SYMMETRIC REPRESENTATIONS OF AN INTEGRAL DOMAIN OVER A SUBDOMAIN

Thesis by

Edward Anton Bender

In Partial Fulfillment of the Requirements

For the Degree of

Doctor of Philosophy

California Institute of Technology

Pasadena, California

1966

(submitted February 8, 1966)

ACKNOWLEDGMENTS

I would like to express my gratitude to my research advisor Dr. Olga Taussky Todd for bringing to my attention the area of study dealt with in this thesis, for continually encouraging and guiding my research, and for patiently assisting in the preparation of this material. I would also like to thank Dr. Everett C. Dade for his guidance, especially on Section IV.

I am indebted to the National Science Foundation for a Cooperative Fellowship grant and for a research grant to use an IBM 7094 computer. Further, I wish to thank the California Institute of Technology for teaching assistantships.

ABSTRACT

Let $F(\theta)$ be a separable extension of degree n of a field F. Let Δ and D be integral domains with quotient fields $F(\theta)$ and F respectively. Assume that $\Delta \supseteq D$. A mapping Φ of Δ into the $n \times n$ D matrices is called a Δ/D rep if (i) it is a ring isomorphism and (ii) it maps d onto dI_n whenever $d \in D$. If the matrices are also symmetric, Φ is a Δ/D symrep.

Every Δ/D rep can be extended uniquely to an $F(\theta)/F$ rep. This extension is completely determined by the image of θ. Two Δ/D reps are called equivalent if the images of θ differ by a D unimodular similarity. There is a one-to-one correspondence between classes of Δ/D reps and classes of Δ ideals having an n element basis over D.

The condition that a given Δ/D rep class contain a Δ/D symrep can be phrased in various ways. Using these formulations it is possible to (i) bound the number of symreps in a given class, (ii) count the number of symreps if F is finite, (iii) establish the existence of an $F(\theta)/F$ symrep when n is odd, F is an algebraic number field, and $F(\theta)$ is totally real if F is formally real (for $n = 3$ see Sapiro, "Characteristic polynomials of symmetric matrices" Sibirsk. Mat. Ž. 3 (1962) pp. 280-291), and (iv) study the case $D = Z$, the integers (see Taussky, "On matrix classes corresponding to an ideal and its inverse" Illinois J. Math. 1 (1957) pp. 108-113 and Faddeev, "On the characteristic equations of rational symmetric matrices" Dokl. Akad. Nauk SSSR 58 (1947) pp. 753-754).

The case $D = Z$ and $n = 2$ is studied in detail. Let Δ' be an integral domain also having quotient field $F(\theta)$ and such that $\Delta' \supseteq \Delta$. Let Φ be a Δ/Z symrep. A method is given for finding a Δ'/Z symrep Θ such that the Δ' ideal class corresponding to the class of Θ is an extension to Δ' of the Δ ideal class corresponding to the class of Φ. The problem of finding all Δ/Z symreps equivalent to a given one is studied.

TABLE OF CONTENTS

INTRODUCTION

Let $F(\theta)$ be a separable extension of a field F. It is clear that there is a set $\mathfrak{M}$ of square F matrices isomorphic to $F(\theta)$ with $f \in F$ corresponding to fI; one need only consider the extension generated by the companion matrix of θ. We wish the elements of $\mathfrak{M}$ to be symmetric matrices. Krakowski [10] has shown that this can always be done if F is not formally real, and that for formally real F it is necessary and sufficient that $F(\theta)$ be totally real*. The minimum possible dimension of the symmetric matrices in such a set $\mathfrak{M}$ is not known. We shall study the case when this dimension is $[F(\theta) : F]$.

Related problems deal with the characteristic polynomials of matrices. Let D be an integral domain with quotient field F. Let $p(x)$ be an n^{th} degree monic D polynomial irreducible over F. When D is the integers, the $n \times n$ D matrix roots of $p(x) = 0$ have been studied by

(i) Latimer and MacDuffee [11] who established a correspondence between classes of ideals and classes of such matrices under similarity via a unimodular matrix,

(ii) Taussky [16-19] who found the class corresponding to A'

*Whenever F is formally real and $H \supseteq F$, H is said to be totally real if and only if $H \subseteq \cap R$ $(R \in \mathfrak{R})$ where $\mathfrak{R}$ is the set of real closures of F lying in the algebraic closure of H.

in terms of the class corresponding to A, and studied the classes containing symmetric matrices when $n = 2$, and

(iii) Faddeev [3] who studied the existence of symmetric roots when $n \leq 7$.

For D an algebraic number field and $n = 3$, Sapiro [14] used $\mathfrak{p}$-adic analysis to show that $p(x) = 0$ has a symmetric 3×3 D matrix root if and only if Krakowski's condition holds.

We shall generalize the above questions and results. Suppose Δ is an integral domain with subdomain D and quotient field G, a separable extension of degree n of F, the quotient field of D. A representation of Δ over D (abbreviated Δ/D rep) is a ring isomorphism of Δ onto a ring of $n \times n$ matrices over D such that $d \in D$ goes into dI_n. If the matrices are symmetric, we speak of a Δ/D symrep.

Section I discusses the basic nature of Δ/D reps and generalizes the Latimer-MacDuffee and Taussky correspondences (Theorem 1.5).

