JOURNAL de Théorie des Nombres de BORDEAUX

anciennement Séminaire de Théorie des Nombres de Bordeaux

Marcin MAZUR et Stephen V. ULLOM

Unit indices and cohomology for biquadratic extensions of imaginary quadratic fields

Tome 20, n° 1 (2008), p. 183-204.

<http://jtnb.cedram.org/item?id=JTNB_2008__20_1_183_0>

Journal de Théorie des Nombres
de Bordeaux **20** (2008), 183-204

Unit indices and cohomology for biquadratic extensions of imaginary quadratic fields

par Marcin MAZUR et Stephen V. ULLOM

Résumé. Nous étudions, en tant que module galoisien, le groupe des unités des extensions biquadratiques de corps de nombres L/M. Le 2-rang du premier groupe de cohomologie des unités de L/M est calculé pour M quelconque. Pour M quadratique imaginaire, nous déterminons la plupart des cas (incluant le cas L/M non ramifiée) où l'indice $[V : V_1V_2V_3]$ prend sa valeur maximale 8, avec V les unités modulo la torsion de L et V_i les unités modulo la torsion d'un des trois sous-corps quadratiques de L/M.

Abstract. We investigate as Galois module the unit group of biquadratic extensions L/M of number fields. The 2-rank of the first cohomology group of units of L/M is computed for general M. For M imaginary quadratic we determine a large portion of the cases (including all unramified L/M) where the index $[V : V_1V_2V_3]$ takes its maximum value 8, where V are units mod torsion of L and V_i are units mod torsion of one of the 3 quadratic subfields of L/M.

1. Introduction

This is the first of a series of papers in which we intend to investigate the Galois module structure of units in biquadratic extensions of imaginary quadratic fields. In our earlier work [6] we obtained fairly satisfactory information on the Galois module structure of units modulo torsion in a totally real biquadratic extension of $\mathbb{Q}$ and we hope to get similar results when the base field is an imaginary quadratic field. This is the only case besides $\mathbb{Q}$ where there are no units of infinite order in the base field. One substantial difference though is that the base has now non-trivial class group which has influence on the structure of units.

Manuscrit reçu le 31 janvier 2007.

Let M be an imaginary quadratic field and let L be a biquadratic extension of M, so $\Gamma = \mathrm{Gal}(L/M)$ is the Klein four group . Let V be the group of units modulo torsion of L and let V_i, $i = 1, 2, 3$, be the units modulo torsion of the three quadratic subfields of L/M. Note that each V_i is a Γ-module and as an abstract group is free abelian of rank 1. It is easy to see that the index $Q = [V : V_1V_2V_3]$ is a divisor of 8. Moreover, if $M = \mathbb{Q}$, then the index can not be 8. This paper grew out of our attempt to prove the same for imaginary quadratic base M. It turns out that it is false and Q can be 8. One of the goals of this work is to describe the extensions L/M for which the index is 8. We do not have a full classification of such fields but we can describe a large portion of them which includes all unramified extensions L/M (and we show that in any L/M with $Q = 8$ only primes over 2 can ramify). Note that if $Q = 8$ then V and $V_1 \times V_2 \times V_3$ are isomorphic Γ-modules. In particular, V is a Galois module of type I, using the terminology of [6].

A substantial part of this paper is a consequence of our effort to understand the arithmetic significance of the equality $Q = 8$. This led us to the cohomological calculations presented in section 2, which we believe are of independent interest. As a consequence we compute the 2-rank of the first cohomology group of units for biquadratic extensions L/M with an arbitrary number field M as a base. In section 4 we show that our results provide a more conceptual approach to the main calculation performed in [5] in order to prove Kuroda's class number formula for biquadratic extensions L/M that relates the class number of L to the class numbers of M and the 3 intermediate subfields of L/M.

2. H^1

In this section we use the following notation:

- $\Gamma = \{1, \sigma_1, \sigma_2, \sigma_3\}$ is the Klein four-group;
- W is a Γ-module;
- $W_i = W^{\sigma_i}$, $i = 1, 2, 3$;
- $N = W_1 + W_2 + W_3$;
- $\mathcal{N} = (1 + \sigma_3)W_1 \cap (1 + \sigma_3)W_2 \cap (1 + \sigma_1)W_3$;
- $\mathcal{K} = W^\Gamma \cap (1 - \sigma_3)W_1 \cap (1 - \sigma_3)W_2 \cap (1 - \sigma_1)W_3$.

Furthermore, for an abelian group A we denote by $A[2]$ the kernel of multiplication by 2 on A.

Note that $W^\Gamma = W_i \cap W_j$ for any $i \neq j$, $2W^\Gamma \subseteq \mathcal{N} \subseteq W^\Gamma$, and $\mathcal{K} \subseteq W^\Gamma[2]$. From now on we assume that the following is true for at least two indices $i \in \{1, 2, 3\}$:

$$\text{if } \ m \in W_i \text{ and } 2m \in W^\Gamma \text{ then } m \in W_j + W_k. \qquad (*)$$

(here $\{i, j, k\} = \{1, 2, 3\}$).

The main result of this section is the following theorem.

Theorem 1. *Suppose that W satisfies the condition $(*)$ for at least two indices $i \in \{1,2,3\}$. There is an exact sequence:*

$$0 \longrightarrow W^{\Gamma}[2]/\mathcal{K} \longrightarrow H^1(W_1) \times H^1(W_2) \times H^1(W_3) \longrightarrow H^1(N) \longrightarrow \mathcal{N}/2W^{\Gamma} \longrightarrow 0,$$

where $H^1(W_i) = H^1(\Gamma/\Gamma_i, W_i)$ for $i = 1,2,3$ and $H^1(N) = H^1(\Gamma, N)$. Furthermore, $H^1(N) = H^1(N)[2]$.

Proof. Without any loss of generality we may (and will) assume that $(*)$ holds for $i = 1,2$. Let

$$\mathcal{Z} = \mathcal{Z}(W) = \mathcal{Z}^1(\Gamma, W) = \{f : \Gamma \longrightarrow W : f(\sigma\tau) = f(\sigma) + \sigma f(\tau)\}$$

be the group of 1-cocycles. For any $f \in \mathcal{Z}$ we have $f(1) = 0$. If $z_i = f(\sigma_i)$ then the condition that f is a 1-cocycle is equivalent to the following relations among z_1, z_2, z_3:

$$z_k = z_i + \sigma_i z_j = \sigma_j z_i + z_j, \quad (1 + \sigma_i)z_i = 0$$

for any permutation i, j, k of $1, 2, 3$. Thus the group of 1-cocycles is isomorphic to the group of ordered pairs (z_1, z_2) of elements of W which satisfy the following relations:

$$(1 + \sigma_1)z_1 = 0 = (1 + \sigma_2)z_2; \quad z_1 + \sigma_1 z_2 = \sigma_2 z_1 + z_2. \quad (1)$$

The group $\mathcal{B} = \mathcal{B}(W) = \mathcal{B}^1(\Gamma, W)$ of 1-coboundaries corresponds to the subgroup of pairs (z_1, z_2) such that $z_i = (\sigma_i - 1)z$ for some $z \in W$ and $i = 1, 2$.

We analyze now the groups $\mathcal{Z} = \mathcal{Z}(N)$, $\mathcal{B} = \mathcal{B}(N)$ and $H^1(N) = H^1(\Gamma, N) = \mathcal{Z}/\mathcal{B}$. Consider a 1-cocycle (z_1, z_2) in $\mathcal{Z}$. We may write $z_1 = n_1 + n_2 + n_3$, with $n_i \in W_i$. We have

$$0 = (1 + \sigma_1)(n_1 + n_2 + n_3) = 2n_1 + (1 + \sigma_1)n_2 + (1 + \sigma_1)n_3.$$

Since $(1 + \sigma_1)n_i \in W^{\Gamma}$ for $i = 2, 3$ and $(*)$ holds for $i = 1$, we see that $n_1 \in W_2 + W_3$. Thus we may write $z_1 = m_2 + m_3$, where $m_2 \in W_2$ and $m_3 \in W_3$. Similarly, there are $m_1' \in W_1$, $m_3' \in W_3$ such that $z_2 = m_1' + m_3'$. The last relation of (1) is equivalent to $m_3 + \sigma_1 m_3' = \sigma_2 m_3 + m_3'$. Note that σ_1 and σ_2 act the same on W_3 so we have $\sigma_i(m_3 - m_3') = m_3 - m_3'$ for $i = 1, 2$. This means that $m_3 - m_3' = b \in W^{\Gamma}$. Setting $m_1 = m_1' - b$ we see that

$$z_1 = m_2 + m_3, \ z_2 = m_1 + m_3$$

for some $m_i \in W_i$. The relations (1) are equivalent to

$$(1 + \sigma_3)m_1 = (1 + \sigma_3)m_2 = -(1 + \sigma_1)m_3. \quad (2)$$

This leads us to the group $\mathcal{N} = (1 + \sigma_3)W_1 \cap (1 + \sigma_3)W_2 \cap (1 + \sigma_1)W_3$.

Let X be the subgroup of $W_1 \times W_2 \times W_3$ which consists of triples (m_1, m_2, m_3) which satisfy condition (2). Our discussion above can be summarized as follows: the map $\Phi : (m_1, m_2, m_3) \mapsto (z_1, z_2)$ given by $z_1 = m_2 + m_3$, $z_2 = m_1 + m_3$ is a surjective homomorphism from X onto $\mathcal{Z}$. In order to gain a better understanding of X note that there is a short exact sequence:

$$0 \longrightarrow \mathcal{Z}_1 \times \mathcal{Z}_2 \times \mathcal{Z}_3 \longrightarrow X \longrightarrow \mathcal{N} \longrightarrow 0, \quad (3)$$

where

$$\mathcal{Z}_i = \{n \in W_i : (1 + \sigma_j)n = 0\} = \mathcal{Z}^1(\{1, \sigma_j\}, W_i)$$

and the map $X \longrightarrow \mathcal{N}$ sends (m_1, m_2, m_3) to $(1 + \sigma_3)m_1$.

