J. Aust. Math. Soc. **100** (2016), 21–32
doi:10.1017/S1446788715000270

ELEMENTS OF ORDER FOUR IN THE NARROW CLASS GROUP OF REAL QUADRATIC FIELDS

ELLIOT BENJAMIN[✉] **and C. SNYDER**

(Received 15 February 2015; accepted 28 April 2015; first published online 28 September 2015)

Communicated by W. Zudilin

Abstract

Using the elements of order four in the narrow ideal class group, we construct generators of the maximal elementary 2-class group of real quadratic number fields with even discriminant which is a sum of two squares and with fundamental unit of positive norm. We then give a characterization of when two of these generators are equal in the narrow sense in terms of norms of Gaussian integers.

2010 *Mathematics subject classification*: primary 11R11; secondary 11R29.

Keywords and phrases: quadratic number field, ideal class group, narrow class group.

1. Introduction

Let k be a real quadratic number field with discriminant d_k, fundamental unit ε_k, narrow class group and 2-class group, respectively, $\mathrm{Cl}^+(k)$ and $\mathrm{Cl}_2^+(k)$, and ordinary class group and 2-class group, respectively, $\mathrm{Cl}(k)$ and $\mathrm{Cl}_2(k)$. Finally, if G is a finite abelian group, then $G[2]$ will denote its subgroup of elements of order one or two.

It is well known that $\mathrm{Cl}^+(k)[2]$ is generated by the narrow ideal classes containing the ramified prime ideals of k. However, the analogous case involving $\mathrm{Cl}(k)[2]$ is not always true, that is, the ordinary ideal classes containing the ramified primes generate a subgroup C which is not always all of $\mathrm{Cl}(k)[2]$. This situation occurs if and only if d_k is a sum of two squares and ε_k has positive norm. Now, d_k is a sum of two squares if and only if $d_k = 8^{\mu} p_1 \cdots p_t$, where the p_j are all distinct primes $\equiv 1 \bmod 4$ and $\mu = 0$ or 1, that is, the discriminant is a product of positive prime discriminants (cf. [4, Ch. 2], concerning the material mentioned here; also see [2]).

In [5, Theorem 2], a complete set of generators is obtained for $\mathrm{Cl}(k)[2]$ in the case of odd discriminant which is a sum of two squares. When the fundamental unit is of positive norm, the subgroup C mentioned above is of index two in $\mathrm{Cl}(k)[2]$ and its complement $\mathrm{Cl}(k)[2] - C$ turns out to be generated by ordinary ideal classes containing particular ideals $\mathfrak{a}$ obtained from the decomposition of the discriminant as sums of two

squares; see [5] for the details. The proof involves, roughly speaking, the use of certain cyclic quartic subextensions of $\mathbb{Q}$ containing k in the cyclotomic field $\mathbb{Q}(\zeta_{d_k})$ of d_kth roots of unity and showing that these quartic fields are in one-to-one correspondence with the ideal classes containing the ideals $\mathfrak{a}$.

In this note, we complete the project of determining generators of $\mathrm{Cl}(k)[2]$ by considering the case of even discriminant d_k (which is a sum of two squares and for which the fundamental unit has positive norm). The results are similar to the case of odd discriminant, but we use elementary methods, namely cycles of reduced quadratic forms, to complete our proof, thereby circumventing the use of arithmetic in cyclotomic fields.

We then go on to obtain a characterization, in terms of the norm of certain Gaussian integers, of when two of these generators are equal in the narrow sense.

2. The main result

We start by setting up our assumptions and notation. In light of the last paragraph of the introduction, let $d = p_1 \cdots p_t$ be a product of distinct primes with $p_1 = 2$ and $p_j \equiv 1 \bmod 4$ for $j = 2, \ldots, t$. Let $D = 4d$ and define $k = \mathbb{Q}(\sqrt{d})$; hence, $D = d_k$. It is well known that there are 2^{t-2} pairs of positive integers a, b such that $d = a^2 + b^2$ with $a < b$; cf. [3, Ch. XVI] or almost any elementary number theory text. Notice that $\mathfrak{p}_j = (p_j, \sqrt{d}) = p_j\mathbb{Z} + \sqrt{d}\,\mathbb{Z}$ $(j = 1, \ldots, t)$ are the ramified primes in k. We also assume that the fundamental unit $\varepsilon = \varepsilon_k$ has norm $+1$. Hence, $|\mathrm{Cl}^+(k)| = 2|\mathrm{Cl}(k)|$. However, since d_k is a sum of two squares, $\mathrm{Cl}^+(k)$ and $\mathrm{Cl}(k)$ have equal 2-ranks, which is $t - 1$, and therefore $|\mathrm{Cl}^+(k)[2]| = |\mathrm{Cl}(k)[2]| = 2^{t-1}$.

Denote by $[\mathfrak{a}]_+$ and $[\mathfrak{a}]$ the narrow ideal class and ordinary class, respectively, containing the ideal $\mathfrak{a}$. As is well known, $\mathrm{Cl}^+(k)[2] = \langle [\mathfrak{p}_1]_+, \ldots, [\mathfrak{p}_t]_+ \rangle$, but its 2-rank is $t - 1$, since there is exactly one nontrivial relation among these classes; namely, since $N\varepsilon = +1$, Hilbert's theorem 90 implies that

$$1 = [(1 + \varepsilon)]_+ = [\mathfrak{p}_1^{e_1}]_+ \cdots [\mathfrak{p}_t^{e_t}]_+$$

for some $e_j \in \{0, 1\}$ with not all $e_j = 0$; cf. [4, Proposition 2.4 and its proof] and [5, Proposition 1]. But in the usual sense, $C := \langle [\mathfrak{p}_1], \ldots, [\mathfrak{p}_t] \rangle$ has 2-rank $t - 2$, since there is exactly one more relation among the ramified primes:

$$[\mathfrak{p}_1] \cdots [\mathfrak{p}_t] = [(\sqrt{d})] = 1.$$

(Notice that $[(\sqrt{d})]$ is the identity in $\mathrm{Cl}(k)$, but $[(\sqrt{d})]_+$ is nontrivial in $\mathrm{Cl}^+(k)$.)

