# On the Parity of the Class Number of the Field $\mathbb{Q}\left(\sqrt{p}, \sqrt{q}, \sqrt{r}\right)$


Michal Bulant

Department of Mathematics, Fakulty of Science, Masaryk University
Janáčkovo nám. 2a, 662 95 Brno, Czech Republic


## 1. Introduction

In the paper [1] R. Kučera determines the parity of the class number of any biquadratic field $\mathbb{Q}\left(\sqrt{p}, \sqrt{q}\right)$, where $p$ and $q$ are different primes, $p \equiv q \equiv 1 \pmod 4$. In this paper we extend methods used in [1] to compute the parity of the class number of the field $\mathbb{Q}\left(\sqrt{p}, \sqrt{q}, \sqrt{r}\right)$, where $p, q$ and $r$ are different primes, all congruent to 1 modulo 4.

We now state our result precisely.

**Theorem.** *Let $p, q$ and $r$ be different primes such that $p, q, r \equiv 1 \pmod 4$. Let $h$ denote the class number of $\mathbb{Q}\left(\sqrt{p}, \sqrt{q}, \sqrt{r}\right)$.*

1. *If $\left(\frac{p}{q}\right) = \left(\frac{p}{r}\right) = \left(\frac{q}{r}\right) = -1$, fix $u_{pq}, u_{pr}, u_{qr} \in \mathbb{Z}$ satisfying $u_{pq}^2 \equiv pq \pmod r$, $u_{pr}^2 \equiv pr \pmod q$, $u_{qr}^2 \equiv qr \pmod p$. Then $h$ is even if and only if $\left(\frac{u_{pq}}{r}\right)\left(\frac{u_{pr}}{q}\right)\left(\frac{u_{qr}}{p}\right) = -1$.*
2. *If $\left(\frac{p}{q}\right) = 1$, $\left(\frac{p}{r}\right) = \left(\frac{q}{r}\right) = -1$, then the parity of $h$ is the same as the parity of the class number of the biquadratic field $\mathbb{Q}\left(\sqrt{p}, \sqrt{q}\right)$.*
3. *If $\left(\frac{p}{q}\right) = \left(\frac{q}{r}\right) = 1$, $\left(\frac{p}{r}\right) = -1$, then $h$ is even.*
4. *If $\left(\frac{p}{q}\right) = \left(\frac{p}{r}\right) = \left(\frac{q}{r}\right) = 1$, then $h$ is even. (Moreover, if we denote by $v_{pq}$, $v_{pr}$, $v_{qr}$, $v_{pqr}$ the highest exponents of 2 dividing the class number of $\mathbb{Q}\left(\sqrt{p}, \sqrt{q}\right)$, $\mathbb{Q}\left(\sqrt{p}, \sqrt{r}\right)$, $\mathbb{Q}\left(\sqrt{q}, \sqrt{r}\right)$, $\mathbb{Q}\left(\sqrt{p}, \sqrt{q}, \sqrt{r}\right)$, respectively, then $v_{pqr} \geqslant 1 + v_{pq} + v_{pr} + v_{qr}$.)*

---

The author was financially supported by the Grant Agency of the Czech Republic, grant “Algebraic and Analytic Methods in Number Theory”, No. 201/97/0433

## 2. Cyclotomic units

From here on fix three different primes $p, q$ and $r$, all congruent to 1 modulo 4. Let $E$ be the group of units in $\mathbb{Q}\left(\sqrt{p}, \sqrt{q}, \sqrt{r}\right)$. Let us denote $\zeta_n = e^{2\pi i/n}$ for any positive integer $n$, and $\xi_n = \zeta_n^{(1+n)/2}$ for any positive odd integer $n$. By $\mathrm{Frob}(l, K)$ we mean the Frobenius automorphism of prime $l$ on a field $K$. For any prime $l$ congruent to 1 modulo 4 let $b_l, c_l$ be such integers that $l - 1 = 2^{b_l} c_l$, where $2 \nmid c_l$, and $b_l \geqslant 2$. For this prime $l$ fix a Dirichlet character modulo $l$ of order $2^{b_l}$, and denote it by $\psi_l$. Let $R_l = \{\rho_l^j \mid 0 \leqslant j < 2^{b_l-2}\}$, and $R_l' = \zeta_{2^{b_l}} R_l$, where $\rho_l = e^{4\pi i c_l/(l-1)}$ $(= \zeta_{2^{b_l-1}})$ is a primitive $2^{b_l-1}$th root of unity. Then $\#R_l = \#R_l' = (l-1)/(4c_l)$ (where $\#S$ denotes the number of elements of the set $S$). Further, let $\chi_l$ be a fixed Dirichlet character modulo $l$ of order 4. Note that for any integer $a$ satisfying $\left(\frac{a}{l}\right) = 1$ the value $\chi_l(a)$ does not depend on the choice of the character $\chi_l$.

