ACTA ARITHMETICA
LXXXI.3 (1997)

Elementary abelian 2-primary parts of $K_2\mathcal{O}$ and related graphs in certain quadratic number fields

by

A. Vazzana (Ann Arbor, Mich.)

1. Introduction. Let $d = p_1 \ldots p_k$ be a product of rational primes congruent to $1 \bmod 8$, let $E = \mathbb{Q}(\sqrt{d})$, and let $C(E)$ be the class group of E. The following theorem from [6] gives an explicit set of conditions under which the 2-primary part of $K_2\mathcal{O}_E$ is elementary abelian.

Theorem 1.1. *The* 2*-primary part of* $K_2\mathcal{O}_E$ *is elementary abelian if and only if*

(i) *the* 2*-primary part of the ideal class group* $C(E)$ *is elementary abelian and the norm of the fundamental unit of* E *is* -1, *and*

(ii) *an odd number of the primes* $p_1, \ldots, p_k$ *fail to be represented over* $\mathbb{Z}$ *by the quadratic form* $x^2 + 32y^2$.

In this paper we will prove a similar theorem for the field $F = \mathbb{Q}(\sqrt{2d})$:

Theorem 1.2. *The* 2*-primary part of* $K_2\mathcal{O}_F$ *is elementary abelian if and only if*

(i) *the* 2*-primary part of the ideal class group* $C(E)$ *is elementary abelian and the norm of the fundamental unit of* E *is* -1, *and*

(ii) *an odd number of the primes* $p_1, \ldots, p_k$ *fail to be represented over* $\mathbb{Z}$ *by the quadratic form* $x^2 + 64y^2$.

Both of these theorems were conjectured by P. E. Conner and J. Hurrelbrink in [4]. Despite the similarity of the statements, the proof of Theorem 1.2 is somewhat more involved. We will again make use of a graph associated with the primes $p_1, \ldots, p_k$, and we will study its relationship to a new graph associated with the primes lying over $p_1, \ldots, p_k$ in $\mathbb{Q}(\sqrt{-2})$.

1991 *Mathematics Subject Classification*: Primary 11R70.

Acknowledgements. I would like to thank P. E. Conner for his guidance in the writing of this paper, and J. Hurrelbrink, J. S. Milne, and D. Ruther for their help as well.

2. Part 1 of the proof. The first part of the proof is similar to the first part of the proof of Theorem 1.1. We will show that under the assumption 4-rk $K_2\mathcal{O}_F = 0$, condition (i) of Theorem 1.2 holds. We first observe that this condition can be stated in several ways.

Proposition 2.1. *The following are equivalent*:

(1) *The* 4*-rank of* $C(E)$ *is zero*, *and the norm of the fundamental unit of* E *is* -1.

(2) *The* 4*-rank of the narrow class group of* E *is zero.*

(3) *If* d' *is positive and divides* d *and is a norm from* $E/\mathbb{Q}$, *then* $d' = 1$ *or* d.

(4) *If* d' *is positive and divides* d *and is a norm from* $F/\mathbb{Q}$, *then* $d' = 1$ *or* d.

Proof. The first three conditions were shown to be equivalent in [6, 3.3–3.5]. We now check that (3) and (4) are equivalent. Since each p_i is congruent to 1 mod 8, $(2, d')_2 = 1$ and 2 is a square mod each p_i. Thus $(2, d')_q = 1$ for all rational primes q, and so

$$(2d, d')_q = (d, d')_q$$

for all rational primes q. By the Hasse norm theorem, d' is a global norm if and only if it is a local norm for all q. Thus, d' is a norm from $F/\mathbb{Q}$ if and only if it is a norm from $E/\mathbb{Q}$. ∎

Since (1) and (4) are equivalent, the next proposition completes the first part of the proof.

Proposition 2.2. *Suppose* d' *divides* d *and is a norm from* $F/\mathbb{Q}$. *If* 4-rk $K_2\mathcal{O}_F = 0$, *then* $d' = 1$ *or* d.

Proof. Let S be the set of infinite and dyadic primes of F. We will again make use of the maps $\chi = \chi_1\chi_2 : H_F \to C_S(F)/C_S(F)^2$ defined in [3, 2.5–3.2]. The relevant key fact about χ is that 4-rk $K_2\mathcal{O}_F = 0$ if and only if the kernel of χ has order 2 (see [3, 2.3]). As before, both 2 and d' represent classes in H_F. Also as before, the class of 2 is in the kernel of χ (see [6, 3.1]). If d' is neither 1 nor d, it will represent a nontrivial class in H_F different from the class of 2. Since $\chi_2(\mathrm{cl}(p_i)) = 1$ for all i (see [6, 3.1]), the class of d' is in the kernel of χ_2.

