot \Big(\beta_{qr}^2 \cdot \chi_r(q)\Big)^{x_{qr}} \cdot \big(\beta_{pqr}^2\big)^{x_{pqr}}$$
$$\eta^{1-\sigma_r} = (-\varepsilon_r^2)^{x_r} \cdot \Big(\beta_{qr}^2 \cdot \chi_q(r)\Big)^{x_{qr}} \cdot \Big(\alpha(p,r)\,\varepsilon_p^{-1}\beta_{pr}^2\Big)^{x_{pr}} \cdot \Big(\chi_q(p) \cdot \beta_{pq}^{-2}\beta_{pqr}^2\Big)^{x_{pqr}}$$

Podíváme-li se na výrazy $\eta^{1-\sigma_p}$ a $\eta^{1-\sigma_r}$, je vidět, že nutnou podmínkou toho, aby η mohlo být kvadrátem, je $x_{pr} = 0$. (V případě, že je $x_{pr} = 1$, nemůže být zřejmě např. $\eta^{1-\sigma_p}$ kvadrátem při libovolné další volbě epxonentů. Jak jsme totiž uvedli dříve $\pm\varepsilon_r^{-1}$ není druhou mocninou a všechny ostatní případné činitele v zápisu $\eta^{1-\sigma_p}$ jsou — případně až na znaménko — druhými mocninami.) V následujících výpočtech, vztahujících se k tomuto případu tedy vždy klademe $x_{pr} = 0$.

Věnujme se opět nejprve případu $x_{pqr} = 0$. Tak jako v případě kvadratických zbytků je jedinou možností, jak definovat hledaný křížový homomorfismus f (pomocí funkce g na množině $\{\sigma_p, \sigma_q, \sigma_r\}$) tato:

$$g(\sigma_p) = \varepsilon_p^{x_p} \cdot \beta_{pq}^{x_{pq}}$$
$$g(\sigma_q) = \varepsilon_q^{x_q} \cdot \beta_{pq}^{x_{pq}} \cdot \beta_{qr}^{x_{qr}}$$
$$g(\sigma_r) = \varepsilon_r^{x_r} \cdot \beta_{qr}^{x_{qr}}$$

Využitím vztahů (4) a (5) dostaneme podmínky pro to, aby byla jednotka η kvadrátem v E. Počítejme nejprve podmínku (4):

$$\begin{aligned} 1 = g(\sigma_p)^{1+\sigma_p} &= (-1)^{x_p} \cdot \chi_q(p)^{x_{pq}} \\ 1 = g(\sigma_q)^{1+\sigma_q} &= (-1)^{x_q} \cdot \chi_p(q)^{x_{pq}} \cdot \chi_r(q)^{x_{qr}} \\ 1 = g(\sigma_r)^{1+\sigma_r} &= (-1)^{x_r} \cdot \chi_q(r)^{x_{qr}} \end{aligned} \tag{12}$$

Dále, protože

$$\begin{aligned} g(\sigma_p)^{1-\sigma_q} &= \chi_p(q)^{x_{pq}} \cdot (\beta_{pq}^2)^{x_{pq}} \\ g(\sigma_q)^{1-\sigma_p} &= \chi_q(p)^{x_{pq}} \cdot (\beta_{pq}^2)^{x_{pq}} \\ g(\sigma_q)^{1-\sigma_r} &= \chi_q(r)^{x_{qr}} \cdot (\beta_{qr}^2)^{x_{qr}} \\ g(\sigma_r)^{1-\sigma_q} &= \chi_r(q)^{x_{qr}} \cdot (\beta_{qr}^2)^{x_{qr}} \\ g(\sigma_p)^{1-\sigma_r} &= 1 \\ g(\sigma_r)^{1-\sigma_p} &= 1, \end{aligned}$$

dostáváme podle (5) podmínky

$$\chi_p(q)^{x_{pq}} = \chi_q(p)^{x_{pq}} \quad \text{a} \quad \chi_q(r)^{x_{qr}} = \chi_r(q)^{x_{qr}}. \tag{13}$$

Dosadíme-li teď tyto rovnosti do podmínek (12), máme

$$\begin{aligned} 1 = g(\sigma_p)^{1+\sigma_p} &= (-1)^{x_p} \cdot \chi_q(p)^{x_{pq}} \\ 1 = g(\sigma_q)^{1+\sigma_q} &= (-1)^{x_q} \cdot \chi_q(p)^{x_{pq}} \cdot \chi_r(q)^{x_{qr}} \\ 1 = g(\sigma_r)^{1+\sigma_r} &= (-1)^{x_r} \cdot \chi_r(q)^{x_{qr}} \end{aligned}$$

Z požadavku, aby η nepatřila do žádného z podtěles tělesa $\mathbb{Q}(\sqrt{p}, \sqrt{q}, \sqrt{r})$ řádu 4, nyní plyne, že jak x_{pq}, tak x_{qr} jsou nenulové, tedy rovny jedné. Potom ovšem z podmínek (13) plyne $\chi_p(q) = \chi_q(p)$ a $\chi_r(q) = \chi_q(r)$. Podle Tvrzení 3.1 pak existuje odmocnitelná jednotka v $\mathbb{Q}(\sqrt{p}, \sqrt{q})$ i v $\mathbb{Q}(\sqrt{q}, \sqrt{r})$ a je snadné vidět, že jednotka vyhovující našim podmínkám je právě součin těchto dvou jednotek (případně zbavený čtverce ε_q^2). Jednotka η, splňující $x_{pqr} = 0$, kterou lze v E odmocnit a která by nebyla kombinací jednotek z bikvadratických podtěles, tedy neexistuje.

Buď nyní $x_{pqr} = 1$. Zřejmě stačí najít jedinou jednotku tohoto tvaru, kterou lze odmocnit, ostatní jsou součinem této jednotky a jednotek, které šly odmocnit v podtělesech řádu 4. Rozepišme nyní (jediný možný) tvar funkce g:

$$\begin{aligned} g(\sigma_p) &= \varepsilon_p^{x_p} \cdot \beta_{pq}^{x_{pq}} \cdot \beta_{qr}^{-1} \cdot \beta_{pqr} \\ g(\sigma_q) &= \varepsilon_q^{x_q} \cdot \beta_{pq}^{x_{pq}} \cdot \beta_{qr}^{x_{qr}} \cdot \beta_{pqr} \\ g(\sigma_r) &= \varepsilon_r^{x_r} \cdot \beta_{qr}^{x_{qr}} \cdot \beta_{pq}^{-1} \cdot \beta_{pqr} \end{aligned}$$

