ACTA ARITHMETICA
111.2 (2004)

Galois module structure of units in real biquadratic number fields

by

MARCIN MAZUR (Binghamton, NY)
and STEPHEN V. ULLOM (Urbana, IL)

To the memory of Ali Fröhlich

1. Introduction. Recent years have seen the development of a general theory of the Galois module structure of units in a number field (among many others see Chinburg [3], Fröhlich [7], Burns [2], Weiss [17] and the references there).

We consider here the case when the number field is a totally real Galois extension N of $\mathbb{Q}$ with Galois group the Klein four group. As a Galois module, the group V of units of N modulo $\{\pm 1\}$ can be of four different types. T. Kubota [9] gave examples to show that each type occurs infinitely often but his examples involve fields N with at most four ramified primes only. In Section 5 we show that among the fields N with exactly $r \geq 3$ ramified primes each of the four types occurs infinitely often. In particular, there are infinitely many real biquadratic fields with Minkowski unit and arbitrary many > 1 ramified primes. We believe this is the first example of Minkowski units in noncyclic, totally real extensions with a large number of ramified primes.

We investigate the arithmetic conditions which characterize each type. When there are no ideal classes of order four in the class groups of the quadratic subfields of N, rational congruence conditions characterize the module type. Otherwise the problem is much more subtle and involves non-abelian extensions of the rationals and central class fields. Theorem 7 describes a family of examples where the field N has a Minkowski unit exactly when the central class field of N is different from its genus field.

We consider in particular the case $N = \mathbb{Q}(\sqrt{p}, \sqrt{q})$ with p and q primes. This leads to questions about the 2-part of class groups and the governing fields of Cohn and Lagarias. In Theorem 5 we give an explicit description

2000 *Mathematics Subject Classification*: 11R33, 11R27, 11R29, 11R16, 11R37, 20C05.

of the minimal governing field for the divisibility by 8 of the class number of $\mathbb{Q}(\sqrt{pq})$, where the prime $q \equiv 3 \pmod 4$ is fixed and $p \equiv 1 \pmod 4$ is a variable prime. This complements and sharpens some results previously obtained by Stevenhagen [16] and Morton [12].

2. Units in real biquadratic fields. In this section we recall results due to S. Kuroda [10] and T. Kubota [9] about units in real biquadratic fields and we derive from these results a classification of the (possible) Galois module structure of units modulo torsion.

Let N be a real biquadratic extension of $\mathbb{Q}$. We consider N as a subfield of $\mathbb{R}$, so it is ordered. The Galois group of $N/\mathbb{Q}$ is the Klein 4-group $\Gamma = \{1, \sigma_1, \sigma_2, \sigma_3\}$. Thus N has three real quadratic subfields K_1, K_2, K_3, which are the fixed fields of $\sigma_1, \sigma_2, \sigma_3$ respectively. Write $K_i = \mathbb{Q}(\sqrt{\Delta_i})$, where Δ_i is a square-free positive integer. Let $U_N = U$ be the group of units of N and let U_i be the group of units of K_i. Let ε_i be the fundamental unit of K_i (in what follows, by *the* fundamental unit of a real quadratic subfield of $\mathbb{R}$ we mean the one which is larger than 1; in turn *a* fundamental unit is any unit which generates the group of units modulo torsion).

By Dirichlet's unit theorem, the group $V_N = V = U/\{\pm 1\}$ is a free abelian group of rank 3. In what follows, we use the same notation for units and their images in V. By Kubota [9], we have the following possibilities for a system of fundamental units of U (i.e. $\mathbb{Z}$-basis of V):

Type I: (i) $\varepsilon_1, \varepsilon_2, \varepsilon_3$, (ii) $\sqrt{\varepsilon_i}, \varepsilon_j, \varepsilon_k$, (iii) $\sqrt{\varepsilon_i}, \sqrt{\varepsilon_j}, \varepsilon_k$;
Type II: (i) $\sqrt{\varepsilon_i\varepsilon_j}, \varepsilon_j, \varepsilon_k$, (ii) $\sqrt{\varepsilon_i\varepsilon_j}, \varepsilon_j, \sqrt{\varepsilon_k}$;
Type III: $\sqrt{\varepsilon_1\varepsilon_2}, \sqrt{\varepsilon_2\varepsilon_3}, \sqrt{\varepsilon_3\varepsilon_1}$;
Type IV: (i) $\sqrt{\varepsilon_1\varepsilon_2\varepsilon_3}, \varepsilon_2, \varepsilon_3$ with ε_l of norm 1 for $l = 1, 2, 3$,
(ii) $\sqrt{\varepsilon_1\varepsilon_2\varepsilon_3}, \varepsilon_2, \varepsilon_3$ with ε_l of norm -1 for $l = 1, 2, 3$;

here $\{i, j, k\} = \{1, 2, 3\}$ and in all cases except IV(ii) any ε_i that appears under a square root has norm 1.

In order to describe a way to determine the actual case for a given field N define $\widehat{\varepsilon}_i$ by

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

Suppose first that the norm of ε_i is 1 for at least one i. Then every unit in U is of the form $\pm\sqrt{\widehat{\varepsilon}_1^{m_1}\widehat{\varepsilon}_2^{m_2}\widehat{\varepsilon}_3^{m_3}}$ for some integers m_1, m_2, m_3. In order to describe precisely which triples (m_1, m_2, m_3) can occur (and this is equivalent to the identification of the appropriate case) we need to introduce further notation.

For a real quadratic field $M = \mathbb{Q}(\sqrt{\Delta})$ (with square-free integer Δ) and a norm 1 unit η of M, there is an integer a of M, unique up to sign, such that a is not divisible by any rational prime and $\eta = a/\overline{a}$, where $\overline{a}$ is the conjugate of a (the existence of a follows from Hilbert's Theorem 90).

Define $\delta(\eta) = a\overline{a}$. It is easy to see that $\delta(\eta)$ is a square-free divisor of the discriminant of M. In fact, since the ideal (a) generated by a is ambiguous, it is a product of distinct ramified prime ideals and a principal ideal generated by a rational integer. Since no rational prime divides a, we see that (a) is a product of distinct ramified prime ideals, i.e. that $a\overline{a}$ is a square-free divisor of the discriminant of M. We may write $\eta = u + w\sqrt{\Delta}$ for some rational numbers u, w. Then $\delta(\eta)$ is simply the square-free part of the integer $2u+2$ provided $\eta \neq -1$. In fact, since $\delta(\eta)$ is square-free, this follows from the equalities

$$2u + 2 = \frac{(a+\overline{a})^2}{a\overline{a}} = \delta(\eta)\left(\frac{a+\overline{a}}{a\overline{a}}\right)^2.$$

Returning to our biquadratic field N such that at least one of the ε_i has norm 1, let $\delta_i = \delta(\widehat{\varepsilon}_i)$. Then by Kubota [9, Hilfssatz 11], $\sqrt{\widehat{\varepsilon}_1^{m_1}\widehat{\varepsilon}_2^{m_2}\widehat{\varepsilon}_3^{m_3}} \in U$ iff $\delta_1^{m_1}\delta_2^{m_2}\delta_3^{m_3}$ is a square in N. Since $\delta_1^{m_1}\delta_2^{m_2}\delta_3^{m_3}$ is an integer, the last condition is equivalent to $\delta_1^{m_1}\delta_2^{m_2}\delta_3^{m_3}$ being a square in K_i for some i.

In the case when all ε_i have norm -1, we have only two possibilities, namely I(i) or IV(ii). Write $\varepsilon_i = u_i + w_i\sqrt{\Delta_i}$. Consider the four rational numbers

$$u_1u_2u_3 + w_1w_2w_3\sqrt{\Delta_1\Delta_2\Delta_3} \pm u_1 \pm u_2 \pm u_3$$

where the number of minus signs is odd. According to Kubota, case IV(ii) occurs iff all four numbers are squares in N.

We now discuss the structure of V as a $\mathbb{Z}\Gamma$-module. Note that $V^\Gamma = \{1\}$, so in particular the trace element $\Sigma = 1+\sigma_1+\sigma_2+\sigma_3$ annihilates V. In other words, V is an $\mathbb{A} = \mathbb{Z}\Gamma/(\Sigma)$-module. In the remainder of the paragraph we use additive notation. For each $i = 1, 2, 3$ define a $\mathbb{Z}\Gamma$-module A_i to be a free $\mathbb{Z}$ module of rank 1 with a generator a_i such that $\sigma_i a_i = a_i$ and $\sigma_j a_i = -a_i$ for $j \neq i$. In other words, A_i is isomorphic to $\mathbb{Z}\Gamma/(1-\sigma_i, 1+\sigma_j, 1+\sigma_k)$. The $\mathbb{Z}\Gamma$-modules B_i, $i = 1, 2, 3$, are defined as free $\mathbb{Z}$-modules of rank 2 with a basis b_i, c_i such that $\sigma_i b_i = -b_i$, $\sigma_j b_i = c_i$, $\sigma_k b_i = -c_i$, where $\{i, j, k\} = \{1, 2, 3\}$. It is easy to see that B_i is isomorphic to $\mathbb{Z}\Gamma/(\Sigma, 1+\sigma_i)$. Finally, let J be the augmentation ideal of $\mathbb{Z}\Gamma$. Note that all these modules are in fact $\mathbb{A}$-modules.

