æ

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, Faculty of Science, Masaryk University
Janáčkovo nám. 2a, 662 95 Brno, Czech Republic

1. Introduction

In the paper [2] R. Kučera determines the parity of the class number of any biquadratic field $\mathbb{Q}\left(\sqrt{p},\sqrt{q}\right)$ and $\mathbb{Q}\left(\sqrt{p},\sqrt{2}\right)$, where p and q are different primes, $p \equiv q \equiv 1 \pmod 4$. In the paper [1] we applied his method and computed 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.

Here we present that result together with the case $p = 2$.

Theorem. *Let p, q and r be different primes either congruent to 1 modulo 4 or equal to 2. Let us denote by (a/b) the Kronecker symbol. Further, denote for any prime $l \equiv 1 \pmod 4$ by χ_l one of the Dirichlet characters modulo l of order 4 and by χ_2 one of the Dirichlet characters modulo 16 of order 4. Let h denote the class number of $\mathbb{Q}\left(\sqrt{p},\sqrt{q},\sqrt{r}\right)$.*

1. *If $(p/q) = (p/r) = (q/r) = -1$, then h is even if and only if $\chi_p(qr) \cdot \chi_q(pr) \cdot \chi_r(pq) = -1$.*
2. *If $(p/q) = 1$, $(p/r) = (q/r) = -1$, 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 $(p/q) = (q/r) = 1$, $(p/r) = -1$, then h is even.*
4. *If $(p/q) = (p/r) = (q/r) = 1$, 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 proof of the theorem in the case $p, q, r \equiv 1 \pmod 4$ can be found in [1]. In this paper we prove the theorem in the case when exactly one of primes p, q, r is equal to 2.

æ

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

We now fix for the rest of this paper two different primes p, q, both congruent to 1 modulo 4. We denote by E the group of units in the field $\mathbb{Q}\left(\sqrt{2}, \sqrt{p}, \sqrt{q}\right)$. 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 ψ_l. Let $R_l = \left\{\rho_l^j \mid 0 \leqslant j < 2^{b_l - 2}\right\}$, 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, for each l, where $l \equiv 1 \pmod 4$ or $l = 2$, we fix one of the characters χ_l as defined in the theorem. Note that for any integer a satisfying $(a/l) = 1$ the value $\chi_l(a)$ does not depend on the choice of the character χ_l.

Let $J = \{2\} \cup \{a \in \mathbb{Z} \mid a \text{ is a prime congruent to 1 modulo 4}\}$. We let $n_{\{2\}} = 8$ and $n_{\{l\}} = l$ for any other element of J. For any finite subset S of J we let (by convention, an empty product is 1)

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

For any $l \in S$ we denote by σ_l the nontrivial automorphism in the group $\mathrm{Gal}\left(K_S/K_{S\setminus\{l\}}\right)$. Let us further define

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

where $\pi_S = \prod_{l \in S} l$. It is easy to see that ε_{π_S} are units in K_S (in particular, $\varepsilon_2 = -1 + \sqrt{2}$). Let C be the group generated by -1 and by all conjugates of ε_{π_S}, where $S \subseteq \{2, p, q\}$. It can be shown (see [3]) that units $\{-1, \varepsilon_2, \varepsilon_p, \varepsilon_q, \varepsilon_{2q}, \varepsilon_{2q}, \varepsilon_{pq}, \varepsilon_{2pq}\}$ form a basis of C, and that $[E : C] = 2^4 \cdot h$, where h is the class number of $\mathbb{Q}\left(\sqrt{2}, \sqrt{p}, \sqrt{q}\right)$.

We shall study the structure of C in order to find the subgroup of E of the sufficiently low index in E. Then we will be able to discuss the parity of h. We know from the results in [2] that for units $\varepsilon_{2p}, \varepsilon_{2q}$, and ε_{pq} there exist units β_{2p}, β_{2q}, and β_{pq} in $\mathbb{Q}\left(\sqrt{2}, \sqrt{p}, \sqrt{q}\right)$ respectively, such that $\varepsilon_{2p} = \beta_{2p}^2, \varepsilon_{2q} = \beta_{2q}^2$, and $\varepsilon_{pq} = \beta_{pq}^2$, where

$$\beta_{2p} = \prod_{\substack{0 < a < 16p \\ a \equiv 1 \pmod{16} \\ (a/p) = 1}} (\zeta_{16p}^{-a} - \zeta_{16p}^{a}) \quad \text{and} \quad \beta_{pq} = \prod_{\substack{0 < a < pq \\ \psi_p(a) \in R_p \\ (a/q) = 1}} (\xi_{pq}^{a} - \xi_{pq}^{-a})$$

and the definition of β_{2q} is analogical to the definition of β_{2p}. Here we show that for ε_{2pq} there also exists a unit β_{2pq} in E, such that $\varepsilon_{2pq} = \beta_{2pq}^2$. When we show this, we will have the subgroup of E generated by the units $\{-1, \varepsilon_2, \varepsilon_p, \varepsilon_q, \beta_{2p}, \beta_{2q}, \beta_{pq}, \beta_{2pq}\}$ of the index h.

