Applications of the Quaternions to the Study of Imaginary Quadratic Ring Class Groups

Thesis by

Phil Hanlon

In Partial Fulfillment of the Requirements

for the Degree of

Doctor of Philosophy

California Institute of Technology

Pasadena, California

1981

(Submitted May 15, 1981)

Acknowledgements

I am deeply indebted to Professor Olga Taussky Todd, my thesis advisor, for her patience, encouragement and inspiration. She expended time and effort generously on my behalf and I am very grateful.

Others at Caltech deserve mention. Thanks are due to Pat Morton for sharing with me so much of his knowledge, to Professor R. P. Dilworth for his frequent guidance and to Anton Schep, Helene Shapiro, Rob Calderbank, Claire O'Keefe, Guido Janssen, Pat Morton and Dr. Bill Squires for their friendship and encouragement. Fran Williams, Lillian Chappelle and Shelly Moore comprise an exceptional secretarial staff -- I appreciate all they've done.

I thank my parents most of all. Without their constant love and support, none of this would have been possible.

Abstract

Let $m = m_1 f^2$ where m_1 is a square-free positive integer and m is congruent to 1 or 2 mod 4. A theorem of Gauss (see [5]) states that the number of ways to write m as a sum of 3 squares is 12 times the size of the ring class group with discriminant $-4m$ in the field $\mathbb{Q}(\sqrt{-m_1})$. The proof given by Gauss involves the arithmetic of binary quadratic forms; Venkow (see [12]) obtained an alternative proof by embedding the field $\mathbb{Q}(\sqrt{-m_1})$ in the quaternion algebra over $\mathbb{Q}$. This thesis takes Venkow's proof as its starting point. We prove several further facts about the correspondence established by Venkow and apply these results to the study of imaginary quadratic ring class groups.

Let H denote the quaternion algebra over $\mathbb{Q}$, let E denote the maximal order in H and let U denote the group of 24 units in E. Let $B_1(m)$ be the set of quaternions in E with trace 0 and norm m. The group U acts on $B_0(m)$ by conjugation; let $B_1(m)$ denote the set of orbits of $B_0(m)$ under the action of U. For $\mu = ui_1 + vi_2 + wi_3 \in B_1(m)$ we let $[u,v,w]$ denote the orbit containing μ.

Venkow proved Gauss's result by defining a sharply transitive action of $\Gamma(m)$, the ring class group with discriminant $-4m$, on $B(m)$. In chapter 2 we establish some more subtle properties of this action. The prime 2 ramifies in the extension $\mathbb{Q}(\sqrt{-m_1})$ and its prime divisor $\mathfrak{p}_2$ is a regular ideal with respect to the discriminant $-4m$. It is shown that the class containing $\mathfrak{p}_2$ maps $[u,v,w]$ to $[-u,-w,-v]$. It is shown that if an ideal class $\mathfrak{C}$ maps $[r,s,t]$ to $[u,v,w]$ then the class $\mathfrak{C}^{-1}$ maps $[-r,-s,-t]$ to $[-u,-v,-w]$. From these two facts, several results follow. If $\mathfrak{C}$ maps $[r,s,o]$ to $[u,v,w]$ then $\mathfrak{C}$ has

order 2 iff one of u, v or w is 0. If $\mathcal{C}$ maps $[r,s,o]$ to $[u,v,v]$ then $\mathcal{C}$ has order 4 and the class $\mathcal{C}^2$ contains $\mathcal{P}_2$. If $\mathcal{C}$ maps $[r,s,o]$ to $[u,v,w]$ then $\mathcal{C}^{-1}$ maps $[r,s,o]$ to $[-u,-v,-w]$. If m can be written as a sum of two squares then a class $\mathcal{C}$ is the square of another class (i.e. $\mathcal{C}$ is in the principal genus) iff $\mathcal{C}$ maps some bundle $[u,v,w]$ to $[-u,-v,-w]$.

We apply these results to the following problem; given an odd prime p and an odd integer n, in which ring class groups are the prime divisors of p regular ideals in classes of order n? It is shown that the number of such ring class groups having discriminant $-4m$ where m is a sum of two squares is related to the class number $h(-4p)$ of the field $\mathbb{Q}(\sqrt{-p})$. For $n = 3$ the number is given by

$$\begin{cases} \frac{1}{16} f(p)h(-4p) - 6h(-4p) + 2 & \text{if } p \equiv 1 \bmod 4 \\ \frac{1}{8} f(p)h(-4p) - 6h(-4p) & \text{if } p \equiv 3 \bmod 8 \\ 0 & \text{if } p \equiv 7 \bmod 8. \end{cases}$$

Here $f(p)$ is the number of ways to write p as a sum of 4 squares plus the number of ways to write $4p$ as a sum of 4 odd squares. A simple algorithm for producing the discriminants of all such ring class groups is given. Similar, but more complicated formulas hold for odd numbers n greater than 3.

Contents

Introduction

The aim of the present work is to study the ring class groups $\Gamma(m)$ in the imaginary quadratic extensions $\mathbb{Q}(\sqrt{-m})$. Let m be congruent to 1 or 2 mod 4. In Disquitiones Arithmeticae, Gauss proved that $h(m)$, the order of $\Gamma(m)$, is related to the number of integral representations of m by the quadratic form $x^2 + y^2 + z^2$.

Theorem: (Gauss) Let $t(m)$ be the number of vectors $(x,y,z) \in \mathbb{Z}^3$ with $\gcd(x,y,z) = 1$ and with $x^2 + y^2 + z^2 = m$. Then

$$t(m) = 12\, h(m).$$

The proof of this theorem given by Gauss is indirect in the sense that it gives no explicit 12 to 1 correspondence between the integral representations of m by the form $x^2 + y^2 + z^2$ and the classes in $\Gamma(m)$. In the mid 1920's, Venkow discovered a new proof of this theorem which does display a direct correspondence.

The idea of Venkow's proof is to view the equation $x^2+y^2+z^2 = m$ as a norm equation in the Hurwitz quaternions. The ring, E, of Hurwitz quaternions is the ring E in the rational quaternion algebra with $\mathbb{Z}$-basis i_1, i_2, i_3 and $\delta = \frac{1}{2}(1 + i_1 + i_2 + i_3)$. For $\mu = w + xi_1 + yi_2 + zi_3$ in H, the norm of μ, denoted $N\mu$, is $w^2 + x^2 + y^2 + z^2$ and the trace of μ, denoted $Tr\mu$, is $2w$. If μ is not in $\mathbb{Q}$ then the minimal polynomial of μ over $\mathbb{Q}$ is $\lambda^2 - (Tr\mu)\lambda + N\mu$. So μ has minimal polynomial $\lambda^2 + m = 0$ iff $w = 0$ and $x^2 + y^2 + z^2 = m$. Hence the integral representations of m by the form $x^2 + y^2 + z^2$ are in 1 - 1 correspondence with the embeddings of $\mathbb{Q}(\sqrt{-m})$ in E.

The group of units U in E has order 24 and acts on E by conjugation. If α and β are elements of E in the same orbit under this action then α and β satisfy the same minimal polynomial over $\mathbb{Q}$. Let $B_1(m)$ denote the set of orbits containing Hurwitz quaternions with relatively prime coefficients which satisfy the polynomial $\lambda^2 + m = 0$.

Venkow defined an action of $\Gamma(m)$ on $B_1(m)$ which he showed to be transitive. He also showed that the stabilizer of any element of $B_1(m)$ is the identity in $\Gamma(m)$ from which it follows that $h(m) = |B_1(m)|$. Lastly Venkow showed that every orbit in $B_1(m)$ has size 12. Thus Venkow showed that the $t(m)$ integral representations of m by $x^2 + y^2 + z^2$ are in one to one correspondence $(x^2 + y^2 + z^2 \leftrightarrow xi_1 + yi_2 + zi_3)$ with the embeddings of $\mathbb{Q}(\sqrt{-m})$ in E. These in turn are divided into $h(m)$ orbits each of size 12 and so it follows that $t(m) = 12\, h(m)$.

This is a brief outline of Venkow's proof written in the language of permutation representations. Venkow's original proof was not written in such a way; Hans Peter Rehm is responsible for having reformulated the original work using modern ideas and language.

The present work is divided into four chapters. Chapter 1 contains background material about the Hurwitz quaternions and about ring class groups in imaginary quadratic extensions. Chapter 2 is a detailed explanation of Venkow's proof of the theorem. In Chapter 3 we examine the action of $\Gamma(m)$ on $B_1(m)$ defined by Venkow. We prove several new facts about this action, some of which are similar to results of Mac Duffee (see Mac Duffee [7]) and Taussky (see Taussky [11]). The

role played in this work by the ring E is played in their work by the ring of 2 by 2 $\mathbb{Z}$-matrices. Their results deal with classes of 2×2 $\mathbb{Z}$-matrices under unimodular similarity.

In Chapter 4 we use the facts proved in Chapter 3 to answer the following question. Let p be an odd prime. How many imaginary quadratic ring class groups $\Gamma(m)$, with m a sum of two squares, have the property that the prime divisors of (p) are regular ideals in classes of order 3 in $\Gamma(m)$? It is shown that this number is related to $h(p)$, the class number of $\mathbb{Q}(\sqrt{-p})$ and that all such m are generated by values of a certain form.

In the conclusion we list some unsolved problems which stem from this work.

Chapter 1. Ring Class Groups in $\mathbb{Q}(\sqrt{-m})$ and the Quaternion Algebra.

Let m be a positive (rational) integer which is congruent to 1 or 2 mod 4. Write $m = m_1 f^2$ where m_1 is square-free. Let K be the field $\mathbb{Q}(\sqrt{-m_1})$ and let $\mathcal{O}$ be the maximal order in K.

Definition 1.1. The *ring mod f*, $\mathcal{O}_f$, is the suborder of $\mathcal{O}$ with $\mathbb{Z}$-module basis 1 and $f\sqrt{-m_1}$.

Let A denote the semigroup of ideals in $\mathcal{O}$ and let B_f denote the subgroup of A consisting of ideals $\mathfrak{a}$ with $(N\mathfrak{a},f) = 1$.

Definition 1.2. An ideal $\mathfrak{a}$ of $\mathcal{O}_f$ is *regular* if $\mathfrak{a} = \mathcal{O}_f \cap \mathfrak{J}$ for some $\mathfrak{J} \in B_f$.

Let A_f denote the semigroup of regular ideals of $\mathcal{O}_f$ and let P_f denote the subsemigroup of A_f consisting of the ideals which are principal in $\mathcal{O}_f$. Define *equivalence*, denoted $\sim$, of ideals in A_f as follows; for $\mathfrak{a}_1, \mathfrak{a}_2 \in A_f$, we say $\mathfrak{a}_1 \sim \mathfrak{a}_2$ iff there exist $(\gamma_1), (\gamma_2) \in P_f$ with $(\gamma_1)\mathfrak{a}_1 = (\gamma_2)\mathfrak{a}_2$. Let $\Gamma(m)$ denote the set of equivalence classes of A_f. The multiplication in A_f induces a multiplication in $\Gamma(m)$. With this multiplication, $\Gamma(m)$ is an abelian semigroup. In fact, $\Gamma(m)$ is a finite, abelian group (see Cohn [1]) called the *ring class group with discriminant -4m*. If $f = 1$, the ring class group is exactly the class group of the number field $\mathbb{Q}(\sqrt{-m_1})$.

Let $\mathfrak{a} \in A_f$ and suppose $\mathfrak{a}$ has $\mathbb{Z}$-basis $(a,b+f\sqrt{-m_1})$. The ideal in A_f with $\mathbb{Z}$-basis $(a,b-f\sqrt{-m_1})$ is called the *conjugate* of $\mathfrak{a}$ and is denoted $\mathfrak{a}'$. We will use the fact that if $\mathfrak{a}$ is in the class $\mathcal{C}$ then $\mathfrak{a}'$ is in the class $\mathcal{C}^{-1}$.

Example 1.1. Let $m = 41$, so $m_1 = 41$ and $f = 1$. In this case $\Gamma(m)$ is the class group of the field $\mathbb{Q}(\sqrt{-41})$. The group $\Gamma(m)$ is isomorphic to $\mathbb{Z}_8$ and the class $\mathfrak{C}$ containing the ideal $\mathfrak{a} = (3,1+\sqrt{-41})$ generates $\Gamma(m)$. The following table gives a representative ideal from each class.

Class	Representative Ideal
1	(1)
$\mathfrak{C}$	$(3,1+\sqrt{-41})$
$\mathfrak{C}^2$	$(9,7+\sqrt{-41})$
$\mathfrak{C}^3$	$(6,5+\sqrt{-41})$
$\mathfrak{C}^4$	$(2,1+\sqrt{-41})$
$\mathfrak{C}^5$	$(6,5-\sqrt{-41})$
$\mathfrak{C}^6$	$(9,7-\sqrt{-41})$
$\mathfrak{C}^7$	$(3,1-\sqrt{-41})$.

Table I. The group $\Gamma(41)$.

Two classes $\mathfrak{C}$ and $\mathfrak{D}$ in $\Gamma(m)$ are in the same *genus* if their ratio $\mathfrak{C}\mathfrak{D}^{-1}$ is a square in $\Gamma(m)$. Thus $\Gamma(41)$ is composed of two genera $\{1,\mathfrak{C}^2,\mathfrak{C}^4,\mathfrak{C}^6\}$ and $\{\mathfrak{C},\mathfrak{C}^3,\mathfrak{C}^5,\mathfrak{C}^7\}$. The subgroup of squares in $\Gamma(m)$ is a genus, called the *principal genus* and denoted here by $\Gamma^2(m)$. Clearly $\Gamma(m)/\Gamma^2(m)$ is an elementary abelian 2-group. In Disquitiones Arithmeticae [5], Gauss introduces $\Gamma(m)/\Gamma^2(m)$ by means of binary characters on $\Gamma(m)$ and shows that $|\Gamma(m)/\Gamma^2(m)| = 2^{t-1}$ where t is the number of distinct prime divisors of $4m$.

The *ring class number* $h(m)$ is the order of $\Gamma(m)$. When $f = 1$, $h(m)$ is the usual class number of the field $\mathbb{Q}(\sqrt{-m})$. In general $h(m_1)|h(m_1 f^2)$ as we will see in Section 3. The following theorem of

Gauss gives a simple means of computing $h(m)$.

Theorem 1.1. (Gauss [5]) Let $t(m)$ denote the number of vectors $(x,y,z) \in \mathbb{Z}^3$ with $\gcd(x,y,z) = 1$ and with $x^2 + y^2 + z^2 = m$. Then

$$h(m) = \frac{t(m)}{12} \qquad \text{if} \quad m \equiv 1, 2 \mod 4$$

$$h(m) = \frac{t(m)}{24} \qquad \text{if} \quad m \equiv 3 \mod 8 \quad m > 3$$

$$h(3) = 1 = \frac{t(3)}{8}$$

Gauss's proof of Theorem 1.1 is in Disquitiones Arithmeticae written in the language of binary quadratic forms. One can show that there is a $1 - 1$ correspondence between classes of binary quadratic forms with discriminant $-4m$ and classes of ideals in the ring $\mathcal{O}_f$. For details of this correspondence see Cohn [1], chapter 14 (note that weak and strict equivalence of forms coincide since the discriminant is negative). The final statement of the theorem appears in articles 289-292 though the proof relies on previous work from Section V. Gauss's proof has the interesting feature that it gives no 12 to 1 correspondence, when $m \equiv 1 \mod 4$, and no 24 to 1 correspondence, when $m \equiv 3 \mod 8$ between the triples counted by $t(m)$ and the form classes counted by $h(m)$.

In 1922, Venkow [12] published an elegant new proof of Theorem 1.1. This proof displays an explicit correspondence between the triples counted by $t(m)$ and the classes counted by $h(m)$. The proof makes use of the maximal order of the rational quaternion algebra and will be outlined in the next section.

Example 1.2. As an example of Theorem 1.1 consider $m = 41$. In this

case $h(m)$ is 8 so $t(m) = 96$. The 96 ways to write 41 as a sum of three squares come from the following three representations $41 = u^2 + v^2 + w^2$ by permuting the order of u, v and w and changing their signs.

$$41 = 0^2 + 4^2 + 5^2$$
$$41 = 3^2 + 3^2 + 4^2$$
$$41 = 1^2 + 2^2 + 6^2.$$

Next let $m = 163$. Here $t(m) = 24$, the representations of 163 coming as above from the representation

$$163 = 1^2 + 9^2 + 9^2.$$

By Theorem 1.1 $h(163) = 1$, as is well-known.

We end this section with a brief introduction to the Hurwitz quaternions along with some facts about them that will be of interest to us in later chapters.

Definition 1.3. The *quaternion algebra* H over $\mathbb{Q}$ is the 4 dimensional $\mathbb{Q}$-algebra with vector space basis $1, i_1, i_2, i_3$ and with multiplication of basis elements according to the rules

(A) $1 \cdot i_r = i_r \cdot 1 = i_r \qquad r = 1, 2, 3$

(B) $i_r^2 = -1 \qquad r = 1, 2, 3$

(C) $i_1 i_2 = -i_2 i_1 = i_3$, $i_2 i_3 = -i_3 i_2 = i_1$, $i_3 i_1 = -i_1 i_3 = i_2$.

If $\alpha = a + bi_1 + ci_2 + di_3 \in H$ the *conjugate* of α, denoted $\bar{\alpha}$ is the quaternion $\bar{\alpha} = a - bi_1 - ci_2 - di_3$. The *norm* and *trace* of α, denoted $N\alpha$ and $Tr\alpha$ are given by

$$N\alpha = \alpha\bar{\alpha} = a^2 + b^2 + c^2 + d^2$$

and $Tr\alpha = \alpha + \overline{\alpha} = 2a$.

Note that both $N\alpha$ and $Tr\alpha$ are rational; if $\alpha \notin \mathbb{Q}$ then the minimal polynomial of α over $\mathbb{Q}$ is

$$m_\alpha(x) = x^2 - (Tr\alpha)x + N\alpha .$$

In particular if $Tr\alpha = 0$ and $N\alpha = m$ then α satisfies the minimal polynomial $x^2 + m$ over $\mathbb{Q}$. It is easily seen that $N\alpha = N\overline{\alpha}$ and that conjugation is an anti-isomorphism of H; i.e. $\overline{(\alpha\beta)} = \overline{\beta}\,\overline{\alpha}$. Since $N\alpha = 0$ iff $\alpha = 0$ it follows that H is a division algebra over $\mathbb{Q}$.

Quaternions α with $N\alpha$, $Tr\alpha \in \mathbb{Z}$ are called *integral quaternions*. Integral quaternions can have non-integral coefficients. In particular we shall deal with the quaternion

$$\delta = \frac{1}{2}(1 + i_1 + i_2 + i_3)$$

for which we have $N\delta = Tr\delta = 1$.

Definition 1.4. Let E be the $\mathbb{Z}$-module in H spanned by i_1, i_2, i_3, δ; so $E = \{z_0\delta + z_1 i_1 + z_2 i_2 + z_3 i_3 : z_i \in \mathbb{Z}\}$. Then E is called the set of *Hurwitz quaternions*.