Potom získáme z (4) následující podmínky:

$$\begin{aligned} 1 = g(\sigma_p)^{1+\sigma_p} &= (-1)^{x_p} \cdot \chi_q(p)^{x_{pq}} \cdot \beta_{qr}^{-2} \cdot \chi_q(r) \cdot \beta_{qr}^2 = (-1)^{x_p} \cdot \chi_q(p)^{x_{pq}} \cdot \chi_q(r) \\ 1 = g(\sigma_q)^{1+\sigma_q} &= (-1)^{x_q} \cdot \chi_p(q)^{x_{pq}} \cdot \chi_r(q)^{x_{qr}} \\ 1 = g(\sigma_r)^{1+\sigma_r} &= (-1)^{x_r} \cdot \chi_q(r)^{x_{qr}} \cdot \beta_{pq}^{-2} \cdot \chi_q(p) \cdot \beta_{pq}^2 = (-1)^{x_r} \cdot \chi_q(r)^{x_{qr}} \cdot \chi_q(p) \end{aligned} \tag{14}$$

Abychom ověřili podmínky (5) z Tvrzení 2.3, spočítáme

$$\begin{aligned} g(\sigma_p)^{1-\sigma_q} &= \chi_p(q)^{x_{pq}} \cdot (\beta_{pq}^2)^{x_{pq}} \cdot \chi_r(q) \cdot \beta_{qr}^{-2} \cdot \beta_{pqr}^2 \\ g(\sigma_q)^{1-\sigma_p} &= \chi_q(p)^{x_{pq}} \cdot (\beta_{pq}^2)^{x_{pq}} \cdot \chi_q(r) \cdot \beta_{qr}^{-2} \cdot \beta_{pqr}^2 \end{aligned}$$

a dostaneme podmínku

$$\chi_p(q)^{x_{pq}} \cdot \chi_r(q) = \chi_q(p)^{x_{pq}} \cdot \chi_q(r) \tag{15}$$

Protože p a r vystupují v tomto případě symetricky, dostáváme podmínku

$$\chi_r(q)^{x_{qr}} \cdot \chi_p(q) = \chi_q(r)^{x_{qr}} \cdot \chi_q(p) \tag{15a}$$

Protože platí

$$\begin{aligned} g(\sigma_p)^{1-\sigma_r} &= \beta_{qr}^{-2} \cdot \chi_q(r) \cdot \chi_q(p) \cdot \beta_{pq}^{-2}\beta_{pqr}^2 \\ g(\sigma_r)^{1-\sigma_p} &= \beta_{pq}^{-2} \cdot \chi_q(p) \cdot \chi_q(r) \cdot \beta_{qr}^{-2}\beta_{pqr}^2 \end{aligned}$$

je rovnost $g(\sigma_p)^{1-\sigma_r} = g(\sigma_r)^{1-\sigma_p}$ v našem případě vždy splněna.

Dáme-li teď dohromady podmínky (14) s (15) a (15a), dostaneme

$$\begin{aligned} 1 &= (-1)^{x_p} \cdot \chi_p(q)^{x_{pq}} \cdot \chi_r(q) \\ 1 &= (-1)^{x_q} \cdot \chi_p(q)^{x_{pq}} \cdot \chi_r(q)^{x_{qr}} \\ 1 &= (-1)^{x_r} \cdot \chi_p(q) \cdot \chi_r(q)^{x_{qr}} \end{aligned}$$

Aby tedy jednotka η byla v E kvadrátem, je podle (15) a (15a) nutné, aby

$$\chi_q(r) = \chi_r(q) \iff \chi_q(p) = \chi_p(q).$$

Navíc, pokud $\chi_q(r) \neq \chi_r(q)$ a $\chi_q(p) \neq \chi_p(q)$, nutně $x_{pq} = x_{qr} = 1$ a rovněž $x_p = x_q = x_r$, kde $(-1)^{x_p} = \chi_p(q) \cdot \chi_r(q)$. Pokud $\chi_q(r) = \chi_r(q)$ a stejně tak $\chi_q(p) = \chi_p(q)$, volme $x_{pq} = x_{qr} = 0, x_q = 0, (-1)^{x_p} = \chi_r(q)$ a $(-1)^{x_r} = \chi_p(q)$. Pak jsou všechny předchozí podmínky splněny, je tedy splněna postačující podmínka existence odmocnitelné jednotky η s příslušnými, výše popsanými hodnotami exponentů. Pokud $\chi_q(r){\cdot}\chi_r(q) \neq \chi_q(p){\cdot}\chi_p(q)$, pak je nutně jeden z těchto součinů roven 1. Bez újmy na obecnosti můžeme předpokládat, že platí $\chi_q(p) \cdot \chi_p(q)$. Pak ovšem podle poznámky za Tvrzením 3.1 existuje odmocnitelná jednotka již v tělese $\mathbb{Q}\left(\sqrt{p}, \sqrt{r}\right)$. Protože požadovaná odmocnitelná jednotka v tomto případě existuje vždy, dokázali jsme pro případ $\left(\frac{p}{q}\right) = \left(\frac{q}{r}\right) = 1$, $\left(\frac{p}{r}\right) = -1$ tvrzení věty, tedy že počet tříd divizorů je v tomto případě vždy sudý.

Dva nezbytky

V tomto případě předpokládáme $\left(\frac{p}{q}\right) = 1, \left(\frac{p}{r}\right) = \left(\frac{q}{r}\right) = -1$. Hledejme opět v E jednotku η, kterou lze odmocnit, ve tvaru $\eta = \pm\varepsilon_p^{x_p}\varepsilon_q^{x_q}\varepsilon_r^{x_r}\beta_{pq}^{x_{pq}}\beta_{pr}^{x_{pr}}\beta_{qr}^{x_{qr}}\beta_{pqr}^{x_{pqr}}$, kde všechny exponenty patří do množiny $\{0,1\}$. Buď nejprve $x_{pqr} = 0$. Potom s využitím vztahů (7) a (9) dostáváme

$$\begin{aligned} \eta^{1-\sigma_p} &= (-\varepsilon_p^2)^{x_p} \cdot \left(\beta_{pq}^2 \cdot \chi_q(p)\right)^{x_{pq}} \cdot \left(\alpha(r,p)\,\varepsilon_r^{-1}\beta_{pr}^2\right)^{x_{pr}} \\ \eta^{1-\sigma_q} &= (-\varepsilon_q^2)^{x_q} \cdot \left(\beta_{pq}^2 \cdot \chi_p(q)\right)^{x_{pq}} \cdot \left(\alpha(r,q)\,\varepsilon_r^{-1}\beta_{qr}^2\right)^{x_{qr}} \\ \eta^{1-\sigma_r} &= (-\varepsilon_r^2)^{x_r} \cdot \left(\alpha(p,r)\,\varepsilon_p^{-1}\beta_{pr}^2\right)^{x_{pr}} \cdot \left(\alpha(q,r)\,\varepsilon_q^{-1}\beta_{qr}^2\right)^{x_{qr}} \end{aligned}$$