We have the following

THEOREM 1. *The $\mathbb{Z}\Gamma$-module V is isomorphic to*

(1) $A_1 \oplus A_2 \oplus A_3$ *if V is of type* I;
(2) $A_k \oplus B_k$ *if V is of type* II;
(3) J *if V is of type* III;
(4) $\mathbb{A}$ *if V is of type* IV.

REMARKS. (1) It is easy to see that the $\mathbb{Z}\Gamma$-modules $A_1 \oplus A_2 \oplus A_3$, $A_i \oplus B_i$, $i = 1, 2, 3$, J and $\mathbb{A}$ are pairwise nonisomorphic. It follows from the results of Nazarova [14] that in fact these 6 isomorphism types exhaust all possibilities for an $\mathbb{A}$-module which is free of rank 3 over $\mathbb{Z}$ (see also [5]).

(2) For any pair i, j there is an automorphism f of Γ such that the modules $A_i \oplus B_i$ and $\mathbb{Z}\Gamma \otimes_R (A_j \oplus B_j)$ are isomorphic, where $R = \mathbb{Z}\Gamma$ and $\mathbb{Z}\Gamma$ is considered as an R-algebra via f. This means that from the arithmetic point of view these modules are indistinguishable, which justifies the fact that all of them constitute the same type.

(3) Recall that a *Minkowski unit* of a finite Galois extension L of $\mathbb{Q}$ is a unit u which generates the group V of units of L modulo torsion as a module over the group ring $\mathbb{Z}\Gamma$, where Γ is the Galois group of $L/\mathbb{Q}$. It is known that if L is totally real then it has Minkowski unit iff V is isomorphic to $\mathbb{Z}\Gamma/(\Sigma)$ as $\mathbb{Z}\Gamma$-module ([13]). In particular, a real biquadratic field has a Minkowski unit iff it is of type IV and then $\sqrt{\varepsilon_1\varepsilon_2\varepsilon_3}$ is a Minkowski unit.

Proof of Theorem 1. For type I define a homomorphism $f : A_1 \oplus A_2 \oplus A_3 \to V$ as follows:

- $f(a_i) = \varepsilon_i$ for all i in case (i);
- $f(a_i) = \sqrt{\varepsilon_i}$, $f(a_j) = \varepsilon_j$, $f(a_k) = \varepsilon_k$ in case (ii);
- $f(a_i) = \sqrt{\varepsilon_i}$, $f(a_j) = \sqrt{\varepsilon_j}$, $f(a_k) = \varepsilon_k$ in case (iii).

It is clear that f is well defined as a homomorphism of $\mathbb{Z}$-modules and it is surjective, hence it is an isomorphism (since both modules have the same rank). It is straightforward to check that f is Γ-equivariant so it is an isomorphism of $\mathbb{Z}\Gamma$-modules.

For type II, define a homomorphism $f : A_k \oplus B_k \to V$ as follows:

- $f(b_k) = \sqrt{\varepsilon_i\varepsilon_j}$, $f(c_k) = \sqrt{\varepsilon_i\varepsilon_j}/\varepsilon_j$, $f(a_k) = \varepsilon_k$ in case (i);
- $f(b_k) = \sqrt{\varepsilon_i\varepsilon_j}$, $f(c_k) = \sqrt{\varepsilon_i\varepsilon_j}/\varepsilon_j$, $f(a_k) = \sqrt{\varepsilon_k}$ in case (ii).

Again, f is well defined and surjective as a homomorphism of $\mathbb{Z}$-modules and therefore it is an isomorphism. A straightforward verification shows that f is Γ-equivariant.

For type III, define $f : J \to V$ by $f(1 - \sigma_i) = \sqrt{\varepsilon_j\varepsilon_k}$ for $i = 1, 2, 3$. As above, this is a surjective homomorphism of free $\mathbb{Z}$-modules of the same rank, hence an isomorphism. It is Γ-equivariant by trivial verification.

For type IV define an $\mathbb{A}$-module homomorphism $f : \mathbb{A} \to V$ by $f(1) = \sqrt{\varepsilon_1\varepsilon_2\varepsilon_3}$. Since $\sigma_i(\sqrt{\varepsilon_1\varepsilon_2\varepsilon_3}) = \varepsilon_i/\sqrt{\varepsilon_1\varepsilon_2\varepsilon_3}$, we see that f is onto. Since both $\mathbb{A}$ and V are free $\mathbb{Z}$-modules of rank 3, f is an isomorphism. ∎

3. Biquadratic fields with at most three ramified primes. In this section we focus on the biquadratic extensions N of the form $\mathbb{Q}(\sqrt{p_1}, \sqrt{p_2})$, where p_1, p_2 are distinct primes. The quadratic subfields of N are $K_i = \mathbb{Q}(\sqrt{p_i})$, $i = 1, 2$, and $K_3 = \mathbb{Q}(\sqrt{p_1p_2})$. The cases when neither of the primes is $\equiv 3 \pmod 4$ or both of them are $\equiv 3 \pmod 4$ are rather simple and they are due to Kubota [9]; we collect the results for completeness. Let $\sigma_N = (n_1, n_2, n_3)$, where n_i is the norm of a fundamental unit ε_i of K_i. Recall that V_N is the group of units of N modulo torsion.

THEOREM 2 (Kubota [9]). (i) *Suppose that* $N = \mathbb{Q}(\sqrt{p_1}, \sqrt{p_2})$, *where* $p_1 \equiv 1 \pmod 4$, $p_2 \not\equiv 3 \pmod 4$ *are primes. Then* V_N *is of type* I *if* $\sigma_N = (-1,-1,+1)$ *and of type* IV *if* $\sigma_N = (-1,-1,-1)$. *In the former case*, $\varepsilon_1, \varepsilon_2, \sqrt{\varepsilon_3}$ *is a basis of* V_N.

(ii) *Suppose that* $N = \mathbb{Q}(\sqrt{2}, \sqrt{p_1})$, *where* $p_1 \equiv 3 \pmod 4$ *is a prime* (*so* $p_2 = 2$). *Then* V_N *is of type* I *and has a basis* $\sqrt{\varepsilon_1}, \varepsilon_2, \sqrt{\varepsilon_3}$.

(iii) *Suppose that* $N = \mathbb{Q}(\sqrt{p_1}, \sqrt{p_2})$, *where* $p_1 \equiv 3 \pmod 4$ *and* $p_2 \equiv 3 \pmod 4$. *Then* V_N *is of type* II *and has a basis* $\sqrt{\varepsilon_1\varepsilon_2}, \sqrt{\varepsilon_3}, \varepsilon_1$.

Proof. By the Brauer class number formula [8, p. 318] we have

$$h_N = eh_1h_2h_3/4$$

where $e = [U : U_1U_2U_3] \in \{1, 2, 4\}$ (recall that U, U_i are the groups of units of N, K_i respectively) and h_i (resp. h_N) is the class number of K_i (resp. N).

In case (i), the class number h_3 is even and h_1h_2 is odd. Since N is an unramified extension of K_3, the Hilbert class field of K_3 is contained in the Hilbert class field of N. Thus $h_3/2$ divides h_N. In particular, $e \neq 1$. Since $N\varepsilon_1 = -1 = N\varepsilon_2$, we see that V_N is of type IV if $N\varepsilon_3 = -1$ and it is of type I with basis $\varepsilon_1, \varepsilon_2, \sqrt{\varepsilon_3}$ when $N\varepsilon_3 = 1$ (see the description of possible systems of fundamental units in Section 2).

In cases (ii) and (iii), the product $h_1h_2h_3$ is odd, so $e = 4$. Since $\sigma_N = (1, -1, 1)$ in case (ii), we see that in this case V_N is of type I with basis $\sqrt{\varepsilon_1}, \varepsilon_2, \sqrt{\varepsilon_3}$.

Finally, case (iii) follows from our discussion in Section 2 and the observation that modulo squares in N we have $\delta_1 =_2 2 =_2 \delta_2$ and $\delta_3 = p_1$ (see [9] for full details and Section 5 for more on the deltas). ∎

REMARK. Theorem 2 reduces the question of the type of V_N in the above situation to the determination of the norm of a fundamental unit of $\mathbb{Q}(\sqrt{p_1p_2})$, where $p_1 \equiv 1 \pmod 4$ and $p_2 \not\equiv 3 \pmod 4$ are primes. This is a classical problem for which no satisfactory solution has been found. It is known however that if either $p_1 \equiv 5 \pmod 8$ and $p_2 = 2$ or $p_1 \equiv p_2 \equiv 1 \pmod 4$ and $(p_1/p_2) = -1$ then the norm of a fundamental unit is -1 (see [4, p. 147]).