We will show that the class of d' is in the kernel of χ_1, and hence in the kernel of χ. Thus, we will arrive at a contradiction. Let σ be the generator of $\mathrm{Gal}(F/\mathbb{Q})$. We can write $d' = \alpha\sigma(\alpha)$ for some α in F^*. Write out the factorization of the fractional ideal

$$\alpha\mathcal{O}_F = \prod_{\text{primes } Q} Q^{n_Q}$$

into prime ideals of $\mathcal{O}_F$. If $\sigma(Q) \neq Q$, then Q does not lie over one of the p_i. For such a Q, $-n_Q$ must be the exact power of Q appearing in the factorization of $\sigma(\alpha)\mathcal{O}_F$. Now n_Q is the exact power of $\sigma(Q)$ dividing $\sigma(\alpha)\mathcal{O}_F$, and so $-n_Q$ is the exact power of $\sigma(Q)$ dividing $\alpha\mathcal{O}_F$. Thus we can write

$$\alpha\mathcal{O}_F = \frac{AB}{\sigma(B)}$$

where A and B are fractional ideals of F with $\sigma(A) = A$. The fractional ideal $B\sigma(B)$ is principally generated by some β in $\mathbb{Q}^*$, and so $\sigma(B) = \beta/B$. Now we compute:

$$d'\mathcal{O}_F = \alpha\sigma(\alpha)\mathcal{O}_F = A^2 = \alpha^2\beta^2/B^4.$$

By definition, $\chi_1(\mathrm{cl}(d'))$ is the image of $\alpha\beta B^{-2}$ in $C_S(F)/C_S(F)^2$. Hence the class of d' is in the kernel of χ_1. ■

3. Graphs.

3. Graphs. Let Λ be a finite graph and let V be its set of vertices. For our purposes, a graph will consist of a set of vertices V, and a subset $\mathcal{E}_\Lambda$ of $V \times V$ of edges such that (v, v) is not in $\mathcal{E}_\Lambda$ for any v of V. That is, each pair of vertices has one or zero edges between them, and no vertex is adjacent to itself.

Definition 3.1. An *Eulerian vertex decomposition* (EVD) of Λ is an unordered pair of subsets $\{V_1, V_2\}$ of V such that

(1) $V_1 \cap V_2 = \emptyset$ and $V_1 \cup V_2 = V$, and

(2) every vertex in V_i is adjacent to an even number of vertices in V_j for $i \neq j$, $i, j = 1, 2$.

Every graph has the trivial EVD, $\{\emptyset, V\}$. EVD's turned up in the proof of Theorem 1.1 in another restatement of its condition (i). They will play an even greater role in the proof of Theorem 1.2.

Let G be a group of order 2 with generator T acting on the set of vertices of a graph Λ preserving the set of edges. That is, vertices v and v' are adjacent in Λ if and only if $T(v)$ and $T(v')$ are adjacent in Λ.

Definition 3.2. If $T(v) \neq v$ for every vertex v, then we can form the *quotient graph* $\Gamma = \Lambda/G$ as follows. The set of vertices W of Γ is the set of orbits of T. Let $\phi : V \to W$ be the map taking a vertex to its orbit. For any v and v' in V, $\phi(v)$ and $\phi(v')$ will be adjacent in Γ if and only if v and v' are adjacent in Λ or v and $T(v')$ are adjacent in Λ, but not both.

We observe that the cardinality of V is twice the cardinality of W. Our goal is to relate the existence of nontrivial EVD's of Γ to the existence of nontrivial EVD's of Λ. We will show

THEOREM 3.3. *Λ has no nontrivial EVD's if and only if*

(1) *Γ has no nontrivial EVD's*, *and*

(2) *the number of edges of $\mathcal{E}_\Lambda$ which are orbits of T is odd.*

We will prove this through a sequence of lemmas.

LEMMA 3.4. *Suppose $\{V_1, V_2\}$ is a nontrivial EVD of Λ. If $T(V_1) \neq V_2$, then Γ has a nontrivial EVD.*

Proof. We will first show that any EVD of Λ which is stable under T projects to an EVD of Γ, and then we will see that any nontrivial EVD of Λ such that $T(V_1) \neq V_2$ gives rise to a nontrivial EVD of Λ which is stable under T. Suppose $T(V_1) = V_1$. Set $W_1 = \phi(V_1)$ and $W_2 = \phi(V_2)$. Then W_1 and W_2 do not intersect, their union is all of W, and they are both nonempty. Suppose w is in W_1 and $\phi(v) = w$ for some v in V_1. Let n_v be the number of vertices in V_2 adjacent to v. Then

$$\begin{aligned} n_v = {} & \operatorname{card}\{v' \in V_2 : v \text{ and } v' \text{ are adjacent and } v \text{ and } T(v') \text{ are adjacent}\} \\ & + \operatorname{card}\{v' \in V_2 : v \text{ and } v' \text{ are adjacent and} \\ & \qquad\qquad v \text{ and } T(v') \text{ are not adjacent}\}. \end{aligned}$$

Vertices in the first set occur in pairs, and the order of the second set is exactly the number n_w of vertices in W_2 adjacent to w. Thus n_v is congruent to n_w mod 2. Since n_v is even, n_w must also be even. Similarly, if w is in W_2, then w is adjacent to an even number of vertices in W_1. Thus, $\{W_1, W_2\}$ is a nontrivial EVD of Γ.

