

Orders in Quadratic Fields. IV

By R. A. MOLLIN

Department of Mathematics and Statistics, 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}_Δ 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

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 " $4N(\alpha) = |\text{Tr}(\alpha)|^2 + D$ ". It should be " $4N(\alpha) = |\text{Tr}(\alpha)|^2 - \Delta$ ". 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 $2N(I) + |\text{Tr}(\alpha)|$ 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 $s | \Delta$ where s is even and D is odd.

the only place in the literature where it appears *in ideal-theoretic terms* is in [1] which is a mine-field 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}_Δ , then there exists some $\alpha \in I$ with $I = [N(I), \alpha]$ and $|\text{Tr}(\alpha)| \leq N(I)$ where $\text{Tr}(\alpha)$ denotes the trace of α . Furthermore, $|\text{Tr}(\alpha)|$ is unique (i.e. if $I = [N(I), \alpha] = [N(I), \beta]$ and $|\text{Tr}(\alpha)| \leq N(I)$, $|\text{Tr}(\beta)| \leq N(I)$, then $|\text{Tr}(\alpha)| = |\text{Tr}(\beta)|$).*
- (b) *If I is a primitive ideal of \mathcal{O}_Δ and $I = [N(I), \alpha]$ with $|\text{Tr}(\alpha)| \leq N(I)$, then I is a reduced ideal if and only if $|\alpha| \geq N(I)$.*
- (c) *If I is a reduced ideal of \mathcal{O}_Δ , then $N(I) < \sqrt{|\Delta|/3}$.*
- (d) *If I is a primitive ideal of \mathcal{O}_Δ , 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}_Δ , with $|b_i| \leq \alpha_i$ and $c_i = (b_i^2 - \Delta)/(4\alpha_i)$, 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 \mathcal{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}_Δ with $|\text{Tr}(\alpha)| \leq N(I)$, and I is in an ambiguous class of \mathcal{O}_Δ , then either $N(I)$ or $2N(I) + |\text{Tr}(\alpha)|$ 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 $4N(\alpha) - \text{Tr}(\alpha)^2 = -\Delta$, so if I is reduced, then $|\alpha| \geq N(I)$. Since $|\text{Tr}(\alpha)|$