Masaryk University

Faculty of Science

Class Number Parity of a Compositum of Quadratic Fields

Dissertation thesis

Author: Michal Bulant
Advisor: Radan Kučera
Branch: Algebra, Number Theory and Mathematical Logic

Brno, September 2002

This dissertation is dedicated to my wife, who supported me during the (not so short) time of my studies and to my daughters Alena, Lucie, and Petra, without whose constant assistance I would probably have finished it much sooner.

Acknowledgement:
I would like to thank my advisor, professor Radan Kučera for his invaluable comments during my work on this dissertation. I am also grateful to many teachers and students of the faculty for providing friendly and collaborative environment.

Brno, 30/9/2002 Michal Bulant

Department of Mathematics, Faculty of Science,
Masaryk University, Janáčkovo nám. 2a,
662 95 Brno, Czech Republic
bulant@math.muni.cz

Contents

Introduction

Units and class group. Let us first recall some basic definitions. An *algebraic number field* K is a finite extension of rationals $\mathbb{Q}$, an *algebraic integer* is a root of a monic polynomial over the ring of integers $\mathbb{Z}$. Although the ring R of all algebraic integers of the field K is a natural generalization of $\mathbb{Z}$ it need not be a unique factorization domain (nor principal ideal domain). On the other hand, every nonzero ideal of R can be uniquely written as a product of prime ideals.

Any mapping sending an element a of R to the principal ideal aR defines a homomorphism from the multiplicative semigroup $R^\times$ into multiplicative semigroup of nonzero ideals $I^\times$. Let $K^\times$ denote the multiplicative group of the field K and I_f the group of fractional ideals of R. Then I_f is a free abelian group over prime ideals of R and we have the following exact sequence:

$$1 \to E \to K^* \to I_f \to C\ell \to 1$$

with E being the group of units of R, and $C\ell$ is the class group of R. E is finitely generated (by Dirichlet theorem) and $C\ell$ is finite. The size of the class group is given by the *class number* (the order of $C\ell$), while the magnitude of E can be measured by the *regulator*.

For the understanding of the arithmetic of R we would like to know

- explicit generators of E
- a structure of $C\ell$ (or at least the class number $h = |C\ell|$).

Relations between h and arithmetic of R. Let us now formulate a few results demonstrating the connection between class number of K and arithmetic of R:

- $h = 1$ if and only if R is a unique factorization domain
- $h = 2$ iff factorization in R is not unique in general but any two factorizations of a given element of R have the same number of factors.

Even a partial information on h can be valuable: it is well known that if a product of two relatively prime rational integers is a square of a rational integer then each of them has to be a square, up to a sign. And the same holds true for any powers. The reason for this is that $\mathbb{Z}$ is unique factorization domain. Nevertheless for any

positive integer m we have the following generalization to the ring R of algebraic integers of a general field K: h is relatively prime to m if and only if for any two relatively prime integers we have: if their product is the mth power of an integer then each of them is a unit multiple of the mth power of an integer.

$$(h,m)=1 \Longleftrightarrow \forall\, a,b \in R\colon \Big((\exists\, c,x,y \in R:\ ax+by=1 \wedge ab=c^m) \\ \Longrightarrow (\exists\, e \in E\, \exists\, d \in R:\ a=ed^m)\Big)$$

Now, we will consider abelian fields, i.e. finite Galois extensions of $\mathbb{Q}$ with abelian Galois group. There is an *analytic class number formula* which can be used for the calculation of the product of h and the regulator but for the determination of the regulator we still need to explicitly know the generators of E. The best known algorithms for this task are of sub-exponential time complexity and therefore can be used only for fields of small degree (or discriminant).

Due to the Kronecker-Weber theorem the abelian fields can be characterized as subfields of cyclotomic fields. Let us first begin with cyclotomic fields.

Circular units of cyclotomic fields. Let $m>1$ be a rational integer, $m \not\equiv 2 \pmod 4$. The mth cyclotomic field $K_m=\mathbb{Q}(\zeta_m)$ is obtained by adjoining the primitive mth root of unity $\zeta_m=e^{2\pi i/m}$ to $\mathbb{Q}$. The group of circular units C_m of the mth cyclotomic field K_m is defined as the intersection of the group of all units E_m of K_m and the subgroup of the multiplicative group generated by all circular numbers $1-\zeta_m^a$

$$C_m = E_m \cap \langle \{1-\zeta_m^a;\ a \in \mathbb{Z},\ 0<a<m\} \rangle.$$

It is easy to find a finite set of explicit generators of C_m. This point is one of the important properties of C_m (recall that to find explicit generators of the full group of units is usually out of our possibilities). Another important fact is that C_m is of finite index in E_m and that there is a connection between this index and the class number h^+ of the maximal real subfield $\mathbb{R} \cap K_m$ of the mth cyclotomic field. Namely, we have the following Sinnott formula:

$$[E_m : C_m] = 2^s \cdot h^+,$$

where s is determined by the number n of primes dividing m as follows

$$s=\begin{cases} 0, & \text{if } n=1, \\ 2^{n-2}+1-n, & \text{if } n \geq 2. \end{cases}$$

It is easy to see that for any odd prime p this formula implies that $p|h^+$ if and only if there is a noncircular unit ε such that ε^p is circular:

$$p|h^+ \Longleftrightarrow \exists\, \varepsilon \in E_m \setminus C_m : \varepsilon^p \in C_m.$$

But it is not easy at all to construct such a unit. Another question is how to show that it is not circular. Here a useful tool could be a basis of C_m, i.e. an independent system of generators (modulo torsion). Such a basis of the group of circular units of the mth cyclotomic field was found independently by Gold, Kim and Kučera.

Circular units of abelian fields. The notion of circular units can be generalized to any abelian field, we will mention two (probably most important) possible ways. Having an abelian field k we can take the smallest cyclotomic field K_m containing k.

