PACIFIC JOURNAL OF MATHEMATICS
Vol. 122, No. 1, 1986

REPRESENTATIONS OF TERNARY QUADRATIC FORMS AND THE CLASS NUMBER OF IMAGINARY QUADRATIC FIELDS

THOMAS R. SHEMANSKE

In this paper, we consider the norm form of a definite rational quaternion algebra restricted to the elements of trace zero in a maximal order of the algebra. When the algebra has class number one, we derive an equation which relates the representation numbers of the norm form to the class number of imaginary quadratic extensions of the rational numbers.

0. Introduction. Kneser [**8**] observed that the existence of a relation between these two quantities is not unexpected. When compared to the Dirichlet class number formula, the Minkowski-Siegel formulas suggest a connection between the weighted average of the number of primitive representations of an integer m by the different forms in the genus of a given definite ternary quadratic form and the number of ideal classes in an order of $\mathbf{Q}(\sqrt{-m})$ (e.g. see [**3**] Appendix B). This connection is evidenced by comparing the local p-factors in each formula. In the case that the genus consists of only one class, one derives information about the representation numbers of the given form. However, this approach has two disadvantages. First, the job of determining the p-factors for primes p dividing twice the discriminant of the form is at best awkward, and second, such an analytic proof would not provide as explicit a correspondence between ideal classes and primitive elements as the one given by the arithmetic approach which we shall use.

In [**6**], Gauss showed that the number of primitive integral solutions (i.e. $x, y, z \in \mathbf{Z}$ and $(x, y, z) = 1$) to $x^2 + y^2 + z^2 = m$ is a constant multiple of the class number of primitive binary quadratic forms of discriminant $-4m$; the constant is 12 or 24 depending only on the congruence class of m modulo 4. In the 1920's, Venkov [**15**] elegantly reproved Gauss' result by viewing the ternary form as the (reduced) norm of a generic element of trace zero in the maximal order

$$\Lambda = \mathbf{Z}\left(\frac{1 + i + j + k}{2}\right) + \mathbf{Z}i + \mathbf{Z}j + \mathbf{Z}k$$

(Hurwitz's quaternions) in the quaternion algebra $(\frac{-1,-1}{\mathbf{Q}})$. Rehm [**11**] recently reproved some of Venkov's results in a more modern framework.

In this paper, we extend the ideas of Venkov and Rehm to consider ternary forms realized by restricting the norm form of various definite quaternion algebras over $\mathbf{Q}$ to the elements of trace zero. Such a form has the shape $ax^2 + by^2 + abz^2$ with $a, b \in \mathbf{Q}^\times$. There are two natural lines along which to generalize the results of Gauss and Venkov. One can ask for the number of primitive integral solutions to equations of the form $ax^2 + by^2 + abz^2 = m$, or one may take the reduced norm form of the quaternion algebra and restrict it to the elements of trace zero in various orders in the algebra and ask for a characterization of its representation numbers on these orders. In [13], we considered the first question; in the present paper, we consider the second. The questions are, of course, intimately related—they coincide in the case of Hurwitz's quaternions and the maximal order Λ above. The main constraint to obtaining a generalization of Gauss' result using Venkov's ideas is the need to choose a quaternion algebra in which the (maximal) orders are principal ideal rings. Generalizations to algebras with class numbers greater than one are under present consideration by the author, although they require adelic methods which we have circumvented here by restricting to the class number one case.

Let $\mathfrak{A}$ be a definite rational quaternion algebra of class number one and Λ a maximal order in $\mathfrak{A}$. It will turn out that the only such algebras are those ramified at a unique finite prime q (and at infinity). Let m be a positive integer not divisible by 4 and write $m = m_0 f^2$ with m_0 square-free. Denote by $T(m)$ the number of primitive $\mu \in \Lambda$ with trace 0 and reduced norm m, and let $h(m)$ denote the order of the ideal class group of proper $\mathcal{O}_f$-ideals in $\mathbf{Q}(\sqrt{-m})$. Let $\omega(m)$ denote the number of units in $\mathcal{O}_f$ and $|\Lambda^\times|$ the order of the unit group, $\Lambda^\times$, of Λ.

We obtain the following theorem:

THEOREM. *Suppose that* $T(m) > 0$. *Then*

$$\frac{\omega(m)T(m)}{h(m)} = \begin{cases} |\Lambda^\times|\varepsilon_m & \text{if } q \mid m \\ 2|\Lambda^\times|\varepsilon_m & \text{if } q \nmid m \end{cases}$$

where

$$\varepsilon_m = \begin{cases} 1 & \text{if } m \equiv 1, 2 \pmod 4 \\ 2 & \text{if } m \equiv 7 \pmod 8 \\ 4 & \text{if } m \equiv 3 \pmod 8). \end{cases}$$

The idea of the proof is quite straightforward. Basically, it follows the general plan described by Venkov and utilizes the modern framework which Rehm has presented. Specifically, in each algebra $\mathfrak{A}$ we first fix a

maximal order Λ. For a given positive integer m, we consider all primitive $\lambda \in \Lambda$ such that $\lambda^2 = -m$ and form the "root bundle" $[\lambda] = \{\varepsilon\lambda\varepsilon^{-1} | \varepsilon \in \Lambda^\times\}$ where $\Lambda^\times$ is the unit group of Λ. Let W denote the set of all such root bundles and let G denote the ideal class group of proper $\mathcal{O}_f$-ideals. Following Rehm, we define a map which induces a group action of G on W. The theorem is obtained by determining the number of orbits under this action and the number of primitive "roots" contained in each root bundle.

There are a number of technical difficulties which arise and encumber the general implementation of this plan of proof. They necessitate a detailed analysis of the arithmetic of the individual maximal orders Λ and an investigation of the connection between the arithmetic of the quadratic field $\mathbf{Q}(\sqrt{-m})$ and of its various embeddings in the algebra $\mathfrak{A}$.

This paper is divided into four sections. The first two contain notation and general results about rational quaternion algebras. The third is devoted to the detailed analysis of the arithmetic of the maximal order, the definition of Rehm's map, a study of the bundles and of the connection between the arithmetic in the maximal order and in quadratic subfields of the algebra. An example is worked out in detail at the end of this section. The fourth section describes the results which one obtains regarding integral representations. In general, the notation used is that of [**11**].

The author wishes to thank J. Cremona and A. Pizer for useful conversations, and M. Kneser for comments and suggestions about [**13**] which are reflected in this present work.

1. Notation. Let $\mathbf{Z}$, $\mathbf{Q}$, $\mathbf{R}$ denote the rational integers, rational numbers and real numbers respectively. For a finite prime p of $\mathbf{Q}$, denote by $\mathbf{Q}_p$ the field of p-adic numbers and by $\mathbf{Z}_p$ the subring of p-adic integers. We shall also let ∞ denote the infinite prime of $\mathbf{Q}$ and sometimes denote $\mathbf{R}$ by $\mathbf{Q}_\infty$. For a ring R, denote by $R^\times$ the group of all invertible elements of R, and by $M_2(R)$ the ring of 2×2 matrices with entries in R. Finally, if $A \subset B$ are groups, let $[B: A]$ denote the index of A in B.

We now remind the reader of some of the basic facts concerning quaternion algebras. The reader is referred to [**12**] or [**16**] for more detail. Let K be a field (of characteristic not two) and $a, b \in K^\times$. We denote by

$$\mathfrak{A} = \left(\frac{a,b}{K}\right)$$

the quaternion algebra over K with basis (as a K-vector space) $1, i, j, k$ subject to the relations $i^2 = a$, $j^2 = b$, $ij = k = -ji$. If L is an extension

field of K, then

$$\left(\frac{a,b}{K}\right) \otimes_K L \simeq \left(\frac{a,b}{L}\right).$$

For $\alpha = w + xi + yj + zk \in \mathfrak{A}$, we define the conjugate of α to be $\bar{\alpha} = w - xi - yj - zk$. One verifies that $\overline{\alpha + \beta} = \bar{\alpha} + \bar{\beta}$, $\overline{\alpha\beta} = \bar{\beta}\bar{\alpha}$, $\bar{\bar{\alpha}} = \alpha$ and $\overline{r\alpha} = r\bar{\alpha}$ for $r \in K$. Using this notion, we define the (*reduced*) *norm* of α by $N(\alpha) = \alpha\bar{\alpha}$ $(= w^2 - ax^2 - by^2 + abz^2)$ and the (*reduced*) *trace* of α by $\mathrm{Tr}(\alpha) = \alpha + \bar{\alpha}$ $(= 2w)$. In particular, $N(\alpha), \mathrm{Tr}(\alpha) \in K$. It is easy to check that if $\alpha \in \mathfrak{A}$ and $\alpha \notin K$, then the minimal polynomial over K of which α is a root is $X^2 - \mathrm{Tr}(\alpha)X + N(\alpha)$.

If $\mathfrak{A}$ is a quaternion algebra over $\mathbf{Q}$, and p is a prime of $\mathbf{Q}$ (finite or infinite), denote by $\mathfrak{A}_p$ the quaternion algebra $\mathfrak{A} \otimes_{\mathbf{Q}} \mathbf{Q}_p$. If L is a $\mathbf{Z}$-submodule of Λ, and p any finite prime of $\mathbf{Q}$, let $L_p = L \otimes_{\mathbf{Z}} \mathbf{Z}_p$. Let p be any prime of $\mathbf{Q}$. Up to isomorphism, there are precisely two quaternion algebras over $\mathbf{Q}_p$: $M_2(\mathbf{Q}_p)$ and the unique quaternion division algebra over $\mathbf{Q}_p$. We say that p *ramifies* in $\mathfrak{A}$ if $\mathfrak{A}_p$ is a division algebra, and that p *splits* otherwise. The set of ramified primes is finite, even in number (counting ∞), and characterizes $\mathfrak{A}$ up to isomorphism.

Let $K = \mathbf{Q}$ or $\mathbf{Q}_p$ (p finite) and let $\mathcal{O}$ be the ring of integers in K. If $\mathfrak{A}$ is a quaternion algebra over K, then by an *order* in $\mathfrak{A}$, we shall mean a free $\mathcal{O}$-module Λ of rank 4 which is also a subring of $\mathfrak{A}$ containing 1. One can show that for α in an order Λ, $N(\alpha)$ and $\mathrm{Tr}(\alpha)$ are in $\mathcal{O}$. For this and other details concerning quaternion algebras, the reader is referred to [**12**].

Throughout, we shall be concerned with definite quaternion algebras

$$\mathfrak{A} = \left(\frac{a,b}{\mathbf{Q}}\right).$$

We may and therefore shall assume that $a, b \in \mathbf{Z}$ and $a, b < 0$. Note that this makes the norm form positive definite and hence makes $\mathfrak{A}$ a division algebra. Let $\Lambda \subset \mathfrak{A}$ be an order and $\mu \in \Lambda$. For a finite prime p of $\mathbf{Q}$ we say that μ is *p-primitive* if whenever $\mu = c\nu$ with $c \in \mathbf{Z}$, $\nu \in \Lambda$, then $p \nmid c$. We say that μ is *primitive* if it is p-primitive for all primes p.

2. Preliminaries. Throughout, let $\mathfrak{A}$ be a definite rational quaternion algebra. The following result is well-known.

PROPOSITION 2.1. *Let $\mu \in \mathfrak{A}$, $\mu \notin \mathbf{Q}$. Then the centralizer of μ in $\mathfrak{A}$ is the subfield of $\mathfrak{A}$, $\mathbf{Q}(\mu) = \{r + s\mu | r, s \in \mathbf{Q}\}$.*

Let m be a positive integer and $\mu, \nu \in \mathfrak{A}$ with $\mu^2 = \nu^2 = -m$. We characterize the set $A_{\mu,\nu} = \{\alpha \in \mathfrak{A} | \alpha\mu = \nu\alpha\}$ with

PROPOSITION 2.2. *$A_{\mu,\nu}$ is a right $\mathbf{Q}(\mu)$-vector space of dimension* 1.

Proof. Since $\mu^2 = \nu^2 = -m$, the map $\mu \to \nu$ induces an isomorphism of $\mathbf{Q}(\mu)$ and $\mathbf{Q}(\nu)$ which, by the Skolem-Noether theorem [**12**], extends to an inner automorphism of $\mathfrak{A}$. Thus there exists an $\alpha_0 \in \mathfrak{A}^\times$ such that $\nu = \alpha_0 \mu \alpha_0^{-1}$. Let $\beta \in A_{\mu,\nu}$, $\beta \neq 0$. Since $\alpha_0 \mu \alpha_0^{-1} = \nu = \beta \mu \beta^{-1}$, $\alpha_0^{-1}\beta$ is in the centralizer of μ. By Proposition 2.1, we have $\alpha_0^{-1}\beta \in \mathbf{Q}(\mu)$ or $\beta \in \alpha_0 \mathbf{Q}(\mu)$ from which the proposition follows.

In this paper, we are interested in definite rational quaternion algebras, $\mathfrak{A}$, which have class number one (i.e. the maximal orders all have class number one). Since $\mathfrak{A}$ is definite, it is ramified at infinity and hence at an odd number of finite primes. It follows from the class number formula [**2**], [**5**] for maximal orders, that class number one occurs if and only if $\mathfrak{A}$ is ramified at infinity and at precisely one of the primes $q = 2$, 3, 5, 7, 13. A useful table of class and type numbers of Eichler (in particular maximal) orders can be found in [**9**]. The case of $q = 2$ is that of Hurwitz's quaternions which has been considered in [**11**], [**15**], so we shall concern ourselves with the other four cases.

