Class Number Parity of a Compositum of Five Quadratic Fields

Michal Bulant

Abstract. In this paper we show that the class number of the field $\mathbb{Q}\left(\sqrt{p}, \sqrt{q}, \sqrt{r}, \sqrt{s}, \sqrt{t}\right)$ is even for p, q, r, s, t being different primes either equal to 2 or congruent to 1 modulo 4. This result is based on our previous results about the parity of the class number in the case of the field $\mathbb{Q}\left(\sqrt{p}, \sqrt{q}, \sqrt{r}\right)$.

1. Introduction

Here we formulate the main result of this paper:

Theorem 1. *Let p, q, r, s, t be different primes either equal to 2 or congruent to 1 modulo 4. Then the class number of the field $\mathbb{Q}\left(\sqrt{p}, \sqrt{q}, \sqrt{r}, \sqrt{s}, \sqrt{t}\right)$ is an even number.*

Remark. In the following whenever we talk about primes without further specification we will implicitly assume that $p = 2$ or $p \equiv 1 \pmod 4$.

1.1. Notation. In this section we introduce the notation we shall use throughout this paper.

$S \ldots$ a finite nonempty set of distinct positive primes not congruent to 3 modulo 4
$n_S = \prod_{l \in S} l,\ m_S = \prod_{l \in S} m_{\{l\}}$, where $m_{\{2\}} = 8, m_{\{l\}} = l$ for $l \neq 2$
$(p/q) \ldots$ Kronecker symbol
χ_p (p an odd prime, resp. $p = 2$)... Dirichlet character of order 4 mod p (resp. mod 16)
$K_S = \mathbb{Q}\left(\sqrt{p}\,; p \in S\right)$
$\mathbb{Q}^S = \mathbb{Q}\left(\zeta_{m_S}\right)$, where $\zeta_n = e^{2\pi i/n},\ \xi_n = e^{\pi i/n}$
$\sigma_l \ldots$ unique automorphism for $l \in S$ determined by $\mathrm{Gal}\left(K_S/K_{S \setminus \{l\}}\right) = \{1, \sigma_l\}$
$\mathrm{Frob}(l, K) \ldots$ the Frobenius automorphism of prime l on a field K
$E_S \ldots$ the group of units in K_S
$C_S \ldots$ the group generated by -1 and all conjugates of ε_{n_T}, where $T \subseteq S$, and

$$\varepsilon_{n_T} = \begin{cases} 1 & \text{if} \quad T = \emptyset, \\ \frac{1}{\sqrt{l}} \mathrm{N}_{\mathbb{Q}^T/K_T}(1 - \zeta_{m_T}) & \text{if} \quad T = \{l\}, \\ \mathrm{N}_{\mathbb{Q}^T/K_T}(1 - \zeta_{m_T}) & \text{if} \quad \#T > 1 \end{cases}$$

The author was financially supported by the Grant Agency of the Czech Republic, grant 201/01/0471.

1.2. The index of C. In the paper [**4**] Kučera proves the following result:

Proposition 1. *$\{-1\} \cup \{\varepsilon_{n_T}; \emptyset \neq T \subseteq S\}$ form a basis of C_S, moreover*

$$[E_S : C_S] = 2^{2^s - s - 1} \cdot h_S,$$

where h_S is the class number of K_S and $s = \#S$.

The index of C_S plays the key role in our considerations. In the papers [**3**], [**1**] it has been proved that ε_{pq}, and ε_{pqr} are squares in E_S. We will need a similar result for ε_{pqrs}, and ε_{pqrst} but we can prove even more general statement. First, we formulate one auxiliary definition:

Definition. 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 $b_l \geq 2$. For this prime l fix a Dirichlet character modulo l of order 2^{b_l}, and denote it by ψ_l. Let

$$R_l = \left\{ \rho_l^j \;\middle|\; 0 \leq j < 2^{b_l - 2} \right\}, \text{ and } R_l' = \zeta_{2^{b_l}} \cdot R_l$$

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.

Remark. It is easy to see that $\#R_l = \#R_l' = (l-1)/4c_l$.

Now we can state and proof the promised result.

