J. Aust. Math. Soc. **93** (2012), 115–120
doi:10.1017/S1446788712000626

RELATIONS IN THE 2-CLASS GROUP OF QUADRATIC NUMBER FIELDS

F. LEMMERMEYER

(Received 15 April 2011; accepted 1 February 2012; first published online 7 February 2013)

Communicated by J. O. Shallit

Dedicated to the memory of Alf van der Poorten

Abstract

We construct a family of ideals representing ideal classes of order two in quadratic number fields and show that relations between their ideal classes are governed by certain cyclic quartic extensions of the rationals.

2010 *Mathematics subject classification*: primary 11R11; secondary 11R29.
Keywords and phrases: quadratic number field, ideal class group, genus theory.

1. Introduction

Let $m = p_1 \times p_t$ be a product of pairwise distinct primes $p_j \equiv 1 \bmod 4$. Then m can be written as a sum of two squares, say $m = a_j^2 + 4b_j^2$, in 2^{t-1} essentially different ways (that is, neglecting the signs of a_j and b_j).

We define ideals $\mathfrak{a}_j = (2b_j + \sqrt{m}, a_j)$ in the ring of integers of the quadratic number field $K = \mathbb{Q}(\sqrt{m})$. Since

$$\begin{aligned}\mathfrak{a}_j^2 &= ((2b_j + \sqrt{m})^2, a_j(2b_j + \sqrt{m}), a_j^2)\\ &= ((2b_j + \sqrt{m})^2, a_j(2b_j + \sqrt{m}), m - 4b_j^2)\\ &= (2b_j + \sqrt{m})(2b_j + \sqrt{m}, a_j, 2b_j - \sqrt{m})\\ &= (2b_j + \sqrt{m})(4b_j, a_j, 2b_j - \sqrt{m}) = (2b_j + \sqrt{m})\end{aligned}$$

is principal, the ideals $\mathfrak{a}_j$ have order dividing 2.

The 'canonical' ideals generating classes of order dividing 2 are the products of ramified prime ideals. Letting $\mathfrak{p}_j$ denote the prime ideal above the prime p_j, we have $\mathfrak{p}_j^2 = (p_j)$. Thus each of the 2^t ideals

$$\mathfrak{b}_e = \mathfrak{p}_1^{e_1} \cdot \mathfrak{p}_t^{e_t}, \quad e = (e_1, \ldots, e_t) \in \mathbb{F}_2^t,$$

generates a class of order dividing 2. Among these ideal classes there are two trivial relations coming from the fact that the ideals $(1) = \prod \mathfrak{p}_j^0$ and $(\sqrt{m}) = \prod \mathfrak{p}_j^1$ are principal (in the usual sense; the ideal class of $(\sqrt{m})$ is principal in the strict sense if and only if the fundamental unit ε of K has norm -1).

The following result is well known.

PROPOSITION 1. *There is a nontrivial relation among the ideal classes of the ideals $\mathfrak{b}_e$ if and only of the norm of the fundamental unit ε of K is $+1$.*

PROOF. If $\prod \mathfrak{p}_j^{e_j} = (\alpha)$ is principal, then $(\alpha)^2 = \prod p_j^{e_j}$, hence $\eta = \alpha^2 / \prod p_j^{e_j}$ is a unit with norm $+1$. If η is a square, then so is $\prod p_j^{e_j}$, which is only possible for $e = (0, \dots, 0)$ and $e = (1, \dots, 1)$. Thus if there is a nontrivial relation among the classes of the ramified ideals, then there is a nonsquare unit with positive norm; this implies that $N\varepsilon = +1$.