Denote by $\mathfrak{A}(q)$ the unique (up to isomorphism) rational quaternion algebra ramified precisely at the primes q, ∞. From Proposition 5.1, 5.2 of [**10**], we have that if $q \equiv 3\ (4)$,

$$\mathfrak{A}(q) = \left(\frac{-1, -q}{\mathbf{Q}}\right)$$

and if $q \equiv 5\ (8)$,

$$\mathfrak{A}(q) = \left(\frac{-2, -q}{\mathbf{Q}}\right).$$

Moreover, a maximal order $\Lambda(q)$ of $\mathfrak{A}(q)$ (in terms of the canonical basis of $\mathfrak{A}(q)$) is given by:

$$\Lambda(q) = \mathbf{Z}\left(\frac{1+j}{2}\right) + \mathbf{Z}\left(\frac{i+k}{2}\right) + \mathbf{Z}j + \mathbf{Z}k \quad \text{if } q \equiv 3\ (4) \text{ or}$$

$$\Lambda(q) = \mathbf{Z}\left(\frac{1+j+k}{2}\right) + \mathbf{Z}\left(\frac{i+2j+k}{4}\right) + \mathbf{Z}j + \mathbf{Z}k \tag{2.1}$$

$$\text{if } q \equiv 5\ (8).$$

We also fix for the remainder of the paper the order

$$\Lambda_0 = \mathbf{Z} + \mathbf{Z}i + \mathbf{Z}j + \mathbf{Z}k \tag{2.2}$$

Henceforth, we restrict to the case of class number one, i.e. $q = 3$, 5, 7, 13. Since class number one implies that the type number is one, any two maximal orders of $\mathfrak{A}(q)$ are conjugate (by an element of $\mathfrak{A}(q)^\times$). Furthermore, since the questions which we wish to consider regard the representation numbers of the norm form restricted to a maximal order,

the answers will be independent of the particular maximal order we choose. Thus for convenience, we shall restrict our attention to the maximal order $\Lambda(q)$ defined above.

Let $\mathfrak{A} = \mathfrak{A}(q)$ and $\Lambda = \Lambda(q)$. Recall that $\Lambda_0 \subset \Lambda$. We want to consider the notion of primitive elements in both Λ_0 and Λ. We record some elementary observations as:

LEMMA 2.3. (1) *Let $\mu \in \Lambda_0$ and $p \in \mathbf{Z}$ a prime. Then*

(a) *μ is p-primitive in Λ implies μ is p-primitive in Λ_0;*

(b) *μ is primitive in Λ implies μ is primitive in Λ_0;*

(c) *μ is primitive in Λ_0 implies μ is p-primitive in Λ for all primes $p > 2$;*

(d) *μ is primitive in Λ_0 and $N(\mu) \not\equiv 0$ (4) implies μ is primitive in Λ.*

(2) *Let $\nu \in \Lambda$ be primitive in Λ. Then $4\nu \in \Lambda_0$ and is p-primitive in Λ for all primes $p > 2$.*

Let m be a positive integer and write $m = m_0 f^2$ with m_0 square-free. Let $\mu, \nu \in \Lambda$ be primitive in Λ with $\mu^2 = \nu^2 = -m$. We wish to consider the set $T_{\mu,\nu} = \{\lambda \in \Lambda | \lambda\nu = \nu\lambda\}$. It is clear that $T_{\mu,\nu} = A_{\mu,\nu} \cap \Lambda$ (i.e., the intersection of a rank 4 $\mathbf{Z}$-module and a two-dimensional $\mathbf{Q}$-vector space) is a free $\mathbf{Z}$-module of rank 2.

Write

$$\mathfrak{A} = \mathfrak{A}(q) = \left(\frac{-a, -q}{\mathbf{Q}}\right)$$

with $a = 1$ if $q \equiv 3$ (4), and $a = 2$ if $q \equiv 5$ (8).

LEMMA 2.4. *With the above notation, suppose that $(f, 2q) = 1$. Then there exists a $\mathbf{Z}$-basis ξ, η of $T_{\mu,\nu}$ such that $(N(\eta), f) = 1$.*

Proof. Let $\mu_0 = 4\mu$, $\nu_0 = 4\nu$. Then by Lemma 2.3, $\mu_0, \nu_0 \in \Lambda_0$ and are p-primitive for all primes $p > 2$. Let $\mu_0 = x_1 i + x_2 j + x_3 k$ and $\nu_0 = y_1 i + y_2 j + y_3 k$. Then $x_l, y_l \in \mathbf{Z}$, $l = 1, 2, 3$ and the greatest common divisors (x_1, x_2, x_3) and (y_1, y_2, y_3) have only 2 as a possible prime divisor. Since $\mu^2 = \nu^2 = -m$, one checks that for any $\lambda \in \Lambda$ the element $\lambda\mu + \nu\lambda$ is in $T_{\mu,\nu}$. Consider the elements $\gamma_1, \gamma_2, \gamma_3$ in $T_{\mu,\nu}$ defined by:

$$\gamma_1 = 4(\mu + \nu) = (x_1 + y_1)i + (x_2 + y_2)j + (x_3 + y_3)k,$$

$$\gamma_2 = 4(i\mu + \nu i) = -a(x_1 + y_1) + a(y_3 - x_3)j + (x_2 - y_2)k,$$

$$\gamma_3 = 4(j\mu + \nu j) = -q(x_2 + y_2) + q(x_3 - y_3)i + (y_1 - x_1)k.$$

One computes

$$N(\gamma_1) = 2(16m + ax_1y_1 + qx_2y_2 + aqx_3y_3),$$

$$N(\gamma_2) = 2a(16m + ax_1y_1 - qx_2y_2 - aqx_3y_3),$$

$$N(\gamma_3) = 2q(16m - ax_1y_1 + qx_2y_2 - aqx_3y_3).$$

Let p be a prime dividing f. Then one of γ_1, γ_2, γ_3 has norm not divisible by p. Otherwise, since $p \nmid 2q$ we have

$$A\begin{pmatrix} x_1y_1 \\ x_2y_2 \\ x_3y_3 \end{pmatrix} \equiv 0 \pmod{p} \quad \text{where } A = \begin{pmatrix} a & q & aq \\ a & -q & -aq \\ -a & q & -aq \end{pmatrix}$$

and since $\det(A) = 2(aq)^2 \not\equiv 0\,(p)$ we must have $x_1y_1 \equiv x_2y_2 \equiv x_3y_3 \equiv 0\,(p)$. Clearly, p cannot divide all the x_i's since μ_0 is p-primitive. Moreover, p cannot divide two of the x_i's since this would imply p divides the third. Thus p divides at most one x_i. But this implies p divides at least 2 and hence all three y_i's, contradicting ν_0 is p-primitive. Thus one of γ_1, γ_2 or γ_3 has norm not divisible by p.

It is now a standard argument which shows that a basis of the desired type can be found.

3. The Form $ax^2 + qy^2 + aqz^2$. For the remainder of the paper we fix

$$\mathfrak{A} = \mathfrak{A}(q) = \left(\frac{-a, -q}{\mathbf{Q}}\right)$$

with $a = 1$ if $q = 3, 7$, and $a = 2$ if $q = 5, 13$. We let $\Lambda = \Lambda(q)$ be the maximal order given in (2.1) and Λ_0 the suborder given in (2.2). Observe that for $\alpha = w + xi + yj + zk \in \mathfrak{A}$, $N(\alpha) = w^2 + ax^2 + qy^2 + aqz^2$, so that the norm form restricted to elements of trace zero yields the ternary form of interest.

Let m be a positive integer not divisible by 4. We are interested in characterizing the number of primitive elements μ in Λ which satisfy $\mathrm{Tr}(\mu) = 0$ and $N(\mu) = m$, i.e., $\mu^2 + m = 0$. By a *primitive root of* $X^2 + m$, we shall always mean a μ as above. Note that if we were interested in characterizing the number of primitive integral solutions (i.e., $x, y, z \in \mathbf{Z}$ and $(x, y, z) = 1$) to the equation $ax^2 + qy^2 + aqz^2 = m$, then since there is an obvious correspondence between the solution (x, y, z) and the element $\mu = xi + yj + zk \in \Lambda_0$ (of norm m), we would seek our characterization (as above) in terms of the elements of Λ_0 (see [**13**]).

3.1. *The Arithmetic of* Λ. We begin with a study of the arithmetic of the maximal order Λ.

PROPOSITION 3.1. (1) *Every left* Λ*-ideal is principal.* (2) $\Lambda^\times$, *the group of units in* Λ, *is a finite group.*

Proof. The first statement is true since Λ has class number one. For the second, recall that $\varepsilon \in \Lambda$ is a unit if and only if $N(\varepsilon) = 1$. Since the norm form is positive definite and Λ a lattice, the result is clear.

PROPOSITION 3.2. *Let* $\lambda \in \Lambda$, $N(\lambda) \equiv 0 \pmod{q}$. *Then* $\lambda \in \Lambda j = j\Lambda$ *where* j *is the element of the canonical basis of* $\mathfrak{A}$ *satisfying* $j^2 = -q$.

Proof. Since $N(j) = q$, $\Lambda_q j = j\Lambda_q$ (see Theorem 13.2 of [**12**]), and for primes $p \neq q$, $j \in \Lambda_p^{\times}$, whence $j\Lambda = \Lambda j = \{\lambda \in \Lambda | N(\lambda) \equiv 0 \ (q)\}$ since it is true in all localizations. Here we use the local-global correspondence of orders and ideals (see Proposition 5.1 of [**16**]).

PROPOSITION 3.3. *There are precisely three integral left* Λ*-ideals of (reduced) norm* 2, *denoted* $\Lambda\tau_1$, $\Lambda\tau_2$, $\Lambda\tau_3$. *The union of these ideals contains all the elements of* Λ *of even norm.*

Proof. Since 2 is a split prime in $\mathfrak{A}$, Λ_2 is isomorphic to $M_2(\mathbf{Z}_2)$, and therefore contains 3 distinct integral left Λ_2-ideals of norm 2 (Theorem 2.3 of [**16**]). From the local-global correspondence, it follows that there are at most 3 integral left Λ-ideals of norm 2. One then checks directly that in each of our four algebras, there are 3 distinct ideals. The second statement follows from Theorem 19.6 of [**12**].

Now let m be a positive integer not divisible by 4 and write $m = m_0 f^2$ with m_0 square-free. Let μ be a primitive root of $X^2 + m$ in Λ. We want to connect the arithmetic of the quadratic field $\mathbf{Q}(\sqrt{-m})$ with that of $\mathbf{Q}(\mu) \subset \mathfrak{A}$. We begin with

PROPOSITION 3.4. *Let* $\mathcal{O}_\mu = \Lambda \cap \mathbf{Q}(\mu)$. *Then* $\mathbf{Z} + \mathbf{Z}\mu \subset \mathcal{O}_\mu \subset \mathbf{Z} + \mathbf{Z}(1 + \mu)/2$. *Moreover,* $\mathcal{O}_\mu = \mathbf{Z} + \mathbf{Z}(1 + \mu)/2$ *if and only if* $(1 + \mu)/2 \in \Lambda$. *In particular, if* $m \equiv 1, 2\ (4)$, *then* $\mathcal{O}_\mu = \mathbf{Z} + \mathbf{Z}\mu$.

Proof. Clearly, $\mathbf{Z} + \mathbf{Z}\mu \subset \mathcal{O}_\mu$ and $\mathcal{O}_\mu$ is an order in $\mathbf{Q}(\mu)$. Let $\omega = \mu$ if $m \equiv 1, 2\ (4)$ or $\omega = (f + \mu)/2$ if $m \equiv 3\ (4)$. Then the maximal order of $\mathbf{Q}(\mu)$ is $\mathbf{Z} + \mathbf{Z}f^{-1}\omega$, so that $\mathcal{O}_\mu = \mathbf{Z} + \mathbf{Z}lf^{-1}\omega$ for some non-zero integer l. It follows from the primitivity of μ that $lf^{-1} \in \mathbf{Z}$, from which the first statement is immediate. The second statement is obvious. Finally, since $(1 + \mu)/2 \in \Lambda$ implies $N((1 + \mu)/2) = (1 + m)/4 \in \mathbf{Z}$, we have $(1 + \mu)/2 \in \Lambda$ only if $m \equiv 3\ (4)$, which completes the proof.

3.2. *The Map* Δ. For m and μ as above, let ϕ_μ: $\mathbf{Q}(\sqrt{-m}) \to \mathbf{Q}(\mu)$ be the canonical embedding sending $\sqrt{-m}$ to μ. For a $\mathbf{Z}$-submodule M of $\mathbf{Q}(\sqrt{-m})$, denote by M_μ, the image $\phi_\mu(M)$. Write $m = m_0 f^2$ where m_0 is square-free and let

$$\omega = \begin{cases} \sqrt{-m_0} & m_0 \equiv m \equiv 1, 2\ (4) \\ \dfrac{1 + \sqrt{-m_0}}{2} & m_0 \equiv m \equiv 3\ (4). \end{cases}$$

Denote by $\mathcal{O}_l = \mathbf{Z} + \mathbf{Z}l\omega$ the uniquely determined suborder of index l in the maximal order $\mathbf{Z} + Z\omega$ of $\mathbf{Q}(\sqrt{-m})$. Since $2 \nmid f$, $\mathcal{O}_f$ can also be written as

$$\mathcal{O}_f = \begin{cases} \mathbf{Z} + \mathbf{Z}\sqrt{-m} & m \equiv 1, 2\ (4) \\ \mathbf{Z} + \mathbf{Z}\dfrac{1 + \sqrt{-m}}{2} & m \equiv 3\ (4). \end{cases}$$

By Proposition 3.4, $\Lambda \cap \mathbf{Q}(\mu)$ equals $\mathcal{O}_{f,\mu}$ if $m \equiv 1, 2\ (4)$ or $m \equiv 3\ (4)$ and $(1 + \mu)/2 \notin \Lambda$, and $\mathcal{O}_{2f,\mu}$ otherwise.