Not all integral quaternions are Hurwitz quaternions; for example $\alpha = (\frac{2}{3})i_1 + (\frac{2}{3})i_2 + (\frac{1}{3})i_3$ has trace 0 and norm 1 but α is not an element of E. One can check that E is a maximal order in H; i.e. E satisfies the following four conditions,

(i) E contains a vector space basis for H over $\mathbb{Q}$.

(ii) E is a subring of H and $1 \in E$.

(iii) Each element of E satisfies a minimal equation over $\mathbb{Q}$ having coefficients in $\mathbb{Z}$.

(iv) E is not properly contained in any other subset of H with properties (i)-(iii).

In fact E is the unique maximal order in H. For a proof of this fact see Dickson, *Algebras and Their Arithmetics* [3], Section 91. The following theorem due to Hurwitz will be very important in what follows.

Theorem 1.2. (Hurwitz [6], pg. 313) The quaternion norm, restricted to E, is a Euclidean norm; i.e. given $\alpha, \beta \in E$, with $\beta \neq 0$, there exist $\eta, \rho \in E$ and $\pi, \sigma \in E$ with

$$\alpha = \eta\beta + \rho \quad N(\rho) < N(\beta)$$

$$\text{and} \quad \alpha = \beta\pi + \sigma \quad N(\sigma) < N(\beta).$$

The proof is in Dickson [3] on pages 148 and 149 and will not be repeated here. However we illustrate the theorem in the next example.

Example 1.3. Let $\alpha, \beta \in E$. This example first explains how to choose η and ρ so that $\alpha = \eta\beta + \rho$ and $N\rho < N\beta$, and then illustrates this algorithm with $\alpha = 1 + 4i_2 + 5i_3$ and $\beta = 3$.

Step 1: Let $h = \alpha\bar{\beta}$ and $m = N\beta$. Write $h = h_0\delta + h_1 i_1 + h_2 i_2 + h_3 i_3$ and write $\eta = x_0\delta + x_1 i_1 + x_2 i_2 + x_3 i_3$ where the x_0, x_1, x_2, x_3 are to be determined.

Step 2: Choose η so that $N(h - m\eta) < m^2$ as follows;

(1) Choose $x_o \in \mathbb{Z}$ so that $|h_o - mx_o| \leq \frac{m}{2}$ (here x_o will be either $[\frac{h_o}{m}]$ or $[\frac{h_o}{m}] + 1$ where $[\frac{h_o}{m}]$ is the integer part of h_o/m).

(2) Choose $x_t \in \mathbb{Z}$ $(t = 1,2,3)$ so that

$$|h_o + 2h_t - mx_o - 2mx_t| \leq m.$$

Since $h - m\eta = \frac{1}{2}(h_0 - mx_0)$

$$+ \frac{1}{2}(h_0 + 2h_1 - mx_0 - 2mx_1)i_1$$

$$+ \frac{1}{2}(h_0 + 2h_2 - mx_0 - 2mx_2)i_2$$

$$+ \frac{1}{2}(h_0 + 2h_3 - mx_0 - 2mx_3)i_3$$

we have

$$N(h - m\eta) = \frac{1}{4}(h - mx_0)^2 + \frac{1}{4}\sum_{t=1}^{3}(h_0 + 2h_t - mx_0 - 2mx_t)^2$$

so $N(h - m\eta) \leq \frac{m^2}{16} + \frac{1}{4}3m^2 = \frac{13}{16}m^2 < m^2$.

Step 3: Let $\rho = \alpha - \eta\beta$ where η is as above.

Then

$$m^2 > N(h - \eta m) = N(\alpha\bar{\beta} - \eta\beta\bar{\beta}) = N(\alpha - \eta\beta)N(\bar{\beta})$$

so $m^2 > mN(\rho)$ which shows that η and ρ as chosen here can be used in Theorem 1.2.

Now let $\alpha = 1 + 4i_2 + 5i_3$ and $\beta = 3$. Thus $h = 3 + 12i_2 + 15i_3$ and $m = 9$. We must choose x_0, x_1, x_2, x_3 to satisfy

(1) $3 - 9x_0 \leq \frac{9}{2}$ - choose $x_0 = 0$

(2) $3 - 18x_1 \leq 9$ - choose $x_1 = 0$

(3) $3 + 24 - 18x_2 \leq 9$ - choose $x_2 = 1$

(4) $3 + 30 - 18x_3 \leq 9$ - choose $x_3 = 2$.

Let $\eta = i_2 + 2i_3$ and let $\rho = (1 + 4i_2 + 5i_3) - (i_2 + 2i_3)3$ so $\rho = 1 + i_2 - i_3$. Note that $N\rho = 3 < 9 = N\beta$.

In the above case $\beta = N\rho = \rho\bar{\rho}$ so ρ is a right divisor of β. Also $\alpha = \eta\beta + \rho = (\eta\bar{\rho} + 1)\rho$ thus ρ is a right divisor of α as well.

Furthermore, $N\rho = 3 = \gcd(N\alpha, N\beta)$ so ρ is a greatest common right divisor of α and β. In fact for any pair $\alpha, \beta \in E$ we obtain a greatest common right divisor of α and β by repeated use of Theorem 1.2.

Corollary 1.1. (Euclidean Algorithm for E) Let $\alpha, \beta \in E$. Suppose $\eta_1, \ldots, \eta_{r+1}$ and $\rho_1, \ldots, \rho_r$ are elements of E such that

$$\begin{aligned} \alpha &= \eta_1\beta + \rho_1 && N(\rho_1) < N(\beta) \\ \beta &= \eta_2\rho_1 + \rho_2 && N(\rho_2) < N(\rho_1) \\ \rho_1 &= \eta_3\rho_2 + \rho_3 && N(\rho_3) < N(\rho_2) \\ &\vdots && \vdots \\ \rho_{r-1} &= \eta_{r+1}\rho_r. \end{aligned}$$

Then ρ_r is a greatest common right divisor of α and β in E.

The algorithm given in Example 1.3 chooses ρ such that $N\rho < \frac{13}{16}N\beta$. One can show that the Euclidean algorithm for E finds a greatest common divisor of α and β in no more than $C \log(\min(N\alpha, N\beta))$ steps where C is a constant. From Corollary 1.1 we obtain three further results all due to Hurwitz.

Corollary 1.2. (Hurwitz [6], pg. 313) The ring E is a principal ideal ring, i.e. every left ideal A of E can be written $A = E\alpha$ for $\alpha \in E$.

The quaternion α in Corollary 1.2 is determined up to left multiplication by a unit; α is the greatest common right divisor of all elements of A. Hence α can be obtained using the Euclidean algorithm.

Corollary 1.3. (Hurwitz [6], pg. 314) If δ is a greatest common right divisor of α and β in E then there exist $\eta_1, \eta_2 \in E$ such that

$$\eta_1\alpha + \eta_2\beta = \delta.$$

Corollary 1.4. (Hurwitz [6], pg. 322) Let $\alpha \in E$ and let p be a prime in $\mathbb{Z}$. If p divides $N\alpha$ then there exist $\Pi_1, \Pi_2 \in E$ with $N\Pi_1 = N\Pi_2 = p$ such that Π_1 is a right divisor of α and Π_2 is a left divisor of α.

Proof. Suppose to the contrary that no quaternion of norm p is a right divisor of α. By the Euclidean algorithm we have that α and p are relatively prime in E. Hence by Corollary 1.3 there exist $\eta_1, \eta_2 \in E$ with

$$\eta_1\alpha + \eta_2 p = 1.$$

Now $\quad N(\eta_1)N(\alpha) = N(1 - \eta_2 p) = (1 - \eta_2 p)(\overline{1 - \eta_2 p})$

hence $\quad N(\eta_1)N(\alpha) = (1 - \eta_2 p)(1 - \overline{\eta}_2 p) = 1 - Tr(\eta_1)p + p^2$

so $\quad N(\eta_1)N(\alpha) = 1 + tp$ where $t \in \mathbb{Z}$. This contradicts the assumption that p divides $N\alpha$.

Example 1.4. Let $\alpha = 3 - 2i_1 + i_2 - i_3$ so $N\alpha = 15$. We can factor α

$$\text{as } \alpha = (1 + i_1 - i_2)(-2i_1 + i_2)$$

$$\text{or as } \alpha = (+i_1 + 2i_3)(-i_1 + i_2 - i_3)$$

The first factorization gives α as a quaternion of norm 3 times a quaternion of norm 5. The latter factorization gives α as a quaternion of norm 5 times a quaternion of norm 3.

Definition 1.5. Let U denote the group of units in the ring E.

A Hurwitz quaternion ε is a unit in E if and only if $N\varepsilon = 1$. The group of units in E has order 24 and is generated multiplicatively by δ, i_1 and i_2. There are 8 units with exactly one nonzero coefficient, $\{1, \pm i_1, \pm i_2, \pm i_3\}$. The remaining 16 units have 4 nonzero coefficients and are listed below;

$$\pm \tfrac{1}{2}(1 + i_1 + i_2 + i_3) \qquad \pm \tfrac{1}{2}(1 - i_1 - i_2 - i_3)$$

$$\pm \tfrac{1}{2}(1 - i_1 + i_2 + i_3) \qquad \pm \tfrac{1}{2}(1 + i_1 - i_2 - i_3)$$

$$\pm \tfrac{1}{2}(1 + i_1 - i_2 + i_3) \qquad \pm \tfrac{1}{2}(1 - i_1 + i_2 - i_3)$$

$$\pm \tfrac{1}{2}(1 + i_1 + i_2 - i_3) \qquad \pm \tfrac{1}{2}(1 - i_1 - i_2 + i_3).$$

The group U acts on E by conjugation; this action will play a fundamental role in what follows. The following table is included for reference.

Table II. $U/\pm 1$ acting on E by conjugation

ε	$\varepsilon(a + bi_1 + ci_2 + di_3)\varepsilon^{-1}$
1	$a + bi_1 + ci_2 + di_3$
i_1	$a + bi_1 - ci_2 - di_3$
i_2	$a - bi_1 + ci_2 - di_3$
i_3	$a - bi_1 - ci_2 + di_3$
$\frac{1}{2}(1 + i_1 + i_2 + i_3)$	$a + di_1 + bi_2 + ci_3$
$\frac{1}{2}(-1 + i_1 - i_2 + i_3)$	$a + di_1 - bi_2 - ci_3$
$\frac{1}{2}(-1 + i_1 + i_2 - i_3)$	$a - di_1 + bi_2 - ci_3$
$\frac{1}{2}(-1 - i_1 + i_2 + i_3)$	$a - di_1 - bi_2 + ci_3$
$\frac{1}{2}(1 - i_1 - i_2 - i_3)$	$a + ci_1 + di_2 + bi_3$
$\frac{1}{2}(1 + i_1 + i_2 - i_3)$	$a + ci_1 - di_2 - bi_3$
$\frac{1}{2}(1 - i_1 + i_2 + i_3)$	$a - ci_1 + di_2 - bi_3$
$\frac{1}{2}(1 + i_1 - i_2 + i_3)$	$a - ci_1 - di_2 + bi_3$

The three facts stated in the next lemma follow by inspection of Table II.

Lemma 1.1. For all $\mu \in E$ and $\varepsilon \in U$,

(i) $N(\varepsilon\mu\varepsilon^{-1}) = N(\mu)$

(ii) $Tr(\varepsilon\mu\varepsilon^{-1}) = Tr(\mu)$.

(iii) If all coefficients of μ are integers then all coefficients of $\varepsilon\mu\varepsilon^{-1}$ are integers and the greatest common divisor of the coefficients of μ equals the greatest common divisor of the coefficients of $\varepsilon\mu\varepsilon^{-1}$.

Definition 1.6. Let $\mu \in E$. The *bundle of* μ, denoted $[\mu]$, is

$$[\mu] = \{\varepsilon\mu\varepsilon^{-1} : \varepsilon \in U\}.$$

If $\mu = ui_1 + vi_2 + wi_3$ we may also denote $[\mu]$ by $[u,v,w]$. Let θ be a bundle and let $\mu \in \theta$. Define the *norm of* θ, denote $N\theta$, and *trace of* θ, denoted $Tr\theta$,

by $$N\theta = N\mu \quad \text{and} \quad Tr\theta = Tr\mu.$$

By Lemma 1.1 the norm and trace of θ are well-defined; i.e. independent of the choice of μ from θ.

Bundles of trace 0 will be of particular interest to us. If θ is a bundle, $\mu \in \theta$ and $Tr\theta = 0$ then all coefficients of μ are integers. So the following definition makes sense.

Definition 1.7. Let θ be a bundle of trace 0 and let $\mu \in \theta$. Define the *content* of θ, denoted $c\theta$ to be the greatest common divisor of the coefficients of μ. By Lemma 1.1 (iii), $c(\theta)$ is well-defined.

Example 1.5. Let $\mu = 6i_1 + 3i_2$, and let $\theta = [\mu]$. Then θ contains the following 12 quaternions;

$$(6i_1 + 3i_2) \quad (-6i_1 + 3i_2) \quad (6i_1 - 3i_2) \quad (-6i_1 - 3i_2)$$

$$(6i_2 + 3i_3) \quad (-6i_2 + 3i_3) \quad (6i_2 - 3i_3) \quad (-6i_2 - 3i_3)$$

$$(3i_1 + 6i_3) \quad (-3i_1 + 6i_3) \quad (3i_1 - 6i_3) \quad (-3i_1 - 6i_3).$$

Here we have $N\theta = 45$, $Tr\theta = 0$ and $C\theta = 3$. The next two lemmas show that with a few exceptions, the size of a bundle is always 12. The first lemma is due to Hurwitz, the second to Venkow.

Lemma 1.2. (Hurwitz [6], pg. 308) If $\mu \in H - \mathbb{Q}$ then the centralizer of μ in H is exactly the set of rational polynomials in μ.

Suppose $\mu \in E$, with $N\mu > 3$, and $Tr\mu = 0$, and suppose the coefficients of μ are relatively prime. Any rational polynomial in μ can be put in the form $q_0 + q_1\mu$ where $q_0, q_1 \in \mathbb{Q}$ hence the only rational polynomials in μ which are units are ± 1. So for such μ, the centralizer of μ in U is the subgroup $\{\pm 1\}$. So

$$|[\mu]| = \frac{|U|}{|C_U(\mu)|} = \frac{24}{2} = 12$$

here $C_U(\mu)$ denotes the centralizer of μ in U. This proves the following lemma.

Lemma 1.3. (Venkow [12]) Suppose θ is a bundle with $N\theta > 3$, $Tr\theta = 0$ and $c(\theta) = 1$. Then the size of θ is 12.

We finish this section with three technical results about E.

Lemma 1.4. Let $\mu = ui_1 + vi_2 + wi_3$ be a nonzero element of E with $\gcd(u,v,w) = 1$. Let $\beta = \sigma + xi_1 + yi_2 + zi_3$ be an element of E.

The $\beta\mu\beta^{-1} = -\mu$ iff $\sigma = 0$ and $xu + yv + zw = 0$.

Proof. Let $S = \{\alpha \in E : \alpha\mu = -\mu\alpha\}$ and let

$$T = \{xi_1 + yi_2 + zi_3 : xu + yv + zw = 0\}.$$

Rehm shows that S is a rank 2 $\mathbb{Z}$-module (see [9], pg. 9). It is clear that T is a rank 2 $\mathbb{Z}$-module. This lemma states that $S = T$.

First observe that $T \subseteq S$. For if $\beta = xi_1 + yi_2 + zi_3 \in T$ then

$\beta\mu\bar{\beta} = (xi_1 + yi_2 + zi_3)(ui_1 + vi_2 + wi_3)(-xi_1 - yi_2 - zi_3)$ so

$\beta\mu\bar{\beta} = (i_1(wy - vz) + i_2(uz - wx) + i_3(vx - uy))(-xi_1 - yi_2 - zi_3)$.

Hence $\beta\mu\bar{\beta} = i_1(-z^2u + xzw - y^2u + xyv)$

$$+i_2(-x^2v + xyu - z^2v + yzw)$$

$$+i_3(-y^2w + yzv - x^2w + xzu).$$

So $\beta\mu\bar{\beta} = i_1(-u(y^2 + z^2) + (xyv + xzw))$

$$+i_2(-v(x^2 + z^2) + (xyu + yzw)) \qquad (*)$$

$$+i_3(-w(x^2 + y^2) + (xzu + yzv))$$

The linear condition $xu + yv + zw = 0$ gives

(1) $x(yv + zw) = -x^2u$

(2) $y(xu + zw) = -y^2v$

(3) $z(xu + yv) = -z^2w$.

Substituting (1), (2) and (3) into (*) gives $\beta\mu\bar{\beta} = N\beta(-ui_1 - vi_2 - wi_3)$ and so $\beta\mu\beta^{-1} = -\mu$. This shows $T \subseteq S$.

Next we show that every element of S has trace 0. Assume to the contrary that $\beta \in S$ and $Tr(\beta) \neq 0$. Write $\beta = \sigma + xi_1 + yi_2 + zi_3$

and note that

$$\beta^2\mu\beta^{-2} = \beta(\beta\mu\beta^{-1})\beta^{-1} = \beta(-\mu)\beta^{-1} = -(\beta\mu\beta^{-1}) = \mu \qquad \text{so}$$

β^2 centralizes μ. Thus $\beta^2 = q_1 + q_2\mu$ with $q_1, q_2 \in \mathbb{Q}$.

A straightforward computation shows that

$$\beta^2 = (\sigma^2 - x^2 - y^2 - z^2) + 2\sigma(xi_1 + yi_2 + zi_3).$$

As $\sigma \neq 0$ we see that $xi_1 + yi_2 + zi_3 = qu$ with $q = \frac{q_2}{2\sigma}$.

Thus $\beta\mu\beta^{-1} = \mu$ which is a contradiction.

Hence $Tr(\beta) = 0$ for all $\beta \in S$. So if $\beta \in S$ then all coefficients of β are integers. Since $(u,v,w) = 1$ there exists a 3×3 unimodular $\mathbb{Z}$-matrix

$$M = \begin{pmatrix} m_{11} & m_{12} & m_{13} \\ m_{21} & m_{22} & m_{23} \\ m_{31} & m_{32} & m_{33} \end{pmatrix}$$

with $M\begin{pmatrix} u \\ v \\ w \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$. Let $K = m_{21}i_1 + m_{22}i_2 + m_{23}i_3$ and let $\xi = m_{31}i_1 + m_{32}i_2 + m_{33}i_3$; K and ξ are in T, hence S. Also $\det M = \pm 1$ implies that the 3 2×2 minors of

$$\begin{pmatrix} m_{21} & m_{22} & m_{23} \\ m_{31} & m_{32} & m_{33} \end{pmatrix}$$

are relatively prime. So K and ξ form a $\mathbb{Z}$-module basis for S, which completes the proof that $S = T$ (see Smith [10], pg. 365).

The next two results deal with the action of U on E by left multiplication. The following table is included for reference;

the notation $\langle a,b,c,d\rangle$ is used to abbreviate $a + bi_1 + ci_2 + di_3$.

