Orders in Quadratic Fields. IV

By R. A. MOLLIN

Department of Mathematics and Statistcs, The University of Calgary, Canada

(Communicated by Shokichi IYANAGA, M. J. A., Sept. 12, 1995)

Abstract: We give ideal-theoretic proofs of results for class groups of complex quadratic fields which have some valuable consequences.

1. Introduction. This continues work begun [3]-[4], and [6] to which we refer the reader for notation and background. In this paper we prove a result, Theorem 2.1, which appears without proof in the literature, at least in ideal-theoretic terms. The consequences of this result are far-reaching, as depicted by Corollaries 2.1-2.2. This sequence of results sets the stage to consider a "modified" conjecture posed in [3]. and consequences of it, which will appear in subsequent work.

2. Results. We first remind the reader that the ideal I is *reduced* in $\mathcal{O}_\Delta$ for $\Delta < 0$ if there is no $\alpha \in I$ such that $|\alpha| < N(I)$, where $|\alpha|^2 = N(\alpha)$.

Now we state the main result. Unfortunately the only place in the literature where it appears *in ideal-theoretic terms* is in [1] which is a minefield of misprints and erroneous statements.[1)] Thus, a valid proof is in order.

Theorem 2.1. *If $\Delta < 0$ is a fundamental discriminant, then each of the following holds*:

(a) *If I is a primitive ideal of $\mathcal{O}_\Delta$, then there exists some $\alpha \in I$ with $I = [N(I), \alpha]$ and $|Tr(\alpha)| \leq N(I)$ where $Tr(\alpha)$ denotes the trace of α. Furthermore, $|Tr(\alpha)|$ is unique (i.e. if $I = [N(I), \alpha] = [N(I), \beta]$ and $|Tr(\alpha)| \leq N(I)$, $|Tr(\beta)| \leq N(I)$, then $|Tr(\alpha)| = |Tr(\beta)|$).*

(b) *If I is a primitive ideal of $\mathcal{O}_\Delta$ and $I = [N(I), \alpha]$ with $|Tr(\alpha)| \leq N(I)$, then I is a reduced ideal if and only if $|\alpha| \geq N(I)$.*

(c) *If I is a reduced ideal of $\mathcal{O}_\Delta$, then $N(I) < \sqrt{|\Delta|/3}$.*

(d) *If I is a primitive ideal of $\mathcal{O}_\Delta$, and $N(I) < \sqrt{|\Delta|/4}$, then I is a reduced ideal.*

(e) *If $I_i = [\alpha_i, (b_i + \sqrt{\Delta})/2]$ (for $i = 1,2$) are two distinct, equivalent, reduced ideals in $\mathcal{O}_\Delta$, with $|b_i| \leq \alpha_i$ and $c_i = (b_i^2 - \Delta)/(4a_i)$, then $a_1 = a_2 = a$, $|b_1| = |b_2| = b$, and $c_1 = c_2 = c$. Also, if $b \neq a$, then $c = a$. (This tells us that there are at most two reduced ideals in any class of C_Δ, and when two such ideals are in a class, then they are conjugates of one another.)*

(f) *If $I = [N(I), \alpha]$ is an ideal of $\mathcal{O}_\Delta$ with $|Tr(\alpha)| \leq N(I)$, and I is in an ambiguons class of $\mathcal{O}_\Delta$, then either $N(I)$ or $2N(I) + |Tr(\alpha)|$ is a divisor of Δ.*

Proof. Part (a) follows from the fact that $I = [N(I), nN(I) \pm \alpha]$ for any $n \in \mathbf{Z}$. Part (b) follows from the very definition of a reduced ideal, given at the outset of this section.

To prove part (c), we observe that if $I = [N(I), \alpha]$, then $4N(\alpha) - Tr(\alpha)^2 = -\Delta$, so if I is reduced, then $|\alpha| \geq N(I)$. Since $|Tr(\alpha)|$