When m is not square-free, we must extend our notion of the ideal class group of $\mathbf{Q}(\sqrt{-m})$. In the case of imaginary quadratic fields, there are several equivalent formulations. We shall consider the ideal class group of (fractional) proper $\mathcal{O}_f$-ideals (see §4.4 of [**14**]) where by proper $\mathcal{O}_f$-ideal we mean a fractional $\mathcal{O}_f$-ideal whose coefficient ring is $\mathcal{O}_f$ or equivalently, in terms of adeles, a "locally principal" $\mathcal{O}_f$-ideal. In this setting, two proper $\mathcal{O}_f$-ideals I, J are equivalent if and only if $I = \lambda J$ for some $\lambda \in \mathbf{Q}(\sqrt{-m})^{\times}$. All ideals are assumed to be non-zero. An equivalent notion and one which we shall also use is that of a regular ideal. We shall discuss regular $\mathcal{O}_f$-ideals in more detail somewhat later. For the equivalence of the notions of regular and proper $\mathcal{O}_f$-ideals, see §10 of [**4**] and Proposition 4.11 of [**14**]. Also note that the class number which arises here is also equal to the number of equivalence classes of primitive binary quadratic forms of discriminant $-4m$ (or $-m$) (see Chapter 15 of [**4**] or §2.7 of [**1**]).

PROPOSITION 3.5. *Let* $\mathcal{O}_\mu = \Lambda \cap \mathbf{Q}(\mu)$ *and let* J *be a fractional proper* $\mathcal{O}_\mu$*-ideal. Then* $\Lambda J \cap \mathbf{Q}(\mu) = J$.

Proof. Rehm's proof [**11**] of the analogous proposition for Hurwitz's quaternions remains valid here, however for the convenience of the reader we sketch the argument. We may assume that $J \subset \mathcal{O}_\mu$. By ΛJ we mean the $\mathbf{Z}$-module of $\mathfrak{A}$ generated by all elements of the form $\lambda\alpha$, $\lambda \in \Lambda$, $\alpha \in J$.

Since $1 \in \Lambda$ we have $J \subset \Lambda J \cap \mathbf{Q}(\mu)$. Conversely, since J is invertible, there is a $\mathbf{Z}$-module $J^{-1} \subset \mathbf{Q}(\mu)$ such that $J \cdot J^{-1} = \mathcal{O}_\mu$. Now $J \subset \mathcal{O}_\mu$ so that $\Lambda J \cap \mathbf{Q}(\mu) \subset \Lambda \cap \mathbf{Q}(\mu) = \mathcal{O}_\mu$. Thus

$$\begin{aligned} \Lambda J \cap \mathbf{Q}(\mu) &= (\Lambda J \cap \mathbf{Q}(\mu)) \cdot \mathcal{O}_\mu \\ &= (\Lambda J \cap \mathbf{Q}(\mu)) = J^{-1}J \subset (\Lambda JJ^{-1} \cap \mathbf{Q}(\mu)J^{-1}) \cdot J \\ &= (\Lambda\mathcal{O}_\mu \cap \mathbf{Q}(\mu)) = \mathcal{O}_\mu \cdot J = J. \end{aligned}$$

Fix m, μ as above and let G denote the ideal class group of proper $\mathcal{O}_f$-ideals in $\mathbf{Q}(\sqrt{-m})$. For any $\mu \in \Lambda$ with $\mu^2 = -m$, denote by $[\mu] = \{\varepsilon\mu\varepsilon^{-1} | \varepsilon \in \Lambda^\times\}$ and call $[\mu]$ the *bundle* of the root μ. Denote by $W = \{[\mu] | \mu \in \Lambda,\ \mu^2 = -m\}$, the set of *root bundles*. We want to define an action of G on W and from this to deduce a relation between $|G|$ and the number of primitive representations of $ax^2 + qy^2 + aqz^2$. Following [**11**], we define a map Δ: $G \times W \to W$ as follows.

For a proper $\mathcal{O}_f$-ideal I and a primitive root μ of $X^2 + m$ in Λ, the set ΛI_μ is a fractional left Λ-ideal and, by Proposition 3.1, it is principally generated, say $\Lambda I_\mu = \Lambda\kappa$ where $\kappa = \kappa(I, \mu)$ depends both upon the ideal I and the element μ. κ is determined up to left multiplication by elements of $\Lambda^\times$ and so $\nu = \kappa\mu\kappa^{-1}$ is determined up to inner automorphisms induced by the units of Λ. We shall subsequently show that $\kappa\mu\kappa^{-1} \in \Lambda$. Define Δ by $\Delta(I, [\mu]) = [\kappa\mu\kappa^{-1}]$.

Rehm's proof [**11**] that the map Δ is well-defined when Λ is Hurwitz's quaternions remains valid in our present context, however since this map is central to this paper, we shall sketch the proof.

With I, μ and κ as above, we see that

$$\Lambda\kappa\mu\kappa^{-1} = \Lambda I_\mu\mu\kappa^{-1} = \Lambda\mu I_\mu\kappa^{-1} \subset \Lambda I_\mu\kappa^{-1} = \Lambda\kappa\kappa^{-1} = \Lambda$$

since $I_\mu \subset \mathbf{Q}(\mu)$ centralizes μ (Proposition 2.1). Thus $\kappa\mu\kappa^{-1} \in \Lambda$ and since norm and trace are preserved under conjugation, $\Delta(I, [\mu]) = [\kappa\mu\kappa^{-1}] \in W$. We have already observed that $[\kappa\mu\kappa^{-1}]$ is independent of the choice of κ in $\Lambda I_\mu = \Lambda\kappa$.

The image of Δ depends only on the bundle $[\mu]$ and not on the choice of element used to define it. If $\varepsilon \in \Lambda^\times$ and $\nu = \varepsilon\mu\varepsilon^{-1} \in [\mu]$ we can choose $\kappa(I, \nu) = \kappa\varepsilon^{-1} = \kappa(I, \mu)\varepsilon^{-1}$ since $\Lambda I_\nu = \Lambda\varepsilon I_\mu\varepsilon^{-1} = \Lambda\kappa\varepsilon^{-1}$. Thus $\Delta(I, [\nu]) = [\kappa\varepsilon^{-1}\nu\varepsilon\kappa^{-1}] = [\kappa\mu\kappa^{-1}]$.

If $I = \mathcal{O}_f\alpha$, $\alpha \in \mathbf{Q}(\sqrt{-m})^\times$ is a principal ideal, then $I_\mu = \phi_\mu(I) = \mathcal{O}_{f,\mu}\beta$, $\beta = \phi_\mu(\alpha)$. We may choose $\kappa = \beta \in \mathbf{Q}(\mu)$, the centralizer of μ, and hence $\Delta(I, [\mu]) = [\mu]$. It follows that Δ depends only upon the ideal class and we may therefore restrict ourselves to integral proper $\mathcal{O}_f$-ideals. Thus Δ is a well-defined map. Also, if I, $J \in G$ and $[\mu] \in W$, then a straightforward computation shows that $\Delta(IJ, [\mu]) = \Delta(I, \Delta(J, [\mu]))$.

In particular, Δ induces an action of the ideal class group G on the set of root bundles W. Later, we shall restrict Δ to a subset of W on which the left kernel of Δ will consist of the set of principal proper $\mathcal{O}_f$-ideals. This will imply that all orbits under this action have the same size ($= |G|$). To proceed, we need information on the root bundles of primitive elements in Λ.

3.3. *The Root Bundles.* Throughout this section, let m be a positive integer not divisible by 4 and μ a primitive root of $X^2 + m$ in Λ.

PROPOSITION 3.6. *Let* $\mathcal{O}_\mu = \Lambda \cap \mathbf{Q}(\mu)$. *Then* $[\mu]$ *consists of* $|\Lambda^\times|/|\mathcal{O}_\mu^\times|$ *elements.*

Proof. By definition, $\Lambda^\times$ acts transitively on $[\mu]$ by conjugation. The stabilizer of μ consists of the set of $\varepsilon \in \Lambda^\times$ such that $\varepsilon\mu\varepsilon^{-1} = \mu$. By Proposition 2.1, $\varepsilon \in \mathbf{Q}(\mu)$ and hence $\varepsilon \in \mathcal{O}_\mu^\times$. Conversely, every element of $\mathcal{O}_\mu^\times$ stabilizes μ and is in $\Lambda^\times$. The result is now immediate.

REMARK 3.7. By Proposition 3.4, $|\mathcal{O}_\mu^\times| = 2$ with 2 exceptions: $|\mathcal{O}_\mu^\times| = 4$ if $m = 1$ and, $|\mathcal{O}_\mu^\times| = 6$ if $m = 3$ and $(1 + \mu)/2 \in \Lambda$.

The following is an elementary, but technical lemma which we require.

LEMMA 3.8. *Let* m *and* μ *be as above. Then*
(1) $m = N(\mu) \not\equiv 0 \pmod{q^2}$.
(2) *The prime* q *does not split in* $\mathbf{Q}(\sqrt{-m})$.

Proof. μ primitive in Λ implies that $4\mu \in \Lambda_0$ and 4μ is q-primitive in Λ. Let $4\mu = xi + yj + zk$, $x, y, z \in \mathbf{Z}$. Clearly $N(\mu) \equiv 0\ (q^2)$ if and only if $N(4\mu) \equiv 0\ (q^2)$, and $N(4\mu) = ax^2 + qy^2 + aqz^2$ where $a = 1$ if $q \equiv 3\ (4)$ and $a = 2$ if $q \equiv 5\ (8)$. $N(4\mu) \equiv 0\ (q^2)$ implies $q|x$ and hence, $y^2 + az^2 \equiv 0\ (q)$. Since $q \nmid a$, we see that $q|y \Leftrightarrow q|z$. Moreover, if $q \nmid yz$, then $y^2 + az^2 \equiv 0\ (q)$ yields $(\frac{-a}{q}) = -1$, a contradiction. Thus $q|x$, $q|y$, and $q|z$. But this contradicts that 4μ is q-primitive, hence (1). For (2), observe that since $q^2 \nmid m$, the prime q ramifies in $\mathbf{Q}(\sqrt{-m})$ if and only if $q \| m$. If $q \nmid m$, then since $16m = N(4\mu) \equiv ax^2\ (q)$, $q \nmid x$ and so $(\frac{-m}{q}) = (\frac{-a}{q}) = -1$ which implies that q is inert in $\mathbf{Q}(\sqrt{-m})$. This yields (2).

PROPOSITION 3.9. *Let* $\kappa \in \mathfrak{A}^\times$ *be such that* $\kappa\mu\kappa^{-1} \in \Lambda$. *Then* $\kappa\mu\kappa^{-1}$ *is primitive in* Λ.

Proof. Write $\kappa\mu\kappa^{-1} = c\nu$ with $c \in \mathbf{Z}$, $\nu \in \Lambda$ primitive and write $m = m_0 f^2$ with m_0 square-free. Since $N(\nu) \in \mathbf{Z}$ and $m = m_0 f^2 = N(\mu) = N(\kappa\mu\kappa^{-1}) = c^2 N(\nu)$, we have $c|f$. By Lemma 3.8, $q \nmid f$, and since $m \not\equiv 0\ (4)$, $2 \nmid f$. Thus $(f, 2q) = 1$ and so, by Lemma 2.4, there exists an $\eta \in \Lambda$ such that $\eta\mu\eta^{-1} = \kappa\mu\kappa^{-1}$ and $(N(\eta), f) = 1$. Now $\mu = c\eta^{-1}\nu\eta = c \cdot (\bar{\eta}\nu\eta/N(\eta)) \in \Lambda$, and since $(N(\eta), f) = 1$ and $c|f$, it follows that $\eta^{-1}\nu\eta \in \Lambda$. Since μ is primitive, $c = \pm 1$, and so $\kappa\mu\kappa^{-1}$ is primitive.

REMARK 3.10. It is clear that if μ is a primitive root of $X^2 + m$ in Λ, that the same is true of every element of $[\mu]$. In view of Proposition 3.9, we can (and shall) restrict the map Δ to the set of bundles of primitive roots of $X^2 + m$, and hence obtain an induced group action on this smaller set.

There is one further complication which is suggested by Proposition 3.4. We wish to further restrict our attention to the subset of the "primitive bundles" $[\mu]$ for which $\mathcal{O}_{f,\mu} = \Lambda \cap \mathbf{Q}(\mu)$ and still to be able to infer information about the set of all primitive bundles. There is no problem when $m \equiv 1, 2\ (4)$, so we restrict our attention to the case $m \equiv 3\ (4)$.

Let $\Lambda\tau_1$, $\Lambda\tau_2$, $\Lambda\tau_3$ be the three integral left Λ-ideals of norm 2 given in Proposition 3.3. We fix this notation, so that any subsequent reference to τ_j refers to these τ_j.