The nature of Δ/D symreps is studied in Section II. Theorem 2.2 reformulates the question of existence of symreps in a given class of Δ/D reps in a variety of ways. These depend on the orthogonality of the characteristic vectors of a symmetric matrix. This leads to a formulation in terms of quadratic forms. Let $\mathfrak{a}$ be in the class of ideals corresponding to the given rep class. By Theorem 1.5 there is an n element basis $\alpha_1,\ldots,\alpha_n$ for $\mathfrak{a}$ over D. There is a symrep in the given class if and only if for some

$\lambda \in G$ the quadratic form $\Sigma(\mathrm{tr}_{G/F}\, \lambda\alpha_i\alpha_j)x_i x_j$ is equivalent over D to a sum of n squares (see [14] where D = F and G is replaced by a direct sum of fields, also see [3] where D = Z). In Theorem 2.5 we bound the number of symreps in a class by the cardinality of the group of orthogonal $n \times n$ D matrices times the cardinality of a quotient group of units in a suitable extension of Δ which depends on the symrep class.

In Section III the existence of G/F symreps is guaranteed when F is finite. The number of symreps is computed.

In Section IV we take F to be an algebraic number field. Theorem 4.1 generalizes a method of Sapiro to all odd n: the quadratic form problem of Section II mentioned above has a solution if and only if the corresponding problems do for all $\mathfrak{p}$-adic completions of F. The infinite spots yield Krakowski's condition. A series of lemmas deals with the finite spots. This results in Theorem 4.2 which states that Krakowski's condition is necessary and sufficient for the existence of G/F symreps when n is odd.

Section V briefly considers D = Z.

The easiest case in which $D \neq F$ is the case D = Z and n = 2. This is dealt with in Section VI. We start by applying the results of Sections II and V (Theorems 6.2 and 6.3)

(i) to show that a class containing symreps contains four (resp. eight) if there exists (resp. does not exist) a unit of norm -1 in an appropriate extension of Δ which depends on the symrep class (the same one as in Section II), and

(ii) to characterize classes with symreps when Δ is the ring of integers in G. Nearly all of Theorem 6.3 is contained in Taussky's work [18,19]. The remainder of the section uses special properties available when $D = Z$ and $n = 2$ in order to deal with two questions. Let Δ' be an integral domain also having quotient field G and such that $\Delta' \supseteq \Delta$. Let C be an ideal class of Δ corresponding to the class of a Δ/D symrep; if C is extended to an ideal class C' of Δ', exhibit a symrep (if any exist) in the corresponding class of Δ'/D reps. This is solved by Theorem 6.4 and we find that such a symrep always exists if Δ' is contained in the ring of integers of G. In the second problem we are given a Δ/D symrep and asked to find all equivalent ones. This is only partially solved. We introduce a function called the conjugator. A complete knowledge of its values would simplify the problem. All we can provide is a partial description of its nature (Theorem 6.6).

I. REPRESENTATIONS IN GENERAL

Throughout this thesis Δ will be an integral domain with subdomain D. The quotient fields will be G and F respectively. We assume that G is a separable extension of F of finite degree n. Thus G is a simple extension of F and we may write $G = F(\theta)$ for some θ.

Definition 1.1. A mapping $\Phi(\alpha)$ taking every $\alpha \in \Delta$ onto an $n \times n$ matrix over D is a representation of Δ in D if

(i) Φ is a ring isomorphism and

(ii) whenever $d \in D$ we have $\Phi(d) = dI_n$. We abbreviate this to Δ/D rep. If the matrices are symmetric, Φ is called a Δ/D symrep. Let Φ and Ψ be two Δ/D reps. If there exists a D unimodular matrix T (i.e., a matrix over D whose determinant is a D unit) such that $T\Phi(\alpha)T^{-1} = \Psi(\alpha)$ for all $\alpha \in \Delta$, then we say Φ is equivalent to Ψ.

Lemma 1.1. The above definition leads to an equivalence relation. Further, if T is an $n \times n$ D unimodular matrix and Φ is a Δ/D rep, then $T\Phi(\alpha)T^{-1} = \Psi(\alpha)$ defines another Δ/D rep.

Proof. If A is a D matrix and T is a D unimodular matrix and both are $n \times n$, then TAT^{-1} is a D matrix. Since $|TS| = |T| \cdot |S|$ and the units in D form a group, the $n \times n$ D unimodular matrices form a group. Write $T(\Phi) = \Psi$ if

$T\,\Phi(\alpha)T^{-1} = \Psi(\alpha)$ for all $\alpha \in \Delta$. Then we have $(TS)(\Phi) = T(S(\Phi))$. The lemma follows from the closure and inverse properties of a group.

When we specialize Δ to G and D to F, we have one of the questions mentioned in the Introduction. The problem of symmetric D matrix roots of irreducible characteristic polynomials over D is also included. To see this, take $\Delta = D[\theta]$, where θ is a root of the polynomial in question, then apply the following lemma.

<u>Lemma 1.2</u>. Let Φ be a Δ/D rep and let $\alpha \in \Delta$. If $p(x)$ is a D polynomial, then $\Phi(p(\alpha)) = p(\Phi(\alpha))$. Further, the characteristic roots of $\Phi(\alpha)$ are the conjugates of α over F.