Table III. U/±1 acting on E by left multiplication

ε	$\varepsilon\langle a,b,c,d\rangle$
$\langle 1,0,0,0\rangle$	$\langle a,b,c,d\rangle$
$\langle 0,1,0,0\rangle$	$\langle -b,a,-d,c\rangle$
$\langle 0,0,1,0\rangle$	$\langle -c,d,a,-b\rangle$
$\langle 0,0,0,1\rangle$	$\langle -d,-c,b,a\rangle$
$\langle \frac{1}{2},\frac{1}{2},\frac{1}{2},\frac{1}{2}\rangle$	$\langle \frac{(a-b-c-d)}{2}, \frac{(a+b-c+d)}{2}, \frac{(a+b+c-d)}{2}, \frac{(a-b+c+d)}{2}\rangle$
$\langle -\frac{1}{2},\frac{1}{2},-\frac{1}{2},\frac{1}{2}\rangle$	$\langle \frac{(-a-b+c-d)}{2}, \frac{(a-b-c-d)}{2}, \frac{(-a+b-c-d)}{2}, \frac{(a+b+c-d)}{2}\rangle$
$\langle -\frac{1}{2},\frac{1}{2},\frac{1}{2},-\frac{1}{2}\rangle$	$\langle \frac{(-a-b-c+d)}{2}, \frac{(a-b+c+d)}{2}, \frac{(a-b-c-d)}{2}, \frac{(-a-b+c-d)}{2}\rangle$
$\langle -\frac{1}{2},-\frac{1}{2},\frac{1}{2},\frac{1}{2}\rangle$	$\langle \frac{(-a+b-c-d)}{2}, \frac{(-a-b-c+d)}{2}, \frac{(a+b-c+d)}{2}, \frac{(a-b-c-d)}{2}\rangle$
$\langle \frac{1}{2},-\frac{1}{2},-\frac{1}{2},-\frac{1}{2}\rangle$	$\langle \frac{(a+b+c+d)}{2}, \frac{(-a+b+c-d)}{2}, \frac{(-a-b+c+d)}{2}, \frac{(-a+b-c+d)}{2}\rangle$
$\langle \frac{1}{2},\frac{1}{2},\frac{1}{2},-\frac{1}{2}\rangle$	$\langle \frac{(a-b-c+d)}{2}, \frac{(a+b+c+d)}{2}, \frac{(a-b+c-d)}{2}, \frac{(-a-b+c+d)}{2}\rangle$
$\langle \frac{1}{2},-\frac{1}{2},\frac{1}{2},\frac{1}{2}\rangle$	$\langle \frac{(a+b-c-d)}{2}, \frac{(-a+b-c+d)}{2}, \frac{(a+b+c+d)}{2}, \frac{(a-b-c+d)}{2}\rangle$
$\langle \frac{1}{2},\frac{1}{2},-\frac{1}{2},\frac{1}{2}\rangle$	$\langle \frac{(a-b+c-d)}{2}, \frac{(a+b-c-d)}{2}, \frac{(-a+b+c-d)}{2}, \frac{(a+b+c+d)}{2}\rangle$

Lemma 1.5. Let $\delta = a + bi_1 + ci_2 + di_3 \in E$ and suppose ε is a unit for which we have either

(A) $\varepsilon\delta = a - bi_1 - ci_2 + di_3$

or (B) $\varepsilon\delta = a - bi_1 + ci_2 - di_3$

or (C) $\varepsilon\delta = a + bi_1 - ci_2 - di_3$.

Then for some $\rho \in U$, the quaternion $\rho\delta$ has 2 zero coefficients.

Assume (A) holds, so $\varepsilon\delta = a - bi_1 - ci_2 + di_3$. Then $\varepsilon\delta = i_3\delta\, i_3^{-1}$ so $i_3(\varepsilon\delta)i_3^{-1} = \delta$ so $\delta = (i_3\varepsilon\, i_3^{-1})(i_3\delta\, i_3^{-1}) = (i_3\varepsilon\, i_3^{-1})(\varepsilon\delta)$. (*)

From (*) we have $i_3\, \varepsilon\, i_3^{-1} = \varepsilon^{-1} = \overline{\varepsilon}$. By inspection of Table II we have $\varepsilon = \pm 1, \pm i_1$ or $\pm i_2$.

If $\varepsilon = 1$ then $a + bi_1 + ci_2 + di_3 = a - bi_1 - ci_2 + di_3$ so $b = c = 0$. Let $\rho = 1$.

If $\varepsilon = -1$ then $-a - bi_1 - ci_2 - di_3 = a - bi_1 - ci_2 + di_3$ so $a = d = 0$. Let $\rho = 1$.

If $\varepsilon = i_1$ then $-b + ai_1 - di_2 + ci_3 = a - bi_1 - ci_2 + di_3$ so $a = -b$ and $c = d$. Let $\rho = \frac{1}{2}(1 + i_1 - i_2 - i_3)$.

If $\varepsilon = -i_1$ then $b - ai_1 + di_2 - ci_3 = a - bi_1 - ci_2 + di_3$ so $a = b$ and $c = -d$. Let $\rho = \frac{1}{2}(1 + i_1 - i_2 - i_3)$.

If $\varepsilon = i_2$ then $-c + di_1 + ai_2 - bi_3 = a - bi_1 - ci_2 + di_3$ so $a = -c$ and $b = -d$. Let $p = \frac{1}{2}(1 + i_1 + i_2 + i_3)$.

If $\varepsilon = -i_2$ then $c - di_1 - ai_2 + bi_3 = a - bi_1 - ci_2 + di_3$ so $a = c$ and $b = d$. Let $\rho = \frac{1}{2}(1 - i_1 - i_2 - i_3)$.

Cases (B) and (C) are handled similarly.

Lemma 1.6. If α is an element of E then for some unit $\varepsilon \in U$, all coefficients of $\varepsilon\alpha$ are in $\mathbb{Z}$.

Proof. We need only consider $\alpha = \frac{a}{2} + \frac{b}{2}i_1 + \frac{c}{2}i_2 + \frac{d}{2}i_3$ where all of a, b, c, d are odd integers.

Case 1: $a \equiv b \equiv c \equiv d \bmod 4$.
In this case let $\varepsilon = \frac{1}{2}(1 - i_1 - i_2 - i_3)$. Then $Tr(\varepsilon\alpha) = \frac{1}{4}(a+b+c+d)$ so $Tr(\varepsilon\alpha) \in \mathbb{Z}$. It follows that all coefficients of $\varepsilon\alpha$ are in $\mathbb{Z}$.

Case 2: Exactly three of a, b, c, d are congruent mod 4.
If $-a \equiv b \equiv c \equiv d \bmod 4$ let $\varepsilon = \frac{1}{2}(1 + i_1 + i_2 + i_3)$.
Then $Tr(\varepsilon\alpha) = \frac{1}{4}(a - b - c - d)$ so $Tr(\varepsilon\alpha) \in \mathbb{Z}$, hence all coefficients of $\varepsilon\alpha$ are in $\mathbb{Z}$. If $a \equiv -b \equiv c \equiv d \bmod 4$ let $\varepsilon = \frac{1}{2}(1 + i_1 - i_2 - i_3)$, if $a \equiv b \equiv -c \equiv d \bmod 4$ let $\varepsilon = \frac{1}{2}(1 - i_1 + i_2 - i_3)$ and if $a \equiv b \equiv c \equiv -d \bmod 4$ let $\varepsilon = \frac{1}{2}(1 - i_1 - i_2 + i_3)$. In each of these cases we have $Tr(\varepsilon\alpha) \in \mathbb{Z}$ so all coefficients of $\varepsilon\alpha$ are in $\mathbb{Z}$.

Case 3: Two of a, b, c, d are congruent to 1 mod 4, and two of a, b, c, d are congruent to -1 mod 4, so $a + b + c + d \equiv 0 \bmod 4$.
Let $\varepsilon = \frac{1}{2}(1 - i_1 - i_2 - i_3)$. Then $Tr(\varepsilon\alpha) = \frac{1}{4}(a+b+c+d)$ so all coefficients of $\varepsilon\alpha$ are in $\mathbb{Z}$.

Chapter 2. Venkow's Proof of Theorem 1.1.

In this section we sketch Venkow's proof of Theorem 1.1. The proof in detail can be found (in Russian) in Venkow's original paper and a somewhat modernized proof can be found in the article by Rehm [9].

Let m be an integer greater than 3 with $m \equiv 1, 2 \bmod 4$ or $m \equiv 3 \bmod 8$. Let $T(m)$ denote the set of triples $(x,y,z) \in \mathbb{Z}^3$ with $\gcd(x,y,z) = 1$, and $x^2 + y^2 + z^2 = m$. According to the notation of Theorem 1.1, $t(m)$ denotes the size of $T(m)$.

The mapping $(x,y,z) \leftrightarrow xi_1 + yi_2 + zi_3$ is a 1 - 1 correspondence between the elements of $T(m)$ and the Hurwitz quaternions of norm m and trace 0 having relatively prime coefficients. Let $B_1(m)$ denote the set of bundles $[\mu]$ with $N([\mu]) = m$, $Tr([\mu]) = 0$ and $c([\mu]) = 1$. Combining the 1 - 1 correspondence above with the fact that all bundles in $B_1(m)$ have size 12 (by Lemma 1.3) gives that $12|B_1(m)| = t(m)$. So to prove Theorem 1.1 it suffices to prove the following two equalities;

$$\begin{aligned} |B_1(m)| &= h(m) \quad \text{if} \quad m \equiv 1, 2 \bmod 4 \\ |B_1(m)| &= 2h(m) \quad \text{if} \quad m \equiv 3 \bmod 8. \end{aligned} \tag{2.1}$$

To prove the equalities (2.1) Venkow made use of an action of the ring class group $\Gamma(m)$ on $B_1(m)$ which we now discuss in some detail.

Let $\theta \in B_1(m)$ and let $\mu = ui_1 + vi_2 + wi_3$ be an element of θ. Then $N\mu = m$ and $Tr\mu = 0$ so μ satisfies the minimal equation $x^2 + m = 0$ over $\mathbb{Q}$. Hence the mapping $\sqrt{-m} \to \mu$ induces a field isomorphism from $\mathbb{Q}(\sqrt{-m})$ onto $\mathbb{Q}(\mu)$ which maps the suborder $\mathcal{O}_f$ onto $E \cap \mathbb{Q}(\mu)$. This isomorphism establishes a 1 - 1 correspondence

between integral ideals of the suborder $\mathcal{O}_f$ and ideals in the ring $E \cap \mathbb{Q}(\mu)$. If $\mathfrak{a} = (a, b+\mu)$ is an integral ideal of $\mathcal{O}_f$ we let $\mathfrak{a}_\mu$ denote its image $\mathfrak{a}_\mu = (a, b+\mu)$ in $E \cap \mathbb{Q}(\mu)$.

To define Venkow's action of $\Gamma(m)$ on $B_1(m)$ we start with an action of the semigroup of regular integral ideals on $B_1(m)$. We first need two facts.

Lemma 2.1. (Venkow [12] or Rehm [9], pg. 6) Let $\mathfrak{a}$ be a regular integral ideal of $\mathcal{O}_f$ and let $\theta \in B_1(m)$. If μ_1, μ_2 are elements of θ and K_1, K_2 are elements of E which satisfy $E\mathfrak{a}_{\mu_1} = EK_1$ and $E\mathfrak{a}_{\mu_2} = EK_2$, then

(a) $(K_1\mu_1K_1^{-1})$ and $(K_2\mu_2K_2^{-1})$ are elements of E with relatively prime coefficients.

(b) $[K_1\mu_1K_1^{-1}] = [K_2\mu_2K_2^{-1}]$.

Definition 2.1. Let $\mathfrak{a}$ be a regular integral ideal of $\mathcal{O}_f$. Define a map $\Pi_{\mathfrak{a}}$ from $B_1(m)$ to $B_1(m)$ in the following way; given a bundle $\theta \in B_1(m)$, choose $\mu \in \theta$ and $K \in E$ such that $E\mathfrak{a}_\mu = EK$. Let $\Pi_{\mathfrak{a}}(\theta) = [K\mu K^{-1}]$.

By Lemma 2.1 the map $\Pi_{\mathfrak{a}}$ is well-defined and maps $B_1(m)$ into $B_1(m)$.

Example 2.1. Let $m = 41$, let $\mathfrak{a}$ be the principal ideal $(5+8\sqrt{-41})$ and let $\theta = [1,6,2]$. Choose $\mu = i_1 + 6i_2 + 2i_3$ so $\mathfrak{a}_\mu = (E \cap \mathbb{Q}(\mu))(5+8\mu)$. Thus $E\mathfrak{a}_\mu = E(5+8\mu)$ so we can choose $K = 5 + 8\mu$. Hence $\Pi_{\mathfrak{a}}([\mu]) = [(5+8\mu)\mu(5+8\mu)^{-1}] = [\mu]$. In this case $\Pi_{\mathfrak{a}}$ fixes θ.

Next let $\mathfrak{I} = (3, 1+\sqrt{-41})$ and let $\theta = [0,4,5]$. Choose

$\mu = 4i_2 + 5i_3$ so $E\mathfrak{J}_\mu = \{e_1 3 + e_2(1+\mu) : e_1, e_2 \in E\}$. In example 1.3 we showed that $(1 + i_2 - i_3)$ is a greatest common right divisor of 3 and $1 + \mu$ hence we may choose $K = (1 + i_2 - i_3)$. So

$$\Pi_{\mathfrak{J}}([0,4,5]) = [(1 + i_2 - i_3)(4i_2 + 5i_3)(1 + i_2 - i_3)^{-1}] = [1,6,2].$$

Venkow proved the following very important result.

Lemma 2.2. (Venkow [12] or Rehm [9], pg. 6) Let $\mathfrak{a}$ and $\mathfrak{J}$ be regular integral ideals of $\mathcal{O}_f$, and let θ be an element of $B_1(m)$. Then

(a) $\Pi_{\mathfrak{a}\mathfrak{J}}(\theta) = \Pi_{\mathfrak{a}}(\Pi_{\mathfrak{J}}(\theta))$.

(b) If $\mathfrak{a}$ and $\mathfrak{J}$ are in the same class of $\Gamma(m)$ then $\Pi_{\mathfrak{a}} = \Pi_{\mathfrak{J}}$.

Definition 2.2. Let $\mathcal{C}$ be a class in $\Gamma(m)$, and let $\theta \in B_1(m)$. Define $\mathcal{C}(\theta)$ to be $\Pi_{\mathfrak{a}}(\theta)$ for $\mathfrak{a}$ an ideal chosen from $\mathcal{C}$.

Note that $\Pi_{\mathfrak{a}}(\theta)$ is independent of the choice of $\mathfrak{a} \in \mathcal{C}$ by Lemma 2.2 (b) so $\mathcal{C}(\theta)$ is well-defined. Also by Lemma 2.2 (a) we have

$$(\mathcal{C}\mathcal{D})(\theta) = \mathcal{C}(\mathcal{D}(\theta))$$

for all $\mathcal{C}, \mathcal{D} \in \Gamma(m)$ and $\theta \in B_1(m)$. So $\mathcal{C} : \theta \to \mathcal{C}(\theta)$ is an action of $\Gamma(m)$ on $B_1(m)$. The main result of Venkow's original paper on this subject is the following fact about this action.

Theorem 2.1. (Venkow [12] or Rehm [9], pg. 9) Let $\Gamma(m)$ act on $B_1(m)$ as above.

(a) If $\theta \in B_1(m)$ and $\mathcal{C} \in \Gamma(m)$, then $\mathcal{C}(\theta) = \theta$ iff $\mathcal{C}$ is the class of principal ideals (i.e. the identity in $\Gamma(m)$).

(b) If $m \equiv 1, 2 \bmod 4$ then $\Gamma(m)$ acts transitively on $B_1(m)$.

(c) If $m \equiv 3 \bmod 8$ then $B_1(m)$ splits into exactly two orbits.

As a corollary of this theorem we have the equalities labelled (2.1).

Corollary 2.1. (Venkow [12] or Rehm [9], pg. 10) If $m \equiv 1, 2 \bmod 4$ then $|\Gamma(m)| = |B_1(m)|$ and if $m \equiv 3 \bmod 8$ then $2|\Gamma(m)| = |B_1(m)|$.

Proof. Let $\theta \in B_1(m)$. Then the size of the orbit containing θ is $|\Gamma(m)|$ divided by the size of the stabilizer in $\Gamma(m)$ of θ. By Theorem 2.1, only the identity stabilizes θ so the size of the orbit containing θ is $|\Gamma(m)|$. This corollary follows immediately from Theorem 2.1 (b), (c).

Example 2.2. Let $m = 41$. Since $m \equiv 1 \bmod 4$ we know that $\Gamma(41)$ acts transitively on $B_1(41)$. Let $\theta = [0,4,5]$. If C_1 and C_2 are distinct classes in $\Gamma(m)$ then $C_1(\theta)$ and $C_2(\theta)$ must be distinct bundles. Otherwise we have $C_1(\theta) = C_2(\theta)$ so $(C_2^{-1}C_1)(\theta) = \theta$. Hence the nontrivial class $C_2^{-1}C_1$ stabilizes θ which contradicts Theorem 2.1. So given any bundle $[u,v,w] \in B_1(41)$ there is a unique class mapping θ to $[u,v,w]$. Below we see $B_1(41)$; beside each bundle $[u,v,w]$ is the unique class $\mathcal{S} \in \Gamma(41)$ with $\mathcal{S}([0,4,5]) = [u,v,w]$. Recall from Example 1.1 that $\Gamma(41)$ is cyclic of order 8 generated by the class C which contains $\sigma = (3,1+\sqrt{-41})$.

$[0,4,5]$ 1

$[0,5,4]$ C^4

$[3,4,4]$ C^2	$[-3,-4,-4]$ C^6
$[1,2,6]$ C^3	$[-1,-2,-6]$ C^5
$[1,6,2]$ C	$[-1,-6,-2]$ C^7

Note that $\mathcal{C}^i$ and $\mathcal{C}^{-i}$ lie opposite the vertical symmetry line and that $\mathcal{C}^4$ maps [u,v,w] to [-u,-w,-v] for all bundles [u,v,w].

This elegant proof of Theorem 1.1 was the content of Venkow's 1923 paper. The ideas can be pushed a bit further by considering the semigroup of classes of integral ideals rather than just the group of classes of regular integral ideals. This generalization is delayed until more machinery has been established.

Chapter 3. A Closer Look at Venkow's Work.

In this section we study the action of $\Gamma(m)$ on $B_1(m)$ in more detail. Our method of attack is to study the greatest common right divisor $K \in E$ which arises when we write $E\mathfrak{A}_\mu = EK$. From facts about these greatest common divisors K we derive facts about the mapping $\Pi_{\mathfrak{A}}$.

Definition 3.1. Let K and μ be elements of E and suppose the minimal equation of μ over $\mathbb{Q}$ is $x^2 + m = 0$. We say K is an *ideal quaternion with respect to* μ if there exists an integral ideal $\mathfrak{A}$ of $\mathfrak{O}_f$ which satisfies $E\mathfrak{A}_\mu = EK$.

We begin with two lemmas concerning ideal quaternions, the first of which is due to Venkow.

Lemma 3.1. (Venkow [12]) Let $\mathfrak{A}$ be an integral ideal of $\mathfrak{O}_f$ and let $K \in E$. If $E\mathfrak{A}_\mu = EK$, then

$$\mathfrak{A}_\mu = (EK \cap \mathbb{Q}(\mu)).$$

A consequence of Lemma 3.1 is that if K is an ideal quaternion with respect to μ then there is a unique integral ideal $\mathfrak{A}$ of $\mathfrak{O}_f$ which satisfies $E\mathfrak{A}_\mu = EK$.