Proposition 2. *If $\#S > 1$ then ε_{n_S} is a square in K_S.*

Proof. Consider sets P, M_l defined by

$$P = \left\{ a \in \mathbb{Z} \;\middle|\; 0 < a < m_S,\, (a/l) = 1 \text{ for any } l \in S \right\},$$

and

$$M_l = P \cap \left\{ a \in \mathbb{Z} \;\middle|\; 0 < a < m_S,\, \psi_l(a) \in R_l \right\} \text{ for any odd } l \in S.$$

For any $a \in P$ and any odd $l \in S$ we have either $a \in M_l$ or $m_S - a \in M_l$. Therefore

$$\begin{aligned} \varepsilon_{n_S} &= \prod_{a \in P} (1 - \zeta_{m_S}^a) = \prod_{a \in M_l} (1 - \zeta_{m_S}^a)(1 - \zeta_{m_S}^{-a}) \\ &= \prod_{a \in M_l} (1 - \xi_{m_S}^{2a})(1 - \xi_{m_S}^{-2a}) = \prod_{a \in M_l} (\xi_{m_S}^{-a} - \xi_{m_S}^a)(\xi_{m_S}^a - \xi_{m_S}^{-a}). \end{aligned}$$

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

$$\beta_{n_S} = \prod_{a \in M_l} (\xi_{m_S}^a - \xi_{m_S}^{-a}).$$

Now we have to show that $\beta_{n_S} \in K_S$. We will distinguish two cases — either $2 \notin S$ or $2 \in S$: In the first case, let σ be an element of the Galois group $\mathrm{Gal}\left(\mathbb{Q}^S / K_S\right)$. Then there exists an integer k such that $\sigma(\zeta_{m_S}) = \zeta_{m_S}^k$. We have $k \in P$, and

$$\beta_{n_S}^\sigma = \prod_{a \in M_l} (\xi_{m_S}^{ak} - \xi_{m_S}^{-ak}) = \beta_{n_S} \cdot (-1)^{\#\{\, a \in M_l \,|\, \psi_l(ak) \notin R_l \,\}},$$

and since for any $d \in M_l$ the number of elements a of the set M_l, such that $\psi_l(a) = \psi_l(d)$, is equal to $c_l \prod_{t \in S \setminus \{l\}} (t-1)/2$ which is an even integer, we have $\beta_{n_S}^\sigma = \beta_{n_S}$, i.e. $\beta_{n_S} \in K_S$.

Let now $2 \in S$. First, write ε_{n_S} in a slightly modified way:

$$\varepsilon_{n_S} = \prod_{a \in P} (1 - \zeta_{m_S}^a) = \xi_{m_S}^{\sum a} \cdot \prod_{a \in P} (\xi_{m_S}^{-a} - \xi_{m_S}^a)$$

where the sum is taken over $a \in P$. This sum is easily seen to be divisible by m_S, therefore

$$\varepsilon_{n_S} = \pm \prod_{\substack{0<a<2m_S \\ a\equiv\pm1 \pmod{16} \\ \forall t\in S:(a/t)=1}} (\xi_{m_S}^{-a} - \xi_{m_S}^{a}) = \pm \prod_{\substack{0<a<2m_S \\ a\equiv1 \pmod{16} \\ \forall t\in S:(a/t)=1}} (\xi_{m_S}^{-a} - \xi_{m_S}^{a})^2.$$

Let us now define γ_{n_S} by

$$\gamma_{n_S} = \prod_{\substack{0<a<2m_S \\ a\equiv1 \pmod{16} \\ \forall t\in S:(a/t)=1}} (\xi_{m_S}^{-a} - \xi_{m_S}^{a}).$$

Then $\varepsilon_{m_S} = \pm\gamma_{n_S}^2$. We prove $\gamma_{n_S} \in K_S$. Let us take any $\tau \in \mathrm{Gal}\left(\mathbb{Q}\left(\xi_{m_S}\right)/K_S\right)$. Then there is $t \in \mathbb{Z}$ satisfying $(t/l) = 1$ for each $l \in S$ such that $\xi_{m_S}^{\tau} = \xi_{m_S}^{t}$. So $t \equiv \pm1 \pmod 8$. We will show that $\gamma_{n_S}^{\tau} = \gamma_{n_S}$. This fact is easy to see in the case $t \equiv 1 \pmod{16}$. If $t \equiv 9 \pmod{16}$, then $t' = t + m_S \equiv 1 \pmod{16}$, $\xi_{m_S}^{t'} = -\xi_{m_S}^{t}$, and

$$\gamma_{n_S}^{\tau} = \prod_a (\xi_{m_S}^{-at} - \xi_{m_S}^{at}) = (-1)^{\prod_{l\in S\setminus\{2\}}(l-1)/2} \prod_a (\xi_{m_S}^{-at'} - \xi_{m_S}^{at'}) = \gamma_{n_S}.$$