Our goal is to find 'natural' ideals whose classes in the usual sense span the complement, $\mathrm{Cl}(k)[2] - C$; cf. [5, Theorem 2(b)]. To this end, we start by considering the set

$$\mathcal{S}^+ = \{c \in \mathrm{Cl}^+(k) : c^2 = [(\sqrt{d})]_+\}.$$

Observe that the classes in $\mathcal{S}^+$ are all of order four.

Proposition 2.1. *The cardinality of $\mathcal{S}^+$ is 2^{t-1}.*

https://doi.org/10.1017/S1446788715000270 Published online by Cambridge University Press

Proof. Notice that $\mathcal{S}^+$ is nonempty by [4, Proposition 2.12] or, more directly, since $d = a^2 + b^2$ as above, the ideal $\mathfrak{a}^2 = (a, b + \sqrt{d}\,)^2 = (b + \sqrt{d}\,)$ and since $N(b + \sqrt{d}\,) = -a^2 < 0$, $[\mathfrak{a}]_+^2 = [(\sqrt{d}\,)]_+$. We now claim that there is a bijection between $\mathcal{S}^+$ and $\mathrm{Cl}^+(k)[2]$. For, let c_0 be a fixed class in $\mathcal{S}^+$. Then consider the map on $\mathcal{S}^+$ given by $c \mapsto c_0 c$ for all c in $\mathcal{S}^+$. But $(c_0 c)^2 = 1$ and thus $c_0 c$ is an ambiguous ideal class, whence generated by an ambiguous ideal (cf. [4, Proposition 2.9]), which therefore is a product of a principal ideal generated by a rational number with a product of ramified primes. Hence, $c_0 c = c'$ for some $c' \in \mathrm{Cl}^+(k)[2]$. It is easy to see that this mapping is bijective from $\mathcal{S}^+$ onto $\mathrm{Cl}^+(k)[2]$. Since we know that $|\mathrm{Cl}^+(k)[2]| = 2^{t-1}$, we are done. □

Next, we look for a natural set of ideals whose classes make up $\mathcal{S}^+$. Let $\mathcal{A}$ be the set of ideals $\mathfrak{a} = (a, b + \sqrt{d}\,)$, where a, b range over all integers with $a > 0$ such that $d = a^2 + b^2$. Notice that the cardinality of $\mathcal{A}$ is 2^t. We are now interested in the cardinality of $\mathcal{A}^+ = \{[\mathfrak{a}]_+ : \mathfrak{a} \in \mathcal{A}\}$ and $\mathcal{A}^o = \{[\mathfrak{a}] : \mathfrak{a} \in \mathcal{A}\}$. We will see that $|\mathcal{A}^+| = 2^{t-1}$ and $|\mathcal{A}^o| = 2^{t-2}$ and that each class in $\mathcal{A}^+$ contains exactly two ideals in $\mathcal{A}$ and each class in $\mathcal{A}^o$ contains exactly four ideals in $\mathcal{A}$.

Let us state part of all this as a proposition.

Proposition 2.2. *The cardinality* $|\mathcal{A}^+| \le 2^{t-1}$.

Proof. By the proof of Proposition 2.1, we see that $\mathcal{A}^+ \subseteq \mathcal{S}^+$ and so the result follows from Proposition 2.1. □

One of our main results is the following theorem.

Theorem 2.3. *The cardinality* $|\mathcal{A}^+| = 2^{t-1}$. *Therefore,* $\mathcal{A}^+ = \mathcal{S}^+$. *Moreover, each class in* $\mathcal{A}^+$ *contains exactly two distinct ideals in* $\mathcal{A}$.

The proof involves converting the narrow ideal classes to cycles of reduced quadratic forms and showing that each form corresponding to an ideal in $\mathcal{A}$ lies in a cycle containing exactly one other form corresponding to another ideal in $\mathcal{A}$; refer to [1, Ch. 5]. We give this correspondence explicitly only for ideals in $\mathcal{A}$; again cf. [1] for a full description. Recall that in particular if $\mathfrak{a} = (a, b + \sqrt{d}\,)$, with positive integers a, b such that $d = a^2 + b^2$, then the corresponding quadratic form is given by

$$\frac{N(ax + (b + \sqrt{d}\,)y)}{N\mathfrak{a}} = \frac{a^2x^2 + 2abxy + (b^2 - d)y^2}{a} = ax^2 + 2bxy - ay^2 = (a, 2b, -a),$$

for brevity. For the conjugate ideal $\mathfrak{a}' = (a, b - \sqrt{d}\,)$, the corresponding form is $(-a, 2b, a)$.

Now, recall that two quadratic forms $f(x, y)$ and $g(x, y)$ are properly equivalent if there exists a matrix

$$\begin{pmatrix} m & n \\ u & v \end{pmatrix}$$

with integral entries and determinant 1 such that $f(mx + ny, ux + vy) = g(x, y)$. It is then well known that two forms are properly equivalent if and only if they correspond

https://doi.org/10.1017/S1446788715000270 Published online by Cambridge University Press

to ideals in the same narrow ideal class. Each narrow ideal class corresponds to a unique cycle of reduced forms and conversely. A form (a, b, c) of positive discriminant $D = b^2 - 4ac$ is defined to be reduced if $|\sqrt{D} - 2|a|| < b < \sqrt{D}$. We also define the following reduction algorithm ϱ on a form (a, b, c) with positive discriminant D:

$$\varrho(a, b, c) = \left(c, r(-b, c), \frac{r(-b, c)^2 - D}{4c}\right),$$

where, for integers u, v, $v \neq 0$, $r(u, v)$ is the unique integer r such that $r \equiv u \bmod 2v$ and $-|v| < r \leq |v|$ if $|v| > \sqrt{D}$, and $\sqrt{D} - 2|v| < r < \sqrt{D}$ if $|v| < \sqrt{D}$. Observe that $r(u, v)$ is an even function of the second argument. (Notice, too, that if we know two of the coefficients of a reduced form and its discriminant, then we know the form completely. We will sometimes denote the missing coefficient by $*$.)