<u>Proof</u>. Write $p(x) = \Sigma a_k x^k$. Then

$$\Phi(p(\alpha)) = \Phi(\Sigma a_k \alpha^k) = \Sigma\Phi(a_k)\Phi(\alpha)^k = \Sigma a_k I_n\, \Phi(\alpha)^k = p(\Phi(\alpha)) .$$

Let $q(x)$ be an irreducible F polynomial for α. Since F is the quotient field of D, there is an $m \neq 0$ in D such that $p(x) = mq(x)$ is a D polynomial. Now $0 = \Phi(p(\alpha)) = p(\Phi(\alpha))$. Hence every characteristic root of $\Phi(\alpha)$ is a root of $p(x) = 0$.

From the lemma we see that if there is a Δ/D rep, then every element in Δ is a zero of an nth degree monic D polynomial, the characteristic polynomial of its image. If $\Delta = D[\theta]$, this condition on elements of Δ is sufficient to guarantee a Δ/D rep (but not a Δ/D symrep), for we may take $\Phi(\theta)$ to be the companion matrix for the monic D polynomial for θ. In general it is not known if the condition that the elements of Δ satisfy monic nth degree D polynomials is sufficient to guarantee a Δ/D rep. The corollaries to Theorem 1.5 will give additional results on this question. Sometimes it is useful to note that if Δ' is an integral domain such that Δ/Δ' and Δ'/D reps (symreps) exist, then there is a Δ/D rep (symrep). To see this, let Θ and Φ be the Δ/Δ' and Δ'/D reps respectively and define $\Psi(\alpha) = (\Phi(a_{ij}))$ where $(a_{ij}) = \Theta(\alpha)$ and $\alpha \in \Delta$.

The lemma is also useful in showing

Theorem 1.1. Every Δ/D rep Φ can be extended to a G/F rep in exactly one way. We shall refer to this extension as Φ also. The image of α^{-1} is the matrix inverse of $\Phi(\alpha)$. If Φ is a symrep, so is the extension. A partial converse is true: given D and a G/F rep Φ, there is a Δ with quotient field G such that Φ is an extension of a Δ/D rep.

Proof. If $\alpha \neq 0$, then $\Phi(\alpha)$ has no characteristic roots equal to zero by the lemma. Thus $\Phi(\alpha)$ is nonsingular. The quotient field of $\Phi(\Delta)$ under matrix inverse provides a G/F rep which is an extension of Φ. Let Ψ be an extension of Φ to G. If $\alpha \in \Delta$, then $I = \Phi(1) = \Psi(1) = \Psi(\alpha^{-1})\Psi(\alpha) = \Psi(\alpha^{-1})\Phi(\alpha)$. Hence $\Psi(\alpha^{-1}) = \Phi(\alpha)^{-1}$ and so Ψ is uniquely determined on G, the quotient field of Δ. We prove the partial converse. Suppose $\Phi(\theta) = ((\alpha_{ij}/\beta_{ij}))$ where $\alpha_{ij}, \beta_{ij} \in D$. Let $\alpha = \left(\prod_{i,j} \beta_{ij}\right)\theta$. Then Φ is the extension of a $D[\alpha]/D$ rep.

Corollary 1.1.1. The nature of a Δ/D rep is completely determined by the image of θ under the extension to a G/F rep. The Δ/D rep is a symrep if and only if the image of θ is symmetric. Two Δ/D reps Φ and Ψ are equivalent if and only if for some D unimodular matrix T

$$T\Phi(\theta)T^{-1} = \Psi(\theta) .$$

Proof. The result is clear since $G = F(\theta)$ and for $f \in F$, the image is fI_n.

We shall find it convenient to deal with $\Phi(\theta)$ rather than Φ. The above corollary shows that this is possible.

Definition 1.2. Let Φ be a Δ/D rep (symrep) with $\Phi(\theta) = A$. We shall speak of the Δ/D rep (symrep) A and the equivalence class $C(A) = \{B : \Psi(\theta) = B$ and Ψ is equivalent to $\Phi\}$.

By Corollary 1.1.1, $C(A) = \{B : B = TAT^{-1}$ for some D unimodular matrix $T\}$.

In the proof of Lemma 1.2 the condition $\Phi(d) = dI_n$ for $d \in D$ was essential. It is also of central importance in our later work. The following example shows that much of our work would not hold if we removed the condition $\Phi(d) = dI_n$. It is suggested that the reader refer to it later if any question as to the usefulness of the condition arises. Let D' be an integral domain, x an indeterminate, $D = D'[x^n]$, and $\Delta = D'[x]$. Let $\mathcal{S}$ be a finite set of positive integers. Let a matrix E_k be defined for each $k \in \mathcal{S}$ such that

(i) $E_k^2 = E_k$ all $k \in \mathcal{S}$

(ii) $\Sigma \dim E_k = n$ (sum over $k \in \mathcal{S}$)

(iii) for some $k \in \mathcal{S}$ we have $E_k \neq 0$.

For $p(x) \in \Delta$ define $\Phi(p(x)) = \Sigma \oplus p(x^{kn})E_k$ (direct sum over $k \in \mathcal{S}$). Then Φ satisfies all the conditions for a Δ/D rep except possibly $\Phi(d) = dI_n$ whenever $d \in D$. We can even extend it to a ring isomorphism on G. As an example let $n = 2$ and $E_1 = (0)$ and $E_2 = (1)$.

The fact that F is not a finite extension of its prime field is essential in this type of example. We shall see that $\Phi(d) = dI_n$ is redundant when F is its prime field and nearly redundant when F is a finite extension of its prime field.