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 $\gamma_{n_S}^{\tau} = \gamma_{n_S}$, therefore indeed $\gamma_{n_S} \in K_S$. Moreover, as ε_{n_S} is a positive real number (it is a norm from an imaginary abelian field to a real one), we have $\varepsilon_{n_S} = +\gamma_{n_S}^2$.

Finally, we have also $\varepsilon_{n_S} = \beta_{n_S}^2$, therefore $\beta_{n_S} = \pm\gamma_{n_S}$ which yields $\beta_{n_S} \in K_S$ too. $\square$

For later reference we state the definition of β once again:

Definition. For any $T \subseteq S$, $\#T > 1$ we define

$$\beta_{n_T} = \prod_{a\in M_l} (\xi_{m_T}^{a} - \xi_{m_T}^{-a}),$$

where M_l is defined as in the beginning of the proof of Proposition 2.

Remark. Although β_{n_T} is defined in the way depending on the choice of $l \in T$ and on the particular selection of the character ψ_l it is easy to see that these choices can influence only the sign of β_{n_T}. As we are not interested in this sign we do not specify the choice of l and ψ_l precisely.

Putting last result together with Proposition 1 we obtain the following assertion:

Proposition 3. *Let*

$$C'_S = \left\langle \{-1\} \cup \{\varepsilon_T;\, T \subseteq S, \#T = 1\} \cup \{\beta_T;\, T \subseteq S, \#T > 1\} \right\rangle.$$

Then

$$[E_S : C'_S] = h_S.$$

As an easy consequence of this proposition we get the following

Corollary. *h_S is even if and only if $C'_S \cap \left(E_S^2 \setminus C'^2_S\right) \neq \emptyset$.*

Thus there is a square in $\mathbb{Q}$ which is not a square in C'_S if and only if the class number h_S of K_S is even. The conditions of existence of such a unit were succesfully found for the fields K_S, where the set S has up to 3 elements. The results are quoted below.

In the theorems of [**1**] and [**2**] it has been shown that whenever there are primes p, q, r where at least 2 of the Kronecker symbols $(p/q), (p/r), (q/r)$ are equal to 1 then the class number of the field $\mathbb{Q}\left(\sqrt{p}, \sqrt{q}, \sqrt{r}\right)$ is even. As we will use this result later together with the main result (concerning the biquadratic case) of the paper [**3**] it is useful to formulate them here:

Theorem 2. *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 $\chi_q(p) = \chi_p(q)$.*

Theorem 3. *Let p, q and r be different primes either congruent to 1 modulo 4 or equal to 2. 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 $v_{pqr} \geq 1 + v_{pq} + v_{pr} + v_{qr}$.)*

2. Possible cases

First, let us state an easy consequence of class field theory (cf. e.g. Theorem 10.1 in [**5**]):

Lemma 1. *Let S, T be sets of primes as above, and $S \subseteq T$. If the class number of K_S is even then also the class number of K_T is an even number.*

From the previous lemma it follows that we can limit ourselves only to those cases where the class number of any subfield K_J, $J \subset S$ is an odd number. The following lemma easily follows from Theorem 3 and Lemma 1.

Lemma 2. *If the class number of the field $\mathbb{Q}\left(\sqrt{p}, \sqrt{q}, \sqrt{r}, \sqrt{s}, \sqrt{t}\right)$ is odd then the following must be satisfied: There exist four distinct primes p_1, p_2, p_3, p_4 from the set $\{p, q, r, s, t\}$ such that either*

- *for any distinct $i, j \in \{1, 2, 3, 4\}$, $(p_i/p_j) = -1$, or*
- *exactly one pair $i_0, j_0 \in \{1, 2, 3, 4\}$ of distinct indices satisfies $(p_i/p_j) = 1$; any other pair of indices i, j yields $(p_i/p_j) = -1$.*