Nutnou podmínkou toho, aby η byla druhou mocninou v E je požadavek, aby všechny tři výrazy byly rovněž v E druhými mocninami. Rozeberme nejprve výraz $\eta^{1-\sigma_p}$. Má-li být v E druhou mocninou, musí být $x_{pr} = 0$, protože jinak bude jedním z činitelů, vystupujících v zápise $\eta^{1-\sigma_p}$ jednotka $\pm\varepsilon_r^{-1}$, kterou ale nelze odmocnit a ostatními činiteli budou (až na znaménko) druhé mocniny jednotek v E. Stejnou úvahou pro výraz $\eta^{1-\sigma_q}$ dostáváme nutnou podmínku $x_{qr} = 0$. Nyní, aby i $\eta^{1-\sigma_r}$ byla druhou mocninou v E, musí být $x_r = 0$ (jinak by $\eta^{1-\sigma_r} = (-\varepsilon_r^2)$ a to není druhá mocnina v E, protože ani -1 není druhou mocninou). To ale znamená $\eta^{1-\sigma_r} = 1$, neboli $\eta^{\sigma_r} = \eta$, je tedy η prvkem tělesa $\mathbb{Q}\big(\sqrt{p}, \sqrt{q}\big)$ a tento případ je již vyřešen v Tvrzení 3.1.

Uvažme nyní případ $x_{pqr} = 1$. Podle (6),(7) a (9) máme $\beta_{pqr}^{1+\sigma_p} = \beta_{qr}^{1-\sigma_r} = \alpha(q,r)\,\varepsilon_q^{-1}\beta_{qr}^2$ a tedy

$$\eta^{1-\sigma_p} = (-\varepsilon_p^2)^{x_p} \cdot \Big(\beta_{pq}^2 \cdot \chi_q(p)\Big)^{x_{pq}} \cdot \Big(\alpha(r,p)\,\varepsilon_r^{-1}\beta_{pr}^2\Big)^{x_{pr}} \cdot \Big(\alpha(q,r)\,\varepsilon_q\beta_{qr}^{-2}\beta_{pqr}^2\Big)$$

Nejprve si uvědomme, že jednotka $\pm\varepsilon_q\varepsilon_r^{-1}$ není v E druhou mocninou (kdyby byla, pak je druhou mocninou i $\pm\varepsilon_q\varepsilon_r^{-1}\cdot\varepsilon_r^2 = \pm\varepsilon_q\varepsilon_r$, ta ale není podle poznámky v úvodu kapitoly). Nyní ale vidíme, že nelze zvolit hodnoty x_p, x_{pq} a x_{pr} tak, aby $\eta^{1-\sigma_p}$ byla kvadrátem v E. Dokázali jsme tedy, že v tělese $\mathbb{Q}\big(\sqrt{p}, \sqrt{q}, \sqrt{r}\big)$ neexistuje odmocnitelná jednotka požadovaného tvaru, která by nebyla prvkem tělesa $\mathbb{Q}\big(\sqrt{p}, \sqrt{q}\big)$ (v tělesech $\mathbb{Q}\big(\sqrt{p}, \sqrt{r}\big)$ a $\mathbb{Q}\big(\sqrt{q}, \sqrt{r}\big)$ žádná taková neexistuje) a proto je parita počtu tříd divizorů tělesa $\mathbb{Q}\big(\sqrt{p}, \sqrt{q}, \sqrt{r}\big)$ stejná jako u tělesa $\mathbb{Q}\big(\sqrt{p}, \sqrt{q}\big)$.

Tři nezbytky

I v tomto případě budeme hledat nutné a postačující podmínky toho, že lze v grupě E odmocnit jednotku tvaru $\eta = \pm\varepsilon_p^{x_p}\varepsilon_q^{x_q}\varepsilon_r^{x_r}\beta_{pq}^{x_{pq}}\beta_{pr}^{x_{pr}}\beta_{qr}^{x_{qr}}\beta_{pqr}^{x_{pqr}}$, kde všechny exponenty jsou prvky množiny $\{0,1\}$. Za tímto účelem spočítáme nejprve hodnoty výrazů $\eta^{1-\sigma_p}, \eta^{1-\sigma_q}, \eta^{1-\sigma_r}$ v případě, kdy $\left(\frac{p}{q}\right) = \left(\frac{p}{r}\right) = \left(\frac{q}{r}\right) = -1$. Přitom je nutné spočítat jen jeden z těchto výrazů, ostatní dostaneme díky symetrii pomocí cyklické záměny p, q a r. Spočítejme např.

$$\eta^{1-\sigma_p} = \Big(\varepsilon_p^{1-\sigma_p}\Big)^{x_p}\Big(\beta_{pq}^{1-\sigma_p}\Big)^{x_{pq}}\Big(\beta_{pr}^{1-\sigma_p}\Big)^{x_{pr}}\Big(\beta_{pqr}^{1-\sigma_p}\Big)^{x_{pqr}}.$$

Před vlastním výpočtem vypočtěme nejprve výraz $\beta_{pqr}^{1-\sigma_p}$. Podle vztahu (6) máme

$$\beta_{pqr}^{1-\sigma_p} = \beta_{pqr}^2 \cdot \Big(\beta_{pqr}^{1+\sigma_p}\Big)^{-1} = \beta_{pqr}^2 \cdot \Big(\beta_{qr}^{1-\sigma_q\sigma_r}\Big)^{-1}.$$

Přitom podle (9) platí

$$\begin{aligned}
\beta_{qr}^{1-\sigma_q\sigma_r} &= \beta_{qr}^{1-\sigma_q}\Big(\beta_{qr}^{1-\sigma_r}\Big)^{\sigma_q} = \beta_{qr}^2\cdot\alpha(r,q)\cdot\varepsilon_r^{-1}\cdot\Big(\beta_{qr}^2\cdot\alpha(q,r)\cdot\varepsilon_q^{-1}\Big)^{\sigma_q} = \\
&= \alpha(r,q)\cdot\alpha(q,r)\cdot\varepsilon_r^{-1}\cdot\varepsilon_q^{-\sigma_q}\cdot\Big(\beta_{qr}^{1+\sigma_q}\Big)^2 = \\
&= \alpha(r,q)\cdot\alpha(q,r)\cdot\varepsilon_r^{-1}(-\varepsilon_q)\cdot(\alpha(r,q)\,\varepsilon_r)^2 = -\alpha(r,q)\cdot\alpha(q,r)\,\varepsilon_q\varepsilon_r.
\end{aligned}$$