Now suppose $T(V_1) \neq V_1$. Set

$$\begin{aligned} V_1' &= (V_1 \cap T(V_2)) \cup (V_2 \cap T(V_1)), \\ V_2' &= (V_1 \cap T(V_1)) \cup (V_2 \cap T(V_2)). \end{aligned}$$

We see that V_1' is nonempty since $T(V_1) \neq V_1$, and V_2' is also nonempty since $T(V_1) \neq V_2$. We also observe that V_1' and V_2' do not intersect, their union is all of V, and $T(V_1') = V_1'$. Thus if we show that $\{V_1', V_2'\}$ is an EVD, we will have reduced the problem to the first case, and we will be done.

First consider v in V_1'. Without loss of generality, assume v is in V_1. Let n_v be the number of vertices in V_2 adjacent to v. We know $T(v)$ is in V_2, so let $n_{T(v)}$ be the number of vertices in V_1 adjacent to $T(v)$. This number is also the number of vertices in $T(V_1)$ adjacent to v. We have

$$\begin{aligned} n_v = {} & \operatorname{card}\{v_2 \in V_2 \cap T(V_1) : v \text{ and } v_2 \text{ are adjacent}\} \\ & + \operatorname{card}\{v_2 \in V_2 \cap T(V_2) : v \text{ and } v_2 \text{ are adjacent}\}, \\ n_{T(v)} = {} & \operatorname{card}\{v_1 \in T(V_1) \cap V_1 : v \text{ and } v_1 \text{ are adjacent}\} \\ & + \operatorname{card}\{v_1 \in T(V_1) \cap V_2 : v \text{ and } v_1 \text{ are adjacent}\}. \end{aligned}$$

Since $n_v + n_{T(v)}$ is even, the number of vertices in V_2' adjacent to v is even.

Now suppose v is in V_2'. Without loss of generality, assume v is in V_1. Let n_v be the number of elements in V_2 adjacent to v. As $T(v)$ is also in V_1, let $n_{T(v)}$ be the number of vertices in V_2 adjacent to $T(v)$. This is also the number of vertices in $T(V_2)$ adjacent to v. So

$$\begin{aligned} n_v = {} & \operatorname{card}\{v_2 \in V_2 \cap T(V_2) : v \text{ and } v_2 \text{ are adjacent}\} \\ & + \operatorname{card}\{v_2 \in V_2 \cap T(V_1) : v \text{ and } v_2 \text{ are adjacent}\}, \\ n_{T(v)} = {} & \operatorname{card}\{v_2 \in T(V_2) \cap V_1 : v \text{ and } v_2 \text{ are adjacent}\} \\ & + \operatorname{card}\{v_2 \in T(V_2) \cap V_2 : v \text{ and } v_2 \text{ are adjacent}\}. \end{aligned}$$

Since $n_v + n_{T(v)}$ is even, so is the number of vertices in V_1' adjacent to v. Thus $\{V_1', V_2'\}$ is in fact an EVD. ∎

Lemma 3.5. *If Λ has an EVD of the form $\{V_1, T(V_1)\}$, then the number of edges of $\mathcal{E}_\Lambda$ which are orbits is even.*

Proof. Let n be the number of edges running between the sets V_1 and $T(V_1)$. Since $\{V_1, T(V_1)\}$ is an EVD, n is certainly even. Now

$$\begin{aligned} n = {} & \operatorname{card}\{(v, T(v)) \in V_1 \times T(V_1) : v \text{ and } T(v) \text{ are adjacent}\} \\ & + \operatorname{card}\{(v_1, v_2) \in V_1 \times T(V_1) : T(v_1) \neq v_2 \text{ and} \\ & \qquad v_1 \text{ and } v_2 \text{ are adjacent}\}. \end{aligned}$$

Since v_1 and v_2 are adjacent if and only if $T(v_1)$ and $T(v_2)$ are adjacent, elements in the second set above occur in pairs. Thus, the cardinality of the first set is even. ∎

Putting Lemmas 3.4 and 3.5 together, we have shown that if Γ has no nontrivial EVD's and the number of edges of $\mathcal{E}_\Lambda$ which are also orbits of T is odd, then Λ has no nontrivial EVD's. Next we prove half of the other direction.