Let μ be an element of E which satisfies $x^2 + m = 0$ and let K be any element of E. Then $EK \cap \mathbb{Q}(\mu) \subseteq EK$ so

(*) $E(EK \cap \mathbb{Q}(\mu)) \subseteq EK$.

Lemma 3.1 says that K is an ideal quaternion with respect to μ iff the inclusion in (*) is an actual equality.

Lemma 3.2. Let m be congruent to 1 or 2 mod 4. Let K be an ideal quaternion with respect to μ and let $\mathfrak{A}$ be the integral ideal of $\mathcal{O}_f$ which satisfies $\mathfrak{A}_\mu = EK \cap \mathbb{Q}(\mu)$. Then $NK = N\mathfrak{A}$ where $N\mathfrak{A}$ denotes the norm of $\mathfrak{A}$ as an ideal in $\mathcal{O}_f$ (i.e. the index $\mathfrak{A}$ in $\mathcal{O}_f$), and where NK denotes $K\bar{K}$, the quaternion norm of K.

Proof: Without loss of generality we may assume that $\mathfrak{A}$ cannot be written in the form $z\mathfrak{J}$ where $z \in \mathbb{Z}$ and $\mathfrak{J}$ is an integral ideal. Assume $\mathfrak{A} = (a, b+\mu)$ where $a, b \in \mathbb{Z}$ and $a > 0$. We must show $a = K\bar{K}$.

Consider $EK \cap \mathbb{Z}$. This is an ideal of $\mathbb{Z}$ which contains NK so $EK \cap \mathbb{Z} = s\mathbb{Z}$ where $s \mid NK$. Write $s = eK$ for $e \in E$. Now

$$NK = (\frac{NK}{s})s = (\frac{NK}{s})eK = (\frac{NK}{s})(\bar{e}\bar{K}) = (\frac{NK}{s})\bar{K}\bar{e} = \bar{K}(\frac{NK}{s})\bar{e}.$$

Multiplying both sides of this equation on the left by $(\bar{K})^{-1}$ we have $K = (\frac{NK}{s})\bar{e}$. Hence

$$\mathfrak{A}_\mu = (EK \cap \mathbb{Q}(\mu)) = (E(\frac{NK}{s})\bar{e} \cap \mathbb{Q}(\mu)) = (\frac{NK}{s})(E\bar{e} \cap \mathbb{Q}(\mu))$$

so $\mathfrak{A}_\mu = (\frac{NK}{s})\mathfrak{J}_\mu$ where $\mathfrak{J}_\mu$ is the integral ideal of $\mathbb{Z}[\mu]$ given by $(E\bar{e} \cap \mathbb{Q}(\mu))$. By hypothesis, $\frac{NK}{s} = 1$ so $EK \cap \mathbb{Z} = (NK)\mathbb{Z}$. Thus

$$(NK)\mathbb{Z} = (EK \cap \mathbb{Z}) = (EK \cap \mathbb{Q}) \cap \mathbb{Z} = \mathfrak{A}_\mu \cap \mathbb{Z} = a\mathbb{Z}$$

hence $a = NK$ as was to be shown.

Example 3.1: Let $m = 41$ and $\mathfrak{A} = (3, 1+\sqrt{-41})$. If $\mu = 4i_2 + 5i_3$ then $E\mathfrak{A}_\mu = EK$ where $K = \frac{1}{2}(-1-3i_1-i_2+i_3)$. Note $NK = 3 = N\mathfrak{A}$. Next let $\eta = i_1 + 2i_2 + 6i_3$. Here $E\mathfrak{A}_\eta = EK_1$ where $K_1 = \frac{1}{2}(-1-i_1+i_2+3i_3)$. Again $NK_1 = 3$.

The next theorem gives a characterization of ideal quaternions which is in practice more applicable than the definition. We do not assume in this theorem that the coefficients of μ are relatively prime.

Theorem 3.1. Let $K \in E$ and suppose NK is an odd prime. Then K is an ideal quaternion with respect to μ iff $K\mu K^{-1} \in E$.

Proof. The forward direction is a result due to Venkow which was stated earlier as Lemma 2.1 (a). Conversely, suppose $K\mu K^{-1}$ is an element of E. Our first step is to reduce to the case where $K = a + bi_1 + ci_2 + di_3$ with $a, b, c, d \in \mathbb{Z}$ and $a \not\equiv 0 \bmod p$.

Let ε be a unit. Then εK is an ideal quaternion with respect to μ iff K is an ideal quaternion with respect to μ and $K\mu K^{-1} \in E$ iff $(\varepsilon K)\mu(\varepsilon K)^{-1} \in E$. Furthermore $NK = N\varepsilon K$ so without loss of generality we may premultiply K by any unit ε. Therefore by Lemma 1.6 we may assume that $a, b, c, d \in \mathbb{Z}$. Premultiply K by $1, i_1, i_2$ or i_3 so that $a \not\equiv 0 \bmod p$. Let $\mu = ui_1 + vi_2 + wi_3$; our first step is to compute $K\mu\overline{K}$.

$$\begin{aligned} K\mu\overline{K} = {} & i_1(up - 2u(c^2 + d^2) + 2v(bc - ad) + 2w(ac + bd)) \\ & + i_2(vp - 2v(b^2 + d^2) + 2u(ad + bc) + 2w(-ab + cd)) \\ & + i_3(wp - 2w(b^2 + c^2) + 2u(-ac + bd) + 2v(ab + cd)). \end{aligned}$$

The condition $K\mu K^{-1} \in E$ together with the fact that p is odd gives us the following three congruences from the above expression for $K\mu\overline{K}$;

(A) $-u(c^2 + d^2) + v(bc - ad) + w(ac + bd) \equiv 0 \bmod p$

(B) $-v(b^2 + d^2) + u(ad + bc) + w(-ab + cd) \equiv 0 \bmod p$

(C) $-w(b^2 + c^2) + u(-ac + bd) + v(ab + cd) \equiv 0 \bmod p.$

Choose $\ell \in \{0,1,2,\ldots,p-1\}$ such that

(D) $a\ell + bu + cv + dw \equiv 0 \bmod p.$

$$\begin{aligned} a(-b\ell + au + cw - dv) &\equiv -b(-bu - cv - dw) + a^2u + acw - adv \\ &\equiv u(a^2 + b^3) + v(-ad + bc) + w(ac + bd) \\ &\equiv up + (-u(c^2 + d^2) + v(bc - ad) + w(ac + bd) \\ &\equiv 0 \bmod p \text{ by congruence (A).} \end{aligned}$$

Thus we have

(E) $-b\ell + (au + cw - dv) \equiv 0 \bmod p.$

Similarly we obtain

(F) $-c\ell + (av - bw + du) \equiv 0 \bmod p$ using congruence (B)

(G) $-d\ell + (aw + bv - cu) \equiv 0 \bmod p$ using congruence (C).

Now

$$\begin{aligned} (\ell + \mu)\overline{K} = {} & (a\ell + bu + cv + dw) \\ & + i_1(-b\ell + (au + cw - dv)) \\ & + i_2(-c\ell + (av - bw + du)) \\ & + i_3(-d\ell + (aw + bv - cu)). \end{aligned}$$

The congruences (D)-(G) imply that $(\ell + \mu)K^{-1} = \rho \in E$ so $\rho K = \ell + \mu$. Hence $\mathcal{O}_\mu = (p, \ell + \mu)$ and $EK = E\mathcal{O}_\mu$ as $N(K) = N\mathcal{O}_\mu = p$.

Example 3.2. Let $m = 59$, let $\mu = i_1 + 3i_2 + 7i_3$ and let $K_1 = 2 + i_1$. Then $K_1\mu K_1^{-1} = i_1 - (\frac{19}{5})i_2 + (\frac{33}{5})i_3$ so K_1 is not an ideal quaternion with respect to μ.

Next let $K = 2i_1 + i_2$. Then $K\mu K^{-1} = 3i_1 - i_2 - 7i_3$ so K is an ideal quaternion with respect to μ. The proof of Theorem 3.1

describes how to find the ideal $EK \cap \mathbb{Q}(\mu)$. First premultiply K by a unit εK so that $Tr(\varepsilon K) \not\equiv 0 \bmod NK$. In our case let $\varepsilon = i_1$ so $Tr(\varepsilon K) = -4$, and $\varepsilon K = -2 + i_3$. Writing $\varepsilon K = a + bi_1 + ci_2 + di_3$ and $\mu = ui_1 + vi_2 + wi_3$ we need to find ℓ between 0 and 4 such that $a\ell + bu + cv + dw \equiv 0 \bmod NK$. So in our case we need $-2\ell + 7 \equiv 0 \bmod 5$. Choose $\ell = 1$. Then $EK \cap \mathbb{Q}(\mu) = (NK, \ell + \mu) = (5, 1 + \mu)$.

The reverse direction of Theorem 3.1 is false in the case $p = 2$. Consider for example $m = 11$ with $\mu = i_1 + 3i_2 + i_3$ and $k = i_2 - i_3$. Here $K\mu K^{-1} = -i_1 - i_2 - 3i_3$ so $K\mu K^{-1} \in E$, but EK does not equal $E\mathcal{O}_\mu$ for any ideal $\mathcal{O}$ of $\mathcal{O}^-$. To see this, suppose to the contrary that $\mathcal{O}$ is an ideal of $\mathcal{O}^-$ and $E\mathcal{O}_\mu = EK$. Then $N\mathcal{O} = 2$ by Lemma 3.2, but 2 remains prime in the extension $\mathbb{Q}(\sqrt{-11})$ so there are no ideals of norm 2. The next theorem discusses the case $p = 2$.

Theorem 3.2. Let $K \in E$ with $NK = 2$ and let μ be an element of E with $N\mu = m$ and $Tr\mu = 0$. Then K is an ideal quaternion with respect to μ if $m \equiv 1, 2 \bmod 4$, and is not if $m \equiv 3 \pmod 8$.

Proof. Let $a + bi_1 + ci_2 + di_3$ be a Hurwitz quaternion of norm 2. Since 8 cannot be written as a sum of four odd squares we have $a, b, c, d \in \mathbb{Z}$. Thus exactly two of a, b, c, d are 0 and the other two are ± 1. So there are exactly 24 Hurwitz quaternions of norm 2 which are listed below:

$$\pm 1 \pm i_1 \qquad \pm 1 \pm i_2 \qquad \pm 1 \pm i_3$$

$$\pm i_1 \pm i_2 \qquad \pm i_1 \pm i_3 \qquad \pm i_2 \pm i_3.$$

Hence if μ_1 and μ_2 are Hurwitz quaternions of norm 2 then $\mu_1 = \varepsilon\mu_2$ for some unit ε. So either all Hurwitz quaternions of norm 2 are ideal

quaternions with respect to μ or no Hurwitz quaternions of norm 2 are ideal quaternions with respect to μ. The former case occurs exactly when there are integral ideals of norm 2, by Lemma 3.1. This is true iff $m \equiv 1, 2 \bmod 4$ (see Cohn [1], pg. 90).

For the remainder of this section we let C_2 denote the class in $\Gamma(m)$ which contains the prime divisor of (2). If $m \equiv 3 \bmod 8$ then C_2 is the identity class, but for $m \equiv 1, 2 \bmod 4$, C_2 is nontrivial. The action of C_2 on $B_1(m)$ is described in the following corollary to Theorem 3.2.

Corollary 3.1. If $m \equiv 1, 2 \bmod 4$ and $[u,v,w] \in B_1(m)$ then

$$C_2([u,v,w]) = [-u,-w,-v].$$

In particular, C_2 has order 2.

Proof. Since $m \equiv 1, 2 \bmod 4$, there exist ideals $\mathfrak{A}$ in $\mathcal{O}_f$ of norm 2. Let μ denote the quaternion $ui_1 + vi_2 + wi_3$. Then $E\mathfrak{A}_\mu = E(i_2 - i_3)$ since any pair of Hurwitz quaternions of norm 2 differ by left unit multiplication (see proof of Theorem 3.2).

Note $(i_2 - i_3)(ui_1 + vi_2 + wi_3)(i_2 - i_3)^{-1} = -ui_1 - wi_2 - vi_3$

which completes the proof.

Example 3.3. Let $m = 41$. Then $C_2 = C^4$ where C is the class containing the ideal $(3, 1 + \sqrt{-41})$ (see Example 1.1).

By Corollary 3.1 we have

$$C_2([0,4,5]) = [0,-5,-4] = [0,5,4]$$

$$C_2([3,4,4]) = [-3,-4,-4]$$

and $$C_2([1,2,6]) = [-1,-6,-2].$$

In the case $m \equiv 3 \bmod 8$, the set $B_1(m)$ breaks into two orbits under the action of $\Gamma(m)$ according to the rule $[u,v,w]$ and $[-u,-w,-v]$ lie in distinct orbits. Conjugation by the quaternion $K = i_2 - i_3$ sends $(ui_1 + vi_2 + wi_3)$ to $(-ui_1 - wi_2 - vi_3)$ but in the case $m \equiv 3 \bmod 8$, K is not the greatest common right divisor of an ideal $E\mathcal{O}_\mu$. This will not be proved here.

The next simple observation will turn out to be very important.

Lemma 3.3. Let $\mathcal{C}$ be a class in $\Gamma(m)$ and let $[\eta]$ and $[\mu]$ be in $B_1(m)$. Suppose $\mathcal{C}([\mu]) = [\eta]$. Then $\mathcal{C}^{-1}([-\mu]) = [-\eta]$.

Proof. Let $\mathcal{O}$ be an ideal in $\mathcal{C}$; choose K in E such that $E\mathcal{O}_\mu = EK$ and $K\mu K^{-1} = \eta$. Write $\mathcal{O}_\mu = (a, b + \mu)$ and observe that $\mathcal{O}'_{-\mu} = (a, b-(-\mu)) = (a, b+\mu)$. Hence $E\mathcal{O}'_{-\mu} = EK$ and so K is a greatest common right divisor for the ideal $E\mathcal{O}'_{-\mu}$. Also $\mathcal{O}'$ is the class $\mathcal{C}^{-1}$ so

$$\mathcal{C}^{-1}([-\mu]) = [K(-\mu)K^{-1}] = [-(K\mu K^{-1})] = [-\eta].$$

The next theorem is an immediate consequence of Lemma 3.3.

Theorem 3.3. Let $[\mu]$ be a bundle in $B_1(m)$ and let $\mathcal{D}$ be the class in $\Gamma(m)$ which maps $[\mu]$ to $[-\mu]$. If $\mathcal{C}$ is in $\Gamma(m)$ and $\mathcal{C}([\mu]) = [\eta]$ then $\mathcal{D}\mathcal{C}^{-1}([\mu]) = [-\eta]$.

Example 3.4. Let $m = 173$. We have $h(m) = 14$; the set $B_1(m)$ is listed below:

$$[10,8,3] \qquad [-10,-8,-3]$$

$$[10,3,8] \qquad [-10,-3,-8]$$

$$[11,6,4] \qquad [-11,-6,-4]$$

$$[11,4,6] \qquad [-11,-4,-6]$$

$$[12,5,2] \qquad [-12,-5,-2]$$

$$[12,2,5] \qquad [-12,-2,-5]$$

$$[0,2,13]$$

$$[0,13,2]$$

Let μ be $10i_1 + 8i_2 + 3i_3$ and let $\mathfrak{D}$ be the class in $\Gamma(m)$ containing the ideal $\mathfrak{A} = (9, 4-\sqrt{-173})$. Then $E\mathfrak{A}_\mu = EK$ where $K = 2 - 2i_1 - 2i_2$ and $K\mu K^{-1} = -\mu$. Thus $\mathfrak{D}([10,8,3]) = [-10,-8,-3]$.

Let $\mathfrak{C}$ be the ideal class containing the ideal $\mathfrak{J} = (19, 6-\sqrt{-173})$, and let $\mu = 10i_1 + 8i_2 + 3i_3$ as above. Then $E\mathfrak{J}_\mu = E\rho$ where $\rho = \frac{1}{2}(7 + 5i_1 + i_2 + i_3)$, and $\rho\mu\rho^{-1} = 10i_1 + 3i_2 + 8i_3$. So $\mathfrak{C}([10,8,3]) = [10,3,8]$.

$$\begin{array}{ccc} [10,8,3] & \xrightarrow{\quad\mathfrak{D}\quad} & [-10,-8,-3] \\ \mathfrak{C}\downarrow & \nearrow_{\mathfrak{D}\mathfrak{C}^{-1}} & \\ [10,3,8] & & [-10,-3,-8] \end{array}$$

By theorem 3.3 we have

$$(\mathfrak{A}\mathfrak{C}^{-1})([10,8,3]) = [-10,-3,-8].$$

Also by theorem 3.2 we have $\mathfrak{C}_2([10,8,3]) = [-10,-3,-8]$. So $\mathfrak{C}_2 = \mathfrak{A}\mathfrak{C}^{-1}$ and $\mathfrak{C} = \mathfrak{A}\mathfrak{C}_2$.

Next let $\mathfrak{F}$ be the class which satisfies $\mathfrak{F}([10,8,3]) = [0,4,13]$. By Theorem 3.3 we have

$$(\mathfrak{A}\mathfrak{F}^{-1})([10,8,3]) = [0,-2,-13].$$

But $[0,2,13] = [0,-2,-13]$ and so $\mathfrak{A}\mathfrak{F}^{-1} = \mathfrak{F}$. Consequently

$$\mathfrak{A} = \mathfrak{F}^2$$

so $\mathfrak{A}$ is in the principal genus.

Lastly note that since $\Gamma(m)$ has order 14, it can be written as $\mathbb{Z}_2 \times \mathbb{Z}_7$. Since $\mathfrak{A}$ is a square, it must have order 7 and $\mathfrak{C}_2$ is known to be the unique class of order 2. Hence $\Gamma(m) \cong \langle \mathfrak{C}_2 \rangle \times \langle \mathfrak{A} \rangle$ and so $\Gamma(m)$ is cyclically generated by $\mathfrak{C} = \mathfrak{A}\mathfrak{C}_2$.

We now list and illustrate several corollaries to Theorem 3.3.

Corollary 3.2. Suppose m can be written as a sum of 2 squares. Say $m = r^2 + s^2$. Let $\mathfrak{C} \in \Gamma(m)$ and suppose $\mathfrak{C}([0,r,s]) = [u,v,w]$. Then

(a) $\mathfrak{C}^{-1}([o,r,s]) = [-u,-v,-w]$.

(b) $\mathfrak{C}^2 = 1$ iff one of u, v or w is 0.

(c) If two of u, v or w have equal absolute values, then $\mathfrak{C}$ has order 4 and $\mathfrak{C}^2 = \mathfrak{C}_2$.

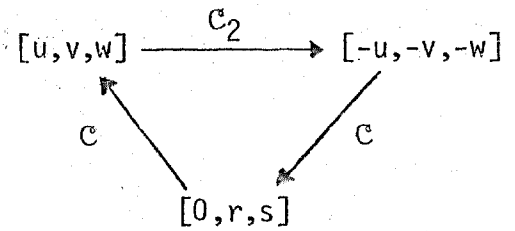
(d) $\mathfrak{C}$ is in the principal genus (i.e. $\mathfrak{C}$ is a square in $\Gamma(m)$) iff $\mathfrak{C}([\mu]) = [-\mu]$ for some $[\mu] \in B_1(m)$.