We want now to see which elements of X are mapped by Φ into $\mathcal{B}$. Suppose that $n = n_1 + n_2 + n_3 \in N$ (where $n_i \in W_i$) satisfies

$$m_2 + m_3 = (\sigma_1 - 1)n, \quad m_1 + m_3 = (\sigma_2 - 1)n,$$

where $(m_1, m_2, m_3) \in X$. This is equivalent to

$$m_1 + (1 - \sigma_3)n_1 = m_2 + (1 - \sigma_3)n_2 = (\sigma_1 - 1)n_3 - m_3 = w,$$

where $w \in W^\Gamma$. In other words, if $\Phi(m_1, m_2, m_3) \in \mathcal{B}$, then there exist $w \in W^\Gamma$ and $n_i \in W_i$ such that

$$m_1 = w + (\sigma_3 - 1)n_1, \quad m_2 = w + (\sigma_3 - 1)n_2, \quad m_3 = -w + (\sigma_1 - 1)n_3.$$

Conversely, if m_i are given by the above formulas then $(m_1, m_2, m_3) \in X$ and $\Phi(m_1, m_2, m_3) \in \mathcal{B}$. We can summarize this as follows. For $i \in \{1, 2, 3\}$ choose $j \neq i$ and define

$$\mathcal{B}_i = \{m \in W_i : m = (\sigma_j - 1)n \text{ for some } n \in W_i\} = \mathcal{B}^1(\{1, \sigma_j\}, W_i),$$

and let $D = \{(w, w, -w) : w \in W^\Gamma\}$. Then the preimage of $\mathcal{B}$ under Φ is equal to $Y = \mathcal{B}_1 \times \mathcal{B}_2 \times \mathcal{B}_3 + D$. Note that $D \cap \mathcal{Z}_1 \times \mathcal{Z}_2 \times \mathcal{Z}_3 = D[2]$, where $D[2]$ is the kernel of multiplication by 2 on D. The exact sequence (3) restricted to Y is

$$0 \longrightarrow \mathcal{B}_1 \times \mathcal{B}_2 \times \mathcal{B}_3 + D[2] \longrightarrow Y \longrightarrow 2W^\Gamma \longrightarrow 0,$$

Thus we get an exact sequence

$$0 \longrightarrow \mathcal{Z}_1 \times \mathcal{Z}_2 \times \mathcal{Z}_3/(\mathcal{B}_1 \times \mathcal{B}_2 \times \mathcal{B}_3 + D[2]) \longrightarrow X/Y \longrightarrow \mathcal{N}/2W^\Gamma \longrightarrow 0$$

which can be written as

$$0 \longrightarrow D[2]/(\mathcal{B}_1 \times \mathcal{B}_2 \times \mathcal{B}_3 \cap D[2]) \longrightarrow \mathcal{Z}_1 \times \mathcal{Z}_2 \times \mathcal{Z}_3/\mathcal{B}_1 \times \mathcal{B}_2 \times \mathcal{B}_3 \longrightarrow X/Y \longrightarrow \mathcal{N}/2W^\Gamma \longrightarrow 0,$$

or equivalently

$$0 \longrightarrow D[2]/C \longrightarrow H^1(W_1) \times H^1(W_2) \times H^1(W_3) \longrightarrow H^1(N) \longrightarrow \mathcal{N}/2W^\Gamma \longrightarrow 0,$$

where $H^1(W_i) = H^1(\Gamma/\{1, \sigma_i\}, W_i) = \mathcal{Z}_i/\mathcal{B}_i$ and $C = \mathcal{B}_1 \times \mathcal{B}_2 \times \mathcal{B}_3 \cap D[2]$. Recall now that D is naturally isomorphic to W^Γ via $W^\Gamma \ni w \mapsto (w, w, -w) \in D$. Under this identification $C = \mathcal{B}_1 \times \mathcal{B}_2 \times \mathcal{B}_3 \cap D[2]$ corresponds to $\mathcal{K} = W^\Gamma \cap (1-\sigma_3)W_1 \cap (1-\sigma_3)W_2 \cap (1-\sigma_1)W_3$. Thus we get the exact sequence claimed in the statement of the theorem.

In order to prove that $2H^1(N) = 0$ consider a $1-$cocycle f represented by $z_1 = m_2 + m_3$ and $z_2 = m_1 + m_3$. Note that $2z_1 = (1-\sigma_1)z_1 + (1+\sigma_1)z_1 = (1-\sigma_1)(m_1 + m_2 + m_3)$ and similarly $2z_2 = (1-\sigma_2)z_2 + (1+\sigma_2)z_2 = (1-\sigma_2)(m_1 + m_2 + m_3)$. It follows that $2f$ is a coboundary. □

Corollary 1. *Suppose that in addition to the assumptions of Theorem 1 we assume that W is a finitely generated abelian group. Then*

$$|H^1(N)| = |H^1(W_1)||H^1(W_2)||H^1(W_3)|[\mathcal{N} : 2W^\Gamma]/[W^\Gamma[2] : \mathcal{K}].$$

□

Corollary 2. *Suppose that W is a Γ-module which satisfies the following condition for at least two indices $i \in \{1, 2, 3\}$:*

$$\text{if } \ m \in W_i \text{ and } 2m \in W^\Gamma \text{ then } m \in W^\Gamma. \qquad (**)$$

Then $\mathcal{K} = 0$ and we have the following exact sequence:

$$0 \longrightarrow W^\Gamma[2] \longrightarrow H^1(W_1) \times H^1(W_2) \times H^1(W_3) \longrightarrow H^1(N) \longrightarrow \mathcal{N}/2W^\Gamma \longrightarrow 0.$$

Proof. Note that the condition $(**)$ for i implies $(*)$ for the same i. Thus in order to justify Corollary 2 we only need to show that $\mathcal{K} = 0$. If $w \in \mathcal{K}$ then $w = (\sigma_i - 1)n_i$ for some $n_i \in W_i$. It follows that $2n_i = (1+\sigma_i)n_i - w \in W^\Gamma$. If i is such that $(**)$ holds for it then $n_i \in W^\Gamma$ and consequently $w = 0$. □

Usually we are interested in $H^1(W)$ rather than just $H^1(N)$. The exact sequence of cohomology applied to

$$0 \longrightarrow N \longrightarrow W \longrightarrow W/N \longrightarrow 0$$

yields the exact sequence

$$0 \longrightarrow N^\Gamma \longrightarrow W^\Gamma \longrightarrow (W/N)^\Gamma \longrightarrow H^1(N) \longrightarrow H^1(W) \longrightarrow H^1(W/N).$$

Note that W/N is an elementary abelian 2-group with trivial Γ action. Furthermore, since $W^\Gamma \subseteq N$, the map $W^\Gamma \longrightarrow (W/N)^\Gamma$ is trivial. Thus we have the exact sequence

$$0 \longrightarrow W/N \longrightarrow H^1(N) \longrightarrow H^1(W) \longrightarrow H^1(W/N).$$

The following observation is quite useful

Theorem 2. *Suppose that W has the following property :*

$$\text{if } m \in W \text{ and } 2m \in W^{\Gamma} \text{ then } m \in N. \qquad (***)$$

Then every element of order 2 in $H^1(W)$ belongs to the image of $H^1(N)$.

Proof. Let f be a cocycle representing an element of order 2 in $H^1(W)$. We need to show that the values of f are in N. There is $m \in W$ such that $2f(\sigma) = (\sigma - 1)m$ for $\sigma \in \Gamma$. Note that

$$m = (m + f(\sigma_1)) + (m + f(\sigma_2)) - \sigma_1(m + f(\sigma_3)).$$

Indeed, the right hand side is $2m - \sigma_1(m) + f(\sigma_1) + f(\sigma_2) - \sigma_1 f(\sigma_3)$. Since $\sigma_1(m) = 2f(\sigma_1) + m$ and $f(\sigma_2) = f(\sigma_1) + \sigma_1 f(\sigma_3)$, the claim follows. Observe now that

$$\sigma_i(m + f(\sigma_i)) = \sigma_i(m) + \sigma_i(f(\sigma_i)) = [2f(\sigma_i) + m] - f(\sigma_i) = m + f(\sigma_i)$$

and therefore $m + f(\sigma_i) \in W_i$. Thus we may write $m = m_1 + m_2 + m_3$ with $m_i \in W_i$. Thus $2f(\sigma_i) = (1 + \sigma_i)(m_j + m_k) + 2(m_j + m_k)$, i.e.

$$2[f(\sigma_i) - (m_j + m_k)] = (1 + \sigma_i)(m_j + m_k) \in W^{\Gamma}.$$

By our assumption about W we get $f(\sigma_i) - (m_j + m_k) \in N$ and therefore $f(\sigma_i) \in N$. □

Corollary 3. *Suppose that W satisfies $(***)$ and also $(*)$ for at least two indices $i \in \{1, 2, 3\}$. Then we have an exact sequence*

$$0 \longrightarrow W/N \longrightarrow H^1(N) \longrightarrow H^1(W)[2] \longrightarrow 0.$$

Proof. By Theorem 1 we have $2H^1(N) = 0$ so the image of $H^1(N)$ in $H^1(W)$ is contained in $H^1(W)[2]$. On the other hand, Theorem 2 says that $H^1(W)[2]$ is contained in the image of $H^1(N)$. Thus the image of $H^1(N)$ in $H^1(W)$ is equal to $H^1(W)[2]$. □

3. Units

We apply now the results of section 2 to units in biquadratic extensions L/M of number fields. Thus $\Gamma = \{1, \sigma_1, \sigma_2, \sigma_3\} = \mathrm{Gal}(L/M)$. We use the following notation:

- U_L, U_M are the units of L and M respectively;
- U_i is the group of units of L^{σ_i};
- N_i is the norm map from L^{σ_i} to M;
- $v = \begin{cases} 1, & \text{if } L \subseteq M(\sqrt{U_M}); \\ 0, & \text{otherwise} \end{cases}$
- $q = [U_L : U_1 U_2 U_3]$;
- t_∞ is the number of infinite places of M which are complexified in L;

- r is the $\mathbb{Z}$-rank of U_M;
- λ is the $\mathbb{Z}$-rank of U_L.

The main result of this section is the following theorem.

Theorem 3. *Let L/M be a biquadratic extension of number fields. Then*

$$|H^1(U)[2]| = 2^{3r+v+5-2t_\infty} \frac{[N_1(U_1) \cap N_2(U_2) \cap N_3(U_3) : U_M^2]}{q \prod_{i=1}^3 [N_i(U_i) : U_M^2]}.$$

Furthermore, $\lambda - r = 3r + 3 - 2t_\infty$.