Celkem tedy máme

$$\beta_{pqr}^{1-\sigma_p} = -\alpha(r,q)\cdot\alpha(q,r)\,\varepsilon_q^{-1}\varepsilon_r^{-1}\cdot\beta_{pqr}^2 \tag{16}$$

a

$$\begin{aligned}
&\eta^{1-\sigma_p} = \\
&= (-\varepsilon_p^2)^{x_p}\cdot\Big(\alpha(q,p)\,\varepsilon_q^{-1}\beta_{pq}^2\Big)^{x_{pq}}\Big(\alpha(r,p)\,\varepsilon_r^{-1}\beta_{pr}^2\Big)^{x_{pr}}\Big(-\alpha(r,q)\cdot\alpha(q,r)\,\varepsilon_q^{-1}\varepsilon_r^{-1}\cdot\beta_{pqr}^2\Big)^{x_{pqr}}.
\end{aligned}$$

Jak jsme předeslali, cyklickou záměnou p, q a r dostaneme vztahy

$$\begin{aligned}
&\eta^{1-\sigma_q} = \\
&= (-\varepsilon_q^2)^{x_q} \cdot \Big(\alpha(p,q)\,\varepsilon_p^{-1}\beta_{pq}^2\Big)^{x_{pq}} \Big(\alpha(r,q)\,\varepsilon_r^{-1}\beta_{qr}^2\Big)^{x_{qr}} \Big(-\alpha(r,p)\cdot\alpha(p,r)\,\varepsilon_p^{-1}\varepsilon_r^{-1}\cdot\beta_{pqr}^2\Big)^{x_{pqr}} \\
&\eta^{1-\sigma_r} = \\
&= (-\varepsilon_r^2)^{x_r} \cdot \Big(\alpha(p,r)\,\varepsilon_p^{-1}\beta_{pr}^2\Big)^{x_{pr}} \Big(\alpha(q,r)\,\varepsilon_q^{-1}\beta_{qr}^2\Big)^{x_{qr}} \Big(-\alpha(q,p)\cdot\alpha(p,q)\,\varepsilon_p^{-1}\varepsilon_q^{-1}\cdot\beta_{pqr}^2\Big)^{x_{pqr}}.
\end{aligned}$$

Rozeberme nejprve případ $x_{pqr} = 0$. Potřebujeme zvolit příslušné hodnoty exponentů tak, aby výrazy $\eta^{1-\sigma_p}, \eta^{1-\sigma_q}, \eta^{1-\sigma_r}$ byly druhými mocninami v grupě jednotek E, přitom aby byly různé od 1. Z uvedeného rozkladu jednotky $\eta^{1-\sigma_p}$ je vidět, že

$$\eta^{1-\sigma_p} = \nu^2 \cdot (\pm(\varepsilon_q^{-1})^{x_{pq}} \cdot (\varepsilon_r^{-1})^{x_{pr}}),$$

pro vhodnou jednotku ν, což ale podle poznámky na začátku této kapitoly není v E druhá mocnina kromě případu $x_{pq} = x_{pr} = 0$. V tom případě ovšem musí být i $x_p = 0$ a je $\eta^{1-\sigma_p} = 1$, což znamená, že $\eta \in \mathbb{Q}(\sqrt{q}, \sqrt{r})$ a není tedy námi požadovanou jednotkou.

Buď nyní $x_{pqr} = 1$. Potom je ze stejného důvodu jako v předchozím odstavci nutné, aby $x_{pq} = x_{pr} = 1$. Použitím stejného argumentu pro výraz $\eta^{1-\sigma_q}$ dostáváme navíc i $x_{qr} = 1$. Hledaná jednotka η je tedy tvaru

$$\eta = \pm\varepsilon_p^{x_p}\varepsilon_q^{x_q}\varepsilon_r^{x_r}\beta_{pq}\beta_{pr}\beta_{qr}\beta_{pqr}.$$

Poté, co jsme získali toto upřesnění tvaru jednotky η, můžeme zapsat $\eta^{1-\sigma_p}$ takto:

$$\begin{aligned}
\eta^{1-\sigma_p} &= (-\varepsilon_p^2)^{x_p} \cdot \Big(\alpha(q,p)\,\varepsilon_q^{-1}\beta_{pq}^2\Big)\Big(\alpha(r,p)\,\varepsilon_r^{-1}\beta_{pr}^2\Big)\Big(-\alpha(r,q)\cdot\alpha(q,r)\,\varepsilon_q^{-1}\varepsilon_r^{-1}\cdot\beta_{pqr}^2\Big) = \\
&= (-1)\cdot(-\varepsilon_p^2)^{x_p}\cdot\big(\alpha(q,p)\cdot\alpha(q,r)\big)\cdot\big(\alpha(r,p)\cdot\alpha(r,q)\big)\cdot\varepsilon_q^{-2}\varepsilon_r^{-2}\beta_{pq}^2\beta_{pr}^2\beta_{pqr}^2,
\end{aligned}$$

a tedy podle Tvrzení 2.6 dostáváme

$$\eta^{1-\sigma_p} = (-1)\cdot(-\varepsilon_p^2)^{x_p}\cdot\chi_q(pr)\cdot\chi_r(pq)\cdot\varepsilon_q^{-2}\varepsilon_r^{-2}\beta_{pq}^2\beta_{pr}^2\beta_{pqr}^2.$$

Označíme-li ještě pro zkrácení zápisu $s_p = \chi_r(pq)\cdot\chi_q(pr)$, $s_q = \chi_r(pq)\cdot\chi_p(qr)$, $s_r = \chi_q(pr)\cdot\chi_p(qr)$, můžeme psát

$$\begin{aligned}
\eta^{1-\sigma_p} &= (-\varepsilon_p^2)^{x_p}\cdot(-s_p)\cdot\varepsilon_q^{-2}\varepsilon_r^{-2}\beta_{pq}^2\beta_{pr}^2\beta_{pqr}^2 \\
\eta^{1-\sigma_q} &= (-\varepsilon_q^2)^{x_q}\cdot(-s_q)\cdot\varepsilon_p^{-2}\varepsilon_r^{-2}\beta_{pq}^2\beta_{qr}^2\beta_{pqr}^2\ . \\
\eta^{1-\sigma_r} &= (-\varepsilon_r^2)^{x_r}\cdot(-s_r)\cdot\varepsilon_p^{-2}\varepsilon_q^{-2}\beta_{pr}^2\beta_{qr}^2\beta_{pqr}^2
\end{aligned}$$

Je zřejmé, že nutnými podmínkami pro to, aby η mohla být v E kvadrátem, jsou

$$\begin{aligned}
(-1)^{x_p} &= -s_p \\
(-1)^{x_q} &= -s_q \\
(-1)^{x_r} &= -s_r
\end{aligned} \tag{17}$$

Dále si uvědomme, že čísla s_p, s_q, s_r nabývají pouze hodnot ± 1 a platí pro ně identita $s_p \cdot s_q = s_r$. Z toho je vidět, že hodnotu -1 musí nabývat sudý počet z těchto tří čísel, tedy buď jsou všechna s rovna jedné nebo je rovno jedné právě jedno z nich. Podle tohoto kritéria nyní rozdělíme naše úvahy na dva případy.