Now we discuss the most interesting case when $p_1 = p \equiv 1 \pmod 4$ and $p_2 = q \equiv 3 \pmod 4$. As in the proof of Theorem 2, we see that the index $[U : U_1U_2U_3] > 1$. Moreover, $\sigma_N = (-1, 1, 1)$ in this case. We claim that $\sqrt{\varepsilon_2} \notin N$. Otherwise, we would have $N = K_2(\sqrt{\varepsilon_2})$, so only the prime divisors of 2 may ramify in N/K_2, which is evidently false since the primes of N over p ramify in N/K_2. These observations combined with the description of fundamental systems of units in Section 2 imply that either $\varepsilon_1, \varepsilon_2, \sqrt{\varepsilon_3}$ or $\varepsilon_1, \varepsilon_2, \sqrt{\varepsilon_2\varepsilon_3}$ is a fundamental system of units of U. In the former case, V_N is of type I and in the latter case it is of type II.

Our next goal is to understand the arithmetic conditions which govern the type of V_N. We prove the following result.

THEOREM 3. *Let* $N = \mathbb{Q}(\sqrt{p}, \sqrt{q})$, *where* $p \equiv 1 \pmod 4$ *and* $q \equiv 3 \pmod 4$ *are primes. Then* V_N *is of type* I *iff the prime ideal of* $\mathbb{Q}(\sqrt{pq})$ *over* p *is principal. If this is the case then* $\varepsilon_1, \varepsilon_2, \sqrt{\varepsilon_3}$ *is a system of fundamental units of* U. *Otherwise*, V_N *is of type* II *and* $\varepsilon_1, \varepsilon_2, \sqrt{\varepsilon_2\varepsilon_3}$ *is a system of fundamental units. In particular*:

(1) *if* $(p/q) = 1$ *and* $p \equiv 5 \pmod 8$ *then* V_N *is of type* I;
(2) *if* $(p/q) = -1$ *then* V_N *is of type* II.

REMARK. Kubota [9, pp. 73–74] has obtained a similar result to (1), (2) using the δ-function.

Proof of Theorem 3. The only thing left in order to prove the first part of the theorem is that $\sqrt{\varepsilon_3} \in N$ iff the prime ideal $\mathfrak{p}$ of $K_3 = \mathbb{Q}(\sqrt{pq})$ over p is principal.

Note that $\mathfrak{p}$ is principal iff the equation $x^2 - pqy^2 = \pm p$ is solvable in integers x, y, i.e. iff $pz^2 - qy^2 = \pm 1$ is solvable in integers z, y. Thus if $\mathfrak{p}$ is principal and z, y are integers satisfying $pz^2 - qy^2 = \pm 1$ (in fact, -1 is not possible here) then $\eta = z\sqrt{p} - y\sqrt{q}$ is a unit in N which is not in K_3 but whose square is in K_3. It follows that η^2 is an odd power of ε_3, i.e. $\sqrt{\varepsilon_3} \in N$.

Conversely, suppose that $\sqrt{\varepsilon_3} \in N$. We may write $\sqrt{\varepsilon_3} = s + t\sqrt{p}$ for some $s, t \in K_3$. Taking squares, we see that $st = 0$, so $s = 0$ and $\sqrt{\varepsilon_3} = t\sqrt{p}$. Thus the algebraic integer $\sqrt{p\varepsilon_3}$ belongs to K_3 and has norm $\pm p$ hence generates $\mathfrak{p}$.

To prove the last part of the result recall that if either $(p/q) = -1$ or $p \equiv 5 \pmod 8$ then the 2-part of the class group of K_3 is cyclic of order 2 ([4, p. 145]). It follows that N is the Hilbert 2-class field of $K_3 = \mathbb{Q}(\sqrt{pq})$. If $(p/q) = -1$ then $(q/p) = -1$ and the equation $pz^2 - qy^2 = \pm 1$ has no solutions in integers. Thus $\mathfrak{p}$ is not principal and we get (2). If $(p/q) = 1$ then p is not inert in N, so $\mathfrak{p}$ splits completely in N. If furthermore $p \equiv 5 \pmod 8$ then N is the Hilbert 2-class field of K_3, so $\mathfrak{p}$ is principal by class field theory. This proves (1). ■

The case when $(p/q) = 1$ and $p \equiv 1 \pmod 8$ is much harder essentially because the class group of K_3 contains elements of order 4 (see Section 5) and so Kubota's technique to find δ_3 by genus characters cannot be applied. In Section 4, we solve the problem (Theorem 5) under the assumption that the class number of K_3 is not divisible by 8. It turns out that our problem is closely related to governing fields as defined by Cohn and Lagarias.

The following result is useful for numerical computations:

Lemma 1. *Let $p \equiv 1 \pmod 4$ and $q \equiv 3 \pmod 4$ be primes. Denote by $\mathfrak{p}$ and $u + w\sqrt{pq}$ the prime over p and the fundamental unit of $\mathbb{Q}(\sqrt{pq})$ respectively. Then $\mathfrak{p}$ is principal iff u is odd. Furthermore, if $p \equiv 1 \pmod 8$ and $\mathfrak{p}$ is principal then the quartic residue symbol $(q/p)_4 = 1$.*

Proof. We use the notation introduced above, so $\mathbb{Q}(\sqrt{pq}) = K_3$, $\varepsilon_3 = u + w\sqrt{pq}$, etc. Recall that $\delta_3 \mid 2pq$ is the square-free part of $2(u+1)$ and that $\sqrt{\varepsilon_3} \in N$ iff δ_3 is a square in N. In our situation the last condition is equivalent to δ_3 being odd. Thus by Theorem 3, $\mathfrak{p}$ is principal iff δ_3 is odd. If u is even then the square-free part of $2(u+1)$ is even, so δ_3 is even. Suppose now that u is odd. From $u^2 - pqw^2 = 1$ we conclude that $w = 2w_1$ is even and $v(v-1) = pqw_1^2$, where $v = (u+1)/2$. It is then clear that the square-free part of $2(u+1) = 4v$ is odd.

Recall now that $\mathfrak{p}$ is principal iff $px^2 - qy^2 = 1$ is solvable in integers (the left hand side is $\equiv 0, 1 \pmod 4$ so it cannot be -1). In particular, $-1 \equiv qy^2 \pmod p$. Since -1 is a 4th power modulo p when $p \equiv 1 \pmod 8$, we have $(q/p)_4 = 1$ iff $(y/p) = 1$. Write $y = 2^l z$ with z odd. Then $(y/p) = (z/p) = (p/z) = (px^2/z) = (1 + qy^2/z) = (1/z) = 1$. ∎

Remark. We will have a more conceptual explanation of the equality $(q/p)_4 = 1$ in the next section.

Remark. With a little more effort one can see that $\mathfrak{p}$ is principal iff $\delta_3 = p$. If $\mathfrak{p}$ is not principal then either the prime $\mathfrak{q}$ above 2 is principal and

$$\delta_3 = \begin{cases} 2 & \text{if } (2/p) = (2/q) = 1, \\ 2pq & \text{if } (2/p) = -(2/q) = 1, \end{cases}$$

or $\mathfrak{pq}$ is principal and

$$\delta_3 = \begin{cases} 2p & \text{if } (p/q) = (2/q), \\ 2q & \text{if } (p/q) = -(2/q). \end{cases}$$

4. Governing fields. In this section we investigate the divisibility by 8 of the class number $h(4pq)$ of the quadratic number field $K = \mathbb{Q}(\sqrt{pq})$, where $p \equiv 1 \pmod 4$, $q \equiv 3 \pmod 4$ are primes. As a corollary we get an arithmetic criterion for the prime of K over p to be principal if $h(4pq)$ is not divisible by 8.

As we remarked before, if $p \equiv 5 \pmod 8$ or if $(p/q) = -1$ then the 2-part of the class group of K is cyclic of order 2. Thus we will assume from now on that $p \equiv 1 \pmod 8$ and $(p/q) = 1$. The 2-part Cl_2 of the class group of K is cyclic of order at least 4. Moreover, the fundamental unit of K has norm 1 and the 2-part of the narrow class group of K equals $\mathbb{Z}/2\mathbb{Z} \times \mathrm{Cl}_2$. From the results of Stevenhagen [16] we know that there is a normal extension of $\mathbb{Q}$, called a *governing field*, such that the Artin class of a prime p in this field determines whether 8 divides $h(4pq)$ or not. The description of this field given by Stevenhagen is not sufficient for our purposes, since it is not clear which Artin classes correspond to divisibility by 8 and which do not. Below we describe the minimal governing field for the divisibility by 8 of the class number $h(4pq)$.

For each m let H_{2^m} be the unramified extension of K corresponding to $\mathrm{Cl}_2/2^m\mathrm{Cl}_2$. The field H_2 equals $K(\sqrt{p}) = \mathbb{Q}(\sqrt{p}, \sqrt{q})$. The following explicit description of the field H_4 is a key step in determining the governing field.

THEOREM 4. *Let $p \equiv 1 \pmod 8$ and $q \equiv 3 \pmod 4$ be primes such that $(p/q) = 1$. The unique unramified cyclic degree 4 extension H_4 of $K = \mathbb{Q}(\sqrt{pq})$ equals $H_2(\sqrt{z}) = \mathbb{Q}(\sqrt{p}, \sqrt{q}, \sqrt{z})$, where z is any totally positive integer in $F = \mathbb{Q}(\sqrt{p})$ whose norm is an odd power of q.*

Proof. It is a classical result that the Galois group Γ of $H_4/\mathbb{Q}$ is dihedral. We provide a short argument for the convenience of the reader. Note that Γ cannot be abelian. Being a nonabelian group of order 8, Γ is either dihedral or quaternion. Let Γ_1 be the subgroup of Γ which fixes K. Since H_4/K is unramified, the inertia group of any ramified prime of $H_4/\mathbb{Q}$ has trivial intersection with Γ_1. But in the quaternion group all nontrivial subgroups contain the center, so Γ cannot be quaternion.

