50. *Quadratic Irrationals, Ambiguous Classes and Symmetry in Real Quadratic Fields*

By R. A. MOLLIN

Department of Mathematics, University of Calgary, Canada

(Communicated by Shokichi IYANAGA, M. J. A., Sept. 12, 1994)

Abstract: It is the purpose of this paper to set down the relationship between symmetry in the continued fraction expansion of a quadratic irrational, and the number of ambiguous ideals in an associated class of the class group of a real quadratic field. We also clear up some misconceptions in the literature pertaining to ambiguous classes.

In what follows we will establish the equivalence between real quadratic irrationals (with what we call pure symmetric period), and ambiguous classes having at most one ambiguous ideal in the class group of a real quadratic field. Although this should be well known, it is not set down anywhere in the literature. Moreover, what *is* set down is often misleading or simply wrong. We will point out some of these inaccuracies and set them straight.

First we need some background and notation.

Let D be a positive square-free integer and set

$$\omega = (\sigma - 1 + \sqrt{D})/\sigma$$

where $\sigma = 2$ if $D \equiv 1 (mod\ 4)$ and $\sigma = 1$ otherwise. The *discriminant* Δ of the real quadratic field $K = Q(\sqrt{D})$ is given by $\Delta = (2/\sigma)^2 D$. If $[\alpha, \beta]$ denotes the module $\{\alpha x + \beta y : x, y \in \boldsymbol{Z}\}$ then the *maximal order* (or ring of integers) O_Δ of K is $[1, \omega]$. The *norm* $N(\alpha)$ of $\alpha \in K$ is equal to $\alpha\alpha'$ where α' is the *algebraic conjugate* of α. The class group of K is denoted by C_Δ.

An ideal of O_Δ can be written as $I = [a, b + c\omega]$ where $a, b, c \in \boldsymbol{Z}$ with $a, c > 0$, $c \mid b$, $c \mid a$, and $ac \mid N(b + c\omega)$. Conversely, if $a, b, c \in \boldsymbol{Z}$ with $c \mid b$, $c \mid a$ and $ac \mid N(b + c\omega)$ then $[a, b + c\omega]$ is an ideal of O_Δ. In an ideal $I = [a, b + c\omega]$ with $a, c > 0$ the *norm of the ideal* I, $N(I)$ is given by $N(I) = ac > 0$. If $c = 1$ then I is said to be a *primitive* ideal. The *conjugate ideal* of $I = [a, b + \omega]$ is $I' = [a, b + \omega']$. An ideal I is called *reduced* if it is primitive and does not contain any non-zero element α such that both $|\alpha| < N(I)$, and $|\alpha'| < N(I)$. The class of an ideal I in O_Δ is denoted by $\{I\}$. For further details on the above, the reader is referred to [7].

At this juncture, we introduce continued fractions into the discussion. Given a *quadratic irrational* $\gamma \in K$ we may write $\gamma = (P + \sqrt{D})/Q$ where P, $Q \in \boldsymbol{Z}$ with $Q \neq 0$, and Q divides $N(P + \sqrt{D})$. Furthermore,

$$\gamma = \langle q_0, q_1, \ldots, q_i, \gamma_{i+1} \rangle$$

denotes the *continued fraction expansion* of γ where

$$\gamma_{i+1} = (P_{i+1} + \sqrt{D})/Q_{i+1}$$

and

$$q_i = \lfloor \gamma_i \rfloor,$$
$$P_{i+1} = q_i Q_i - P_i,$$
$$Q_{i+1} = (D - P_{i+1}^2)/Q_i,$$

for $i = 0,1,2,\ldots$

Every such γ is known to be *eventually periodic*; i.e.,

$$\gamma = \langle q_0, q_1, \ldots, q_{i-1}, \overline{q_i, q_{i+1}, \ldots, q_{l-1}} \rangle.$$

Furthermore, if γ is *reduced*; i.e., $\gamma > 1$ and $-1 < \gamma' < 0$, then γ is *purely periodic*; i.e.,

$$\gamma = \langle \overline{q_0, q_1, \ldots, q_{l-1}} \rangle$$

of *period length* l. For further details on quadratic irrationals, the reader is referred to [6, section 10.4, pp. 374-390].

Now we establish the beautiful connection between the ideal theory and the theory of continued fractions. For proofs and further details the reader is referred to [7].