Proof. We apply the results of section 2 to $W = U_L$. Clearly $W_i = U_i$, $W^\Gamma = U_M$, and $W^\Gamma[2] = \{\pm 1\}$. Note that U_L satisfies the condition $(***)$. In fact, if $u \in U_L$ and $u^2 \in U_M$ then u belongs to one of the quadratic subfields of L/M. Furthermore, U_L satisfies $(*)$ for at least two indices i. Indeed, if L cannot be obtained from M by adjoining square roots of two units of M then U_i/U_M has no 2-torsion for at least two indices i. It follows that in this case U_L satisfies $(**)$ (hence also $(*)$) for at least two indices i. Also, by Corollary 2, $\mathcal{K} = 0$ and therefore $[W^\Gamma : \mathcal{K}] = 2$. If $L = M(\sqrt{u_1}, \sqrt{u_2})$ for some units $u_1, u_2 \in U_M$ then we may assume that $\sqrt{u_i} \in U_i$ for $i = 1, 2$ and setting $u_3 = u_1 u_2$ we see that $\sqrt{u_3} \in U_3$. If $w \in U_i$ is a unit such that $w^2 \in U_M$ then $w\sqrt{u_j} \in U_k$ and $w = (\sqrt{u_j})^{-1}(w\sqrt{u_j}) \in U_j U_k$. It follows that $(*)$ holds in this case for all i. Furthermore, we have $-1 = \sqrt{u_i}/\sigma_j(\sqrt{u_i}) \in (1 - \sigma_j)W_i$. Thus $-1 \in \mathcal{K}$ and $[W^\Gamma : \mathcal{K}] = 1$. We see that $[W^\Gamma : \mathcal{K}] = 2^{1-v}$, where

$$v = \begin{cases} 1, & \text{if } L \subseteq M(\sqrt{U_M}); \\ 0, & \text{otherwise} \end{cases}$$

By Corollary 1 we get

$$|H^1(N)| = |H^1(U_1)||H^1(U_2)||H^1(U_3)|[\mathcal{N} : U_M^2]/2^{1-v},$$

where $N = U_1 U_2 U_3$ and $\mathcal{N} = N_1(U_1) \cap N_2(U_2) \cap N_3(U_3)$. Here N_i stands for the norm map from L^{σ_i} to M. Let $q = [U_L : U_1 U_2 U_3] = [W : N]$. We have $|H^1(N)| = q|H^1(U_L)[2]|$ by Corollary 3. Thus

$$|H^1(U_L)[2]| = |H^1(U_1)||H^1(U_2)||H^1(U_3)|[\mathcal{N} : U_M^2]/q2^{1-v}. \qquad (4)$$

Now we need to recall a formula for $H^1(U)$, where U is the group of units in a quadratic extension K/M. The group U has a subgroup of finite index V such that

$$V \oplus \mathbb{Z} = \oplus_v Ind_{G_v}^G(\mathbb{Z})$$

where v runs over infinite places of M and G is the Galois group of K/M. Since G is cyclic, we can use the calculus of Herbrand indexes. Note that $h(W) = h(U)$ and $h(\mathbb{Z}) = 2$. Thus $h(U) = h(W \oplus \mathbb{Z})/2$. If G_v is trivial, then $H^i(G, Ind_{G_v}^G(\mathbb{Z})) = H^i(1, \mathbb{Z}) = 0$ and $h(Ind_{G_v}^G(\mathbb{Z})) = 1$. If $G_v = G$, which happens iff v is a real place which is complexified in K, then

$h(Ind_{G_v}^{G}(\mathbb{Z})) = 2$. Let t_∞ be the number of such places. We see that $h(W \oplus \mathbb{Z}) = 2^{t_\infty}$ and therefore $h(U) = 2^{t_\infty - 1}$. Recall that $\hat{H}^0(U) = U_M/N_{K/M}(U)$ so

$$|\hat{H}^0(U)| = |U_M/U_M^2|/[N_{K/M}(U) : U_M^2] = 2^{r+1}/[N_{K/M}(U) : U_M^2],$$

where r is the $\mathbb{Z}$-rank of U_M. Thus

$$|H^1(U)| = |\hat{H}^0(U)|/h(U) = 2^{r+2-t_\infty}/[N_{K/M}(U) : U_M^2].$$

Using this formula for each of the groups U_i we see that (4) can be written as follows:

$$|H^1(U)[2]| = 2^{3(r+2)-t_{\infty,1}-t_{\infty,2}-t_{\infty,3}} \frac{[N_1(U_1) \cap N_2(U_2) \cap N_3(U_3) : U_M^2]}{2^{1-v} q \prod_{i=1}^{3} [N_i(U_i) : U_M^2]},$$

where $t_{\infty,i}$ is the number of real places of M which are complexified in L^{σ_i} (such places are often called ramified, but there are many benefits of considering them as unramified with residue degree 2; hence we try to avoid this terminology). Since every real place of M which complexifies in L complexifies in exactly two quadratic subextensions of L/M, we have $t_{\infty,1} + t_{\infty,2} + t_{\infty,3} = 2t_\infty$, where t_∞ is the number of real places of M which are complexified in L. Thus

$$|H^1(U)[2]| = 2^{3r+v+5-2t_\infty} \frac{[N_1(U_1) \cap N_2(U_2) \cap N_3(U_3) : U_M^2]}{q \prod_{i=1}^{3} [N_i(U_i) : U_M^2]}.$$

The equality $\lambda - r = 3r + 3 - 2t_\infty$ is a straightforward consequence of Dirichlet's Unit Theorem. □

Lemma 1. *Let x be a generator of the 2-torsion of the group of roots of unity μ_L. Then $H^1(\Gamma, \mu_L) = H^1(\Gamma, \mu_L)[2]$ and*

$$|H^1(\Gamma, \mu_L)[2]| = \begin{cases} 4 & \text{if } x \in U_i \text{ for some } i \text{ and } \sigma_j(x) = x^{\pm 1} \text{ for } j \neq i; \\ 2 & \text{in all other cases.} \end{cases}$$

Proof. Let μ be the 2-torsion of μ_L. Then $H^1(\Gamma, \mu_L) = H^1(\Gamma, \mu)$. We will apply the results of section 2 to $W = \mu$. Since the subgroups of μ are linearly ordered by inclusion, we may assume that $\mu_1 \supseteq \mu_2 \supseteq \mu_3$, where $\mu_i = \mu^{\sigma_i}$. It follows that $\mu_2 = \mu_3 = \mu^\Gamma$. Consequently, μ satisfies $(**)$ for at least two indices $i \in \{1, 2, 3\}$ and also satisfies $(***)$. Furthermore, we have $\mathcal{N} = (\mu^\Gamma)^2$ and $\mathcal{K} = 1$ (we use the notation established in section 2). Thus Theorem 1 (applied to $N = \mu_1$) yields

$$0 \longrightarrow \pm 1 \longrightarrow H^1(\mu_1) \times H^1(\mu_2) \times H^1(\mu_3) \longrightarrow H^1(\Gamma, \mu_1) \longrightarrow 0,$$

where $H^1(\mu_i) = H^1(\Gamma/\{1, \sigma_i\}, \mu_i)$. Note that $|H^1(\mu_i)| = 2$ for $i = 2, 3$ since μ_i is a trivial Γ-module. Since Herbrand index of a finite module is 1, we have $|H^1(\mu_1)| = |\hat{H}^0(\mu_1)|$. The generator of $\Gamma/\{1, \sigma_1\}$ acts on μ_1 as

automorphism of order ≤ 2, hence it is one of $x \mapsto x$, $x \mapsto x^{-1}$, $x \mapsto x^{2^n \pm 1}$, where $|\mu_1| = 2^{n+1}$. It is now straightforward to see that

$$|H^1(\mu_1)| = \begin{cases} 2 & \text{if } \sigma_2(x) = x^{\pm 1}; \\ 1 & \text{in all other cases.} \end{cases}$$

Thus

$$|H^1(\Gamma, \mu_1)| = \begin{cases} 4 & \text{if } \sigma_2(x) = x^{\pm 1}; \\ 2 & \text{in all other cases.} \end{cases}$$

If $\mu \neq \mu_1$ then $|\mu| \geq 8$ and Γ acts faithfully on μ. Thus σ_i acts on μ via $x \mapsto x^{1+2^n}$ for some i, and then μ^2 is fixed by this automorphism but $\mu^2 \not\subseteq \mu^\Gamma$. It follows that $i = 1$, $\mu_1 = \mu^2$ and σ_2 acts on μ_1 as $x \mapsto x^{-1}$. Thus $|H^1(\Gamma, \mu_1)| = 4$. By Corollary 3 we get $|H^1(\Gamma, \mu)[2]| = 2$. Finally, it is easy to check that every 1-cocycle in $\mathcal{Z}(\Gamma, \mu)$ has values in μ^2 so $H^1(\Gamma, \mu)[2] = H^1(\Gamma, \mu)$. □

Let us now consider more carefully a special case when M is an imaginary quadratic field. In this case we have $r = v = t_\infty = 0$ and Theorem 3 gives the following equality

$$|H^1(U)[2]| = 2^5 \frac{[N_1(U_1) \cap N_2(U_2) \cap N_3(U_3) : U_M^2]}{q \prod_{i=1}^3 [N_i(U_i) : U_M^2]}.$$

Note that the groups U_i have $\mathbb{Z}$-rank 1, so we may speak about fundamental units of U_i (i.e. generators of U_i modulo torsion). Clearly $[N_i(U_i) : U_M^2] \leq 2$ and equality holds iff either $\sqrt{-1} \notin M$ and U_i has fundamental unit of norm -1 or $M = \mathbb{Q}[\sqrt{-1}]$ and U_i has fundamental unit of norm $\sqrt{-1}$. We have the following

Lemma 2. *Let M be an imaginary quadratic field. Then $(U_L/\mu_L)^\Gamma = 1$ and $H^1(\Gamma, \mu_L)$ embeds into $H^1(\Gamma, U_L)$.*

Proof. Let $V_L = U_L/\mu_L$. If $a \in V_L^\Gamma$ then a is represented by a unit $a \in U_L$ such that $\sigma_i(u) = \epsilon_i u$ for some $\epsilon_i \in \mu_L$, $i = 1, 2, 3$. Thus $u^k \in U_M$ for k divisible by the orders of ϵ_i. Since $U_M \subseteq \mu_L$, we have $u \in \mu_L$ and $a = 1$. This shows that $V_L^\Gamma = 1$.