- We can consider all circular units of K_m which are in our field k, i.e. the intersection $C_W = k \cap C_m$. Since this approach is mentioned in the Washington's monograph on cyclotomic fields ([**7**]) we shall call it Washington's group of circular units of k.
- For each cyclotomic field $K_n \subseteq K_m$ we can take the norm $N_{K_n/k\cap K_n}$ from K_n to its intersection with k to map the group C_n of circular units of K_n to our field k. Sinnott's group C_S of circular units of k is then generated by all these norms of circular units (together with -1):

$$C_S = \langle \{N_{K_n/k\cap K_n}(\eta);\ K_n \subseteq K_m,\ \eta \in C_n\} \cup \{-1\}\rangle$$

Although the Washington's group contains the Sinnott's one, so at first glance it looks better, it is difficult to work with. It can be seen immediately that we have a finite set of explicit generators of C_S — which we usually do not have for C_W. Moreover there is the Sinnott formula for the index $[E : C_S]$ of C_S in the full group E of units of k giving a connection with the class number h^+ of the maximal real subfield $\mathbb{R} \cap k$ of k – which is not the case of C_W. Unfortunately the mentioned formula is not as easy as we have seen in the case of cyclotomic field:

$$[E : C_S] = h^+ Q \,\frac{\prod_{p|m}[k_p : \mathbb{Q}]}{[k : \mathbb{Q}]}\, 2^{-g}(e^+\mathbb{Z}[G] : e^+U).$$

Here Q is the Hasse unit index of k, which is 1 or 2, the product is taken over the rational primes p dividing m and $[k_p : \mathbb{Q}]$ is the degree of the maximal subfield k_p of k ramified only at p. In our case this subfield is the intersection of k and a suitable cyclotomic field, so the whole fraction is easy to compute. A rational integer g is little bit more difficult — if k is real then $g = 1 - [k : \mathbb{Q}]$, but if k is imaginary then we know only that g is between the number of primes $p|m$ with k_p imaginary and the number of them with $[k_p : \mathbb{Q}]$ even. Nevertheless Kučera has found that this problem can be overcome if we enlarge the set of generators of C_S by adding a generator $\sqrt{p}$ for each $p|m$ such that $\sqrt{p} \in k$. Then this little bit larger group is still generated by a finite set of explicit generators but the corresponding

formula is of the same shape with g being the number of primes $p|m$ with $[k_p : \mathbb{Q}]$ even. The most complicated factor in the formula is the index $(e^+\mathbb{Z}[G] : e^+U)$ of Sinnott module in the integral group ring of the Galois group. This factor has been computed explicitly by Sinnott in the following cases:

- m is divisible by at most two primes;
- the Galois group G of k is cyclic;
- the Galois group G of k is the direct product of its inertia groups;
- some very special subfields of the fields from the previous item;
- compositum of any number of quadratic fields (due to Kučera, see [**6**]).

Applications. Let us finally discuss those cases when the group of circular units can be used to get some divisibility relations for the class number of a given abelian field k.

To get it we need to know the index of this group in the full group of units, which can be done either using Sinnott's formula (if the index of the Sinnott module is known for k) or constructing a basis of this group and computing its regulator. This index is then obtained as a product of some known factor and the class number h^+ of the maximal real subfield of k.

Then there is a more difficult task: for a given prime p find a unit outside of the group of circular units whose pth power is in this group or to prove that such a unit does not exist. The problem is that although we are able to work explicitely (and easily enough) with circular units, we do not have any tool to work with the noncircular ones. In fact, there are only two possibilities:

- either to work in the group of circular units of the smallest cyclotomic field containing k, which means to search for this unit inside the Washington's group of circular units of k,
- or to construct a number in k, e.g. by some procedure based on Hilbert theorem 90, and to show that the obtained number is a noncircular unit.

Let us mention several examples where the suggested approach really works.

In the book [**4**] Conner and Hurrelbrink determine the parity of the class number of any biquadratic field up to the cases $\mathbb{Q}(\sqrt{p}, \sqrt{q})$ where p, q are different primes $p \equiv q \equiv 1 \pmod 4$ satisfying $(p/q) = 1$, and $\mathbb{Q}(\sqrt{p}, \sqrt{2})$ where a prime p is congruent to 1 mod 8. Using the described way Kučera has obtained the criterion for the parity of the class number of these fields in terms of biquadratic characters (see [**5**], or slightly modified version in Proposition 1.11).

I have extended this technique to determine the class number of the field $\mathbb{Q}(\sqrt{p}, \sqrt{q}, \sqrt{r})$, where again p, q, r are primes congruent to 1 mod 4 in the paper [**2**] to get the exact characterization of the fields of this type of an odd class number (see Chapter 1 of this thesis). In the paper [**3**] (Chapter 2) I have completed the octic case by considering $p = 2$.

In this thesis I have tried to find n such that any compositum of n quadratic fields has to have an even class number. I was able to prove that this is really true for $n = 5$ (Theorem 3 of Chapter 3). I have not been successful in the solving the same question for $n = 4$ yet as there still remain some unanswered questions in this case (see Chapter 4).

CHAPTER 1

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

1. Introduction

In the paper [5] R. Kučera determines the parity of the class number of any biquadratic field $\mathbb{Q}(\sqrt{p}, \sqrt{q})$, where p and q are different primes, $p \equiv q \equiv 1 \pmod 4$. In this chapter we extend methods used in [5] to compute the parity of the class number of the field $\mathbb{Q}(\sqrt{p}, \sqrt{q}, \sqrt{r})$, where p, q and r are different primes, all congruent to 1 modulo 4.

We now state our result precisely.

THEOREM 1. *Let p, q and r be different primes such that $p, q, r \equiv 1 \pmod 4$. Let h denote the class number of $\mathbb{Q}(\sqrt{p}, \sqrt{q}, \sqrt{r})$.*
1. If $(p/q) = (p/r) = (q/r) = -1$, 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 $(u_{pq}/r)(u_{pr}/q)(u_{qr}/p) = -1$.
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 $\mathbb{Q}(\sqrt{p}, \sqrt{q})$.
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 $\mathbb{Q}(\sqrt{p}, \sqrt{q})$, $\mathbb{Q}(\sqrt{p}, \sqrt{r})$, $\mathbb{Q}(\sqrt{q}, \sqrt{r})$, $\mathbb{Q}(\sqrt{p}, \sqrt{q}, \sqrt{r})$, respectively, then $v_{pqr} \geq 1 + v_{pq} + v_{pr} + v_{qr}$.)

