ACTA ARITHMETICA
LXXIII.1 (1995)

On elementary abelian 2-Sylow K_2 of rings of integers of certain quadratic number fields

by

P. E. Conner and J. Hurrelbrink (Baton Rouge, La.)

I. Introduction. A large number of papers have contributed to determining the structure of the tame kernel $K_2\mathcal{O}_F$ of algebraic number fields F. Recently, for quadratic number fields F whose discriminants have at most three odd prime divisors, 4-rank formulas for $K_2\mathcal{O}_F$ have been made very explicit by Qin Hourong in terms of the *indefinite* quadratic form $x^2 - 2y^2$ (see [7], [8]).

We have made a successful effort, for quadratic number fields $F = \mathbb{Q}(\sqrt{\pm p_1 p_2})$, to characterize in terms of *positive definite* binary quadratic forms, when the 2-Sylow subgroup of the tame kernel of F is elementary abelian.

This makes determining exactly when the 4-rank of $K_2\mathcal{O}_F$ is zero, computationally even more accessible. For arbitrary algebraic number fields F with 4-rank of $K_2\mathcal{O}_F$ equal to zero, it has been pointed out that the Leopoldt conjecture for the prime 2 is valid for F, compare [6].

We consider this paper to be an addendum to the Acta Arithmetica publications [7], [8]. It grew out of our circulated 1989 notes [3].

Acknowledgements. We gratefully acknowledge fruitful long-term communications on this topic with Jerzy Browkin.

II. Statement of results. We consider quadratic fields $\mathbb{Q}(\sqrt{\pm p_1 p_2})$ with two odd (positive) prime numbers p_1, p_2.

For *real* quadratic fields, concerning the question of when the 2-Sylow subgroup of the tame kernel is elementary abelian, we concentrate on the most involved case $p_1 \equiv p_2 \equiv 1 \bmod 8$ and prove:

Theorem 1. *Let* $E=\mathbb{Q}(\sqrt{p_1 p_2})$ *with rational primes* $p_1 \equiv p_2 \equiv 1 \bmod 8$. *Then* 2*-Sylow* $K_2\mathcal{O}_E$ *is elementary abelian if and only if*

(i) $(p_1/p_2) = -1$ *and*

(ii) *exactly one of the two primes p_1, p_2 fails to be represented over $\mathbb{Z}$ by the quadratic form $x^2 + 32y^2$.*

For *imaginary* quadratic fields, we concentrate on the most involved case (up to the order of p_1, p_2)

$$p_1 \equiv 7 \bmod 8, \quad p_2 \equiv 1 \bmod 8 \quad \text{and} \quad (p_1/p_2) = 1$$

and prove:

THEOREM 2. *Let $L = \mathbb{Q}(\sqrt{-p_1 p_2})$ with rational primes $p_1 \equiv 7 \bmod 8$, $p_2 \equiv 1 \bmod 8$, $(p_1/p_2) = 1$. Let $h(K)$ denote the class number of $K = \mathbb{Q}(\sqrt{-2p_1})$. Then 2-Sylow $K_2\mathcal{O}_L$ is elementary abelian if and only if*

$$p_2 = x^2 + 32y^2 \quad \text{and} \quad p_2^{h(K)/4} = 2a^2 + p_1 b^2 \quad \text{with } b \not\equiv 0 \bmod p_2$$

either both have integral solutions, or neither one has an integral solution.

III. Proof of Theorem 1. We consider $E = \mathbb{Q}(\sqrt{p_1 p_2})$ with primes $p_1 \equiv p_2 \equiv 1 \bmod 8$. By definition, 2-Sylow $K_2\mathcal{O}_E$ is elementary abelian if and only if the 4-rank of $K_2\mathcal{O}_E$ is zero. By [4, 2.3] we have

(1) $$\text{4-rk}\, K_2\mathcal{O}_E = 0 \text{ if and only if 2-rk ker}\, \chi = 1$$

where $\chi : H_E \to C_S(E)/C_S(E)^2$ is the homomorphism given in [4, 2.1]. Here $C_S(E)$ denotes the S-ideal class group of E with S being the set of infinite and dyadic places of E. Since the square class of 2 lies in the kernel of χ we can restate (1) as

(2) 4-rk $K_2\mathcal{O}_E = 0$ if and only if ker χ is generated by the class of 2 in E^*/E^{*2}.