Proof. Assume that for any four distinct primes p_1, p_2, p_3, p_4 from the set $\{p, q, r, s, t\}$ there are at least two pairs of indices yielding quadratic residues. It can be easily seen that there must be three primes q_1, q_2, q_3 from the set $\{p, q, r, s, t\}$ such that $(q_1/q_2) = (q_1/q_3) = 1$. By Theorem 3 it means that the class number of the field $\mathbb{Q}\left(\sqrt{q_1}, \sqrt{q_2}, \sqrt{q_3}\right)$ is even and by Lemma 1 we get a contradiction. $\square$

According to Lemma 2 and thanks to the symmetry we can now investigate the class number of $\mathbb{Q}\left(\sqrt{p}, \sqrt{q}, \sqrt{r}, \sqrt{s}\right)$ only in the following cases:

(1) all pairs are mutual non-residues.
(2) $(p/q) = 1$, all the other pairs form quadratic non-residues

We will be able to prove that in both cases there is an additional square in the subgroup C'_S and therefore (thanks to Corollary following Proposition 3) the class number of the field $\mathbb{Q}\left(\sqrt{p}, \sqrt{q}, \sqrt{r}, \sqrt{s}\right)$ and thus also the class number of the original field is an even number.

2.1. Search for an additional square. In the following paragraphs we will consider the two cases individually to prove that in each of them we can find a unit of the form

$$\eta = \prod_{k\in S} \varepsilon_k^{x_{\{k\}}} \cdot \prod_{\substack{J\subseteq S\\ \#J\geq 2}} \beta_{n_J}^{x_J}$$

which is a square in E. We will need the following Proposition 3.3 of [**1**] which provides us with the necessary tools. Recall that the field K_S is abelian and that its Galois group can be viewed as a (multiplicative) vector space over $\mathbb{F}_2$ with basis $\{\sigma_l \,|\, l \in S\}$.

Proposition 4. *If there exists a function $g : \{\sigma_l \,|\, l \in S\} \to K_S^\times$, which satisfies $\varepsilon^{1-\sigma_l} = g(\sigma_l)^2$ for any $l \in S$ and conditions*

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

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

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

From this proposition it is evident that it will be necessary to know the action of homomorphisms σ_l on the generators of C_S, and C'_S. As this task was already considered in [**3**] and [**1**], we will only cite those results here:

Proposition 5. *Let $T \subseteq S$ be arbitrary (nonempty), and $l \in T$, then*

$$(\varepsilon_{n_T})^{1+\sigma_l} = \begin{cases} -1 & \text{if } T = \{l\}, \\ (l/k)\cdot \varepsilon_k^{1-\mathrm{Frob}(l,K_{\{k\}})} & \text{if } T = \{l,k\}, l \neq k, \\ \varepsilon_{n_{T\setminus\{l\}}}^{1-\mathrm{Frob}(l,K_{T\setminus\{l\}})} & \text{if } \#T > 2. \end{cases}$$

Let us now define an auxiliary function α using notation introduced in the previous section. We define

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

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

$$\alpha_2(s) = \begin{cases} -1 & \text{if } s \equiv 5 \pmod{16}, \\ 1 & \text{if } s \equiv 13 \pmod{16}. \end{cases}$$

We need the following statement for the calculations in the next section:

Lemma 3. *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. This is Proposition 6 of [**2**]. □

The next proposition is in fact a stronger variant of Proposition 5.

Proposition 6. *Let $T \subseteq S$ be arbitrary, $\#T > 1$, and $l \in T$. Then*

$$\beta_{n_T}^{1+\sigma_l} = \begin{cases} \chi_k(l) & \text{if } T = \{k, l\}, (k/l) = 1 \\ \alpha_k(l)\varepsilon_k & \text{if } T = \{k, l\}, (k/l) = -1 \\ \beta_{n_{T\setminus\{l\}}}^{1-\mathrm{Frob}\left(l, K_{T\setminus\{l\}}\right)} & \text{if } \#T > 2. \end{cases}$$

Proof. For the proofs of the first two assertions see [**3**], and [**2**]. We now present a proof of the third case which is in fact an easy variation of the proof of the same statement for the case $\#T = 3$ in [**1**].