Definition 1. To each quadratic irrational $\gamma = (P + \sqrt{D})/Q$ there corresponds the O_Δ-ideal $I = [Q/\sigma, (P + \sqrt{D})/\sigma]$ which we denote by $[\gamma] = I$.

As a result of Definition 1, we say that γ *is reduced* if $[\gamma]$ is reduced, and we denote the period length of the continued fraction expansion of γ by $l(\gamma)$. Furthermore, the ideals $[\gamma_i] = (Q_i/\sigma, (P_i + \sqrt{D})/\sigma]$ for $0 \leq i \leq l - 1$ (where $l = l(\gamma)$) are *all* the reduced ideals equivalent to $[\gamma] = [\gamma_0]$ where $P = P_0$ and $Q = Q_0$. Also, since $l(\gamma_i) = l(\gamma)$ for all i with $0 \leq i \leq l$ then we denote this common period by $l(\mathscr{C})$ where $\mathscr{C}$ is the class of C_Δ containing $[\gamma]$.

Definition 2. If $\gamma = (P = \sqrt{D})/Q$ is a reduced quadratic irrational then γ is said to have a purely periodic continued fraction expansion with symmetry or we simply say that γ has *pure symmetric period* if

$$\gamma = \langle \overline{q_0, q_1, \ldots, q_{l-1}} \rangle$$

where the word $q_0 q_1 \cdots q_{l-1}$ is a palindrome.

Now we prove a useful technical result which will allow us to establish the equivalence between pure symmetry and certain ambiguous ideal classes.

Lemma 1. *Let $\mathscr{C}$ be an ambiguous class of reduced ideals in O_Δ, then $\mathscr{C}$ has at most one ambiguous ideal in it if and only if there exists a reduced ideal $I \in \mathscr{C}$ with $I' = I_{l-1}$ where $l = l(\mathscr{C})$.*

Proof. If there is an ideal $I \in \mathscr{C}$ with $I' = I_{l-1}$ then $D = P_0^2 + Q_0^2 = P_l^2 + Q_l^2$ where $I = [Q_0/\sigma, (P_0 + \sqrt{D})/\sigma]$. If there are 2 ambiguous ideals in $\mathscr{C}$ (the most possible in any ambiguous class of reduced ideals) then, by Theorem 3.4 of [5], l is even and both Q_0/σ and $Q_{l/2}/\sigma$ divide Δ. Moreover, Q_0/σ is square-free, being the norm of reduced ambiguous ideal. Since $\Delta = 4D/\sigma^2 = (2P_0/\sigma)^2 + (2Q_0/\sigma)^2$ then, if Q_0/σ indeed divides Δ, then $(Q_0/\sigma)^2$ divides Δ forcing $Q_0/\sigma = 1$ or 2. If $Q_0/\sigma = 1$ then $D = (2P_0/\sigma)^2 + 4$ forcing $l = 1$, a contradiction. If $Q_0/\sigma = 2$ then 4 divides Δ forcing $\sigma = 1$, but then $D = 4P_0^2 + 16$, a contradiction.

Conversely, assume that $\mathscr{C}$ has at most one ambiguous ideal in it. If

there are no ambiguous ideals in $\mathscr{C}$ then the result follows from Lemmas 3.3-3.4 of [5]. If $\mathscr{C}$ has exactly one ambiguous ideal in it then, by Theorems 3.1 and 3.4 of [5], l must be odd. Hence, $Q_{(l-1)/2} = Q_{(l+1)/2}$. Set $I = [Q_{(l+1)/2}/\sigma, (P_{(l+1)/2} + \sqrt{D})/\sigma]$ then $D = P^2_{(l+1)/2} + Q^2_{(l+1)/2}$ and the result follows from Lemma 3.3 of [5].

Now we establish the aforementioned equivalence.

Theorem 1. *Let $\mathscr{C}$ be a class of reduced ideals in O_Δ, then the following are equivalent.*

(1) *There exists a reduced quadratic irrational γ with pure symmetric period such that $[\gamma] \in \mathscr{C}$.*

(2) *There exists a reduced quadratic irrational γ such that $\gamma\gamma' = -1$ and $[\gamma] \in \mathscr{C}$.*

(3) *$\mathscr{C}$ is an ambiguous class containing at most one ambiguous ideal.*

Proof. By Hasse [3], if $\gamma = \overline{\langle q_0, q_1, \ldots, q_{l-1}\rangle}$. then

$$-1/\gamma' = \overline{\langle q_{l-1}, q_{l-2}, \ldots, q_0\rangle};$$

whence, we have the equivalence of (1) and (2).