Conversely, if $N\varepsilon = +1$, then $\varepsilon = \alpha^{1-\sigma}$ for some $\alpha \in O_K$ by Hilbert's theorem 90, where σ is the nontrivial automorphism of $K/\mathbb{Q}$. Since (α) is fixed by the Galois group of $K/\mathbb{Q}$, the ideal (α) is a product of a rational integer and a ramified ideal. Cancelling the rational factors, we see that we may assume that (α) is a product of ramified prime ideals. The equations $\alpha = 1$ and $\alpha = \sqrt{m}$ would imply that $\varepsilon = \pm 1$; thus the relation $(\alpha) = \prod \mathfrak{p}_j^{e_j}$ is necessarily nontrivial. □

The goal of this paper is to clarify the relations between the ideals $\mathfrak{a}_j$ and $\mathfrak{b}_e$. Our main result is the following

THEOREM 2. *Let $K = \mathbb{Q}(\sqrt{m})$ be a quadratic number field, where $m = p_1 \times p_t$ is a product of primes $p_j \equiv 1 \bmod 4$, and denote the fundamental unit of K by ε.*

(a) *If $N\varepsilon = -1$, then the ideal classes $[\mathfrak{a}_j]$ are pairwise distinct and represent the 2^{t-1} classes of order dividing 2 in $\mathrm{Cl}(K)$. Each ideal $\mathfrak{a}_j$ is equivalent to a unique ramified ideal $\mathfrak{b}_e$. In particular, exactly one of the $\mathfrak{a}_j$ is principal; if $\mathfrak{a}_j = (\alpha)$, then*

$$\eta = \frac{2b_j + \sqrt{m}}{\alpha^2}$$

is a unit with norm -1 (equal to ε if α is chosen suitably).

(b) *If $N\varepsilon = +1$, then there is a subgroup C with index 2 in the group $\mathrm{Cl}(K)[2]$ of ideal classes of order dividing 2 such that each class in C is represented by two ramified ideals $\mathfrak{b}_e$ (thus C is the group of strongly ambiguous ideal classes in K). Each class in $\mathrm{Cl}(K)[2] \setminus C$ is represented by two ideals $\mathfrak{a}_j$.*

The proof of Theorem 2 uses certain quadratic extensions of $\mathbb{Q}(\sqrt{m})$, namely cyclic quartic subextensions of the field $\mathbb{Q}(\zeta_m)$ of mth roots of unity. It is perhaps surprising that relations in the class group of K are governed by *ramified* extensions of K; note, however, that if K_1 and K_2 are two cyclic quartic extensions as above, then the compositum K_1K_2 contains a third quadratic extension K_3/K, and that this extension is unramified: in fact, it is part of the genus class field of K.

https://doi.org/10.1017/S1446788712000626 Published online by Cambridge University Press

Here is an example. Let $m = 5 \times 13 \times 29 = 1885$; then $m = 6^2 + 43^2 = 11^2 + 42^2 = 21^2 + 38^2 = 27^2 + 34^2$, and we consider the ideals $\mathfrak{a}_1 = (6 + \sqrt{m}, 43)$, $\mathfrak{a}_2 = (42 + \sqrt{m}, 11)$, $\mathfrak{a}_3 = (38 + \sqrt{m}, 21)$, $\mathfrak{a}_4 = (34 + \sqrt{m}, 27)$. Since $N\varepsilon = +1$, none of these ideals is principal. In fact we have $\mathfrak{a}_2 \sim \mathfrak{a}_3$ and $\mathfrak{a}_1 \sim \mathfrak{a}_4$. If $\mathfrak{p}$ denotes the ideal with norm 5, then the ideal classes of order two are represented by $\mathfrak{p}$, $\mathfrak{a}_1$ and $\mathfrak{a}_2 \sim \mathfrak{a}_1\mathfrak{p}$.

The ramified prime ideal above 29 is principal (in fact, $N(87 + 2\sqrt{1885}) = 29$), those above 5 and 13 are not. In particular, $\sqrt{\varepsilon} = 2\sqrt{65} + 3\sqrt{29}$.

2. Cyclic quartic extensions

Let $m = a^2 + 4b^2$ be a squarefree odd integer; then it is the discriminant of the quadratic number field $k = \mathbb{Q}(\sqrt{m})$. In the following, we will always assume that $m = p_1 \times p_t$, where the $p_j \equiv 1 \bmod 4$ are prime numbers.