We have directly from the definition

$$\varepsilon_{2pq} = \prod_a (1 - \zeta_{8pq}^a) = \zeta_{16pq}^s \cdot \prod_a (\zeta_{16pq}^{-a} - \zeta_{16pq}^a),$$

where $s = \sum_a a$ with a in the products and the sum running through the set of all positive integers $a < 8pq$ satisfying $a \equiv \pm 1 \pmod 8$ and $(a/p) = (a/q) = 1$. It is easy to see that $8pq \mid \sum_a a$. Further if $a \equiv \pm 9 \pmod{16}$, then $a + 8pq \equiv \pm 1 \pmod{16}$, therefore

$$\varepsilon_{2pq} = \pm \prod_{\substack{0<a<16pq \\ a\equiv\pm 1 \pmod{16} \\ (a/p)=(a/q)=1}} (\zeta_{16pq}^{-a} - \zeta_{16pq}^a) = \pm \prod_{\substack{0<a<16pq \\ a\equiv 1 \pmod{16} \\ (a/p)=(a/q)=1}} (\zeta_{16pq}^{-a} - \zeta_{16pq}^a)^2.$$

Now, if we define β_{2pq} by the formula

$$\beta_{2pq} = \prod_{\substack{0<a<16pq \\ a\equiv 1 \pmod{16} \\ (a/p)=(a/q)=1}} (\zeta_{16pq}^{-a} - \zeta_{16pq}^a),$$

we get $\varepsilon_{2pq} = \pm\beta_{2pq}^2$. We will prove that $\beta_{2pq} \in \mathbb{Q}\left(\sqrt{2}, \sqrt{p}, \sqrt{q}\right)$. Let us take any $\tau \in \mathrm{Gal}\left(\mathbb{Q}(\zeta_{16pq})/\mathbb{Q}\left(\sqrt{2}, \sqrt{p}, \sqrt{q}\right)\right)$. Then there is $t \in \mathbb{Z}$ satisfying $t \equiv \pm 1 \pmod 8$ and $(t/p) = (t/q) = 1$ such that $\zeta_{16pq}^\tau = \zeta_{16pq}^t$. We will show that $\beta_{2pq}^\tau = \beta_{2pq}$. This fact is easy to see in the case $t \equiv 1 \pmod{16}$. If $t \equiv 9 \pmod{16}$, then $t' = t + 8pq \equiv 1 \pmod{16}$, $\zeta_{16pq}^{t'} = -\zeta_{16pq}^t$, and

$$\beta_{2pq}^\tau = \prod_a (\zeta_{16pq}^{-at} - \zeta_{16pq}^{at}) = (-1)^{(p-1)(q-1)/4} \prod_a (\zeta_{16pq}^{-at'} - \zeta_{16pq}^{at'}) = \beta_{2pq}.$$

In the remaining case $t \equiv -1 \pmod 8$ let $t' = -t$. Then $t' \equiv 1 \pmod 8$ and the same equation as above yields again $\beta_{2pq}^\tau = \beta_{2pq}$, therefore indeed $\beta_{2pq} \in \mathbb{Q}\left(\sqrt{2}, \sqrt{p}, \sqrt{q}\right)$. Finally, as ε_{2pq} is a positive real number (it is a norm from an imaginary abelian field to a real one), we have $\varepsilon_{2pq} = +\beta_{2pq}^2$.

Now we can conclude that the class number h of the field $\mathbb{Q}\left(\sqrt{2}, \sqrt{p}, \sqrt{q}\right)$ is even if and only if there are $x_2, x_p, x_q, x_{2p}, x_{2q}, x_{pq}, x_{2pq} \in \{0, 1\}$, such that

$$\eta = |\varepsilon_2^{x_2} \varepsilon_p^{x_p} \varepsilon_q^{x_q} \beta_{2p}^{x_{2p}} \beta_{2q}^{x_{2q}} \beta_{pq}^{x_{pq}} \beta_{2pq}^{x_{2pq}}| \neq 1$$

is a square in E. The set of all such possible η can be restricted using the next statement, which is taken from [3]:

Proposition 1. *Let $S \subseteq J$ finite and $l \in S$ arbitrary. Then*

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

From this proposition it follows that

$$(\pm\varepsilon_2)^{1+\sigma_2} = (\pm\varepsilon_p)^{1+\sigma_p} = (\pm\varepsilon_q)^{1+\sigma_q} = -1,$$

hence none of $\pm\varepsilon_2, \pm\varepsilon_p, \pm\varepsilon_q$ could be a square in E. Since

$$(\pm\varepsilon_2\varepsilon_p)^{1+\sigma_2} = -\varepsilon_p^2, \quad (\pm\varepsilon_2\varepsilon_q)^{1+\sigma_2} = -\varepsilon_q^2, \quad (\pm\varepsilon_p\varepsilon_q)^{1+\sigma_p} = -\varepsilon_q^2,$$

none of $\pm\varepsilon_2\varepsilon_p, \pm\varepsilon_2\varepsilon_q, \pm\varepsilon_p\varepsilon_q$ could be a square, and finally nor $\pm\varepsilon_2\varepsilon_p\varepsilon_q$ could be a square in E, because

$$(\pm\varepsilon_2\varepsilon_p\varepsilon_q)^{1+\sigma_2} = -\varepsilon_p^2\varepsilon_q^2.$$

3. Crossed homomorphisms and units

Let us preserve the terminology of the previous section and put $G = \mathrm{Gal}\,(K_S/\mathbb{Q})$. By a crossed homomorphism we mean a function $f : G \to K_S$ such that for all $\sigma, \tau \in G$,

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

The following proposition, which is taken from [3], represents the essential condition which will be used to test whether given unit is a square in K_S.

Proposition 2. *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 ε 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 $\varepsilon^{1-\sigma} = f(\sigma)^2$ (we can put $f(\sigma) = \eta^{1-\sigma}$).

The proof of this proposition (which can be found in [3]) leads to Hilbert theorem 90. In the paper [1] we formulated a weaker condition, which will be more appropriate for our purposes than one of the Proposition 2. This weaker condition is stated in the following proposition.

Proposition 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 ε or $-\varepsilon$ is a square in K_S.

In the next section we shall discuss whether a given unit $\eta \in C$ is a square in E or not. For this purpose we shall use Proposition 3. We have in our case $S = \{2, p, q\}$ and thus we want to know how automorphisms σ_2, σ_p and σ_q act on arbitrary unit η which can be generated by $\{-1, \varepsilon_2, \varepsilon_p, \varepsilon_q, \beta_{2p}, \beta_{2q}, \beta_{pq}, \beta_{2pq}\}$. First, we recall result of this type proved in [2].

Proposition 4. *If p, q are distinct primes either even or congruent to 1 modulo 4, and $(p/q) = 1$, then*

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

In the paper [1] there is proved an analogy to Proposition 4 in the case where p and q are primes, $p, q \equiv 1 \pmod 4$ and $(p/q) = -1$. We will present that result together with the case when one of primes is equal to 2. For the presentation of that result we should first define an auxiliary function α (in the same way as in [1]) using notation introduced in the previous section. We define

$$\begin{aligned}\alpha(l, s) =& (-1)^{\#\left\{ 0<a<l \,|\, \psi_l(as)\in R_l,\, \psi_l(a)\in R_l' \right\}} \\ & \cdot (-1)^{\#\left\{ 0<a\leqslant (l-1)/2 \,|\, \psi_l(a)\notin R_l\cup R_l' \right\}}\end{aligned}$$

for any prime $l \equiv 1 \pmod 4$ and any integer s, which is a nonresidue modulo l. We also define the function α in the case $l = 2$ and $s \equiv 5 \pmod 8$ by the formula

$$\alpha(2, s) = \begin{cases} -1 & \text{if } s \equiv 5 \pmod{16}, \\ 1 & \text{if } s \equiv 13 \pmod{16}. \end{cases}$$

The result mentioned above is stated in the following proposition.

Proposition 5. *If p and q are distinct primes either even or congruent to 1 modulo 4, and $(p/q) = -1$, then*

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

Proof. The case when both primes are odd is proved in [1], here we assume that $q = 2$ and p is an odd prime congruent to 1 modulo 4. From here on to the end of this section we let $\psi = \psi_p$, $R = R_p$, and $R' = R_p'$.

First, we prove the formula $\beta_{2p}^{1+\sigma_2} = \alpha(p, 2)\varepsilon_p$. We have

$$\begin{aligned}\beta_{2p} &= \prod_{\substack{0<a<16p \\ (a/p)=1 \\ a\equiv 1 \pmod{16}}} (\zeta_{16p}^{-a} - \zeta_{16p}^{a}) = (-1)^{(p-1)/4} \cdot \prod_{\substack{0<a<16p \\ a\equiv \pm 1 \pmod{16} \\ \psi(a)\in R}} (\zeta_{16p}^{-a} - \zeta_{16p}^{a}) \\ &= \pm \zeta_{16p}^{-r} \cdot \prod_{\substack{0<a<8p \\ a\equiv \pm 1 \pmod 8 \\ \psi(a)\in R}} (1 - \zeta_{8p}^{a}),\end{aligned}$$