LEMMA 3.11. *Let* $\nu \in \Lambda$, $\mathrm{Tr}(\nu) = 0$. *Then there exists a* τ, *equal to one of the* τ_j, *for which* $\tau\nu\tau^{-1} \in \Lambda$.

Proof. If $N(\nu) \equiv 0\ (2)$, then by Proposition 3.3, $\nu \in \Lambda\tau$ for $\tau =$ some τ_j, $j = 1, 2,$ or 3. Since $\tau \in \Lambda$, it is clear that $\Lambda\tau \subset \tau^{-1}\Lambda\tau$, and hence that $\tau\nu\tau^{-1} \in \Lambda$. If $N(\nu) \equiv 1\ (2)$, then $N(1 + \nu) \equiv 0\ (2)$, so that $1 + \nu \in \tau^{-1}\Lambda\tau$ as above. Since $\tau^{-1}\Lambda\tau$ is an order, the result follows.

Let $\Gamma_j = \Lambda \cap \tau_j^{-1}\Lambda\tau_j$, $j = 1, 2, 3$. Since $\Lambda\tau_j$ has index 4 in Λ ($N(\tau_j) = 2$), and $\Lambda\tau_j \not\subset \Gamma_j \subset \Lambda$, Γ_j has index 1 or 2 in Λ. However, $\Lambda = \Gamma_j$ implies $\tau_j\Lambda = \Lambda\tau_j$ is a two-sided Λ-ideal of norm 2, which is impossible since even $\Lambda_2 = \Lambda \otimes_{\mathbf{Z}} \mathbf{Z}_2$ has no two-sided ideals of norm 2 [**16**]. Thus each Γ_j is an Eichler order of index 2 in Λ.

LEMMA 3.12. Γ_1, Γ_2, *and* Γ_3 *are distinct suborders of* Λ.

Proof. It suffices to show that their localizations $\Gamma_j \otimes_{\mathbf{Z}} \mathbf{Z}_2$ are distinct. By elementary divisors, we have $[\Lambda_2 : \Gamma_j \otimes_{\mathbf{Z}} \mathbf{Z}_2] = 2$. Since $\Gamma_j \otimes_{\mathbf{Z}} \mathbf{Z}_2 \subset \Lambda_2 \cap \tau_j^{-1}\Lambda_2\tau_j \subset \Lambda_2$, and since Λ_2 has no two-sided ideals of norm 2, we have $\Gamma_j \otimes_{\mathbf{Z}} \mathbf{Z}_2 = \Lambda_2 \cap \tau_j^{-1}\Lambda_2\tau_j$. Since the prime 2 splits in $\mathfrak{A}$, Λ_2 is isomorphic to $R = M_2(\mathbf{Z}_2)$, so that $\Gamma_j \otimes_{\mathbf{Z}} \mathbf{Z}_2 \simeq R \cap t_j^{-1}Rt_j$ where Rt_j, $j = 1, 2, 3$, are the three integral left R-ideals of norm 2. We may assume that

$$t_1 = \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}, \quad t_2 = \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} \quad \text{and} \quad t_3 = \begin{pmatrix} 1 & 1 \\ 0 & 2 \end{pmatrix}.$$

Then

$$L_1 = R \cap t_1^{-1}Rt_1 = \left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in R | b \equiv 0\ (2)\right\};$$

$$(3.1)\quad L_2 = R \cap t_2^{-1}Rt_2 = \left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in R | c \equiv 0\ (2)\right\};$$

$$L_3 = R \cap t_3^{-1}Rt_3 = \left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in R | a + b + c + d \equiv 0\ (2)\right\}.$$

These are clearly distinct, which establishes the claim.

PROPOSITION 3.13. *Let m be a positive integer not divisible by* 4 *and μ a primitive root of $X^2 + m$ in Λ. Then*

(1) *μ is an element of precisely one or all three of the Γ_js.*

(2) *$\mu \in \Gamma_1 \cap \Gamma_2 \cap \Gamma_3$ if and only if $(1 + \mu)/2 \in \Lambda$.*

(3) *If $m \equiv 1, 2\ (4)$ or $m \equiv 3\ (4)$ and $(1 + \mu)/2 \notin \Lambda$, then there is a unique $j = 1, 2,$ or 3 such that $\mu \in \Gamma_j$ (i.e., such that $\tau_j \mu \tau_j^{-1} \in \Lambda$).*

Proof. We have previously observed that $(1 + \mu)/2 \in \Lambda$ only if $m \equiv 3\ (4)$. The third statement is now immediate from the first two. Also observe that if p is an odd prime, $\Gamma_j \otimes_{\mathbf{Z}} \mathbf{Z}_p = \Lambda_p$, so by the local-global correspondence of orders, $\mu \in \Gamma_j$ if and only if $\mu \in \Gamma_j \otimes_{\mathbf{Z}} \mathbf{Z}_2$ and similarly, $(1 + \mu)/2 \in \Lambda$ if and only if $(1 + \mu)/2 \in \Lambda_2$.

It is an elementary exercise in group theory that if G is a group with subgroups H, K of finite index, then $H \cap K$ has finite index in G and $[G: H \cap K] \leq [G: H][G: K]$. Thus $\Gamma_1 \cap \Gamma_2 \cap \Gamma_3$ has at most index 8 in Λ. Clearly $(\Gamma_1 \cap \Gamma_2 \cap \Gamma_3) \otimes_{\mathbf{Z}} \mathbf{Z}_2 \subset \bigcap_{j=1}^{3}(\Gamma_j \otimes_{\mathbf{Z}} \mathbf{Z}_2)$, and since $\Gamma_j \otimes_{\mathbf{Z}} \mathbf{Z}_2 \simeq L_j$ (see (3.1)) and

$$L_1 \cap L_2 \cap L_3 = \left\{\begin{pmatrix} a & 2b \\ 2c & d \end{pmatrix} \in R | a \equiv d\ (2)\right\}$$

has index 8 in R, we have $(\Gamma_1 \cap \Gamma_2 \cap \Gamma_3) \otimes_{\mathbf{Z}} \mathbf{Z}_2 = \bigcap_{j=1}^{3}(\Gamma_j \otimes_{\mathbf{Z}} \mathbf{Z}_2)$. Thus, $\mu \in \Gamma_1 \cap \Gamma_2 \cap \Gamma_3$ if and only if $\mu \in \bigcap_{j=1}^{3}(\Gamma_j \otimes_{\mathbf{Z}} \mathbf{Z}_2)$. Since $\Lambda_2 \simeq R = M_2(\mathbf{Z}_2)$, we translate our questions to R. Under the isomorphism, let μ correspond to $A \in R$.

By Lemma 3.11, μ is an element of at least one Γ_j and hence A is an element of at least one L_j. It is clear from the characterization of the L_j and of $L_1 \cap L_2 \cap L_3$ above, that since $\mathrm{Tr}(A) = 0$, if A is contained in two of the L_js, it is contained in the third. This establishes the first claim.

Now if $A = \left(\begin{smallmatrix} a & 2b \\ 2c & d \end{smallmatrix}\right) \in L_1 \cap L_2 \cap L_3$, then since $m = N(A) \equiv ad \equiv -a^2 \equiv 0, 3\ (4)$ and $m \not\equiv 0\ (4)$, $2 \nmid a$, whence $(1 + A)/2 \in R$. Conversely, if $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in R$ with $\mathrm{Tr}(A) = 0$ and $(1 + A)/2 \in R$, then $2 \nmid a$, $2 \mid b$ and $2 \mid c$ which implies that $A \in L_1 \cap L_2 \cap L_3$. This completes the proof of the proposition.

Let m be a positive integer not divisible by 4 and write $m = m_0 f^2$ with m_0 square-free. Let $W_0 = \{[\mu] \mid \mu \in \Lambda,\ \mu^2 + m = 0, \text{ and } \mu \text{ primitive in } \Lambda\}$ Also, let $W_1 = \{[\mu] \in W_0 \mid \Lambda \cap \mathbf{Q}(\mu) = \mathcal{O}_{f,\mu}\}$ and let $W_2 = \{[\mu] \in W_0 \mid \Lambda \cap \mathbf{Q}(\mu) = \mathcal{O}_{2f,\mu}\}$. By Proposition 3.4, W_0 is the disjoint union of W_1 and W_2, and if $m \equiv 1, 2\ (4)$, $W_2 = \varnothing$. So we again restrict our attention to the case $m \equiv 3\ (4)$.

PROPOSITION 3.14. *There is a correspondence between the elements of* W_1 *and* W_2. *If* $m \equiv 7\ (8)$, *this correspondence is* 1–1, *while if* $m \equiv 3\ (8)$, $m > 3$, *the correspondence is* 1–3.

We observe that this correspondence is to be expected since if $h(\mathcal{O})$ denotes the order of the ideal class group of proper $\mathcal{O}$-ideals in $\mathbf{Q}(\sqrt{-m})$, then it is well known [**14**] that

$$h(\mathcal{O}_{2f}) = \begin{cases} 3h(\mathcal{O}_f) & \text{if } m \equiv 3\ (8),\ m > 3; \\ h(\mathcal{O}_f) & \text{if } m \equiv 7\ (8) \text{ or } m = 3. \end{cases}$$

Proof. Let $[\mu] \in W_2$. Then μ is a primitive root of $X^2 + m$ for which, by Proposition 3.4, $(1 + \mu)/2 \notin \Lambda$. By Proposition 3.13, there exists a unique $\tau_j (j = 1, 2, 3)$ such that $\tau_j \mu \tau_j^{-1} \in \Lambda$. It is a straightforward local computation which verifies that $[\tau_j \mu \tau_j^{-1}] \in W_1$. Conversely, suppose $[\mu] \in W_1$. Let $\mu_j = \tau_j \mu \tau_j^{-1}$, $j = 1, 2, 3$. By Proposition 3.13, $\mu_j \in \Lambda$ for all $j = 1, 2, 3$. Another easy local computation shows that if $m \equiv 3\ (8)$, then all three $[\mu_j]$ are in W_2, whereas if $m \equiv 7\ (8)$, there is a unique j such that $[\mu_j] \in W_2$.

It remains to show that these "maps" provide the desired correspondences. First, we consider the case of $m \equiv 7\ (8)$. Given $[\mu] \in W_2$, there exists a unique τ (equal to some τ_j) such that $[\tau \mu \tau^{-1}] \in W_1$, and given this bundle in W_1, there exists a unique ρ (equal to some τ_j) such that $[\rho\tau\mu(\rho\tau)^{-1}] \in W_2$. We claim that $[\rho\tau\mu(\rho\tau)^{-1}] = [\mu]$.

We have previously chosen the τ_j so that $\Lambda\tau_j \to \Lambda_2\tau_j \to Rt_j$ under localization and identification of Λ_2 with $R = M_2(\mathbf{Z}_2)$ where the t_j are as in (3.1). One checks that t_2t_1, t_1t_2 and t_2t_3 are all in $2 \cdot R^\times$. Thus, given any τ_j, there exists a τ_i such that $\tau_i\tau_j \in 2 \cdot \Lambda_2^\times$, and since the τ's all have norm 2, $\tau_i\tau_j \in \Lambda_p^\times = 2 \cdot \Lambda_p^\times$ for all primes $p > 2$. Now for the τ chosen above, there exists a ξ (equal to some τ_j) such that $\xi\tau \in 2 \cdot \Lambda_p^\times$ for all primes p. From the local-global correspondence, it follows that $\xi\tau \in 2 \cdot \Lambda^\times$, and hence that $[\xi\tau\mu(\xi\tau)^{-1}] \in W_2$. Since ρ is the unique τ_j such that $[\rho\tau\mu(\rho\tau)^{-1}] \in W_2$, we have $\xi = \rho$, and our claim is established. A similar argument establishes the other half of the 1–1 correspondence in the case $m \equiv 7\ (8)$.

Next, suppose that $m \equiv 3\ (8)$. Exactly as above, the composite "map" $W_2 \to W_1 \to W_2$ is the identity. Let $[\mu] \in W_1$. As we saw above, $\mu_j \equiv \tau_j \mu \tau_j^{-1} \in \Lambda$ and $[\mu_j] \in W_2$ for all j. We need to verify that all the bundles $[\mu_j]$ correspond (i.e., map back) to $[\mu]$ and that the three bundles $[\mu_j]$ are, in fact, distinct. In answer to the first, we see that given any $[\mu_j]$ there exists a unique ρ (equal to some τ_k) such that $[\rho\mu_j\rho^{-1}] \in W_1$. On the other hand, there exists a ξ (equal to some τ_k) such that $\xi\tau_j \in 2 \cdot \Lambda^\times$ and hence for which $[\xi\mu_j\xi^{-1}] = [\mu] \in W_1$. Thus $\rho = \xi$ by uniqueness and so each $[\mu_j]$ corresponds to $[\mu]$. If the three bundles $[\mu_j]$ are not distinct, then two of them must coincide, say $[\mu_j] = [\mu_k]$. But this is true if and only if $\mu_j = \varepsilon\mu_k\varepsilon^{-1}$ for some $\varepsilon \in \Lambda^\times$, and hence if and only if $\alpha = \tau_j^{-1}\varepsilon\tau_k$ normalizes μ. By Proposition 2.1, $\alpha \in \mathbf{Q}(\mu)$. Now $2\alpha \in \Lambda \cap \mathbf{Q}(\mu) = \mathbf{Z} + \mathbf{Z}(1 + \mu)/2$ and using this and the fact that $N(2\alpha) = 4$ (and $m > 3$) we deduce that $\alpha = \pm 1$. Thus $\Lambda\tau_j = \Lambda\varepsilon\tau_k = \Lambda\tau_k$, whence $j = k$. This completes the proof.