It follows that the extension H_4/F is biquadratic. Thus there is a totally positive algebraic integer z in F such that $H_4 = F(\sqrt{q}, \sqrt{z})$. Let w be any such integer with minimal possible number of different prime divisors. We will show that the ideal (w) is a power of a prime ideal over q.

Genus theory tells us that the class number of F is odd. We claim that each prime divisor of w occurs in the prime factorization of (w) with an odd exponent. In fact, suppose $(w) = \mathfrak{p}^{2k}\mathfrak{a}$ with $\mathfrak{p}$ prime and $\mathfrak{a}$ prime to $\mathfrak{p}$. Some odd power $\mathfrak{p}^l = (s)$ is principal. Thus $w' = w^l/s^{2k}$ is a totally positive integer with smaller number of prime divisors than w and clearly $H_4 = F(\sqrt{q}, \sqrt{w'})$, which contradicts our choice of w.

On the other hand, since $F(\sqrt{w})/F$ is unramified at primes not dividing $2q$, all prime divisors of w prime to $2q$ occur in the prime factorization of the ideal (w) with even exponents, so w does not have any such prime divisors. In other words, the norm of w has no prime divisors different from 2 and q.

Since $(q/p) = 1 = (2/p)$, the primes 2 and q split in F. Let $\mathfrak{q}_1$, $\mathfrak{q}_2$ be the primes of F over q and $\mathfrak{p}_1, \mathfrak{p}_2$ be the primes over 2. Thus $(w) = \mathfrak{p}_1^a\mathfrak{p}_2^b\mathfrak{q}_1^c\mathfrak{q}_2^d$ and we may assume that $a \geq b$ and $c \geq d$. Now $(\mathfrak{q}_1\mathfrak{q}_2)^d = (q)^d$ so if $d > 0$ then $w' = w/q^d$ is a totally positive integer with fewer prime divisors than w such that $H_4 = F(\sqrt{q}, \sqrt{w'})$, which contradicts our choice of w. Thus $d = 0$.

Let $\overline{w}$ be the conjugate of w. Since Γ has unique normal subgroup of order 2 and it fixes the normal subfield H_2, the extension $F(\sqrt{w})/\mathbb{Q}$ is not normal. Consequently, $F(\sqrt{w}) \neq F(\sqrt{\overline{w}})$. Thus the quadratic subextensions of H_4/F

are H_2, $F(\sqrt{w})$ and $F(\sqrt{\overline{w}})$. Note that both $\mathfrak{p}_1$ and $\mathfrak{p}_2$ ramify in H_2. Let $\mathfrak{P}$ be a prime of H_4 over $\mathfrak{p}_1$. The inertia group $I(\mathfrak{P})$ of $\mathfrak{P}$ has order 2, since H_4/K is unramified. Thus the fixed field of $I(\mathfrak{P})$ is a quadratic subextension of H_4/F in which $\mathfrak{p}_1$ is unramified. Consequently, $\mathfrak{p}_1$ is unramified in one of the fields $F(\sqrt{w})$, $F(\sqrt{\overline{w}})$. Equivalently, one of the primes $\mathfrak{p}_1$, $\mathfrak{p}_2$ does not ramify in $F(\sqrt{w})$, so one of the integers a, b is even and therefore 0. Thus $b = 0$, since $a \geq b$. Note now that $\mathbb{Q}(\sqrt{w\overline{w}}) = \mathbb{Q}(\sqrt{2^a q^c})$ is a quadratic subfield of H_4 so a is even and consequently $a = 0$. Thus $(w) = \mathfrak{q}_1^c$. If $c = 0$ then w would be a unit, which is not possible since the fundamental unit of F has norm -1. Thus c is odd and therefore the norm of w is an odd power of q.

Let now z be any totally positive integer in F whose norm is an odd power of q. Thus $(z) = \mathfrak{q}_1^m \mathfrak{q}_2^n$ and $m + n$ is odd. It follows that $z^c/q^{nc}w^{m-n}$ is a totally positive unit of F, hence a square in F. Since both c and $m - n$ are odd, either z/w or z/qw is a square in F. In particular, $H_4 = H_2(\sqrt{w}) = H_2(\sqrt{z})$ since $\sqrt{q}$ is in H_2. ∎

Corollary 1. *The prime ideal of K over p splits completely in H_4 iff $(q/p)_4 = 1$.*

Proof. By Theorem 4, there is a totally positive integer z in F such that $H_4 = H_2(\sqrt{z})$ and the norm of z is an odd power of q. Note that since q is odd and $p \equiv 1 \pmod 8$, we can write $z = a + b\sqrt{p}$ for some rational integers a, b. Thus $a^2 - pb^2 = q^t$ for some odd integer t.

A prime $\mathfrak{p}$ over p in K splits completely in H_4 iff the residue fields of the prime ideals over $\mathfrak{p}$ in H_4 are the prime fields of characteristic p, which is equivalent to z being a square modulo $\mathfrak{p}$, i.e. a being a square modulo p. But $a^2 \equiv q^t \pmod p$, so a is a square modulo p iff q is a 4th power modulo p, i.e. $(q/p)_4 = 1$. ∎

Corollary 2. *If $h(4pq)$ is not divisible by* 8 *and $(q/p)_4 = 1$ then the prime ideal of K over p is principal and V_N is of type* I *for $N = \mathbb{Q}(\sqrt{p}, \sqrt{q})$.*

Proof. If $h(4pq)$ is not divisible by 8 then H_4 is the Hilbert 2-class field of K. By the previous corollary and the assumption that $(q/p)_4 = 1$, we see that the prime ideal $\mathfrak{p}$ over p in K splits completely in the Hilbert 2-class field of K and hence in the Hilbert class field of K, since $\mathfrak{p}^2$ is principal. Thus the ideal $\mathfrak{p}$ is principal by class field theory. ∎

Corollary 3 (Brown [1]). *If either $8 \mid h(4pq)$ or the prime in K over p is principal then $(q/p)_4 = 1$.*

Proof. Let $\mathfrak{p}$ be the prime ideal of K above p and let H_{2^k} be the Hilbert 2-class field of K. Since $\mathfrak{p}^2$ is principal, $\mathfrak{p}$ splits completely in $H_{2^{k-1}}$ and it splits completely in H_{2^k} iff $\mathfrak{p}$ is principal. Since we assumed that either $k \geq 3$ or $\mathfrak{p}$ is principal, $\mathfrak{p}$ splits completely in H_4, so $(q/p)_4 = 1$ by Corollary 1. ∎

Remark. The last corollary was obtained in [1] using the theory of binary quadratic forms.

We record the following curious corollary, which belongs to a family of results called reflection theorems. We do not know of any direct proof of this result.

Corollary 4. *If* $8 \mid h(4pq)$ *then* $8 \mid h(-pq)$.

Proof. It is a direct consequence of Corollary 3 and a result of Rédei [15] which says that $8 \mid h(-pq)$ iff $(-q/p)_4 = 1$. ∎

Now we can state and prove the main result of this section. First we define a number field

$$M = \mathbb{Q}(\sqrt[4]{q}, \zeta_8, \sqrt{\alpha}),$$

where ζ_8 is a primitive 8th root of 1 and α is a generator of the prime ideal $\mathfrak{g}$ of $\mathbb{Q}(\sqrt{q})$ over 2. Note that $\mathfrak{g}$ is indeed principal, since $\mathfrak{g}^2 = (2)$ and the class number of $\mathbb{Q}(\sqrt{q})$ is odd by genus theory. The field M as defined above seems to depend on the choice of a generator α but it is in fact independent of such a choice. In fact, we have the following

Lemma 2. *The field* $M_2 = \mathbb{Q}(\zeta_8, \sqrt{\alpha})$ *is a normal extension of* $\mathbb{Q}$ *of degree* 16 *which does not depend on the choice of* α. *Consequently*, $M/\mathbb{Q}$ *is a normal extension of degree* 32 *independent of the choice of* α.

Proof. Let β be the conjugate of α. Thus $\alpha\beta = \pm 2$ and α/β is a unit. Since both $\sqrt{2}$ and $\sqrt{-2}$ belong to $\mathbb{Q}(\zeta_8)$, we see that $M_2 = \mathbb{Q}(\zeta_8, \sqrt{\alpha}) = \mathbb{Q}(\zeta_8, \sqrt{\beta})$. Since $\mathbb{Q}(\zeta_8, \sqrt{q})/\mathbb{Q}$ is normal of degree 8, it follows that $M_2/\mathbb{Q}$ is normal of degree 16 and $M = M_2(\sqrt[4]{q})$ is normal over $\mathbb{Q}$ of degree 32.