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 $\mathbb{Q}(\sqrt{p}, \sqrt{q}, \sqrt{r})$. 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 $b_l \geq 2$. For this prime l fix a Dirichlet character modulo l of order 2^{b_l}, and denote it by ψ_l. Let $R_l = \left\{ \rho_l^j \;\middle|\; 0 \leq j < 2^{b_l - 2} \right\}$, 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 χ_l be a fixed Dirichlet character

modulo l of order 4. Note that for any integer a satisfying $(a/l)=1$ the value of $\chi_l(a)$ does not depend on the choice of the character χ_l.

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

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

By σ_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

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

It is easy to see that ε_{n_S} are units in K_S. Let C be the group generated by -1 and by all conjugates of ε_{n_S}, where $S\subseteq\{p,q,r\}$. Theorem 1 of [**6**] 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 $\mathbb{Q}(\sqrt{p},\sqrt{q},\sqrt{r})$.

In [**5**] it is proved that $\varepsilon_{pq},\varepsilon_{pr},\varepsilon_{qr}$ are squares in $\mathbb{Q}(\sqrt{p},\sqrt{q},\sqrt{r})$, i.e. there are such units $\beta_{pq},\beta_{pr},\beta_{qr}$ in $\mathbb{Q}(\sqrt{p},\sqrt{q},\sqrt{r})$ that $\varepsilon_{pq}=\beta_{pq}^2,\varepsilon_{pr}=\beta_{pr}^2$, and $\varepsilon_{qr}=\beta_{qr}^2$ (see also Proposition 3.2). The unit β_{pq} is defined by the relation $\beta_{pq}=\prod_{a\in M_{pq}}(\xi_{pq}^a-\xi_{pq}^{-a})$, where $M_{pq}=\{a\in\mathbb{Z}\,|\,0<a<pq,(a/q)=1,\psi_p(a)\in R_p\}$, and the units β_{pr},β_{qr} are defined analogously.

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

$$\varepsilon_{pqr}=\prod_{\substack{0<a<pqr\\(a/p)=(a/q)=(a/r)=1}}(1-\zeta_{pqr}^a)=\prod_{a\in M}(1-\zeta_{pqr}^a)(1-\zeta_{pqr}^{-a})=$$
$$=\prod_{a\in M}(1-\xi_{pqr}^{2a})(1-\xi_{pqr}^{-2a})=\prod_{a\in M}(\xi_{pqr}^{-a}-\xi_{pqr}^{a})(\xi_{pqr}^{a}-\xi_{pqr}^{-a}).$$

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

$(k/q)=(k/r)=1$, and

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

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 $c_p(q-1)(r-1)/4$, which is an even integer, we have $\beta_{pqr}^{\sigma}=\beta_{pqr}$, i.e. $\beta_{pqr}\in\mathbb{Q}(\sqrt{p},\sqrt{q},\sqrt{r})$.

Thus we have a subgroup of E generated by the set of units $\{-1,\varepsilon_p,\varepsilon_q,\varepsilon_r,\beta_{pq},\beta_{pr},\beta_{qr},\beta_{pqr}\}$ 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 η 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 [**6**]:

LEMMA 1.1. *In the notation of the beginning of this section let $S\subseteq J$ finite and $l\in S$. Then*

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

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 $\mathbb{Q}(\sqrt{p},\sqrt{q},\sqrt{r})$. 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 $\mathbb{Q}(\sqrt{p},\sqrt{q},\sqrt{r})$, 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 [**6**].

PROPOSITION 1.2. *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 $\varepsilon^{1-\sigma} = f(\sigma)^2$ (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 $\{\sigma_l \,|\, l \in S\}$.

PROPOSITION 1.3. *Let a function $g : \{\sigma_l \,|\, l \in S\} \to K_S$ satisfy the following conditions:*

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

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

For any positive integer t let $S_t = \{k \in S \,|\, k < t\}$. 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) $f|_{\{\sigma_l \,|\, l\in S\}} = g$.
(2) It is easy to see that if such g satisfying (1a), (1b), 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 1.3 until we prove some auxiliary lemmas.

LEMMA 1.4. *If the conditions in Proposition 1.3 hold for g, and f is defined in the same way as in Proposition 1.3, 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

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

Now from the condition (1b)

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

□

LEMMA 1.5. *If the conditions in Proposition 1.3 hold for g, and f is defined in the same way as in Proposition 1.3, 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

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

Lemma 1.4 implies that

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

If $l \notin T$ then $\tau = \rho\omega$, and using Lemma 1.4 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 (1a) it follows that $f(\sigma_l)^{-\sigma_l} = f(\sigma_l)$, which finally yields $f(\sigma_l\tau) = f(\tau)f(\sigma_l)^{-\tau\sigma_l} = f(\tau)f(\sigma_l)^{\tau} = f(\tau)f(\sigma_l)f(\tau)^{\sigma_l-1} = f(\sigma_l)f(\tau)^{\sigma_l}$ with one more application of Lemma 1.4 □

We are now ready to prove Proposition 1.3.

PROOF OF PROPOSITION 1.3. 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 $T \subsetneq V$ 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 1.5 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 Proposition 1.2 and Proposition 1.3 into one criterion which will be often useful in the next section.

PROPOSITION 1.6. *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*

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

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

then ε or $-\varepsilon$ is a 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 σ. 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 1.3. 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 would like to apply this proposition to the case $S = \{p,q,r\}$, i.e. to the octic field $K_S = \mathbb{Q}(\sqrt{p},\sqrt{q},\sqrt{r})$. In this case the 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 η from the subgroup of E generated by $\{-1, \varepsilon_p, \varepsilon_q, \varepsilon_r, \beta_{pq}, \beta_{pr}, \beta_{qr}, \beta_{pqr}\}$.

In [5] it is proved that if $(p/q) = 1$ then $\beta_{pq}^{1+\sigma_q} = (v/p)$, 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 1.7. *If p, q are primes congruent to 1 modulo 4, and $(p/q) = 1$, 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 $(p/q) = -1$. 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

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

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

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

where a in the sum is running over all quadratic residues modulo p satisfying $0 < a < p$. Now, we define

$$\alpha_l(s) = (-1)^{\#\{\,0<a<l \,|\, \psi_l(as)\in R_l,\, \psi_l(a)\in R_l'\,\}} \cdot (-1)^{\#\{\,0<a\le (l-1)/2 \,|\, \psi_l(a)\notin R_l\cup R_l'\,\}}$$

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 ψ_l, from the following proposition it is clear that α_l 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.