Let $q \in T$, $q \neq l$ odd, and put $\psi = \psi_q$, $R = R_q$. Then

$$\beta_{n_T}^{1+\sigma_l} = \prod_{\substack{0<a<m_T \\ \psi(a)\in R,\, l\nmid a \\ \forall t\neq l:(a/t)=1}} (\xi_{m_T}^a - \xi_{m_T}^{-a}) = \xi_{m_T}^s \prod_{\substack{0<a<m_T \\ \psi(a)\in R,\, l\nmid a \\ \forall t\neq l:(a/t)=1}} (1 - \zeta_{m_T}^{-a}),$$

where $s = \sum_a a$ with a running through the same set as in the previous products. It is easy to see that $m_{\{l\}} \mid s$, and that

$$s \equiv \varphi(m_{\{l\}}) \sum_{\substack{0<a<m_{T\setminus\{l\}} \\ \psi(a)\in R, \\ \forall t\neq l:(a/t)=1}} a \pmod{m_{T\setminus\{l\}}},$$

where φ is the usual Euler function.

Hence (a in the following products runs through the same set as in the previous sum)

$$\begin{aligned}\beta_{n_T}^{1+\sigma_l} &= \Big(\prod_a \xi_{m_T}^{m_{\{l\}}a}\Big)^{1-\mathrm{Frob}\left(l,\mathbb{Q}\left(\xi_{m_{T\setminus\{l\}}}\right)\right)^{-1}} \prod_a (1 - \zeta_{m_{T\setminus\{l\}}}^{-a})^{1-\mathrm{Frob}\left(l,\mathbb{Q}\left(\zeta_{m_{T\setminus\{l\}}}\right)\right)^{-1}} \\ &= \prod_a \Big(\xi_{m_T}^{m_{\{l\}}a} - \xi_{m_T}^{-m_{\{l\}}a}\Big)^{1-\mathrm{Frob}\left(l,\mathbb{Q}\left(\xi_{m_{T\setminus\{l\}}}\right)\right)^{-1}} = \beta_{n_{T\setminus\{l\}}}^{1-\mathrm{Frob}\left(l,K_{T\setminus\{l\}}\right)^{-1}}\end{aligned}$$

since $\beta_{n_{T\setminus\{l\}}} \in K_{T\setminus\{l\}}$. □

Having the relations from the last section handy, we can try to find units satisfying Proposition 4.

2.2. All pairs non-residues. At first, we will calculate $\beta_{pqrs}^{1+\sigma_p}$.

$$\begin{aligned}\beta_{pqrs}^{1+\sigma_p} &= \beta_{qrs}^{1-\sigma_q\sigma_r\sigma_s} = \beta_{qrs}^{1-\sigma_q} \cdot \left(\beta_{qrs}^{1-\sigma_r}\right)^{\sigma_q} \cdot \left(\beta_{qrs}^{1-\sigma_s}\right)^{\sigma_q\sigma_r} \\ &= \beta_{qrs}^{2} \cdot (-\alpha_r(s)\alpha_s(r)\varepsilon_s^{-1}\varepsilon_r^{-1}) \\ &\cdot \left(\beta_{qrs}^{2} \cdot (-\alpha_q(s)\alpha_s(q)\varepsilon_q^{-1}\varepsilon_s^{-1})\right)^{\sigma_q} \\ &\cdot \left(\beta_{qrs}^{2} \cdot (-\alpha_q(r)\alpha_r(q)\varepsilon_q^{-1}\varepsilon_r^{-1})\right)^{\sigma_q\sigma_r} \\ &= \left(\beta_{qrs}^{2}\right)^{1+\sigma_q+\sigma_q\sigma_r} \cdot (-\alpha_r(s)\alpha_s(r)\varepsilon_s^{-1}\varepsilon_r^{-1}) \\ &\cdot (\alpha_q(s)\alpha_s(q)\varepsilon_q\varepsilon_s^{-1}) \\ &\cdot (-\alpha_q(r)\alpha_r(q)\varepsilon_q\varepsilon_r) \\ &= -\beta_{qrs}^{2} \cdot \chi_r(qs)\chi_s(rq)\chi_q(rs).\end{aligned}$$