Some basic facts concerning the description of abelian extensions of the rationals via characters can be found in [2]. The field of mth roots of unity has Galois group isomorphic to $(\mathbb{Z}/m\mathbb{Z})^\times \simeq \prod(\mathbb{Z}/p_j\mathbb{Z})^\times$, hence has $G = (\mathbb{Z}/4\mathbb{Z})^t$ as a quotient. This group G is the Galois group of the compositum F of the cyclic quartic extensions inside the fields $\mathbb{Q}(\zeta_{p_j})$. The character group $X = X(G)$ is generated by quartic Dirichlet characters $\chi_j = \chi_{p_j}$, and the cyclic quartic subfields of L (and of $\mathbb{Q}(\zeta_m)$) correspond to cyclic subgroups of X with order four.

Suppose that χ is a character generating such a cyclic group of order four, and let $L/\mathbb{Q}$ be the corresponding cyclic quartic extension. Then $\chi = \prod \chi_j^{e_j}$ with $0 \le e_j < 4$. The order of χ is four if and only if at least one exponent e_j is odd. By the conductor-discriminant formula, the field L has discriminant m^3 if and only if all the e_j are odd. Thus these characters correspond to vectors $e = (e_1, \ldots, e_t)$ with $e_j \in \{1, 3\}$. The cyclic quartic extensions $L/\mathbb{Q}$ inside F with discriminant m^3 correspond to subgroups generated by such characters, and since each subgroup contains two such characters (χ and χ^3), we have following proposition.

Proposition 3. *Let $m = p_1 \times p_t$ be a product of distinct primes $p_j \equiv 1 \bmod 4$. Then there are 2^{t-1} cyclic quartic extensions $L/\mathbb{Q}$ with conductor m and discriminant m^3.*

These extensions can be constructed explicitly as the following proposition.

Proposition 4. *Let $m = p_1 \times p_t$ be a product of pairwise distinct primes $p \equiv 1 \bmod 4$. Then there exist 2^{t-1} ways of writing $m = a_j^2 + 4b_j^2$ as a sum of two squares (up to sign). For each j, the extensions*

$$L = \mathbb{Q}\left(\sqrt{m + 2b_j\sqrt{m}}\right)$$

are the 2^{t-1} different cyclic quartic extension of $\mathbb{Q}$ with discriminant m^3.

We use this result, which we will prove below, in the following proof.

Proof of Theorem 2. Assume first that $N\varepsilon = -1$. We have to show that the classes of the ideals $\mathfrak{a}_j = (2b_j + \sqrt{m}, a_j)$ are pairwise distinct.

https://doi.org/10.1017/S1446788712000626 Published online by Cambridge University Press

Assume to the contrary that $\mathfrak{a}_j \sim \mathfrak{a}_k$; then there exists some $\xi \in K$ with $\mathfrak{a}_j = \xi\mathfrak{a}_k$. Squaring gives the equation $(2b_j + \sqrt{m}) = \xi^2(2b_k + \sqrt{m})$ of ideals, hence there exists a unit $\eta \in O_K^\times$ such that $2b_j + \sqrt{m} = \eta\xi^2(2b_k + \sqrt{m})$. This means that the square roots of $(2b_j + \sqrt{m})\sqrt{m}$ and $\eta(2b_k + \sqrt{m})\sqrt{m}$ must generate the same extension. Since $\mathbb{Q}(\sqrt{(2b_j + \sqrt{m})\sqrt{m}})$ is a cyclic quartic extension inside $\mathbb{Q}(\zeta_m)$, so is the extension on the right-hand side. But this implies that $N\eta = +1$, and the fact that $N\varepsilon = -1$ implies that $\eta = \pm\varepsilon^{2n}$. Subsuming the unit into ξ shows that we may assume that $\eta = \pm 1$. If $\eta = -1$, the extension on the right-hand side will ramify at 2, and this finally shows that η is a square. Thus we have $\mathbb{Q}(\sqrt{(2b_j + \sqrt{m})\sqrt{m}}) = \mathbb{Q}(\sqrt{(2b_k + \sqrt{m})\sqrt{m}})$ and this can only hold if $j = k$.

We have shown that exactly one ideal $\mathfrak{a}_j$ is principal, say $\mathfrak{a}_j = (\alpha)$. Since $(\alpha)^2 = \mathfrak{a}_j^2 = (2b_j + \sqrt{m})$ there exists a unit η such that $\eta\alpha^2 = 2b_j + \sqrt{m}$. Taking the norm shows that $N\eta = -1$ as claimed.