Note that $(\alpha/\beta)\beta^2 = \pm 2$, so $\pm\alpha/\beta$ are not squares in $\mathbb{Q}(\sqrt{q})$. Thus $\alpha/\beta = \pm 2/\beta^2$ is an odd power of a fundamental unit of $\mathbb{Q}(\sqrt{q})$. It follows that $2/\beta^2 = \eta^{2k+1}$ for a fundamental unit η and some integer k, i.e. $\eta = 2/\eta^{2k}\beta^2$. Now if α' is another generator of $\mathfrak{g}$ then $\alpha' = \pm\eta^m\alpha = \pm 2^m\alpha/(\eta^k\beta)^{2m}$. Since $\sqrt{\pm 2} \in M_2$, we see that $\sqrt{\alpha'} \in M_2$ so $M_2 = \mathbb{Q}(\zeta_8, \sqrt{\alpha'})$. ∎

Our main result says that M is the minimal governing field for the divisibility by 8 of the class number $h(4pq)$. Here we think of q as fixed and $p \equiv 1 \pmod 4$ as varying.

Theorem 5. *The class number* $h(4pq)$ *is divisible by* 8 *iff* p *splits completely in* M.

Proof. Note that for $p \equiv 1 \pmod 4$ the condition that $p \equiv 1 \pmod 8$ is equivalent to the fact that p splits completely in $\mathbb{Q}(\zeta_8)$. Since $4 \nmid h(4pq)$ if $p \equiv 5 \pmod 8$, the theorem is true for primes $p \equiv 5 \pmod 8$. So we can restrict our attention to primes $p \equiv 1 \pmod 8$. Suppose first that $8 \mid h(4pq)$. Then $(q/p)_4 = 1$ by Corollary 3, so p splits completely in $\mathbb{Q}(\sqrt[4]{q}, \zeta_8)$. The field H_4 is a biquadratic extension of $\mathbb{Q}(\sqrt{q})$ ramified only at the primes over p. Since the class number of $\mathbb{Q}(\sqrt{q})$ is odd, class field theory tells us that the Galois group of the maximal 2-elementary abelian extension of $\mathbb{Q}(\sqrt{q})$ ramified only at primes over p equals $W/W^2\,\mathrm{Im}(E)$, where $W = (O/\mathfrak{p}_1)^\times \times (O/\mathfrak{p}_2)^\times \simeq \mathbb{Z}/(p-1)\times\mathbb{Z}/(p-1)$, $\mathfrak{p}_1$, $\mathfrak{p}_2$ are the primes of $\mathbb{Q}(\sqrt{q})$ over p, and $\mathrm{Im}(E)$ is the image of the units of O in W (here O is the ring of integers of $\mathbb{Q}(\sqrt{q})$). Note that W/W^2 has order 4, so $\mathrm{Im}(E)$ is contained in W^2. Let $\mathfrak{p}$ be the prime ideal of K over 2. Since $\mathfrak{p}^2$ is principal and $8\mid h(4pq)$, the ideal $\mathfrak{p}$ splits completely in H_4. Thus there are four primes in H_4 over 2 and therefore the prime $\mathfrak{g} = (\alpha)$ of $\mathbb{Q}(\sqrt{q})$ over 2 splits completely in H_4. Thus $\mathfrak{g}$ has trivial Artin symbol in W/W^2, so α is in W^2 (that is, α is a square mod pO). This implies that p splits completely in M by Kummer's criterion [8, Theorem 23].

Conversely, suppose that p splits completely in M. Then it splits completely in $\mathbb{Q}(\sqrt[4]{q},\zeta_8)$, so $(q/p)_4 = 1$. Moreover, α is in W^2 and therefore $\mathfrak{g}$ splits completely in H_4. Thus the prime $\mathfrak{p}$ over 2 splits completely in H_4. Suppose $h(4pq)$ is not divisible by 8. Then the ideal of K over p is principal by Corollary 2 and therefore $\mathfrak{p}$ is not principal (some ambiguous prime ideal is not principal by genus theory). But then $\mathfrak{p}$ cannot split completely in the Hilbert 2-class field of K, which is H_4, a contradiction. Thus $8\mid h(4pq)$. ∎

Let $M_1 = \mathbb{Q}(\sqrt[4]{q},\zeta_8)$ and recall that $M_2 = \mathbb{Q}(\sqrt{q},\zeta_8,\sqrt{\alpha})$. Both M_1, M_2 are normal over $\mathbb{Q}$ and $[M : M_i] = 2$. Let τ_i be the nontrivial automorphism of M which fixes M_i.

Corollary 5. *The Artin symbol of a prime of M above p equals τ_1 iff the class number $h(4pq)$ is not divisible by 8 and the prime of K above p is principal.*

Proof. The Artin symbol of a prime above p equals τ_1 iff p does not split completely in M but it splits completely in M_1. This is equivalent to $(q/p)_4 = 1$ and $8\nmid h(4pq)$. By Corollaries 2 and 3 the last conditions are equivalent to $8\nmid h(4pq)$ and the prime of K over p being principal. ∎

Corollary 6. *The Artin symbol of a prime of M above p equals τ_2 iff the class number $h(4pq)$ is not divisible by 8 and the prime of K above 2 is principal.*

Proof. The Artin symbol of a prime above p equals τ_2 iff p does not split completely in M but it splits completely in M_2. By the first paragraph of the proof of Theorem 5, this is equivalent to $8\nmid h(4pq)$ and the complete splitting of the prime $\mathfrak{g}$ of $\mathbb{Q}(\sqrt{q})$ above 2 in H_4. In the course of the proof of Theorem 5 we saw that $\mathfrak{g}$ splits completely in H_4 iff the prime $\mathfrak{p}$ of K over 2 splits completely in H_4. Since the condition $8\nmid h(4pq)$ is equivalent to

H_4 being the Hilbert 2-class field of K and the prime $\mathfrak{p}$ splits completely in the Hilbert 2-class field iff it is principal, the result follows. ■

5. Minkowski units and many ramified primes. In this section we show that there exist biquadratic real fields with Minkowski units and arbitrarily many ramified primes. T. Kubota showed that there are infinitely many real biquadratic fields with a Minkowski unit, but in his examples the number of ramified primes does not exceed 4. We show more generally that each of the possible four types for V_N can be realized for infinitely many real biquadratic fields N with exactly r ramified primes for each $r > 2$.

Let N be a biquadratic number field as in Section 2. Recall that if at least one of the quadratic subfields of N has fundamental unit of norm 1 then the unit group U of N consists of elements of the form $\pm\sqrt{\widehat{\varepsilon}_1^{m_1}\widehat{\varepsilon}_2^{m_2}\widehat{\varepsilon}_3^{m_3}}$, where m_1, m_2, m_3 are such that $\delta_1^{m_1}\delta_2^{m_2}\delta_3^{m_3}$ is a square in N. Thus we need to get a better understanding of the quantities δ_i.

Let $M = \mathbb{Q}(\sqrt{\Delta})$ (Δ square-free) be a real quadratic number field of discriminant d and let ε be the fundamental unit of M. Recall that we defined $\widehat{\varepsilon}$ to be ε if the norm of ε is 1 and ε^2 otherwise. Also, $\delta_M = \delta$ is defined as $\delta(\widehat{\varepsilon})$. A nice description of δ can be obtained from genus theory. We already know that δ is a positive square-free integer which is a product of some of the prime numbers which ramify in M. Note that from the equality $\widehat{\varepsilon} = a/\overline{a}$ it follows that the ideal (a) is a principal ambiguous ideal generated by a totally positive element $|a|$. Thus the product of the prime ideals which divide δ is trivial in the narrow class group of M. Genus theory tells us that the ramified primes of M generate the subgroup of ambiguous ideal classes (in the narrow sense) and that there is exactly one relation among the classes of ramified primes. It follows that this relation involves exactly the ramified primes which divide $\delta = a\overline{a}$. In particular, if the fundamental unit of M has norm -1, then $\delta = \Delta$ (since $\varepsilon\Delta$ is totally positive and the product of all the ramified primes of M equals $(\varepsilon\Delta)$).

If the fundamental unit has norm 1 the determination of the prime divisors of δ is a much more subtle problem. However, if the narrow class group of M does not have any elements of order 4 then the problem simplifies significantly, since the natural map from the group of ambiguous classes to the genus class group is an isomorphism and the triviality of an ideal class in the genus class group is detected by the genus characters (see [11, Sections 2.2 and 2.3]). As observed by Rédei, the 4-rank of the narrow class group is determined by the genus characters as well. A convenient way of organizing the information coming from genus characters is in the form of the so-called Rédei matrix. Recall that the discriminant d of M can be uniquely written (up to order of factors) as a product of prime discriminants $d = d_1 \ldots d_t$. Here d_i is either one of -4, ± 8 or $d_i = (-1)^{r_i} p_i$ where p_i is an odd prime such that $p_i \equiv 1 + 2r_i \pmod 4$. Define

$$a_{i,j} = \begin{cases} (d_i/p_j) & \text{if } i \neq j, \\ (d_i'/p_i) & \text{otherwise, where } d_i d_i' = d. \end{cases}$$

Here (d_i/p_j) is the Kronecker symbol, which coincides with the Legendre symbol for odd p_j. Define a $t \times t$ matrix $R = (R_{i,j})$ over the field $\mathbb{F}_2$ by $a_{i,j} = (-1)^{R_{i,j}}$. We call R the *Rédei matrix* of M (strictly speaking, it depends on the order of the factors in the factorization of d). Note that the column sums of R are all 0. Thus R has rank at most $t-1$ and the rank is exactly $t-1$ iff the narrow class group of M has no elements of order 4 ([11, Theorem 2.17]). Now if the rank of R is exactly $t-1$ then there is a unique vector $\mathbf{v} \neq 0$ such that $R\mathbf{v} = 0$, and p_i divides δ iff the ith coordinate of $\mathbf{v}$ is 1.