As we suppose that the class number of the field $\mathbb{Q}\left(\sqrt{q}, \sqrt{r}, \sqrt{s}\right)$ is an odd number, which is by the Theorem 3 equivalent to $\chi_q(rs)\chi_r(qs)\chi_s(qr) = 1$, then we finally have

$$\beta_{pqrs}^{1+\sigma_p} = -\beta_{qrs}^{2}.$$

Now, if we put

$$\begin{aligned} g(\sigma_p) &= \beta_{pqrs}\beta_{qrs}^{-1}\varepsilon_p \\ g(\sigma_q) &= \beta_{pqrs}\beta_{prs}^{-1}\varepsilon_q \\ g(\sigma_r) &= \beta_{pqrs}\beta_{pqs}^{-1}\varepsilon_r \\ g(\sigma_s) &= \beta_{pqrs}\beta_{pqr}^{-1}\varepsilon_s, \end{aligned}$$

we can see that the unit $\eta = |\varepsilon_p\varepsilon_q\varepsilon_r\varepsilon_s\beta_{pqrs}|$ is the required additional square in E by verification of conditions (1) and (2) of Proposition 4. Thanks to the perfect symmetry we can always verify only one instance of these conditions:

$$g(\sigma_p)^{1+\sigma_p} = \beta_{pqrs}^{1+\sigma_p} \cdot \beta_{qrs}^{-\sigma_p-1} \cdot (-1) = \beta_{qrs}^{2} \cdot \beta_{qrs}^{-2} = 1$$

$$\begin{aligned} g(\sigma_p)^{1-\sigma_q} &= \chi_p(rs)\chi_r(ps)\chi_s(pr) \cdot \beta_{prs}^{-2}\beta_{qrs}^{-2}\varepsilon_r\varepsilon_s \cdot (-\alpha_r(s)\alpha_s(r)) \cdot \beta_{pqrs}^{2} \\ g(\sigma_q)^{1-\sigma_p} &= \chi_q(rs)\chi_r(qs)\chi_s(qr) \cdot \beta_{prs}^{-2}\beta_{qrs}^{-2}\varepsilon_r\varepsilon_s \cdot (-\alpha_r(s)\alpha_s(r)) \cdot \beta_{pqrs}^{2}, \end{aligned}$$

which implies $g(\sigma_p)^{1-\sigma_q} = g(\sigma_q)^{1-\sigma_p}$, using the assumption about the class number of the octic subfields $\mathbb{Q}\left(\sqrt{p}, \sqrt{r}, \sqrt{s}\right)$, and $\mathbb{Q}\left(\sqrt{q}, \sqrt{r}, \sqrt{s}\right)$, and the derived equality $\chi_p(rs)\chi_r(ps)\chi_s(pr) = \chi_q(rs)\chi_r(qs)\chi_s(qr) = 1$.

2.3. One residual pair. Let us suppose that $(p/q) = 1$ and all other pairs form non-residues. Further, from the condition that $\mathbb{Q}\left(\sqrt{p}, \sqrt{q}\right)$, $\mathbb{Q}\left(\sqrt{p}, \sqrt{r}, \sqrt{s}\right)$, and $\mathbb{Q}\left(\sqrt{q}, \sqrt{r}, \sqrt{s}\right)$ have all an odd class number we may use the following relations in our reasoning:

- $\chi_p(q) \cdot \chi_q(p) = -1$
- $\chi_p(rs)\chi_r(ps)\chi_s(pr) = 1$
- $\chi_q(rs)\chi_r(qs)\chi_s(qr) = 1$

Lemma 4. $\chi_p(rs)\chi_q(rs)\chi_r(pq)\chi_s(pq) = 1$.

Proof. By the assumptions made above we have $\chi_p(rs)\chi_q(rs)\chi_r(pq)\chi_s(pq) = \left(\chi_p(rs)\chi_r(ps)\chi_s(pr)\right)\left(\chi_q(rs)\chi_r(qs)\chi_s(qr)\right) = 1$, using the evident equalities $\chi_r(pq) = -\chi_r(ps)\chi_r(qs)$ and $\chi_s(pq) = -\chi_s(pr)\chi_s(qr)$. □