Let $J = \{l \in \mathbb{Z} \mid l \text{ is a positive prime congruent to 1 modulo 4}\}$. For any finite subset $S$ of $J$ let (by convention, an empty product is 1)

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

By $\sigma_l$, where $l \in S$, we denote the automorphism determined by $\mathrm{Gal}\left(K_S / K_{S\setminus\{l\}}\right) = \{1, \sigma_l\}$. Let us further define

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

It is easy to see that $\varepsilon_{n_S}$ are units in $K_S$. Let $C$ be the group generated by $-1$ and by all conjugates of $\varepsilon_{n_S}$, where $S \subseteq \{p, q, r\}$. Theorem 1 of [2] states that $\{-1, \varepsilon_p, \varepsilon_q, \varepsilon_r, \varepsilon_{pq}, \varepsilon_{pr}, \varepsilon_{qr}, \varepsilon_{pqr}\}$ is a basis of $C$, and that $[E : C] = 2^4 \cdot h$, where $h$ is the class number of the field $\mathbb{Q}\left(\sqrt{p}, \sqrt{q}, \sqrt{r}\right)$.

In [1] it is proved that $\varepsilon_{pq}, \varepsilon_{pr}, \varepsilon_{qr}$ are squares in $\mathbb{Q}\left(\sqrt{p}, \sqrt{q}, \sqrt{r}\right)$, i.e. there are such units $\beta_{pq}, \beta_{pr}, \beta_{qr}$ in $\mathbb{Q}\left(\sqrt{p}, \sqrt{q}, \sqrt{r}\right)$ that $\varepsilon_{pq} = \beta_{pq}^2, \varepsilon_{pr} = \beta_{pr}^2$, and $\varepsilon_{qr} = \beta_{qr}^2$. The unit $\beta_{pq}$ is defined by the relation $\beta_{pq} = \prod_{a \in M_{pq}} (\xi_{pq}^a - \xi_{pq}^{-a})$, where $M_{pq} = \{a \in \mathbb{Z} \mid 0 < a < pq, \left(\frac{a}{q}\right) = 1, \psi_p(a) \in R_p\}$, and the units $\beta_{pr}, \beta_{qr}$ are defined analogously.

In this paragraph we show that $\varepsilon_{pqr}$ is also a square in $\mathbb{Q}\left(\sqrt{p}, \sqrt{q}, \sqrt{r}\right)$. Let us define $M = \left\{ a \in \mathbb{Z} \mid 0 < a < pqr, \left(\frac{a}{q}\right) = \left(\frac{a}{r}\right) = 1, \psi(a) \in R \right\}$, where $\psi = \psi_p$ and $R = R_p$. For any $a \in \mathbb{Z}$ satisfying $0 < a < pqr$ and $\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right) = \left(\frac{a}{r}\right) = 1$ we have either $a \in M$ or $pqr - a \in M$. Therefore

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

Since $2 \mid \#M$, we can write $\varepsilon_{pqr} = \beta_{pqr}^2$, where

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

Now we have to show that $\beta_{pqr} \in \mathbb{Q}\left(\sqrt{p}, \sqrt{q}, \sqrt{r}\right)$. For, let $\sigma$ be an element of the Galois group $\mathrm{Gal}\left(\mathbb{Q}(\zeta_{pqr}) / \mathbb{Q}\left(\sqrt{p}, \sqrt{q}, \sqrt{r}\right)\right)$. Then there is an integer $k$ such that $\sigma(\zeta_{pqr}) = \zeta_{pqr}^k$. We have $\left(\frac{k}{p}\right) = \left(\frac{k}{q}\right) = \left(\frac{k}{r}\right) = 1$, and

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

and since for any $d \in M$ the number of elements $a$ of the set $M$, such that $\psi(a) = \psi(d)$, is equal to $c(q-1)(r-1)/4$, which is an even integer, we have $\beta_{pqr}^\sigma = \beta_{pqr}$, i.e. $\beta_{pqr} \in \mathbb{Q}\left(\sqrt{p}, \sqrt{q}, \sqrt{r}\right)$.