Lemma 3.6. *If Γ has a nontrivial EVD, then so does Λ.*

Proof. Suppose $\{W_1, W_2\}$ is a nontrivial EVD of Γ. Let $V_1 = \phi^{-1}(W_1)$ and $V_2 = \phi^{-1}(W_2)$. For v in V_1, let n_v be the number of vertices in V_2 adjacent to v. Also let $n_{\phi(v)}$ be the number of vertices of W_2 adjacent to $\phi(v)$. Then, as in the proof of Lemma 3.4, n_v is congruent to $n_{\phi(v)}$ mod 2, and so n_v is even. ∎

DEFINITION 3.7. For a finite graph Λ, order the vertices $v_1, \ldots, v_r$ of V. Define the *modified adjacency matrix* M^Λ to be the $r \times r$ matrix over $\mathbb{F}_2$ such that for $i \neq j$, $M^\Lambda_{ij} = 1$ if and only if v_i and v_j are adjacent. Each diagonal entry is the sum of the other $r-1$ entries in its row.

We observe that M^Λ is symmetric and the entries of each row (and hence column) sum to zero. This implies that M^Λ has rank at most $r-1$.

PROPOSITION 3.8. *M^Λ has rank $r-1$ if and only if Λ has no nontrivial EVD's.*

Proof. If M^Λ has rank less than $r-1$, then the first $r-1$ rows are not linearly independent. Thus some subset of the first $r-1$ rows sum to the zero vector. Let V_1 be the set of vertices corresponding to this set of rows. Let $V_2 = V - V_1$. Notice that since the sum of all of the rows is the zero vector, the set of rows corresponding to vertices in V_2 also sum to the zero vector. Pick v_i from V_1. The sum of the ith coordinates of rows corresponding to vertices in V_2 is zero. Hence v_i is adjacent to an even number of vertices in V_2. Similarly, every vertex in V_2 is adjacent to an even number of vertices in V_1, and we have shown $\{V_1, V_2\}$ is an EVD.

On the other hand, suppose $\{V_1, V_2\}$ is a nontrivial EVD. We will show that the rows corresponding to vertices in V_1 sum to the zero vector. First, if v_i is in V_2, then we know that the sum of the ith entries of rows corresponding to vertices in V_1 is zero. If v_i is in V_1, then the sum of the ith entries of rows corresponding to vertices in V_2 is zero. Since the sum of the ith entry of all rows is zero, the sum of the ith entries of rows corresponding to vertices in V_1 must also be zero. Therefore, these rows sum to the zero vector. ■

Remark 3.9. We can actually show more. Vectors in $\mathbb{F}_2^r$ killed by M^Λ are in two-to-one correspondence with EVD's of Γ. Thus, if t is the rank of M^Λ, then the total number of EVD's is 2^{r-t-1}.

Now we consider the modified adjacency matrix of a graph Λ with T acting on it as above. Choose and order a set of representatives $v_1, \ldots, v_k$ of the orbits of T. For $1 \leq i \leq k$, let $v_{k+i} = T(v_i)$. We claim that M^Λ can be written as

$$M^\Lambda = \begin{pmatrix} A & B \\ B & A \end{pmatrix}$$

where A and B are symmetric $k \times k$ matrices. Let $1 \leq i, j \leq k$. Then v_i and v_j are adjacent if and only if v_{k+i} and v_{k+j} are adjacent. Thus the upper left block is the same as the lower right block. Similarly, v_i and v_{k+j} are adjacent if and only if v_{k+i} and v_j are adjacent, and so the upper right block and lower left block are the same. Since M^Λ is symmetric, A and B must also be symmetric. We are now ready to finish the proof of Theorem 3.3.

Lemma 3.10. *If Λ has no nontrivial EVD's, then the number of edges of $\mathcal{E}_\Lambda$ which are orbits of T is odd.*