1) Platí $\mathbf{s_p = s_q = s_r = 1}$

Z podmínek (17), uvedených v předchozím odstavci, nyní plyne, že $x_p = x_q = x_r = 1$. Pokusme se opět najít funkci $g : \{\sigma_p, \sigma_q, \sigma_r\} \to \mathbb{Q}\left(\sqrt{p}, \sqrt{q}, \sqrt{r}\right)$ tak, aby splňovala podmínky (4) a (5) z Tvrzení 2.3. Zřejmě jediným možným způsobem (až na znaménko, které však nehraje roli) jak g definovat, je následující:

$$\begin{aligned} g(\sigma_p) &= \varepsilon_p \varepsilon_q^{-1} \varepsilon_r^{-1} \beta_{pq} \beta_{pr} \beta_{pqr} \\ g(\sigma_q) &= \varepsilon_p^{-1} \varepsilon_q \varepsilon_r^{-1} \beta_{pq} \beta_{qr} \beta_{pqr} \\ g(\sigma_r) &= \varepsilon_p^{-1} \varepsilon_q^{-1} \varepsilon_r \beta_{pr} \beta_{qr} \beta_{pqr} \end{aligned}$$

Ověřme nejprve podmínku (4). Zřejmě stačí testovat pouze $g(\sigma_p)$, protože všechny podmínky, kladené v tomto případě na čísla p, q, r, jsou symetrické. Podle (2),(9) a (16) tedy máme

$$\begin{aligned} g(\sigma_p)^{1+\sigma_p} &= \varepsilon_p^{1+\sigma_p} \varepsilon_q^{-2} \varepsilon_r^{-2} \beta_{pq}^{1+\sigma_p} \beta_{pr}^{1+\sigma_p} \beta_{pqr}^{1+\sigma_p} = \\ &= (-1) \cdot \varepsilon_q^{-2} \varepsilon_r^{-2} \cdot \big(\alpha(q,p)\, \varepsilon_q\big)\big(\alpha(r,p)\, \varepsilon_r\big) \cdot \big(-\alpha(r,q)\, \varepsilon_r \cdot \alpha(q,r)\, \varepsilon_q\big) = s_p, \end{aligned} \tag{18}$$

což je podle předpokladu rovno 1. Stejně se dokáže, že za daných předpokladů je $g(\sigma_q)^{1+\sigma_q} = g(\sigma_r)^{1+\sigma_r} = 1$.

Věnujme se nyní podmínce (5). Opět ji stačí ověřit pro dvojici automorfismů σ_p, σ_q, pro zbylé dvě dvojice dostaneme výsledek cyklickou záměnou p, q a r. Potřebujeme tedy spočítat výrazy $g(\sigma_p)^{1-\sigma_q}$ a $g(\sigma_q)^{1-\sigma_p}$ a udat podmínku, za které si jsou rovny.

$$\begin{aligned} g(\sigma_p)^{1-\sigma_q} &= \left(\varepsilon_q^{1-\sigma_q}\right)^{-1} \left(\beta_{pq}^{1-\sigma_q}\right) \left(\beta_{pqr}^{1-\sigma_q}\right) = \\ &= \left(-\varepsilon_q^{-2}\right) \cdot \left(\beta_{pq}^2 \alpha(p,q)\, \varepsilon_p^{-1}\right) \cdot \left(-\alpha(p,r)\alpha(r,p)\, \varepsilon_p^{-1} \varepsilon_r^{-1} \beta_{pqr}^2\right) = \\ &= \varepsilon_p^{-2} \varepsilon_q^{-2} \varepsilon_r^{-1} \beta_{pq}^2 \cdot \chi_p(qr) \cdot \alpha(r,p) \cdot \beta_{pqr}^2 \end{aligned} \tag{19}$$

Symetricky

$$g(\sigma_q)^{1-\sigma_p} = \varepsilon_p^{-2} \varepsilon_q^{-2} \varepsilon_r^{-1} \beta_{pq}^2 \cdot \chi_q(pr) \cdot \alpha(r,q) \cdot \beta_{pqr}^2.$$

Potom platí $g(\sigma_p)^{1-\sigma_q} = g(\sigma_q)^{1-\sigma_p}$ právě tehdy, když $\chi_p(qr) \cdot \alpha(r,p) = \chi_q(pr) \cdot \alpha(r,q)$. Protože ale z $s_r = 1$ plyne $\chi_p(qr) = \chi_q(pr)$, musí platit $\alpha(r,p) = \alpha(r,q)$, což znamená podle Tvrzení 2.6, že $\chi_r(pq) = -1$.

Jak jsme již poznamenali, všechny výpočty lze provést cyklicky i pro zbylé podmínky a dostaneme $\chi_q(pr) = \chi_p(qr) = -1$. Jsou-li tedy splněny tyto podmínky, pak podle Tvrzení 2.3 je $\eta = \pm\varepsilon_p \varepsilon_q \varepsilon_r \beta_{pq} \beta_{pr} \beta_{qr} \beta_{pqr}$ v E druhou mocninou jednotky.

2) Právě jedno z čísel $\mathbf{s_p, s_q, s_r}$ je rovno 1

Bez újmy na obecnosti lze (díky symetrii) předpokládat, že $s_p = 1, s_q = s_r = -1$. Potom podle podmínek (17) platí $x_p = 1, x_q = 0, x_r = 0$. Hodnoty funkce g v $\sigma_p, \sigma_q, \sigma_r$ jsou pak určeny následovně:

$$\begin{aligned} g(\sigma_p) &= \varepsilon_p \varepsilon_q^{-1} \varepsilon_r^{-1} \beta_{pq} \beta_{pr} \beta_{pqr} \\ g(\sigma_q) &= \varepsilon_p^{-1} \varepsilon_r^{-1} \beta_{pq} \beta_{qr} \beta_{pqr} \\ g(\sigma_r) &= \varepsilon_p^{-1} \varepsilon_q^{-1} \beta_{pr} \beta_{qr} \beta_{pqr} \end{aligned}$$

Poznamenejme opět, že v tomto případě vůči sobě vystupují symetricky q a r. V dalším proto budeme výpočty redukovat a pro r odvodíme, kdykoli to bude potřebné, vztahy z odpovídajících vztahů pro q.

Ověřme nejprve podmínku (4). Je třeba dokázat, že

$$g(\sigma_p)^{1+\sigma_p} = g(\sigma_q)^{1+\sigma_q} = g(\sigma_r)^{1+\sigma_r} = 1$$

. Vztah $g(\sigma_p)^{1+\sigma_p} = 1$ plyne z výpočtu téže podmínky v předešlém případě (viz (18)), neboť hodnoty $g(\sigma_p)$ jsou v obou těchto případech stejné. Počítejme nyní $g(\sigma_q)^{1+\sigma_q}$. Využijeme i nyní výpočtu (18) a dostaneme

$$\big(g(\sigma_q)\varepsilon_q)\big)^{1+\sigma_q} = s_q.$$

Protože ale $\varepsilon_q^{1+\sigma_q} = -1$ a $s_q = -1$, je i v tomto případě $g(\sigma_q)^{1+\sigma_q} = 1$. Symetricky i $g(\sigma_r)^{1+\sigma_r} = 1$.