Theorem 1.2. If F is Q or the integers modulo a prime and Φ is a ring isomorphic map of Δ onto a set of $n \times n$ matrices over D, then Φ is a Δ/D rep.

Proof. Let k and m be integers and let $\Phi(1) = E$. Then $\Phi(k) = \Phi(1) + \cdots + \Phi(1) = kE$ and, when $k/m \in D$,

$m\Phi(k/m) = m\Phi(1)\Phi(k/m) = \Phi(m)\Phi(k/m) = \Phi(k) = kE$. Since F is its own prime field, $\Phi(d) = dE$ for $d \in D$. We must show that $E = I_n$. We may choose $\alpha \in \Delta$ so that $G = F(\alpha)$ and $\Phi(\alpha)$ is a D matrix. Let $p(x) = \Sigma a_i x^i$ be the characteristic polynomial of $\Phi(\alpha)$. Then $0 = p(\Phi(\alpha))E = \Sigma a_i E\Phi(\alpha)^i = \Sigma\Phi(a_i)\Phi(\alpha^i) = \Phi(\Sigma a_i \alpha^i) = \Phi(p(\alpha))$. Since $p(\alpha) \in \Delta$ and Φ is an isomorphism, $p(\alpha) = 0$. The monic irreducible F polynomial q for α has degree $[F(\alpha) : F] = n$ and q divides p which is of degree n. Thus $p = q$. Hence zero is not a root of $p = 0$. Thus $\Phi(\alpha)$ is nonsingular. Since $\Phi(\alpha) = \Phi(\alpha)E$, it follows that $E = I_n$.

When F is a finite extension of its prime field we cannot hope to get a result as strong as Theorem 1.2 since automorphisms of G need not be trivial on F. The best we can hope for is that dI_n will be the image of σd where σ is an isomorphism of F into the field G. This is in fact true.

Theorem 1.3. Let F be a finite extension of its prime field Π. Let Θ map Δ ring isomorphically into $n \times n$ D matrices. Then there is a unique extension of Θ to a ring isomorphism Θ^* of G into $n \times n$ F matrices. There is an isomorphism σ of G into its normal completion such that $\Theta^*\sigma$ is a $\sigma^{-1}G/F$ rep where $\Theta^*\sigma(\alpha) = \Theta^*(\sigma(\alpha))$ for $\alpha \in \sigma^{-1}G$.

Proof. In the course of the proof we shall develop the diagram shown here.

$$\begin{tikzcd}
 & \Omega \arrow[dl, dash] \arrow[dr, dash] & & & \\
\Pi(\psi') \arrow[d, dash] \arrow[drr, dash] & & G = \Pi(\psi) \arrow[ll] \arrow[dll, dash] \arrow[d, dash, "n"] \arrow[dr, "\Theta^*"] \arrow[ddrr, bend left, "\Psi"] & & \\
K \arrow[drr, dash] & & F = \Pi(\varphi) \arrow[ll, "\sigma"'] \arrow[d, dash, "m"] \arrow[dr, "\Phi"] & \begin{array}{c} n \times n \\ \text{over} \\ F \end{array} & \\
 & & \Pi & \begin{array}{c} m \times m \\ \text{over} \\ \Pi \end{array} & \begin{array}{c} mn \times mn \\ \text{over} \\ \Pi \end{array}
\end{tikzcd}$$

All finite extensions of Π are separable so we may write $G = \Pi(\psi)$ and $F = \Pi(\varphi)$ for some $\psi \in \Delta$ and $\varphi \in F$. Let $m = [F : \Pi]$. Let Ω be the algebraic closure of G. Let Φ be the F/Π rep determined by mapping φ onto its companion matrix.

Define $\Psi(\alpha)$ for $\alpha \in \Delta$ to be $(\Phi(a_{ij}))$ where $(a_{ij}) = \Phi(\alpha)$. By Theorem 1.2, Ψ is a Δ/Π rep. By Theorem 1.1, Ψ can be extended uniquely to a G/Π rep. We have $\Psi(\alpha) = (\Phi(a_{ij}(\alpha)))$ for all $\alpha \in G$ since Ψ is extended to G by operations that can be performed blockwise. Let $\Theta^*(\alpha) = (a_{ij}(\alpha))$. This is clearly an extension of Θ to all of G since Ψ is a G/Π rep. It is unique since if Θ^{**} is an extension with $\Theta^{**}(\alpha) \neq \Theta^*(\alpha)$ with $\alpha \in G$, the corresponding Ψ's are unequal on α, contradicting the uniqueness of the extension of Ψ to a G/Π rep. We have $\pi I_{mn} = \Psi(\pi) = (\Phi(a_{ij}))$ for $\pi \in \Pi$ where $(a_{ij}) = \Theta^*(\pi)$. Thus $\Phi(a_{ii}) = \pi$ and $\Phi(a_{ij}) = 0$ for $i \neq j$. Since Φ is an F/Π rep we have $a_{ii} = \pi$ and $a_{ij} = 0$ for $i \neq j$. Thus $\Theta^*(\pi) = \pi I_n$.