If $N\varepsilon = +1$, on the other hand, we first show that none of the ideals $\mathfrak{a}_j$ is equivalent to a ramified ideal $\mathfrak{b}_e$. In fact, if $\mathfrak{a}_j = \xi\mathfrak{b}_e$ for some $\xi \in K^\times$, then squaring yields $2b_j + \sqrt{m} = \eta\xi^2 m_1$ for $m_1 = \prod p_j^{e_j}$ and some unit η. Taking norms shows that $N\eta = -1$, which contradicts our assumptions.

Next we show that among the classes of $\mathfrak{a}_j$, each ideal class occurs twice. In fact, if $\mathfrak{a}_j \sim \mathfrak{a}_k$, say $\mathfrak{a}_j = \xi\mathfrak{a}_k$, then $2b_j + \sqrt{m} = \eta\xi^2(2b_k + \sqrt{m})$. Up to squares, η is equal to one of the units $\pm 1, \pm\varepsilon$. As above, $\eta = -1$ and $\eta = -\varepsilon$ are impossible, since the places at infinity ramify in the extension $K(\sqrt{\eta(2b_k + \sqrt{m})\sqrt{m}})/K$ but not in $K(\sqrt{(2b_j + \sqrt{m})\sqrt{m}})/K$. Thus either $\eta = 1$ and $j = k$, or $\eta = \varepsilon$.

Thus each $\mathfrak{a}_j$ is equivalent to at most one other $\mathfrak{a}_k$. Since there are 2^{t-1} ideals $\mathfrak{a}_j$, which are distributed among the 2^{t-1} ideal classes of order two in $\mathrm{Cl}(K)[2] \setminus C$, it follows that each $\mathfrak{a}_j$ is equivalent to exactly one other $\mathfrak{a}_k$ as claimed. □

3. Generators of cyclic quartic extensions

In this section we will give a proof of Proposition 4.

Kummer generators over $\mathbb{Q}(i)$. Cyclic quartic extensions $L/\mathbb{Q}$ become Kummer extensions over $\mathbb{Q}' = \mathbb{Q}(i)$: with $L' = L(i)$ we have $L' = \mathbb{Q}'(\sqrt[4]{\alpha})$ for some $\alpha \in \mathbb{Q}(i)$. Such an extension L' will be normal over $\mathbb{Q}$ if and only if $\alpha^{1-\sigma} = \alpha_\sigma^2$ is a square in $\mathbb{Q}'$, where σ is the nontrivial automorphism of $\mathbb{Q}'/\mathbb{Q}$, and will be abelian over $\mathbb{Q}$ if and only if σ acts on α_σ as on a fourth root of unity, that is, if and only if $\alpha_\sigma^\sigma = \alpha_\sigma^{-1}$.

Since $\alpha_\sigma^{\sigma+1} = 1$, Hilbert's theorem 90 implies that $\alpha_\sigma = \mu^{\sigma-1} = \overline{\mu}/\mu$ for some $\mu \in \mathbb{Z}[i]$. Thus $\alpha^{1-\sigma} = (\overline{\mu}/\mu)^2$. This equation is solved by $\alpha = \mu\overline{\mu}^3 = m\overline{\mu}^2$, where $m = \mu\overline{\mu}$ is a positive integer. Galois theory actually shows that this is the only solution up to multiplying α by some nonzero rational number.

We claim that α can be chosen in such a way that 2 is unramified in $L'/\mathbb{Q}'$. Since $k' = \mathbb{Q}'(\sqrt{\alpha}) = \mathbb{Q}'(\sqrt{m})$, the prime above 2 does not ramify in the quadratic

https://doi.org/10.1017/S1446788712000626 Published online by Cambridge University Press

subextension $k'/\mathbb{Q}'$. In order for 2 to be unramified in L'/k' we have to make sure that $\sqrt{\alpha} = \overline{\mu}\sqrt{m} \equiv \mu\sqrt{m} \bmod 4$ is congruent to a square modulo 4 in k' (see [1] for the decomposition law in quadratic and, more generally, Kummer extensions of prime degree). If we write $\mu = a + 2bi$, then $\mu \equiv \pm 1 + 2i \bmod 4$ if $m \equiv 5 \bmod 8$, hence