Thus we have a subgroup of $E$ generated by $\{-1, \varepsilon_p, \varepsilon_q, \varepsilon_r, \beta_{pq}, \beta_{pr}, \beta_{qr}, \beta_{pqr}\}$ of index $h$, which implies that $h$ is even if and only if there are $x_p, x_q, x_r, x_{pq}, x_{pr}, x_{qr}, x_{pqr} \in \{0, 1\}$, such that

$$\eta = |\varepsilon_p^{x_p} \varepsilon_q^{x_q} \varepsilon_r^{x_r} \beta_{pq}^{x_{pq}} \beta_{pr}^{x_{pr}} \beta_{qr}^{x_{qr}} \beta_{pqr}^{x_{pqr}}| \neq 1$$

is a square in $E$.

In this paragraph we show that such $\eta$ can exist only if at least one of $x_{pq}, x_{pr}, x_{qr}, x_{pqr}$ is nonzero. We will use the next statement taken from [2]:

**Lemma 2.1.** *In the notation of the beginning of this section let $S \subseteq J$ finite and $l \in S$. Then*

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

**Remark.** This lemma implies that

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

hence none of $\pm\varepsilon_p, \pm\varepsilon_q, \pm\varepsilon_r$ could be a square in $\mathbb{Q}\left(\sqrt{p}, \sqrt{q}, \sqrt{r}\right)$. Since

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

none of $\pm\varepsilon_p\varepsilon_q, \pm\varepsilon_p\varepsilon_r, \pm\varepsilon_q\varepsilon_r$ could be a square, and finally nor $\pm\varepsilon_p\varepsilon_q\varepsilon_r$ could be a square in $\mathbb{Q}\left(\sqrt{p}, \sqrt{q}, \sqrt{r}\right)$, because

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

## 3. Preliminaries

Using previous notation let $G = \mathrm{Gal}(K_S/\mathbb{Q})$. We say that a function $f : G \to K_S$ is a crossed homomorphism if for all $\sigma, \tau \in G$,

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

Let us further denote by $E_S$ the group of units of the field $K_S$. The following proposition is taken from [2].

**Proposition 3.1.** *Let $\varepsilon \in E_S$ be such that there is a crossed homomorphism $f : G \to K_S$ satisfying $\varepsilon^{1-\sigma} = f(\sigma)^2$ for any $\sigma \in G$. Then $\varepsilon$ or $-\varepsilon$ is a square in $K_S$.*

On the other hand, it is easy to see that if $\varepsilon = \pm\eta^2$ for suitable $\eta \in K_S$, then there is a crossed homomorphism $f : G \to K_S$ satisfying $\varepsilon^{1-\sigma} = f(\sigma)^2$ (put $f(\sigma) = \eta^{1-\sigma}$).

We now want to formulate a weaker condition, which will be useful in testing whether given $\eta \in E_S$ is a square in $E_S$. The following proposition is our first step. Let us notice that $G = \mathrm{Gal}(K_S/\mathbb{Q})$ can be considered as a (multiplicative) vector space over $\mathbb{F}_2$ with basis $\{\sigma_l \mid l \in S\}$.

**Proposition 3.2.** *Let a function $g : \{\sigma_l \mid l \in S\} \to K_S$ satisfies the following conditions:*

$$\forall l \in S: \qquad g(\sigma_l)^{1+\sigma_l} = 1 \tag{1}$$
$$\forall p_1, p_2 \in S: \qquad g(\sigma_{p_1})^{1-\sigma_{p_2}} = g(\sigma_{p_2})^{1-\sigma_{p_1}} \tag{2}$$

*For any positive integer $t$ let $S_t = \{k \in S \mid k < t\}$. Let us define a function $f : G \to K_S^\times$ by*

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

*where $V$ is any subset of $S$. Then $f$ is a crossed homomorphism.*

**Remarks.**

1) $f|_{\{\sigma_l \mid l \in S\}} = g$.
2) It is easy to see that if such $g$ satisfying (1), (2), exists, then these conditions are also satisfied by any function $g_1$, such that $g_1(\sigma_s)/g(\sigma_s) \in \{-1, 1\}$ for each $s \in S$.

We postpone the proof of Proposition 3.2 until we prove some auxiliary lemmas.