Recall that this algorithm produces a reduced form in finitely many steps and that once a reduced form is obtained then the algorithm cycles through a finite set of reduced forms of even order and moreover all reduced forms fall into one of a finite set of disjoint cycles. If (a, b, c) is a reduced form, then $\varrho(a, b, c)$ is given explicitly as $\varrho(a, b, c) = (c, r(-b, c), (r^2 - D)/(4c))$ with

$$r = r(-b, c) = -b + 2|c|\left\lfloor \frac{b + \sqrt{D}}{2|c|} \right\rfloor,$$

where $\lfloor x \rfloor$ denotes the integral part of the real number x.

We now go back to the forms $(\pm a, 2b, \mp a)$. Notice that their discriminant is $D = 4(b^2 + a^2) = 4d$. First we note the following result.

Proposition 2.4. *Suppose that $D = 4(a^2 + b^2)$ with $a, b > 0$. Then the forms $(\pm a, 2b, \mp a)$ are all reduced.*

Proof. Observe that $(\pm a, 2b, \mp a)$ is reduced if and only if $|\sqrt{D} - 2a| < 2b < \sqrt{D}$. The latter inequality is clearly valid since $4b^2 < 4a^2 + 4b^2 = D$. On the other hand, $|\sqrt{D} - 2a| < 2b$ if and only if $(\sqrt{D} - 2a)^2 < 4b^2$ if and only if $D + 4a^2 - 4a\sqrt{D} < 4b^2$ if and only if $8a^2 + 4b^2 - 4a\sqrt{D} < 4b^2$ if and only if $8a^2 - 4a\sqrt{D} < 0$ if and only if $2a - \sqrt{D} < 0$ if and only if $2a < \sqrt{D}$ if and only if $4a^2 < D = 4a^2 + 4b^2$ if and only if $0 < 4b^2$, this last of which is certainly true. □

For use below, notice that if (a, b, c) is reduced, then a and c are of opposite sign and, as we already know, b is positive.

The following is a general useful result about certain cycles of reduced forms.

Proposition 2.5. *Let (a_0, b_0, c_0) be a reduced form with positive discriminant and let $\varrho^j(a_0, b_0, c_0) = (a_j, b_j, c_j)$ for any integer j with cycle length $2n$, that is, $(a_j, b_j, c_j) = (a_i, b_i, c_i)$ if and only if $j \equiv i \bmod 2n$. Suppose further that $a_0 = -c_0$. Then*

$$(a_{-j}, b_{-j}, c_{-j}) = (-c_j, b_j, -a_j).$$

Moreover, the form (a_n, b_n, c_n) satisfies the property $a_n = -c_n$.

https://doi.org/10.1017/S1446788715000270 Published online by Cambridge University Press

Proof. By the proof of [1, Proposition 5.6.6], we have for any reduced form (a, b, c)

$$\varrho^{-1}(a, b, c) = \left(\frac{r(-b, a)^2 - D}{4a}, r(-b, a), a\right),$$

with

$$r(-b, a) = -b + 2|a|\left\lfloor \frac{b + \sqrt{D}}{2|a|} \right\rfloor.$$

Here ϱ is interpreted as a bijection on any cycle and hence ϱ^{-1} is well defined on cycles. We show that

$$(a_{-j}, b_{-j}, c_{-j}) = (-c_j, b_j, -a_j)$$

by induction on j. Notice that the result holds for $j = 0$, since $a_0 = -c_0$. Now assume that

$$(a_{-j}, b_{-j}, c_{-j}) = (-c_j, b_j, -a_j)$$

holds. We then need to show that

$$(a_{-j-1}, b_{-j-1}, c_{-j-1}) = (-c_{j+1}, b_{j+1}, -a_{j+1}).$$

To this end,

$$(a_{-j-1}, b_{-j-1}, c_{-j-1}) = \varrho^{-1}(a_{-j}, b_{-j}, c_{-j}) = (*, r(-b_{-j}, a_{-j}), a_{-j}) = (*, r(-b_j, -c_j), -c_j).$$

On the other hand,

$$(a_{j+1}, b_{j+1}, c_{j+1}) = \varrho(a_j, b_j, c_j) = (c_j, r(-b_j, c_j), *).$$

Comparing coefficients, we see that $a_{j+1} = c_j = -a_{-j} = -c_{-j-1}$ and $b_{j+1} = r(-b_j, c_j) = r(-b_j, -c_j) = b_{-j-1}$. These two equalities force $c_{j+1} = -a_{-j-1}$, as desired.

Now apply this result when $j = n$. Then

$$(a_n, b_n, c_n) = (a_{-n}, b_{-n}, c_{-n}) = (-c_n, b_n, -a_n)$$

and therefore $a_n = -c_n$. □

Now we show that there are at most two forms $(a_j, b_j, -a_j)$ in any cycle.

Proposition 2.6. *Let (a_0, b_0, c_0) be a reduced form with positive discriminant and let $\varrho^j(a_0, b_0, c_0) = (a_j, b_j, c_j)$ for any integer j with cycle length $2n$ and suppose that $a_0 = -c_0$. If (a_ℓ, b_ℓ, c_ℓ) satisfies $c_\ell = -a_\ell$, then $\ell \equiv 0 \bmod n$.*

Proof. Suppose for the sake of argument that there is an ℓ where $0 < \ell < n$ such that (a_ℓ, b_ℓ, c_ℓ) with $c_\ell = -a_\ell$. Then, by Proposition 2.5 (with (a_ℓ, b_ℓ, c_ℓ) replacing (a_0, b_0, c_0)),

$$(a_{\ell-j}, b_{\ell-j}, c_{\ell-j}) = (-c_{\ell+j}, b_{\ell+j}, -a_{\ell+j})$$

for all j. In particular, for $j = \ell$,

$$(a_0, b_0, c_0) = (-c_{2\ell}, b_{2\ell}, -a_{2\ell}).$$

Hence, $c_{2\ell} = -a_0$, $b_{2\ell} = b_0$ and $a_{2\ell} = -c_0$. Therefore, $(a_{2\ell}, b_{2\ell}, c_{2\ell}) = (-c_0, b_0, -a_0) = (a_0, b_0, c_0)$, which contradicts the fact that our cycle length is $2n$. □

https://doi.org/10.1017/S1446788715000270 Published online by Cambridge University Press

This completes the proof of Theorem 2.3; for each $\mathfrak{a} \in \mathcal{A}$, the class $[\mathfrak{a}]_+$ contains exactly one other ideal in $\mathcal{A}$, whence it follows that $\mathcal{A}^+$ is half as large as $\mathcal{A}$.