where $r = \sum_a a$ with a running through the same set as in the last product. It is easy to see that $8 \mid r$ (hence $\zeta_{16p}^{r} \in \mathbb{Q}(\zeta_p)$), and that

$$r \equiv 2 \sum_{\substack{0<a<p \\ \psi(a)\in R}} a \pmod p.$$

Let t be an integer satisfying $t \equiv 1 \pmod{p}$, and $t \equiv 3 \pmod{16}$, and $\tau \in \mathrm{Gal}\left(\mathbb{Q}(\zeta_{16p})/\mathbb{Q}\right)$ be the automorphism determined by $\zeta_{16p}^{\tau} = \zeta_{16p}^{t}$. Then σ_2 is the restriction of τ on the field $\mathbb{Q}\left(\sqrt{2}, \sqrt{p}\right)$. Then

$$(\zeta_{16p}^{-r})^{1+\tau} = \zeta_{16p}^{-2r} = \prod_{\substack{0<a<p \\ \psi(a)\in R}} (\zeta_p^{(1-p)/4})^{-a}.$$

Hence

$$\begin{aligned}\beta_{2p}^{1+\sigma_2} &= (\zeta_{16p}^{-r})^{1+\tau} \prod_{\substack{0<a<8p \\ a\equiv\pm 1 \pmod 8 \\ \psi(a)\in R}} (1-\zeta_{8p}^{a})^{1+\tau} \\ &= \prod_{\substack{0<a<p \\ \psi(a)\in R}} (\zeta_p^{(1-p)/4})^{-a} \cdot \prod_{\substack{0<a<8p \\ 2\nmid a,\, \psi(a)\in R}} (1-\zeta_{8p}^{a}).\end{aligned}$$

As it can be easily seen, we have for a fixed integer b

$$\prod_{\substack{0<a<8p \\ 2\nmid a,\, a\equiv b \pmod p}} (1-\zeta_{8p}^{a}) = (1-\zeta_p^{b})^{1-\mathrm{Frob}\left(2,\mathbb{Q}\left(\sqrt{p}\right)\right)^{-1}},$$

and therefore we can continue our calculations as follows:

$$\begin{aligned}\beta_{2p}^{1+\sigma_2} &= \prod_{\substack{0<a<p \\ \psi(a)\in R}} (\zeta_p^{(1-p)/4})^{-a} (1-\zeta_p^{a})^{1-\mathrm{Frob}\left(2,\mathbb{Q}\left(\sqrt{p}\right)\right)^{-1}} \\ &= \prod_{\substack{0<a<p \\ \psi(a)\in R}} (\xi_p^{-a}-\xi_p^{a})^{1-\mathrm{Frob}(2,\mathbb{Q}(\zeta_p))^{-1}} \\ &= \prod_{\substack{0<a<p \\ \psi(a)\in R}} (\xi_p^{-a}-\xi_p^{a}) \prod_{\substack{0<a<p \\ \psi(a)\in R}} (\xi_p^{-aq'}-\xi_p^{aq'})^{-1},\end{aligned}$$

where $q' \in \mathbb{Z}$ is an inverse of 2 modulo p. Now multiply both sides of this equation by

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

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

$$\begin{aligned}
\beta_{2p}^{1+\sigma_2} &\prod_{\substack{(a/p)=-1\\ \psi(a)\notin R'}} (\xi_p^a - \xi_p^{-a})^{-1} \prod_{\psi(a)\in R} (\xi_p^{aq'} - \xi_p^{-aq'}) = \\
&= \prod_{\psi(a)\in R} (\xi_p^a - \xi_p^{-a}) \prod_{\substack{(a/p)=-1\\ \psi(a)\notin R'}} (\xi_p^a - \xi_p^{-a})^{-1} = \\
&= \prod_{\psi(a)\notin R\cup R'} (\xi_p^a - \xi_p^{-a})^{-1} \prod_{(a/p)=1} (\xi_p^a - \xi_p^{-a}) = \\
&= \prod_{\psi(a)\in R\cup R'} (\xi_p^{-a} - \xi_p^a)^{-1} \prod_{(a/p)=1} (\xi_p^{-a} - \xi_p^a) = \\
&= \xi_p^{-\sum_a a} \cdot \prod_{\psi(a)\in R\cup R'} (\xi_p^{-a} - \xi_p^a)^{-1} \prod_{(a/p)=1} (1 - \zeta_p^a) = \\
&= \prod_{\psi(a)\in R\cup R'} (\xi_p^{-a} - \xi_p^a)^{-1} \cdot \sqrt{p} \cdot \varepsilon_p,
\end{aligned}$$