[1)] Since no corrigenda for [1] has appeared, we provide the following analysis as a service to the reader. The definition of "primitive" on page 109 is incorrect, since any product of two distinct split prime ideals of "$\mathcal{O}_K$" would be a counterexample. In Lemma 2.2, the word "primitive" should be added to the condition for the ideal. On page 110, Theorem 2.7 is false as stated since the word "primitive" should be replaced by the word "reduced". In Algorithm 3.1 on page 110, they incorrectly assert that $Ne(\gamma)$ is "unique unless" $\gamma = \pm 1/2$. In fact, it is unique unless $\gamma = m/2$ where $m \in \mathbf{Z}$ is odd. Also, there is a misprint where they say "$x = 1/2$" when they mean "$\gamma = \pm 1/2$". Furthermore, on page 115 they attempt to give a proof of Theorem 2.1(f). However, in paragraph 4, it is erroneously stated that "$4N(\alpha) = |Tr(\alpha)|^2 + D$". It should be "$4N(\alpha) = |Tr(\alpha)|^2 - \Delta$" In fact, throughout the balance of their discussion they confuse the discriminant and the radicand, sometimes in the same sentence. In paragraph 7, it is claimed that either $N(I)$ or $2N(I) + |Tr(\alpha)|$ divides D when in fact they mean Δ, since otherwise $I = [2, 1 + \sqrt{-5}]$ is a counterexample. Yet, in the first sentence of paragraph 6 they do seem to mean D since otherwise their ideals $[s, \sqrt{D}]$ are not even primitive; and if they *do* mean D, then the proof is not complete since they do not account for those $s \mid \Delta$ where s is even and D is odd.

$\leq N(I)$, then $-\Delta = 4N(\alpha) - Tr(\alpha)^2 \geq 4N(\alpha) - N(I)^2 = 4|\alpha|^2 - N(I)^2 \geq 4N(I)^2 - N(I)^2 = 3N(I)^2$.

To prove (d) we note that, if $N(I) < \sqrt{|\Delta|/4}$, and $|\alpha| < N(I)$, then $N(\alpha) < |\Delta|/4 = N(\alpha) - Tr(\alpha)^2/4$, a contradiction.

The proof of (e) is more involved. By part (b), we may assume that $c_i \geq a_i$ for $i = 1,2$. We may assume, without loss of generality, that $a_1 \geq a_2$. Also, since $I_1 I_2' \sim 1$, then $I_1 I_2' = (\alpha)$ where $\alpha \in I_1$. Therefore, there exist $x, y \in \boldsymbol{Z}$ such that

(2.1) $$2\alpha = 2xa_1 + b_1 y + y\sqrt{\Delta}.$$

By taking norms and dividing by $4a_1$ in (2.1), we get

(2.2) $$a_1 \geq a_2 = x^2 a_1 + xyb_1 + y^2 c_1.$$

Therefore,

(2.3) $$a_1 \geq x^2 a_1 + xyb_1 + y^2 a_1.$$

Hence, $xyb_1 \leq 0$. We now show that $xy = 0$. If $b_1 > 0$ and $xy < 0$, then $xyb_1 \geq xya_1$. By (2.3) we get

$$a_1 \geq x^2 a_1 + xya_1 + y^2 a_1,$$

i.e.

$$1 \geq x^2 + xy + y^2 = (x+y)^2 - xy,$$

or

$$1 > 1 + xy > (x+y)^2,$$

a contradiction. The case where $b_1 < 0$ and $xy > 0$ is similar. Thus, we have $xy = 0$. We observe that $b_1 \neq 0$ since $b_1 = 0$ would force $b_2 = 0$ and $a_1 = a_2$ via (2.1)-(2.3), contradicting that $I_1 \neq I_2$. If $y = 0$, then $a_1 = a_2 = |b_1| = |b_2|$ by (2.1)-(2.3). If $y \neq 0$ and $x = 0$, then by (2.1)-(2.3), $a_1 = a_2 = c_1 = a$, say. A similar argument shows that $c_2 = a$.

Finally, we establish (f). Let $I = [N(I), (b + \sqrt{\Delta})/2] = [N(I), \alpha]$ be an ideal in an ambiguous class of $\mathcal{O}_\Delta$ with $|Tr(\alpha)| = b \leq N(I)$. If $I = I'$, then $N(I)$ divides Δ, since $\alpha + \alpha' \in I$ in that case. We may now assume that $I \neq I'$. First we assume that $N(I) > 1$ and $gcd(N(I), |\Delta|) = 1$. By standard facts (see [2] for example), $I^2 = [N(I)^2, \beta] \sim 1$, where $\beta = (b_3 + \Delta)/2$ and b_3 is determined modulo $2N(I)^2$. Therefore, $|b_3| < 2N(I)^2 < -2\Delta/3$, and so $N(\beta) < N(\omega\Delta)^2$ provided that $-\Delta > 8$ which we may assume. Now we may invoke [4, Lemma 2, p. 178],[2] to get that $N(\beta) = N(I)^2$, i.e. $\Delta = b_3^2 - 4N(I)^2$. From [2], it easily follows that $b_3 = b$. Hence, $\Delta = (b - 2N(I))(b + 2N(I))$, i.e. $2N(I) + |Tr(\alpha)|$ divides $|\Delta|$.