**Lemma 3.1.** *If the conditions in Proposition 3.2 hold for $g$, and $f$ is defined in the same way as in Proposition 3.2, then for any automorphism $\tau \in G$ and prime $l \in S$*

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

**Proof.** Let $T \subseteq S$ be such that $\tau = \prod_{t\in T} \sigma_t$. Then

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

Now from the condition (2)

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

□

**Lemma 3.2.** *If the conditions in Proposition 3.2 hold for $g$, and $f$ is defined in the same way as in Proposition 3.2, then for any automorphism $\tau \in G$ and prime $l \in S$*

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

**Proof.** Let $T \subseteq S$ be such that $\tau = \prod_{t\in T} \sigma_t$. Further, let $\rho = \prod_{t\in T\cap S_l} \sigma_t$ a $\omega = \prod_{t\in T\setminus(S_l\cup\{l\})} \sigma_t$. From the definition of $f$ we have

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

Lemma 3.1 implies that

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

If $l \notin T$ then $\tau = \rho\omega$, and using Lemma 3.1 we get

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

Let us consider the second case $l \in T$, i.e. $\tau = \rho\sigma_l\omega$. Then $f(\tau) = f(\tau\sigma_l)f(\sigma_l)^{\tau\sigma_l}$. From the condition (1) follows that $f(\sigma_l)^{-\sigma_l} = f(\sigma_l)$, hence

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

with one more application of Lemma 3.1 □

We are now ready to prove Proposition 3.2.

**Proof of Proposition 3.2.** Let $\sigma, \tau \in G$, and let $V \subseteq S$ be determined by $\sigma = \prod_{s\in V} \sigma_s$. The case $V = \emptyset$ is trivial. Let us suppose that $V \neq \emptyset$, and that for every $T \subsetneqq V$ holds

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

Let $m = \min V, \omega = \prod_{s\in V\setminus\{m\}} \sigma_s$. Then $\sigma = \sigma_m\omega$, and from the definition of $f$ we have $f(\sigma) = f(\sigma_m)f(\omega)^{\sigma_m}$. Lemma 3.2 now yields

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

and the induction hypothesis for $V \setminus \{m\}$ gives

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

Proposition follows. □

We shall now combine Propositions 3.1 and 3.2 into one criterion which will be often useful in the next section.

**Proposition 3.3.** *If there exists a function* $g : \{\sigma_l \mid l \in S\} \to K_S^\times$, *which satisfies* $\varepsilon^{1-\sigma_l} = g(\sigma_l)^2$ *for any* $l \in S$ *and conditions*

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

$$\forall p_1, p_2 \in S: \qquad g(\sigma_{p_1})^{1-\sigma_{p_2}} = g(\sigma_{p_2})^{1-\sigma_{p_1}} \tag{2}$$

*then is* $\varepsilon$ *or* $-\varepsilon$ *the square in* $K_S$.

**Proof.** We must only prove that the crossed homomorphism $f$ induced by the function $g$ satisfies $\varepsilon^{1-\sigma} = f(\sigma)^2$ for any $\sigma \in G$.

For, let $\sigma \in G$ be any automorphism, and let us write it as $\sigma = \prod_{t \in T} \sigma_t$, where $T \subseteq S$ is determined by $\sigma$. We prove our assertion by induction on $\#T$. The case $T = \emptyset$ is trivial. In the case $\#T = 1$ we use the assumption and the remark after Proposition 3.2. Otherwise, let $P$ and $Q$ be proper subsets of $T$ such that $P \cap R = \emptyset$ and $\sigma = \prod_{j \in P} \sigma_j \cdot \prod_{k \in R} \sigma_k$. Let $\tau = \prod_{j \in P} \sigma_j$ a $\omega = \prod_{k \in R} \sigma_k$. Then $\sigma = \tau\omega$, and the induction hypothesis gives $\varepsilon^{1-\tau} = f(\tau)^2$ a $\varepsilon^{1-\omega} = f(\omega)^2$. Hence

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

The proposition is proved. □

We want to apply this proposition to the case $S = \{p, q, r\}$, i.e. to the octic field $K_S = \mathbb{Q}\left(\sqrt{p}, \sqrt{q}, \sqrt{r}\right)$. In this case the Galois group $G = \mathrm{Gal}(K_S/\mathbb{Q})$ is generated by the automorphisms $\sigma_p, \sigma_q, \sigma_r$, so we have to compute how act these automorphisms on arbitrary unit $\eta$ from the subgroup of $E$ generated by $\{-1, \varepsilon_p, \varepsilon_q, \varepsilon_r, \beta_{pq}, \beta_{pr}, \beta_{qr}, \beta_{pqr}\}$.

In [1] it is proved that if $\left(\frac{p}{q}\right) = 1$ then $\beta_{pq}^{1+\sigma_q} = \left(\frac{v}{p}\right)$, where $v \in \mathbb{Z}$ is such that $v^2 \equiv q \pmod p$. This fact we formulate in the following proposition using the notation introduced in the previous section.