From the long exact sequence of cohomology applied to the exact sequence $0 \longrightarrow \mu_L \longrightarrow U_L \longrightarrow V_L \longrightarrow 0$ we immediately get the embedding of $H^1(\Gamma, \mu_L)$ into $H^1(\Gamma, U_L)$. □

Theorem 4. *Let M be an imaginary quadratic field. Then $q \leq 8$ and the equality holds iff $H^1(\Gamma, U_L)[2] = H^1(\Gamma, \mu_L)$ and one of the following conditions is satisfied:*

(1) *$\sqrt{-1} \notin L$ and each L_i has a fundamental unit of norm 1.*
(2) *$\sqrt{-1} \in L$, $\sqrt{-1} \notin M$, $\sqrt{2} \notin L$ and each L_i has a fundamental unit of norm 1.*

(3) $\sqrt{-1} \in M$, $\sqrt{-2} \notin L$ *and each* L_i *has a fundamental unit of norm* 1.
(4) $\sqrt{-2} \in M$, $\sqrt{-1} \notin L$ *and each* L_i *has a fundamental unit of norm* 1.
(5) $L = M(\sqrt{-1}, \sqrt{2})$ *and each of* $M(\sqrt{-1})$, $M(\sqrt{-2})$ *has fundamental units of norm* 1.
(6) $L_i = \mathbb{Q}(\sqrt{-1}, \sqrt{-2})$ *for some* i *and each of* L_j, L_k *has fundamental unit of norm* 1.

Proof. We use the equality

$$|H^1(U)[2]| = 2^5 \frac{[N_1(U_1) \cap N_2(U_2) \cap N_3(U_3) : U_M^2]}{q \prod_{i=1}^3 [N_i(U_i) : U_M^2]}.$$

In cases (1)-(4) we have $|H^1(\Gamma, \mu_L)[2]| = 4$ by Lemma 1. Thus $|H^1(\Gamma, U_L)[2]| \geq 4$ by Lemma 2. If $|H^1(\Gamma, U_L)[2]| \geq 8$ then $q \leq 4\frac{[N_1(U_1)\cap N_2(U_2)\cap N_3(U_3):U_M^2]}{\prod_{i=1}^3 [N_i(U_i):U_M^2]} \leq 4$. If $|H^1(\Gamma, U_L)[2]| = 4$ then $q = 8$ iff $\frac{[N_1(U_1)\cap N_2(U_2)\cap N_3(U_3):U_M^2]}{\prod_{i=1}^3 [N_i(U_i):U_M^2]} = 1$, which happens iff each L_i has a fundamental unit of norm 1.

In cases (5) and (6) Lemma 1 yields $|H^1(\Gamma, \mu_L)[2]| = 2$. Thus $|H^1(\Gamma, U_L)[2]| \geq 2$ by Lemma 2. In case (5) the field $L_i = M(\sqrt{2})$ has a unit of norm -1 and therefore $[N_i(U_i) : U_M^2] = 2$. Similarly, in case (6) the field $L_i = \mathbb{Q}(\sqrt{-1}, \sqrt{-2})$ has a unit of norm $\sqrt{-1}$ (namely the primitive 8-th root of unity) and therefore $[N_i(U_i) : U_M^2] = 2$. Thus

$$q \leq 16 \frac{1}{|H^1(\Gamma, U_L)[2]|} \frac{[N_1(U_1) \cap N_2(U_2) \cap N_3(U_3) : U_M^2]}{\prod_{j \neq i} [N_j(U_j) : U_M^2]}$$

and the equality $q = 8$ holds iff $|H^1(\Gamma, U_L)[2]| = 2$ (i.e. $H^1(\Gamma, U_L)[2] = H^1(\Gamma, \mu_L)$) and both L_j, L_k have fundamental units of norm 1. □

In an unpublished manuscript Lemmermeyer speculates about the upper bound for q in biquadratic extensions. For imaginary quadratic M his upper bound is 8, which agrees with the upper bound we obtained. He suggests though that if L/M is unramified then the equality is obtained only if the 2-part of the class group of M is of type $(2, 2)$ and L has odd class number. The example following Proposition 7 in section 5 shows that this is false.

In our investigation of the Galois module structure of V_L we are interested not in the index q but rather in the index $Q = [U_L : \mu_L U_1 U_2 U_3]$. When M is an imaginary quadratic field then $q = Q$ except perhaps when $L = M(\sqrt{-1}, \sqrt{2})$. In this case we have in fact $q = 2Q$ as we will now show. It amounts to proving that $w = u_1 u_2 u_3$ is not possible, where w is a primitive 8-th root of 1 and $u_i \in U_i$. Since $V = V_1 \times V_2 \times V_3$, the equality $w = u_1 u_2 u_3$ implies that the image of u_i in V_i is trivial for $i = 1, 2, 3$, i.e. each u_i is a root of unity. Since w has order 8, at least one of u_1, u_2, u_3 would have order divisible by 8, which is not possible.

4. Capitulation

The equality of Theorem 3 resembles some formulas in the paper [5] by Lemmermeyer, which are key to his proof of Kuroda's class number formula for biquadratic extensions. We show now that indeed his computations are essentially equivalent to Theorem 3, except that his paper contains a small but confusing mistake (it does not however affect the validity of his results). Our results provide therefore a more conceptual explanation of Lemmermeyer's computation.

We start with some general observations. For a number field L we denote by I_L, P_L the groups of fractional ideals and fractional principal ideals respectively. Suppose that L/M is a Galois extension with Galois group Γ. Let $H = \mathrm{Ker}(Cl_M \longrightarrow Cl_L)$ be the capitulation kernel and set $B = \mathrm{Im}(Cl_M \longrightarrow Cl_L)$. By A we denote the subgroup of Cl_L consisting of strictly ambiguous ideal classes. Thus we have the following exact sequence

$$0 \longrightarrow P_L^\Gamma \longrightarrow I_L^\Gamma \longrightarrow A \longrightarrow 0.$$

Applying the snake lemma to the following diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & P_M & \longrightarrow & I_M & \longrightarrow & Cl_M & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & P_L^\Gamma & \longrightarrow & I_L^\Gamma & \longrightarrow & A & \longrightarrow & 0 \end{array}$$

(note that the left two vertical arrows are injective) we get the exact sequence

$$0 \longrightarrow H \longrightarrow P_L^\Gamma/P_M \longrightarrow I_L^\Gamma/I_M \longrightarrow A/B \longrightarrow 0.$$

Recall now that applying the long exact sequence of cohomology to the exact sequence of Γ-modules

$$0 \longrightarrow U_L \longrightarrow L^\times \longrightarrow P_L \longrightarrow 0$$

and using Hilbert's Theorem 90 we get an exact sequence

$$0 \longrightarrow U_M \longrightarrow M^\times \longrightarrow P_L^\Gamma \longrightarrow H^1(U_L) \longrightarrow 0$$

which allows us to identify P_L^Γ/P_M with $H^1(U_L)$. Thus we have the following exact sequence

$$0 \longrightarrow H \longrightarrow H^1(U_L) \longrightarrow I_L^\Gamma/I_M \longrightarrow A/B \longrightarrow 0. \qquad (\diamond)$$

The group I_L^Γ/I_M is fairly easy to describe. It is a direct sum of cyclic groups $\mathbb{Z}/e(\mathfrak{p})\mathbb{Z}$ indexed by prime ideals $\mathfrak{p}$ of M which ramify in L, where $e(\mathfrak{p})$ is the ramification index of $\mathfrak{p}$. Thus

$$|I_L^\Gamma/I_M| = 2^{s+t},$$

where t is the number of primes of M which ramify in L and s is the number of primes of M which are totally ramified in L.

Suppose now that Γ is the Klein four-group. A substantial part of Lemmermeyer's paper is devoted to his formula (2.5) for the index $[R : R_\pi]$. Here R is the group of fractional ideals of L of the form $I_1 I_2 I_3$, where I_i is the image of an ambiguous fractional ideal of L_i. He defines R_π as the principal ideals of R but this is incorrect. It should be defined as those principal fractional ideals of L whose square comes from a principal ideal of M. This is in fact the group Lemmermeyer uses in his computations so the mistake does not affect the validity of his results. Let R_π^* be the group of principal ideals in R. Let A^* be the image of R in A, so $[R : R_\pi^*] = |A^*|$.

From the point of view of the sequence $(\diamond)$, the image of R in I_L^Γ/I_M coincides with $(I_L^\Gamma/I_M)[2]$ and A^*/B is the image of $(I_L^\Gamma/I_M)[2]$ in A/B. Let $H^1(U_L)^*$ be the preimage of $(I_L^\Gamma/I_M)[2]$ in $H^1(U_L)$. Then we have an exact sequence

$$0 \longrightarrow H \longrightarrow H^1(U_L)^* \longrightarrow (I_L^\Gamma/I_M)[2] \longrightarrow A^*/B \longrightarrow 0$$

from which we get $|A^*| = 2^t h_M/|H^1(U_L)^*|$. Under the surjection $P_L^\Gamma \longrightarrow H^1(U_L)$ the group R_π^* is mapped onto $H^1(U_L)^*$ and R_π is the preimage in R_π^* of $H^1(U_L)[2]$. Thus $[R_\pi^* : R_\pi] = [H^1(U_L)^* : H^1(U_L)[2]]$. Consequently,

$$\begin{aligned}[R : R_\pi] = |A^*|[R_\pi^* : R_\pi] &= (2^t h_M/|H^1(U_L)^*|)[H^1(U_L)^* : H^1(U_L)[2]] \\ &= 2^t h_M/|H^1(U_L)[2]|\end{aligned}$$

Thus Theorem 2 gives us a formula for $[R : R_\pi]$ which coincides with the formula obtained by Lemmermeyer. It would be interesting to find a direct relation of $H^1(U_L)[2]$ to Kuroda's class number formula.

5. The unit index

In this section we use the following notation.