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

We have proved the following proposition.

Proposition 1.8. *If p, q are primes congruent to 1 modulo 4, and $(p/q) = -1$, then*

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

PROPOSITION 1.9. *If m,n are quadratic nonresidues modulo p, then*

$$\alpha_p(m)\cdot\alpha_p(n) = -\chi_p(mn).$$

PROOF. Let us denote $\#\{\,0<a<p \mid \psi(am)\in R,\ \psi(a)\in R'\,\}$ 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 $p-1=2^bc$, where c is odd, and $b\geq 2$. Let g be a primitive root modulo p satisfying $\psi(g)=\zeta_{2^b}$. Then $m\equiv g^k \pmod p$, where $0\leq k<p-1$. Write k in the form $k=k_1\cdot 2^b+k_2$, where $0\leq k_2<2^b$, and k_2 is an odd integer. Now

$$\begin{aligned}\tau_\psi(p,m) &= \#\Big\{\,0<a<p \;\Big|\; \psi(am)\in R,\ \psi(a)\in R'\,\Big\}\\ &= \#\left\{x\cdot 2^b+y \;\middle|\; 0\leq x<c, 0\leq y<2^{b-1}, 2\nmid y, \left\langle\frac{y+k}{2^b}\right\rangle<\frac12\right\}\\ &= c\cdot\#\left\{y \;\middle|\; 0\leq y<2^{b-1}, 2\nmid y, \left\langle\frac{y+k_2}{2^b}\right\rangle<\frac12\right\}.\end{aligned}$$

Let us first consider the case $0\leq k_2<2^{b-1}$. Then the conditions on y are equivalent to $0\leq (y-1)/2<2^{b-2}-(k_2+1)/2$, where y is odd. Hence $\tau_\psi(p,m)=c\cdot(2^{b-2}-(k_2+1)/2)$. If $2^{b-1}\leq k_2<2^b$, then the above conditions are equivalent to $2^{b-2}>(y-1)/2\geq 2^{b-1}-(k_2+1)/2$, 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 ψ)

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

If we now put $\chi=\psi^{2^{b-2}}$, then χ 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 $(-1)^{\#\{\,0<a\leq(p-1)/2\,\mid\,\psi(a)\notin R\cup R'\,\}}$ (the second factor in $\alpha_p(m)$) does not depend on m we have $\alpha_p(m)\cdot\alpha_p(n)=((-1)^{(p-1)/4}\cdot i\chi(m))\cdot((-1)^{(p-1)/4}\cdot i\chi(n))=-\chi(mn)$. Since mn is a quadratic residue modulo p, we have $\chi(mn)=\chi_p(mn)$, and the proposition is proved. □

PROPOSITION 1.10. *If p,q,r are primes congruent to 1 modulo 4, then*

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

PROOF.

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

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 $0<a<pr$, $\psi(a)\in R$, $(a/r)=1$. 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 $\beta_{pr}\in\mathbb{Q}(\sqrt{p},\sqrt{r})$, we have $\beta_{pr}^{1-\mathrm{Frob}(q,\mathbb{Q}(\zeta_{pr}))^{-1}} = \beta_{pr}^{1-\mathrm{Frob}\left(q,\mathbb{Q}(\sqrt{p},\sqrt{r})\right)}$, 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 [5], which will be useful in our considerations.

PROPOSITION 1.11. *Let p and q be different primes such that $p\equiv q\equiv 1 \pmod 4$. Let h be the class number of $\mathbb{Q}(\sqrt{p},\sqrt{q})$.*
1. *If $(p/q)=-1$, then h is odd.*
2. *If $(p/q)=1$, then h is even, if and only if $\chi_q(p)=\chi_p(q)$.*

REMARK. In [5] it is shown that if $(p/q)=-1$, then in the group of units of the biquadratic field $\mathbb{Q}(\sqrt{p},\sqrt{q})$ 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 $(p/q)=1$ 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 η 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 $g:\{\sigma_p,\sigma_q,\sigma_r\}\to\mathbb{Q}(\sqrt{p},\sqrt{q},\sqrt{r})$ satisfying $\eta^{1-\sigma}=g(\sigma)^2$ for any $\sigma\in\{\sigma_p,\sigma_q,\sigma_r\}$ and conditions (1a), (1b).

Let us now consider four cases separately:

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

At first, let us suppose that $(p/q)=(p/r)=(q/r)=1$. By Proposition 1.10 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 1.6 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 $\mathbb{Q}(\sqrt{p},\sqrt{q},\sqrt{r})$ is an even number. Moreover, if we denote by v_{pq}, v_{pr}, v_{qr} the dyadic valuation of the class number of $\mathbb{Q}(\sqrt{p},\sqrt{q})$, $\mathbb{Q}(\sqrt{p},\sqrt{r})$, $\mathbb{Q}(\sqrt{q},\sqrt{r})$, 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 $\mathbb{Q}(\sqrt{j},\sqrt{k})$. 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 $(p/q) = (q/r) = 1$, $(p/r) = -1$. An easy calculation yields

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

From these equations it follows that a necessary condition in order to η 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 (1a) and (1b) yield after some calculations conditions

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

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 η 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 1.11. 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 the conditions (1a),(1b) are satisfied, and η is therefore a square in C, i.e. the class number h is in this case even.

Let us now suppose $(p/q) = 1$, $(q/r) = (p/r) = -1$. At first, let $x_{pqr} = 0$. Then we have again by Proposition 1.7 and Proposition 1.8

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

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

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

which cannot be a square in E ($\pm\varepsilon_q\varepsilon_r^{-1}$ is not a square according to the remark after Lemma 1.1). Hence we have proved that η is a square in $\mathbb{Q}(\sqrt{p},\sqrt{q},\sqrt{r})$ if and only if it is a square in $\mathbb{Q}(\sqrt{p},\sqrt{q})$, which implies that the parity of the class number h of the field $\mathbb{Q}(\sqrt{p},\sqrt{q},\sqrt{r})$ is the same as the parity of the class number of the field $\mathbb{Q}(\sqrt{p},\sqrt{q})$.

Let us now consider the last (most difficult) case $(p/q) = (q/r) = (p/r) = -1$. Using Proposition 1.8 and Proposition 1.10 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

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

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 1.1 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 1.9 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 β 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 the identity $s_p s_q = s_r$ holds true. From this it 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 consider these two cases separately.