It turns out that any matrix which can be a Rédei matrix is in fact a Rédei matrix for some real quadratic number field. More precisely, we have the following

LEMMA 3. *Let $r_i \in \{0,1\}$ be such that $\sum_{i=1}^{t} r_i$ is even. Consider a $t \times t$ matrix $R = (R_{i,j})$ over the field $\mathbb{F}_2$ such that the column sums of R are 0 and $R_{i,j} = r_i r_j + R_{j,i}$ for all $i \neq j$. Then there are infinitely many real quadratic fields M with odd discriminant $d = p_1 \ldots p_t$ such that $p_i - 1 \equiv 2r_i \pmod 4$ and whose Rédei matrix is R.*

Proof. Let $R = (R_{i,j})$ and set $a_{i,j} = (-1)^{R_{i,j}}$. We must find primes $p_1, \ldots, p_t$ such that $p_i \equiv 1 + 2r_i \pmod 4$ and $a_{i,j} = ((-1)^{r_i} p_i/p_j) = (-1)^{r_i r_j}(p_i/p_j)$ for all $i > j$. In fact, the quadratic reciprocity implies then that for $i < j$ we have

$$(-1)^{r_i r_j}(p_i/p_j) = (p_j/p_i) = (-1)^{r_i r_j} a_{j,i} = a_{i,j},$$

so R is the Rédei matrix of $\mathbb{Q}(\sqrt{p_1 \ldots p_t})$. We construct the primes p_i inductively. For p_1 we may choose any prime $\equiv 1 + 2r_1 \pmod 4$. Suppose we already have $p_1, \ldots, p_s$ such that $p_i \equiv 1 + 2r_i \pmod 4$ $(i = 1, \ldots, s)$ and $(-1)^{r_i r_j}(p_i/p_j) = a_{i,j}$ for all $1 \leq j < i \leq s$. We need a prime $p_{s+1} \equiv 1 + 2r_{s+1} \pmod 4$ such that $(-1)^{r_{s+1} r_j}(p_{s+1}/p_j) = a_{s+1,j}$ for $j = 1, \ldots, s$. There are integers m_j such that $(m_j/p_j) = (-1)^{r_{s+1} r_j} a_{s+1,j}$. Any prime p which satisfies the congruences $p \equiv 1 + 2r_{s+1} \pmod 4$, $p \equiv m_j \pmod{p_j}$, $j = 1, \ldots, s$, can be taken for p_{s+1}. By the Chinese Remainder Theorem and Dirichlet's theorem there are infinitely many such primes p. ∎

We are now ready to prove our main result. Note that it follows from Theorem 2 that if N is a real biquadratic field with exactly two ramified primes then V_N is either of type I or of type IV and both types occur for infinitely many fields N. We prove the following

Theorem 6. *Let $t \geq 3$. Each of the possible four types of V_N occurs for infinitely many real biquadratic fields N with exactly t ramified primes.*

The remainder of this section is devoted to a proof of this theorem.

First we handle type IV, i.e. the case when N has a Minkowski unit. This happens iff one of the following holds:

- all ε_i have norm 1, and δ_1, δ_2, δ_3 are not squares in L and $\delta_1\delta_2\delta_3$ is a square in L;
- all ε_i have norm -1 and the index $q = [U : U_1U_2U_3] > 1$.

It turns out that when $t = 3$ and V_N is of type IV then the second possibility occurs. This case is more delicate than the other cases and will be covered in Theorem 7 below.

To show the result for $t \geq 4$ we concentrate only on the first possibility. Furthermore, we assume that $(\Delta_1, \Delta_2) = 1$, so $\Delta_3 = \Delta_1\Delta_2$. To guarantee that the fundamental units have norm 1 we assume that each Δ_i has at least one prime divisor $\equiv 3 \pmod 4$. It follows that each $\delta_i \neq \pm 1$ (it is not hard to see that $\delta(\eta)$ is never ± 1 for a fundamental unit η). Thus $\delta_1\delta_2\delta_3$ is a square in N iff $\delta_1\delta_2\delta_3 = \Delta_i m^2$ or $\delta_1\delta_2\delta_3 = m^2$ for some i and some integer m. In order to avoid any problems with divisibility by 2, we assume further that the Δ_i are odd and $\equiv 1 \pmod 4$. Thus $\delta_i \mid \Delta_i$ and $1 < \delta_i < \Delta_i$. We set $\delta_i' = \Delta_i/\delta_i$. It is easy to see that $\delta_1\delta_2\delta_3$ is a square in N iff one of the following equalities holds: $\delta_3 = \delta_1'\delta_2$, or $\delta_3 = \delta_1'\delta_2'$, or $\delta_3 = \delta_1\delta_2'$, or $\delta_3 = \delta_1\delta_2$. Note also that since δ_i is a proper divisor of Δ_i, neither δ_1 nor δ_2 can be a square in N. Also, if δ_3 is a square in N then $\delta_3 = \Delta_i$ for $i = 1$ or 2 and then $\delta_1\delta_2\delta_3$ cannot be a square in N. It follows that under the assumptions made N has a Minkowski unit iff $\delta_1\delta_2\delta_3$ is a square in N.

In order to construct required fields N, define for each even k a matrix $R_k = (b_{i,j})$ over $\mathbb{F}_2$ by setting $b_{i+1,i} = 1$, $b_{j,i} = 0$ for $j - i \geq 2$, $b_{i,j} = 1 - b_{j,i}$ for $i < j$ and $b_{i,i}$ chosen so that the column sums of R_k are all 0. It is clear that the rank of R_k is $k - 1$. Define vectors $\mathbf{v}_k \in \mathbb{F}_2^k$ by $\mathbf{v}_2 = (0,1)^{\mathrm{t}}$ and $\mathbf{v}_{k+2} = (u_1, \ldots, u_k, 0, 1)^{\mathrm{t}}$ where $(1-u_1, \ldots, 1-u_k)^{\mathrm{t}} = \mathbf{v}_k$. An easy induction shows that $R_k\mathbf{v}_k = 0$.

For each odd $k \geq 3$ define $R_k = \widehat{R}_{k-1} + S_k$, where $\widehat{R}_{k-1} = \left(\begin{smallmatrix} 0 & 0 \\ 0 & R_{k-1} \end{smallmatrix}\right)$ and $S_k = (s_{i,j})$ with $s_{i,j} = 1$ if $1 \leq i, j \leq 2$ and $s_{i,j} = 0$ otherwise. Again, it is straightforward to check that R_k has rank $k-1$ and if $\mathbf{v}_{k-1} = (u_1, \ldots, u_{k-1})^{\mathrm{t}}$ then $\mathbf{v}_k = (u_1, u_1, u_2, \ldots, u_{k-1})^{\mathrm{t}}$ satisfies $R_k\mathbf{v}_k = 0$.

By Lemma 3, for each $t \geq 2$ there exist infinitely many discriminants $d = p_1 \ldots p_t$ with $p_1 \equiv 2t - 1 \pmod 4$ and $p_i \equiv 3 \pmod 4$ for $i > 1$ such that the Rédei matrix of the field $K = \mathbb{Q}(\sqrt{d})$ equals R_t. Note that for $t \geq 4$ the Rédei matrix corresponding to $K_1 = \mathbb{Q}(\sqrt{p_1 \ldots p_{t-2}})$ equals R_{t-2} and the Rédei matrix corresponding to $K_2 = \mathbb{Q}(\sqrt{p_{t-1}p_t})$ is $\left(\begin{smallmatrix} 1 & 0 \\ 1 & 0 \end{smallmatrix}\right)$. Consider the biquadratic field $N = K_1K_2$. All 3 quadratic subfields of N have Rédei matrices of maximal possible rank. Moreover, if $\delta_j = \delta_{K_j}$, $j = 1, 2$, and $\delta = \delta_K$, then $\delta_2 = p_t$, p_i divides δ_1 iff the ith coordinate of $\mathbf{v}_{t-1}$ is 1, and p_i divides δ iff the ith coordinate of $\mathbf{v}_t$ is 1. From our description of $\mathbf{v}_t$ we see immediately that $\delta\delta_1\delta_2 = p_1 \dots p_{t-2}p_t^2$, which is a square in N. Thus N has a Minkowski unit. This proves the result for type IV and all $t \geq 4$. As was mentioned earlier, the case of $t = 3$ will be settled in Theorem 7.