Now we have the following corollary to the theorem.

COROLLARY 2.7. *The cardinality of $\mathcal{A}^o$ is 2^{t-2}, in which each ordinary ideal class contains exactly four ideals of $\mathcal{A}$. Moreover,* $\mathrm{Cl}(k)[2] - C = \mathcal{A}^o$.

PROOF. The first statement is clear, as any ordinary ideal class of $\mathcal{A}^o$ is a union of two disjoint narrow classes in $\mathcal{A}^+$, namely, $[\mathfrak{a}] = [\mathfrak{a}]_+ \cup [\mathfrak{a}(\sqrt{d})]_+$.

For the last statement, notice that since $\mathcal{A}^o \subseteq \mathrm{Cl}(k)[2]$, we need only show that $\mathcal{A}^o$ and C are disjoint. But this is easy, for since $\mathrm{Cl}(k) \simeq \mathrm{Cl}^+(k)/\langle[(\sqrt{d})]_+\rangle$ we see that if $[\mathfrak{a}] \in \mathcal{A}^o \cap C$ with $\mathfrak{a} \in \mathcal{A}$, then $[\mathfrak{a}] = [\mathfrak{b}]$ for some product of ramified primes $\mathfrak{b}$. But, by the isomorphism above, this ideal class equality translates to

$$\{[\mathfrak{a}]_+, [\mathfrak{a}(\sqrt{d})]_+\} = \{[\mathfrak{b}]_+, [\mathfrak{b}(\sqrt{d})]_+\}.$$

In particular, since the narrow ideal classes in the right-hand set are each of order two, we conclude that $[\mathfrak{a}]_+$ is of order two, contradicting the fact that the elements of $\mathcal{A}^+$ are all of order four. □

REMARKS. The results and proofs in this section remain valid (with some minor modifications) when generalized in *two directions*: for any real quadratic number field k whose discriminant d_k is a sum of two squares but of *arbitrary parity* and whose fundamental unit ε_k has norm of *arbitrary sign*.

Suppose first that $d = d_k$ is odd, say $d = p_1 \cdots p_t$ for primes $p_j \equiv 1 \bmod 4$, and with $N\varepsilon_k = +1$. The only modification in the above presentation is in the definition of the set of ideals $\mathcal{A}$ just after Proposition 2.1, where we now assume that a is odd and b even. In the proof of Theorem 2.3, the correspondence between ideal classes and classes of forms remains the same, but the forms now have discriminant $4d_k$. However, the Sylow 2-subgroups of the groups of classes of forms (ideals) of discriminant d_k and $4d_k$ are all isomorphic and therefore no change in the proof is necessary. In this situation, we get a slightly stronger result than in [5], since we are considering narrow rather than ordinary equivalence. See the second example in the following section.

When $N\varepsilon_k = -1$, the results and proofs still hold. In fact, $\mathcal{S}^+ = \mathcal{A}^+$ and each still has 2^{t-1} elements; but in this case

$$\mathcal{S}^+ = \mathrm{Cl}^+(k)[2] = \mathrm{Cl}(k)[2].$$

From this it is easy to see that precisely two ideals $\mathfrak{a}$ and $\mathfrak{a}'$ in $\mathcal{A}$ are equivalent to an ideal $\mathfrak{b}$ which is a product of ramified primes, since the $[\mathfrak{b}]$ generate $\mathrm{Cl}(k)[2]$ in this case.

3. Two examples

We now give an example illustrating the results above. We then revisit the example in [5].

https://doi.org/10.1017/S1446788715000270 Published online by Cambridge University Press

Example 3.1. Consider $d = 2 \cdot 5 \cdot 41 = 410$ and let $k = \mathbb{Q}(\sqrt{410})$. The fundamental unit $\varepsilon = 81 + 4\sqrt{410}$ has norm $= +1$. Let $\mathfrak{p}_2, \mathfrak{p}_5, \mathfrak{p}_{41}$ be (all the ramified) primes above $2, 5, 41$, respectively. Since

$$1 + \varepsilon = 82 + 4\sqrt{410} = 2(41 + 2\sqrt{410})$$

and $N(41 + 2\sqrt{410}) = +41$,

$$\mathfrak{p}_{41} = (41 + 2\sqrt{410}) \overset{+}{\sim} 1,$$

where $\overset{+}{\sim}$ denotes narrow equivalence and $\sim$ will mean ordinary equivalence below. Hence,

$$\mathrm{Cl}^+(k)[2] = \langle [\mathfrak{p}_2]_+, [\mathfrak{p}_5]_+ \rangle,$$

which has order four.