Nyní ověřme podmínku (5). Ukážeme nejprve podmínky, za kterých bude platit rovnost $g(\sigma_p)^{1-\sigma_q} = g(\sigma_q)^{1-\sigma_p}$, z toho vyvodíme díky symetrii podmínky pro rovnost $g(\sigma_p)^{1-\sigma_r} = g(\sigma_r)^{1-\sigma_p}$ a pak vyjádříme podmínky pro $g(\sigma_q)^{1-\sigma_r} = g(\sigma_r)^{1-\sigma_q}$. Podle (19) máme

$$g(\sigma_p)^{1-\sigma_q} = \varepsilon_p^{-2}\varepsilon_q^{-2}\varepsilon_r^{-1}\beta_{pq}^2 \cdot \chi_p(qr) \cdot \alpha(r,p) \cdot \beta_{pqr}^2.$$

Podle stejné rovnosti (po příslušné permutaci proměnných) pak máme

$$\big(g(\sigma_q)\varepsilon_q\big)^{1-\sigma_p} = \varepsilon_p^{-2}\varepsilon_q^{-2}\varepsilon_r^{-1}\beta_{pq}^2 \cdot \chi_q(pr) \cdot \alpha(r,q) \cdot \beta_{pqr}^2.$$

Protože $\varepsilon_q^{1-\sigma_p} = 1$, je nutnou a postačující podmínkou požadované rovnosti platnost $\chi_p(qr) \cdot \alpha(r,p) = \chi_q(pr) \cdot \alpha(r,q)$ a protože $\chi_p(qr) \cdot \chi_q(pr) = s_r = -1$, je hledanou podmínkou $\alpha(r,p) = -\alpha(r,q)$, neboli podle Tvrzení 2.6 platnost $\chi_r(pq) = 1$. Analogicky dostáváme díky symetrii podmínku $\chi_q(pr) = 1$.

Hledejme nyní podmínky pro splnění rovnosti

$$g(\sigma_q)^{1-\sigma_r} = g(\sigma_r)^{1-\sigma_q}.$$

S využitím rovnosti (19) dostáváme

$$\big(g(\sigma_q)\,\varepsilon_q\big)^{1-\sigma_r} = \varepsilon_p^{-1}\varepsilon_q^{-2}\varepsilon_r^{-2}\beta_{qr}^2 \cdot \chi_q(pr) \cdot \alpha(p,q) \cdot \beta_{pqr}^2.$$

Podobně

$$\big(g(\sigma_r)\varepsilon_r\big)^{1-\sigma_q} = \varepsilon_p^{-1}\varepsilon_q^{-2}\varepsilon_r^{-2}\beta_{qr}^2 \cdot \chi_r(pq) \cdot \alpha(p,r) \cdot \beta_{pqr}^2.$$

Protože opět $\varepsilon_q^{1-\sigma_r} = \varepsilon_r^{1-\sigma_q} = 1$, dostáváme podmínku $\chi_q(pr) \cdot \alpha(p,q) = \chi_r(pq) \cdot \alpha(p,r)$ a protože $\chi_q(pr) \cdot \chi_r(pq) = s_p = 1$, nutně $\alpha(p,q) = \alpha(p,r)$, neboli $\chi_p(qr) = -1$.

Protože nalezené nutné podmínky pro $\chi_r(pq), \chi_q(pr)$ a $\chi_p(qr)$ vyhovují i zadaným hodnotám $s_p = 1, s_q = s_r = -1$, jsou splněny podmínky (5) a je tedy při splnění těchto podmínek podle Tvrzení 2.3 jednotka $\eta = \pm\varepsilon_p\beta_{pq}\beta_{pr}\beta_{qr}\beta_{pqr}$ v grupě jednotek E druhou mocninou.

V obou případech jsme tak dokázali tvrzení věty, týkající se kvadratických nezbytků, přičemž konkrétní formulaci, uvedenou ve Větě 1, dostaneme aplikací Lemmatu 1.1. □

4. Tabulky

V této kapitole uvedeme tabulky všech trojic prvočísel $p, q, r \equiv 1 \pmod 4$ takových, že $p, q, r < 100$. Tabulky budou rozděleny na čtyři části podle vzájemného vztahu těchto prvočísel — totiž, zdali jsou si navzájem kvadratickými zbytky či nikoli. Zároveň uvedeme ve všech případech počet tříd divizorů tělesa $\mathbb{Q}\left(\sqrt{pq}, \sqrt{r}\right)$ vypočtený pomocí Buchmannova subexponenciálního algoritmu. Tento algoritmus je součástí programu PARI-GP verze 1.38, který vytvořili pánové C. Batut, D. Bernardi, H. Cohen a M. Olivier na univerzitě v Bordeaux (viz [1]). Počet tříd divizorů tohoto tělesa uvádíme proto, že je v přímém vztahu s počtem tříd divizorů tělesa $\mathbb{Q}\left(\sqrt{p}, \sqrt{q}, \sqrt{r}\right)$. Z Class Field Theory (viz např. [7, str. 336]) totiž plyne, že počet tříd divizorů tělesa $\mathbb{Q}\left(\sqrt{p}, \sqrt{q}, \sqrt{r}\right)$ je sudý, právě když je počet tříd divizorů tělesa $\mathbb{Q}\left(\sqrt{pq}, \sqrt{r}\right)$ dělitelný číslem 4.

Tři nezbytky

V této části budou uvedena prvočísla $p < q < r < 100$ taková, že $p, q, r \equiv 1 \pmod 4$ a $\left(\frac{p}{q}\right) = \left(\frac{p}{r}\right) = \left(\frac{q}{r}\right) = -1$. Označíme-li dále jako u_{pq}, u_{pr}, u_{qr} taková celá čísla, že $u_{pq}^2 \equiv pq \pmod r$, $u_{pr}^2 \equiv pr \pmod q$, $u_{qr}^2 \equiv qr \pmod p$, víme podle Věty 1, že h je sudé právě tehdy, když $\left(\frac{u_{pq}}{r}\right)\left(\frac{u_{pr}}{q}\right)\left(\frac{u_{qr}}{p}\right) = -1$. V tabulce uvedeme čísla p, q, r, dále čísla $\left(\frac{u_{pq}}{r}\right)$, $\left(\frac{u_{pr}}{q}\right)$, $\left(\frac{u_{qr}}{p}\right)$. Pro srovnání uvedeme počet tříd divizorů h_1 tělesa $\mathbb{Q}\left(\sqrt{pq}, \sqrt{r}\right)$.