In order to handle the remaining three types, we define inductively for each integer $k \geq 0$ a $(2k+1) \times (2k+1)$ matrix M_k over $\mathbb{F}_2$ such that:

(1) M_k is nonsingular;
(2) all diagonal entries of M_k are equal to $k+1 \pmod 2$;
(3) the column sums of M_k are all 1;
(4) if $M_k = (a_{i,j})$, then $a_{i,j} = 1 + a_{j,i}$ for all $i \neq j$.

Set $M_0 = (1)$. If M_k is already defined then denote its first row by $\mathbf{w} = (k+1, \dots)$, let $\widehat{\mathbf{w}}$ be the vector such that $\mathbf{w} + \widehat{\mathbf{w}} = (1, \dots, 1)$ and define M_{k+1} by

$$M_{k+1} = \left(\begin{array}{cc|c} k & k+1 & \widehat{\mathbf{w}} \\ k & k & \mathbf{w} \\ \hline \mathbf{w}^{\mathrm{t}} & \widehat{\mathbf{w}}^{\mathrm{t}} & M_k + I_k \end{array}\right).$$

It is clear that M_{k+1} has properties (2)–(4). To see that it is nonsingular note that adding the first row to the second gives

$$A = \left(\begin{array}{cc|c} k & k+1 & \widehat{\mathbf{w}} \\ 0 & 1 & 1 \\ \hline \mathbf{w}^{\mathrm{t}} & \widehat{\mathbf{w}}^{\mathrm{t}} & M_k + I_k \end{array}\right).$$

Note that in spite of (4), the addition of 1 to each entry of $M_k + I_k$ results in the matrix M_k^{t}. Thus adding the second row of A to all other rows results in

$$B = \left(\begin{array}{cc|c} k & k & \mathbf{w} \\ 0 & 1 & 1 \\ \hline \mathbf{w}^{\mathrm{t}} & \mathbf{w}^{\mathrm{t}} & M_k^{\mathrm{t}} \end{array}\right).$$

The third column of B is $(k+1, 1, \mathbf{w})^{\mathrm{t}}$ so adding the third column to the first two columns produces

$$C = \left(\begin{array}{cc|c} 1 & 1 & \mathbf{w} \\ 1 & 0 & 1 \\ \hline 0 & 0 & M_k^{\mathrm{t}} \end{array}\right)$$

and it is clear that C is invertible, since M_k^{t} is.

Having defined M_k let us introduce for each $k > 0$ a $2k \times 2k$ matrix N_{2k} by

$$N_{2k} = \left(\begin{array}{c|c} M_{k-1} & 0 \\ \hline 1 & 0 \end{array}\right).$$

It is clear that N_{2k} has property (4), rank $2k-1$, its column sums are all 0 and $N_k(0,\ldots,0,1)^{\mathrm{t}} = 0$. Finally, we define $(2k+1)\times(2k+1)$ matrices N_{2k+1} by $N_{2k+1} = \widehat{N}_{2k} + S_{2k+1}$, where $\widehat{N}_{2k} = \left(\begin{smallmatrix} 0 & 0 \\ 0 & N_{2k}\end{smallmatrix}\right)$ and $S_{2k+1} = (s_{i,j})$ with $s_{i,j} = 1$ if $1 \le i,j \le 2$ and $s_{i,j} = 0$ otherwise. It is straightforward to see that N_{2k+1} has rank $2k$ and column sums equal to 0. Moreover, $N_{2k+1}(0,\ldots,0,1)^{\mathrm{t}} = 0$.

By Lemma 3, for any $t \ge 4$ there exist infinitely many odd discriminants $d = p_1 \ldots p_t$ with $p_1 \equiv 2t-1 \pmod 4$ and $p_i \equiv 3 \pmod 4$ for all $i > 1$ such that the Rédei matrix of the field $K_1 = \mathbb{Q}(\sqrt{d})$ equals N_t. Thus, $\delta_1 = \delta_{K_1} = p_t$. Let $l = 3$ if t is even and $l = 4$ otherwise. Note that the Rédei matrix of $K_2 = \mathbb{Q}(\sqrt{p_l p_{l+1} \ldots p_t})$ is equal to N_{t+1-l}. In particular, $\delta_2 = \delta_{K_2} = p_t$. Consider the quartic field $N = K_1K_2$. Its third quadratic subfield is $K_3 = \mathbb{Q}(\sqrt{p_1p_2\ldots p_{l-1}})$, so $\delta_3 = \delta_{K_3}$ is a proper, nontrivial divisor of $p_1 \ldots p_{l-1}$. It is now clear that the only nontrivial case when $\delta_1^{m_1}\delta_2^{m_2}\delta_3^{m_3}$ is a square in N is when m_1, m_2 are odd and m_3 is even. Thus the units of N modulo torsion are of type II. This takes care of type II when $t \ge 4$. Since Theorem 2 settles the case $t = 3$, Theorem 6 is proved for type II.

To get units modulo torsion of type III we need to use quadratic fields whose discriminants are not coprime. Let $t \ge 2$ be an integer. As above, by Lemma 3, there exist odd discriminants $d = p_1 \ldots p_t$ with $p_1 \equiv 2t-1 \pmod 4$ and $p_i \equiv 3 \pmod 4$ for all $i > 1$ such that the Rédei matrix of the field $K_1 = \mathbb{Q}(\sqrt{d})$ equals N_t. Thus, $\delta_1 = \delta_{K_1} = p_t$. There exist infinitely many primes $p_t' \equiv 3 \pmod 4$ such that $p_t' \ne p_i$ for all i and the Rédei matrix of the field $K_2 = \mathbb{Q}(\sqrt{d'})$ equals N_t as well, where $d'p_t = dp_t'$. In particular, $\delta_2 = \delta_{K_2} = p_t'$. Consider the field $N = K_1K_2$. The third quadratic subfield is $K_3 = \mathbb{Q}(\sqrt{p_tp_t'})$ so $\delta_3 = \delta_{K_3} \in \{p_t, p_t'\}$. In any case, all three numbers $\delta_i\delta_j$ are squares in N and these are the only nontrivial relations among δ_i's modulo squares. Thus the units of N modulo torsion are of type III and exactly $t+1$ primes ramify in N. Consequently, our result for type III has been proved.

Finally, to get units modulo torsion of type I it is enough to have no nontrivial relations modulo squares among δ's. To achieve that start with $t \ge 3$ and the matrix N_t. As before, there exist odd discriminants $d = p_1 \ldots p_t$ with $p_1 \equiv 2t-1 \pmod 4$ and $p_i \equiv 3 \pmod 4$ for all $i > 1$ such that the Rédei matrix of the field $K_1 = \mathbb{Q}(\sqrt{d})$ equals N_t. Thus, $\delta_1 = \delta_{K_1} = p_t$. There exist infinitely many pairs of different primes $p_{t-1}' \equiv 3 \pmod 4$, $p_t' \equiv 3 \pmod 4$ such that the sets $\{p_{t-1}', p_t'\}$ and $\{p_1, \ldots, p_t\}$ are disjoint, $(p_{t-1}/p_{t-1}') = 1$,

$(p_{t-1}/p'_t) = 1$, $(p_t/p'_{t-1}) = -1$, $(p_t/p'_t) = 1$ and the Rédei matrix of the field $K_2 = \mathbb{Q}(\sqrt{d'})$ equals N_t as well, where $d'p_{t-1}p_t = dp'_{t-1}p'_t$. The third quadratic subfield of $N = K_1K_2$ is $K_3 = \mathbb{Q}(\sqrt{p_{t-1}p_tp'_{t-1}p'_t})$ so the Rédei matrix of this field is

$$R = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

This matrix has rank 3 and $R(1,0,0,1)^{\mathrm{t}} = 0$. Thus $\delta_3 = \delta_{K_3} = p_{t-1}p'_t$. It is now evident that there are no nontrivial relations modulo squares among δ_i's. Thus the units of N modulo torsion are of type I and exactly $t+2$ primes ramify in N. This settles the result for type I and $t \geq 5$. It remains to consider the cases when $t = 3$ or $t = 4$. The case of $t = 3$ follows from our next result, Theorem 7. In order to handle the case $t = 4$ consider the matrix

$$P = \begin{pmatrix} 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 1 \end{pmatrix}.$$

This matrix has rank 3 and $P(1,1,0,0)^{\mathrm{t}} = 0$. There exist infinitely many quadruples p_1, p_2, p_3, p_4 of primes congruent to $3 \pmod 4$ such that the Rédei matrix of the field $K_3 = \mathbb{Q}(\sqrt{p_1p_2p_3p_4})$ is P. Thus $\delta_3 = \delta_{K_3} = p_1p_2$. Let $K_1 = \mathbb{Q}(\sqrt{p_1p_2})$ and $K_2 = \mathbb{Q}(\sqrt{p_3p_4})$. Thus $\delta_1 = \delta_{K_1} = p_1$ and $\delta_2 = \delta_{K_2} = p_3$. It follows that the only relation modulo squares among δ_1, δ_2, δ_3 is $\delta_3 =_2 1$. Thus the field $N = \mathbb{Q}(\sqrt{p_1p_2}, \sqrt{p_3p_4})$ is of type I(ii).