**Proposition 3.4.** *If* $p, q$ *are primes congruent to* 1 *modulo* 4, *and* $\left(\frac{p}{q}\right) = 1$, *then*

$$\beta_{pq}^{1+\sigma_q} = \chi_p(q).$$

In this paragraph we prove a similar formula for $\beta_{pq}^{1+\sigma_q}$ in the case $\left(\frac{p}{q}\right) = -1$. To the end of this section let us assume that $\psi = \psi_p$, $R = R_p$, and $R' = R'_p$. Then

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

where $s = \sum_a a$ with $a$ running through the same set of integers as in the previous products. It is easy to see that $q \mid s$, and that $s \equiv (q-1)\sum_a a \pmod p$, where the last sum is taken over all integers $a$ satisfying $0 < a < p$, $\psi(a) \in R$. Thus we have (in all following products $a$ runs over the same set as in the last sum)

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

where $q' \in \mathbb{Z}$ is an inverse of $q$ modulo $p$. Now multiply both sides of this equation by

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

and an easy calculation yields (in all following products we assume also $0 < a < p$)

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

where $a$ in the sum is running over all quadratic residues modulo $p$ satisfying $0 < a < p$. Now, we define $\alpha(l, s) = (-1)^{\#\left\{ 0<a<l \,|\, \psi_l(as)\in R_l,\, \psi_l(a)\in R_l' \right\}} \cdot (-1)^{\#\left\{ 0<a\leqslant \frac{l-1}{2} \,|\, \psi_l(a)\notin R_l\cup R_l' \right\}}$ for any prime $l \equiv 1 \pmod 4$ and any integer $s$, which is nonresidue modulo $l$.

**Remark.** Although we have defined $\alpha(l, s)$ by means of some fixed character $\psi_l$, from the following proposition it is clear that $\alpha$ does not depend on the choice of this character.

If we recall that $\sqrt{l} = \prod_{a=1}^{(l-1)/2} (\xi_l^{-a} - \xi_l^{a})$ for any prime $l$ congruent to 1 modulo 4, we can finish our calculations.

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

We have proved the following proposition.

**Proposition 3.5.** *If $p, q$ are primes congruent to 1 modulo 4, and $\left(\frac{p}{q}\right) = -1$, then*

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

**Proposition 3.6.** *If $m, n$ are quadratic nonresidues modulo $p$, then*

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

**Proof.** Let us denote $\#\{ 0 < a < p \,|\, \psi(am) \in R,\ \psi(a) \in R' \}$ by $\tau_\psi(p, m)$ (it is the exponent of one of the factors in $\alpha(p, m)$). Let $b, c$ be such integers that $p - 1 = 2^b c$, where $c$ is odd, and $b \geqslant 2$. Let $g$ be a primitive root modulo $p$ satisfying $\psi(g) = \zeta_{2^b}$. Then $m \equiv g^k \pmod p$, where $0 \leqslant k < p - 1$. Write $k$ in the form $k = k_1 \cdot 2^b + k_2$, where $0 \leqslant k_2 < 2^b$, and $k_2$ is an odd integer. Now

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

Let us first consider the case $0 \leqslant k_2 < 2^{b-1}$. Then the conditions on $y$ are equivalent to $0 \leqslant (y - 1)/2 < 2^{b-2} - (k_2 + 1)/2$, where $y$ is odd. Hence $\tau_\psi(p, m) = c \cdot (2^{b-2} - (k_2 + 1)/2)$. If $2^{b-1} \leqslant k_2 < 2^b$, then the above conditions are equivalent to $2^{b-2} > (y - 1)/2 \geqslant 2^{b-1} - (k_2 + 1)/2$, where again $y$ is odd. We obtain $\tau_\psi(p,m) = c \cdot ((k_2+1)/2 - 2^{b-2})$. Thus in both cases we have (note that the result still depends on the choice of $\psi$)

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

If we now put $\chi = \psi^{2^{b-2}}$, then $\chi$ is a Dirichlet character modulo $p$ of order 4. We can reformulate the previous statement as $(-1)^{\tau_\psi(p,m)} = (-1)^{(p-1)/4} \cdot i\chi(m)$. From this equation and from the fact that $(-1)^{\#\left\{\, 0<a\leqslant\frac{p-1}{2} \,\mid\, \psi(a)\notin R\cup R' \,\right\}}$ (the second factor in $\alpha(p,m)$) does not depend on $m$ we have

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

Since $mn$ is a quadratic residue modulo $p$, we have $\chi(mn) = \chi_p(mn)$, and the proposition is proved. □