p	q	r	$\left(\frac{u_{pq}}{r}\right)$	$\left(\frac{u_{pr}}{q}\right)$	$\left(\frac{u_{qr}}{p}\right)$	h_1
5	13	37	−1	1	1	4
5	13	73	1	−1	1	4
5	13	97	−1	1	−1	2
5	17	37	−1	−1	−1	4
5	17	73	−1	1	−1	2
5	17	97	−1	−1	−1	4
5	37	97	1	−1	−1	2
5	53	73	−1	−1	1	2
13	37	89	−1	−1	1	6
13	37	97	1	1	−1	52
13	41	89	1	1	−1	12
13	41	97	−1	−1	1	2
17	29	37	1	−1	1	4
17	29	41	1	1	1	2
17	29	61	−1	1	−1	2
17	29	73	1	−1	1	4
17	29	97	−1	−1	1	2
17	37	61	−1	1	1	4
17	37	97	1	−1	−1	6
17	41	97	−1	1	−1	6
29	37	61	−1	1	−1	2
29	37	89	−1	1	−1	2
29	37	97	1	−1	1	4
29	41	89	1	1	−1	4
29	41	97	−1	−1	1	2
29	61	89	1	−1	−1	2
37	61	89	1	−1	−1	2

Dva nezbytky

Zde uvedeme v tabulce prvočísla $p, q, r \equiv 1 \pmod 4$. Pro tato prvočísla bude platit $\left(\frac{p}{q}\right) = 1$ a $\left(\frac{q}{r}\right) = \left(\frac{p}{r}\right) = -1$. Tato prvočísla uvedeme opět v rozsahu $p, q, r < 100$, přitom díky symetrii stačí uvést případy, splňující $p < q$. Podle Věty 1 je parita počtu tříd divizorů tělesa $\mathbb{Q}\left(\sqrt{p}, \sqrt{q}, \sqrt{r}\right)$ sudá právě tehdy, když $\left(\frac{u_p}{q}\right) = \left(\frac{u_q}{p}\right)$, kde $u_p, u_q \in \mathbb{Z}$ jsou taková, že $u_p^2 \equiv p \pmod q$ a $u_q^2 \equiv q \pmod p$. V tabulce uvedeme kromě čísel p, q, r ještě tato čísla $\left(\frac{u_p}{q}\right)$ a $\left(\frac{u_q}{p}\right)$ a počet tříd divizorů h_1 tělesa $\mathbb{Q}\left(\sqrt{pq}, \sqrt{r}\right)$ vypočtený pomocí programu PARI-GP. Musí tedy platit, že h_1 je dělitelné 4 právě tehdy, když je $\left(\frac{u_p}{q}\right) = \left(\frac{u_q}{p}\right)$.

p	q	r	$\left(\frac{u_p}{q}\right)$	$\left(\frac{u_q}{p}\right)$	h_1
5	29	17	-1	-1	8
5	29	37	-1	-1	8
5	29	73	-1	-1	4
5	29	97	-1	-1	4
5	41	13	-1	1	2
5	41	17	-1	1	2
5	41	53	-1	1	6
5	41	97	-1	1	6
5	61	17	-1	1	10
5	61	37	-1	1	2
5	61	53	-1	1	2
5	89	13	-1	-1	4
5	89	37	-1	-1	8
13	17	5	1	-1	2
13	17	37	1	-1	2
13	17	41	1	-1	2
13	17	73	1	-1	2
13	17	97	1	-1	2
13	29	37	-1	1	2
13	29	41	-1	1	2
13	29	73	-1	1	2
13	29	89	-1	1	2
13	29	97	-1	1	2
13	53	5	1	1	4
13	53	41	1	1	4
13	53	73	1	1	12
13	61	37	1	1	4
13	61	89	1	1	4
17	53	5	-1	-1	8
17	53	41	-1	-1	24
17	53	61	-1	-1	4
17	53	73	-1	-1	8
17	89	29	-1	1	2
17	89	37	-1	1	2
17	89	41	-1	1	2
17	89	61	-1	1	2

p	q	r	$\left(\frac{u_p}{q}\right)$	$\left(\frac{u_q}{p}\right)$	h_1
29	53	41	-1	1	2
29	53	61	-1	1	2
29	53	73	-1	1	2
37	41	13	1	-1	2
37	41	17	1	-1	2
37	41	29	1	-1	2
37	41	89	1	-1	2
37	41	97	1	-1	6
37	53	5	-1	1	6
37	53	61	-1	1	2
37	73	5	1	-1	2
37	73	13	1	-1	18
37	73	17	1	-1	2
37	73	29	1	-1	2
41	61	17	-1	-1	4
41	61	29	-1	-1	4
41	61	53	-1	-1	8
41	61	89	-1	-1	8
41	73	13	1	-1	6
41	73	17	1	-1	6
41	73	29	1	-1	6
41	73	53	1	-1	6
53	89	41	-1	1	6
53	89	61	-1	1	2
53	97	5	-1	1	6
53	97	41	-1	1	2
61	73	17	-1	1	2
61	73	29	-1	1	2
61	73	53	-1	1	2
61	97	17	1	-1	2
61	97	29	1	-1	2
61	97	37	1	-1	2
73	89	13	1	1	4
73	89	29	1	1	12
73	97	5	1	-1	2
73	97	13	1	-1	2
73	97	17	1	-1	2
73	97	29	1	-1	2
89	97	13	-1	1	6
89	97	29	-1	1	10
89	97	37	-1	1	2
89	97	41	-1	1	2

Jeden nezbytek

V této části budou uvedena prvočísla $p, q, r < 100$ taková, že $p, q, r \equiv 1 \pmod 4$ a $\left(\frac{p}{q}\right) = \left(\frac{p}{r}\right) = 1, \left(\frac{q}{r}\right) = -1$. Díky symetrii stačí uvést pouze ty trojice, pro které $q < r$. Podle Věty 1 je v tomto případě parita počtu tříd divizorů h tělesa $\mathbb{Q}\left(\sqrt{p}, \sqrt{q}, \sqrt{r}\right)$ vždy sudá. Podrobněji, zvolíme-li čísla $u_{p,q}, u_{q,p}, u_{p,r}, u_{r,p} \in \mathbb{Z}$ taková, že $u_{p,q}^2 \equiv p \pmod q), u_{q,p}^2 \equiv q \pmod p), u_{p,r}^2 \equiv p \pmod r$ a $u_{r,p}^2 \equiv r \pmod p$ a označíme-li jako v_{pqr} nejvyšší exponent čísla 2, dělící h, platí

$$v_{pqr} \geqslant 1 + \frac{1}{2}\left(\left(\frac{u_{p,q}}{q}\right)\left(\frac{u_{q,p}}{p}\right) + 1\right) \cdot \left(\left(\frac{u_{p,r}}{r}\right)\left(\frac{u_{r,p}}{p}\right) + 1\right).$$