Let $C(E)$ denote the (ordinary) ideal class group of E. We have 2-rk $C(E) = 1$, compare [2, 18.3] and 2-rk$C_S(E) = 1$ also since $C_S(E)/C_S(E)^2 \cong C(E)/C(E)^2$. Let $\mathfrak{P}_1$ denote the prime ideal of $\mathcal{O}_E$ lying over the ramified prime p_1, say.

Assume now that 2-Sylow $K_2\mathcal{O}_E$ is elementary abelian. If the class of $\mathfrak{P}_1$ were a square in $C(E)$, then the class of p_1 would be in the kernel of both the homomorphisms χ_1 and χ_2 defined in [4, 2.5 and 3.1] and hence in the kernel of $\chi = \chi_1\chi_2$ (see [4, 3.2]). However by (2), the class of p_1 in E^*/E^{*2} does not lie in ker χ. Thus, the class of $\mathfrak{P}_1$, whose square is 1, is a nonsquare in $C(E)$. So, 2-Sylow $C(E)$ is generated by the class of $\mathfrak{P}_1$ and 4-rk $C(E) = 0$.

We have shown that 2-Sylow $C(E)$ is elementary abelian. This implies that $(p_1/p_2) = -1$ (compare [2, 19.6]), and in that case the norm of the fundamental unit of E is -1 (see [2, 19.9]). In other words, we concluded that the 2-Sylow subgroup of the narrow ideal class group of E is elementary abelian. In terms of the graph $\Gamma(E)$ of E (see [5]) this means that $\Gamma(E)$ is given by $p_1\bullet\!\!-\!\!\bullet p_2$, which is equivalent to the Legendre symbol (p_1/p_2) being -1.

Thus we have:

(3) $(p_1/p_2) = -1$ if and only if 2-Sylow $C(E)$ is elementary abelian and the norm of the fundamental unit of E is -1.

In order to finish the proof of Theorem 1 it now suffices to prove that under the assumption of 2-Sylow $C(E)$ being elementary abelian and $N\varepsilon = -1$ for the fundamental unit of ε of E, we have:

2-Sylow $K_2\mathcal{O}_E$ is elementary abelian if and only if exactly one of the primes p_1, p_2 fails to be represented over $\mathbb{Z}$ by the quadratic form $x^2 + 32y^2$.

Consider the subgroup U_S^+ of E^*/E^{*2} consisting of square classes of totally positive S-units of E. The 2-rank of U_S^+ is 2; the kernel of χ is generated by the class of 2 in E^*/E^{*2} if and only if $U_S^+ \cap H_E$ is generated by the class of 2. Since the elements of H_E are square classes of elements in E^* which are norms from $E(\sqrt{-1})$ over E, we have obtained so far:

(4) 2-Sylow $K_2\mathcal{O}_E$ is elementary abelian if and only if $(p_1/p_2) = -1$ and there exists a totally positive S-unit π of E that fails to be a norm from $E(\sqrt{-1})$ over E.

We will now use reciprocity of Hilbert symbols to relate the last condition to the positive definite form $x^2 + 32y^2$. Let D_1 be one of the two dyadic primes of E. For a totally positive S-unit π of E, all we have to characterize is

$$(\pi, -1)_{D_1} = -1.$$

Now, $(\pi, -1)_{D_1} = (2, \varepsilon)_{D_1}$, where ε is the fundamental unit of E. We are going to characterize

$$(2, \varepsilon)_{D_1} = -1.$$

Let $\mathfrak{D}$ be the dyadic prime of $E(\sqrt{-1})$ over D_1. We have $(2, \varepsilon)_{D_1} = (1 + i, \varepsilon)_{\mathfrak{D}}$, where $i^2 = -1$. So, exactly when is

$$(1 + i, \varepsilon)_{\mathfrak{D}} = -1\ ?$$

We want to characterize this in terms of the quadratic field $\mathbb{Q}(\sqrt{-1})$. Since ε is of norm -1, there exists a δ in $\mathbb{Q}(\sqrt{-1})$ such that δ and $\varepsilon \in E$ have the same square class in $E(\sqrt{-1})$ and $N_{\mathbb{Q}(\sqrt{-1})/\mathbb{Q}}(\delta) = p_1p_2$ in $\mathbb{Q}^*/\mathbb{Q}^{*2}$. We ask: when is