3.4. *The set $T_{\mu,\nu}$.* To recall the notation, let

$$\mathfrak{A} = \left(\frac{-a, -q}{\mathbf{Q}}\right)$$

with $a = 1$ if $q \equiv 3\ (4)$ and $a = 2$ if $q \equiv 5\ (8)$; let Λ be the maximal order given in (2.1). Let m be a positive integer not divisible by 4 and let μ, ν be primitive roots of $X^2 + m$ in Λ.

In order to obtain information on the number of orbits into which the set of root bundles W_0 decomposes under the action of the ideal class group G, we must analyze the set $T_{\mu,\nu} = \{\lambda \in \Lambda \mid \lambda\mu = \nu\lambda\}$.

$\Lambda T_{\mu,\nu}$, the $\mathbf{Z}$-module generated by all elements of the form γt, $\gamma \in \Lambda$, $t \in T_{\mu,\nu}$, is an integral left Λ-ideal and so by Proposition 3.1 is principally generated, say $\Lambda T_{\mu,\nu} = \Lambda\rho$. We shall show that the only possible prime divisors of the norm of ρ, $N(\rho)$, are 2 and q and we shall discuss the conditions for and implications of each occurrence.

LEMMA 3.15. *With the notation as above, the only possible prime divisors of $N(\rho)$ are 2 and q.*

Proof. Since $T_{\mu,\nu} = T_{\alpha\mu,\alpha\nu}$ for $\alpha \in \mathbf{Q}^\times$ and 4μ, $4\nu \in \Lambda_0$, we may assume that $\mu, \nu \in \Lambda_0$ and are p-primitive for all primes $p > 2$. Suppose that there is a prime $p \neq 2, q$ such that $N(\rho) \equiv 0 \pmod{p}$. Since ρ is a common right divisor of every element of $T_{\mu,\nu}$, it follows that $N(\gamma) \equiv 0 \pmod{p}$ for all $\gamma \in \Lambda T_{\mu,\nu}$. It is easy to check that $\lambda\mu + \nu\lambda \in T_{\mu,\nu}$ for any

$\lambda \in \Lambda$. Put

$$\gamma_1 = a(\mu + \nu) + i(i\mu + \nu i)$$
$$\gamma_2 = q(\mu + \nu) + j(j\mu + \nu j)$$
$$\gamma_3 = aq(\mu + \nu) + k(k\mu + \nu k).$$

Then $\gamma_1, \gamma_2, \gamma_3 \in \Lambda T_{\mu,\nu}$. Setting $\nu = ui + vj + wk \in \Lambda_0$ (p-primitive), and $N(\gamma_l) \equiv 0\,(p)$ for $l = 1, 2, 3$ we have the system

$$A\begin{pmatrix} u^2 \\ v^2 \\ w^2 \end{pmatrix} \equiv 0\,(p) \quad \text{where} \quad A = \begin{pmatrix} 0 & 1 & a \\ 1 & 0 & q \\ a & q & 0 \end{pmatrix}.$$

Since $\det(A) = 2aq$, one can view A as an element of $\mathrm{GL}(3, \mathbf{Z}/p\mathbf{Z})$, hence u, v, w must be divisible by p contradicting p-primitivity of ν. This completes the proof.

LEMMA 3.16. *Let the notation be as above. If $q \mid m$ then $q \nmid N(\rho)$ for any primitive integral roots μ, ν. Conversely, if $q \nmid m$ then there exist μ, ν primitive roots of $X^2 + m$ in Λ with $\Lambda \cdot T_{\mu,\nu} = \Lambda\rho$ and $N(\rho) = q$.*

Proof. Let μ, ν be given. By Proposition 2.2, $T_{\mu,\nu} = \lambda_0\mathbf{Q}(\mu) \cap \Lambda$ where λ_0 is any element of $\mathfrak{A}^\times$ such that $\lambda_0\mu\lambda_0^{-1} = \nu$. We may assume that $\lambda_0 = w + xi + yj + zk$ is a primitive element of Λ_0.

Suppose $q \mid m$. Since ρ is a common right divisor of every element of $T_{\mu,\nu}$, we need only show that there exists an element of $T_{\mu,\nu}$ with norm not divisible by q. Thus we consider elements of the form $\lambda_0(r + s\mu)$; r, $s \in \mathbf{Q}$.

If $N(\lambda_0) \not\equiv 0\,(q)$ then λ_0 will do, so we assume $N(\lambda_0) = w^2 + ax^2 + qy^2 + aqz^2 \equiv 0\,(q)$. Since $(\frac{-a}{q}) = -1$, we must have $w \equiv x \equiv 0\,(q)$, and since λ_0 is primitive in Λ_0, $N(\lambda_0) \not\equiv 0\,(q^2)$. As in the previous lemma, we may assume that μ, $\nu \in \Lambda_0$ and are p-primitive for all primes $p > 2$. Let $\mu = ri + sj + tk \in \Lambda_0$. Using the q-primitivity of μ and that $m = N(\mu) = ar^2 + qs^2 + aqt^2 \equiv 0\,(q)$, we have $q \mid r$, $q^2 \nmid m$ and hence that $N(\lambda_0\mu/q) \not\equiv 0\,(q)$. Moreover, we easily see that $\lambda_0\mu/q \in \Lambda$ since it is in Λ_p for all primes p-recall, that since q ramifies in $\mathfrak{A}$, $\Lambda_q = \{\alpha \in \mathfrak{A}_q \mid N(\alpha) \in \mathbf{Z}_q\}$. Thus $\lambda_0\mu/q \in \Lambda \cap \lambda_0\mathbf{Q}(\mu) = T_{\mu,\nu}$.

To prove the converse, we assume $q \nmid m$. Let μ be a primitive root of $X^2 + m$ in Λ and $\nu = j\mu j^{-1}$. By Propositions 3.2 and 3.9, ν is also a primitive root of $X^2 + m$ in Λ. We show that every element of $T_{\mu,\nu}$ has norm divisible by q.

$T_{\mu,\nu} = T_{4\mu,4\nu}$, so letting $4\mu = ri + sj + tk$, every element of $T_{\mu,\nu}$ is of the form

$$\gamma = j \cdot \left(\frac{w}{x} + \frac{y}{z}(ri + sj + tk) \right)$$

where $w, x, y, z \in \mathbf{Z}$, $(w, x) = (y, z) = 1$. Also note that 4μ is p-primitive for all primes $p > 2$. We shall show that there is not choice of w, x, y, z for which $\gamma \in \Lambda$ and $N(\gamma) \not\equiv 0\ (q)$.

$$N(\gamma) = q\left(\frac{(wz)^2 + 16m(xy)^2}{(xz)^2} \right),$$

so in order to have $N(\gamma) \not\equiv 0\ (q)$, we must have $q \mid xz$. However, since $\gamma \in \Lambda$ implies $N(\gamma) \in \mathbf{Z}$, we must also have $(wz)^2 + 16m(xy)^2 \equiv 0\ (q)$. Since $16m = ar^2 + qs^2 + aqt^2 \equiv ar^2\ (q)$ and since $q \nmid m$, $q \nmid r$. Thus $(wz)^2 + a(rxy)^2 \equiv 0\ (q)$. However, $(\frac{-a}{q}) = -1$ which implies that $q \mid wz$ and $q \mid xy$. Now $q \mid w \Leftrightarrow q \mid y$. If $q \mid w$ (and hence $q \mid y$), then $q \nmid xz$ so that $N(\gamma) \equiv 0\ (q)$. Thus we may assume that $q \nmid w$, $q \nmid y$, $q \mid x$, $q \mid z$. Now

$$\gamma = \frac{-qsy}{z} + \frac{qty}{z} i + \frac{w}{x} j - \frac{ry}{z} k,$$

and since the coefficient of j is w/x with $q|x$ and $q \nmid w$, $\gamma \notin \Lambda$. Thus every element of $T_{\mu,\nu}$ has norm divisible by q.

Finally, we consider the ideal $\Lambda T_{\mu,\nu}$. A typical element is of the form $\Sigma \lambda_i t_i$ with $\lambda_i \in \Lambda$, $t_i \in T_{\mu,\nu}$. By Proposition 3.2 we may write $\lambda_i t_i = \lambda_i' j$ for some $\lambda_i' \in \Lambda$ and so j is a common right divisor of every element of $\Lambda T_{\mu,\nu}$. Thus $\Lambda\rho = \Lambda T_{\mu,\nu} \subset \Lambda j$. Since $j \in T_{\mu,\nu}$ the opposite inclusion is immediate, and this completes the proof.

With ρ as above, we consider the case of $N(\rho) = 2^n$. Let ν be a primitive root of $X^2 + m$ in Λ. We are interested in characterizing the bundle $[\rho\nu\rho^{-1}]$ when $\rho\nu\rho^{-1} \in \Lambda$. By Proposition 3.3, we may write $\rho = \sigma_n\sigma_{n-1} \cdots \sigma_1$ where each σ_l is one of the τ_j of Proposition 3.3 (the generators of the integral left Λ-ideals of norm 2). Let $\nu_0 = \nu$ and $\nu_l = \sigma_l \nu_{l-1} \sigma_l^{-1}$, $1 \le l \le n$. Since conjugation by σ_l does not induce an automorphism of Λ, it is not clear that $\nu_l \in \Lambda$. We begin with

LEMMA 3.17. *Let the notation be as above, and assume that* $\rho\nu\rho^{-1} \in \Lambda$. *Then we may assume* $\nu_l \in \Lambda$ *for all* l, $0 \le l \le n$.

Proof. The general idea is that if $\nu_{l-1} \in \Lambda$ and $\nu_l \notin \Lambda$, then since $\nu_n = \rho\nu\rho^{-1} \in \Lambda$ there is a smallest $p \ge 1$ such that $\nu_{l+p} \in \Lambda$. In fact, we shall show that $\nu_{l+1} \in \Lambda$ and $[\nu_{l+1}] = [\nu_{l-1}]$, so that we may write $\rho = \varepsilon\sigma_n' \cdots \sigma_{l+2}'\sigma_{l-1} \cdots \sigma_1$ for some $\varepsilon \in \Lambda^\times$, eliminating that portion of the ν_l's outside Λ.

Formally we proceed by induction on n. For $n = 0$ the result is clear. Now assume $n > 0$ and that the lemma is true for any ρ with $\rho\nu\rho^{-1} \in \Lambda$ and $N(\rho) = 2^h$, $h < n$. Suppose that $\nu_0, \nu_1 \cdots \nu_{l-1} \in \Lambda$ and $\nu_l \notin \Lambda$. Since $\nu_n \in \Lambda$, $l < n$, so there is a smallest $p \geq 1$ such that $\nu_{l+p} \in \Lambda$. We claim that $\sigma_{l+p}\sigma_{l+p-1} \in 2 \cdot \Lambda^\times$ from which it follows that $[\nu_{l+p}] = [\nu_{l+p-2}]$ and hence that $\nu_{l+p-2} \in \Lambda$. By the minimality of p, we have $p = 1$ so that $[\nu_{l+1}] = [\nu_{l-1}]$. If $\sigma_{l+1}\sigma_l = 2\omega$ for some $\omega \in \Lambda^\times$, then

$$\nu_{l+1} = 2\omega\nu_{l-1}(2\omega)^{-1} = \omega\nu_{l-1}\omega^{-1}$$

and

$$\nu_{l+2} = \sigma_{l+2}\nu_{l+1}\sigma_{l+2}^{-1} = \sigma_{l+2}\omega\nu_{l-1}\omega^{-1}\sigma_{l+2}^{-1}.$$

By Proposition 3.3, $\sigma_n\sigma_{n-1} \cdots \sigma_{l+2}\omega = \varepsilon\sigma_n' \cdots \sigma_{l+2}'$ for some $\varepsilon \in \Lambda^\times$ and where each σ_k' is one of the τ_j's. Setting $\rho' = \sigma_n' \cdots \sigma_{l+2}'\sigma_{l-1} \cdots \sigma_1$, we have $[\rho'\nu\rho'^{-1}] = [\rho\nu\rho^{-1}]$, and we are done by induction. It remains only to verify the claim.

As we saw in Proposition 3.14, given a τ_j, there exists a τ_i such that $\tau_i\tau_j \in 2 \cdot \Lambda^\times$. To show that if $\sigma_{l+p}\sigma_{l+p-1} \notin 2\Lambda^\times$ implies $\nu_{l+p} \notin \Lambda$ reduces to a local question at the prime 2 which, using the t_i of (3.1), is easily resolved.

3.5. *The Image of $\mathcal{O}_f$-ideals in Λ.* Let m be a positive integer not divisible by 4 and write $m = m_0 f^2$ with m_0 square-free. Let $\mathcal{O}_f$ be the uniquely determined suborder of index f in the maximal order of $\mathbf{Q}(\sqrt{-m})$.