If (2) holds then let $I = [\gamma] = [Q_0/\sigma, (P_0 + \sqrt{D})/\sigma]$. Thus,

$$D = P^2 + Q^2 = P_0^2 + Q_0^2 = P_l^2 + Q_l^2.$$

However, $D = P_l^2 + Q_l Q_{l-1}$. Therefore, $Q_{l-1} = Q_l = Q_0$. Moreover, by [7, Lemma 6.1, p. 418] we have that $q_{l-1} = \lfloor (P_{l-1} + \sqrt{D})/Q_{l-1} \rfloor = \lfloor (P_l + \sqrt{D})/Q_{l-1} \rfloor = \lfloor (P_0 + \sqrt{D})/Q_0 \rfloor = q_0$; whence, $P_l = q_{l-1}Q_{l-1} - P_{l-1} = q_0 Q_0 - P_{l-1} = P_0$; whence, $P_1 = P_{l-1}$. Since $I' = [Q_0/\sigma, (P_1 + \sqrt{D})/\sigma]$ by Lemma 3.1 of [5], then

$$I' = [Q_{l-1}/\sigma, (P_{l-1} + \sqrt{D})/\sigma] = I_{l-1};$$

whence $I \sim I'$ and so I is in an ambiguous class. By Lemma 1, there is at most one ambiguous ideal in this class. Thus, we have established that (2) implies (3).

Finally we assume (3) and prove (2). By Lemma 1, there is a reduced ideal $I \in \mathscr{C}$ with $I' = I_{l-1}$. Set $I = [Q_0/\sigma, (P_0 + \sqrt{D})/\sigma]$ then $I' = [Q_{l-1}/\sigma, (P_{l-1} + \sqrt{D})/\sigma]$. Therefore, by Lemma 3.1 of [5], $I = (I')' = [Q_{l-1}/\sigma, (P_l + \sqrt{D})/\sigma]$. However, by Lemma 3.2 of [5], $P_l = P_0$ and $Q_{l-1} = Q_0$ so $D = P_0^2 + Q_0^2$. Setting $\gamma = P_0 + \sqrt{D}/Q$ yields (2).

Remark 1. In the case where an ambiguous class contains 2 ambiguous ideals (excluded by Theorem 1) we "just miss" having pure symmetric period; i.e., if $[\gamma] = [Q/\sigma, (P + \sqrt{D})/\sigma]$ is in an ambiguous class containing 2 ambiguous ideals then $l(\gamma)$ is even, and $\gamma = \overline{\langle q_0, q_1, \ldots, q_{l-1}\rangle}$ where $q_1 q_2 \cdots q_{l-1}$ is a palindrome but $q_0 q_1 \cdots q_{l-1}$ is not. For instance,

Example 1. Set $D = 385 = 5 \cdot 7 \cdot 11$, and let $[\gamma] = [7, (7 + \sqrt{385})/27]$, then $\gamma = \overline{\langle 1, 1, 9, 6, 2, 3, 2, 6, 9, 1\rangle}$. Here $l(\gamma) = 10$, and $[\gamma]$ is ambiguous and equivalent to $J = [5, (15 + \sqrt{385})/2]$, the other ambiguous ideal in the class. Thus symmetry is ultimately tied to ambiguity.

Now we illustrate Theorem 1.

Example 2. If $D = 145 = 5 \cdot 29$ then letting $[\gamma] = [4, (9 + \sqrt{145})/2]$ we get $\gamma = \overline{\langle 2, 1, 1, 1, 2\rangle}$ and the class of $[\gamma]$ contains exactly one ambiguous ideal, namely $[\gamma_{(l-1)/2}] = [5, (5 + \sqrt{145})/2]$. Here $l(\gamma) = 5$ and $[\gamma]'$

$= [\gamma_{l-1}] = [4, (7 + \sqrt{145})/2]$.

Example 3. Let $D = 221 = 13 \cdot 17$ and set $[\gamma] = [5, (11 + \sqrt{221})/2]$ then $\gamma = \langle 2, 1, 1, 2 \rangle$ and the class of $[\gamma]$ contains no ambiguous ideals.