**Proposition 3.7.** *If $p, q, r$ are primes congruent to* 1 *modulo* 4*, then*

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

**Proof.**

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

where $s = \sum_a a$ with $a$ running through the same set as in the previous products. It is easy to see that $q \mid s, r \mid s$, and that $s \equiv (q-1)\sum_a a \pmod{pr}$, where the last sum is taken over integers $a$ satisfying $0 < a < pr$, $\psi(a) \in R$, $\left(\frac{a}{r}\right) = 1$. Hence (in all following products runs $a$ through the same set as in the previous sum)

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

Since $\beta_{pr} \in \mathbb{Q}\left(\sqrt{p},\sqrt{r}\right)$, we have $\beta_{pr}^{1-\mathrm{Frob}(q,\mathbb{Q}(\zeta_{pr}))^{-1}} = \beta_{pr}^{1-\mathrm{Frob}\left(q,\mathbb{Q}\left(\sqrt{p},\sqrt{r}\right)\right)}$, and the proposition is proved.

## 4. Proof of the theorem

In this section we prove the theorem stated in the introduction. First, we state the main result from [1], which will be useful in our considerations.

**Proposition 4.1.** *Let $p$ and $q$ be different primes such that $p \equiv q \equiv 1 \pmod 4$. Let $h$ be the class number of $\mathbb{Q}\left(\sqrt{p}, \sqrt{q}\right)$.*

1. *If $\left(\frac{p}{q}\right) = -1$, then $h$ is odd.*
2. *If $\left(\frac{p}{q}\right) = 1$, then $h$ is even, if and only if $\chi_q(p) = \chi_p(q)$.*

**Remark.** In [1] it is shown that if $\left(\frac{p}{q}\right) = -1$, then in the group of units of the biquadratic field $\mathbb{Q}\left(\sqrt{p}, \sqrt{q}\right)$ does not exist any unit of the form $|\varepsilon_p^{x_p}\varepsilon_q^{x_q}\beta_{pq}^{x_{pq}}| \neq 1$, where $x_p, x_q, x_{pq} \in \{0,1\}$, which is a square of another unit (here $\beta_{pq}^2 = \varepsilon_{pq}$). In the case $\left(\frac{p}{q}\right) = 1$ it is proved that such unit exists if and only if $\chi_q(p) = \chi_p(q)$, and that this unit is equal to $|\beta_{pq}|$, if $\chi_q(p) = \chi_p(q) = 1$, and to $|\varepsilon_p\varepsilon_q\beta_{pq}|$, if $\chi_q(p) = \chi_p(q) = -1$.

Consider now a unit $\eta = |\varepsilon_p^{x_p}\varepsilon_q^{x_q}\varepsilon_r^{x_r}\beta_{pq}^{x_{pq}}\beta_{pr}^{x_{pr}}\beta_{qr}^{x_{qr}}\beta_{pqr}^{x_{pqr}}| \neq 1$, where $x_p, x_q, x_r, x_{pq}, x_{pr}, x_{qr}, x_{pqr} \in \{0,1\}$. We have proved earlier that, in order to $\eta$ be a square in $E$, at least one of $x_{pq}, x_{pr}, x_{qr}, x_{pqr}$ should be nonzero, and there should exist a function $g : \{\sigma_p, \sigma_q, \sigma_r\} \to \mathbb{Q}\left(\sqrt{p}, \sqrt{q}, \sqrt{r}\right)$ satisfying $\eta^{1-\sigma} = g(\sigma)^2$ for any $\sigma \in \{\sigma_p, \sigma_q, \sigma_r\}$ and conditions (1), (2).

Let us now consider four cases separately:

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

At first, let us suppose that $\left(\frac{p}{q}\right) = \left(\frac{p}{r}\right) = \left(\frac{q}{r}\right) = 1$.