On the other hand, since $(\sqrt{410}) = \mathfrak{p}_2\mathfrak{p}_5\mathfrak{p}_{41} \overset{+}{\sim} \mathfrak{p}_2\mathfrak{p}_5$, we see that $[\mathfrak{p}_2] = [\mathfrak{p}_5]$. Hence, $C = \langle [\mathfrak{p}_2] \rangle$ has order two, which is of index two in $\mathrm{Cl}(k)[2]$. To generate the rest of $\mathrm{Cl}(k)[2]$, we consider the set of ideals $\mathcal{A}$ as follows: notice that 410 is a sum of two squares in essentially two ways, $410 = 11^2 + 17^2 = 7^2 + 19^2$, in which case $\mathcal{A} = \{\mathfrak{a}_1, \mathfrak{a}_2, \mathfrak{a}_3, \mathfrak{a}_4, \mathfrak{a}_1', \mathfrak{a}_2', \mathfrak{a}_3', \mathfrak{a}_4'\}$, where

$$\mathfrak{a}_1 = (11, 17 + \sqrt{410}), \quad \mathfrak{a}_2 = (7, 19 + \sqrt{410}),$$
$$\mathfrak{a}_3 = (17, 11 + \sqrt{410}), \quad \mathfrak{a}_4 = (19, 7 + \sqrt{410}),$$

and the rest the corresponding conjugate ideals. To see which ideals in $\mathcal{A}$ are equivalent in the narrow sense, we calculate the cycle of reduced forms corresponding to these ideals:

$$\begin{aligned}
\mathfrak{a}_1 \leftrightarrow\ & ((11, 34, -11), (-11, 32, 14), (14, 24, -19), \\
& (-19, 14, 19), (19, 24, -14), (-14, 32, 11)), \\
\mathfrak{a}_2 \leftrightarrow\ & ((7, 38, -7), (-7, 32, 22), (-22, 12, -17), \\
& (-17, 22, 17), (17, 12, -22), (-22, 32, 7)), \\
\mathfrak{a}_3 \leftrightarrow\ & ((17, 22, -17), (-17, 12, 22), (22, 32, -7), \\
& (-7, 38, 7), (7, 32, -22), (-22, 12, 17)), \\
\mathfrak{a}_4 \leftrightarrow\ & ((19, 14, -19), (-19, 24, 14), (14, 32, -11), \\
& (-11, 34, 11), (11, 32, -14), (-14, 24, 19));
\end{aligned}$$

the cycles for the conjugates are obtained by switching the signs on the outer coefficients. From this,

$$\mathfrak{a}_1 \overset{+}{\sim} \mathfrak{a}_4', \quad \mathfrak{a}_2 \overset{+}{\sim} \mathfrak{a}_3', \quad \mathfrak{a}_3 \overset{+}{\sim} \mathfrak{a}_2', \quad \mathfrak{a}_4 \overset{+}{\sim} \mathfrak{a}_1'.$$

Therefore, $\mathcal{A}^+ = \{[\mathfrak{a}_1]_+, [\mathfrak{a}_2]_+, [\mathfrak{a}_3]_+, [\mathfrak{a}_4]_+\}$. On the other hand, notice that

$$\mathfrak{a}_1 \sim \mathfrak{a}_4' \sim \mathfrak{a}_4 \sim \mathfrak{a}_1', \quad \mathfrak{a}_2 \sim \mathfrak{a}_3' \sim \mathfrak{a}_3 \sim \mathfrak{a}_2',$$

in which case $\mathcal{A}^o = \{[\mathfrak{a}_1], [\mathfrak{a}_2]\}$.

Therefore,

$$\mathrm{Cl}(k)[2] = \{[(1)], [\mathfrak{p}_2], [\mathfrak{a}_1], [\mathfrak{a}_2]\}.$$

https://doi.org/10.1017/S1446788715000270 Published online by Cambridge University Press

Example 3.2. Now consider $d = 5 \cdot 13 \cdot 29 = 1885$; cf. [5]. Let $k = \mathbb{Q}(\sqrt{1885})$ and so $d = d_k$. Then $\mathcal{A} = \{\mathfrak{a}_1, \mathfrak{a}_2, \mathfrak{a}_3, \mathfrak{a}_4, \mathfrak{a}_1', \mathfrak{a}_2', \mathfrak{a}_3', \mathfrak{a}_4'\}$, where $\mathfrak{a}_1 = (43, 6 + \sqrt{1885})$, $\mathfrak{a}_2 = (11, 42 + \sqrt{1885})$, $\mathfrak{a}_3 = (21, 38 + \sqrt{1885})$, $\mathfrak{a}_4 = (27, 34 + \sqrt{1885})$. We calculate the cycle of reduced forms corresponding to a couple of these ideals:

$$\begin{aligned}\mathfrak{a}_1 \leftrightarrow\ & ((43, 12, -43), (-43, 74, 12), (12, 70, -55), (-55, 40, 27),\\ & (27, 68, -27), (-27, 40, 55), (55, 70, -12), (-12, 74, 43)),\\ \mathfrak{a}_2 \leftrightarrow\ & ((11, 84, -11), (-11, 70, 60), (60, 50, -21),\\ & (-21, 76, 21), (21, 50, -60), (-60, 70, 11)).\end{aligned}$$

From this, we get the following narrow equivalence among the ideals of $\mathcal{A}$:

$$\mathfrak{a}_1 \overset{+}{\sim} \mathfrak{a}_4, \quad \mathfrak{a}_2 \overset{+}{\sim} \mathfrak{a}_3', \quad \mathfrak{a}_3 \overset{+}{\sim} \mathfrak{a}_2', \quad \mathfrak{a}_1' \overset{+}{\sim} \mathfrak{a}_4'.$$

Notice that we need the conjugates of the $\mathfrak{a}_j$ in order to cover all of $\mathcal{S}^+$ as the $\mathfrak{a}_j$ are by themselves insufficient for this purpose.

4. A related result

We now consider a slightly different but related phenomenon. In the above examples we discovered which of the ideals $\mathfrak{a}_j$ and $\mathfrak{a}_j'$ $(j = 1, \dots, 4)$ are narrowly equivalent by considering cycles of reduced quadratic forms. But it turns out that there is another way to check when these ideals are equivalent, which we now discuss.