(e) $\mathcal{C}$ has order 3 iff all of u, v and w are nonzero and $\mathcal{C}([u,v,w]) = [-u,-v,-w]$.

Proof: (a) Let $\mu = ri_1 + si_2$. Since $[\mu] = [-\mu]$ we have $1([\mu]) = [-\mu]$ where 1 denotes the identity class in $\Gamma(m)$. Part (a) now follows from Theorem 3.3.

(b) $\mathcal{C}^2 = 1$ iff $\mathcal{C}([0,r,s]) = \mathcal{C}^{-1}([0,r,s])$. By part (a) $\mathcal{C}^{-1}([0,r,s]) = [-u,-v,-w]$ and so $\mathcal{C}^2 = 1$ iff $[u,v,w] = [-u,-v,-w]$ iff one of u, v or w is 0.

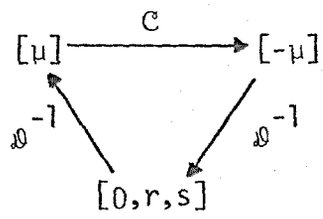
(c) Assume that two of u, v or w have equal absolute values. Without loss of generality we may assume that $v = w$. Thus $-ui_1 - vi_2 - wi_3 = -ui_1 - wi_2 - vi_3$ so $\mathcal{C}_2([u,v,w]) = [-u,-v,-w]$.



Note that $\mathcal{C}([-u,-v,-w]) = [0,r,s]$ by part (a) and so $\mathcal{C}\mathcal{C}_2\mathcal{C}([0,r,s]) = [0,r,s]$. It follows that $\mathcal{C}\mathcal{C}_2 = 1$ so $\mathcal{C}_2 = \mathcal{C}^2$ (since $\mathcal{C}_2^{-1} = \mathcal{C}_2$). This proves part (c).

(d) First assume that $\mathcal{C}$ is in the principal genus; say $\mathcal{C} = \mathcal{D}^2$. Let $[\mu] = \mathcal{D}^{-1}([0,r,s])$ so $\mathcal{D}([0,r,s]) = [-\mu]$ by part (a). Hence $\mathcal{C}([\mu]) = \mathcal{D}^2(\mathcal{D}^{-1}([0,r,s])) = \mathcal{D}([0,r,s]) = [-\mu]$.

Conversely suppose $\mathcal{C}([\mu]) = [-\mu]$. Choose $\mathcal{D}$ such that $\mathcal{D}^{-1}([0,r,s]) = [\mu]$. Then $\mathcal{D}([0,r,s]) = [-\mu]$ so $\mathcal{D}^{-1}([-\mu]) = [0,r,s]$. Hence $\mathcal{C}\mathcal{D}^{-2}([0,r,s]) = [0,r,s]$.



Hence $C\mathcal{O}^{-2} = 1$ so $C = \mathcal{O}^2$.

(e) First suppose that C has order 3. Then all of u, v and w are nonzero by (b). Also $C^{-1} = C^2$ so

$$C([u,v,w]) = C(C([0,r,s])) = C^2([0,r,s]) = C^{-1}([0,r,s]) = [-u,-v,-w].$$

The last equality holding by (a).

Conversely suppose $C([u,v,w]) = [-u,-v,-w]$ and that all of u, v and w are nonzero. Then

$C^2[0,r,s]) = C([u,v,w]) = [-u,-v,-w] = C^{-1}([0,r,s])$ again by (a).

So by Theorem 2.1 (a) $C^2 = C^{-1}$ and $C^3 = 1$. If $C = 1$ then $[u,v,w] = [0,r,s]$ so one of u, v or w is 0.

Example 3.5. Let $m = 41$. Note $m = r^2 + s^2$ where $r = 4$ and $s = 5$. Below we see the same figure as in Example 2.2. The 8 bundles in $B_1(m)$ appear; beside each bundle $[\mu]$ is the class C^i which maps $[0,4,5]$ to $[\mu]$.

$[0,4,5]$ 1

$[0,5,4]$ C^4

$[3,4,4]$ C^2 $\qquad$ $[-3,-4,-4]$ C^6

$[1,2,6]$ C^3 $\qquad$ $[-1,-2,-6]$ C^5

$[1,6,2]$ C $\qquad$ $[-1,-6,-2]$ C^7

Note that C^i and C^{-i} map $[0,4,5]$ to bundles $[\mu]$ and $[-\mu]$ respectively. This is the statement of Corollary 3.2 (a). The subgroup of squares in $\Gamma(m)$ is the subgroup $\{1, C^2, C^4, C^6\}$. By inspection of the diagram above one sees that these are exactly the classes which map $[\mu]$ to $[-\mu]$ for some bundle $[\mu]$. This is the statement of Corollary 3.2 (d).

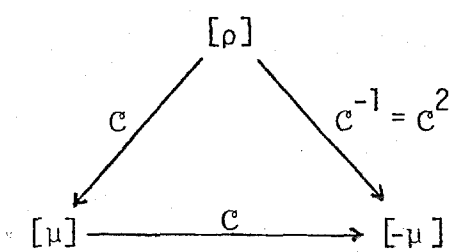
In the next example we consider, for the prime $p = 3$, a question which we take up in the next chapter for all primes p. This example is intended to display some of the basic ideas which we will use in Chapter 4.

Example 3.6. In this example we use Corollary 3.2 (e) to find all m which satisfy properties (i) and (ii) below;

(i) m can be written as a sum of two squares.

(ii) (3) splits in $\mathbb{Q}(\sqrt{-m})$ and the prime divisors of (3) are regular ideals in classes of order 3 in the ring class group $\Gamma(m)$ with discriminant $-4m$.

Let m satisfy (i) and (ii); write $m = r^2 + s^2$ with $\gcd(r,s) = 1$ and let $\mathfrak{p}$ and $\mathfrak{p}'$ be the prime divisors of (3) in $\mathcal{O}_f$. Let C denote the class in $\Gamma(m)$ containing $\mathfrak{p}$, let $\rho = ri_1 + si_2$ and let $\mu \in C([\rho])$. Note that $C([\mu]) = [-\mu]$ by Corollary 3.2 (e).



Choose Hurwitz quaternions α and β such that

(1) $E\wp_\mu = E\beta$

(2) $E\wp'_\mu = E\alpha$

(3) $\beta\mu\beta^{-1} = -\mu$

(4) $\alpha\mu\alpha^{-1} = \rho$.

We know that α is a Hurwitz quaternion of norm 3 and that β is a Hurwitz quaternion of norm 3 and trace 0 (β has trace 0 by Lemma 1.4).

Let $\alpha = a + bi_1 + ci_2 + di_3$, let $\beta = xi_1 + yi_2 + zi_3$ and let $\mu = ui_1 + vi_2 + wi_3$. By Lemma 1.4 we have

(5) $xu + yv + zw = 0$,

By (4) and the fact that the i_3 coefficient of ρ is 0 we have

(6) $(-2ac + 2bd)u + (2ab + 2cd)v + (a^2 - b^2 - c^2 + d^2)w = 0$

Notice that if α and β are specified, relations (5) and (6) determine the vector (u,v,w) up to a constant multiple. We will show later that conditions (5) and (6) are independent.

These conditions determine the line in $\mathbb{R}^3$ generated by the vector (u,v,w). But u, v, w are relatively prime integers hence the vector (u,v,w) is determined up to ± 1. Thus m is determined from knowing only α and β!

We consider all pairs (α,β) where α is a Hurwitz quaternion of norm 3 and β is a Hurwitz quaternion of norm 3 and trace 0. We construct a vector (u,v,w) consisting of relatively prime integers

which satisfy (5) and (6). Then we let $m = u^2 + v^2 + w^2$. For example, if $\alpha = \frac{1}{2} + \frac{i_1}{2} + \frac{i_2}{2} + 3\frac{i_3}{2}$ and $\beta = i_1 + i_2 + i_3$ then relations (5) and (6) read

(5) $u + v + w = 0$

(6) $2u - v + 2w = 0$.

The only triples (u,v,w) consisting of relatively prime integers which satisfy (5) and (6) are $\pm(1,0,-1)$ and $m = 2$. As another possibility, let $\alpha = \frac{1}{2}(3 + i_1 + i_2 + i_3)$ and let $\beta = -i_1 + i_2 - i_3$. Then equations (5) and (6) become

(5) $-u - v - w = 0$

(6) $-u + 2v + 2w = 0$

Substituting equation (5) in equation (6) we obtain $(-u) + 2v + 2(-u + v) = 0$ so $-3u + 4v = 0$. We must choose $(u,v,w) = \pm(4,3,-1)$, and $m = 26$.

If one continues this procedure until all pairs (α,β) have been considered, one finds that 2 and 26 are the only values of m which appear. In $\mathbb{Q}(\sqrt{-2})$ the class group has order 1, but in $\mathbb{Q}(\sqrt{-26})$ the prime divisors of (3) do lie in classes of order 3. Hence 26 is the only value of m which satisfies conditions (i) and (ii).

The algorithm used in this example is exactly the one used in the next section where odd primes other than 3 are considered.

The next result is a corollary of Theorem 3.3.

Corollary 3.3. Let m be congruent to 1 or 2 mod 4. Suppose m can be written as a square plus two times a square, say $m = r^2 + 2s^2$. Let $C \in \Gamma(m)$ and suppose $C([r,s,s]) = [u,v,w]$.

Then

(a) $\mathcal{C}$ has order 2 iff two of u, v, w have equal absolute values.

(b) $\mathcal{C}_2$ is in the principal genus iff m can be written as a sum of 2 squares.

Proof. (a) By Corollary 3.1 we know that $\mathcal{C}_2([r,s,s]) = [-r,-s,-s]$. Now $\mathcal{C}$ has order 2 iff $\mathcal{C}\mathcal{C}_2 = \mathcal{C}^{-1}\mathcal{C}_2$ which is true iff $\mathcal{C}\mathcal{C}_2([r,s,s]) = \mathcal{C}^{-1}\mathcal{C}_2([r,s,s])$. By Theorem 3.3 we have $\mathcal{C}^{-1}\mathcal{C}_2([r,s,s]) = [-u,-v,-w]$. By Corollary 3.1 we have $\mathcal{C}\mathcal{C}_2([r,s,s]) = \mathcal{C}_2([u,v,w] = [-u,-w,-v]$. So $\mathcal{C}$ has order 2 iff $[-u,-v,-w] = [-u,-w,-v]$ which is true iff two of u, v, w have equal absolute values.

(b) First suppose that $\mathcal{C}_2$ is in the principal genus, say $\mathcal{C}_2 = \mathcal{D}^2$. Let $[u,v,w] = \mathcal{D}([r,s,s])$. By Theorem 3.3 we have $[-u,-v,-w] = \mathcal{D}^{-1}\mathcal{C}_2([r,s,s])$. So

$$[u,v,w] = \mathcal{D}([r,s,s]) = \mathcal{D}^{-1}\mathcal{C}_2([r,s,s]) = [-u,-v,-w].$$

Thus one of u, v, w is 0 so m can be written as a sum of two squares.

Conversely suppose that m can be written as $m = u^2 + v^2$. Let $\mathcal{D}$ be the class with $\mathcal{D}([o,u,v]) = [r,s,s]$. By Corollary 3.2 (c) we have $\mathcal{D}^2 = \mathcal{C}_2$ so $\mathcal{C}_2$ is in the principal genus.

Example 3.7. Let $m = 57$. Then $B_1(m)$ looks like

$$[4,4,5] \qquad [-4,-4,-5]$$
$$[2,2,7] \qquad [-2,-2,-7].$$

By Corollary 3.3 (a) we have that every class in $\Gamma(57)$ has order 2. Hence $\Gamma(57) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.

To end this section we return to Venkow's ideas in Chapter 2 and generalize them from the group of regular integral ideals to the semigroup of integral ideals. For the remainder of Chapter 3 we assume f is square-free. Let R_f denote the semigroup of integral ideals of O_f^- and let P_f denote the sub-semigroup of R_f consisting of the ideals which are principal in O_f^-.

Definition 3.2. Let $S(m)$ be the abelian semigroup R_f/P_f. We call $S(m)$ the *ring semigroup* with discriminant $-4m$.

Dade, Taussky and Zassenhaus [2] studied the structure of $S(m)$ and showed that the lattice of idempotents in $S(m)$ is isomorphic to the lattice of divisors of f. This will show up clearly in what follows.

Definition 3.3. For each d which divides f, let $B_d(m)$ denote the set of bundles θ with $N\theta = m$, $Tr\theta = 0$ and $c(\theta) = d$. Let $B(m) = \bigcup_{d|f} B_d(m)$.

Definition 2.1 can be extended from regular integral ideals to all integral ideals.

Definition 3.4. Let $\sigma\mathfrak{l}$ be an integral ideal of O_f^-. Define a map $\Pi_{\sigma\mathfrak{l}}$ from $B(m)$ to $B(m)$ in the following way; given a bundle $\theta \in B(m)$, choose $\mu \in \theta$ and $K \in E$ such that $E\sigma\mathfrak{l}_\mu = EK$. Let $\Pi_{\sigma\mathfrak{l}}(\theta) = [K\mu K^{-1}]$.

The analogue of Lemma 2.2 holds; the same proof Venkow used for Lemma 2.2 can be used here.

Lemma 3.4. Let $\mathfrak{a}$ and $\mathfrak{J}$ be integral ideals of $\mathcal{O}_f$ and let θ be an element of $B(m)$. Then

(a) $\Pi_{\mathfrak{a}\mathfrak{J}}(\theta) = \Pi_{\mathfrak{a}}(\Pi_{\mathfrak{J}}(\theta))$

(b) If $\mathfrak{a}$ and $\mathfrak{J}$ are in the same class of $S(m)$ then $\Pi_{\mathfrak{a}} = \Pi_{\mathfrak{J}}$.

Define an action of $S(m)$ on $B(m)$ by saying that if $\theta \in B(m)$ and $\mathcal{C} \in S(m)$ then $\mathcal{C}(\theta) = \Pi_{\mathfrak{a}}(\theta)$ where $\mathfrak{a}$ is an ideal chosen arbitrarily from $\mathcal{C}$. By Lemma 3.4 this is a well-defined action of $S(m)$ on $B(m)$. If $\mathcal{C}$ is a class in $S(m)$ which is not invertible then the map

$$\theta \to \mathcal{C}(\theta)$$

is not a 1-1 map. Our analysis of the action of $S(m)$ on $B(m)$ is based on the following theorem.

Theorem 3.4. Let p be a prime which divides f and let θ be a bundle in $B_e(m)$ where e divides f. Let $\mathcal{C}_p$ be the class in $S(m)$ which contains the ideal $\mathfrak{a}_p = (p, \sqrt{-m})$. Then

(a) $\mathcal{C}_p(\theta) = \theta$ if p divides e.

(b) $\mathcal{C}_p(\theta) \in B_{ep}(m)$ if p and e are relatively prime.

Proof. First suppose that p divides e. Let μ be an element of θ; write $\mu = p(ui_1 + vi_2 + wi_3)$ where $u, v, w \in \mathbb{Z}$. It is clear that p is a right divisor in E of both p and μ so $E\mathfrak{a}_p = Ep$. Thus $\mathcal{C}_p(\theta) = [p\mu p^{-1}] = \theta$.

Next assume that p and e are relatively prime. Since p^2 divides $N\mu$ we can find K_1 in E such that $NK_1 = p$ and $\mu K_1^{-1} \in E$ (this follows from Corollary 1.4). Likewise since p divides

$N(\mu K_1^{-1})$ there exists $K_2 \in E$ such that $NK_2 = p$ and $K_2^{-1}(\mu K_1^{-1}) \in E$. Thus

$$\mu = K_2 \mu_1 K_1 \qquad (*)$$

where $\mu_1 \in E$. From (*) we have

$$\overline{K}_2 \mu (\overline{K}_2)^{-1} = \mu K_1 K_2$$

$$K_1 \mu K_1^{-1} = K_1 K_2 \mu$$

hence both $\overline{K}_2 \mu (\overline{K}_2)^{-1}$ and $K_1 \mu K_1^{-1}$ are elements of E. Thus K_1 and $\overline{K}_2$ are each ideal quaternions with respect to μ by Theorem 3.1. However each has norm p and $\mathfrak{A}_p = \mathfrak{A}_p'$ is the only integral ideal in $\mathfrak{O}_f$ of norm p. Thus

$$E\overline{K}_2 = E\mathfrak{A}_p = EK_1$$

so $\overline{K}_2 = \varepsilon K_1$ for ε a unit. Thus

$$K_1 \mu K_1^{-1} = K_1 K_2 \mu_1 = \varepsilon^{-1}(\overline{K}_2 K_2)\mu_1 = p(\varepsilon^{-1}\mu_1).$$

so $c(K_1 \mu K_1^{-1}) = pc(\mu_1) = pe$, which shows that $\mathcal{C}(\theta) \in B_{ep}(m)$.

Definition 3.5. For each d dividing f, let $\mathcal{C}_d$ denote the class in $\Gamma(m)$ which contains the ideal $\mathfrak{A}_d = (d, \sqrt{-m})$.

Lemma 3.5. If d and e are divisors of f then $\mathcal{C}_d \mathcal{C}_e = \mathcal{C}_\ell$ where $\ell = \ell cm(d,e)$.

Proof. It suffices to show that $\mathfrak{A}_d \mathfrak{A}_e$ is equivalent to $\mathfrak{A}_\ell$, where $\ell = \ell cm(d,e)$. Let $g = gcd(d,e)$. We have

$$\mathfrak{A}_d \mathfrak{A}_e = (de, d\sqrt{-m}, e\sqrt{-m}, m) = (g)(\ell, \tfrac{d}{g}\sqrt{-m}, \tfrac{e}{g}\sqrt{-m}, \tfrac{m}{g})$$

and $(\ell, \frac{d}{g}\sqrt{-m}, \frac{e}{g}\sqrt{-m}, \frac{m}{g}) = (\ell, \sqrt{-m})$ since $\frac{d}{g}$ and $\frac{e}{g}$ are relatively prime and since ℓ divides $\frac{m}{g}$. Thus $\mathfrak{A}_d \mathfrak{A}_e = (g)\mathfrak{A}_\ell$ so $\mathcal{C}_d \mathcal{C}_e = \mathcal{C}_\ell$.

Note that if we let $d = e$ in Lemma 3.5 we have that each $\mathcal{C}_d$ is idempotent in $S(m)$. Dade, Taussky and Zassenhaus [2] showed that the classes $\mathcal{C}_d$ are the only idempotents in $S(m)$.

Definition 3.6. Let d be a divisor of f. Let $S_d(m)$ be the group of all classes in $S(m)$ of the form $\mathcal{C}_d\mathcal{C}$ where $\mathcal{C}$ is in $\Gamma(m)$.

Note that each set $S_d(m)$ is a group with identity $\mathcal{C}_d$ and that $S_1(m) = \Gamma(m)$. Gauss showed that $S_d(m)$ and $S_e(m)$ are disjoint if $d \neq e$ and that $S(m) = \bigcup_{d|f} S_d(m)$ (see Gauss [5], article 161). The next two lemmas lead up to the last theorem of this chapter.