$s_p = s_q = s_r = 1$

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

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

Then we have

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

Symmetrically also $g(\sigma_q)^{1+\sigma_q} = g(\sigma_r)^{1+\sigma_r} = 1$. The condition (1a) from Proposition 1.6 is thus satisfied. Further,

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

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 (1b) 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 1.9 $\chi_r(pq) = -1$.

This calculation can be carried out symmetrically, and we get by the Proposition 1.6 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 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 only 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 (1a). 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 (1b). 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

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

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 $\alpha_r(p) = -\alpha_r(q)$. Using the assertion of Proposition 1.9 we can write this condition 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

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

and

$$\left(g(\sigma_r)\varepsilon_r\right)^{1-\sigma_q} = \varepsilon_p^{-1}\varepsilon_q^{-2}\varepsilon_r^{-2}\beta_{qr}^2\cdot\chi_r(pq)\cdot\alpha_p(r)\cdot\beta_{pqr}^2.$$

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 1.9 equivalent to $\chi_p(qr) = -1$. By the Proposition 1.6 we get in this case of s_p, s_q and s_r that 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.

CHAPTER 2

On the Parity of the Class Number of the Field $\mathbb{Q}(\sqrt{2}, \sqrt{p}, \sqrt{q})$

1. Introduction

In the paper [5] R. Kučera determines the parity of the class number of any biquadratic field $\mathbb{Q}(\sqrt{p}, \sqrt{q})$ and $\mathbb{Q}(\sqrt{p}, \sqrt{2})$, where p and q are different primes, $p \equiv q \equiv 1 \pmod 4$. In Chapter 1 we applied his method and computed the parity of the class number of the field $\mathbb{Q}(\sqrt{p}, \sqrt{q}, \sqrt{r})$, 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 2. *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 $\mathbb{Q}(\sqrt{p}, \sqrt{q}, \sqrt{r})$.*
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 $\mathbb{Q}(\sqrt{p}, \sqrt{q})$.
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 $\mathbb{Q}(\sqrt{p}, \sqrt{q})$, $\mathbb{Q}(\sqrt{p}, \sqrt{r})$, $\mathbb{Q}(\sqrt{q}, \sqrt{r})$, $\mathbb{Q}(\sqrt{p}, \sqrt{q}, \sqrt{r})$, respectively, then $v_{pqr} \geq 1 + v_{pq} + v_{pr} + v_{qr}$.)

The proof of the theorem in the case $p, q, r \equiv 1 \pmod 4$ is contained in Section 4 of Chapter 1. In this chapter we prove the theorem in the case when exactly one of primes p, q, r is equal to 2.

2. Cyclotomic units

We now fix for the rest of this chapter two different primes p, q, both congruent to 1 modulo 4. We denote by E the group of units of the field $\mathbb{Q}(\sqrt{2}, \sqrt{p}, \sqrt{q})$. 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 $b_l \geq 2$. For this prime l fix a Dirichlet character modulo l of order 2^{b_l}, and denote it by ψ_l. Let $R_l = \left\{\rho_l^j \;\middle|\; 0 \leq j < 2^{b_l-2}\right\}$, 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 $J = \{2\} \cup \{a \in \mathbb{Z} \,|\, a \text{ is a prime congruent to 1 modulo 4}\}$. 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)

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

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 [6]) 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 $\mathbb{Q}(\sqrt{2},\sqrt{p},\sqrt{q})$.

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 [5] that for units $\varepsilon_{2p}, \varepsilon_{2q}$, and ε_{pq} there exist units β_{2p}, β_{2q}, and β_{pq} in $\mathbb{Q}(\sqrt{2},\sqrt{p},\sqrt{q})$ respectively, such that $\varepsilon_{2p} = \beta_{2p}^2, \varepsilon_{2q} = \beta_{2q}^2$, and $\varepsilon_{pq} = \beta_{pq}^2$, where

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

and the definition of β_{2q} is analogical to the definition of β_{2p} (see also Proposition 3.2). Here we show that for ε_{2pq} there also exists a unit β_{2pq} in E, such that $\varepsilon_{2pq} = \beta_{2pq}^2$. After showing this fact we will have the subgroup of E generated by $\{-1, \varepsilon_2, \varepsilon_p, \varepsilon_q, \beta_{2p}, \beta_{2q}, \beta_{pq}, \beta_{2pq}\}$ 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 $a\equiv\pm1 \pmod 8$ and $(a/p)=(a/q)=1$. It is easy to see that $8pq \mid \sum_a a$. Further if $a\equiv\pm9 \pmod{16}$, then $a+8pq\equiv\pm1 \pmod{16}$, therefore

$$\varepsilon_{2pq}=\pm\prod_{\substack{0<a<16pq\\ a\equiv\pm1(16)\\ (a/p)=(a/q)=1}}(\zeta_{16pq}^{-a}-\zeta_{16pq}^{a})=\pm\prod_{\substack{0<a<16pq\\ a\equiv1(16)\\ (a/p)=(a/q)=1}}(\zeta_{16pq}^{-a}-\zeta_{16pq}^{a})^2.$$

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

$$\beta_{2pq}=\prod_{\substack{0<a<16pq\\ a\equiv1(16)\\ (a/p)=(a/q)=1}}(\zeta_{16pq}^{-a}-\zeta_{16pq}^{a}),$$

we get $\varepsilon_{2pq}=\pm\beta_{2pq}^2$. We will prove that $\beta_{2pq}\in\mathbb{Q}(\sqrt{2},\sqrt{p},\sqrt{q})$. Let us take any $\tau\in\mathrm{Gal}\left(\mathbb{Q}(\zeta_{16pq})/\mathbb{Q}(\sqrt{2},\sqrt{p},\sqrt{q})\right)$. Then there is $t\in\mathbb{Z}$ satisfying $t\equiv\pm1 \pmod 8$ 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 $t\equiv1 \pmod{16}$. If $t\equiv9 \pmod{16}$, then $t'=t+8pq\equiv1 \pmod{16}$, $\zeta_{16pq}^{t'}=-\zeta_{16pq}^{t}$, 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 $t'\equiv1 \pmod 8$ and the same equation as above yields again $\beta_{2pq}^{\tau}=\beta_{2pq}$, therefore indeed $\beta_{2pq}\in\mathbb{Q}(\sqrt{2},\sqrt{p},\sqrt{q})$. Finally, as ε_{2pq} is a positive real number (it is a norm from an imaginary abelian field to a real one), we have $\varepsilon_{2pq}=+\beta_{2pq}^2$.