Zejména, platí-li $\left(\frac{u_{p,q}}{q}\right)\left(\frac{u_{q,p}}{p}\right) = \left(\frac{u_{p,r}}{r}\right)\left(\frac{u_{r,p}}{p}\right) = 1$, pak podle Věty 1 platí $8 \mid h$. Kromě těchto čísel uvedeme v tabulce ještě počet tříd divizorů h_1 tělesa $\mathbb{Q}\left(\sqrt{pq}, \sqrt{r}\right)$ vypočtený pomocí programu PARI-GP. Podle předchozích poznámek musí být číslo h_1 v tomto případě vždy dělitelné 4.

p	q	r	$\left(\frac{u_{p,q}}{q}\right)$	$\left(\frac{u_{q,p}}{p}\right)$	$\left(\frac{u_{p,r}}{r}\right)$	$\left(\frac{u_{r,p}}{p}\right)$	h_1
5	29	41	−1	−1	−1	1	4
5	29	61	−1	−1	−1	1	4
5	29	89	−1	−1	−1	−1	32
5	41	89	−1	1	−1	−1	4
5	61	89	−1	1	−1	−1	4
13	17	29	1	−1	−1	1	4
13	17	61	1	−1	1	1	4
13	29	61	−1	1	1	1	4
13	53	61	1	1	1	1	16
17	13	89	1	−1	−1	1	8
29	5	13	1	−1	−1	−1	4
29	5	53	−1	−1	−1	1	4
37	41	53	1	−1	−1	1	4
37	53	73	−1	1	1	−1	4
41	5	37	−1	1	1	−1	4
41	5	73	−1	1	1	−1	8
41	37	61	1	−1	−1	−1	4
53	13	37	1	−1	1	1	8
53	13	89	1	1	−1	1	8
53	13	97	1	1	−1	1	8
53	17	29	1	−1	−1	−1	4
53	17	37	1	−1	−1	−1	4
53	17	97	−1	−1	−1	1	4
53	29	37	1	−1	1	−1	16
53	29	89	−1	1	−1	1	4
53	29	97	−1	1	−1	1	4
53	37	89	−1	1	−1	1	4
53	37	97	−1	1	−1	1	4

p	q	r	$\left(\frac{u_{p,q}}{q}\right)$	$\left(\frac{u_{q,p}}{p}\right)$	$\left(\frac{u_{p,r}}{r}\right)$	$\left(\frac{u_{r,p}}{p}\right)$	h_1
61	5	13	1	1	1	−1	4
61	5	73	−1	1	−1	1	4
61	5	97	−1	1	1	−1	8
61	13	41	−1	−1	1	1	8
61	13	73	1	1	−1	1	8
61	13	97	1	1	1	−1	8
61	41	97	−1	−1	1	−1	4
73	37	61	1	−1	−1	1	4
73	37	89	1	−1	1	1	4
73	37	97	1	−1	1	−1	4
73	41	89	1	−1	1	1	12
73	41	97	1	−1	1	−1	12
73	61	89	−1	1	1	1	4
89	5	17	1	−1	−1	−1	4
89	5	53	1	−1	−1	−1	4
89	5	73	1	1	−1	−1	16
89	5	97	−1	−1	−1	1	12
89	17	73	1	1	1	−1	4
89	17	97	−1	1	−1	1	4
89	53	73	1	1	1	−1	4
97	53	61	−1	1	1	−1	44
97	53	73	−1	1	1	−1	4
97	61	89	1	−1	−1	1	4

Zbytky

V této části budou uvedena prvočísla $p, q, r < 100$ taková, že $p, q, r \equiv 1 \pmod 4$ a $\left(\frac{p}{q}\right) = \left(\frac{p}{r}\right) = \left(\frac{q}{r}\right) = 1$. Díky symetrii stačí uvést pouze ty trojice, pro které $p < q < r$. Označme dále symboly $u_{p,q}, u_{q,p}, u_{p,r}, u_{r,p}, u_{q,r}, u_{r,q}$ taková celá čísla, že platí

$$\forall k, j \in \{p, q, r\}, k \neq j : u_{k,j} \equiv k \pmod j.$$

Podle Věty 1 je počet tříd divizorů h tělesa $\mathbb{Q}\left(\sqrt{p}, \sqrt{q}, \sqrt{r}\right)$ vždy sudý. Podrobněji podle téže věty pro největší exponent 2 dělící h (který značíme v_{pqr}) platí

$$v_{pqr} \geqslant 1 + \#\left\{(k, j) \mid k, j \in \{p, q, r\}, \left(\frac{u_{k,j}}{j}\right) = \left(\frac{u_{j,k}}{k}\right)\right\}.$$

V tabulce uvedeme navíc pro srovnání počet tříd divizorů h_1 tělesa $\mathbb{Q}\left(\sqrt{pq}, \sqrt{r}\right)$ vypočtený pomocí programu PARI-GP. Ten musí být podle poznámky na začátku kapitoly dělitelný čtyřmi.

p	q	r	$\left(\frac{u_{p,q}}{q}\right)$	$\left(\frac{u_{q,p}}{p}\right)$	$\left(\frac{u_{p,r}}{r}\right)$	$\left(\frac{u_{r,p}}{p}\right)$	$\left(\frac{u_{q,r}}{r}\right)$	$\left(\frac{u_{r,q}}{q}\right)$	h_1
5	41	61	−1	1	−1	1	−1	−1	16
13	17	53	1	−1	1	1	−1	−1	8
13	29	53	−1	1	1	1	−1	1	8
17	53	89	−1	−1	−1	1	−1	1	16
37	41	73	1	−1	1	−1	1	−1	16
41	61	73	−1	−1	1	−1	−1	1	8
53	89	97	−1	1	−1	1	−1	1	32
61	73	97	−1	1	1	−1	1	−1	48
73	89	97	1	1	1	−1	−1	1	16

5. Literatura

[1] C. Batut, D. Bernardi, H. Cohen, and M. Olivier. *User's Guide to PARI-GP*, 1995.

[2] Z. I. Borevich and I. R. Shafarevich. *Number Theory.* Academic Press, 1966.

[3] K. Ireland and M. Rosen. *A Classical Introduction to the Modern Number Theory.* Number 84 in Graduate Texts in Mathematics. Springer-Verlag, 1990.

[4] R. Kučera. On the parity of the class number of a biquadratic field. *Journal of Number Theory*, 52(1):43–52, May 1995.

[5] R. Kučera. On the Stickelberger ideal and circular units of a compositum of quadratic fields. *Journal of Number Theory*, 56(1):139–166, Jan. 1996.

[6] B. L. van der Waerden. *Algebra.* Springer-Verlag, 1971.

[7] L. C. Washington. *Introduction to Cyclotomic Fields.* Number 83 in Graduate Texts in Mathematics. Springer-Verlag, 1982.