- $M = \mathbb{Q}(\sqrt{-A})$ is an imaginary quadratic field, where A is a positive, square-free integer;
- L is a biquadratic extension of M;
- U is the group of units of L and $V = U/\mu_L$.
- $\Gamma = \{1, \sigma_1, \sigma_2, \sigma_3\}$ is the Galois group of L/M, L_i is the fixed field of σ_i;
- U_i is the group of units of L_i; $V_i = U_i/\mu_{L_i}$.
- ε_i is a fundamental unit of U_i (i.e. a unit which generates V_i). We may (and will) assume that the norm from L_i to M of ε_i is a root of unity of order a power of 2 (more precisely, it is one of $1, -1, \sqrt{-1}$).

By Dirichlet's Unit Theorem, the group V is a free abelian group of rank 3. In what follows, we use the same notation for units and their images in V. The norm map for a finite extension F/K of fields is denoted by $N_{F/K}$.

If u is a unit of L then we write $u(i)$ for the norm $N_{L/L_i} u$ of u.

Lemma 3. $V^2 \subseteq V_1V_2V_3$.

Proof. Let $u \in U$. Note that $u(1)u(2)u(3) = u^2N_{L/M}u$, i.e. $u^2 = u(1)u(2)u(3)/N_{L/M}u$. It follows that $U/U_1U_2U_3$ is an elementary abelian 2-group and so is $V/V_1V_2V_3$. Since V is a free abelian group of rank 3, we have $[V : V_1V_2V_3] \leq 8$. □

We call a prime ideal **odd** if it contains an odd prime number.

Lemma 4. *Suppose there is a unit $u \in U$ of infinite order such that $v = u^2 \in U_1$ but $u \notin U_1$. Then the sets of odd primes of M which ramify in L_2 and L_3 are disjoint and their union is the set of odd primes which ramify in L_1.*

Proof. We have $L = L_1(\sqrt{v})$. From the theory of ramification in Kummer extensions (see [1], section I.6) odd primes of L_1 are unramified in L/L_1. Thus if an odd prime of M ramifies in L/M then it must ramify in L_1/M and its ramification degree in L/M is 2. Thus the inertia subgroup of this prime has order 2 and it is unramified in the fixed field of the inertia, which must be one of L_2, L_3. Finally, since $L = L_2L_3$, every prime which ramifies in L/M must ramify in one of L_2/M or L_3/M. □

Proposition 1. *Suppose that $V_iV_j \subseteq V^2$ for some $i \neq j \in \{1, 2, 3\}$. Then no odd prime of M ramifies in L_k/M, where $\{i, j, k\} = \{1, 2, 3\}$.*

Proof. We may assume that $i = 1$, $j = 2$. Our assumptions imply that there are units $w_1, w_2 \in U$ and torsion units $\chi_1, \chi_2 \in U$ such that $w_i^2 = \chi_i\varepsilon_i$ for $i = 1, 2$. We may assume that the orders of χ_1, χ_2 are powers of 2. Clearly $w_i \notin U_i$ but w_i raised to sufficiently large power of 2 belongs to U_i. Thus there exist units u_1, u_2 such that $u_i^2 \in U_i$ but $u_i \notin U_i$, $i = 1, 2$. By Lemma 4, odd primes which ramify in L_3 are disjoint from primes which ramify in L_i and ramify in L_{3-i} for $i = 1, 2$, which is a clear contradiction. □

Proposition 2. *If $[V : V_1V_2V_3] = 8$ then no odd prime of M ramifies in L/M.*

Proof. The equality $[V : V_1V_2V_3] = 8$ is equivalent to $V^2 = V_1V_2V_3$. Proposition 2 is therefore a straightforward consequence of Proposition 1. □

Proposition 3. *Suppose that either $\sqrt{-1} \notin L$ or $A > 2$. Any unit $u \in U$ such that $N_{L/M}(u)$ has odd order is of the form $u = \pm\sqrt{r\hat{\varepsilon}_1^{m_1}\hat{\varepsilon}_2^{m_2}\hat{\varepsilon}_3^{m_3}}$, where*

$$\hat{\varepsilon}_i = \begin{cases} \varepsilon_i & \text{if the norm of } \varepsilon_i \text{ is } 1, \\ \varepsilon_i^2 & \text{otherwise} \end{cases}$$

and r is a root of unity.

Any $u \in U$ such that $N_{L/M}(u)$ has even order is of the form $u = \pm\sqrt{r\varepsilon_1^{m_1}\varepsilon_2^{m_2}\varepsilon_3^{m_3}}$, where r is a root of unity and $1 \equiv m_1 \equiv m_2 \equiv m_3 \pmod 2$.

Proof. Our assumption guarantees that the norms from L_i to M and from L to M of any torsion unit have odd order. We may assume that $N_{L/M}(u) = \pm 1$. We may write $u(i) = \varepsilon_i^{a_i} t_i$, where t_i is a torsion unit in U_i of norm 1. Note that

$$\pm 1 = N_{L/M}(u) = N_{L_j/M}(u(j)) = N_{L_j/M}(t_j) N_{L_j/M}(\varepsilon_j)^{a_j} = N_{L_j/M}(\varepsilon_j)^{a_j}.$$

Suppose that $N_{L/M}(u) = 1$. Then $1 = N_{L_j/M}(\varepsilon_j)^{a_j}$. In particular, a_j is even if ε_j has norm -1. Thus $u^2 = u^2 N_{L/M}(u) = u(1)u(2)u(3) = r\hat{\varepsilon}_1^{m_1}\hat{\varepsilon}_2^{m_2}\hat{\varepsilon}_3^{m_3}$.

If $N_{L/M}(u) = -1$ then $N_{L_j/M}(\varepsilon_j)^{a_j} = -1$, so ε_j has norm -1 and a_j is odd. Again $u^2 = u^2 N_{L/M}(u) = -u(1)u(2)u(3) = r\varepsilon_1^{m_1}\varepsilon_2^{m_2}\varepsilon_3^{m_3}$, where all m_i are odd. □

As a straightforward corollary we get

Corollary 4. *If either $\sqrt{-1} \notin L$ or $A > 2$ and if ε_i is a square in V then the norm of ε_i is 1.* □

Before we proceed any further let us recall some useful facts about units in real quadratic fields which we combine in the following lemma (see [6] for more details).

Lemma 5. *Let K be a real quadratic field with a fundamental unit of norm 1 and let σ be the non-trivial automorphism of K. There exists unique positive integer $\delta = \delta(K)$ that is a square-free divisor of the discriminant d of K such that for some (or, equivalently, any) unit $\varepsilon > 0$ in K which is not a square in K we have $\delta = a\sigma(a)$ for some integer a of K satisfying $\varepsilon = \sigma(a)/a$. We have $K(\sqrt{\pm\varepsilon}) = K(\sqrt{\pm\delta})$.*

For a square free divisor $m > 0$ of d the following are equivalent:

1. *$m = \delta$;*
2. *m is a norm of an integer in K;*
3. *$-n$ is a norm of an integer in K, where $n \neq m$ is the unique square-free positive divisor of d such that nm is a square in K.*

We will need later the following immediate corollary

Corollary 5. *Let K be a real quadratic field with fundamental unit of norm 1 and discriminant d. Denote by m the odd part of d. Then $\delta = 2$ iff 2 ramifies in K and 2 is a norm of an integer of K, and $\delta \in \{m, 2m\}$ iff 2 ramifies in K and -2 is a norm of an integer of K.*

Lemma 6. *Let $K = M(i) = \mathbb{Q}(\sqrt{-A}, i)$ and let $K^+ = \mathbb{Q}(\sqrt{A})$. Denote by v a fundamental unit of K^+. The unit index of K/K^+ is 2 iff 2 ramifies in K^+ and either 2 or -2 is a norm of an integer in K^+. Moreover, if the unit index is 2, then the norm of v is 1, $u = \sqrt{iv}$ is a fundamental unit of K and $N_{K/M}(u) = 1$ iff 2 is a norm of an integer in K^+.*

Proof. Let $\{1, \tau_1, \tau_2, \tau_3\}$ be the Galois group of $K/\mathbb{Q}$, where τ_1 fixes M, τ_2 fixes K^+. If $A = 2$ then it is known that the unit index is 1, so we assume that $A > 2$.

Suppose first that 2 ramifies in K^+ and $\pm 2 = x\tau_1(x)$ is a norm of an integer $x \in K^+$. Then $(1+i)/x$ is a unit of K, so the unit index must be 2.

Suppose now that the unit index is 2. Thus $u^2 = rv$ for some unit u of K and a root of unity r in K. Since $i \in K$ (and K does not contain a primitive eight root of 1), we may assume that either $r = 1$ or $r = i$. Thus $N_{K/M}(u)^2 = N_{K/M}(r)N_{K/M}(v) = N_{K^+/\mathbb{Q}}(v) = \pm 1$. Since $i \notin M$, we have $N_{K/M}(u) = \pm 1$ and therefore $N_{K^+/\mathbb{Q}}(v) = 1$. Thus we may assume that v is totally positive. The equality $u^2 = v$ would imply that u is totally real, hence $K = K^+(u)$ would be real, which is false. Therefore $u^2 = iv$. Recall now that, since v has norm 1, there is a square-free positive divisor $\delta = \delta(v)$ of the discriminant of K^+ and an integer x of K^+ such that $v = \tau_1(x)/x$ and $x\tau_1(x) = \delta$. It follows that

$$iv = (1+i)\tau_1(x)/(1-i)x = (1+i)(1-i)x\tau_1(x)/[(1-i)x]^2 = 2\delta/[(1-i)x]^2$$

and consequently $u = \pm\sqrt{2\delta}/(1-i)x$. Thus $\sqrt{2\delta}$ is in K and hence in K^+. If δ is odd then $A = 2\delta$ and $y = \sqrt{A}/x$ is an integer in K^+ of norm -2. Also, 2 ramifies in K^+ and the norm $N_{K/L}(u) = u\tau_1(u) = -1$.

If δ is even then either $2A = \delta$ or $\delta = 2$. In the former case, $y = 2\sqrt{A}/x$ is an integer in K^+ of norm -2, 2 ramifies in K^+ and the norm $N_{K/L}(u) = u\tau_1(u) = -1$. In the latter case, 2 ramifies in K^+ and it is the norm of x. Also, $N_{K/L}(u) = u\tau_1(u) = 1$. This completes the proof. □

In the remaining part of this section we are going to investigate biquadratic extensions L/M with unit index $Q = 8$. By Proposition 2, only primes over 2 can ramify in L/M. If L/M is unramified, then by genus theory L is contained in the genus field of M. In particular, L is abelian over $\mathbb{Q}$ and $L = ML^+$ for unique real biquadratic field L^+. The following proposition describes another instance when $Q = 8$ implies that $L = ML^+$ for a real biquadratic field L^+.