Remark 2. In [1], Harvey Cohn asserts that there can be at most one ambiguous class without any ambiguous ideals in the class group of a real quadratic field. We showed this to be false in the extreme in [5].

We provide an explanation here, not explicitly given in [5], to show that the elementary abelian 2-subgroup $C_{\Delta,2}$ of C_Δ for $\Delta > 0$ may be generated by ambiguous classes without ambiguous ideals.

Let t be the number of distinct prime divisors of a discriminant $\Delta > 0$ *excluding one* prime $p \equiv 3 (mod\ 4)$ whenever Δ has such a prime divisor, then, by Gauss, $C_{\Delta,2}$ has order 2^{t-1}; i.e., there are 2^{t-1} pairwise inequivalent ambiguous classes of (reduced) ideals. If one of these classes has *no* ambiguous ideal in it then (as proved in Lemma 3.4 of [5]) D is necessarily a sum of two relatively prime squares and $N(\varepsilon_\Delta) = 1$. Therefore, it is clear that t represents the number of distinct prime divisors of Δ in this case.

We now demonstrate that if C_Δ contains one ambiguous class without ambiguous ideals then $C_{\Delta,2}$ is generated by ambiguous classes without ambiguous ideals. First we observe that the subgroup $C_{\Delta,1}$ consisting of classes with ambiguous ideals must have $t - 2$ generators. To see this, we note that (by Theorem 3.3 of [5]), each such class must have exactly 2 ambiguous ideals in it. (Observe as well that $t \geq 2$ since $t = 1$ implies $N(\varepsilon_\Delta) = -1$. Moreover, if $t = 2$, then $C_{\Delta,1}$ has order 1; i.e., is trivial so that there are of course zero generators.) If we take an ambiguous class, $\{I\}$, without ambiguous ideals and form its product with each of the aforementioned $t - 2$ generators, then these new $t - 2$ classes together with $\{I\}$ yield $t - 1$ classes which generate $C_{\Delta,2}$, and each of these $t - 1$ classes has no ambiguous ideal in it (observing that the product of an ambiguous class without ambiguous ideals and that of an ambiguous class with ambiguous ideals yields an ambiguous class without ambiguous ideals).

The above elucidation contains the subtle point missed by Cohn in [1]; viz. that there are either *no* ambiguous classes without ambiguous ideal (in which case $C_{\Delta,2} = C_{\Delta,1}$ of order 2^{t-1}), or their number *coincides* with the number of ambiguous classes *with* ambiguous ideals, (in which case $|C_{\Delta,2}| = |C_{\Delta,1}| = 2^{t-2}$). Moreover, as shown above, in the latter case $C_{\Delta,2}$ is actually generated by ambiguous classes without ambiguous ideals.

Since [1] is considered to be one of the best sources (and deservedly so!) for this material it is worth clearing up this misconception.

Other errors in the literature concerning ambiguous classes occur for example in [2] which we corrected and generalized in [4]. It is therefore the hope that this paper helps the reader to see a clear overview of what is a very beautiful topic.

Acknowledgement. The author's research is supported by NSERC Canada grant # 8484. The author also thanks the referee for useful comments which improved the readability and clarity of the paper.

References

[1] H. Cohn: A Second Course in Number Theory. Wiley, New York (1962).
[2] F. Halter-Koch: Prime-producing quadratic polynomials and class numbers of quadratic orders. Computational Number Theory (eds. A. Pohst, *et al.*) de Gruyter, Berlin, pp. 73–82 (1991).
[3] H. Hasse: Vorlesungen über Zahlentheorie. section 16, Berechnung der Grundeinheit, Springer-Verlag (1964).
[4] R. A. Mollin: Ambiguous classes in quadratic fields. Math. Comp., **61**, 355–360 (1993).
[5] ——: The Palindromic Index——a measure of ambiguous cycles of reduced ideals without any ambiguous ideals in real quadratic orders (to appear: Séminaire de Théorie des nombres de Bordeaux).
[6] K. H. Rosen: Elementary Number Theory and Its Applications. Addison-Wesley, London, Sydney (1984).
[7] H. C. Williams and M. C. Wunderlich: On the parallel generation of the residues for the continued fraction factoring algorithm. Math. Comp., **177**, 405–423 (1987).