Lemma 3.6. Suppose e divides f. Let $\mathfrak{A}$ be an ideal in $\mathfrak{O}$ with $\mathbb{Z}$-basis $(a, b+\sqrt{-m_1})$ where a is relatively prime to f. Let $\mathfrak{A}_f$ be the regular ideals in $\mathfrak{O}_f$ and $\mathfrak{O}_{f/e}$ given by $\mathfrak{A}_f = \mathfrak{O}_f \cap \mathfrak{A}$ and $\mathfrak{A}_e = \mathfrak{O}_{f/e} \cap \mathfrak{A}$ respectively. Let $\mathcal{C}$ and $\hat{\mathcal{C}}$ be the classes in $\Gamma(m)$ and $\Gamma(m/e^2)$ containing $\mathfrak{A}_f$ and $\mathfrak{A}_e$. Let $[eu,ev,ew]$ be a bundle in $B_e(m)$ and let $[r,s,t] = \hat{\mathcal{C}}([u,v,w])$. Then $\mathcal{C}([eu,ev,ew]) = [er,es,et]$.

Proof. Note that $\mathfrak{A}_f$ and $\mathfrak{A}_e$ have $\mathbb{Z}$-bases given by $(a, f(b+\sqrt{-m_1}))$ and $(a, \frac{f}{e}(b+\sqrt{-m_1}))$ respectively. Let K be a greatest common right divisor of a and $\frac{f}{e}(b+\sqrt{-m_1})$; choose K so that $K(ui_1 + vi_2 + wi_3)K^{-1} = (ri_1 + si_2 + ti_3)$. Observe that K is also a greatest common right divisor of a and $\frac{f}{e}(b+\sqrt{-m_1})$ since a and e are relatively prime. Thus

$$\begin{aligned}\mathcal{C}([eu,ev,ew]) &= [K(eui_1 + evi_2 + ewi_3)K^{-1}] \\ &= [e(K(ui_1 + vi_2 + wi_3)K^{-1})] \\ &= [e(ri_1 + si_2 + ti_3)] = [er,es,et].\end{aligned}$$

This result gives us the next lemma.

Lemma 3.7. Let e divide f and suppose that m is congruent to 1 or 2 mod 4.

(a) If $C \in \Gamma(m)$ and $\theta \in B_e(m)$ then $C(\theta) \in B_e(m)$.

(b) If θ_1 and θ_2 are in $B_e(m)$ then there exists $C \in \Gamma(m)$ such that $C(\theta_1) = \theta_2$.

Proof. We first prove (a). Let $\mathfrak{A}_f$ be an ideal from C. Write $\mathfrak{A}_f = \mathfrak{A} \cap \mathcal{O}_f$ and let $\mathfrak{A}_e = \mathfrak{A} \cap \mathcal{O}_{f/e}$. Let $\hat{C}$ be the class in $\Gamma(m/e_2)$ which contains $\mathfrak{A}_e$. Let $\theta = [eu,ev,ew]$, and let $\hat{C}([u,v,w]) = [r,s,t]$. By Lemma 2.1 (a) we have that $\gcd(r,s,t) = 1$. By Lemma 3.6 we have $C([eu,ev,ew]) = [er,es,et]$ and so

$$c(C(\theta)) = e.$$

We next prove (b). Let $\theta_1 = [eu,ev,ew]$ and let $\theta_2 = [er,es,et]$. By Theorem 2.1 (b) there exists a class $\hat{C}$ in $\Gamma(m/e^2)$ such that $\hat{C}([u,v,w]) = [r,s,t]$. Choose an ideal $\mathfrak{A}$ of $\mathcal{O}$ with $N\mathfrak{A}$ relatively prime to f such that $\mathfrak{A} \cap \mathcal{O}_{f/e}$ is in $\hat{C}$. Let C be the class in $\Gamma(m)$ containing the ideal $\mathfrak{A} \cap \mathcal{O}_f$. By Lemma 3.6 we have $C(\theta_1) = \theta_2$.

Theorem 3.5. Let m be congruent to 1 or 2 mod 4, let d and e be divisors of f and let $\ell = \ell cm(d,e)$. Then

$$S_d(m)(B_e(m)) = B_\ell(m)$$

where $S_d(m)(B_e(m))$ denotes the set of all $C(\theta)$ for $C \in S_d(m)$ and $\theta \in B_e(m)$.

Proof. Let C be an element of $S_d(m)$ and let θ be in $B_e(m)$. Write $C = \mathfrak{s}C_sC_t$ where $t = \gcd(d,e)$ and $s = d/t$. By Theorem 3.4 (a) we have $C_t(\theta) = \theta$ and by Theorem 3.4 (b) we have $C_s(\theta) \in B_\ell(m)$. Thus $\mathfrak{s}(C_2(\theta)) = C(\theta)$ is in $B_\ell(m)$ by Lemma 3.7 (a) so $S_d(m)(B_e(m)) \subseteq B_\ell(m)$. Equality holds by Lemma 3.7 (b) which completes the proof.

Example 3.8. Let $m = 585 = 5 \cdot 13 \cdot 3^2$. Here $m_1 = 65$ and $f = 3$. The group $\Gamma(585)$ has order 16 and

$$\Gamma(585) \cong \mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_2.$$

$\Gamma(585)$ is generated by C_2, the class containing $(2,3+\sqrt{-585})$, by C_{11}, the class containing $(11,3+\sqrt{-585})$ and by C_{101}, the class containing $(101,18+\sqrt{-585})$. The class C_{11} has order 4 and the classes C_2 and C_{101} have order 2. The set $B_3(585)$ has size 8. Below see $B(585)$; the 16 bundles in $B_1(585)$ appear on top and the 8 bundles in $B_3(585)$ appear on the bottom. Beside each bundle θ in $B(585)$ is a class C which maps $[1,10,22]$ to θ.

1	[1,10,22]	[-1,-10,-22]	c_{101}
c_2c_{101}	[1,22,10]	[-1,-22,-10]	c_2
$c_2c_{11}^3c_{101}$	[4,13,20]	[-4,-13,-20]	$c_{11}c_2$
c_{11}	[4,20,13]	[-4,-20,-13]	$c_{11}^3c_{101}$
$c_{11}^2c_{101}c_2$	[10,14,17]	[-10,-14,-17]	$c_{11}^2c_2$
c_{11}^2	[10,17,14]	[-10,-17,-14]	$c_{11}^2c_{101}$
c_{11}^3	[8,11,20]	[-8,-11,-20]	$c_{11}c_{101}$
$c_{11}c_{101}c_2$	[8,20,11]	[-8,-20,-11]	$c_{11}^3c_2$
$c_2c_{11}c_3$	[6,15,18]	[-6,-15,-18]	$c_2c_3c_{11}^3$
c_3c_{11}	[6,18,15]	[-6,-18,-15]	c_3c_{11}

[0,3,24] $c_{11}^2c_2c_3$

[0,24,3] $c_{11}^2c_3$

[0,12,21] c_2c_3

[0,21,12] c_2

Chapter 4. Imaginary Quadratic Fields Where a Prime has Order 3.

In this chapter we apply the machinery developed in Chapter 3 to answer the following question for all odd primes p. Which imaginary quadratic ring class groups $\Gamma(m)$ for m a sum of two squares have the property that the prime divisors of (p) are regular ideals in classes of order 3 in $\Gamma(m)$? The methods we use to answer this question are similar to those used to answer the same question for $p = 3$ in Example 3.6.

Section 1. The Quadratic Form φ'.

Throughout this section, p is a fixed odd prime. Let $m = m_1 f^2$ be a positive integer congruent to 1 or 2 mod 4 where m_1 is square-free and positive. Assume that p does not divide m and that the prime divisors $\mathfrak{p}$ and $\mathfrak{p}'$ of (p) in $\mathcal{O}_f$ are in classes of order 3 in $\Gamma(m)$. Assume in addition that m can be written as a sum of 2 relatively prime squares.

Lemma 4.1. Let $m = r^2 + s^2$ where $(r,s) = 1$. Suppose $\Pi_{\mathfrak{p}}$ maps the bundle $[r,s,o]$ to $[-u,-v,-w]$

1. $\Pi_{\mathfrak{p}'}$ maps $[r,s,0]$ to $[-u,-v,-w]$ and $\Pi_{\mathfrak{p}'}$ maps $[u,v,w]$ to $[r,s,0]$.

2. $\Pi_{\mathfrak{p}}$ maps $[u,v,w]$ to $[-u,-v,-w]$.

Proof. Let $\mathcal{C}$ denote the class in Γ containing $\mathfrak{p}$. Then $\mathfrak{p}'$ belongs to $\mathcal{C}^{-1}$ so $\Pi_{\mathfrak{p}'}$ maps $[u,v,w]$ to $[r,s,0]$. By Corollary 3.2 (a) we have that $\Pi_{\mathfrak{p}'}$ maps $[r,s,0]$ to $[-u,-v,-w]$ which proves 1.

Since $\mathcal{C}$ has order 3 we have that $\mathfrak{p}$ and $(\mathfrak{p}')^2$ belong to the

same class. $\Pi_{(\rho')^2}$ maps $[u,v,w]$ to $[-u,-v,-w]$ by (1) which completes the proof.

Definition 4.1. Let A denote the set of Hurwitz quaternions of norm p and let B denote the set of Hurwitz quaternions of norm p and trace 0.

Let r, s, u, v, w be as in Lemma 4.1, let $\mu = ui_1 + vi_2 + wi_3$ and let $\rho = ri_1 + si_2$. Let β_1 be a greatest common right divisor of $E\rho_\mu$ and let α_1 be a greatest common right divisor of $E\rho'_\mu$. By Lemma 2.1 we have $\alpha_1\mu\alpha_1^{-1} \in [\rho]$ and $\beta_1\mu\beta_1^{-1} \in [-\mu]$. Premultiply α_1 and β_1 by appropriate units to obtain α and β which satisfy

$$\begin{aligned} \alpha\mu\alpha^{-1} &= \rho \\ \beta\mu\beta^{-1} &= -\mu \end{aligned} \tag{4.1}$$

By Lemma 1.4, the latter equation implies that $\beta \in B$ so the pair (α,β) comes from $A \times B$.

Applying Lemma 1.4 to the equations in (4.1) and observing that the i_3 coefficient of ρ is 0 we obtain the following 3 conditions on α, β and μ;

(i) The coefficient of i_3 in $\alpha\mu\alpha^{-1}$ is 0.

(ii) $Tr(\beta\bar{\mu}) = 0$.

(iii) $(u,v,w) = 1$.

We begin with a pair $(\alpha,\beta) \in A \times B$ and construct the $\mu \in E$ which satisfy conditions (i), (ii) and (iii). Given α and β, conditions (i) and (ii) put two linear conditions on u, v and w thus constraining the vector (u,v,w) to a line in $\mathbb{R}^3$. Condition

(iii) determines (u,v,w) up to a change in sign. For a given α and β, the algorithm breaks down iff one of u, v or w is 0.

To construct such an algorithm we begin with a function φ' which for a pair $(\alpha,\beta) \in A \times B$ yields an integer vector (u',v',w') on the same line in $\mathbb{R}^3$ as (u,v,w). We define φ' in such a way as to facilitate the analysis when one of u', v', or w' is 0.

Definition 4.2. Define $\varphi' : A \times B \to \mathbb{Z}^5$ as follows; for $(\alpha,\beta) \in A \times B$ with $\alpha = a + bi_1 + ci_2 + di_3$ and $\beta = xi_1 + yi_2 + zi_3$ define

$$\varphi'(\alpha,\beta) = (u',v',w',r',s')$$

where
$$u' = y(-a^2+b^2+c^2-d^2) + 2z(ab+cd)$$
$$v' = x(a^2-b^2-c^2+d^2) + 2z(ac-bd)$$
$$w' = 2x(-ab-cd) + 2y(-ac+bd)$$
$$r' = u'(a^2+b^2-c^2-d^2) + 2v'(bc-ad) + 2w'(bd+ac)$$
$$s' = v'(a^2-b^2+c^2-d^2) + 2u'(ad+bc) + 2w'(cd-ab).$$

One can check that all of u', v', w', r', s' are integers even in the case where the coefficients of α are odd integers divided by 2. We begin with a lemma which lists some properties of φ'.

Lemma 4.2. Let α, β and u', v', w', r', s' be as in Definition 4.2. Then

(a) $xu' + yv' + zw' = 0$

(b) $2u'(bd-ac) + 2v'(cd+ab) + w'(a^2-b^2-c^2+d^2) = 0.$

(c) $\alpha(u'i_1 + v'i_2 + w'i_3)\bar{\alpha} = r'i_1 + s'i_2$

(d) $\gcd(u',v',w') = \gcd(r',s')$

or $\operatorname{pgcd}(u',v',w') = \gcd(r',s')$

or $p^2\gcd(u',v',w') = \gcd(r',s')$

(e) If $(r',s') = (u',v',w')$ or $(r',s') = p^2(u',v',w')$ then $(u'i_1 + v'i_2 + w'i_3)$ has 2 zero components.

(f) $\varphi'(i_1\alpha,\beta) = (-u',-v',-w',-r',s')$.

$\varphi'(i_2\alpha,\beta) = (-u',-v',-w',r',-s')$.

$\varphi'(i_3\alpha,\beta) = (u',v',w',-r',-s')$.

Proof. The proofs of (a), (b) and (f) are simple computations. We now prove (c); to do so it suffices to show that

$$\alpha(u'i_1 + v'i_2 + w'i_3)p = (r'i_1 + s'i_2)\alpha.$$

$$(r'i_1 + s'i_2)\alpha = (r'i_1 + s'i_2)(a + bi_1 + ci_2 + di_3)$$

$$\begin{aligned}
&= (-b(u'(a^2 + b^2 - c^2 - d^2) + 2v'(bc - ad) + 2w'(bd + ac) \\
&\quad -c(v'(a^2 - b^2 + c^2 - d^2) + 2u'(ad + bc) + 2w'(cd - ab)) \\
&\quad +i_1(a(u'(a^2 + b^2 - c^2 - d^2) + 2v'(bc - ad) + 2w'(bd + ac)) \\
&\quad +d(v'(a^2 - b^2 + c^2 - d^2) + 2u'(ad + bc) + 2w'(cd - ab))) \\
&\quad +i_2(-d(u'(a^2 + b^2 - c^2 - d^2) + 2v'(bc - ad) + 2w'(bd + ac)) \\
&\quad +a(v'(a^2 - b^2 + c^2 - d^2) + 2u'(ad + bd) + 2w'(cd - ab))) \\
&\quad +i_3(c(u'(a^2 + b^2 - c^2 - d^2) + 2v'(bc - ad) + 2w\ (bd + ac)) \\
&\quad -b(v'(a^2 - b^2 + c^2 - d^2) + 2u'(ad + bc) + 2w'(cd - ab))).
\end{aligned}$$

Rewriting each of these coefficients we obtain,

$$(r'i_1 + s'i_2)\alpha =$$

$$(-bu'(a^2+b^2+c^2+d^2) + 2du'(bd-ac) - cv'(a^2+b^2+c^2+d^2)$$

$$+2dv'(cd+ab) - dw'(a^2+b^2+c^2+d^2) + dw'(a^2-b^2-c^2+d^2))$$

$$+i_1(au'(a^2+b^2+c^2+d^2) + 2cu'(bd-ac) - dv'(a^2+b^2+c^2+d^2)$$

$$+2cv'(ab+cd) + cw'(a^2+b^2+c^2+d^2) - cw'(-a^2+b^2+c^2-d^2))$$

$$+i_2(du'(a^2+b^2+c^2+d^2) + 2bu'(ac-bd) + av(a^2+b^2+c^2+d^2)$$

$$-2bv'(ab+cd) - bw(a^2+b^2+c^2+d^2) + bw'(-a^2+b^2+c^2-d^2))$$

$$+i_3(-cu'(a^2+b^2+c^2+d^2) + 2au'(ac-bd) + bv'(a^2+b^2+c^2+d^2)$$

$$+2av'(-ab-cd) + aw'(a^2+b^2+c^2+d^2) + aw'(-a^2+b^2+c^2-d^2)).$$

Applying the orthogonality condition given in part (b) of this lemma we can simplify the above expression.

$$(r'i_1 + s'i_2)\alpha = ((-bu'-cv'-dw') + i_1(au'-dv'+cw')$$

$$+i_2(du'+av'-bw') + i_3(-cu'+bv'+aw'))(a^2+b^2+c^2+d^2)$$

so

$$(r'i_1 + s'i_2)\alpha = (a+bi_1+ci_2+di_3)(u'i_1+v'i_2+w'i_3)p.$$

Next we prove (d). By the equations for r' and s' given in definition 4.2 it is clear that $\gcd(u',v',w') \mid \gcd(r',s')$. Also by part (c) of this lemma we have

$$p^2(u'i_1 + v'i_2 + w'i_3) = \bar{\alpha}(r'i_1 + s'i_2)\alpha \qquad (4.2).$$

The equation (4.2) expresses p^2u', p^2v' and p^2w' as $\mathbb{Z}$-linear combinations of r' and s' thus showing that $\gcd(r',s') \mid p^2\gcd(u',v',w')$, and this proves (d).

To prove (e) assume first that $\gcd(r',s') = \gcd(u',v',w')$.

Let $\mu = \frac{p}{\gcd(r',s')}(u'i_1 + v'i_2 + w'i_3) = ui_1 + vi_2 + wi_3$

and $\varphi = \frac{1}{\gcd(r',s')}(r'i_1 + s'i_2) = ri_1 + si_2$.

Note that $(r,s) = 1$ and that $(u,v,w) = p$.

Let $\mathcal{O}_\rho = p\mathbb{Z} + \mathbb{Z}(ri_1 + si_2)$ and observe that

$$\alpha(ui_1 + vi_2 + wi_3)\alpha^{-1} = (ri_1 + si_2)$$

by part (c) of this lemma. So $N(\mu) = N(\rho) = -(ri_1 + si_2)^2$ hence p divides $(ri_1 + si_2)^2$. Thus $\mathcal{O}_\rho$ is an ideal in $\mathbb{Z}[p]$. Also

$$(\bar{\alpha})^{-1}(ui_1 + vi_2 + wi_3)\bar{\alpha} = ri_1 + si_2$$

and $(\bar{\alpha})^{-1}(ui_1 + vi_2 + wi_3) \in E$ since $p \mid \gcd(u,v,w)$. So $\bar{\alpha}$ is a greatest common right divisor of $E\mathcal{O}_\rho$. Clearly $\mathcal{O}'_\rho = \mathcal{O}_\rho$ hence $[u,v,w] = [-u,-v,-w]$ which completes the proof of (e) in the case $\gcd(u',v',w') = \gcd(r',s')$. The case $p^2\gcd(u',v',w') = \gcd(r',s')x$ is similar.

The rest of this section is spent characterizing those pairs (α,β) where one of u', v' or w' is 0.

Definition 4.3. Let $(\alpha,\beta) \in A \times B$ and let $\varphi'(\alpha,\beta) = (u',v',w',r',s')$. If one of u', v' or w' is 0 then (α,β) is called a *degenerate pair*, and we say that φ' *degenerates* at (α,β).