Summarising these results we can conclude that the class number h of the field $\mathbb{Q}(\sqrt{2},\sqrt{p},\sqrt{q})$ 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

$$\eta=|\varepsilon_2^{x_2}\varepsilon_p^{x_p}\varepsilon_q^{x_q}\beta_{2p}^{x_{2p}}\beta_{2q}^{x_{2q}}\beta_{pq}^{x_{pq}}\beta_{2pq}^{x_{2pq}}|\neq1$$

is a square in E. The set of all such possible η can be restricted using the next statement, which is taken from [**6**]:

LEMMA 2.1. *Let $S\subseteq J$ finite and $l\in S$ arbitrary. Then*

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

REMARK. This lemma is in fact the same as Lemma 1.1 but now we allow also $l=2$.

From this lemma 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

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 1.3. In our case we have $S = \{2, p, q\}$ 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 [5].

PROPOSITION 2.2. *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 Proposition 1.7 we have proved an analogy to Proposition 2.2 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 the primes is equal to 2. For the presentation of that result we recall the auxiliary function α (defined in Chapter 1) using notation introduced in the previous section. We define

$$\alpha_l(s) = (-1)^{\#\left\{\, 0<a<l \,\mid\, \psi_l(as)\in R_l,\, \psi_l(a)\in R_l' \,\right\}} \cdot (-1)^{\#\left\{\, 0<a\le (l-1)/2 \,\mid\, \psi_l(a)\notin R_l\cup R_l' \,\right\}}$$

for any prime $l \equiv 1 \pmod 4$ and any integer s, which is nonresidue modulo l.

We also define the function α_l 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 2.3. *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 Proposition 1.8, 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

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

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 $\tau\in\mathrm{Gal}\,(\mathbb{Q}(\zeta_{16p})/\mathbb{Q})$ be the automorphism determined by $\zeta_{16p}^{\tau}=\zeta_{16p}^{t}$. Then σ_2 is the restriction of τ onto the field $\mathbb{Q}(\sqrt{2},\sqrt{p})$. 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

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

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

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

and therefore we can continue our calculations as follows:

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

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

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

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 2.4. *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 Proposition 1.9 if p is an odd prime. If $p = 2$ then the assertion is trivial. □

In Chapter 1 it is shown how automorphisms from the Galois group of the field extension $\mathbb{Q}(\sqrt{p},\sqrt{q},\sqrt{r})/\mathbb{Q}$ 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 2.5. *Let p, q, and r are distinct primes either congruent to 1 modulo 4 or equal to 2. Then*

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

PROOF. The case when all primes are odd is proved in Proposition 1.10. Now we can assume without loss of generality that p and q are odd primes congruent to 1 modulo 4, and $r = 2$. We have to prove two equalities:

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

Let us prove the first equality:

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

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

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

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

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

where the last equation holds because $\beta_{2q}\in\mathbb{Q}(\sqrt{2},\sqrt{q})$. All the products and the sum in the calculation above 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 a modified form:

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

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 onto the field $\mathbb{Q}(\sqrt{2},\sqrt{p},\sqrt{q})$.

Hence we have

$$\beta_{2pq}^{1+\sigma_2} = (\zeta_{16pq}^{-r})^{1+\tau} \cdot \prod_{\substack{0<a<8pq \\ a\equiv\pm1\,(8) \\ \psi(a)\in R,\,(a/q)=1}} (1-\zeta_{8pq}^{a})^{1+\tau} = \zeta_{8pq}^{-r} \cdot \prod_{\substack{0<a<8pq \\ 2\nmid a,\,(a/q)=1 \\ \psi(a)\in R}} (1-\zeta_{8pq}^{a})$$

$$= \zeta_{8pq}^{-r} \cdot \prod_{\substack{0<a<pq \\ \psi(a)\in R,\,(a/q)=1}} (1-\zeta_{pq}^{a})^{1-\mathrm{Frob}(2,\mathbb{Q}(\zeta_{pq}))^{-1}}$$

$$= \left(\prod_{\substack{0<a<pq \\ \psi(a)\in R,\,(a/q)=1}} \xi_{pq}^{-a} \right)^{1-\mathrm{Frob}(2,\mathbb{Q}(\zeta_{pq}))^{-1}} \cdot \prod_{\substack{0<a<pq \\ \psi(a)\in R,\,(a/q)=1}} (1-\zeta_{pq}^{a})^{1-\mathrm{Frob}(2,\mathbb{Q}(\zeta_{pq}))^{-1}}$$

$$= \prod_{\substack{0<a<pq \\ \psi(a)\in R,\,(a/q)=1}} (\xi_{pq}^{a}-\xi_{pq}^{-a})^{1-\mathrm{Frob}(2,\mathbb{Q}(\zeta_{pq}))^{-1}} = \beta_{pq}^{1-\mathrm{Frob}(2,\mathbb{Q}(\zeta_{pq}))^{-1}}.$$

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

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

4. Proof of the theorem

Having all the necessary information about the units from the previous section handy we can 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 Chapter 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.

This proof uses the same auxiliary results as the one of the main theorem of the Chapter 1. We outline the main ideas of the proof again to allow standalone reading of this chapter. The reader is advised to fill in details using the previous chapter.

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 for η to be 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 $g : \{\sigma_p, \sigma_q, \sigma_r\} \to \mathbb{Q}(\sqrt{p},\sqrt{q},\sqrt{r})$ satisfying $\eta^{1-\sigma} = g(\sigma)^2$ for any $\sigma \in \{\sigma_p, \sigma_q, \sigma_r\}$, and conditions (1a),(1b) of Proposition 1.3.

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 2.5 $\beta_{pqr}^{1+\sigma_p}=\beta_{pqr}^{1+\sigma_q}=\beta_{pqr}^{1+\sigma_r}=1$. Therefore we can put $\eta=|\beta_{pqr}|$, satisfying conditions of Proposition 1.6. Hence $|\beta_{pqr}|$ is the required square in E and the class number of the field $\mathbb{Q}(\sqrt{p},\sqrt{q},\sqrt{r})$ 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 page 15.