Let us now calculate $\beta_{pqrs}^{1+\sigma_p}, \beta_{pqrs}^{1+\sigma_r}$ (the other norms we can get by the symmetry):

$$\begin{aligned}\beta_{pqrs}^{1+\sigma_p} &= \beta_{qrs}^{1-\sigma_r\sigma_s} = \beta_{qrs}^{1-\sigma_r} \cdot \left(\beta_{qrs}^{1-\sigma_s}\right)^{\sigma_r} \\ &= \beta_{qrs}^2 \cdot (-\alpha_q(s)\alpha_s(q)\varepsilon_q^{-1}\varepsilon_s^{-1}) \cdot \left(-\beta_{qrs}^2 \cdot \alpha_q(r)\alpha_r(q)\varepsilon_q^{-1}\varepsilon_r^{-1}\right)^{\sigma_r} \\ &= \varepsilon_q^2\varepsilon_s^2 \cdot (-\alpha_q(s)\alpha_s(q)\varepsilon_q^{-1}\varepsilon_s^{-1}) \cdot (\alpha_q(r)\alpha_r(q)\varepsilon_q^{-1}\varepsilon_r) \\ &= -\alpha_q(r)\alpha_r(q)\alpha_q(s)\alpha_s(q)\varepsilon_r\varepsilon_s\end{aligned}$$

By a similar calculation we get

$$\begin{aligned}\beta_{pqrs}^{1+\sigma_r} &= \beta_{pqs}^{1-\sigma_p\sigma_q\sigma_s} = \beta_{pqs}^{1-\sigma_p} \cdot \left(\beta_{pqs}^{1-\sigma_q}\right)^{\sigma_p} \cdot \left(\beta_{pqs}^{1-\sigma_s}\right)^{\sigma_p\sigma_q} \\ &= (\alpha_q(s)\varepsilon_q\beta_{qs}^{-2}\beta_{pqs}^2) \cdot (\alpha_p(s)\varepsilon_p\beta_{ps}^{-2}\beta_{pqs}^2)^{\sigma_p} \cdot (\chi_p(q)\chi_q(p)\beta_{pqs}^2)^{\sigma_p\sigma_q} \\ &= -\alpha_q(s)\alpha_p(s)\chi_p(q)\chi_q(p)\varepsilon_p\varepsilon_q\varepsilon_s^2\beta_{ps}^{-2}\beta_{qs}^{-2}\beta_{pqs}^2 \\ &= \alpha_q(s)\alpha_p(s)\varepsilon_p\varepsilon_q\varepsilon_s^2\beta_{ps}^{-2}\beta_{qs}^{-2}\beta_{pqs}^2,\end{aligned}$$

where the last equation follows from our assumption that $\chi_p(q)\chi_q(p) = -1$.

Put now $\eta_1 = \beta_{pr}^{-1}\beta_{ps}^{-1}\beta_{qr}^{-1}\beta_{qs}^{-1}\beta_{pqrs}$. We get

$$\eta_1^{1-\sigma_p} = \chi_q(rs)\chi_r(pq)\chi_s(pq)\beta_{pr}^{-2}\beta_{ps}^{-2}\beta_{pqrs}^2 = \chi_p(rs)\beta_{pr}^{-2}\beta_{ps}^{-2}\beta_{pqrs}^2$$

and

$$\eta_1^{1-\sigma_r} = \chi_p(rs)\chi_q(rs)\varepsilon_s^{-2}\beta_{pr}^{-2}\beta_{ps}^2\beta_{qr}^{-2}\beta_{qs}^2\beta_{pqs}^{-2}\beta_{pqrs}^2$$

(the equations for $\eta^{1-\sigma_q}$ and $\eta^{1-\sigma_s}$ we get by the symmetry).

Let $x_p = \chi_p(rs), x_q = \chi_q(rs), x_r = x_s = \chi_p(rs)\chi_q(rs)$, and

$$\delta_l = \begin{cases} 1 & \text{if } x_l = 1 \\ \varepsilon_l & \text{if } x_l = -1 \end{cases}$$

for any $l \in \{p, q, r, s\}$. Further, let

$$\eta = \eta_1 \prod_{l\in\{p,q,r,s\}} \delta_l,$$

and

$$\begin{aligned}g(\sigma_p) &= \delta_p\beta_{pr}^{-1}\beta_{ps}^{-1}\beta_{pqrs} \\ g(\sigma_r) &= \delta_r\varepsilon_s^{-1}\beta_{pr}^{-1}\beta_{ps}\beta_{qr}^{-1}\beta_{qs}\beta_{pqs}^{-1}\beta_{pqrs}\end{aligned}$$

and symmetrically for $g(\sigma_q), g(\sigma_s)$. Then $\eta^{1-\sigma_l} = g(\sigma_l)^2$ for any $l \in \{p, q, r, s\}$.