$$(1 + i, \delta)_{\mathfrak{D}} = -1\ ?$$

With $D=(1+i)$, the dyadic prime in $\mathbb{Q}(\sqrt{-1})$, this amounts to: when is

$$(1+i,\delta)_D=-1 \ ?$$

Let P_j and $\overline{P}_j$ be the primes of $\mathbb{Q}(\sqrt{-1})$ lying over $p_j, j=1,2$. Since $\mathrm{ord}_{P_j}(\delta)+\mathrm{ord}_{\overline{P}_j}(\delta)\equiv 1 \bmod 2$, we may assume that $\mathrm{ord}_{P_j}(\delta)\equiv 1 \bmod 2$, $j=1,2$. Now we can make the essential step: we have

$$(1+i,\,\delta)_D=(1+i,\,\delta)_{P_1}(1+i,\,\delta)_{P_2}$$

with the Hilbert symbols on the right hand side given by the 4-th power symbols $\left[\frac{2i}{P_j}\right]_4$, $j=1,2$. So

$$(1+i,\,\delta)_D=\left[\frac{2i}{P_1}\right]_4\left[\frac{2i}{P_2}\right]_4$$

and, by [1], the symbol $\left[\frac{2i}{P_j}\right]_4$ is -1 if and only if the rational prime p_j is not of the form x^2+32y^2 over $\mathbb{Z}$.

We have obtained

$$(\pi,-1)_{D_1}=\left[\frac{2i}{p_1}\right]_4\left[\frac{2i}{p_2}\right]_4=-1 \tag{5}$$

if and only if exactly one of the primes p_1,p_2 fails to be represented over $\mathbb{Z}$ by the quadratic form x^2+32y^2.

In view of (4), this completes the proof of Theorem 1. ■

We have given the proof of Theorem 1 via (3) and (5) in order to suggest the following generalizations.

IV. Conjectures

CONJECTURE 1. *Let* $E=\mathbb{Q}(\sqrt{p_1\dots p_k})$ *with distinct rational primes* $p_i\equiv 1 \bmod 8$, $i=1,\dots,k$. *Then* 2*-Sylow* $K_2\mathcal{O}_E$ *is elementary abelian if and only if*

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

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

Since the analogy with Theorem 1 is so beautiful we are going to state without proof:

THEOREM 1′. *Let* $F=\mathbb{Q}(\sqrt{2p_1p_2})$ *with rational primes* $p_1\equiv p_2\equiv 1 \bmod 8$. *Then* 2*-Sylow* $K_2\mathcal{O}_F$ *is elementary abelian if and only if*

(i) $(p_1/p_2)=-1$ *and*

(ii) *exactly one of the two primes* p_1,p_2 *fails to be represented over* $\mathbb{Z}$ *by the quadratic form* x^2+64y^2.

Regarding Theorem 1′ we suggest the generalization:

Conjecture 1′. *Let $F = \mathbb{Q}(\sqrt{2p_1 \dots p_k})$ with distinct rational primes $p_i \equiv 1 \bmod 8, i = 1, \dots, k$. Put $E = \mathbb{Q}(\sqrt{p_1 \dots p_k})$. Then 2-Sylow $K_2\mathcal{O}_F$ is elementary abelian if and only if*

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

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

By the above and [3], the conjectures are valid for $k = 1$ and $k = 2$.

In Theorem 1′ and Conjecture 1′ the quadratic form $x^2 + 64y^2$ replaces naturally the quadratic form $x^2 + 32y^2$ from Theorem 1 and Conjecture 1 in view of Gauss's famous result: For a prime $p \equiv 1 \bmod 8$, the fourth power symbol $\left[\frac{2}{p}\right]_4$ is -1 if and only if p is not of the form $x^2 + 64y^2$ over $\mathbb{Z}$; see e.g. [9, p. 84].

V. Numerical illustration in the real case. Among the three primes 17, 41, and 73, the prime $41 = 3^2 + 32 \cdot 1^2$ is the only one that is represented over $\mathbb{Z}$ by the form $x^2 + 32y^2$. We have $(17/41) = (17/73) = -1$ and $(41/73) = +1$. Hence, by Theorem 1:

For $E = \mathbb{Q}(\sqrt{17 \cdot 41})$, 2-Sylow $K_2\mathcal{O}_E$ is elementary abelian.
For $E = \mathbb{Q}(\sqrt{17 \cdot 73})$, 2-Sylow $K_2\mathcal{O}_E$ is *not* elementary abelian.
For $E = \mathbb{Q}(\sqrt{41 \cdot 73})$, 2-Sylow $K_2\mathcal{O}_E$ is *not* elementary abelian.