The roots of $\Phi(\varphi)$ are the conjugates of φ over Π. By Lemma 1.2 applied to the G/Π rep Ψ, the roots of $\Psi(\psi)$ are the conjugates of ψ over Π. We have $\Psi(\psi) = (\Phi(a_{ij})) = (p_{ij}(\Phi(\varphi))$ where $\Theta(\psi) = (a_{ij})$ and p_{ij} is a Π polynomial such that $p_{ij}(\varphi) = a_{ij}$. By Williamson's theorem [21] the roots of $\Psi(\psi)$ are the roots of $(p_{ij}(\varphi^{(k)}))$ for $1 \leq k \leq m$. In particular, the roots of $\Theta(\psi) = (p_{ij}(\varphi))$ are roots of $\Psi(\psi)$. Thus the roots of $\Theta(\psi)$ are conjugates of ψ over Π. Let one such root be ψ'. Since $\Theta(\psi)$ is an $n \times n$ F matrix, ψ' has at most n conjugates over F. Thus $[F(\psi') : \Pi] = [F(\psi') : F]\cdot m \leq nm = [\Pi(\psi') : \Pi] \leq [F(\psi')\cdot\Pi]$. Hence $F(\psi') = \Pi(\psi')$ and ψ' has n conjugates over F and $F \subseteq \Pi(\psi')$.

Let $K = \{\alpha : \Theta^*(\alpha)$ is a scalar matrix and $\alpha \in G\}$. Since $\Theta(\psi)$ has distinct roots there is an Ω matrix S such that $S\Theta(\psi)S^{-1} = \mathrm{diag}(\psi', \ldots)$ where the entries are the conjugates of ψ' over F. For any $\alpha \in G$ there is a Π polynomial p_α such that $p_\alpha(\psi) = \alpha$. Thus we have that $\Theta^*(\alpha)$ is scalar if and only if $S\Theta^*(\alpha)S^{-1} = \mathrm{diag}(p_\alpha(\psi'), \ldots)$ is scalar. Thus $K = \{p(\psi) : p(\psi') \in F$ and p is a Π polynomial$\}$. As $\Pi(\psi') \supseteq F$, there is an isomorphism $\sigma : F \rightarrowtail K$ such that $\sigma(p(\psi')) = p(\psi)$. Consequently we may extend σ to an isomorphism of G. Consider $\Theta^*\sigma$. Let p be a Π polynomial. If $p(\psi') \in F$, then $\Theta^*\sigma(p(\psi')) = \Theta^*(p(\psi)) = S^{-1}p(S\Theta^*(\psi)S^{-1})S = S^{-1}p(\psi')I_nS = p(\psi')I_n$.

It was mentioned in the introduction that the study of Δ/D rep classes is related to ideal classes. We shall establish this correspondence in precise terms after we have formulated the concept of an M-ideal.

Definition 1.3. A fractional ideal $\mathfrak{a}$ of Δ is a nonempty subset of G such that $\mathfrak{a} + \mathfrak{a} \subseteq \mathfrak{a}$ and $\Delta\mathfrak{a} \subseteq \mathfrak{a}$, and for some $\lambda \in \Delta$ we have $\mathfrak{a} \subseteq \Delta/\lambda$. If $\mathfrak{a}$ has an n element basis when regarded as a module over D we say that $\mathfrak{a}$ is an M-ideal (of Δ over D) and call such a basis a module basis.

Ideals of orders in algebraic number fields need not be M-ideals; however, it is well known that when $D = Z$ every ideal is an M-ideal. There is only one M-ideal of G over F, namely G itself with $1, \theta, \ldots, \theta^{n-1}$ as a basis. These observations will be useful later.

Theorem 1.4. Let $\underline{\alpha}$ be a column vector whose components form a module basis for the M-ideal $\mathfrak{a}$. We call $\underline{\alpha}$ an mbv for $\mathfrak{a}$ (module basis vector). Let $C(\mathfrak{a}) = \{\lambda\mathfrak{a} : \lambda \in G\}$, the class of ideals equivalent to $\mathfrak{a}$. Let $M(\underline{\alpha})$ be the $n \times n$ matrix $(\underline{\alpha}^{(1)}, \ldots, \underline{\alpha}^{(n)})$ where $\underline{\alpha}^{(i)}$ is the ith conjugate of $\underline{\alpha}$. These notations will be used throughout the thesis. We have

(1) $C(\mathfrak{a})$ contains only M-ideals;

(2) $\underline{\beta}$ is another mbv for $\mathfrak{a}$ if and only if $T\underline{\alpha} = \underline{\beta}$ for some D unimodular matrix T;

(3) $|M(\underline{\alpha})| \neq 0$;

(4) $M(\underline{\alpha})'^{-1} = M(\underline{\beta})$ where $\underline{\beta}$ is an mbv for $\mathfrak{a}^{o}$ the complementary ideal $(\mathfrak{a}^{o} = \{\lambda \in G : \operatorname{tr} \lambda\mu \in D$ for all $\mu \in \mathfrak{a}\})$.

Proof.

(1) If $\lambda \in G$, then $\lambda\mathfrak{a}$ has mbv $\lambda\underline{\alpha}$.

(2) If $T\underline{\alpha} = \underline{\beta}$ where T is D unimodular, then $\beta_i \in \mathfrak{a}$. Thus $\mathfrak{b} = (\beta_1,\ldots,\beta_n) \subseteq \mathfrak{a}$. Since T^{-1} is a D matrix, considering $\underline{\alpha} = T^{-1}\underline{\beta}$ gives $\alpha_i \in \mathfrak{b}$ so $\mathfrak{a} \subseteq \mathfrak{b}$. Thus $\mathfrak{a} = \mathfrak{b}$. Conversely, if $\underline{\beta}$ is an mbv for $\mathfrak{a}$, $T\underline{\alpha} = \underline{\beta}$ and $S\underline{\beta} = \underline{\alpha}$ for D matrices T and S. Thus $ST = I$ so $|S|\cdot|T| = 1$. Since $|S|$, $|T| \in D$, they are D units.