where a in the sum is running over all quadratic residues modulo p satisfying $0 < a < p$. If we recall that for any prime l congruent to 1 modulo 4

$$\sqrt{l} = \prod_{a=1}^{(l-1)/2} (\xi_l^{-a} - \xi_l^a),$$

we finally get

$$\beta_{2p}^{1+\sigma_2} = \varepsilon_p \cdot \alpha(p, 2).$$

Now we prove the second assertion of the proposition, namely $\beta_{2p}^{1+\sigma_p} = \alpha(2, p)\varepsilon_2$. We have

$$\beta_{2p}^{1+\sigma_p} = \prod_{\substack{0<a<16p\\ p\nmid a\equiv 1 \pmod{16}}} (\zeta_{16p}^{-a} - \zeta_{16p}^a) = \zeta_{16p}^{-s} \cdot \prod_{\substack{0<a<16p\\ p\nmid a\equiv 1 \pmod{16}}} (1 - \zeta_{8p}^a),$$

where $s = \sum_a a$ with a running through the same set as in the previous products. Again, it is easy to see that $p \mid s$ and that $s \equiv p - 1 \pmod{16}$. Therefore

$$\beta_{2p}^{1+\sigma_p} = (\zeta_{16}^{-1} - \zeta_{16})^{1-\mathrm{Frob}(p,\mathbb{Q}(\zeta_{16}))^{-1}} = \begin{cases} 1 - \sqrt{2} & \text{if } p \equiv 5 \pmod{16}, \\ -1 + \sqrt{2} & \text{if } p \equiv 13 \pmod{16}, \end{cases}$$

which is by the definition equal to $-\varepsilon_2$ in the former case and to ε_2 in the latter one. The proposition is proved. □

Now we present a relation between function α defined above and Dirichlet characters.

Proposition 6. *If p is a prime such that either $p = 2$ or $p \equiv 1 \pmod 4$ and m, n are integers satisfying $m, n \not\equiv 3 \pmod 8$, $(m/p) = (n/p) = -1$, then*

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

Proof. The proposition is proved in [1] if p is an odd prime. If $p = 2$ then the assertion is trivial. □

In the paper [1] it is shown how automorphisms from the Galois group of the field extension $\mathbb{Q}\left(\sqrt{p}, \sqrt{q}, \sqrt{r}\right)/\mathbb{Q}$ act on the unit β_{pqr} in the case when all primes are congruent to 1 modulo 4. Here we state this result together with the case when one of them is equal to 2 and the other are congruent to 1 modulo 4.

Proposition 7. *Let p, q, and r are distinct primes either congruent to 1 modulo 4 or equal to 2. Then*

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

Proof. The case when all primes are odd is proved in [1]. Now we can assume without loss of generality that p and q are odd primes congruent to 1 modulo 4, and $r = 2$. We must prove two equalities:

$$\beta_{2pq}^{1+\sigma_p} = \beta_{2q}^{1-\mathrm{Frob}\left(p, \mathbb{Q}\left(\sqrt{2}, \sqrt{q}\right)\right)} \qquad \text{and} \qquad \beta_{2pq}^{1+\sigma_2} = \beta_{pq}^{1-\mathrm{Frob}\left(2, \mathbb{Q}\left(\sqrt{p}, \sqrt{q}\right)\right)}.$$

Let us prove the first equality:

$$\beta_{2pq}^{1+\sigma_p} = \prod_{\substack{0<a<16pq \\ p \nmid a \equiv 1 \pmod{16} \\ (a/q)=1}} (\zeta_{16pq}^{-a} - \zeta_{16pq}^{a}) = \zeta_{16pq}^{-s} \cdot \prod_{\substack{0<a<16pq \\ p \nmid a \equiv 1 \pmod{16} \\ (a/q)=1}} (1 - \zeta_{8pq}^{a}),$$

where $s = \sum_a a$ with a running through the same set as in the previous products. By the suitable reorganization of the terms in this sum we can easily see that $p \mid s$, $q \mid s$, and that

$$s \equiv (p-1) \cdot \sum_{\substack{0<a<16q \\ a \equiv 1 \pmod{16} \\ (a/q)=1}} a \pmod{16q}.$$