Among the three primes 17, 41, and 73, the prime $73 = 3^2 + 64 \cdot 1^2$ is the only one that is represented over $\mathbb{Z}$ by the form $x^2 + 64y^2$. Hence, by Theorem 1′ :

For $F = \mathbb{Q}(\sqrt{2 \cdot 17 \cdot 41})$, 2-Sylow $K_2\mathcal{O}_F$ is *not* elementary abelian.
For $F = \mathbb{Q}(\sqrt{2 \cdot 17 \cdot 73})$, 2-Sylow $K_2\mathcal{O}_F$ is elementary abelian.
For $F = \mathbb{Q}(\sqrt{2 \cdot 41 \cdot 73})$, 2-Sylow $K_2\mathcal{O}_F$ is *not* elementary abelian.

VI. Proof of Theorem 2. We consider $L = \mathbb{Q}(\sqrt{-p_1p_2})$ with primes $p_1 \equiv 7 \bmod 8$, $p_2 \equiv 1 \bmod 8$ and $(p_1/p_2) = 1$. Let S be the set of infinite and dyadic places of L. The 2-rank of the S-ideal class group of L is 1, compare [4, 7.1]; let $h_S(L)$ denote the S-class number of L. This time, we have by [4, 2.3]:

(6) $$4\text{-rk}K_2\mathcal{O}_L = 0 \text{ if and only if } 2\text{-rk}\ker\chi = 2.$$

In terms of the homomorphism χ_2 one concludes:

(7) 2-Sylow $K_2\mathcal{O}_L$ is elementary abelian if and only if either $h_S(L) \equiv 2 \bmod 4$ and χ_2 is trivial, or $h_S(L) \equiv 0 \bmod 4$ and χ_2 is nontrivial.

We can express the 2-rank of the kernel of χ_2 in terms of the field $L(\sqrt{-1})$ (see [4, 3.9]):

$$\text{2-rk}\ker\chi_2 = 1 + \text{2-rk}C_S(L(\sqrt{-1})).$$

Thus, by [4, 7.3] we find that χ_2 is trivial if and only if $\text{2-rk}C_S(L(\sqrt{-1})) = 2$ if and only if p_2 is represented by x^2+32y^2 over $\mathbb{Z}$. So, we conclude:

(8) 2-Sylow $K_2\mathcal{O}_L$ is elementary abelian if and only if either $h_S(L) \equiv 2 \bmod 4$ and p_2 is represented by x^2+32y^2 over $\mathbb{Z}$, or $h_S(L) \equiv 0 \bmod 4$ and p_2 is *not* represented by x^2+32y^2 over $\mathbb{Z}$.

The issue left is to identify such pairs of primes p_1, p_2 for which $h_S(L) \equiv 2 \bmod 4$. The 2-Sylow subgroup of the ideal class group of the quadratic field $K = \mathbb{Q}(\sqrt{-2p_1})$ is cyclic of order divisible by four (see [2, 18.6 and 19.6]). Hence K admits a unique unramified cyclic extension N of degree 4 over K. The field N has the following properties: N is a quadratic extension of $\mathbb{Q}(\sqrt{-p_1}, \sqrt{2})$, N is normal over $\mathbb{Q}$, and the Galois group of N over $\mathbb{Q}$ is the dihedral group of order 8.

The rational prime p_2 splits in $\mathbb{Q}(\sqrt{-p_1}, \sqrt{2})$. Thus the Artin symbol $\mathfrak{A}(p_2, N/\mathbb{Q})$ is a well-defined central element of $\mathrm{Gal}(N/\mathbb{Q})$. In terms of the Artin symbol we have the following characterization:

(9) $h_S(L) \equiv 2 \bmod 4$ if and only if $\mathfrak{A}(p_2, N/\mathbb{Q}) \neq 1$ if and only if p_2 is not completely split in N over $\mathbb{Q}$.