Proposition 4. *Suppose that L contains a real quadratic subfield $\mathbb{Q}(\sqrt{d})$ of discriminant d. If $[V : V_1V_2V_3] = 8$ then $L = ML^+$ for some totally real biquadratic extension $L^+/\mathbb{Q}$ unless $A > 2$ and one of the following is true:*

(1) *$Q(\sqrt{d}) = Q(\sqrt{2A})$, there are integers a, b such that $2 = a^2 - Bb^2$ where B is the square-free part of $2A$ and $L = \mathbb{Q}(w)$, where w is a root of $P(x) = x^8 + 2(a^2-1)x^4 + 1$;*

(2) *$d = 4A$, there are integers a, b such that $2 = a^2 - Ab^2$ and $L = \mathbb{Q}(w)$, where w is a root of $P(x) = x^8 - 2ax^6 + 2a^2x^4 - 2ax^2 + 1$.*

Proof. Suppose first that $K = \mathbb{Q}(i, \sqrt{2}) \subseteq L$. If $M \not\subset K$ then $L = M(i, \sqrt{2})$, which is not possible since we have noticed at the end of section 3 that $Q = q/2 \leq 4$ in this case. If $M \subset K$ then $K = L_j$ for some j. Since $u = 1 - \sqrt{2}$ is a unit of K, either u or $\zeta_8 u$ is a square in L. Thus L is one of the fields $\mathbb{Q}(\zeta_8, \sqrt{u})$, $\mathbb{Q}(\zeta_8, \sqrt{\zeta_8 u}) = \mathbb{Q}(\zeta_8, \sqrt[4]{2})$. As proved in [2][Example 2.14.], these are the only two dihedral extensions of $\mathbb{Q}$ ramified only at 2, and each has class number 1. Kuroda's class number formula implies that $Q = 4$ for each of these fields, a contradiction.

It follows that K is not a subfield of L. Since L/M is unramified at odd primes by Proposition 2, we see that every odd prime divisor of d must divide A. Thus $A > 2$. By Corollary 4, a fundamental unit $\varepsilon > 0$ of $\mathbb{Q}(\sqrt{d})$ has norm 1. Let $\delta(Q(\sqrt{d})) = \delta$. The assumption $Q = 8$ implies that L contains one of $\sqrt{\varepsilon}$, $\sqrt{-\varepsilon}$, $\sqrt{i\varepsilon}$.

If $\sqrt{\varepsilon} \in L$ then $\mathbb{Q}(\sqrt{\delta})$ is a real quadratic subfield of L different from $\mathbb{Q}(\sqrt{d})$ and we may take $L^+ = \mathbb{Q}(\sqrt{d}, \sqrt{\delta})$.

If $\sqrt{-\varepsilon} \in L$ then $\sqrt{-\delta}$ is in L and therefore $\mathbb{Q}(\sqrt{A\delta})$ is a real quadratic subfield of L. Thus we may take $L^+ = Q(\sqrt{d}, \sqrt{A\delta})$ unless $Ad\delta$ is a perfect square. Suppose then that $Ad\delta$ is a perfect square. If p is an odd prime divisor of δ then p divides d hence also A, and $Ad\delta$ cannot be a perfect square. Thus $\delta = 2$ and $Q(\sqrt{d}) = Q(\sqrt{2A})$. Let B be the square-free part of $2A$. The equality $\delta = 2$ implies that $2 = a^2 - b^2 B$ for some integers a, b such that $\varepsilon = (a + b\sqrt{B})/(a - b\sqrt{B})$. Since $\sqrt{-2} \in L$, we have $i \notin L$ and $\sqrt{-\varepsilon} = \sqrt{-2}/(a - b\sqrt{B}) \in M(\sqrt{-2}) = L_1$. Again from $Q = 8$ we see that L contains either $w = \sqrt{\sqrt{-\varepsilon}}$ or $w = \sqrt{-\sqrt{-\varepsilon}}$. It is easy to see that the minimal polynomial (over $\mathbb{Q}$) of both $\pm\sqrt{-\varepsilon}$ is equal to $x^4 + 2(a^2 - 1)x^2 + 1$ and the minimal polynomial of w is $x^8 + 2(a^2 - 1)x^4 + 1$. Thus L satisfies all the conditions of (1).

Finally, if $\sqrt{i\varepsilon} \in L$ then $i \in L$. If $\mathbb{Q}(\sqrt{d}) \neq \mathbb{Q}(\sqrt{A})$ then we may take $L^+ = \mathbb{Q}(\sqrt{d}, \sqrt{A})$. Suppose then that $\mathbb{Q}(\sqrt{d}) = \mathbb{Q}(\sqrt{A})$. Since $L_1 = M(i)$ has fundamental unit of norm 1 by Corollary 4, Lemma 6 applied to $M(i)$ tells us that either ε is a fundamental unit of L_1 or $\delta = 2$. Let $a + b\sqrt{A}$ be an integer in $\mathbb{Q}(\sqrt{A})$ such that $\delta = a^2 - Ab^2$ and $\varepsilon = (a + b\sqrt{A})/(a - b\sqrt{A})$. Note that $\eta = \sqrt{i\varepsilon} = \sqrt{2\delta}/(1-i)(a-b\sqrt{A})$. Thus $\sqrt{2\delta} \in L$. If $\sqrt{2\delta} \notin \mathbb{Q}(\sqrt{A})$ then $L^+ = Q(\sqrt{A}, \sqrt{2\delta})$. Otherwise $\sqrt{i\varepsilon} \in L_1$ so ε is not a fundamental unit of L_1 and $\delta = 2$. Thus 2 is ramified in $\mathbb{Q}(\sqrt{A})$ and therefore $a, b \in \mathbb{Z}$. The equality $Q = 8$ implies now that either $\sqrt{\eta} \in L$ or $\sqrt{-i\eta} \in L$. Note that η and $-i\eta$ are conjugate over $\mathbb{Q}$ and their minimal polynomial over $\mathbb{Q}$ is $Q(x) = x^4 - 2ax^3 + 2a^2x^2 - 2ax + 1$. Thus both $w = \sqrt{\eta}$ and $w = \sqrt{-i\eta}$ have minimal polynomial over $\mathbb{Q}$ equal to $P(x) = x^8 - 2ax^6 + 2a^2x^4 - 2ax^2 + 1$ and $L = \mathbb{Q}(w)$. In other words, L satisfies all the requirements of (2). $\square$

The exceptions in Proposition 4 are not merely due to the method of its proof. In fact, using PARI and Kuroda's class number formula we checked that $Q = 8$ for $a = 6, 7, 14, 15, 22, 26, 30, 33, 34, 39, 42, 47, 49, 50, 54, 62, 63, 70, 71, 78, 86, 89, 90, 98$ in (1) and for $a = 6, 8, 14, 16, 22, 26, 30, 40, 42, 50, 54, 56, 62, 70, 72, 78, 86, 90, 96, 98$ in (2). Note that in (2) we have no example of $Q = 8$ when a is odd (tested for $3 \le a \le 1000$). It is reasonable to conjecture that $Q \neq 8$ for L as in (2) and any odd a, but at present we are not able to prove this. Perhaps it is worth mentioning that the normal closure F of each of the fields L defined in (1) and (2) is of degree 16 over $\mathbb{Q}$ and the Galois group of $F/\mathbb{Q}$ is isomorphic to the direct product of a cyclic group of order 2 and the dihedral group of order 8. In fact, in (1) the field F is the compositum of $\mathbb{Q}(\sqrt{-1})$ and $\mathbb{Q}(\sqrt{2}, \sqrt{2+a\sqrt{2}}, \sqrt{2-a\sqrt{2}})$ and F is the compositum of $\mathbb{Q}(\sqrt{-1})$ and $\mathbb{Q}\left(\sqrt{-A}, \sqrt{(2+a)+b\sqrt{-A}}, \sqrt{(2+a)-b\sqrt{-A}}\right)$ in case (2).

It follows that there are many biquadratic fields L/M which have index $Q = 8$ but $L/\mathbb{Q}$ is not abelian. We are not able to say much about such fields. Thus we are going to focus our attention on extensions L/M of the form $L = ML^+$ with index $Q = 8$. More precisely, we are going to look for conditions on A and L^+ which guarantee the equality $[V : V_1V_2V_3] = 8$. We will use the following notation:

- L^+ is a real biquadratic extension of $\mathbb{Q}$ and $L = L^+M$;
- L_i^+, $i = 1, 2, 3$ are the quadratic subfields of L^+. In particular, $L_i = L_i^+M$.
- U^+ and V^+ are the units of L^+ and the units of L^+ modulo torsion respectively.
- U_i^+ is the group of units of L_i^+; $V_i^+ = U_i^+$ modulo torsion.
- $\Gamma = \{1, \sigma_1, \sigma_2, \sigma_3\}$ can be canonically identified with the Galois group of $L^+/\mathbb{Q}$ and then L_i^+ is the fixed field of σ_i.
- d_i is the discriminant of L_i^+, D is the discriminant of M.
- ε_i is the unique fundamental unit of L_i^+ which is larger than 1 (we consider L as a subfield of $\mathbb{C}$).

It is known that $[V : V^+] \le 2$ (see [3]). Recall that $[V^+ : V_1^+V_2^+V_3^+] \le 4$. It follows that $[V : V_1V_2V_3] = 8$ iff $[V : V^+] = 2$, $[V^+ : V_1^+V_2^+V_3^+] = 4$, and $[V_i : V_i^+] = 1$ for $i = 1, 2, 3$. In particular, we may choose for a fundamental unit of U_i a fundamental unit of U_i^+ (if the unit index is 8). If ε_i has norm 1 then we set $\delta_i(L_i^+) = \delta_i$.