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 1.11 that the required unit η exists already in the corresponding biquadratic subfield of $\mathbb{Q}(\sqrt{p},\sqrt{q},\sqrt{r})$. Otherwise, it can be easily shown using Proposition 1.3 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, $(p/q)=1,\ (p/r)=(q/r)=-1$. By the exactly same process (now we, of course, allow some of the primes is equal to 2) as on the page 17 in Chapter 1 we deduce that the parity of the class number of $\mathbb{Q}(\sqrt{p},\sqrt{q},\sqrt{r})$ is the same as the parity of the class number of the field $\mathbb{Q}(\sqrt{p},\sqrt{q})$.

The last case $(p/q)=(p/r)=(q/r)=-1$ is the most difficult one. Using again the exactly same reasoning (but using extended underlying results) as on the page 17 in Chapter 1 we can verify that the necessary and sufficient condition for h to be and even number is

$$\chi_p(qr)\cdot\chi_q(pr)\cdot\chi_r(pq)=-1$$

CHAPTER 3

Class Number Parity of a Compositum of Five Quadratic Fields

1. Introduction

Here we formulate the main result of this paper:

THEOREM 3. *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 $\mathbb{Q}(\sqrt{p}, \sqrt{q}, \sqrt{r}, \sqrt{s}, \sqrt{t})$ 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 $l \neq 2$
$(p/q) \ldots$ the Kronecker symbol
χ_p (p an odd prime, resp. $p = 2$)$\ldots$ Dirichlet character of order 4 mod p (resp. mod 16)
$K_S = \mathbb{Q}(\sqrt{p}\,; p \in S)$
$\mathbb{Q}^S = \mathbb{Q}(\zeta_{m_S})$, where $\zeta_n = e^{2\pi i/n}$, $\xi_n = e^{\pi i/n}$
$\sigma_l \ldots$ the unique automorphism for $l \in S$ determined by the relation $\mathrm{Gal}\left(K_S/K_{S\setminus\{l\}}\right) = \{1, \sigma_l\}$
$\mathrm{Frob}(l, K) \ldots$ 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

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

1.2. The index of C. In the paper [**6**] Kučera proves the following result:

PROPOSITION 3.1. *$\{-1\} \cup \{\varepsilon_{n_T}; \emptyset \neq T \subseteq S\}$ 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 paper [**5**] and Section 2 of Chapter 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 will be able to prove even more general statement. First, we formulate an 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 3.2. *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 odd integer k such that $\sigma(\zeta_{m_S}) = \zeta_{m_S}^k$. We have $(k/l) = 1$ for any $l \in S$, and

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

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

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

Let us now define γ_{n_S} by

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

Then $\varepsilon_{m_S} = \pm \gamma_{n_S}^2$. We prove $\gamma_{n_S} \in K_S$. Let us take any $\tau \in \mathrm{Gal}\,(\mathbb{Q}(\xi_{m_S})/K_S)$. Then there is $t \in \mathbb{Z}$ satisfying $(t/l) = 1$ for each $l \in S$ such that $\xi_{m_S}^\tau = \xi_{m_S}^t$. Hence $t \equiv \pm 1 \pmod 8$. 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 implies $\beta_{n_S} \in K_S$ too. □

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 3.2.

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 need to specify the choice of l and ψ_l precisely.

Putting last result together with Proposition 3.1 we obtain the following assertion:

PROPOSITION 3.3. *Let*

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

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 $C'_S \cap (E_S^2 \setminus C_S'^2) \neq \emptyset$.*

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 for the existence of such a unit were succesfully found for the fields K_S, where the set S has up to 3 elements (see Chapters 1 and 2).

In the Theorems 1 and 2 it has been shown that whenever there are such 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 $\mathbb{Q}(\sqrt{p}, \sqrt{q}, \sqrt{r})$ is even. The exact statement of those theorems can be found on pages 7 and 20.

2. Possible cases

First, let us state an easy consequence of class field theory (cf. e.g. Theorem 10.1 in [**7**]):

LEMMA 3.4. *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 2 and Lemma 3.4.

LEMMA 3.5. *If the class number of $\mathbb{Q}(\sqrt{p}, \sqrt{q}, \sqrt{r}, \sqrt{s}, \sqrt{t})$ 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 $i, j \in \{1, 2, 3, 4\}$, $\quad (p_i/p_j) = -1$, or*
- *exactly one pair $i_0, j_0 \in \{1, 2, 3, 4\}$ of distinct indices satisfies $(p_i/p_j) = 1$; for the other pairs of indices i, j the value of Kronecker symbol (p_i/p_j) should be equal to -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 2 it means that the class number of the field $\mathbb{Q}(\sqrt{q}_1, \sqrt{q}_2, \sqrt{q}_3)$ is even and by Lemma 3.4 we get a contradiction. □

According to Lemma 3.5 and thanks to the symmetry we can now investigate the class number of $\mathbb{Q}(\sqrt{p}, \sqrt{q}, \sqrt{r}, \sqrt{s})$ 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 3.3) the class number of the field $\mathbb{Q}(\sqrt{p}, \sqrt{q}, \sqrt{r}, \sqrt{s})$ 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 Proposition 1.6 of Chapter 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 $\{\sigma_l \mid l \in S\}$.

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 [5] and the previous chapters, we will only cite those results here:

PROPOSITION 3.6. *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

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

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 3.7. *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 1.9. □

The next proposition is in fact a stronger variant of Proposition 3.6.

PROPOSITION 3.8. *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 [5], and Proposition 2.3. We now present a proof of the third case which is in fact an easy modification of the proof of the same statement for the case $\#T = 3$ in Proposition 1.10.

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)

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

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 1.6.

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 $\mathbb{Q}(\sqrt{q},\sqrt{r},\sqrt{s})$ is an odd number (which is by Theorem 2 equivalent to the condition $\chi_q(rs)\chi_r(qs)\chi_s(qr) = 1$), 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 (1a) and (1b) of Proposition 1.6. 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 $\mathbb{Q}(\sqrt{p},\sqrt{r},\sqrt{s})$, and $\mathbb{Q}(\sqrt{q},\sqrt{r},\sqrt{s})$, 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 $\mathbb{Q}(\sqrt{p},\sqrt{q})$, $\mathbb{Q}(\sqrt{p},\sqrt{r},\sqrt{s})$, and $\mathbb{Q}(\sqrt{q},\sqrt{r},\sqrt{s})$ 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 3.9. $\chi_p(rs)\chi_q(rs)\chi_r(pq)\chi_s(pq) = 1$.