We have previously defined the sets:

$$W_0 = \{[\mu] \mid \mu \in \Lambda,\ \mu^2 + m = 0, \text{ and } \mu \text{ primitive in } \Lambda\},$$

$$W_1 = \{[\mu] \in W_0 \mid \Lambda \cap \mathbf{Q}(\mu) = \mathcal{O}_{f,\mu}\} \quad \text{and}$$

$$W_2 = \{[\mu] \in W_0 \mid \Lambda \cap \mathbf{Q}(\mu) = \mathcal{O}_{2f,\mu}\}.$$

Recall, that if $m \equiv 1, 2$ (4), then $W_2 = \varnothing$. By Remark 3.10, the map Δ induces a group action of the ideal class group G of proper $\mathcal{O}_f$-ideals on the set W_0. We shall later show that this action restricts to one on W_1. For the moment, we content ourselves with properties of W_1.

Let $[\mu] \in W_1$. In this section, we closely examine the correspondence between proper $\mathcal{O}_f$-ideals I and the generator of the left Λ-ideal ΛI_μ. In the case of Hurwitz's quaternions, the following lemma is implicit in Venkov's work (see p. 242 of [**15**]) and a proof for that case is given in [7].

LEMMA 3.18. *Let I be a proper $\mathcal{O}_f$-ideal and assume that $\Lambda I_\mu = \Lambda\kappa$. Then $\mathcal{N}(I) = N(\kappa)$ (i.e., the norm of the fractional ideal I is equal to the quaternion norm of the generator of the ideal ΛI_μ).*

Proof. It is clear that the restriction of the quaternion norm to $\mathbf{Q}(\mu)$ is the "field" norm from $\mathbf{Q}(\mu)$ to $\mathbf{Q}$. We may assume that I is an integral ideal so that in this case $\mathcal{N}(I) = [\mathcal{O}_f\colon I] = [\mathcal{O}_{f,\mu}\colon I_\mu]$. It now follows easily (see §24 of [**12**]) that $N(\kappa) = N(\Lambda\kappa) = N(\Lambda I_\mu) = [\mathcal{O}_{f,\mu}\colon I_\mu]\cdot\mathbf{Z}$ where N here represents both the norm of elements and of ideals, which completes the proof.

We now discuss some implications of this proposition. Let the notation be as above and let $\mathcal{O}$ denote the maximal order of $\mathbf{Q}(\sqrt{-m})$. Recall [**4**], (Th 10.19) that there is a 1–1 correspondence between regular ideals of $\mathcal{O}$ and $\mathcal{O}_f$ where by a regular $\mathcal{O}$-ideal we mean an integral ideal I with $[\mathcal{O}\colon I]$ relatively prime to f, and by a regular $\mathcal{O}_f$-ideal we mean $\mathcal{O}_f \cap I$ where I is a regular $\mathcal{O}$-ideal. Moreover under this correspondence $[\mathcal{O}\colon I] = [\mathcal{O}_f\colon \mathcal{O}_f \cap I]$.

The prime $2\mathbf{Z}$ ramifies in $\mathcal{O}$ if and only if $m \equiv 1, 2\ (4)$, splits completely if $m \equiv 7\ (8)$, and is inert if $m \equiv 3\ (8)$. By Lemma 3.8, the prime $q\mathbf{Z}$ ramifies if and only if $q \| m$. Since $m \not\equiv 0\ (4)$, both 2 and q are prime to f, whence any prime divisor of $2\mathbf{Z}$ or $q\mathbf{Z}$ is a regular ideal.

It follows that if $\mathcal{P}_2 \mid 2\mathcal{O}$ or $q \mid m$ and $\mathcal{P}_q \mid q\mathcal{O}$, then $\mathcal{P}_2 \cap \mathcal{O}_f$ and $\mathcal{P}_q \cap \mathcal{O}_f$ are regular $\mathcal{O}_f$-ideals of norms 2 and q respectively. Moreover, if $q \nmid m$, then there are no $\mathcal{O}_f$-ideals of norm q since such an ideal would necessarily be regular and hence, would imply the existence of an $\mathcal{O}$-ideal of norm q. By Lemma 3.8, this is impossible since q is inert in $\mathbf{Q}(\sqrt{-m})$.

COROLLARY 3.19. *If $q \mid m$, $\mathcal{P}$ is a prime divisor of $q\mathcal{O}_f$ in $\mathcal{O}_f$ and $[\mu] \in W_1$, then $\Lambda\mathcal{P}_\mu = \Lambda j$.*

Proof. By Lemma 3.18, $\Lambda\mathcal{P}_\mu = \Lambda\kappa$ with $\kappa \in \Lambda$ and $N(\kappa) = q$. By Proposition 3.2, $\kappa = \kappa' j$ for some $\kappa' \in \Lambda$. Since $N(\kappa) = q = N(j)$ we have $N(\kappa') = 1$ so that $\kappa' \in \Lambda^\times$ and $\Lambda\kappa = \Lambda j$ as desired.

COROLLARY 3.20. *Let $m \equiv 1, 2\ (4)$ and μ a primitive root of $X^2 + m$ in Λ. If $\mathcal{P}$ is a prime divisor of $2\mathcal{O}_f$ in $\mathcal{O}_f$, then $\Lambda\mathcal{P}_\mu = \Lambda\tau$, where $\Lambda\tau$ is the unique ideal of norm 2 for which $\tau\mu\tau^{-1} \in \Lambda$.*

Proof. $\Lambda\mathcal{P}_\mu = \Lambda\kappa$ where $N(\kappa) = 2$. By Proposition 3.3, $\Lambda\kappa = \Lambda\tau_1$, $\Lambda\tau_2$, or $\Lambda\tau_3$. By Proposition 3.13, there is a unique τ_i such that $\tau_i\mu\tau_i^{-1} \in \Lambda$, and since $\kappa\mu\kappa^{-1} \in \Lambda$, $\Lambda\kappa = \Lambda\tau_i$.

Let $m \equiv 7\ (8)$ and $[\mu] \in W_1$. By Proposition 3.13, $\tau_i\mu\tau_i^{-1} \in \Lambda$ for all three τ_i as above, but by Proposition 3.14, there is a unique τ_i (call it τ) for which $[\tau\mu\tau^{-1}] \in W_2$. Let $\{\rho, \sigma, \tau\} = \{\tau_1, \tau_2, \tau_3\}$.

COROLLARY 3.21. *Let* $m \equiv 7$ (8) *and the notation be as above and let* $2\mathcal{O}_f = \mathcal{P}_1\mathcal{P}_2$ *be the prime factorization of* $2\mathcal{O}_f$ *in* $\mathcal{O}_f$. *Then* $\{\Lambda\mathcal{P}_{1,\mu}, \Lambda\mathcal{P}_{2,\mu}\} = \{\Lambda\rho, \Lambda\sigma\}$.

Proof. We may take

$$\mathcal{P}_1 = 2\mathcal{O}_f + \mathcal{O}_f\left(\frac{1+\sqrt{-m}}{2}\right) \quad \text{and} \quad \mathcal{P}_2 = 2\mathcal{O}_f + \mathcal{O}_f\left(\frac{1-\sqrt{-m}}{2}\right).$$

Let $\Lambda\mathcal{P}_{j,\mu} = \Lambda\kappa_j$, $j = 1, 2$. $(1 \pm \mu)/2 \in \Lambda\kappa_j$ implies $(1+\mu)/2 \in \kappa_j^{-1}\Lambda\kappa_j$, which in turn implies that $[\kappa_j\mu\kappa_j^{-1}] \in W_1$. Thus $\{\Lambda\mathcal{P}_{1,\mu}, \Lambda\mathcal{P}_{2,\mu}\} \subset \{\Lambda\rho, \Lambda\sigma\}$. We observe that $\Lambda\mathcal{P}_{1,\mu} \neq \Lambda\mathcal{P}_{2,\mu}$ otherwise $(1+\mu)/2$, $(1-\mu)/2 \in \Lambda\kappa_j$ which implies $1 \in \Lambda\kappa_j$, a contradiction. This completes the proof.

3.6. *Determination of the orbits.* Let m be a positive integer not divisible by 4 and write $m = m_0 f^2$ with m_0 square-free. Let $\mathcal{O}_f$ be the unique suborder of index f in the maximal order of $\mathbf{Q}(\sqrt{-m})$ and G the ideal class group of proper $\mathcal{O}_f$-ideals. At the beginning of the last section, we redefined the sets W_0, W_1, W_2 and remarked that the map Δ restricted to a map $\Delta\colon G \times W_0 \to W_0$. We now show that we can further restrict Δ to a map $\Delta\colon G \times W_1 \to W_1$. There is no issue if $m \equiv 1, 2$ (4) since, in that case $W_0 = W_1$, so we restrict our attention to $m \equiv 3$ (4).

PROPOSITION 3.22. *Let* $m \equiv 3$ (4) *be as above and let* $[\mu] \in W_1$. *Then* $\Delta(I, [\mu]) \in W_1$ *for all* $I \in G$.

Proof. Let $I \in G$. We may assume that I is an integral proper $\mathcal{O}_f$-ideal and write $I = J\mathcal{P}_1^r\mathcal{P}_2^s$ where $2 \nmid [\mathcal{O}_f\colon J]$, $2\mathcal{O}_f = \mathcal{P}_1\mathcal{P}_2$ if $m \equiv 7$ (8) and $r, s \geq 0$. If $m \equiv 3$ (8), we may assume that $I = J$. Set $[\nu] = \Delta(\mathcal{P}_1^r\mathcal{P}_2^s, [\mu])$. If $m \equiv 3$ (8), $\nu = \mu$, and it is obvious that $[\nu] \in W_1$, while if $m \equiv 7$ (8), Lemma 3.21 implies $[\nu] \in W_1$. Thus, $\Delta(I, [\mu]) = \Delta(J, [\nu]) = [\kappa\nu\kappa^{-1}]$ where $\Lambda J_\nu = \Lambda\kappa$. Note that $2 \nmid N(\kappa)$. Now $[\kappa\nu\kappa^{-1}] \in W_1$ if an only if $\tau(\kappa\nu\kappa^{-1})\tau^{-1} \in \Lambda$ for all $\tau = \tau_k$, the generators of the left Λ-ideals of norm 2. As we previously observed, since $N(\tau) = 2$, the above will be true if and only if $\tau(\kappa\nu\kappa^{-1})\tau^{-1} \in \Lambda_2$ for all τ as above. Now by Proposition 3.3, $\tau\kappa = \kappa'\tau'$ for some $\kappa' \in \Lambda$ $(2 \nmid N(\kappa'))$ and τ' one of the τ_k's. Thus $\tau(\kappa\nu\kappa^{-1})\tau^{-1} = (\kappa'\tau')\nu(\kappa'\tau')^{-1}$. $[\nu] \in W_1$ implies that $\tau'\nu\tau'^{-1} \in \Lambda$ and, since $2 \nmid N(\kappa')$, $\kappa' \in \Lambda_2^\times$ so that $\kappa'\tau'\nu(\kappa'\tau')^{-1} \in \Lambda_2$, which completes the proof.

Thus the map Δ induces a group action of G on W_1.

LEMMA 3.23. *Let m be a positive integer not divisible by 4 and write $m = m_0 f^2$ with m_0 square-free. Let $[\mu] \in W_1$. Let I be a proper $\mathcal{O}_f$-ideal and suppose that $\Delta(I, [\mu]) = [\rho\nu\rho^{-1}]$ where $[\nu] \in W_1$ and $N(\rho) = 2^n$, $n \geq 0$. Then $[\nu]$ and $[\rho\nu\rho^{-1}]$ are in the same orbit under the action of G.*

Proof. If $m \equiv 3\ (8)$, then since 2 is inert in $\mathbf{Q}(\sqrt{-m})$, $I = 2^r J$ where $r \geq 0$ and $2 \nmid [\mathcal{O}_f : J]$ and so $\rho\nu\rho^{-1} = \nu$. Thus we consider $m \not\equiv 3\ (8)$.

By Proposition 3.3, ρ may be written in the form $\rho = \sigma_n \sigma_{n-1} \cdots \sigma_1$ where each σ_l is one of the generators τ_1, τ_2, or τ_3 of the left Λ-ideals of norm 2. Let $\nu_0 = \nu$ and $\nu_l = \sigma_l \nu_{l-1} \sigma_l^{-1}$, $1 \leq l \leq n$. By Lemma 3.17, we may assume that all $\nu_l \in \Lambda$. If, in addition, each $[\nu_l] \in W_1$, then it follows from Propositions 3.13, 3.14 and Corollaries 3.20, 3.21 that given $[\nu_{l-1}] \in W_1$, there exists a prime $\mathcal{P} \mid 2\mathcal{O}_f$ such that $\Delta(\mathcal{P}, [\nu_{l-1}]) = [\nu_l]$. From this it follows that $[\nu]$ and $[\rho\nu\rho^{-1}]$ are in the same orbit.

Now, we show that we can reduce to the above case. Since $W_0 = W_1$ if $m \equiv 1, 2\ (4)$, we may restrict to $m \equiv 7\ (8)$. Suppose that $[\nu_0], \ldots, [\nu_{l-1}] \in W_1$ and $[\nu_l] \notin W_1$. By Proposition 3.22, $l < n$. Now it follows Proposition 3.13 and from the proof of Proposition 3.14 that together, $[\nu_{l+1}] \in \Lambda$ and $[\nu_l] \in W_2$ imply $\sigma_{l+1}\sigma_l \in 2\Lambda^\times$, whence $[\nu_{l+1}] = [\nu_{l-1}] \in W_1$. The proof is completed by induction on n.

We have shown that the map Δ restricts to a map (also called Δ), Δ: $G \times W_1 \to W_1$. The next proposition says that all of the orbits of the group action have the same ($= |G|$) size.