By Proposition 3.7 we have $\beta_{pqr}^{1+\sigma_p} = \beta_{pqr}^{1+\sigma_q} = \beta_{pqr}^{1+\sigma_r} = 1$. Let $g(\sigma_p) = g(\sigma_q) = g(\sigma_r) = \beta_{pqr}$. It is now easy to see that the conditions of Proposition 3.3 are satisfied, therefore $\eta = |\beta_{pqr}|$ is the required square in $E$. We have proved that in this case the class number $h$ of the field $\mathbb{Q}\left(\sqrt{p}, \sqrt{q}, \sqrt{r}\right)$ is an even number. Moreover, if we denote by $v_{pq}, v_{pr}, v_{qr}$ the dyadic valuation of the class number of $\mathbb{Q}\left(\sqrt{p}, \sqrt{q}\right)$, $\mathbb{Q}\left(\sqrt{p}, \sqrt{r}\right)$, $\mathbb{Q}\left(\sqrt{q}, \sqrt{r}\right)$, respectively, we show that $2^{1+v_{pq}+v_{pr}+v_{qr}} \mid h$. For different $j,k \in \{p,q,r\}$ let $E_{jk}$ denote group of units of the biquadratic field $\mathbb{Q}\left(\sqrt{j}, \sqrt{k}\right)$. If $[\,E_{jk} : \langle -1, \varepsilon_j, \varepsilon_k, \beta_{jk}\rangle\,] = 2^{v_{jk}} \cdot l$, where $2 \nmid l$, then it is easy to see that there exists a unit $\lambda_{jk} \in E$, for which $[\,E_{jk} : \langle -1, \varepsilon_j, \varepsilon_k, \lambda_{jk}\rangle\,] = l$, where $\lambda_{jk}^{2^{v_{jk}}} = |\beta_{jk}\varepsilon_j^{c_j}\varepsilon_k^{c_k}|$, for suitable $c_j, c_k \in \mathbb{Z}$. Then $[\,E : \langle -1, \varepsilon_p, \varepsilon_q, \varepsilon_r, \lambda_{pq}, \lambda_{pr}, \lambda_{qr}, \beta_{pqr}\rangle\,] = h/(2^{v_{pq}+v_{pr}+v_{qr}})$. Since we have proved that $|\beta_{pqr}|$ is a square in $E$, we have $2^{1+v_{pq}+v_{pr}+v_{qr}} \mid h$.

Consider now the case $\left(\frac{p}{q}\right) = \left(\frac{q}{r}\right) = 1$, $\left(\frac{p}{r}\right) = -1$. An easy calculation yields

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

From these equations follows that a necessary condition in order to $\eta$ be a square in $E$ is $x_{pr} = 0$. Let

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

Conditions (1) and (2) yield after some calculations conditions

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

and

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

A necessary condition for $\eta$ being a square in $E$ is therefore

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

If $\chi_q(r) = \chi_r(q)$ or $\chi_q(p) = \chi_p(q)$, the $h$ is even already by the remark after Proposition 4.1. Otherwise if $\chi_q(r) \neq \chi_r(q)$ and $\chi_q(p) \neq \chi_p(q)$, then by the conditions above $x_{pq} = x_{qr} = 1$, and also $x_p = x_q = x_r$, where $(-1)^{x_p} = \chi_q(p)\chi_q(r)$. With these settings are conditions (1),(2) satisfied, and $\eta$ is therefore a square in $C$, i.e. the class number $h$ is in this case even.

Let us now suppose $\left(\frac{p}{q}\right) = 1$, $\left(\frac{q}{r}\right) = \left(\frac{p}{r}\right) = -1$. At first, let $x_{pqr} = 0$. Then we have again by Propositions 3.4 and 3.5

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

Here, $\eta^{1-\sigma_p}, \eta^{1-\sigma_q}$ and $\eta^{1-\sigma_r}$ must be squares in $E$. From this condition follows that $x_{pr} = x_{qr} = x_r = 0$. Thus we get $\eta \in \mathbb{Q}\left(\sqrt{p}, \sqrt{q}\right)$. In the case $x_{pqr} = 1$ we have

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

which cannot be a square in $E$ ($\pm\varepsilon_q\varepsilon_r^{-1}$ is not a square according to the remark after Lemma 2.1). Hence we have proved that $\eta$ is a square in $\mathbb{Q}\left(\sqrt{p}, \sqrt{q}, \sqrt{r}\right)$ if and only if it is a square in $\mathbb{Q}\left(\sqrt{p}, \sqrt{q}\right)$, which implies that the parity of the class number $h$ of the field $\mathbb{Q}\left(\sqrt{p}, \sqrt{q}, \sqrt{r}\right)$ is the same as the parity of the class number of the field $\mathbb{Q}\left(\sqrt{p}, \sqrt{q}\right)$.

Let us now consider the last (most difficult) case $\left(\frac{p}{q}\right) = \left(\frac{q}{r}\right) = \left(\frac{p}{r}\right) = -1$. Using Propositions 3.5 and 3.7 we get $\beta_{pqr}^{1-\sigma_p} = -\alpha(r,q) \cdot \alpha(q,r)\,\varepsilon_q^{-1}\varepsilon_r^{-1} \cdot \beta_{pqr}^2$, and

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

The relations for $\eta^{1-\sigma_q}$ and $\eta^{1-\sigma_r}$ we get by the symmetry. At first, let us suppose that $x_{pqr} = 0$. Again, from the remark after Lemma 2.1 we get $x_{pq} = x_{pr} = 0$, and $x_p = 0$. By the symmetry we finally get $\eta \in \mathbb{Q}$. Hence $x_{pqr} = 1$. The same argument as above gives that $x_{pq} = x_{pr} = 1$, and symmetrically also $x_{qr} = 1$. Using Proposition 3.6 we have