Proof. The matrix M^Λ is row equivalent to

$$\begin{pmatrix} A & B \\ A+B & A+B \end{pmatrix},$$

which in turn is column equivalent to

$$C = \begin{pmatrix} A+B & B \\ 0 & A+B \end{pmatrix}.$$

Recall that if $\phi(v_1) = w_1$ and $\phi(v_2) = w_2$ with $w_1 \neq w_2$, then w_1 and w_2 are adjacent in Γ if and only if either v_1 and v_2 are adjacent in Λ, or v_1 and $T(v_2)$ are adjacent in Λ, but not both. Thus $M^\Gamma = A + B$. As a result, we know that the last k rows of C sum to the zero vector, and by Proposition 3.8, this is the only dependency of the rows. Let $\vec{b} = (b_1, \ldots, b_{2k})$ be the sum of the first k rows of C. Then $\vec{b}$ is not in the span of the last k rows of C. Now $b_1 = \ldots = b_k = 0$, so $\vec{b}' = (b_{k+1}, \ldots, b_{2k})$ is not in the span of the rows of M^Γ. As a result of Lemma 3.6 and Proposition 3.8, the rows of M^Γ span the $(k-1)$-dimensional subspace of $\mathbb{F}_2^k$ consisting of vectors whose entries sum to zero. Thus the sum of the entries of $\vec{b}'$ is nonzero. This sum is the sum of all entries of B. In view of the fact that B is symmetric, this sum is just the trace of B. Since $B_{ii} = 1$ if and only if v_i and $T(v_i)$ are adjacent, we have shown this occurs for an odd number of i. ■

4. Part 2 of the proof. We now define the graphs to which we will apply the theory of Section 3. Let Γ be the graph whose vertices are the primes $p_1, \ldots, p_k$, and such that for $i \neq j$, p_i and p_j are adjacent if and only if $\left(\frac{p_i}{p_j}\right) = -1$. Since the primes are congruent to $1 \bmod 4$, quadratic reciprocity implies that this is well defined. Let $K = \mathbb{Q}(\sqrt{-2})$, and let τ be the generator of $\mathrm{Gal}(K/\mathbb{Q})$. For each i, choose a prime $\mathfrak{P}_i$ of $\mathcal{O}_K$ lying over p_i. Since p_i splits in $\mathcal{O}_K$, we have $p_i\mathcal{O}_K = \mathfrak{P}_i\tau(\mathfrak{P}_i)$. Because $\mathcal{O}_K$ is a PID whose units are $\{\pm 1\}$, every ideal is principally generated with two possible choices for the generator.

Proposition 4.1. *For an appropriate choice π_i of a generator of $\mathfrak{P}_i$, $K(\sqrt{\pi_i})$ and $K(\sqrt{\tau(\pi_i)})$ are dyadically unramified.*

Proof. A generator of $\mathfrak{P}_i$ has the form $\pi_i = a + b\sqrt{-2}$ where a and b are rational integers. For such a and b, $p_i = a^2 + 2b^2$. Since p_i is congruent to $1 \bmod 8$, a must be odd and b must be even. We will consider two cases, and in each case we will show that the discriminant of $K(\sqrt{\pi_i})/K$ is prime to the dyadic prime D of K. For our first case we suppose that b is congruent to $2 \bmod 4$. By replacing π_i with $-\pi_i$ if necessary, we may assume a is congruent to 3 mod 4. Let

$$f(x)=\left(x+\frac{1+(b/2)\sqrt{-2}+\sqrt{\pi_i}}{2}\right)\left(x+\frac{1+(b/2)\sqrt{-2}-\sqrt{\pi_i}}{2}\right).$$

The splitting field for $f(x)$ is $K(\sqrt{\pi_i})$. Multiplying out we get

$$f(x)=x^2+\left(1+\frac{b}{2}\sqrt{-2}\right)x+\frac{1-a-b^2/2}{4}.$$

We see that $\operatorname{disc}(f(x))=\pi_i$, so to show D is unramified we just need to check the coefficients of $f(x)$ are algebraic integers. The coefficient of x is certainly in $\mathbb{Z}(\sqrt{-2})$. Since a is congruent to -1 mod 4 and b is congruent to 2 mod 4, the constant term is in fact an integer. Thus, we have shown $\operatorname{disc}(\mathcal{O}_{K(\sqrt{\pi_i})}/\mathcal{O}_K)=\pi_i$, and so D does not ramify.

For the second case we suppose that b is congruent to 0 mod 4. By replacing π_i with $-\pi_i$ if necessary, we may this time suppose that a is congruent to 1 mod 4. Using the same choice for $f(x)$ we find that the constant term is again an integer since 4 divides both $1-a$ and $b^2/2$. As before, this implies that D does not ramify in $K(\sqrt{\pi_i})$.

The extensions $K(\sqrt{p_i})/K$ and $K(\sqrt{\pi_i})$ are dyadically unramified, and so the composite $K(\sqrt{p_i},\sqrt{\pi_i})$ is a dyadically unramified extension of K. Since $K(\sqrt{\tau(\pi_i)})/K$ is a subextension, it is also dyadically unramified. ■

For $1\le i\le k$, set $\mathfrak{P}_{i+k}=\tau(\mathfrak{P}_i)$ and $\pi_{i+k}=\tau(\pi_i)$. We define Λ to be the graph whose vertices are $\pi_1,\dots,\pi_{2k}$, and such that for $i\ne j$, π_i and π_j are adjacent if and only if $(\pi_i,\pi_j)_{\mathfrak{P}_j}=-1$. We need to check that this is well defined.