Now we can continue our computation of $\beta_{2pq}^{1+\sigma_p}$ as follows:

$$\begin{aligned}
\beta_{2pq}^{1+\sigma_p} &= \zeta_{16q}^{-s/p} \cdot \prod_a (1 - \zeta_{8q}^{a})^{1-\mathrm{Frob}(p, \mathbb{Q}(\zeta_{16q}))^{-1}} \\
&= (\zeta_{16q}^{-\sum_a a})^{1-\mathrm{Frob}(p, \mathbb{Q}(\zeta_{16q}))^{-1}} \cdot \prod_a (1 - \zeta_{8q}^{a})^{1-\mathrm{Frob}(p, \mathbb{Q}(\zeta_{16q}))^{-1}} \\
&= \prod_a (\zeta_{16q}^{-a} - \zeta_{16q}^{a})^{1-\mathrm{Frob}(p, \mathbb{Q}(\zeta_{16q}))^{-1}} = \beta_{2q}^{1-\mathrm{Frob}(p, \mathbb{Q}(\zeta_{16q}))^{-1}} \\
&= \beta_{2q}^{1-\mathrm{Frob}\left(p, \mathbb{Q}\left(\sqrt{2}, \sqrt{q}\right)\right)},
\end{aligned}$$

where the last equation holds because $\beta_{2q} \in \mathbb{Q}\big(\sqrt{2}, \sqrt{q}\big)$. All the products and the sum in the previous paragraph are taken over all positive integers $a < 16q$ satisfying $a \equiv 1 \pmod{16}$, and $(a/q) = 1$.

Now, let us consider the second equality (recall that by the convention introduced earlier we have $\psi = \psi_p$ and $R = R_p$). First, we write the unit β_{2pq} in another form:

$$\begin{aligned}\beta_{2pq} &= \prod_{\substack{0<a<16pq \\ a\equiv 1 \pmod{16} \\ (a/p)=(a/q)=1}} (\zeta_{16pq}^{-a} - \zeta_{16pq}^{a}) = (-1)^{(p-1)(q-1)/8} \cdot \prod_{\substack{0<a<16pq \\ a\equiv \pm 1 \pmod{16} \\ \psi(a)\in R,\,(a/q)=1}} (\zeta_{16pq}^{-a} - \zeta_{16pq}^{a}) \\ &= \zeta_{16pq}^{-r} \cdot \prod_{\substack{0<a<8pq \\ a\equiv \pm 1 \pmod{8} \\ \psi(a)\in R,\,(a/q)=1}} (1 - \zeta_{8pq}^{a}),\end{aligned}$$

where $r = \sum_a a$ with a running through the same set as in the last but one product. It is easy to see that $16 \mid r$, that

$$r \equiv 2 \sum_{\substack{0<a<pq \\ \psi(a)\in R,\,(a/q)=1}} a \pmod{p},$$

and that the same congruence holds also modulo q.

Let t be an integer satisfying $t \equiv 1 \pmod{p}$, $t \equiv 1 \pmod{q}$, and $t \equiv 3 \pmod{16}$, and $\tau \in \mathrm{Gal}\,(\mathbb{Q}(\zeta_{16pq})/\mathbb{Q})$ be the automorphism determined by $\zeta_{16pq}^{\tau} = \zeta_{16pq}^{t}$. Then σ_2 is the restriction of τ on the field $\mathbb{Q}\big(\sqrt{2}, \sqrt{p}, \sqrt{q}\big)$. Hence we have

$$\begin{aligned}\beta_{2pq}^{1+\sigma_2} &= (\zeta_{16pq}^{-r})^{1+\tau} \cdot \prod_{\substack{0<a<8pq \\ a\equiv \pm 1 \pmod{8} \\ \psi(a)\in R,\,(a/q)=1}} (1 - \zeta_{8pq}^{a})^{1+\tau} \\ &= \zeta_{8pq}^{-r} \cdot \prod_{\substack{0<a<8pq \\ 2\nmid a,\,(a/q)=1 \\ \psi(a)\in R}} (1 - \zeta_{8pq}^{a}) = \zeta_{8pq}^{-r} \cdot \prod_{\substack{0<a<pq \\ \psi(a)\in R,\,(a/q)=1}} (1 - \zeta_{pq}^{a})^{1-\mathrm{Frob}(2,\mathbb{Q}(\zeta_{pq}))^{-1}} \\ &= \Bigg(\prod_{\substack{0<a<pq \\ \psi(a)\in R,\,(a/q)=1}} \xi_{pq}^{-a} \Bigg)^{1-\mathrm{Frob}(2,\mathbb{Q}(\zeta_{pq}))^{-1}} \cdot \prod_{\substack{0<a<pq \\ \psi(a)\in R,\,(a/q)=1}} (1 - \zeta_{pq}^{a})^{1-\mathrm{Frob}(2,\mathbb{Q}(\zeta_{pq}))^{-1}} \\ &= \prod_{\substack{0<a<pq \\ \psi(a)\in R,\,(a/q)=1}} (\xi_{pq}^{a} - \xi_{pq}^{-a})^{1-\mathrm{Frob}(2,\mathbb{Q}(\zeta_{pq}))^{-1}} = \beta_{pq}^{1-\mathrm{Frob}(2,\mathbb{Q}(\zeta_{pq}))^{-1}}.\end{aligned}$$