In order to complete the proof of Theorem 6 it remains to produce infinitely many real biquadratic fields with exactly three ramified primes and having a Minkowski unit or of type I. This follows from the following result, which to the best of our knowledge has not been noticed before.

THEOREM 7. *Let* p_1, p_2 *be primes congruent to* $1 \pmod 4$ *and such that* $(p_1/p_2) = -1$. *There exist infinitely many primes* $q \equiv 1 \pmod 4$ *such that the field* $N = \mathbb{Q}(\sqrt{p_1p_2}, \sqrt{qp_1})$ *has a Minkowski unit. Also*, *the field* N *is of type* I(i) *for infinitely many primes* q.

Proof. We assume that $(q/p_i) = -1$ for $i = 1, 2$. This guarantees that all three quadratic subfields of N have fundamental units of norm -1 ([4, Proposition 19.9]). Thus N has a Minkowski unit iff the index $e = [U : U_1U_2U_3] > 1$. Otherwise it is of type I(i). By the Brauer class number formula [8, p. 318] we have $h_N = eh_1h_2h_3/4$. Here h_N, h_1, h_2, h_3 are the class numbers of the fields N, $K_1 = \mathbb{Q}(\sqrt{qp_1})$, $K_2 = \mathbb{Q}(\sqrt{qp_2})$, $K_3 = \mathbb{Q}(\sqrt{p_1p_2})$ respectively. The class numbers h_i, $i = 1, 2, 3$, are congruent to 2 $(\bmod 4)$ by [4, Cor. 19.8]. Thus $e > 1$ iff $4 \mid h_N$ (recall that e is a divisor of 4). Note that the field $M = \mathbb{Q}(\sqrt{p_1}, \sqrt{p_2}, \sqrt{q})$ is an unramified extension of N of degree 2. Thus, by class field theory, the class number of N is divisible by 4 iff the class number h_M of M is even (since the abelianization of a 2-group of order at least 4 has again order at least 4). Thus we need primes q such that M has even (odd) class number. By [6, Theorem 2.15(A)(iv)], M is its own narrow genus field. Convenient necessary and sufficient conditions for M to have even class number follow from a result of Fröhlich [6, addendum II to Theorem 5.6]. In order to recall Fröhlich's criterion we need to set up some notation. For every odd prime p choose once and for all a primitive root modulo p and call it u_p. For distinct odd primes p, q define $[p, q]$ by the congruence $u_p^{[p,q]} \equiv q \pmod{p}$ (so it is defined only up to a multiple of $p - 1$). Suppose that both p and q are $\equiv 1 \pmod 4$. Then $[p, q] \equiv [q, p] \pmod 2$ by quadratic reciprocity. Let $c(p, q) = (-1)^{([p,q]-[q,p])/2}$ (note that $c(p, q) = c(q, p)$).

Suppose now that L is a real abelian number field of 2-power degree over $\mathbb{Q}$ whose Galois group is generated by three independent generators and which is equal to its narrow genus field. Suppose further that exactly three rational primes p_1, p_2, p_3 ramify in L. Then $p_i \equiv 1 \pmod 4$ for $i = 1, 2, 3$. Suppose furthermore that $(p_i/p_j) = -1$, i.e. $[p_i, p_j]$ is odd for $1 \le i < j \le 3$. Then Fröhlich's result states that the class number of L is even iff $c(p_1, p_2)c(p_2, p_3)c(p_3, p_1) = 1$. Equivalently, L has even class number iff the number

$$[p_1, p_2] + [p_2, p_1] + [p_1, p_3] + [p_3, p_1] + [p_2, p_3] + [p_3, p_2]$$

is congruent to 2 $(\bmod 4)$.

We may apply Fröhlich's criterion to our field M. Suppose that $q \equiv 1 \pmod 4$ is a prime such that:

(1) $q \equiv p_1 \pmod{p_2}$;
(2) $q \equiv p_2 \pmod{p_1}$;
(3) p_1p_2 is not a 4th power modulo q.

The first two conditions imply that $(q/p_1) = -1 = (q/p_2)$, $[p_1, q] = [p_1, p_2] \equiv 1 \pmod 2$ and $[p_2, q] = [p_2, p_1] \equiv 1 \pmod 2$. The third condition says that $[q, p_1] + [q, p_2] \equiv 2 \pmod 4$. Thus M has even class number by Fröhlich's criterion. If q satisfies conditions (1), (2) and the negation of (3) then M has odd class number.

It remains to show that there are infinitely many primes q which satisfy conditions (1)–(3) (or (1), (2) and the negation of (3)). This is a consequence of the Chebotarev density theorem. In fact, consider the field

$F = \mathbb{Q}(\zeta_1, \zeta_2, i, \sqrt[4]{p_1p_2})$, where ζ_i is a primitive p_ith root of unity. It is a Galois extension of $\mathbb{Q}$ and it has an automorphism τ such that $\tau(\zeta_i) = \zeta_i^{p_{3-i}}$ for $i = 1, 2$ and $\tau(\sqrt[4]{p_1p_2}) = -\sqrt[4]{p_1p_2}$. Let q be an odd prime such that τ is the Frobenius element of some prime of F above q. A well known description of Frobenius elements in cyclotomic fields implies that conditions (1) and (2) are satisfied. The equality $\tau(\sqrt[4]{p_1p_2}) = -\sqrt[4]{p_1p_2}$ implies condition (3). The Chebotarev density theorem guarantees that the set of such primes q is infinite (and has positive density). A similar argument with τ replaced by an automorphism which fixes $\sqrt[4]{p_1p_2}$ and acts as τ on ζ_1, ζ_2 gives infinitely many primes q which satisfy (1), (2) and the negation of (3). Our proof is therefore complete. ∎

It would be interesting to obtain more precise results about the distribution of the possible types of units modulo torsion among biquadratic extensions of $\mathbb{Q}$. It would also be interesting to analyze the units themselves. In principle, this should not be hard to do and our main reason for not doing it is that there is not such a simple algebraic classification of module types.

Acknowledgments. Thanks to Griff Elder for describing to the second author some results on the classification of $\mathbb{Z}\Gamma$-modules. We are grateful to PARI for providing extensive numerical data which led us to some of the results described in the present work.

References

[1] E. Brown, *Class numbers of real quadratic number fields*, Trans. Amer. Math. Soc. 190 (1974), 99–107.

[2] D. Burns, *On the Galois structure of units in number fields*, Proc. London Math. Soc. (3) 66 (1993), 71–91.

[3] T. Chinburg, *On the Galois structure of algebraic integers and S-units*, Invent. Math. 74 (1983), 321–349.

[4] P. E. Conner and J. Hurrelbrink, *Class Number Parity*, Ser. Pure Math. 8, World Scientific, 1988.

[5] D. Duval, *Sur la structure galoisienne du groupe des unités d'un corps abélien réel de type* (p, p), J. Number Theory 13 (1981), 228–245.

[6] A. Fröhlich, *Central Extensions*, *Galois Groups*, *and Ideal Class Groups of Number Fields*, Contemp. Math. 24, Amer. Math. Soc., 1983.

[7] —, *Units in real abelian fields*, J. Reine Angew. Math. 429 (1992), 191–217.

[8] A. Fröhlich and M. J. Taylor, *Algebraic Number Theory*, Cambridge Stud. Adv. Math. 27, Cambridge Univ. Press, 1991.

[9] T. Kubota, *Über den bizyklischen biquadratischen Zahlkörper*, Nagoya Math. J. 10 (1956), 65–85.

[10] S. Kuroda, *Über den Dirichletschen Körper*, J. Fac. Sci. Imp. Univ. Tokyo Sect. I 4 (1943), Part 5, 383–406.

[11] F. Lemmermeyer, *Reciprocity Laws. From Euler to Eisenstein*, Springer Monogr. Math., Springer, 2000.

[12] P. Morton, *Governing fields for the* 2*-classgroup of* $\mathbb{Q}(\sqrt{-q_1q_2p})$ *and a related reciprocity law*, Acta Arith. 55 (1990), 267–290.

[13] N. Moser, *Unités et nombre de classes d'une extension galoisienne diédrale de* $\mathbb{Q}$, Abh. Math. Sem. Univ. Hamburg 48 (1979), 54–75.

[14] L. A. Nazarova, *Unimodular representations of the four group*, Dokl. Akad. Nauk SSSR 140 (1961), 1011–1014 (in Russian).

[15] L. Rédei, *Aufgabe 175*, Jahresber. DMV 44 (1934), 69; solutions by Rédei, Jahresber. DMV 46 (1936), 49–50, and Scholz, ibid., 80.

[16] P. Stevenhagen, *Ray Class Groups and Governing Fields*, Théorie des Nombres, Année 1988/1989, Fasc. I, Publ. Math. Fac. Sci. Besançon, Univ. Franche-Comté, 1989.

[17] A. Weiss, *Multiplicative Galois Module Structure*, Fields Inst. Monogr. 5, Amer. Math. Soc., 1996.

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

Department of Mathematics
University of Illinois at Urbana-Champaign
1409 W. Green Street
Urbana, IL 61801-2975, U.S.A.
E-mail: ullom@math.uiuc.edu

Received on 22.1.2002
and in revised form on 30.12.2002 (4197)