Proposition 4.2. *For $i\ne j$, $(\pi_i,\pi_j)_{\mathfrak{P}_j}=(\pi_i,\pi_j)_{\mathfrak{P}_i}$.*

Proof. By reciprocity the statement is equivalent to $(\pi_i,\pi_j)_D=1$, where D is the dyadic prime of K. By the previous proposition, the local extension $K_D(\sqrt{\pi_i})/K_D$ is unramified. Thus, every unit in K_D is the norm of a unit from $K_D(\sqrt{\pi_i})$. Since π_j is a unit in K_D, π_j is a norm from $K_D(\sqrt{\pi_i})/K_D$. ■

Now $\operatorname{Gal}(K/\mathbb{Q})$ is a group of order two acting on the set of vertices of Λ without fixed points. Let us check that Γ is the quotient of Λ by $\operatorname{Gal}(K/\mathbb{Q})$. For $i\ne j$,

$$\left(\frac{p_j}{p_i}\right)=(p_i,p_j)_{\mathfrak{P}_i}=(\pi_i,p_j)_{\mathfrak{P}_i}=(\pi_i,\pi_j)_{\mathfrak{P}_i}(\pi_i,\tau(\pi_j))_{\mathfrak{P}_i}.$$

Thus p_i and p_j are adjacent in Γ if and only if either π_i and π_j are adjacent in Λ, or π_i and $\tau(\pi_j)$ are adjacent in Λ, but not both. As a result, Γ is in fact the quotient of Λ by $\operatorname{Gal}(K/\mathbb{Q})$.

LEMMA 4.3. *Λ has no nontrivial EVD's if and only if*

(i) *the 2-primary part of $C(E)$ is elementary abelian and the norm of the fundamental unit of E is -1, and*

(ii) *an odd number of the p_i fail to be represented over $\mathbb{Z}$ by the quadratic form x^2+64y^2.*

Proof. We saw in [6, 3.3–3.5] that Γ has no nontrivial EVD's if and only if condition (i) holds. In view of Theorem 3.3, we only need to check that condition (ii) holds if and only if π_i and $\tau(\pi_i)$ are adjacent for an odd number of i, $1\le i\le k$. By a theorem of Gauss, p_i cannot be represented over $\mathbb{Z}$ by the quadratic form x^2+64y^2 if and only if the fourth power symbol $\left[\frac{2}{p_i}\right]$ is -1 (see e.g. [7, p. 84]). Thus we need to show $\left[\frac{2}{p_i}\right]=(\pi_i,\tau(\pi_i))_{\mathfrak{P}_i}$.

Since p_i is congruent to 1 mod 8, -1 is a fourth power mod p_i, and so 2 is a fourth power mod p_i if and only if -2 is a fourth power mod p_i. Now -2 is a square mod p_i, and so $\left[\frac{2}{p_i}\right]_4=1$ when $\sqrt{-2}$ is a square mod $\mathfrak{P}_i$ and $\left[\frac{2}{p_i}\right]_4=-1$ otherwise. Hence we need to show

$$(\tau(\pi_i),\pi_i)_{\mathfrak{P}_i}=(\sqrt{-2},\pi_i)_{\mathfrak{P}_i}.$$

If we write $\pi_i=a+\sqrt{-2}b$, then $\tau(\pi_i)=a-\sqrt{-2}b$. Since $\tau(\pi_i)$ is congruent to $\tau(\pi_i)-\pi_i$ mod $\mathfrak{P}_i$, we have

$$\tau(\pi_i)\equiv -2\sqrt{-2}b \bmod \mathfrak{P}_i.$$

Since -2 is a square mod $\mathfrak{P}_i$, it remains to show that b is a square mod $\mathfrak{P}_i$. We will show that $\left(\frac{q}{p_i}\right)=1$ for all rational primes q which divide b. First, since p_i is congruent to 1 mod 8, $\left(\frac{q}{p_i}\right)=1$ when $q=2$. Now suppose q is an odd prime dividing b. We have $p_i=a^2+2b^2$, and so p_i is congruent to a^2 mod q. By quadratic reciprocity, this means that $\left(\frac{q}{p_i}\right)=1$. ■

We will now use a theorem of B. Brauckmann which will enable us to connect the 4-rank of $K_2\mathcal{O}_F$ to Λ. Let $L=\mathbb{Q}(\sqrt{-2d})$ and $C_S(L)$ be the S class group of L, where S consists of all infinite and dyadic primes of L.

PROPOSITION 4.4. *The 2-primary part of $K_2\mathcal{O}_F$ is elementary abelian if and only if the 2-primary part of $C_S(L)$ is elementary abelian.*

Proof. See [1, 2.1]. ■

As a result of Proposition 2.2, it is now enough for us to show, under the assumption that condition (i) of Theorem 1.2 holds, that condition (ii) of that theorem is equivalent to the statement 4-rank $C_S(L)=0$.