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

Let $s_p = \chi_r(pq) \cdot \chi_q(pr)$, $s_q = \chi_r(pq) \cdot \chi_p(qr)$, $s_r = \chi_q(pr) \cdot \chi_p(qr)$. It is clear that necessary conditions for $\beta$ being a square in $E$ are $(-1)^{x_p} = -s_p$, $(-1)^{x_q} = -s_q$, and $(-1)^{x_r} = -s_r$, and that for $s_p, s_q, s_r$ holds true the identity $s_p s_q = s_r$. From this follows that either $s_p = s_q = s_r = 1$ or exactly one of $s_p, s_q, s_r$ is equal to 1, and the others are equal to $-1$. Let us now consider these two cases separately.

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

From the conditions above we get $x_p = x_q = x_r = 1$. It is easy to see that the unique possible definition of the function $g$ (up to the uninteresting sign) is

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

Then we have

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

Symmetrically also $g(\sigma_q)^{1+\sigma_q} = g(\sigma_r)^{1+\sigma_r} = 1$. The condition (1) from Proposition 3.3 is thus satisfied. Further,

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

and by the symmetry

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

Then the condition (2) yields that $\chi_p(qr)\cdot\alpha(r,p) = \chi_q(pr)\cdot\alpha(r,q)$. Since $s_r = 1$, we have $\chi_p(qr) = \chi_q(pr)$, and this condition can be written as $\alpha(r,p) = \alpha(r,q)$, i.e. by Proposition 3.6 $\chi_r(pq) = -1$.

This calculation can be carried out symmetrically, and we get by the Proposition 3.3 that $\eta = |\varepsilon_p\varepsilon_q\varepsilon_r\beta_{pq}\beta_{pr}\beta_{qr}\beta_{pqr}|$ is a square in $E$ if and only if $\chi_r(pq) = \chi_q(pr) = \chi_p(qr) = -1$.

**Exactly one of $\mathbf{s_p, s_q, s_r}$ is equal to 1**

We can assume that $s_p = 1, s_q = s_r = -1$. Then $x_p = 1, x_q = 0, x_r = 0$, and $\eta = |\varepsilon_p\beta_{pq}\beta_{pr}\beta_{qr}\beta_{pqr}|$. Again, the unique possible definition of $g$ is

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

Note that in this case we have a symmetry between $q$ and $r$. Let us first check the condition (1). As in the above case we have $g(\sigma_p)^{1+\sigma_p} = s_p = 1$, and from the analogy with the above case we get $g(\sigma_q)^{1+\sigma_q} = s_q\cdot\varepsilon_q^{-1-\sigma_q} = 1$. By the symmetry we have also $g(\sigma_r)^{1+\sigma_r} = 1$. Let us now consider the condition (2). As before, we have

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

and also

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

From these equations we get $g(\sigma_p)^{1-\sigma_q} = g(\sigma_q)^{1-\sigma_p}$ if and only if $\chi_p(qr)\cdot\alpha(r,p) = \chi_q(pr)\cdot\alpha(r,q)$, which is equivalent to $\alpha(r,p) = -\alpha(r,q)$. We can write this condition using Proposition 3.6 as $\chi_r(pq) = 1$. By the symmetry we have a condition $\chi_q(pr) = 1$. Now we determine the condition for $g(\sigma_q)^{1-\sigma_r} = g(\sigma_r)^{1-\sigma_q}$. We have

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

and

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

Since $\varepsilon_q^{1-\sigma_r} = \varepsilon_r^{1-\sigma_q} = 1$, we get the condition $\chi_q(pr)\cdot\alpha(p,q) = \chi_r(pq)\cdot\alpha(p,r)$. Further, since $\chi_q(pr)\cdot\chi_r(pq) = s_p = 1$, we have $\alpha(p,q) = \alpha(p,r)$, and this is by Proposition 3.6 equivalent to $\chi_p(qr) = -1$. By the Proposition 3.3 we have that in this case of $s_p, s_q$ and $s_r$ the unit $\eta = |\varepsilon_p\beta_{pq}\beta_{pr}\beta_{qr}\beta_{pqr}|$ is a square in $E$ if and only if $\chi_r(pq) = \chi_q(pr) = 1$, and $\chi_p(qr) = -1$.

Putting this case together with the former one and with its symmetrical analogies, we obtain the assertion of the remaining part of the theorem.

## 5. References

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

[2] 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.