(3) Clearly $\underline{\alpha}$ is an mbv for G over F. Since the extension is separable, $|M(\underline{\alpha})| \neq 0$.

(4) By the cofactor formula for inverses, the entries in the jth column of $M(\underline{\alpha})'^{-1}$ are symmetric functions in $\theta^{(1)},\ldots,\theta^{(j-1)}, \theta^{(j+1)},\ldots,\theta^{(n)}$. Thus they lie in $F(\theta^{(j)})$; in fact, if a_{ij} and a_{ik} are entries, they are conjugates lying in $F(\theta^{(j)})$ and $F(\theta^{(k)})$ respectively. This gives us $M(\underline{\alpha})'^{-1} = M(\underline{\beta})$ for some $\beta_i \in G$. It is clear that $\mathfrak{a}^{o}$ is an ideal since $\lambda,\eta \in \mathfrak{a}^{o}$ gives $\operatorname{tr}(\lambda + \eta)\mu \in D$ for all $\mu \in \mathfrak{a}$, and $\delta \in \Delta$ gives $\operatorname{tr}(\delta\lambda)\mu = \operatorname{tr} \lambda(\delta\mu) \in D$ for all

$\mu \in \mathfrak{a}$ since $\Delta\mathfrak{a} \subseteq \mathfrak{a}$. We have

$$\mathfrak{a}^{o} = \{\lambda \in G : \operatorname{tr} \lambda\mu \in D \text{ for all } \mu \in \mathfrak{a}\}$$
$$= \{\lambda \in G : \operatorname{tr} \lambda\alpha_i \in D \quad i = 1,2,\ldots,n\} \text{ since } \underline{\alpha} \text{ is an mbv}$$
$$= \{\lambda \in G : M(\underline{\alpha})\underline{m} = \underline{d} \text{ where } m_i = \lambda^{(i)} \text{ and } d_i \in D\}.$$

Now $M(\underline{\alpha})\underline{m} = \underline{d}$ if and only if $\underline{m}' = \underline{d}'\, M(\underline{\alpha})'^{-1} = \underline{d}'M(\underline{\beta})$. This is equivalent to $\lambda \in (\beta_1,\beta_2,\ldots,\beta_n)$. Thus $\underline{\beta}$ is an mbv for the M-ideal $\mathfrak{a}^{o}$.

We can now establish the basic link between M-ideals and Δ/D reps. The proof follows Taussky [16, 19] where the result is established for $D = Z$.

Theorem 1.5. For a given Δ and D there is a one-to-one correspondence between all classes of M-ideals and all classes of Δ/D reps. One such correspondence is given by $C(\mathfrak{a}) \longleftrightarrow C(A)$ where $A = M(\underline{\alpha})J(\theta)M(\underline{\alpha})^{-1}$, the matrix $J(\theta) = \operatorname{diag}(\theta^{(1)},\ldots,\theta^{(n)})$, and $\underline{\alpha}$ is an mbv for $\mathfrak{a}$. We shall use this correspondence throughout the thesis. If $C(\mathfrak{a})$ corresponds to $C(A)$, then $C(\mathfrak{a}^{o})$ corresponds to $C(A')$.

Proof. The equation $A = M(\underline{\alpha})J(\theta)M(\underline{\alpha})^{-1}$ is equivalent to $A\underline{\alpha}^{(i)} = \theta^{(i)}\underline{\alpha}^{(i)}$ for $i = 1,2,\ldots,n$. Thus A is an F matrix. Further, an $n \times n$ F matrix A is a G/F rep if and only if it has a root θ. Then $A\underline{\alpha} = \theta\underline{\alpha}$ for some $\underline{\alpha} \neq 0$ with $\alpha_j \in G$. Then $A\underline{\alpha}^{(i)} = \theta^{(i)}\underline{\alpha}^{(i)}$. Such a matrix A is a Δ/D rep if and only if $p(A)$ is a D matrix whenever $p(\theta) \in \Delta$ and p is an F polynomial.

Since $p(A)\underline{\alpha} = p(\theta)\underline{\alpha}$, it follows that A is a Δ/D rep if and only if $\underline{\alpha}$ is an mbv for the ideal $(\alpha_1,\ldots,\alpha_n)$.