PROPOSITION 3.24. *The left kernel of Δ is the set of principal proper $\mathcal{O}_f$-ideals.*

Proof. If $\Delta(I, [\mu]) = [\mu]$, then $\Lambda I_\mu = \Lambda\kappa$ where κ may be chosen so that $\kappa\mu\kappa^{-1} = \mu$. By Proposition 2.1, $\kappa \in \mathbf{Q}(\mu)$ so that $\mathcal{O}_{f,\mu}\kappa$ is a fractional $\mathcal{O}_{f,\mu}$-ideal in $\mathbf{Q}(\mu)$. By Proposition 3.5,

$$I_\mu = \Lambda I_\mu \cap \mathbf{Q}(\mu) = \Lambda \mathcal{O}_{f,\mu}\kappa \cap \mathbf{Q}(\mu) = \mathcal{O}_{f,\mu}\kappa.$$

Thus I_μ and $I = \phi_\mu^{-1}(I_\mu)$ are principal ideals. This completes the proof of the assertion.

Note that here we use $\phi_\mu^{-1}\phi_\mu(\mathcal{O}_f) = \mathcal{O}_f$, which is not true if $[\mu] \in W_2$.

Now we completely describe the orbits of G acting on W_1.

PROPOSITION 3.25. *Let m be as above and $[\mu] \in W_1$. If $q \mid m$, then*

$$W_1 = \{\Delta(I, [\mu]) \mid I \in G\}; \text{ while if } q \nmid m, \text{ then}$$
$$W_1 = \{\Delta(I, [\mu]) \mid I \in G\} \cup \{\Delta(I, [j\mu j^{-1}]) \mid I \in G\}.$$

Proof. The construction below is analogous to the one given in [**11**]. Let $[\nu]$ be any other element of W_1. The set $T_{\nu,\mu} = \{\lambda \in \Lambda | \lambda\nu = \mu\lambda\}$ is a free $\mathbf{Z}$-module of rank 2 (see discussion prior to Lemma 2.4), say $T_{\nu,\mu} = \mathbf{Z}\xi + \mathbf{Z}\eta$. Note that by Lemma 2.4, we may and do assume that $N(\eta) = \eta\bar{\eta}$ is relatively prime to f. Put $I_\mu = \mathcal{O}_\mu\xi\bar{\eta} + \mathcal{O}_\mu\eta\bar{\eta}$ where $\mathcal{O}_\mu = \Lambda \cap \mathbf{Q}(\mu) = \mathcal{O}_{f,\mu}$. It is easy to see that $\alpha \in T_{\nu,\mu}$ iff $\bar{\alpha} \in T_{\mu,\nu}$ so that $\xi\bar{\eta}$ centralizes μ, and so by Propositions 2.1 and 3.5, $\xi\bar{\eta} \in \mathbf{Q}(\mu) \cap \Lambda = \mathcal{O}_\mu$. Trivially, $\eta\bar{\eta} \in \mathbf{Q} \cap \Lambda \subset \mathcal{O}_\mu$. It follows that I_μ is an integral $\mathcal{O}_\mu$-ideal.

$$\begin{aligned}\Lambda I_\mu &= \Lambda\left(\mathcal{O}_\mu\xi\bar{\eta} + \mathcal{O}_\mu\eta\bar{\eta}\right) = \left(\Lambda\xi + \Lambda\eta\right)\bar{\eta} \\ &= \left(\Lambda T_{\nu,\mu}\right)\bar{\eta} \quad \text{and letting } \Lambda T_{\nu,\mu} = \Lambda\rho \\ &= \Lambda\rho\bar{\eta}.\end{aligned}$$

Let $I = \phi_\mu^{-1}(I_\mu)$. By Lemma 3.15, the only possible prime divisors of $N(\rho)$ are 2, q so that $(N(\rho\bar{\eta}), f) = 1$. Since by Lemma 3.18, $[\mathcal{O}_\mu\colon I_\mu] = N(\rho\bar{\eta})$, I is a regular (i.e., proper) $\mathcal{O}_f$-ideal.

Suppose $q \mid m$. By Lemma 3.16 we may assume that $N(\rho) = 2^n$, $n \geq 0$. If $n = 0$, $\Lambda I_\mu = \Lambda\bar{\eta}$ so that $\Delta(I, [\mu]) = [\bar{\eta}\mu\bar{\eta}^{-1}] = [\nu]$ as desired. If $n > 0$, then by Lemma 3.23 there is a $J \in G$ such that $\Delta(JI, [\mu]) = [\nu]$.

Next suppose $q \nmid m$. Here we may assume $N(\rho) = 2^r q^s \geq 0$, $s = 0, 1$ by Proposition 3.15. If $s = 0$, we are reduced to the above case, so we consider $N(\rho) = q \cdot 2^r$. From the previous case and Proposition 3.2 we can assume the existence of an ideal $J \in G$ such that $\Delta(JI, [\mu]) = [j\nu j^{-1}]$. We shall show that $[\nu] \in \{\Delta(I, [j\mu j^{-1}]) | I \in G\}$.

To accomplish this, we need to look at the set $T_{\nu, j\mu j^{-1}}$. First we claim that $j \cdot T_{\nu, j\mu j^{-1}} = T_{\nu,\mu}$. One inclusion is obvious. For the other, let $\gamma \in T_{\nu,\mu}$. Then $\gamma \in jT_{\nu, j\mu j^{-1}}$ if and only if $j^{-1}\gamma \in \Lambda$. Now $T_{\nu,\mu} = \mathbf{Z}\xi + \mathbf{Z}\eta$ and $\Lambda T_{\nu,\mu} = \Lambda\rho$ with $N(\rho) \equiv 0\ (q)$. Thus both ξ and η have norms divisible by q and so by Proposition 3.2 we may write $T_{\nu,\mu} = j(\mathbf{Z}\xi_1 + \mathbf{Z}\eta_1)$ for some $\xi_1, \eta_1 \in \Lambda$. It follows that $j^{-1}\gamma \in j^{-1}T_{\nu,\mu} = j^{-1}j(\mathbf{Z}\xi_1 + \mathbf{Z}\eta_1) \subset \Lambda$ which establishes the claim.

With $T_{\nu, j\mu j^{-1}} = j^{-1}T_{\nu,\mu} = \mathbf{Z}\xi_1 + \mathbf{Z}\eta_1$ we put $I_{j\mu j^{-1}} = \mathcal{O}_{j\mu j^{-1}}\xi_1\bar{\eta}_1 + \mathcal{O}_{j\mu j^{-1}}\eta_1\bar{\eta}_1$. Then as above,

$$\begin{aligned}\Lambda I_{j\mu j^{-1}} &= \Lambda \cdot T_{\nu, j\mu j^{-1}} \cdot \bar{\eta}_1 = \Lambda j^{-1}T_{\nu,\mu}\bar{\eta}_1 \\ &= \Lambda j^{-1}\Lambda T_{\nu,\mu}\bar{\eta}_1 \quad \text{(by Proposition 3.2)} \\ &= \Lambda j^{-1}\Lambda\rho\bar{\eta}_1 \\ &= \Lambda j^{-1}\rho\bar{\eta}_1 \quad \text{(by Proposition 3.2)}\end{aligned}$$

Let $I = \phi_{j\mu j^{-1}}^{-1}(I_{j\mu j^{-1}})$. Then

$$\begin{aligned}\Delta[I, (j\mu j^{-1})] &= \left[j^{-1}\rho\bar{\eta}_1(j\mu j^{-1})(j^{-1}\rho\bar{\eta}_1)^{-1}\right] \\ &= \left[j^{-1}\rho\bar{\eta}\bar{j}^{-1}(j\mu j^{-1})(j^{-1}\rho\bar{\eta}\bar{j}^{-1})^{-1}\right] \\ &= \left[j^{-1}\rho\bar{\eta}\mu\bar{\eta}^{-1}\rho^{-1}j\right] \\ &= \left[j^{-1}\rho\nu\rho^{-1}j\right] \\ &= \left[\rho_1\nu\rho_1^{-1}\right] \qquad (\rho = j\rho_1).\end{aligned}$$

But $N(\rho_1) = 2^r$, so the above arguments show that $[\rho_1\nu\rho_1^{-1}]$ and $[\nu]$ are in the same orbit.

PROPOSITION 3.26. *If $q \nmid m$ and $[\mu] \in W_1$, then the two orbits $\{\Delta(I, [\mu]) | I \in G\}$ and $\{\Delta(I, [j\mu j^{-1}]) | I \in G\}$ are disjoint.*

Proof. We need only show that the orbits do not coincide. If they did, then there would be an integral proper $\mathcal{O}_f$-ideal I, such that $\Delta(I, [\mu]) = [j\mu j^{-1}]$, so that $\Lambda I_\mu = \Lambda\kappa$ and $\varepsilon\kappa\mu\kappa^{-1}\varepsilon^{-1} = j\mu j^{-1}$ for some $\varepsilon \in \Lambda^\times$. Thus $\varepsilon\kappa \in T_{\mu, j\mu j^{-1}}$ and as we saw in the proof of Lemma 3.16, $\varepsilon\kappa = j\lambda$ for some $\lambda \in \Lambda$. In particular, $q \mid N(\kappa)$ and hence q divides the norm of the ideal I. Let $s = \operatorname{ord}_q N(\kappa)$. If s is even, then κ may be written as $\kappa = \kappa_1 q^{s/2}$ with $\kappa_1 \in \Lambda$, $q \nmid N(\kappa_1)$. But in that case $\varepsilon\kappa_1 \in T_{\mu, j\mu j^{-1}}$ and so must have norm divisible by q, a contradiction. Thus s must be odd, and since $s = \operatorname{ord}_q[\mathcal{O}_f : I]$, this implies the existence of a proper $\mathcal{O}_f$-ideal of norm q, which is impossible since q is inert in $\mathbf{Q}(\sqrt{-m})$ (Lemma 3.8). Thus, the orbits are disjoint.

THEOREM 3.27. *Let m be a positive integer not divisible by 4 and write $m = m_0 f^2$ with m_0 square-free. Let $T(m)$ denote the number of primitive roots of $X^2 + m$ in Λ and let $h(m)$ denote the order of the ideal class group of proper $\mathcal{O}_f$-ideals in $\mathbf{Q}(\sqrt{-m})$. Finally, let $\omega(m)$ denote the number of units in $\mathcal{O}_f$ and $|\Lambda^\times|$ the order of the unit group $\Lambda^\times$. Suppose that $T(m) > 0$. Then*

$$\frac{\omega(m)T(m)}{h(m)} = \begin{cases} |\Lambda^\times|\varepsilon_m & \text{if } q \mid m \\ 2|\Lambda^\times|\varepsilon_m & \text{if } q \nmid m \end{cases}$$

where

$$\varepsilon_m = \begin{cases} 1 & \text{if } m \equiv 1, 2 \pmod 4 \\ 2 & \text{if } m \equiv 7 \pmod 8 \\ 4 & \text{if } m \equiv 3 \pmod 8. \end{cases}$$

Proof. In view of Proposition 3.14, the case of $m = 3$ is special and is most easily checked by hand. Let $t(m)$ denote the number of primitive roots μ of $X^2 + m$ in Λ with $[\mu] \in W_1$. Proposition 3.24 implies that all orbits of the ideal class group G of proper $\mathcal{O}_f$-ideals acting on the set W_1 have $h(m)$ elements. Thus,

$$\begin{aligned} t(m) &= (\text{the number of orbits of } G \text{ acting on } W_1) \\ &\quad \times (\text{the number of bundles per orbit}) \\ &\quad \times (\text{the number of primitive roots per bundle}) \\ &= \begin{cases} 1 & q \mid m \\ 2 & q \nmid m \end{cases} \times h(m) \times \frac{|\Lambda^\times|}{\omega(m)} \end{aligned}$$

by Propositions 3.6, 3.24, 3.25, and 3.26.

Moreover, by Proposition 3.14 and the discussion preceding it, $T(m) = t(m)$ if $m \equiv 1, 2\ (4)$; $T(m) = 2t(m)$ if $m \equiv 7\ (8)$; and $T(m) = 4t(m)$ if $m \equiv 3\ (8)$. Here, the factors of 2 $(= 1 + 1)$ and 4 $(= 1 + 3)$ reflect the 1–1 and 1–3 correspondences of the bundles in W_1 and W_2. This completes the proof.

REMARK 3.28. It is interesting to observe that in the statement of the theorem, the left hand side depends upon the exact value of m whereas the right hand side depends only on the congruence class of m modulo $8q$.

EXAMPLE 3.29. Consider the quaternion algebra

$$\mathfrak{A} = \left(\frac{-2, -5}{\mathbf{Q}}\right)$$

(i.e., $i^2 = -2$, $j^2 = -5$) and a maximal order

$$\Lambda = \mathbf{Z}\left(\frac{1 + j + k}{2}\right) + \mathbf{Z}\left(\frac{i + 2j + k}{4}\right) + \mathbf{Z}j + \mathbf{Z}k$$

in $\mathfrak{A}$. When restricted to the elements of trace zero in $\mathfrak{A}$, the reduced norm has the form $2x^2 + 5y^2 + 10z^2$. In this example, we shall illustrate our results in the case $m = 55$. It is easy to check directly that there are precisely 24 primitive elements of Λ with trace zero and reduced norm 55. We now wish to see how these elements are distributed throughout the bundles in the sets W_1 and W_2.