We will now verify conditions (1), (2) for the pairs $(p, q), (p, r), (r, s)$, which is sufficient thanks to the symmetry. We have

$$\begin{aligned}g(\sigma_p)^{1+\sigma_p} &= \delta_p^{1+\sigma_p}\chi_q(rs)\chi_r(pq)\chi_s(pq) = 1 \\ g(\sigma_r)^{1+\sigma_p} &= \delta_r^{1+\sigma_r}\chi_p(rs)\chi_q(rs) = 1\end{aligned}$$

since $x_l = \delta_l^{1+\sigma_l}$ for any $l \in \{p, q, r, s\}$.

$$\begin{aligned}g(\sigma_p)^{1-\sigma_q} &= -\alpha_p(r)\alpha_p(s)\alpha_r(p)\alpha_s(p) \cdot \varepsilon_r^{-1}\varepsilon_s^{-1}\beta_{pqrs}^2 \\ g(\sigma_q)^{1-\sigma_p} &= -\alpha_q(r)\alpha_q(s)\alpha_r(q)\alpha_s(q) \cdot \varepsilon_r^{-1}\varepsilon_s^{-1}\beta_{pqrs}^2\end{aligned}$$

and as we can get using the above lemmas

$$\alpha_p(r)\alpha_p(s)\alpha_r(p)\alpha_s(p) \cdot \alpha_q(r)\alpha_q(s)\alpha_r(q)\alpha_s(q) = \chi_p(rs)\chi_q(rs)\chi_r(pq)\chi_s(pq) = 1,$$

it follows that $g(\sigma_p)^{1-\sigma_q} = g(\sigma_q)^{1-\sigma_p}$.

In the second case

$$g(\sigma_p)^{1-\sigma_r} = -\chi_p(rs)\alpha_q(s) \cdot \varepsilon_q^{-1}\varepsilon_s^{-2}\beta_{pr}^{-2}\beta_{ps}^{2}\beta_{qs}^{2}\beta_{pqs}^{-2}\beta_{pqrs}^{2}$$
$$g(\sigma_r)^{1-\sigma_p} = -\chi_r(pq)\chi_s(pq)\alpha_q(r) \cdot \varepsilon_q^{-1}\varepsilon_s^{-2}\beta_{pr}^{-2}\beta_{ps}^{2}\beta_{qs}^{2}\beta_{pqs}^{-2}\beta_{pqrs}^{2}$$

which yields similarly as in the previous case that $g(\sigma_p)^{1-\sigma_r} = g(\sigma_r)^{1-\sigma_p}$.

Finally,

$$g(\sigma_r)^{1-\sigma_s} = \alpha_p(r)\alpha_p(s)\alpha_q(r)\alpha_q(s) \cdot \varepsilon_p^{-2}\varepsilon_q^{-2}\varepsilon_r^{-2}\varepsilon_s^{-2}\beta_{pr}^{2}\beta_{ps}^{2}\beta_{qr}^{2}\beta_{qs}^{2}\beta_{pqr}^{-2}\beta_{pqs}^{-2}\beta_{pqrs}^{2}$$
$$g(\sigma_s)^{1-\sigma_r} = \alpha_p(r)\alpha_p(s)\alpha_q(r)\alpha_q(s) \cdot \varepsilon_p^{-2}\varepsilon_q^{-2}\varepsilon_r^{-2}\varepsilon_s^{-2}\beta_{pr}^{2}\beta_{ps}^{2}\beta_{qr}^{2}\beta_{qs}^{2}\beta_{pqr}^{-2}\beta_{pqs}^{-2}\beta_{pqrs}^{2}$$

which is trivially equal.

Thus we have shown that η meets conditions (1), (2) of Proposition 4 and therefore there exists a unit $\eta_1 \in E$ which is the additional required square.

Altogether we get Theorem 1 proved.

References

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

[2] M. Bulant. On the parity of the class number of the field $Q(\sqrt{p}, \sqrt{q}, \sqrt{r})$. *Acta Mathematica et Informatica Universitatis Ostraviensis*, 6:41–52, 1998.

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

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

[5] L. C. Washington. *Introduction to Cyclotomic Fields*. Number 83 in GTM. Springer, 2nd edition, 1997.

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

E-mail address: `bulant@math.muni.cz`