It remains to show that the correspondence is a well defined mapping of classes in both directions. Since $M(\lambda\underline{\alpha}) = M(\underline{\alpha})J(\lambda)$ for $\lambda \in G$, we have $A = M(\lambda\underline{\alpha})J(\theta)M(\lambda\underline{\alpha})^{-1}$. Thus $\lambda\mathfrak{a}$ and $\mathfrak{a}$ give rise to the same Δ/D reps under the correspondence of the theorem. If α is one mbv for $\mathfrak{a}$, then by Theorem 1.4 (2), we have that β is another if and only if $T\underline{\alpha} = \underline{\beta}$ for some D unimodular T. Then $TAT^{-1} = M(\underline{\beta})J(\theta)M(\underline{\beta})^{-1}$ so that $C(\mathfrak{a}) \rightarrow C(A)$ is well defined. We now must show that $C(A) \rightarrow C(\mathfrak{a})$ is well defined. If T is a D unimodular matrix, $A = M(\underline{\alpha})J(\theta)M(\underline{\alpha})^{-1}$, and $TAT^{-1} = M(\underline{\beta})J(\theta)M(\underline{\beta})^{-1}$, then it suffices to show that $M(\underline{\beta}) = TM(\underline{\alpha})J(\lambda)$ for some $\lambda \in G$. Let $B = M(\underline{\beta})^{-1}TM(\underline{\alpha})$. Since $TM(\underline{\alpha})J(\theta)(TM(\underline{\alpha}))^{-1} = TAT^{-1} = M(\underline{\beta})J(\theta)M(\underline{\beta})^{-1}$, we have that B and $J(\theta)$ commute. Since $J(\theta)$ is diagonal and the conjugates of θ are distinct, B is diagonal. By Theorem 1.4 (4) there is a $\underline{\gamma}$ with components in G such that $M(\underline{\beta})^{-1} = M(\underline{\gamma})'$. Thus $b_{ii} = \Sigma_{j,k}\,(\gamma_j t_{jk}\alpha_k)^{(i)}$ and so $B = J(\lambda)$ for some $\lambda \in G$.

Finally we have $A' = M(\underline{\alpha})'^{-1}J(\theta)M(\underline{\alpha})' = M(\underline{\beta})J(\theta)M(\underline{\beta})^{-1}$ where $\underline{\beta}$ is an mbv for $\mathfrak{a}^{o}$ by Theorem 1.4 (4).

<u>Corollary 1.5.1</u>. There is a Δ/D rep if and only if there is an M-ideal of Δ over D.

Corollary 1.5.2. If $D = Z$ and Γ is the ring of algebraic integers in G, then there is a Δ/Z rep if and only if $\Delta \subseteq \Gamma$.

Proof. Suppose $\alpha \in \Delta$ and $\alpha \notin \Gamma$. Then α satisfies no monic Z polynomial. However, α satisfies the characteristic polynomial of its image under any Δ/Z rep. Thus no Δ/Z reps can exist if $\Delta \not\subseteq \Gamma$. Suppose $\Delta \subseteq \Gamma$. It suffices to consider the case $\Delta = \Gamma$ since the case $\Delta \subseteq \Gamma$ follows by restricting a Γ/Z rep. There are M-ideals of Γ over Z.

Corollary 1.5.3. If A is a Δ/D symrep and $B \in C(A)$, then $B' \in C(A)$.

Proof. Since $C(A) = C(B)$, we have $C(B') = C(A') = C(A)$.

II. SYMMETRIC REPRESENTATIONS IN GENERAL

One might hope that the most naïve conjecture is true: whenever $A' \in C(A)$ then $C(A)$ contains a Δ/D -symrep. This is false. A counterexample can easily be constructed as follows. Assume that the monic irreducible F polynomial for θ is a D polynomial. Let $\Delta = D[\theta]$. Since (1) is an M-ideal, Δ/D reps exist, and since $(1)^\circ \in C((1))$ by Lemma 2.1, the rep class corresponding to $C((1))$ contains its transposes by Theorem 1.5. If F is formally real and G is not totally real, Krakowski's condition [10], mentioned in the Introduction, assures us that no Δ/D symreps exist. Theorem 6.3 (2) enables us to construct examples in which Δ/D symreps exist and for $C(A)$ corresponding to $C((1))$ we have $A' \in C(A)$ but $C(A)$ has no symreps (see [18]).

One may then ask what conditions beyond $A' \in C(A)$ are needed. There seems to be no natural answer in terms of M-ideal classes unless D has further properties. One such property is that defined below.

Definition 2.1. We say that $S(G,D)$ holds if (a) if F is formally real, G is totally real and (b) for all W such that

(i) W is a symmetric $n \times n$ D unimodular matrix,

(ii) $|W|$ is a square in D,

(iii) W is positive definite if F is formally real, and

(iv) $W = TT'$ is solvable for an $n \times n$ matrix T over the algebraic closure of F, if F is of characteristic 2, we have that $W = TT'$ is solvable over D.

The following theorem gives some cases in which $S(G,D)$ holds. It will prove quite useful later.

Theorem 2.1. (1) $S(G,D)$ holds for finite D.

(2) $S(G,Z)$ holds for $n \leq 7$ and G totally real.

Proof. (1) Since D is a finite integral domain, $D = F$. Let W be as in the definition for $S(G,D)$. If F does not have characteristic 2, then $S(G,D)$ holds since the class of a quadratic form $x'Wx$ over F with $|W| \neq 0$ is determined by $|W| \cdot F^2$ and n [11, p. 157].

We assume that F has characteristic 2. If W is as in the definition for $S(G,D)$, we shall show that some $w_{ii} \neq 0$. Then two F transformations will be given which can be combined to put W in diagonal form over F. This will be sufficient since every element in a finite field of characteristic 2 is a square.

Let $W = TT'$ over the algebraic closure of F. If $S = T^{-1}$, then $I = SWS'$. Thus $1 = \Sigma_{i,j}\ s_{1i}w_{ij}s_{1j} = \Sigma_i\ s_{1i}^2 w_{ii} + \Sigma_{i<j}\ s_{1i}s_{1j}(w_{ij} + w_{ji}) = \Sigma_i\ s_{1i}^2 w_{ii}$ since $W = W'$. Thus some $w_{ii} \neq 0$.