Let $M=\mathbb{Q}(\sqrt{-2},\sqrt{d})$. Then a theorem of Hasse [5, p. 74] gives us the following formula relating the class numbers of M, K, L, and E:

$$h(M)=\tfrac{1}{2}Qh(K)h(L)h(E), \tag{4.5}$$

where $Q = [\mathcal{O}_M^* : \varepsilon\mathcal{O}_E^*]$ and ε is the fundamental unit of E. Now the dyadic primes of E ramify in M. This means M/E is a type I C-M extension, and in that case $Q = 1$ (see [2, 13.2, 13.4, 13.6]). Let $\mathcal{D}$ be the dyadic prime of L, and let θ be the generator of $\mathrm{Gal}(L/\mathbb{Q})$. Then $\theta(\mathcal{D}) = (D)$, and $\mathcal{D}^2 = \mathcal{D}\theta(\mathcal{D}) = 2\mathcal{O}_L$. So $\mathcal{D}$ has order at most two in $C(L)$. If $\mathcal{D}$ were principal, then we would get a generator $m + n\sqrt{-2d}$ of $\mathcal{D}$ with m and n rational integers. By taking norms we see

$$m^2 + 2dn^2 = \pm 2,$$

which cannot happen if $d > 1$. Thus we have shown that the kernel of the map $C(L) \to C_S(L)$ has order two, or $h_S(L) = \frac{1}{2}h(L)$. Since $h(K) = 1$, (4.5) becomes

$$h(M) = h_S(L)h(E). \tag{4.6}$$

One can compute the following 2-rank formulas using [3, 7.1], and [2, 18.3]:

$$2\text{-rk}\, C_S(L) = k, \qquad 2\text{-rk}\, C(E) = k - 1.$$

Also, using [2, 4.2, 7.4, 9.1], one finds

$$2\text{-rk}\, C(M) = 2k - 1.$$

Since we are assuming condition (i), $k-1$ is the exact power of 2 dividing $h(E)$. Thus, $4\text{-rk}\, C_S(L) = 0$ if and only if $4\text{-rk}\, C(M) = 0$. The following lemma will complete the proof of the theorem:

LEMMA 4.7. *Suppose condition* (i) *of Theorem* 1.2 *holds. Then* $4\text{-rk}\, C(M) = 0$ *if and only if* Λ *has no nontrivial EVD's.*

Proof. Let ε be the fundamental unit of E. By (i) we know $\mathrm{Nm}_{E/\mathbb{Q}}(\varepsilon) = -1$. Thus, $\mathrm{Nm}_{M/K}(\varepsilon) = -1$. Since $\mathcal{O}_K^* = \{\pm 1\}$, $H^0(\mathrm{Gal}(M/K), \mathcal{O}_M^*) = 0$. (Here we are using the modified Tate cohomology.) Let S' be the set of infinite primes of K and the finite primes of K which ramify in M. These finite primes are exactly the $\mathfrak{P}_1, \ldots, \mathfrak{P}_{2k}$. Let $U_{S'}$ be the set of S' units of K. $U_{S'}$ is generated by the set $\{-1, \pi_1, \ldots, \pi_{2k}\}$. Since $h(K) = 1$, Theorem 19.3 of [2] implies that $4\text{-rk}\, C(M) = 0$ if and only if the group

$$\{\mathrm{cl}(y) \in U_{S'}/U_{S'}^2 : y \text{ is a norm from } M/K\}$$

has order 4. Since -1 and d are norms from M/K, this group has order at least 4. It has order greater than 4 exactly when a proper divisor d' of d is a norm from M/K. By the Hasse norm theorem, d' is a norm from M/K if and only if it is a local norm for all primes of K. That is, d' is a norm from M/K if and only if

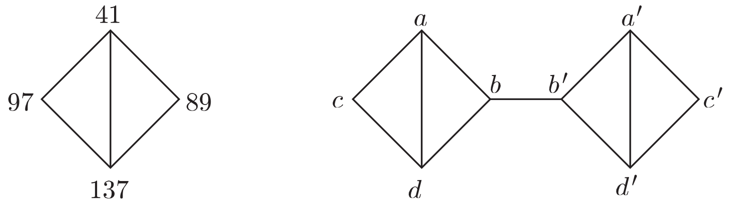
$$(d', d)_{\mathfrak{P}} = 1$$

for all primes $\mathfrak{P}$ of K. Let $V_1 = \{\pi_i : \pi_i \mid d'\}$ and $V_2 = \{\pi_i : \pi_i \nmid d'\}$. If π_i divides d', then