Since $\beta_{pq} \in \mathbb{Q}\big(\sqrt{p}, \sqrt{q}\big)$, we have $\beta_{pq}^{1-\mathrm{Frob}(2,\mathbb{Q}(\zeta_{pq}))^{-1}} = \beta_{pq}^{1-\mathrm{Frob}\left(2,\mathbb{Q}\left(\sqrt{p},\sqrt{q}\right)\right)}$. □

Now we have all information about units needed to prove the theorem.
æ

4. Proof of the theorem

Having all the necessary information about the units from the previous section we could prove the theorem stated in the beginning of this paper. As we have already mentioned, the statement of the theorem in the case when all primes p, q, r are odd (and congruent to 1 modulo 4), is proved in [1]. Now we should consider the case when exactly one of primes p, q, r is equal to 2 and the others are congruent to 1 modulo 4.

However, this proof is rather technical and could be carried out in the very similar way as in the paper [1]. Instead, we present main ideas of the proof hoping that an interested reader can fill details using that paper.

First, we state the main result of [2], which will be useful in a further discussion.

Proposition 8. *Let p and q be different primes such that $p \equiv 1 \pmod 4$ and either $q = 2$ or $q \equiv 1 \pmod 4$. Let h be the class number of $\mathbb{Q}\left(\sqrt{p}, \sqrt{q}\right)$.*
1. *If $(p/q) = -1$, then h is odd.*
2. *If $(p/q) = 1$, then h is even if and only if $\chi_q(p) = \chi_p(q)$.*

As we have already mentioned at the end of the second section, now we shall discuss whether there exists a unit

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

which is a square in E. We have also proved that in order to be η a square in E, at least one of x_{pq}, x_{pr}, x_{qr}, and x_{pqr} should be nonzero, and there should also 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) of Proposition 3.

For this discussion it is necessary to distinguish the following four cases:

- $(p/q) = (p/r) = (q/r) = 1$
- $(p/q) = (p/r) = 1,\ (q/r) = -1$
- $(p/q) = 1,\ (p/r) = (q/r) = -1$
- $(p/q) = (p/r) = (q/r) = -1$

In the first case we have by Proposition 7 $\beta_{pqr}^{1+\sigma_p} = \beta_{pqr}^{1+\sigma_q} = \beta_{pqr}^{1+\sigma_r} = 1$. Therefore we can put $\eta = |\beta_{pqr}|$, satisfying conditions of Proposition 3. Hence $|\beta_{pqr}|$ is the required square in E and the class number of the field $\mathbb{Q}\left(\sqrt{p}, \sqrt{q}, \sqrt{r}\right)$ is an even number. Moreover, this special form of the unit η implies the remaining assertion of the theorem in this case. For the details see [1].

In the second case, $(p/q) = (p/r) = 1,\ (q/r) = -1$, there is always a unit of the required type, which is a square in E. If $\chi_p(q) = \chi_q(p)$ or $\chi_p(r) = \chi_r(p)$, then it is easy to see by Proposition 8 that the required unit η exists already in the corresponding biquadratic subfield of $\mathbb{Q}\left(\sqrt{p}, \sqrt{q}, \sqrt{r}\right)$. Otherwise, it can be easily shown using Proposition 3 that $\eta = |\varepsilon_p^x \varepsilon_q^x \varepsilon_r^x \beta_{pq} \beta_{pr} \beta_{pqr}|$, where $(-1)^x = \chi_p(q)\chi_p(r)$, is a square in E. Therefore the class number h is even in this case too.

Let us now consider the third case, $(p/q) = 1,\ (p/r) = (q/r) = -1$. Let us first

suppose that $x_{pqr} = 0$. Then we have by Propositions 4 and 5

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

If we assume that η is a square in E, then also $\eta^{1-\sigma_p}, \eta^{1-\sigma_q}$ and $\eta^{1-\sigma_r}$ should be squares in E. From this assumption we easily get $x_{pr} = x_{qr} = x_r = 0$, hence $\eta \in \mathbb{Q}\big(\sqrt{p}, \sqrt{q}\big)$. If we suppose that $x_{pqr} = 1$, then 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 should be a square in E. But neither $\pm\varepsilon_q$ nor $\pm\varepsilon_q\varepsilon_r^{-1}$ is a square by Proposition 1, hence $\eta^{1-\sigma_p}$ cannot be a square in E in the case $x_{pqr} = 1$.

We have proved that η is a square in $\mathbb{Q}\big(\sqrt{p}, \sqrt{q}, \sqrt{r}\big)$ exactly when it is a square in $\mathbb{Q}\big(\sqrt{p}, \sqrt{q}\big)$, which means that the parity of the class number of the field $\mathbb{Q}\big(\sqrt{p}, \sqrt{q}, \sqrt{r}\big)$ is the same as the parity of the class number of the field $\mathbb{Q}\big(\sqrt{p}, \sqrt{q}\big)$.