Lemma 4.3. Suppose $(\alpha,\beta) \in A \times B$ is a degenerate pair. Then one of the following conditions must hold;

1. (a) $\alpha = \varepsilon(xi_1 + yi_2 + zi_3)$ for $\varepsilon \in U$

   (b) $\alpha = \varepsilon(-xi_1 + yi_2 + zi_3)$ for $\varepsilon \in U$

(c) $\alpha = \varepsilon(xi_1 - yi_2 + zi_3)$ for $\varepsilon \in U$

(d) $\alpha = \varepsilon(-xi_1 - yi_2 + zi_3)$ for $\varepsilon \in U$

2. $\varepsilon\alpha$ has two zero components for some $\varepsilon \in U$.

Proof. Let $(\alpha,\beta) \in A \times B$ be a degenerate pair with $\alpha = a + bi_1 + ci_2 + di_3$, with $\beta = xi_1 + yi_2 + zi_3$ and with $\varphi'(\alpha,\beta) = (u',v',w',r',s')$. By Lemma 4.2 (d) we know that $\gcd(u',v',w') = \gcd(r',s')$, or $p\gcd(u',v',w') = \gcd(r',s')$ or $p^2\gcd(u',v',w') = \gcd(r',s')$. We examine each of these three cases separately.

Case 1. $\gcd(u',v',w') = \gcd(r',s')$.

Let $\mu = \frac{p}{\gcd(u',v',w')}(u'i_1 + v'i_2 + w'i_3)$ and let

$\rho = \frac{1}{\gcd(r',s')}(r'i_1 + s'i_2)$. Write u, v, w for the coefficients of μ and r, s for the coefficients of ρ. By assumption, one of u, v or w is 0. Assume that $w = 0$; the cases $u = 0$ and $v = 0$ are handled similarly.

Let $m = u^2 + v^2 + w^2 = r^2 + s^2$ and write $m = m_1 f^2$ where m_1 is square-free. Let $\mathcal{O}^-$ denote the maximal order in the field $\mathbb{Q}(\sqrt{-m_1})$ and $\mathcal{O}^-_f$ the suborder with generators $(1,\sqrt{-m})$. Note that $p|m$ so $(p,\sqrt{-m})$ is a $\mathbb{Z}$-basis for an ideal $\mathfrak{a}$ in the order $\mathcal{O}^-_f$.

By Lemma 4.2 (c) we have $\alpha\mu\alpha^{-1} = \rho$ hence

$$(\bar{\alpha})^{-1}\mu\bar{\alpha} = \rho,$$

and $((\bar{\alpha})^{-1}\mu) \in E$ since $p|(u,v,w)$. Also $\alpha\bar{\alpha} = p$ so $\bar{\alpha}$ is a greatest common right divisor of the ideal $E\mathfrak{a}_\rho = E(p,ri_1 + si_2)$.

Next observe that

$$-(i_3\bar{\alpha}i_3^{-1})^{-1}\,\mu(i_3\bar{\alpha}i_3^{-1}) = (i_3\bar{\alpha}i_3^{-1})^{-1}(-\mu)(i_3\bar{\alpha}i_3^{-1})$$

$$= i_3\bar{\alpha}^{-1}i_3^{-1}(i_3\mu i_3^{-1})(i_3\bar{\alpha}i_3^{-1})$$

$$= i_3((\bar{\alpha})^{-1}\mu\bar{\alpha})i_3^{-1} = i_3(ri_1 + si_2)i_3^{-1} = -(ri_1 + si_2).$$

So $i_3\bar{\alpha}i_3^{-1}$ is also a greatest common right divisor of the ideal $E\sigma_\rho$. Hence there is a unit $\varepsilon \in U$ for which

$$i_3\bar{\alpha}i_3^{-1} = \varepsilon(\bar{\alpha}).$$

Now $i_3\bar{\alpha}i_3^{-1} = a + bi_1 + ci_2 - di_3$ and so by Lemma 1.5 with $\delta = \bar{\alpha}$ we have that for some $\rho \in U$, $\rho\bar{\alpha}$ has 2 zero components. Hence the same is true of α, which completes Case 1.

Case 2. $p^2\gcd(u',v',w') = \gcd(r',s')$.

This is handled very much like case 1. Again one finds that $\rho\alpha$ has 2 zero components for some $\rho \in U$.

Case 3. $p\gcd(u',v',w') = \gcd(r',s')$.

Let $\mu = \frac{1}{\gcd(u',v',w')}(u'i_1 + v'i_2 + w'i_3)$ and let

$$\rho = \frac{1}{\gcd(r',s')}(r'i_1 + s'i_2).$$

As before, let u, v and w denote the coefficients of μ; by assumption one of u, v, or w is 0. We consider the case $u = 0$, the cases $v = 0$ and $w = 0$ are handled similarly. We will show $\alpha = \varepsilon\beta$ or $\alpha = \varepsilon(-xi_1 + yi_2 + zi_3)$ for $\varepsilon \in U$.

By Lemma 4.2 (a) we have

$$xu + yv + zw = 0$$

so $\beta\mu\beta^{-1} = -\mu = i_1\mu i_1^{-1}$. Hence $i_1\beta$ centralizes μ so $i_1\beta = q_1 + q_2\mu$ for $q_1, q_2 \in \mathbb{Q}$. By inspection, $i_1\beta = -x - zi_2 + yi_3$ so $q_1 = -x$. Let $\gamma = \gcd(y,z)$, so

$$v = -k(z/\gamma)$$

$$w = k(y/\gamma)$$

for $k \in \mathbb{Q}$. Write $k = k_1/k_2$ with $\gcd(k_1,k_2) = 1$ and $k_2 > 0$. Observe that $k_2 = 1$ since (y/γ) and (z/γ) are relatively prime. So $k = \pm 1$.

Subcase 1. $k = 1$ so $v = -z/\gamma$ and $w = y/\gamma$.

Let $m = \dfrac{y^2+z^2}{\gamma^2} = \dfrac{p-x^2}{\gamma^2}$

and write $m = m_1 f^2$ where m_1 is square-free. Let $\mathcal{O}_f$ denote the suborder in $\mathbb{Q}(\sqrt{-m_1})$ generated by 1 and $\sqrt{-m}$. In the semigroup of ideals in the ring $\mathcal{O}_f$ we have

$$(p) = (p, x + \gamma\sqrt{-m})(p, x - \gamma\sqrt{-m}) .$$

Identify $\sqrt{-m}$ with the quaternion $\mu = -\dfrac{zi_2}{\gamma} + \dfrac{yi_3}{\gamma}$.

Note $x + \gamma\mu = x - zi_2 + yi_3$ is a divisor of both p and $x + \gamma\mu$. Also $x - \gamma\mu = x + zi_2 - yi_3$ is a divisor of both p and $x - \gamma\mu$. Hence α differs from $x + \gamma\mu$ or from $x - \gamma\mu$ by left unit multiplication (in this case the prime divosors of (p) are principal). Assume that α differs from $x + \gamma\mu$ by left unit multiplication (the other case is similar). We have

$$\alpha = \varepsilon_1(x - zi_2 + yi_3) = (\varepsilon_1 i_1)(-xi_1 + yi_2 + zi_3)$$

for ε_1 a unit. This is condition 1b which completes this subcase.

Subcase 2. $k = -1$.

Here a similar argument shows that α differs from $xi_1 + yi_2 + zi_3$ by left unit multiplication. This completes the proof of Lemma 4.3.

The next three lemmas examine the cases when the pair (α,β) satisfy one of the 5 conditions of Lemma 4.3. Together they give a complete characterization of degenerate pairs.

Lemma 4.4 deals with the case where $\varepsilon\alpha$ has 2 zero coefficients for some $\varepsilon \in U$. Note that if $\varepsilon \in \{\pm 1, \pm i_1, \pm i_2, \pm i_3\}$ and $\varepsilon\alpha$ has 2 zero coefficients than α has 2 zero coefficients. If $\varepsilon \in U - \{\pm 1, \pm i_1, \pm i_2, \pm i_3\}$ and $\varepsilon\alpha$ has 2 zero coefficients then all coefficients of α are nonzero and 2 pairs of coefficients have equal absolute values. The reader should bear in mind throughout that if $p \equiv 1 \bmod 4$, there are unique integers x, y with $0 < x < y$ and $x^2 + y^2 = p$. Likewise there are unique odd integers $0 < a < b$ with $(\frac{a}{2})^2 + (\frac{a}{2})^2 + (\frac{b}{2})^2 + (\frac{b}{2})^2 = p$.

Lemma 4.4. Suppose $(\alpha,\beta) \in A \times B$ and $\varphi'(\alpha,\beta) = (u',v',w',r',s')$. Let $\alpha = a + bi_1 + ci_2 + di_3$ and $\beta = xi_1 + yi_2 + zi_3$. Then

1. All of u', v', w' are nonzero in the following cases

   (a) $a = b = 0$ and $x \neq 0$

   $c = d = 0$ and $x \neq 0$

   (b) $a = c = 0$ and $y \neq 0$

   $b = d = 0$ and $y \neq 0$

(c) $a = d, b = c$ and $x \neq 0$

$a = d, b = -c$ and $y \neq 0$

$a = -d, b = c$ and $y \neq 0$

$a = -d, b = -c$ and $x \neq 0$

(d) $a = c, b = d$ and $z \neq 0$

$a = -c, b = -d$ and $z \neq 0$

(e) $a = b, c = -d$ and $z \neq 0$

$a = -b, c = d$ and $z \neq 0$

2. (a) If $a = c$ and $b = -d$ then $u' = 0$.

If $a = -c$ and $b = d$ then $u' = 0$.

(b) If $a = b$ and $c = d$ then $v' = 0$.

If $a = -b$ and $c = -d$ then $v' = 0$.

(c) If $a = d = 0$ then $w' = 0$.

If $b = c = 0$ then $w' = 0$.

Proof. The proof is by computation. The computations in 2. are straightforward and are left to the reader. The computations in 1. are very similar so only one is done. The reader who is interested in completing the rest can use Lemma 4.2 (f) to reduce the number of necessary computations.

We do the first case of 1. Assume that $a = b = 0$ and that $x \neq 0$. Then

$$c^2 = d^2 = p = x^2 + y^2 + z^2$$

and so $\gcd(c,d) = 1$ since p is prime.

$$u' = y(c^2 - d^2) + 2zcd$$
$$v' = x(-c^2 + d^2)$$
$$w' = -2xcd.$$

As $\gcd(c,d) = 1$ we see that $c^2 - d^2 \neq 0$ and v', w' are nonzero. If $u' = 0$ then

$$y(d^2 - c^2) = 2zcd.$$

Since $\gcd(c,d) = 1$ we have $(cd,(c^2 - d^2)) = 1$ and since p is odd we have $(2,(d^2 - c^2)) = 1$. Hence

$$(d^2 - c^2) \mid z \quad \text{and} \quad (2cd) \mid y.$$

Now

$$p = x^2 + y^2 + z^2 > y^2 + z^2 > (2cd)^2 + (d^2 - c^2)^2 = (d^2 + c^2)^2 = p^2$$

and this is a contradiction. This completes the proof of this case and of Lemma 4.4.

Let V denote the subgroup of U generated by i_1 and i_2. This subgroup has index 3 in U; the distinct left cosets are given by

$$U_0 = V, \quad U_1 = \delta V, \quad U_2 = \delta^2 V.$$

Lemma 4.5. Let $(\alpha,\beta) \in A \times B$ and let $\varphi'(\alpha,\beta) = (u',v',w',r',s')$. Suppose $\alpha = a + bi_1 + ci_2 + di_3$ and $\beta = xi_1 + yi_2 + zi_3$ where all of x, y and z are nonzero.

1. If $\alpha = \varepsilon\beta$ for $\varepsilon \in U$ then one of u', v' or w' is 0.

2. Suppose $\alpha = \varepsilon(-xi_1 + yi_2 + zi_3)$ for $\varepsilon \in U$. One of u', v' or w' is 0 iff $\varepsilon \in U_2$.

3. Suppose $\alpha = \varepsilon(xi_1 - yi_2 + zi_3)$ for $\varepsilon \in U$. One of u', v' or w' is 0 iff $\varepsilon \in U_1$.

4. Suppose $\alpha = \varepsilon(xi_1 - yi_2 + zi_3)$ for $\varepsilon \in U$. One of u', v', or w' is 0 iff $\varepsilon \in U_0$.

Proof. The proof is by computation; by Lemma 4.2 (f) only 12 of the 96 possible cases need be considered. The computations are straightforward in the 6 cases where one of u', v', or w' is 0. In the remaining 6 cases, the computations are similar and so only one is done.

Assume $\alpha = \frac{1}{2}(1 + i_1 + i_2 + i_3)(-xi_1 + yi_2 + zi_3)$, so

$$\alpha = \frac{1}{2}(x - y - z) + \frac{i_1}{2}(-x - y + z) + \frac{i_2}{2}(-x + y - z) + \frac{i_3}{2}(x + y + z).$$

Thus

$$4u' = y(-(x^2 - 2xy + y^2 - 2xz + 2yz + z^2) + (x^2 + 2xy + y^2 - 2xz - 2yz + z^2)$$
$$+(x^2 - 2xy + y^2 + 2xz - 2yz + z^2) - (x^2 + 2xy + y^2 + 2xz + 2yz + z^2))$$
$$+2z((x - y - z)(-x - y + z) + (-x + y - z)(x + y + z))$$

so

$$4u' = y(-8yz) + 2z(-x^2 + 2xz + y^2 - z^2 - x^2 - 2xz + y^2 - z^2)$$

$$4u' = 4z(-x^2 - y^2 - z^2)$$

so $u' = -zp$ hence $u' \neq 0$.

$$4v' = x(8yz) + 2z((x - y - z)(-x + y - z) - (-x - y + z)(x + y + z))$$

so $4v' = 16xyz$ hence $v' \neq 0$.

$$2w' = x(2x^2 - 2y^2 + 2z^2) + y(-4xy)$$

so $w' = x(x^2 - 3y^2 + z^2)$.

Hence $w' = 0$ iff $3y^2 = x^2 + z^2$. Assume this is the case. If y is even then $x^2 + z^2 \equiv 0 \bmod 4$ so both x and y are even and this contradicts $\gcd(x,y,z) = 1$. So y is odd and so $x^2 + z^2 \equiv 3 \bmod 4$

which is a contradiction. Thus $w' \neq 0$ which completes the proof of the case $\alpha = \varepsilon(-xi_1 + yi_2 + zi_3)$ and $\varepsilon \in U_1$.

Each of the last two lemmas requires the assumption that all of x, y and z are nonzero. The next lemma deals with the case when one of x, y or z is 0.

Lemma 4.6. Suppose $(\alpha,\beta) \in A \times B$ and $\varphi'(\alpha,\beta) = (u',v',w',r',s')$.

Let $\alpha = a + bi_1 + ci_2 + di_3$ and $\beta = xi_1 + yi_2 + zi_3$. Then

1. If $x = 0$ and either
   (a) $a = b = 0$
   (b) $c = d = 0$
   (c) $a = d$ and $b = c$
   (d) $a = -d$ and $b = -c$

then $v' = w' = 0$.

2. If $y = 0$ and either
   (a) $a = c = 0$
   (b) $b = d = 0$
   (c) $a = d$ and $b = -c$
   (d) $a = -d$ and $b = c$

then $u' = w' = 0$.

3. If $z = 0$ and either
   (a) $a = c$ and $b = d$
   (b) $a = -c$ and $b = -d$
   (c) $a = b$ and $c = -d$
   (d) $a = -b$ and $c = d$

then $u' = v' = 0$.

4. If $\alpha = \varepsilon(-xi_1 + yi_2 + zi_3)$ for $\varepsilon \in U$ and if one of x, y or z is 0 then one of u', v' or w' is 0.

If $\alpha = \varepsilon(xi_1 - yi_2 + zi_3)$ for $\varepsilon \in U$ and if one of x, y or z is 0 then one of u', v' or w' is 0.

If $\alpha = \varepsilon(-xi_1 - yi_2 + zi_3)$ for $\varepsilon \in U$ and if one of x, y or z is 0 then one of u', v' or w' is 0.

Proof. The proofs of 1.-3. are simple computations, and are left to the reader. The proof of 4. is also by computation; we consider the case where $\alpha = \varepsilon(-xi_1 + yi_2 + zi_3)$. By Lemma 4.2 (f) we need only consider $\varepsilon = 1$, δ or δ^2 and $\varepsilon = \delta$ is done in Lemma 4.4.

If $\alpha = (-xi_1 + yi_2 + zi_3)$ then a straightforward computation gives

$$u' = yp$$
$$v' = x(-x^2 - y^2 + 3z^2)$$
$$w' = -4xyz.$$

The assertion clearly follows. If $\alpha = \delta^2(-xi_1 + yi_2 + zi_3)$ then

$$u' = pz$$
$$v' = 4xyz$$
$$w' = x(x^2 - 3y^2 + z^2)$$

and again the assertion follows.

We are now ready to count the number of degenerate pairs $(\alpha,\beta) \in A \times B$.

Theorem 4.1. Let $h(p)$ denote the class number of the field $\mathbb{Q}(\sqrt{-p})$. The number of degenerate pairs $(\alpha,\beta) \in A \times B$ is

$$192(6h(p) - 2) \quad \text{if } p \equiv 1 \bmod 4$$
$$192(6h(p)) \quad \text{if } p \equiv 3 \bmod 8.$$

Proof. Consider first the case $p \equiv 3 \bmod 8$. We know that every degenerate pair must satisfy one of the conditions of Lemma 4.3. Condition 2. cannot be met in this case since a prime congruent to 3 mod 8 cannot be written as a sum of 2 squares. So we only need consider conditions 1a-1d and here Lemma 4.5 is pertinent.

For each $\beta = xi_1 + yi_2 + zi_3 \in B$ there are 24 α satisfying $\alpha = \varepsilon\beta$ with $\varepsilon \in U$, 8 α satisfying $\alpha = \varepsilon(-xi_1 + yi_2 + zi_3)$ with $\varepsilon \in U_2$, 8 α satisfying $\alpha = \varepsilon(xi_1 - yi_2 + zi_3)$ with $\varepsilon \in U_1$, and 8 α satisfying $\alpha = \varepsilon(-xi_1 - yi_2 + zi_3)$ with $\varepsilon \in U_0$. Thus the number of degenerage pairs $(\alpha,\beta) \in A \times B$ is $48 \cdot |B|$. By Theorem 2.1, $|B| = 24h(p)$ so the number of degenerate pairs is

$$48 \cdot |B| = 48 \cdot 24h(p) = 192(6h(p))$$

which completes the proof in the case $p \equiv 3 \bmod 8$.

If $p \equiv 1 \bmod 4$ the situation is more complicated, since the conditions of Lemma 4.4 2. and Lemma 4.6 are met as well as the conditions of Lemma 4.5. Suppose first that $\beta = xi_1 + yi_2 + zi_3 \in B$ and that all of x, y and z are nonzero. The conditions of Lemma 4.4 2. are met by 48 $\alpha \in A$ and the conditions of Lemma 4.5 which give a degenerate pair are met by 48 $\alpha \in A$ (as above). Also these 96 α are distinct since all of x, y and z are nonzero.

If one of x, y or z is 0 then we look at Lemma 4.6 in place of Lemma 4.5. There seem to be 96 α which satisfy the conditions of Lemma 4.6 4..