As before, let $d = p_1 \cdots p_t$, $p_1 = 2$, $p_j \equiv 1 \bmod 4$ $(j = 2, \dots, t)$. (The following arguments remain valid in the case of odd discriminant d, the details of which we leave to the reader.) Let

$$A = \{a + bi : a, b \in \mathbb{Z}, a^2 + b^2 = d\}.$$

Then $|A| = 2^{t+1}$, as is well known. Now, let $\pi_1 = 1 + i$ and, for $j > 1$, let $\pi_j = x_j + y_j i$, where $x_j, y_j \in \mathbb{N}$, y_j even, such that $p_j = x_j^2 + y_j^2$. Let τ be complex conjugation. For each $\underline{\nu} = (\nu_0; \nu_1, \dots, \nu_t) \in \mathbb{F}_2^{t+1}$, where $\mathbb{F}_2$ is a two-element field, let

$$\Pi_{\underline{\nu}} = (-1)^{\nu_0} \pi_1^{\tau^{\nu_1}} \cdots \pi_t^{\tau^{\nu_t}}$$

and so $\Pi_{\underline{\nu}}$ ranges over plus/minus all products of the π_j or $\overline{\pi}_j$. There are thus 2^{t+1} of the $\Pi_{\underline{\nu}}$. Notice that $N\Pi_{\underline{\nu}} = d$. Hence,

$$\{\Pi_{\underline{\nu}} : \underline{\nu} \in \mathbb{F}_2^{t+1}\} = A.$$

We thus have a bijection

$$\eta : A \longrightarrow \mathbb{F}_2^{t+1}$$

given by $a + bi \mapsto \underline{\nu} = (\nu_0; \nu_1, \dots, \nu_t)$, where $a + bi = \Pi_{\underline{\nu}}$.

Now let

$$A^+ = \{a + bi : a \in \mathbb{N}, b \in \mathbb{Z}, a^2 + b^2 = d\},$$

https://doi.org/10.1017/S1446788715000270 Published online by Cambridge University Press

and recall that

$$\mathcal{A} = \{\mathfrak{a} = (a, b + \sqrt{d}\,) : a, b \in \mathbb{Z}, a > 0, a^2 + b^2 = d\},$$

both sets of which have 2^t elements. There is a convenient bijection

$$\varphi : \mathcal{A} \longrightarrow A^+$$

given by $\mathfrak{a} = (a, b + \sqrt{d}) \mapsto a + bi$.

Finally, we get a bijection

$$\psi : \mathcal{A} \longrightarrow \mathbb{F}_2^t$$

given by the composite map

$$\mathcal{A} \xrightarrow{\varphi} A^+ \xrightarrow{\eta|_{A^+}} \mathbb{F}_2^{t+1} \xrightarrow{p} \mathbb{F}_2^t,$$

where $p(\nu_0; \nu_1, \ldots, \nu_t) = (\nu_1, \ldots, \nu_t)$. In brief,

$$\psi(\mathfrak{a}) = (\nu_1, \ldots, \nu_t),$$

where $a + bi = \Pi_{\underline{\nu}}$, with $\underline{\nu} = (\nu_0; \nu_1, \ldots, \nu_t)$. (Notice that the map

$$p \circ \eta|_{A^+} : A^+ \longrightarrow \mathbb{F}_2^t$$

is a bijection.)

Assume now that the fundamental unit has positive norm. In $\mathbb{F}_2^t$, let U be the $\mathbb{F}_2$-subspace generated by $(e_1, \ldots, e_t)$, where $\mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_t^{e_t} \overset{+}{\sim} 1$, for $e_j \in \mathbb{F}_2$, not all the $e_j = 0$ (as above). Hence,

$$U = \{(0, \ldots, 0), (e_1, \ldots, e_t)\}.$$

Given all of this, we have the following proposition.

Proposition 4.1. *For any* $\mathfrak{a}, \mathfrak{b} \in \mathcal{A}$,

$$\mathfrak{a} \overset{+}{\sim} \mathfrak{b} \quad \textit{if and only if } \psi(\mathfrak{a}) - \psi(\mathfrak{b}) \in U.$$

This proposition is an immediate consequence of the following theorem.

Theorem 4.2. *Let* $\mathfrak{a}_1, \mathfrak{a}_2 \in \mathcal{A}$ *and suppose that* $\psi(\mathfrak{a}_1) = (\mu_1, \ldots, \mu_t)$ *and* $\psi(\mathfrak{a}_2) = (\nu_1, \ldots, \nu_t)$. *Then*

$$\mathfrak{a}_1 \mathfrak{a}_2 \overset{+}{\sim} \prod_{\ell=1}^{t} \mathfrak{p}_\ell^{\mu_\ell + \nu_\ell + 1}.$$

Before proving these two results, let us see how this all plays out in our first example above.

Recall that $d = 410 = p_1 p_2 p_3$, with $p_1 = 2, p_2 = 5, p_3 = 41$. (Hence, $t = 3$.) We have from the above

$$\pi_1 = 1 + i, \quad \pi_2 = 1 + 2i, \quad \pi_3 = 5 + 4i.$$

https://doi.org/10.1017/S1446788715000270 Published online by Cambridge University Press

From this, we obtain the relations

$$\Pi_{(0;0,0,0)} = \pi_1\pi_2\pi_3 = -17 + 11i, \quad \Pi_{(0;0,0,1)} = \pi_1\pi_2\overline{\pi}_3 = 7 + 19i,$$
$$\Pi_{(0;0,1,0)} = \pi_1\overline{\pi}_2\pi_3 = 19 + 7i, \quad \Pi_{(0;0,1,1)} = \pi_1\overline{\pi}_2\overline{\pi}_3 = 11 - 17i,$$
$$\Pi_{(0;1,0,0)} = \overline{\pi}_1\pi_2\pi_3 = 11 + 17i, \quad \Pi_{(0;1,0,1)} = \overline{\pi}_1\pi_2\overline{\pi}_3 = 19 - 7i,$$
$$\Pi_{(0;1,1,0)} = \overline{\pi}_1\overline{\pi}_2\pi_3 = 7 - 19i, \quad \Pi_{(0;1,1,1)} = \overline{\pi}_1\overline{\pi}_2\overline{\pi}_3 = -17 - 11i.$$

Notice that there are eight more relations involving the indices $(1; *, *, *)$, which are obtained by multiplying the corresponding relation above by -1, for example $\Pi_{(1;0,0,0)} = 17 - 11i$.