The last case $(p/q) = (p/r) = (q/r) = -1$ is the most difficult one. Using Propositions 4 and 7 we have $\beta_{pqr}^{1-\sigma_p} = -\alpha(r,q) \cdot \alpha(q,r)\varepsilon_q^{-1}\varepsilon_r^{-1} \cdot \beta_{pqr}^2$, and

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

The formulas for $\eta^{1-\sigma_q}$ and $\eta^{1-\sigma_r}$ we get by the symmetry.

If we suppose $x_{pqr} = 0$, we can easily show using Proposition 1 that $x_{pq} = x_{pr} = 0$, and $x_p = 0$, hence (again using symmetrical identities) $\eta \in \mathbb{Q}$.

Hence $x_{pqr} = 1$. One can easily deduce (again using Proposition 1) that $x_{pq} = x_{pr} = x_{qr} = 1$. Using Proposition 6 we get

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

and symmetrical formulas for $\eta^{1-\sigma_r}$ and $\eta^{1-\sigma_r}$. Now, let $s_p = \chi_r(pq) \cdot \chi_q(pr)$, $s_q = \chi_r(pq) \cdot \chi_p(qr)$, and $s_r = \chi_q(pr) \cdot \chi_p(qr)$ (it follows that the possible values of s_p, s_q, and s_r are ± 1, and that $s_p s_q s_r = 1$). From the formulas for $\eta^{1-\sigma_p}$,$\eta^{1-\sigma_q}$, and $\eta^{1-\sigma_r}$ we see that necessary conditions for η being a square in E are

$$(-1)^{x_p} = -s_p,\ (-1)^{x_q} = -s_q, \quad \text{and} \quad (-1)^{x_r} = -s_r.$$

Now, it is useful to distinguish two cases: 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 first consider the case $s_p = s_q = s_r = 1$. Then we have from the conditions above $x_p = x_q = x_r = 1$, which means that only possible form of η, such that η can be a square in E is

$$\eta = |\varepsilon_p \varepsilon_q \varepsilon_r \beta_{pq} \beta_{pr} \beta_{qr} \beta_{pqr}|.$$

Now it is not very hard to show that a function $g : \{\sigma_p, \sigma_q, \sigma_r\} \to \mathbb{Q}\left(\sqrt{p}, \sqrt{q}, \sqrt{r}\right)$ satisfying conditions of Proposition 3 exists if and only if $\chi_p(qr) = \chi_q(pr) = \chi_r(pq) = -1$.

In the case when exactly one of s_p, s_q, s_r is equal to 1, we can assume by the symmetry that $s_p = 1$, and $s_q = s_r = -1$. Again using the above formulas we have $x_p = 1$, $x_q = x_r = 0$, thus

$$\eta = |\varepsilon_p \beta_{pq} \beta_{pr} \beta_{qr} \beta_{pqr}|.$$

It is easy to see that up to signs there is only one possible definition of function $g : \{\sigma_p, \sigma_q, \sigma_r\} \to \mathbb{Q}\left(\sqrt{p}, \sqrt{q}, \sqrt{r}\right)$, such that $\eta^{1-\sigma} = g(\sigma)^2$ for any $\sigma \in \{\sigma_p, \sigma_q, \sigma_r\}$. Verifying condition (1) of Proposition 3 we get $\alpha(r,p) = -\alpha(r,q)$, and $\alpha(q,p) = -\alpha(q,r)$, which is by Proposition 6 equivalent to $\chi_r(pq) = 1$, and $\chi_q(pr) = 1$. The condition (2) yields after some calculations condition $\alpha(p,q) = \alpha(p,r)$, which is equivalent to $\chi_p(qr) = -1$. We can conclude that the unit $\eta = |\varepsilon_p \beta_{pq} \beta_{pr} \beta_{qr} \beta_{pqr}|$ is a square in E (in the case $s_p = 1$, $s_q = s_r = -1$) if and only if $\chi_r(pq) = \chi_q(pr) = 1$, and $\chi_p(qr) = -1$.

As the remaining cases of s_p, s_q, s_r can be carried out symmetrically, we have proved the assertion of the theorem in the last case $(p/q) = (p/r) = (q/r) = -1$.

Acknoledgements

I am very grateful to Radan Kučera for helpful discussion and many suggestions leading to an improvement of this paper.

References

[1] M. Bulant. On the parity of the class number of the field $\mathbb{Q}(\sqrt{p}, \sqrt{q}, \sqrt{r})$. *J. Number Theory*, **68**(1):72–86, Jan. 1998.

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

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

æ