However, if $z = 0$ then $\varepsilon(xi_1 + yi_2 + zi_3) = (-\varepsilon)(-xi_1 - yi_2 + zi_3)$

and $\varepsilon(xi_1 - yi_2 + zi_3) = (-\varepsilon)(-xi_1 + yi_2 + zi_3)$

$$\text{if } y = 0 \text{ then } \varepsilon(xi_1 + yi_2 + zi_3) = \varepsilon(xi_1 - yi_2 + zi_3)$$

$$\text{and } \varepsilon(-xi_1 + yi_2 + zi_3) = \varepsilon(-xi_1 - yi_2 + zi_3)$$

$$\text{if } x = 0 \text{ then } \varepsilon(xi_1 + yi_2 + zi_3) = \varepsilon(-xi_1 + yi_2 + zi_3)$$

$$\text{and } \varepsilon(xi_1 - yi_2 + zi_3) = \varepsilon(-xi_1 - yi_2 + zi_3).$$

So there are 48 α which satisfy the conditions of Lemma 4.6 4..

There are 48 α which satisfy the conditions of Lemma 4.4 2.. Of these, 16 also satisfy the conditions of Lemma 4.6 4. and so are counted twice. In total, 384 pairs (α,β) are counted twice. Pairs (α,β) which satisfy conditions in Lemma 4.6 1.-3. also satisfy the conditions of Lemma 4.6 4. and so these pairs have already been counted.

Thus for each $\beta \in B$ there are 96 α for which (α,β) is a degenerate pair though this counts 384 pairs twice. Hence the total number of degenerate pairs is $96|B| - 384$. By Theorem 2.1, $|B| = 12h(p)$ so the total number of degenerate pairs is

$$192(6h(p)) - 384 = 192(6h(p) - 2).$$

This completes the proof of Theorem 4.1.

Section 2. Classes of order 3.

We begin by defining a function φ on $A \times B$. This function is derived from the function φ' of the previous section.

Definition 4.4. Define $\varphi : A \times B \to E \times E$ as follows; for $(\alpha,\beta) \in A \times B$ let $\varphi'(\alpha,\beta) = (u',v',w',r',s')$. Define $\varphi(\alpha,\beta) = (\mu,\rho)$

$$\mu = \frac{1}{\gcd(u',v',w')}(u'i_1 + v'i_2 + w'i_3).$$

$$\rho = \frac{1}{\gcd(r',s')}(r'i_1 + s'i_2).$$

Lemmas 4.3, 4.4 and 4.5 together show that if u', v' and w' are all nonzero we have

$$\alpha\mu\alpha^{-1} = \rho$$

$$\beta\mu\beta^{-1} = -\mu.$$

The next lemma shows that the only way the above two equations can be satisfied is for $\varphi(\alpha,\beta) = \pm(\mu,\rho)$.

Lemma 4.7. Let $\mu = ui_1 + vi_2 + wi_3 \in E$ with $\gcd(u,v,w) = 1$, let $\rho = ri_1 + si_2 \in E$ with $\gcd(r,s) = 1$ and let $(\alpha,\beta) \in E \times E$. Suppose

$$\alpha\mu\alpha^{-1} = \rho$$

$$\text{and} \quad \beta\mu\beta^{-1} = -\mu.$$

Then $\varphi(\alpha,\beta) = \pm(\mu,\rho)$.

Proof. Let $\alpha = a + bi_1 + ci_2 + di_3$ and $\beta = xi_1 + yi_2 + zi_3$. A simple computation gives that the coefficient of i_3 in $\alpha\mu\bar{\alpha}$ is

$$w(a^2 - b^2 - c^2 + d^2) + 2u(-ac + bd) + 2v(ab + cd).$$

So we have the following linear condition on u, v and w:

$$w(a^2 - b^2 - c^2 + d^2) + 2u(-ac + bd) + 2v(ab + cd) = 0 \qquad (*).$$

The equation $\beta\mu\beta^{-1} = -\mu$ gives the following linear condition on u, v and w:

$$xu + yv + zw = 0 \qquad (**).$$

We next show that the two conditions (*) and (**) are linearly independent over $\mathbb{Q}$. (The reader may want to refer back to Example 3.6.)

Suppose to the contrary that there exists a rational number q with

$$xq = 2(-ac+bd)$$
$$yq = 2(ab+cd)$$
$$zq = a^2 - b^2 - c^2 + d^2.$$

Then $pq^2 = (x^2+y^2+z^2)q^2$

$$= (xq)^2 + (yq)^2 + (zq)^2$$
$$= 4(-ac+bd)^2 + 4(ab+cd)^2 + (a^2-b^2-c^2+d^2)^2$$
$$= 4(a^2c^2 - 2abcd + b^2d^2) + 4(a^2b^2 + 2abcd + c^2d^2)$$
$$+(a^4+b^4+c^4+d^4 - 2a^2b^2 - 2a^2c^2 + 2a^2d^2 + 2b^2c^2 - 2b^2d^2 - 2c^2d^2)$$

so

$$pq^2 = a^4 + b^4 + c^4 + d^4 + 2(a^2b^2 + a^2c^2 + a^2d^2 + b^2c^2 + b^2d^2 + c^2d^2)$$

thus $pq^2 = p^2$ so $q^2 = p$.

Since p is prime, this is a contradiction.

So the two conditions (*) and (**) are linearly independent over $\mathbb{Q}$ hence they determine a line in $\mathbb{R}^3$ on which the vector (u,v,w) must lie.

Let $\varphi(\alpha,\beta) = (\mu_1,\rho_1)$ where $\mu_1 = u_1 i_1 + v_1 i_2 + w_1 i_3$. Then $\gcd(u_1,v_1,w_1) = 1$ and (u_1,v_1,w_1) lies on the same line in $\mathbb{R}^3$ as does (u,v,w). The condition $\gcd(u,v,w) = \gcd(u_1,v_1,w_1)$ implies that $(u,v,w) = \pm(u_1,v_1,w_1)$, which completes the proof.

Let $t(p)$ denote the number of ways to write p as a sum of three squares and let $f(p)$ denote the number of Hurwitz quaternions with norm p (i.e. $f(p)$ is the number of ways to write p as a sum of four squares plus the number of ways to write $4p$ as a sum of four odd squares.) We are now ready to state the main result.

Theorem 4.2. Let $m(p)$ be the number of discriminants $-4m$, with m a sum of two squares, such that the prime divisors of (p) are regular ideals in classes of order 3 in the ring class group with discriminant $-4m$. Here each discriminant is counted with multiplicity 2^{t-1} where t is the number of prime divisors of $4m$. Then

(A) $m(p) = \frac{1}{16} f(p)h(p) - 6h(p) + 2$ if $p \equiv 1 \bmod 4$

(B) $m(p) = \frac{1}{8} f(p)h(p) - 6h(p)$ if $p \equiv 3 \bmod 8$

(C) $m(p) = 0$ if $p \equiv 7 \bmod 8$.

Proof. First we will prove the following two statements which are equivalent to (A) and (B) above by Theorem 2.1.

(A′) $m(p) = \frac{1}{192} |A| \cdot |B| - 6h(p) + 2$ if $p \equiv 1 \bmod 4$

(B′) $m(p) = \frac{1}{192} |A| \cdot |B| - 6h(p)$ if $p \equiv 3 \bmod 8$

(the sets A and B are defined in Definition 4.1).

First suppose the prime divisors of (p) are in classes of order 3 in the ring class group associated with discriminant $-4m$. Assume that m can be written as a sum of 2 squares and that p does not divide m (so the prime divisors of (p) are regular ideals). Choose a pair $(\alpha,\beta) \in A \times B$ according to the following scheme;

1. Choose $\rho = ri_1 + si_2$ with $r^2 + s^2 = m$, $(r,s) = 1$.

2. Choose $\mathfrak{p} = (p, a+\sqrt{-m})$, one of the prime divisors of (p). Let $\mathcal{C}$ denote the ideal class to which $\mathfrak{p}$ belongs.

3. Let $\mathfrak{p}_\rho = (p, a+\rho)$ and let K be a greatest common right divisor of $E\mathfrak{p}_\rho$. Let $\alpha = \overline{K}$ and let $\mu = K\rho K^{-1}$; write $\mu = ui_1 + vi_2 + wi_3$.

4. By Corollary 3.2 (a) the class $\mathcal{C}^{-1} = \mathcal{C}^2$ maps the bundle $[r,s,0]$ to the bundle $[-u,-v,-w]$. Hence $\mathcal{C}$ maps $[u,v,w]$ to $[-u,-v,-w]$. Let $\mathfrak{p}_\mu = (p, a+\mu)$; pick β, a greatest common right divisor of $E\mathfrak{p}$, such that $\beta\mu\beta^{-1} = -\mu$.

By our choice of (α,β) we have

$$\alpha\mu\alpha^{-1} = \rho$$

$$\text{and} \quad \beta\mu\beta^{-1} = -\mu.$$

By Lemma 4.7 we have $\varphi(\alpha,\beta) = \pm(\mu,\rho)$.

Note that (α,β) is *not* a degenerate pair. For if any coefficient of μ is 0 then $[\mu] = [-\mu]$, so $\mathcal{C}$ maps $[\mu]$ to itself since $\beta\mu\beta^{-1} = -\mu$. This implies that $\mathcal{C}$ is the identity class which contradicts the assumption that $\mathcal{C}$ has order 3. Thus we've chosen a nondegenerate pair (α,β).

Conversely, let (α,β) be a nondegenerate pair. Let $\varphi(\alpha,\beta) = (\mu,\rho)$ and let $m = N(\mu)$. By Lemma 4.2 (a) and (c) we have

$$\alpha\mu\alpha^{-1} = \rho$$

$$\text{and} \quad \beta\mu\beta^{-1} = -\mu. \qquad (*)$$

Let $\mathfrak{p}_\mu = \mathbb{Q}(\mu) \cap E\alpha$ and let $\mathfrak{Q}_\mu = \mathbb{Q}(\mu) \cap E\beta$. By the equation in (*) we have $\alpha\mu\alpha^{-1} \in E$ and $\beta\mu\beta^{-1} \in E$ so by Theorem 3.1 we have

$E\mathfrak{P}_\mu = E\alpha$ and $E\mathfrak{Q}_\mu = E\beta$. By Lemma 3.2, $\mathfrak{P}_\mu$ and $\mathfrak{Q}_\mu$ are integral ideals of $\mathbb{Q}(\mu)$ each having norm p. Since μ has 3 nonzero coefficients, $[-\mu] \neq [\rho]$ hence $\mathfrak{P}_\mu \neq \mathfrak{Q}_\mu$. Let $\mathfrak{P}$ and $\mathfrak{Q}$ be the ideals in $\mathbb{Q}(\sqrt{-m})$ whose images under the map $\sqrt{-m} \to \mu$ are $\mathfrak{P}_\mu$ and $\mathfrak{Q}_\mu$ respectively. From the above we see that $\mathfrak{Q} = \mathfrak{P}'$ and $(p) = \mathfrak{P}\mathfrak{P}'$. Henceforth let $\mathfrak{P}'_\mu$ denote $\mathfrak{Q}_\mu$.

Let $\mathfrak{C}$ denote the class in the class group of $\mathbb{Q}(\sqrt{-m})$ which contains $\mathfrak{P}'$. Then $\mathfrak{C}^{-1}$ contains $\mathfrak{P}$ so the equations $E\mathfrak{P}_\mu = E\alpha$ and $\alpha\mu\alpha^{-1} = \rho$ imply that $\mathfrak{C}^{-1}$ maps $[\mu]$ to $[\rho]$. Thus $\mathfrak{C}$ maps $[\rho]$ to $[\mu]$ so $\mathfrak{C}^{-1}$ maps $[\rho]$ to $[-\mu]$ by Corollary 3.2 (a). The equations $E\mathfrak{P}'_\mu = E\beta$ and $\beta\mu\beta^{-1} = -\mu$ imply that $\mathfrak{C}$ maps $[\mu]$ to $[-\mu]$ so $\mathfrak{C}^2$ maps $[\rho]$ to $[-\mu]$. Since the class group action is sharply transitive, $\mathfrak{C}^2 = \mathfrak{C}^{-1}$ and so $\mathfrak{C}^3 = 1$. Also note that μ has three nonzero coefficients so $[\mu] \neq [\rho]$, and hence $\mathfrak{C} \neq 1$. Thus $\mathfrak{C}$ is a class of order 3 containing a prime divisor of (p).

So the map φ defines a many-one correspondence between nondegenerate pairs $(\alpha,\beta) \in A \times B$ and discriminants $-4m$ for which the prime divisors of (p) are regular ideals in classes of order 3 in the ring class group with discriminant $-4m$. We need to compute the exact ratio of this many-one correspondence.

Consider the freedom of choice we have in carrying out the 4 step procedure given at the start of this proof.

1. The bundle containing $\rho = ri_1 + si_2$ can be chosen in 2^{t-1} ways where t is the number of prime divisors of $4m$. Once the bundle containing ρ is chosen, the pair r, s can be picked in 4 ways.

Total choice $4 \cdot 2^{t-1}$.

2. A prime divisor $\mathfrak{p}$ of (ρ) can be chosen in 2 ways.

   Total choice 2.

3. K can be chosen in 24 ways; α and μ are specified by K.

   Total choice 24.

4. β must map μ to $-\mu$ so there are 2 choices for β.

   Total choice 2.

Hence we have $384 \cdot 2^{t-1}$ choices in all when constructing α and β. However the function φ makes an arbitrary choice of either $\mathfrak{p}$ or $\mathfrak{p}'$ at step 2.. To see this suppose $\varphi(\alpha,\beta) = (\mu,\rho)$. Then we have

$$\alpha\mu\alpha^{-1} = \rho \quad \text{and} \quad \beta\mu\beta^{-1} = -\mu$$

so we also have

$$\alpha(-\mu)\alpha^{-1} = -\rho \quad \text{and} \quad \beta(-\mu)\beta^{-1} = -(-\mu).$$

Also $i_3\rho i_3^{-1} = -\rho$ so ρ and $-\rho$ are in the same bundle. By the definition of φ we made a choice between (μ,ρ) and $(-\mu,-\rho)$.

Hence we've shown that there is a $192 \cdot 2^{t-1}$ to 1 correspondence between non-degenerate pairs (α,β) in $A \times B$ and the ring class groups with discriminant $-4m$, with m a sum of two relatively prime squares, in which the prime divisors of (p) are regular and fall in classes of order 3. Applying Theorem 4.1 completes the proof of Theorem 4.2, (A) and (B).

Lastly we must consider the case $p \equiv 7 \pmod 8$. Suppose m can be written as $m = r^2 + s^2$ and suppose that the prime divisors of (p) are regular ideals in classes of order 3 in the ring class group $\Gamma(m)$.

There exist integers a and b such that $p^3 = a^2 + b^2 m$, since there is a principal ideal of norm p^3 in $\mathcal{O}_f$. But now $p^3 \equiv -1 \bmod 8$ so $a^2 + (br)^2 + (bs)^2 \equiv -1 \pmod 8$ and it is well-known that this latter congruence is impossible. Thus $m(p) = 0$ when $p \equiv 7 \pmod 8$.

Conclusion

The work in this thesis suggests some lines of further research. Consider the quadratic space given by $\mathbb{Q}$ and the norm form $x^2 + my^2$. The Clifford Algebra of this quadratic space is the quaternion algebra H (see Edwards and Snapper [5]). One can view the embeddings of $\mathbb{Q}(\sqrt{-m})$ in E as the embeddings of the quadratic space $(\mathbb{Q}, x^2 + y^2 m)$ in its Clifford Algebra. This leads one to ask whether the results discovered by Venkow and extended in this thesis are true of the embeddings of an arbitrary quadratic space in its Clifford Algebra.

Another possible line of research is suggested by work of Pat Morton. Using results of Barracand and Cohn [1], Morton showed that the eighth degree extension $K = \mathbb{Q}(i, \sqrt{i + \sqrt{2}})$ has the property that for all primes p, 8 divides the class number of $\mathbb{Q}(\sqrt{-p})$ iff p splits completely in K (see Morton [9]). This latter condition is equivalent to saying that p is a norm from K since K has class number 1. It is unknown whether there exists a corresponding field F with the property that 16 divides $h(p)$ iff p splits completely in F. There is evidence that 2 should be the only prime to ramify in F, if F exists. Harvey Cohn and Jeff Lagarius have shown that no field F of degree 16 over $\mathbb{Q}$ in which 2 is the only prime to ramify has the desired property (this work is unpublished but in preparation). So the existence of such a field F seems questionable.

There may however be a degree 16 division algebra A over $\mathbb{Q}$ which has the property that 16 divides $h(p)$ iff p is a norm from A. A likely sort of division algebra to consider is one of degree 4 over H, where H denotes the quaternion algebra. It is hoped that

results from this thesis may guide one in choosing the algebra A and then simplify the ensuing proofs. For example one might consider adjoining λ, where is a fourth root of 2, to H with some sort of twisted multiplication. We have that λ^2 is a square-root of 2. For $p \equiv 1, 2 \bmod 4$, $\mathbb{Q}(\sqrt{-p})$ has an ideal square root of (2). Corollary 3.1 from this thesis suggests the multiplication $\lambda^2 i_1 = -i_1\lambda^2$, $\lambda^2 i_2 = -i_3\lambda^2$ and $\lambda^2 i_3 = -i_2\lambda^2$. In this way one might be able to use results from this work to shed light on the above question.

References

[1] P. Barracand and H. Cohn, A Note on primes of type $x^2 + 32y^2$, class number and residuacity, J. reine angew. Math. 238 (1969), pp. 67-70.

[2] Cohn, Harvey, A Classical Invitation to Algebraic Numbers and Class Fields, Springer-Verlag, 1978.

[3] Dade, E. C., Taussky, O., and Zassenhaus, H., On the theory of orders, in particular on the semigroup of ideal classes and genera of an order in an algebraic number field, Math. Ann. 148, 1962.

[4] Dickson, L. E., Algebras and Their Arithmetics, Univ. of Chicago Press, 1923.

[5] Edwards, B. and Snapper, E., Clifford Algebras. (in preparation).

[6] Gauss, C. F., Disquisitiones Arithmeticae, trans. by Arthur A. Clarke, Yale University Press, 1965.

[7] Hurwitz, A., Über die Zahlentheorie der Quaternionen, Mathematische Werke, Band II, Birkhäuser, 1963, pp. 303-330.

[8] MacDuffee, C. C., An Introduction to the Theory of Ideals in Linear Associative Algebras, Trans. of the American Math. Soc. pp. 71-90, 1929.

[9] Morton, P., The Quadratic Number Fields with Cyclic 2-Classgroups, in preparation.

[10] Rehm, H. P., On a Theorem of Gausz concerning the number of integral solutions of the equation $x^2 + y^2 + z^2 = m$, Selected Topics on Ternary Forms and Norms, Olga Taussky Todd, ed., Dekker (to appear).

[11] Smith, H.J.S., On Systems of Indeterminate Linear Equations, Collected Mathematical Papers of Henry J. S. Smith, J.W.L. Glaisher, ed., Oxford at the Clarendon Press, 1894.

[12] Taussky, Olga, On Matrix Classes Corresponding to an Ideal and its Inverse, Illinois Journal of Mathematics, Vol. 1, No. 1, pp. 108-112, 1957.

[13] Venkow, V., On the arithmetic of quaternions, (Russian), Bulletin de l'Académie des Sciences de l'URSS, Part I and II, pp. 205-246, 1922.