On the other hand, $\mathcal{A}$ consists of the following eight ideals:

$$\mathfrak{a}_1 = (11, 17 + \sqrt{410}), \quad \mathfrak{a}_1' = (11, -17 + \sqrt{410}),$$
$$\mathfrak{a}_2 = (7, 19 + \sqrt{410}), \quad \mathfrak{a}_2' = (7, -19 + \sqrt{410}),$$
$$\mathfrak{a}_3 = (17, 11 + \sqrt{410}), \quad \mathfrak{a}_3' = (17, -11 + \sqrt{410}),$$
$$\mathfrak{a}_4 = (19, 7 + \sqrt{410}), \quad \mathfrak{a}_4' = (19, -7 + \sqrt{410}).$$

Hence, $\varphi : \mathcal{A} \longrightarrow A^+$ is given by

$$\varphi(\mathfrak{a}_1) = 11 + 17i = \Pi_{(0;1,0,0)}, \quad \varphi(\mathfrak{a}_1') = 11 - 17i = \Pi_{(0;0,1,1)},$$
$$\varphi(\mathfrak{a}_2) = 7 + 19i = \Pi_{(0;0,0,1)}, \quad \varphi(\mathfrak{a}_2') = 7 - 19i = \Pi_{(0;1,1,0)},$$
$$\varphi(\mathfrak{a}_3) = 17 + 11i = \Pi_{(1;1,1,1)}, \quad \varphi(\mathfrak{a}_3') = 17 - 11i = \Pi_{(1;0,0,0)},$$
$$\varphi(\mathfrak{a}_4) = 19 + 7i = \Pi_{(0;0,1,0)}, \quad \varphi(\mathfrak{a}_4') = 19 - 7i = \Pi_{(0;1,0,1)},$$

whence the function ψ is given by

$$\psi(\mathfrak{a}_1) = (1, 0, 0), \quad \psi(\mathfrak{a}_1') = (0, 1, 1),$$
$$\psi(\mathfrak{a}_2) = (0, 0, 1), \quad \psi(\mathfrak{a}_2') = (1, 1, 0),$$
$$\psi(\mathfrak{a}_3) = (1, 1, 1), \quad \psi(\mathfrak{a}_3') = (0, 0, 0),$$
$$\psi(\mathfrak{a}_4) = (0, 1, 0,), \quad \psi(\mathfrak{a}_4') = (1, 0, 1).$$

Now, since $\mathfrak{p}_3 \overset{+}{\sim} 1$ ($\mathfrak{p}_3$ is $\mathfrak{p}_{41}$ in the example), we see that the subspace U in $\mathbb{F}_2^3$ is

$$U = \langle (0, 0, 1) \rangle = \{(0, 0, 0), (0, 0, 1)\}$$

and, therefore, $\mathbb{F}_2^3/U = \{U, (0, 1, 0) + U, (1, 0, 0) + U, (1, 1, 1) + U\}$, explicitly

$$(0, 1, 0) + U = \{(0, 1, 0), (0, 1, 1)\},$$
$$(1, 0, 0) + U = \{(1, 0, 0), (1, 0, 1)\},$$
$$(1, 1, 1) + U = \{(1, 1, 1), (1, 1, 0)\}.$$

By Proposition 4.1 and the above correspondence, we thus have the four narrow classes

$$[\mathfrak{a}_1]_+ = \{\mathfrak{a}_1, \mathfrak{a}_4'\}, \quad [\mathfrak{a}_2]_+ = \{\mathfrak{a}_2, \mathfrak{a}_3'\}, \quad [\mathfrak{a}_3]_+ = \{\mathfrak{a}_3, \mathfrak{a}_2'\}, \quad [\mathfrak{a}_4]_+ = \{\mathfrak{a}_4, \mathfrak{a}_1'\}.$$

Observe that this is consistent with the results in our example before.

Now we will prove the theorem.

https://doi.org/10.1017/S1446788715000270 Published online by Cambridge University Press

Proof. Let $\mathfrak{a}_j = (a_j, b_j + \sqrt{d}\,)$, where $a_j, b_j \in \mathbb{Z}, a_j > 0, a_j^2 + b_j^2 = d,\ j = 1, 2$. Notice that $N\mathfrak{a}_j = a_j$ and recall that $\mathfrak{a}_j^2 = (b_j + \sqrt{d}\,) \stackrel{+}{\sim} (\sqrt{d}\,)$. Hence, $(\mathfrak{a}_1\mathfrak{a}_2)^2 \stackrel{+}{\sim} 1$, which in turn implies that $\mathfrak{a}_1\mathfrak{a}_2$ is narrowly equivalent to an ambiguous ideal; call it $\mathfrak{a}$, that is, $\mathfrak{a}' = \mathfrak{a}$. By considering the proofs of [4, Propositions 2.9 and 2.4], we see that we may take $\mathfrak{a} = (1 + \lambda)\mathfrak{a}_1\mathfrak{a}_2$, where

$$\lambda = \frac{a_1 a_2}{(b_1 + \sqrt{d}\,)(b_2 + \sqrt{d}\,)}.$$

For, first observe that

$$(\lambda) = \frac{N(\mathfrak{a}_1\mathfrak{a}_2)}{\mathfrak{a}_1^2\mathfrak{a}_2^2}.$$

Next, notice that $\lambda\lambda' = 1$ and hence $1 + \lambda = (1 + \lambda')\lambda$. But then

$$\mathfrak{a}' = (1 + \lambda')\mathfrak{a}_1'\mathfrak{a}_2' = \frac{(1 + \lambda)}{(\lambda)}\frac{\mathfrak{a}_1'\mathfrak{a}_2'\mathfrak{a}_1\mathfrak{a}_2}{\mathfrak{a}_1\mathfrak{a}_2} = (1 + \lambda)\mathfrak{a}_1\mathfrak{a}_2 = \mathfrak{a},$$

as desired.