The characterization (9) does make it possible to restate result (8) in definite terms. The prime p_2 splits in K and p_2 is a norm from K over $\mathbb{Q}$. We write $p_2\mathcal{O}_K = P_2\overline{P}_2$; the class of P_2 is a square in the ideal class group $C(K)$. The prime P_2 of K splits completely in N over K if and only if its class is a fourth power in $C(K)$. Since the 2-Sylow subgroup of $C(K)$ is cyclic we conclude that either $\mathrm{cl}(P_2)^{h(K)/4}$ is trivial in $C(K)$, or $\mathrm{cl}(P_2)^{h(K)/4}$ is the element of order 2 in $C(K)$.

Thus either $P_2^{h(K)/4}$ is principal which occurs if and only if p_2 splits completely in N over $\mathbb{Q}$, or $D \cdot P_2^{h(K)/4}$ is principal, where D is the dyadic prime of K. In view of (9) this yields

(10) $h_S(L) \equiv 2 \bmod 4$ if and only if $p_2^{h(K)/4} = 2a^2 + p_1 b^2$ for some $a, b \in \mathbb{Z}$ with $b \not\equiv 0 \bmod p_2$.

Thus, (8) and (10) combined yield the characterization stated in Theorem 2. ∎

We note that Theorem 2 has been given in definite terms, since there is an effective algorithm to determine the class number of K. If the class number of K is equal to 4, so $h(K)/4 = 1$, then we can drop the restriction $b \not\equiv 0 \bmod p_2$ in the statement of Theorem 2. For example, for $p_1 = 7$ we obtain:

COROLLARY. *Let $L = \mathbb{Q}(\sqrt{-7p})$ with a rational prime $p \equiv 1 \bmod 8$, $(7/p) = 1$. Then 2-Sylow $K_2(\mathcal{O}_L)$ is elementary abelian if and only if*

$$p = x^2 + 32y^2 \quad \text{and} \quad p = 2a^2 + 7b^2$$

either both have integral solutions or neither one has an integral solution.

VII. Numerical illustration in the imaginary case. For $p_1 = 7$ or 23, and $p_2 = 193$ we have $(p_1/p_2) = 1$ and $K = \mathbb{Q}(\sqrt{-2p_1})$ has class number $h(K) = 4$. We have $p_2 = 193 = 2 \cdot 3^2 + 7 \cdot 5^2$ is neither represented by $x^2 + 32y^2$ nor by $2a^2 + 23b^2$ over $\mathbb{Z}$. Hence by Theorem 2:

For $L = \mathbb{Q}(\sqrt{-7 \cdot 193})$, 2-Sylow $K_2\mathcal{O}_L$ is *not* elementary abelian.
For $L = \mathbb{Q}(\sqrt{-23 \cdot 193})$, 2-Sylow $K_2\mathcal{O}_L$ is elementary abelian.

For $p_1 = 31$ and $p_2 = 193$ we have $(p_1/p_2) = 1$ and $K = \mathbb{Q}(\sqrt{-2 \cdot 31})$ has class number $h(K) = 8$. Since neither $p_2 = 193$ is represented by $x^2 + 32y^2$ nor $p_2^2 = 193^2$ is represented by $2a^2 + 31b^2$, we have by Theorem 2:

For $L = \mathbb{Q}(\sqrt{-31 \cdot 193})$, 2-Sylow $K_2\mathcal{O}_L$ is elementary abelian.

References

[1] P. Barrucand and H. Cohn, *Note on primes of type $x^2 + 32y^2$, class number and residuacity*, J. Reine Angew. Math. 238 (1969), 67–70.

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

[3] —, —, *Examples of quadratic number fields with $K_2\mathcal{O}$ containing no element of order four*, circulated notes, 1989.

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

[5] J. Hurrelbrink, *Circulant graphs and 4-ranks of ideal class groups*, ibid. 46 (1994), 169–183.

[6] M. Kolster, *Remarks on étale K-theory and the Leopoldt conjecture*, in: Séminaire de Théorie des Nombres, Paris, 1991-92, Progr. Math. 116, Birkhäuser, 1993, 37–62.

[7] H. Qin, *The 2-Sylow subgroups of the tame kernel of imaginary quadratic fields*, Acta Arith. 69 (1995), 153–169.

[8] —, *The 4-rank of K_2O_F for real quadratic fields*, ibid. 72 (1995), 323–333.

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

DEPARTMENT OF MATHEMATICS
LOUISIANA STATE UNIVERSITY
BATON ROUGE, LOUISIANA 70803
U.S.A.

Received on 27.12.1994
and in revised form on 18.2.1995 (2717)