$$\left(\frac{\pm 1 + 2i + i\sqrt{m}}{1+i}\right)^2 \equiv 2 + (\pm 1 + 2i)\sqrt{m} \equiv (\mp 1 + 2i)\sqrt{m} \mod 4$$

since $2 \equiv 2\sqrt{m} \bmod 4$. Similarly, we have $\mu \equiv \pm 1 \bmod 4$ if $m \equiv 1 \bmod 8$, hence

$$\left(\frac{\pm 1 + i\sqrt{m}}{1+i}\right)^2 \equiv \sqrt{m} \equiv \overline{\mu}\sqrt{m} \mod 4.$$

Thus 2 is unramified in L'/k' if we choose $\mu \equiv 1 \bmod 2$.

We have proved the following lemma.

LEMMA 5. *If $L/\mathbb{Q}$ is a cyclic quartic extension with conductor m, then there exist integers a, b such that $L' = \mathbb{Q}'(\sqrt[4]{\alpha})$ for $\alpha = \mu\overline{\mu}^3$, where $\mu = a + 2bi \in \mathbb{Z}[i]$ and $m = a^2 + 4b^2$. Replacing a by $-a$ or b by $-b$ does not change the extension.*

Kummer generators over $\mathbb{Q}$. Let $L' = \mathbb{Q}'(\sqrt[4]{\alpha})$ be a Kummer extension of degree four over $\mathbb{Q}' = \mathbb{Q}(i)$, and assume that $\alpha = \mu\overline{\mu}^3$ for some $\mu = a + 2bi \in \mathbb{Z}[i]$. Set $\beta = \sqrt[4]{\alpha}$; we claim that $\beta + \beta'$ is an element of $\mathbb{Q}(\sqrt{m})$, where $m = \mu\overline{\mu} = a^2 + 4b^2$. In fact, $(\beta + \beta')^2 = \sqrt{m}(\mu + \overline{\mu}) + 2m = 2m + 2a\sqrt{m}$. This implies that L' contains a quartic subextension $L = \mathbb{Q}(\sqrt{2m + 2a\sqrt{m}})$.

The following lemma shows that L is also generated by $\sqrt{m + 2b\sqrt{m}}$.

LEMMA 6. *Assume that $Ax^2 - By^2 - Cz^2 = 0$. Then*

$$2(x\sqrt{A} + y\sqrt{B})(x\sqrt{A} + z\sqrt{C}) = (x\sqrt{A} + y\sqrt{B} + z\sqrt{C})^2. \tag{1}$$

PROOF. We have

$$\begin{aligned}(x\sqrt{A} + y\sqrt{B} + z\sqrt{C})^2 &= Ax^2 + By^2 + Cz^2 + 2xy\sqrt{AB} + 2xz\sqrt{AC} + 2yz\sqrt{BC} \\ &= 2(Ax^2 + xy\sqrt{AB} + xz\sqrt{AC} + yz\sqrt{BC}) \\ &= 2(x\sqrt{A} + y\sqrt{B})(x\sqrt{A} + z\sqrt{C})\end{aligned}$$

as claimed. □

Since $m - a^2 - 4b^2 = 0$, the lemma shows that $2(\sqrt{m} + a)(\sqrt{m} + 2b)$ is a square in $K = \mathbb{Q}(\sqrt{m})$, hence $2b\sqrt{m} + m$ and $2m + 2a\sqrt{m}$ generate the same quadratic extension of K. This finishes the proof of Proposition 4.

Acknowledgement

I thank the referee for carefully reading the manuscript and for several helpful comments and corrections.

https://doi.org/10.1017/S1446788712000626 Published online by Cambridge University Press

References

[1] E. Hecke, *Lectures on the Theory of Algebraic Numbers* (Springer, New York, 1981).
[2] L. Washington, *Introduction to Cyclotomic Fields* (Springer, New York, 1982).

F. LEMMERMEYER, Mörikeweg 1, 73489 Jagstzell, Germany
e-mail: hb3@ix.urz.uni-heidelberg.de

https://doi.org/10.1017/S1446788712000626 Published online by Cambridge University Press