Now, as observed before, since $(1 + \lambda)\mathfrak{a}_1\mathfrak{a}_2$ is an ambiguous ideal,

$$(1 + \lambda)\mathfrak{a}_1\mathfrak{a}_2 = \mathfrak{b}(c)$$

for some $\mathfrak{b} \mid (\sqrt{d}\,)$ and $c \in \mathbb{Q}$. Hence, notice that $\mathfrak{a}_1\mathfrak{a}_2 \stackrel{+}{\sim} \mathfrak{b}$. Let $q = N\mathfrak{b}$. Then $q \mid d$ and q completely determines $\mathfrak{b}$ and so we need only compute q. From the above,

$$qc^2 = N(\mathfrak{b}(c)) = N((1 + \lambda)\mathfrak{a}_1\mathfrak{a}_2) = a_1 a_2 N(1 + \lambda).$$

Therefore, q is the square-free kernel of $a_1 a_2 N(1 + \lambda)$. A straightforward calculation shows that

$$a_1 a_2 N(1 + \lambda) = (a_1 + a_2)^2 + (b_1 + b_2)^2.$$

Now let $\alpha_j = a_j + b_j i$ for $j = 1, 2$. Then, by the definition of $\psi(\mathfrak{a}_j)$,

$$\alpha_1 = (-1)^{\mu_0}\prod_{\ell=1}^{t}\pi_\ell^{\tau^{\mu_\ell}} \quad \text{and} \quad \alpha_2 = (-1)^{\nu_0}\prod_{\ell=1}^{t}\pi_\ell^{\tau^{\nu_\ell}}.$$

Hence, $\alpha_1 + \alpha_2 = \varrho(\delta + (-1)^{\mu_0+\nu_0}\overline{\delta})$, where

$$\varrho = (-1)^{\mu_0}\prod_{\substack{\ell=1\\ \mu_\ell=\nu_\ell}}^{t}\pi_\ell^{\tau^{\mu_\ell}} \quad \text{and} \quad \delta = \prod_{\substack{\ell=1\\ \mu_\ell\neq\nu_\ell}}^{t}\pi_\ell^{\tau^{\mu_\ell}}.$$

But then

$$(\alpha_1 + \alpha_2)(\overline{\alpha}_1 + \overline{\alpha}_2) = |\alpha_1 + \alpha_2|^2 = |\varrho|^2|\delta + (-1)^{\mu_0+\nu_0}\overline{\delta}|^2 = \prod_{\substack{\ell=1\\ \mu_\ell=\nu_\ell}}^{t} p_\ell \cdot c^2,$$

https://doi.org/10.1017/S1446788715000270 Published online by Cambridge University Press

where $c \in \mathbb{Z}$. More precisely, c may be taken to be twice the real or imaginary part of δ. Thus,

$$q = \prod_{\substack{\ell=1 \\ \mu_\ell = \nu_\ell}}^{t} p_\ell.$$

This implies that

$$\mathfrak{b} = \prod_{\substack{\ell=1 \\ \mu_\ell = \nu_\ell}}^{t} \mathfrak{p}_\ell.$$

Therefore,

$$\mathfrak{a}_1\mathfrak{a}_2 \overset{+}{\sim} \mathfrak{b} = \prod_{\substack{\ell=1 \\ \mu_\ell = \nu_\ell}}^{t} \mathfrak{p}_\ell \overset{+}{\sim} \prod_{\ell=1}^{t} \mathfrak{p}_\ell^{\mu_\ell+\nu_\ell+1},$$

which completes the proof of the theorem. □

We now conclude with a proof of Proposition 4.1.

Proof. Let $\mathfrak{a}, \mathfrak{b} \in \mathcal{A}$ and let $\psi(\mathfrak{a}) = (\mu_1, \ldots, \mu_t)$ and $\psi(\mathfrak{b}) = (\nu_1, \ldots, \nu_t)$. We have the following chain of equivalences: $\mathfrak{a} \overset{+}{\sim} \mathfrak{b}$ if and only if $\mathfrak{a}\mathfrak{b}' \overset{+}{\sim} 1$. But then by Theorem 4.2 $\mathfrak{a}\mathfrak{b}' \overset{+}{\sim} 1$ if and only if $1 \overset{+}{\sim} \prod_{\ell=1}^{t} \mathfrak{p}_\ell^{\mu_\ell+\nu_\ell}$, since $\psi(\mathfrak{b}') = \underline{1} + \psi(\mathfrak{b})$. But $1 \overset{+}{\sim} \prod_{\ell=1}^{t} \mathfrak{p}_\ell^{\mu_\ell+\nu_\ell}$ if and only if $\prod_{\ell=1}^{t} \mathfrak{p}_\ell^{\mu_\ell+\nu_\ell} \in \{(1), \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_t^{e_t}\}$ if and only if $\psi(\mathfrak{a}) - \psi(\mathfrak{b}) = \psi(\mathfrak{a}) + \psi(\mathfrak{b}) \in U$, as desired. □

The proposition and theorem remain valid if $N\varepsilon_k = -1$, as the reader may verify.

References

[1] H. Cohen, *A Course in Computational Algebraic Number Theory* (Springer, New York, 1996).
[2] H. Cohn, *Advanced Number Theory* (Dover, New York, 1980).
[3] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, 4th edn (Oxford University Press, London, 1960).
[4] F. Lemmermeyer, *Reciprocity Laws* (Springer, New York, 2000).
[5] F. Lemmermeyer, 'Relations in the 2-class group of quadratic number fields', *J. Aust. Math. Soc.* **93** (2012), 115–120.

ELLIOT BENJAMIN, Department of Mathematics and Statistics,
University of Maine, Orono, ME 04469, USA
e-mail: ben496@prexar.com

C. SNYDER, Department of Mathematics and Statistics,
University of Maine, Orono, ME 04469, USA
e-mail: snyder@math.umaine.edu

https://doi.org/10.1017/S1446788715000270 Published online by Cambridge University Press