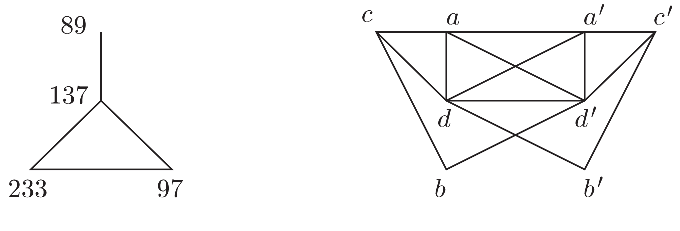
$$(d', d)_{\mathfrak{P}_i} = \left(d', \frac{d}{d'}\right)_{\mathfrak{P}_i} = \left(\pi_i, \frac{d}{d'}\right)_{\mathfrak{P}_i} = \prod_{\pi_j \nmid d'} (\pi_i, \pi_j)_{\mathfrak{P}_i}.$$

Similarly, if $\pi_i \nmid d'$, then $(d', d)_{\mathfrak{P}_i} = \prod_{\pi_j \mid d'} (\pi_i, \pi_j)_{\mathfrak{P}_i}$. Thus $(d, d')_{\mathfrak{P}} = 1$ for all primes of K if and only if $\{V_1, V_2\}$ is an EVD of Λ. This EVD is nontrivial exactly when d' is a proper divisor of d. ∎

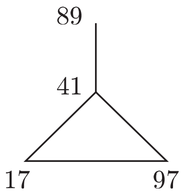
5. Examples. 1. First we take $d = 41 \cdot 89 \cdot 97 \cdot 137$. In this case, condition (1) from Theorem 3.3 fails, since $\{\{41, 137\}, \{89, 97\}\}$ is an EVD of Γ. For the graph Λ, we have labeled the vertices so that $a = -3 + 4\sqrt{-2}$, $b = -9 + 2\sqrt{-2}$, $c = -5 - 6\sqrt{-2}$, and $d = -3 + 8\sqrt{-2}$. The vertices a', b', c', and d' correspond to the conjugates of a, b, c, and d. In this case, only one pair of conjugates are adjacent, so condition (ii) of Theorem 1.2 holds. We see that $\{\{a, a', d, d'\}, \{b, b', c, c'\}\}$ is an EVD for Λ.

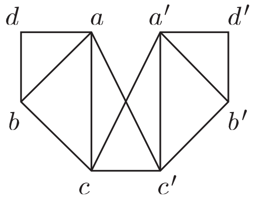


2. Next consider $d = 89 \cdot 97 \cdot 137 \cdot 233$. The graph Γ has no nontrivial EVD's so condition (1) of Theorem 3.3 holds. In the graph Λ we have $a = -9 + 2\sqrt{-2}$, $b = -5 - 6\sqrt{-2}$, $c = -3 + 8\sqrt{-2}$, and $d = 15 - 2\sqrt{-2}$. Since a and d are adjacent to their conjugates, we see that condition (ii) of Theorem 1.2 fails, and $\{\{a, b', c, d'\}, \{a', b, c', d\}\}$ is an EVD of Λ.



3. Finally, let $d = 17 \cdot 41 \cdot 89 \cdot 97$. Then Γ has no nontrivial EVD's, so condition (1) of Theorem 3.3 holds. In Λ, $a = 3 - 2\sqrt{-2}$, $b = -3 + 4\sqrt{-2}$, $c = -9 + 2\sqrt{-2}$, and $d = -5 - 6\sqrt{-2}$. Only one conjugate pair of vertices are adjacent, so condition (ii) of Theorem 1.2 also holds. We see that Λ in fact has no nontrivial EVD's.





References

[1] B. Brauckmann, *The 2-Sylow-subgroup of the tame kernel of number fields*, Canad. J. Math. 43 (1991), 255–264.

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

[3] —, —, *The 4-rank of $K_2\mathcal{O}$*, Canad. J. Math. 41 (1989), 932–960.

[4] —, —, *On elementary abelian 2-Sylow K_2 of rings of integers of certain quadratic number fields*, Acta Arith. 73 (1995), 59–65.

[5] H. Hasse, *Über die Klassenzahl Abelscher Zahlkörper*, Akademie-Verlag, Berlin, 1952.

[6] A. Vazzana, *On the 2-primary part of K_2 of rings of integers in certain quadratic number fields*, Acta Arith. 80 (1997), 225–235.

[7] B. A. Venkov, *Elementary Number Theory*, Wolters-Noordhoff, Groningen, 1970.

Department of Mathematics
University of Michigan
Ann Arbor, Michigan 48109
U.S.A.
E-mail: vazzana@math.lsa.umich.edu

Received on 25.10.1996 (3067)