PROOF. $\chi_p(rs)\chi_q(rs)\chi_r(pq)\chi_s(pq)$ is by the assumptions made above equal to $\big(\chi_p(rs)\chi_r(ps)\chi_s(pr)\big)\big(\chi_q(rs)\chi_r(qs)\chi_s(qr)\big) = 1$, 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 the condition $\chi_p(q)\chi_q(p) = -1$.

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

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

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

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

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

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

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

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

For the second condition we have to compare

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

which yields similarly as above that $g(\sigma_p)^{1-\sigma_r} = g(\sigma_r)^{1-\sigma_p}$.

Finally, we have $g(\sigma_r)^{1-\sigma_s} = \alpha_p(r)\alpha_p(s)\alpha_q(r)\alpha_q(s)\cdot\varepsilon_p^{-2}\varepsilon_q^{-2}\varepsilon_r^{-2}\varepsilon_s^{-2}\cdot\beta_{pr}^2\beta_{ps}^2\beta_{qr}^2\beta_{qs}^2\beta_{pqr}^{-2}\beta_{pqs}^{-2}\beta_{pqrs}^2 = g(\sigma_s)^{1-\sigma_r}$ hence the conditions hold trivially true.

Thus we have shown that η meets conditions (1a), (1b) of Proposition 1.6 and therefore there exists a unit $\eta_1 \in E$ which is the additional required square.

Altogether we get Theorem 3 proved.

CHAPTER 4

Some related questions in this area

1. A compositum of four quadratic fields

As it can be easily seen we are not able to prove results similar to Theorem 3 in case of a compositum of four quadratic fields $\mathbb{Q}(\sqrt{p},\sqrt{q},\sqrt{r},\sqrt{s})$ only using the results presented in the previous chapters. In this case even if we restrict ourselves only to the cases which can potentially yield an odd class number using results of Chapters 1 and 2 there still remains one unsolved case:

- $(p/q) = (r/s) = 1$, the remaining pairs forming quadratic non-residues,

where the primes p,q,r, and s satisfy (besides the usual condition $p,q,r,s \equiv 1 \pmod 4$ or one of them equal to 2) according to Proposition 1.11 the conditions:

$$\chi_p(q)\cdot\chi_q(p) = \chi_r(s)\cdot\chi_s(r) = -1.$$

In Section 4 of Chapter 1 we have proved there there is no appropriate nonsquare circular unit which is a square in E_T for any three-element subset T of the set $S = \{p,q,r,s\}$. In the case of four-element set S we were not able to prove *either existence or non-existence of such unit* in general. We were able to prove the existence of such unit only in the case

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

Therefore we cannot provide complete classification of the fields $\mathbb{Q}(\sqrt{p},\sqrt{q},\sqrt{r},\sqrt{s})$ with an even class number (although our numerical computations shown in the table below suggest that the class number of K_S is probably even already in the case of four-element set S, i.e. that an equivalent of Theorem 3 could hold true even for the fields $\mathbb{Q}(\sqrt{p},\sqrt{q},\sqrt{r},\sqrt{s})$ [1]).

p	q	r	s	$h(\mathbb{Q}(\sqrt{pq},\sqrt{r},\sqrt{s}))$
5	41	53	97	72
5	41	97	193	120
5	41	137	193	8
5	61	157	173	8

[1] We know from the class field theory that if the class number of $\mathbb{Q}(\sqrt{pq},\sqrt{r},\sqrt{s})$ is divisible by 4 then the class number of $\mathbb{Q}(\sqrt{p},\sqrt{q},\sqrt{r},\sqrt{s})$ is an even number.

p	q	r	s	$h(\mathbb{Q}(\sqrt{pq},\sqrt{r},\sqrt{s}))$
5	149	157	197	56
13	17	37	41	8
13	17	37	73	8
13	17	97	193	40
13	17	109	193	8
13	29	37	73	8
13	29	37	137	168
13	29	41	73	24
13	29	73	97	8
13	29	97	193	40
13	113	137	197	72
17	101	109	173	24
17	101	113	173	8
29	53	157	193	120
29	149	157	193	120
37	41	89	109	24
37	41	97	109	24
37	41	97	193	120
37	53	109	193	8
41	113	137	193	8
41	113	181	193	24
61	97	157	173	8
73	149	157	197	8
113	173	181	193	8

Table 1: List of all 4-tuples of primes upto 200, congruent to 1 modulo 4, satisfying $(p/q) = (r/s) = 1$, $\chi_p(q)\cdot\chi_q(p) = \chi_r(s)\cdot\chi_s(r) = -1$, and $\chi_p(rs)\cdot\chi_q(rs)\cdot\chi_r(pq)\cdot\chi_s(pq) = -1$

2. Power of 2 dividing a class number

Numerical results which we have obtained during the work on this paper suggest that in some cases (where we were able to prove that the class number is an even number) the class number is in fact divisible by rather high power of 2.

Probably we could study the group of circular units more deeply to get more exact result about the divisibility of the class number by the power of 2.

3. What about primes congruent to 3 modulo 4?

After reading this paper a natural question can arise: whether similar results can be proved in the case where some of the primes are not congruent to 1 modulo 4. As we were motivated by the work of R. Kučera in [**5**] and [**6**] where the theory was built for the case of primes congruent to 1 modulo 4 we also restricted ourselves to this case.

In the case where some of the primes are congruent to 3 modulo 4 the theory should be appropriately modified and probably some results about the class number could be obtained by studying the group of circular units although it will not be sufficient to work in real extensions of $\mathbb{Q}$ any more and many of the underlying results will need non-apparent replacements.

Bibliography

[1] M. Bulant. Class number parity of a compositum of five quadratic fields. *Acta Mathematica et Informatica Universitatis Ostraviensis, to appear in 2002.*

[2] 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.

[3] 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.

[4] P. E. Conner and J. Hurrelbrink. *Class number parity.* Number 8 in Ser. Pure Math. World Sci., Singapore, 1988.

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

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

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