Recall that W_0 denotes the set of all bundles $[\mu]$ of primitive elements $\mu \in \Lambda$ with $\mu^2 + 55 = 0$. Since $\Lambda^\times$ is a cyclic group of order 6, generated by $\varepsilon = (2 + i - \kappa)/4$, each bundle $[\mu]$ contains 3 elements (Proposition 3.6) and the elements of the bundle will be listed in the following order: $[\mu] = \{\mu, \varepsilon\mu\varepsilon^{-1}, \bar{\varepsilon}\mu\bar{\varepsilon}^{-1}\}$. Also recall that by Proposition 3.4, W_0 is the

disjoint union of the sets W_1 and W_2 where, in this example,

$$W_1 = \left\{[\mu] \in W_0 | \Lambda \cap \mathbf{Q}(\mu) = \mathbf{Z} + \mathbf{Z}\frac{1+\mu}{2}\right\} \quad \text{and}$$
$$W_2 = \{[\mu] \in W_0 | \Lambda \cap \mathbf{Q}(\mu) = \mathbf{Z} + \mathbf{Z}\mu\}.$$

By Proposition 3.14, since $m = 55 \equiv 7\ (8)$, there is a 1–1 correspondence between the elements of W_1 and W_2. To establish the correspondence, we need to determine the three left Λ-ideals of norm 2, $\Lambda\tau_1$, $\Lambda\tau_2$ and $\Lambda\tau_3$ in the notation of Proposition 3.3. They are Λi, $\Lambda i\varepsilon$, and $\Lambda i\bar{\varepsilon}$ where ε is the generator of $\Lambda^\times$ specified above.

Since $5 \mid m$, Proposition 3.25 says that the map Δ induces a transitive group action of the ideal class group G of $\mathbf{Q}(\sqrt{-55})$ on W_1. Specifically, $W_1 = \{\Delta(I, [\mu]) | I \in G\}$ where μ is any fixed primitive root of $X^2 + 55$ with $[\mu] \in W_1$. We shall take $\mu = 3j + k$ as our fixed element.

The ideal class number of $\mathbf{Q}(\sqrt{-55})$ is 4 and representatives of the ideal classes may be taken to be:

$$I_1 \equiv \mathcal{O} = \mathbf{Z} + \mathbf{Z}\frac{1+\sqrt{-55}}{2}, \quad I_2 = 2\mathcal{O} + \mathcal{O}\frac{1+\sqrt{-55}}{2},$$
$$I_3 = 2\mathcal{O} + \mathcal{O}\frac{1-\sqrt{-55}}{2}, \qquad I_4 = 5\mathcal{O} + \mathcal{O}\sqrt{-55}.$$

Note that $2\mathcal{O} = I_2 I_3$ and $5\mathcal{O} = I_4^2$ and the norms of the ideals I_1, I_2, I_3, I_4 are respectively 1, 2, 2, 5.

To employ the map Δ we need to compute κ_l where $\Lambda I_{l,\mu} = \Lambda\kappa_l$, $l = 1, 2, 3, 4$. By Lemma 3.18, the reduced norm of κ_l equals the norm of I_l which greatly simplifies the chore. κ_1 can obviously be chosen to be 1 and, by Corollary 3.20, κ_4 can be chosen to be j. One computes $[\mu] = \{(0,3,1), (\frac{5}{2}, -2, \frac{3}{2}), (-5,-1,0)\}$ where we use (a,b,c) to represent the element $ai + bj + ck$ in Λ. Since

$$\frac{1 + i\varepsilon\mu\varepsilon^{-1}i^{-1}}{2} = \frac{2 + 5i + 4j - 3k}{4} \notin \Lambda,$$

by Corollary 3.21 we may take $\kappa_2 = i$ and $\kappa_3 = i\bar{\varepsilon}$.

Thus $W_1 = \{[\kappa_l \mu \kappa_l^{-1}] | l = 1, 2, 3, 4\}$. Explicitly, we have:

$$[\kappa_1\mu\kappa_1^{-1}] = \{(0,3,1), (\tfrac{5}{2}, -2, \tfrac{3}{2}), (-5,-1,0)\},$$
$$[\kappa_2\mu\kappa_2^{-1}] = \{(0,-3,-1), (\tfrac{-5}{2}, 2, \tfrac{-3}{2}), (5,1,0)\},$$
$$[\kappa_3\mu\kappa_3^{-1}] = \{(-5,1,0), (\tfrac{5}{2}, 2, \tfrac{3}{2}), (0,-3,1)\},$$
$$[\kappa_4\mu\kappa_4^{-1}] = \{(0,3,-1), (5,-1,0), (\tfrac{-5}{2}, -2, \tfrac{-3}{2})\}.$$

According to Proposition 3.14, for each $l = 1, 2, 3, 4$, there is a unique $\tau_h (h = 1, 2, 3)$ such that $[\tau_h(\kappa_l \mu \kappa_l^{-1})\tau_h^{-1}] \in W_2$. It is easy to check that if ν is a primitive root of $X^2 + 55$ in Λ and $\nu \in \mathbf{Z}i + \mathbf{Z}j + \mathbf{Z}k$, then $(1 + \nu)/2 \in \Lambda$, i.e., $[\nu] \in W_1$. Because the elements τ_h are all of the form $i\omega$, $\omega \in \Lambda^\times$ and $i(ai + bj + ck)i^{-1} = ai - bj - ck$, the action of the τ_h on the bundles is easy to determine. Thus, by the above comment, there is for each bundle $[\kappa_l \mu \kappa_l^{-1}]$ only one viable candidate for τ_h (and it works).

The elements of W_2 are $[\nu_1]$, $[\nu_2]$, $[\nu_3]$, $[\nu_4]$ where $\nu_l = \tau_h \kappa_l \mu \kappa_l^{-1} \tau_h^{-1}$, for the appropriate τ_h ($\tau_h = i\varepsilon$ for $l = 1, 2, 3$ and $\tau_h = i\bar{\varepsilon}$ for $l = 4$). Explicitly,

$$[\nu_1] = \left\{\left(\tfrac{5}{2}, 2, \tfrac{-3}{2}\right), \left(\tfrac{15}{4}, \tfrac{-3}{2}, \tfrac{-5}{4}\right), \left(\tfrac{-5}{4}, \tfrac{-1}{2}, \tfrac{-9}{4}\right)\right\},$$
$$[\nu_2] = \left\{\left(\tfrac{-5}{2}, -2, \tfrac{3}{2}\right), \left(\tfrac{-15}{4}, \tfrac{3}{2}, \tfrac{5}{4}\right), \left(\tfrac{5}{4}, \tfrac{1}{2}, \tfrac{9}{4}\right)\right\},$$
$$[\nu_3] = \left\{\left(\tfrac{5}{2}, -2, \tfrac{-3}{2}\right), \left(\tfrac{-5}{4}, \tfrac{1}{2}, \tfrac{-9}{4}\right), \left(\tfrac{15}{4}, \tfrac{3}{2}, \tfrac{-5}{4}\right)\right\},$$
$$[\nu_4] = \left\{\left(\tfrac{-5}{2}, 2, \tfrac{3}{2}\right), \left(\tfrac{5}{4}, \tfrac{-1}{2}, \tfrac{9}{4}\right), \left(\tfrac{-15}{4}, \tfrac{-3}{2}, \tfrac{5}{4}\right)\right\}.$$

This yields the 24 primitive elements λ of Λ with $\lambda^2 + 55 = 0$. Note that while it may seem that "obvious solutions" to $\lambda^2 + 55 = 0$ are missing from the above lists (e.g., $\lambda = (\frac{5}{4}, \frac{1}{2}, \frac{-9}{4})$), these elements are not in Λ.

4. Integral representations. A question related to Theorem 3.27, which was considered in [**13**], is to determine the number of primitive integral solutions (i.e. $x, y, z \in \mathbf{Z}$ and $(x, y, z) = 1$) to $ax^2 + qy^2 + aqz^2 = m$. Since there is an obvious correspondence between a primitive integral solution (x, y, z) and a primitive root $xi + yj + zk$ of $X^2 + m$ in Λ_0, it is natural to try to imitate the results of section 3 by focusing on Λ_0 rather that Λ. However, since Λ_0 does not, in general, have class number one, the work must still be done in Λ. One needs to investigate how many (if any) elements in a given bundle $[\mu]$ ($\mu \in \Lambda$) are actually in Λ_0. Also, one needs to show that the group action induced by the map Δ restricts to one on the set of bundles which contain elements of Λ_0.

It turns out, somewhat curiously, that results regarding integral representations seem to hold for only two of the four algebras (and also Hurwitz's quaternions) which were considered in this paper. It is also of interest to note that it is precisely these three algebras for which a maximal order is a Euclidean ring [**16**]. We state the final results for the algebras

$$\left(\frac{-1, -3}{\mathbf{Q}}\right) \quad \text{and} \quad \left(\frac{-2, -5}{\mathbf{Q}}\right).$$

The results for Hurwitz's quaternions are due to Venkov [**15**].

Let m be a positive integer not divisible by 4 and write $m = m_0 f^2$ with m_0 square-free. Denote by $T_3(m)$ (resp. $T_5(m)$) the number of primitive integral solutions to $x^2 + 3y^2 + 3z^2 = m$ (resp. $2x^2 + 5y^2 + 10z^2 = m$). Let $\mathcal{O}_f$ be the uniquely determined suborder of index f in the maximal order of $\mathbf{Q}(\sqrt{-m})$ and $h(m)$ the order of the ideal class group of proper $\mathcal{O}_f$-ideals.

THEOREM 4.1. *Suppose that* $T_3(m) > 0$. *Then* $T_3(m) = c_3(m)h(m)$ *where*:

$$\text{If } m \equiv 1, 2 \pmod 4 \text{ then } c_3(m) = \begin{cases} 2 & \text{if } 3 \mid m; \\ 4 & \text{if } 3 \nmid m. \end{cases}$$

$$\text{If } \underset{(m>3)}{m \equiv 3 \pmod 8} \text{ then } c_3(m) = \begin{cases} 12 & \text{if } 3 \mid m; \\ 24 & \text{if } 3 \nmid m. \end{cases}$$

$$\text{If } m \equiv 7 \pmod 8 \text{ then } c_3(m) = \begin{cases} 8 & \text{if } 3 \mid m; \\ 16 & \text{if } 3 \nmid m. \end{cases}$$

THEOREM 4.2. *Suppose that* $T_5(m) > 0$. *Then* $T_5(m) = c_5(m)h(m)$ *where*:

$$\text{If } m \equiv 1, 2 \pmod 4 \text{ then } c_5(m) = \begin{cases} 1 & \text{if } 5 \mid m; \\ 2 & \text{if } 5 \nmid m. \end{cases}$$

$$\text{If } m \equiv 7 \pmod 8 \text{ then } c_5(m) = \begin{cases} 2 & \text{if } 5 \mid m; \\ 4 & \text{if } 5 \nmid m. \end{cases}$$

N.B. (1) If $m \equiv 3 \pmod 8$ or $25 \mid m$ then $T_5(m) = 0$.
(2) If $9 \mid m$ then $T_3(m) = 0$.

REFERENCES

[1] Z. Borevich and I. Shafarevich, *Number Theory*, Academic Press, New York, 1966.
[2] H. Brandt, *Idealtheorie in Quaternionenalgebren*, Math. Ann., **99** (1928), 1–29.
[3] J. W. S. Cassels, *Rational Quadratic Forms*, Academic Press, New York, 1978.
[4] H. Cohn, *A Classical Introduction to Algebraic Numbers and Class Fields*, Springer-Verlag, 1978.
[5] M. Eichler, *Uber die Idealklassenzahl total definiter Quaternionenalgebren*, Math. Zeit., **43** (1937), 102–109.
[6] C. F. Gauss, *Disquisitiones Arithmeticae*, translated by Arthur A. Clarke, Yale University Press, 1965.
[7] P. Hanlon, *Applications of Quaternions to the Study of Imaginary Quadratic Class Groups*, Dissertation, California Institute of Technology, 1981.
[8] M. Kneser, Personal Communication.
[9] A. Pizer, *Type numbers of Eichler orders*, J. reine angew. Math., **264** (1973), 76–102.
[10] A. Pizer, *An algorithm for computing modular forms on* $\Gamma_0(N)$, J. Algebra, **64** (1980), 340–390.

[11] H. P. Rehm, *On a theorem of Gauss concerning the number of solutions of the equation* $x^2 + y^2 + z^2 = m$, Lecture Notes in Pure and Applied Mathematics, Volume **79**, Olga Taussky Todd, editor, Dekker.
[12] I. Reiner, *Maximal Orders*, Academic Press, New York, 1975.
[13] T. Shemanske, *Ternary Quadratic Forms and the Arithmetic of Quaternion Algebras*, unpublished.
[14] G. Shimura, *Introduction to the Arithmetic Theory of Automorphic Functions*, Princeton University Press, Princeton, 1971.
[15] B. A. Venkov, *On the arithmetic of quaternion algebras* (Russian), Izv. Akad. Nauk 205–220, 221–246 (1922), 489–509, 532–562, 607–622 (1929).
[16] M-F. Vigneras, *Arithmetique des Algebras de Quaternions*, Lecture Notes in Mathematics, 800, Springer-Verlag.

Received April 12, 1984 and in revised form August 28, 1984.

DARTMOUTH COLLEGE
HANOVER, NH 03755