If $d = gcd(N I), \Delta) > 1$, then an easy exercise shows that $gcd(d, N(I)/d) = 1$, so $I = [d, \alpha]\,[N(I)/d, \alpha] = I_1 I_2$, say. Since $d \mid |\Delta|$, then $I_1^2 \sim 1$ so $I_2^2 \sim 1$, given that I is assumed to be in an ambiguous class. Therefore, by the above argument, $2N(I)/d + |Tr(\alpha)|$ divides $|\Delta|$. if $N(I) > d$. However, $d \mid| Tr(\alpha)|$, so $d \mid N(I)/d$, a contradiction. Hence, $N(I) = d$ divides $|\Delta|$. □

Corollary 2.1. *If $\Delta < 0$ is a discriminant and $I = [N(I), \alpha]$ is an ideal in an ambiguous class of C_Δ with $N(I)$ not dividing Δ, then*

(a) $\Delta \not\equiv 0 \pmod 8$.

(b) *There exists a squarefree divisor $q > N(I)$ of $|\Delta|$ such that $\Delta = q^2 - 4qN(I)$.*

Proof. Continuing from the proof of Theorem 2.1(f), $\Delta = b^2 - 4N(I)^2$. If $q = 2N(I) + |b|$, then $q > N(I)$ and q is square-free. This is (b). If $\Delta \equiv 0 \pmod 8$, then q must be even in the above. Thus, $\Delta \equiv q^2 \pmod 8$ forcing $q \equiv 0 \pmod 4$, a contradiction. This is (a). □

We also get the following which was established in [6].

Corollary 2.2. *If $I_i = [a_i, \alpha_i]$, for $i = 1,2$, are two primitive ideals of $\mathcal{O}_\Delta$ with $\Delta < 0, 1 \leq a_i < \sqrt{-\Delta}/2$, and $I_1 \sim I_2$, them $I_1 = I_2$.*

Proof. By Theorem 2.1(d), the I_i are reduced so that by Theorem 2.1(e), $a_1 = a_2$, and $I_1' = I_2$. If $I_1 \neq I_2$, then by Theorem 2.1(f), $\Delta = b^2 - 4N(I_1)^2$, where $b = |Tr(\alpha_1)|$. However, $N(I_1) < \sqrt{-\Delta/2}$, so $\Delta = b^2 - 4N(I_1)^2 > b^2 + \Delta$, a contradiction. □

The last result says something deeper than what appears on the surface. It says that two distinct reduced ideals can exist in a class of C_Δ, for $\Delta < 0$, if and only if the class is *ambiguous* and there are *no reduced ambiguous ideals* in the class. Furthermore, if there are two distinct reduced ideals in the class, then one is the conjugate of the other $I \neq I'$, and $\sqrt{-\Delta}/2 < N(I) = N(I') < \sqrt{-\Delta}/3$.

In subsequent work we will be able to use the results obtained herein to obtain the proof of a conjecture which amounts to a criterion for $e_\Delta \leq 2$ when $\Delta < 0$. Furthermore, the above, together with a complete description of current algebraic and computational number theory techniques and results will appear in this author's book [5].

[2] Note that, in the statement of Lemma 2 therein, there is a typo; viz. "$N(b + w_\Delta)^2$" should read "$N(b + w_\Delta)$".

Acknowledgement. The author's research is supported by NSERC Canada grant # A8484. The author welcomes the opportunity to thank the referee for very useful observations and suggestions to correct the errors in [1], as well as for a very careful reading of the original manuscript from which this paper arose.

References

[1] J. Buchmann and H.C. Williams: A key-exchange system based on imaginary quadratic fields. J. Cryptology, **1**, 107–118 (1988).

[2] H. W. Lenstra: On the calculation of regulators and class number of quadratic fields. Journeés Arith. Cambridge University Press, pp. 123–150 (1980).

[3] R. A. Mollin: Orders in quadratic fields. I. Proc. Japan Acad., **69A**, 45–48 (1993).

[4] R. A. Mollin: Orders in quadratic fields. III. Proc. Japan. Acad., **70A**, 176–181 (1994).

[5] R. R. Mollin: Quadratics. C. R. C. Press, Florida (1995).

[6] R. A. Mollin and L-C. Zhang: Orders in quadratic fields. II. Proc. Japan Acad, **69A**, 368–371 (1993).