Since we must have $[V^+ : V_1^+V_2^+V_3^+] = 4$, there are three possibilities (after renumbering if necessary; see [6]):

Type I: $\sqrt{\varepsilon_1}, \sqrt{\varepsilon_2}, \varepsilon_3$ is a basis of V^+;

Type II: $\sqrt{\varepsilon_1\varepsilon_2}, \varepsilon_2, \sqrt{\varepsilon_3}$ is a basis of V^+;

Type III: $\sqrt{\varepsilon_1\varepsilon_2}, \sqrt{\varepsilon_2\varepsilon_3}, \sqrt{\varepsilon_3\varepsilon_1}$ is a basis of V^+.

We will consider each type separately.

Proposition 5. *Suppose that the units of L^+ are of type I. Then there is no imaginary quadratic field M such that the unit index of ML^+/M is 8.*

Proof. Suppose that $L = ML^+$ has unit index 8 (and $A > 1$). The units ε_1, ε_2 have norm 1. As in the proof of Proposition 1, no odd prime can ramify in L_3^+. Thus $L_3^+ = \mathbb{Q}(\sqrt{2})$ and there is an odd integer $m > 1$ such that $L_1^+ = \mathbb{Q}(\sqrt{2m})$ and $L_2^+ = \mathbb{Q}(\sqrt{m})$ (possibly after renumbering the fields). Since $\varepsilon_3 = 1+\sqrt{2}$ has norm -1, we must have $i \in L$ and $A = 2$ by Corollary 4. This however implies that there is an odd prime which ramifies in L_2/M, which contradicts Proposition 2.

The above argument did not treat the case of $M = \mathbb{Q}(i)$. Recall that δ_1, δ_2 are squares in L^+. There is no proper and larger than 1 divisor of m which is a square in L^+. Thus we must have $m \equiv -1 \pmod 4$, $d_2 = 4m$, $\delta_2 = 2$. Since $2 = \delta_2$ is a norm of an integer of L_2^+ and 2 ramifies in L_2^+, Lemma 3 tells us that $[V_2 : V_2^+] = 2$ so $[V : V_1V_2V_3]$ cannot be 8. □

It remains to consider the cases when the units of L^+ are of type II or III. Note that in both cases the units ε_1, ε_2, ε_3 have norm 1. In particular, $\sqrt{2} \notin L^+$ since a fundamental unit of $\mathbb{Q}(\sqrt{2})$ has norm -1. If M is an imaginary quadratic field such that the unit index of $L^+M = L/M$ is 8 then for each $i \in \{1, 2, 3\}$ there is a torsion unit ρ of order a power of 2 and such that $\sqrt{\rho\epsilon_i} \in U$. Since $\sqrt{2} \notin L$ and L is not real, the only possibility is that $\rho = -1$ or $\rho = i$. Thus for each $i \in \{1, 2, 3\}$, either $\sqrt{-\varepsilon_i}$ or $\sqrt{i\varepsilon_i}$ belongs to L.

Lemma 7. *Let $L/\mathbb{Q}$ be an abelian extension of type $(2, 2, 2)$. There is at most one imaginary quadratic subfield M of L such that the unit index for L/M is 8.*

Proof. Suppose that M_1, M_2 are two such subfields. Thus odd primes of M_i are unramified in L/M_i by Proposition 2. It follows that the sets of odd primes ramified in $M_i/\mathbb{Q}$ are the same for $i = 1, 2$. Thus no odd prime ramifies in the real quadratic subfield of M_1M_2, i.e. $\sqrt{2} \in L$, which we have seen is not possible. □

Proposition 6. *Suppose that the units of L^+ are of type II. There exists unique imaginary quadratic subfield M of $L^+(i)$ such that the unit index of ML^+/M is 8. Also there exists a unique imaginary quadratic field M such that $i \notin ML^+$ and the unit index of ML^+/M is 8.*

Proof. We first show that there are at most two imaginary quadratic fields M such that the unit index of ML^+/M is 8. Set $L = ML^+$. We have seen that ϵ_i is a fundamental unit of U_i. Recall $L = L^+(\sqrt{-\epsilon_1})$ or $L = L^+(\sqrt{i\epsilon_1})$

and, by Lemma 7, for each of these two choices of L there is at most one imaginary quadratic field M such that L/M has unit index 8. Note also that $i \in L = L^+(\sqrt{i\epsilon_1})$ and $i \notin L^+(\sqrt{-\epsilon_1})$ (otherwise we would have $\sqrt{\epsilon_1} \in L^+$).

To complete the proof it suffices now to find two imaginary quadratic fields M for which the unit index of ML^+/M is 8. We will show that $M = \mathbb{Q}(\sqrt{-d_1d_2})$ and $M = \mathbb{Q}(\sqrt{-2d_1d_2})$ both satisfy this requirement.

Since $\sqrt{\epsilon_1\epsilon_2} \in L^+$, the proof of Lemma 2 shows that no odd prime can ramify in both L_1^+ and L_2^+, i.e. (d_1, d_2) is a power of 2. We may write $d_i = 2^{s_i}a_i$ $(i = 1, 2)$, where a_i are odd and $(a_1, a_2) = 1$. Thus $d_3 = 2^s a_1 a_2$ for some s. Since $\sqrt{2} \notin L^+$, both $a_1 > 1$ and $a_2 > 1$. Let A be either a_1a_2 or $2a_1a_2$. Set $M = \mathbb{Q}(\sqrt{-A})$ and $L = ML^+$. In order to prove that the unit index of L/M is 8 we need to verify that $[V_i : V_i^+] = 1$ for $i = 1, 2, 3$ and $[V : V^+] = 2$.

By Proposition 1 of [4] the equality $[V_i : V_i^+] = 1$ holds iff neither A/δ_i nor Ad_i/δ_i is a square of a rational number. Since the odd part of A is a_1a_2 and the odd part of δ_i divides a_i for $i = 1, 2$ we easily see that $[V_i : V_i^+] = 1$ for $i = 1, 2$. Recall now that $d_3 = 2^s a_1 a_2$ and δ_3 is a square-free proper non-trivial divisor of d_3. Since $Ad_3 = 2^t(a_1a_2)^2$ and δ_3 is square-free, Ad_3/δ_3 can be a square only if $\delta_3 = 2$. This however is not possible since $\sqrt{\delta_3} \in L^+$ and $\sqrt{2} \notin L^+$. Since A and δ_3 are square-free, A/δ_3 is a square iff $A = \delta_3$. Because $\sqrt{\delta_3} \in L^+$ and $\sqrt{A} \notin L_i^+$ for $i = 1, 2$, we would have $\sqrt{\delta_3} \in L_3^+$ and this implies that ε_3 is a square in L_3^+, which is false. Thus we conclude that $[V_3 : V_3^+] = 1$.

In order to show that $[V : V^+] = 2$ it suffices to show that either $\sqrt{-\varepsilon_1}$ or $\sqrt{i\varepsilon_1}$ is in L. This is equivalent to showing that either $\sqrt{-\delta_1}$ or $\sqrt{i\delta_1}$ is in L. Since $\delta_1\delta_2$ is a square in L^+, it differs by a square of a rational number from one of $1, d_1, d_2, d_3$. Note that all these integers have square-free odd parts. Thus the odd part of δ_1 must be either 1 or a_1. In other words, $\delta_1 \in \{2, a_1, 2a_1\}$. Note that $L_3^+ = \mathbb{Q}(\sqrt{A})$ or $L_3^+ = \mathbb{Q}(\sqrt{2A})$ (since d_3 and A have the same odd parts) . Thus L contains either i or $\sqrt{-2}$. If $\delta_1 = 2$ then $\sqrt{-\delta_1} \in L$ if $\sqrt{-2} \in L$ and $\sqrt{i\delta_1} = 1 + i \in L$ if $i \in L$. If $\delta_1 = a_1$ then $L_1^+ = \mathbb{Q}(\sqrt{2a_1})$ and therefore $\sqrt{-\delta_1} = \sqrt{-2}\sqrt{2a_1} \in L$ if $\sqrt{-2} \in L$ and $\sqrt{i\delta_1} = (1 + i)\sqrt{2a_1}/4 \in L$ if $i \in L$. Finally, if $\delta_1 = 2a_1$ then $L_1^+ = \mathbb{Q}(\sqrt{a_1})$ hence $\sqrt{-\delta_1} = \sqrt{-2}\sqrt{a_1} \in L$ if $\sqrt{-2} \in L$ and $\sqrt{i\delta_1} = (1 + i)\sqrt{a_1}/4 \in L$ if $i \in L$. □

Proposition 7. *Suppose that the units of L^+ are of type III and that (d_i, d_j) has an odd prime divisor for any $i, j \in \{1, 2, 3\}$. If for some (all) $i \in \{1, 2, 3\}$ the prime 2 ramifies in L_i^+ and either 2 or -2 is a norm of an integer in L_i^+ then there is no imaginary quadratic field M such that the unit index of ML^+/M is 8. Otherwise there is exactly one imaginary*

quadratic field M such that the unit index of $L = ML^+/M$ is 8. This L does not contain i.

Proof. Recall that the units ε_1, ε_2, ε_3 have norm 1 and all three integers $\delta_i\delta_j$ are squares in L^+. There are three pairwise coprime odd integers a, b, c such that $d_1 = 2^{e_1}ab$, $d_2 = 2^{e_2}bc$, $d_3 = 2^{e_3}ac$. Since (d_i, d_j) has an odd prime divisor, none of a, b, c is 1.

We claim that the odd part of δ_1 must be equal to one of $1, a, b, ab$. To see that suppose that p is a common prime divisor of a and δ_1. Assume that there is a prime divisor q of a which does not divide δ_1. Since neither p nor q divides δ_2, we see that the square-free part of $\delta_1\delta_2$ is divisible by p and not by q. Thus in $K = \mathbb{Q}(\sqrt{\delta_1\delta_2})$ the prime p ramifies and the prime q is not ramified. But K is one of the fields L_i^+ and in each of these fields either both p and q ramify or both are unramified. The contradiction shows that no such q exists, i.e. that either $a|\delta_1$ or $(a, \delta_1) = 1$. The same conclusion holds for b and since $(a, b) = 1$ our claim follows. Of course, the same argument shows that the odd part of δ_2 belongs to $\{1, b, c, bc\}$ and the odd part of δ_3 belongs to $\{1, a, c, ac\}$.

Suppose that $L = ML^+$ has unit index 8 for $M = \mathbb{Q}(\sqrt{-A})$. Note that $abc|A$ by Proposition 2. If $i \in L$, then $L = L^+(i)$ and therefore A is the square-free part of one of d_1, d_2, d_3 or $A = 1$. However neither of these numbers is divisible by abc, a contradiction. Thus $i \notin L$. It follows that $\sqrt{-\varepsilon_i} \in L$ for $i = 1, 2, 3$. Equivalently, L contains $\sqrt{-\delta_i}$, $i = 1, 2, 3$. In particular, L is uniquely determined by L^+ and so is M by Lemma 7. Suppose 2 ramifies in L_1^+ and either 2 or -2 is a norm of an integer in L_1^+. Thus $\delta_1 \in \{2, ab, 2ab\}$ by Lemma 5. Since both $\sqrt{d_1}$ and $\sqrt{-\delta_1}$ are in L, we see that $\sqrt{-2} \in L$ (note that if $\delta_1 = ab$ then $d_1 = 4ab$ and if $\delta_1 = 2ab$ then $d_1 = 8ab$). Thus A is the square-free part of one of $2, 2d_1, 2d_2, 2d_3$, which is not possible since none of these four numbers is divisible by abc. The contradiction shows that either 2 is unramified in L_1^+ or none of 2 and -2 is a norm of an integer in L_1^+. Same conclusion holds for L_2^+ and L_3^+. This proves the first part of the proposition.

In order to prove the second part suppose that either 2 is unramified in L_1^+ or none of 2, -2 is a norm of an integer of L_1^+. We have seen that there is at most one imaginary quadratic field M such that L^+M/M has unit index 8. It suffices to find such a field M. By Lemma 5, the odd part of δ_1 is neither 1 nor ab. Thus it is either a or b. Without any loss of generality we may assume that the odd part of δ_1 is a. Take for A the square-free part of $\delta_1 d_2$. Then $L = L^+\mathbb{Q}(\sqrt{-A})$ contains $\sqrt{-\delta_1} = \sqrt{-A}/\sqrt{d_2}$, hence it contains $\sqrt{-\varepsilon_1}$. Thus $[V : V^+] = 2$. In order to complete the proof we need to show that $[V_i : V_i^+] = 1$ for $i = 1, 2, 3$. By Proposition 1 of [4] it amounts to showing that neither Ad_i nor $Ad_i\delta_i$ is a square of a rational number. This is straightforward since the odd part of A is abc. □

Example. In [6] we proved that given $t \geq 2$ there exist infinitely many sets of $t+1$ primes $p_1, ..., p_t, p_t'$ such that $p_1 \equiv 2t-1 \pmod 4$, $p_i \equiv 3 \pmod 4$ for $i > 1$, $p_t' \equiv 3 \pmod 4$ and the biquadratic field $L^+ = \mathbb{Q}(\sqrt{p_1...p_t}, \sqrt{p_t p_t'}\,)$ has units of type III. Since 2 is unramified in $L^+/\mathbb{Q}$, we see from the proof of Proposition 7 that for $M = \mathbb{Q}(\sqrt{-p_1...p_t p_t'}\,)$ the unit index of ML^+/M is 8. Since primes over 2 do not ramify in ML^+/M, the extension ML^+/M is unramified by Proposition 2. By genus theory, the $2-$rank of the class group of M is t. Thus we get a counterexample to Lemmermeyer's conjecture mentioned at the end of section 3. For an explicit example, take $t = 3$, $p_1 = 5$, $p_2 = 3$, $p_3 = 19$, $p_3' = 31$.

Proposition 8. *Suppose the units of L^+ are of type III and that (d_2, d_3) has no odd prime divisors. If 2 ramifies in L_1^+ and either 2 or -2 is a norm of an integer in L_1^+ then there is no imaginary quadratic field M such that the unit index of ML^+/M is 8. Otherwise, $\mathbb{Q}(\sqrt{-d_1})$ and $\mathbb{Q}(\sqrt{-2d_1})$ are the only imaginary quadratic fields M such that the unit index of ML^+/M is 8.*

Proof. There are coprime odd integers a, b such that $d_1 = 2^{e_1}ab$, $d_2 = 2^{e_2}b$, $d_3 = 2^{e_3}a$. All three integers $\delta_i\delta_j$ are squares in L^+. In particular, since $\delta_2\delta_3$ is a square in L^+, the odd part of δ_2 is in $\{1, b\}$ and the odd part of δ_3 is in $\{1, a\}$. In other words, $\delta_2 \in \{2, b, 2b\}$ and $\delta_3 \in \{2, a, 2a\}$. Note also that the units ε_1, ε_2, ε_3 have norm 1. Since fundamental units of $\mathbb{Q}(\sqrt{2})$ have norm -1, we have $a > 1$ and $b > 1$.

Suppose that $M = \mathbb{Q}(\sqrt{-A})$ is such that the unit index of ML^+/M is 8. Set $L = ML^+$. By Proposition 2, if an odd prime ramifies in $L/\mathbb{Q}$ then it ramifies in $M/\mathbb{Q}$. Thus $ab|A$.

Suppose that $\sqrt{-1} \in L$. Then $\sqrt{A} \in L^+$ and therefore A is the square-free part of d_1. Thus $M = \mathbb{Q}(\sqrt{-d_1})$. Note that $L_1 = \mathbb{Q}(\sqrt{-A}, \sqrt{-1})$ and $L_1^+ = \mathbb{Q}(\sqrt{A})$. Since $[V_1 : V_1^+] = 1$, Lemma 6 implies that either 2 does not ramify in L_1^+ or neither 2 nor -2 is a norm of an integer in L_1^+.

If $\sqrt{-1} \notin L$ then either $\sqrt{\varepsilon_2} \in L$ or $\sqrt{-\varepsilon_2} \in L$. The former case is not possible, since $\sqrt{\varepsilon_2}$ is totally real and ε_2 is not a square in L^+. Thus $\sqrt{-\varepsilon_2} \in L$, which is equivalent to $\sqrt{-\delta_2} \in L$. Recall now that $\delta_2 \in \{2, b, 2b\}$. Furthermore, if $\delta_2 = b$ then $d_2 = 8b$ and if $\delta_2 = 2b$ then $d_2 = 4b$. In any case, we have $\sqrt{-2} \in L$. Thus $L = L^+(\sqrt{-2})$ and therefore $M = \mathbb{Q}(\sqrt{-2d_1})$. We claim furthermore that either 2 does not ramify in L_1^+ or neither 2 nor -2 is a norm of an integer in L_1^+. In fact, suppose the contrary. Thus $2|d_1$. If 2 is a norm of an integer in L_1^+ then $\delta_1 = 2$ by Lemma 5 and if -2 is a norm of an integer in L_1^+ then $2\delta_1$ is a square in L_1^+, again by Lemma 5. In both cases, Proposition 1 of [4] applied to the field $F = L_1 = \mathbb{Q}(\sqrt{d_1}, \sqrt{-2d_1})$ implies that $[V_1 : V_1^+] = 2$, a contradiction.

To complete the proof of Proposition 8 we must show that if either 2 does not ramify in L_1^+ or neither 2 nor -2 is a norm of an integer in L_1^+ and if $M = \mathbb{Q}(\sqrt{-d_1})$ or $M = \mathbb{Q}(\sqrt{-2d_1})$ then the unit index of L/M is 8, where $L = L^+M$.

Case 1. $M = \mathbb{Q}(\sqrt{-d_1})$.
We have $[V_1 : V_1^+] = 1$ by Lemma 6. Since neither d_1/δ_i nor d_1d_i/δ_i is a square of a rational number for $i = 2, 3$, Proposition 1 of [4] implies that $[V_2 : V_2^+] = 1 = [V_3 : V_3^+]$. Since $\delta_2 \in \{2, b, 2b\}$, Lemma 5 implies that 2 ramifies in L_2^+ and ± 2 is a norm of an integer in L_2^+. Thus $\sqrt{i\varepsilon_2} \in L_2^+(\sqrt{-1})$ by Lemma 6. It follows that $[V : V^+] = 2$ and consequently $[V : V_1V_2V_3] = 8$.

Case 2. $M = \mathbb{Q}(\sqrt{-2d_1})$.
If $2d_1/\delta_1$ is a square of a rational number then $\delta_1 \neq 2$ and $2\delta_1$ is a square in L_1^+, so -2 is a norm of an integer in L_1^+ by Lemma 5. If $(2d_1)d_1/\delta_1$ is a square of a rational number then $\delta_1 = 2$ and 2 is a norm of an integer in L_1^+ by Lemma 5. Neither case is possible, so $[V_1 : V_1^+] = 1$ by Proposition 1 of [4]. Since neither $2d_1/\delta_i$ nor $2d_1d_i/\delta_i$ is a square of a rational number for $i = 2, 3$, Proposition 1 of [4] implies that $[V_2 : V_2^+] = 1 = [V_3 : V_3^+]$. Recall that $\delta_2 \in \{2, b, 2b\}$. It follows that $\sqrt{-\delta_2} \in L$, i.e. $\sqrt{-\varepsilon_2} \in L$. Thus $[V : V^+] = 2$. This proves that $[V : V_1V_2V_3] = 8$. □

References

[1] G. Gras, *Class Field Theory*. Springer Monographs in Mathematics, Springer-Verlag, Berlin Heidelberg New York 2003.

[2] D. Harbater, *Galois groups with prescribed ramification*. Contemporary Math. **174** (1994), 35–60.

[3] H. Hasse, *Über die Klassenzahl abelscher Zahlkörper*. Springer-Verlag, Berlin Heidelberg New York Tokyo 1985.

[4] M. Hirabayashi, K. Yoshino, *Unit Indices of Imaginary Abelian Number Fields of Type* $(2, 2, 2)$. J. Number Th. **34** (1990), 346–361.

[5] F. Lemmermeyer, *Kuroda's class number formula*. Acta Arith. **66** (1994), 245–260.

[6] M. Mazur, S. V. Ullom, *Galois module structure of units in real biquadratic number fields*. Acta Arith. **111** (2004), 105–124.

Marcin Mazur
Department of Mathematics
Binghamton University
P.O. Box 6000
Binghamton, NY 13892-6000
E-mail: mazur@math.binghamton.edu

Stephen V. Ullom
Department of Mathematics
University of Illinois at Urbana-Champaign
1409 W. Green Street
Urbana, Illinois 61801-2975
E-mail: ullom@math.uiuc.edu