We may suppose $w_{11} \neq 0$. Let $c_k = w_{1k}/w_{11}$ and

$$R = \begin{pmatrix} c_1 & 0 & & \\ \vdots & 1 & 0 & \\ \vdots & & \ddots & \\ c_n & 0 & & 1 \end{pmatrix} .$$

It is easily verified that $|R| = 1$ and $RWR' = w_{11}I_1 \oplus V$ where V is an $(n - 1) \times (n - 1)$ symmetric F matrix. We may repeat the above procedure on V. Eventually we arrive at the case $SWS' = A \oplus V$ where $A = \text{diag}(a_1,\ldots,a_k)$, S is an F matrix with $|S| = 1$ and (a) V is a symmetric F matrix with $v_{ii} = 0$ for all i or (b) V is of dimension zero. In the latter case the proof is complete. In the former case we shall exhibit an F transformation Q with $QSWS'Q' = A \oplus B$, $|Q| \neq 0$, and $b_{11} \neq 0$. We can then proceed as above using B. Since $|SWS'| \neq 0$, we have $|A| \neq 0$ and $|V| \neq 0$. Since all $v_{ii} = 0$, we may assume $v_{12} \neq 0$. Let E be the $\dim V \times \dim A$ matrix with $e_{21} = 1$ the only nonzero entry. Let

$$Q = \left(\begin{array}{c|c} I & E' \\ \hline VEA^{-1} & I \end{array} \right) .$$

Then since $A = A'$ and $V = V'$ and F has characteristic 2:

$$Q(A \oplus V)Q' = \left(\begin{array}{c|c} A + E'VE & E'V + E'V \\ \hline VE + VE & (VE)A^{-1}(VE)' + V \end{array} \right) = \left(\begin{array}{c|c} A & 0 \\ \hline 0 & B \end{array} \right) .$$

Then $(VE)_{ij} = \delta_{1j}v_{i2}$ gives $(VE)A^{-1}(VE)' = (a_{11}^{-1}v_{i2}v_{j2})$ so that $b_{11} \neq 0$. Expansion of $|Q|$ by minors using successively the $2^{nd}, 3^{rd}, \ldots, \dim A^{th}$ rows gives

$$|Q| = \left|\begin{array}{c|c} 1 & 0\ 1\ 0 \cdots 0 \\ \hline v_{12}/x_{11} & \\ v_{22}/x_{11} & I \\ \vdots & \end{array}\right| .$$

Expansion using successively the $2^{nd}, 4^{th}, 5^{th}, \ldots, \dim B + 1^{st}$ columns gives

$$|Q| = \begin{vmatrix} 1 & 1 \\ v_{22}/x_{11} & 1 \end{vmatrix} = \begin{vmatrix} 1 & 1 \\ 0 & 1 \end{vmatrix} = 1 ,$$

since the $v_{ii} = 0$ by assumption.

(2) This well known result in the theory of quadratic forms can be found in [12, p. 330].

The result of Krakowski mentioned in the Introduction indicates a fundamental difference between the formally real and not formally real cases. At times we shall make a statement such as "if G is totally real, λ is totally positive." In view of Krakowski's result, such a condition on λ would then apply whenever F is formally real and G/F symreps exist.

Many of the results in this thesis depend on being able to view the concept of symreps in terms of other ideas. The following theorem lists a variety of conditions which are equivalent to the existence of a symrep in a given class. The conditions can be found scattered in the literature [3,4,14,17], some implicitly, some explicitly, but not as general as in the theorem. By the inner product $(\underline{\alpha},\underline{\beta})$ we shall mean $\Sigma\alpha_i\beta_i$.

Theorem 2.2. Let A be a Δ/D rep with $C(A)$ corresponding to $C(\mathfrak{a})$. The following conditions are equivalent.

(1) $C(A)$ contains a Δ/D symrep.

(2) For every $B \in C(A)$ there is a D unimodular matrix T such that $T'TB = B'T'T$.

(3) There is an mbv $\underline{\alpha}$ for $\mathfrak{a}$ and a $\mu \in G$ such that $M(\underline{\alpha})'M(\underline{\alpha}) = J(\mu)$. A Δ/D symrep in $C(A)$ is $M(\underline{\alpha})J(\theta)M(\underline{\alpha})^{-1}$, further $\mathfrak{a} = \mu\,\mathfrak{a}^{\circ}$ and, if F is formally real, G is totally real and μ is totally positive.

(4) There is an mbv $\underline{\alpha}$ for $\mathfrak{a}$ and a $\lambda \in G$ such that $M(\underline{\alpha})J(\lambda)M(\underline{\alpha})' = I$. We may take $\lambda\mu = 1$ and $\underline{\alpha}$ as in (3).

(5) For some $\lambda \in G$ and every mbv $\underline{\beta}$ for $\mathfrak{a}$, there is a D unimodular matrix T such that $M(\underline{\beta})J(\lambda)M(\underline{\beta})' = TT'$.

We may replace "every" by "some" in (2) and (5).

Proof. (1) ⇒ (2). We may assume $A = A'$. If $TBT^{-1} = A$ where T is a D unimodular matrix, then $T'TB = T'AT = T'A'T = B'T'T$.

(2) ⇒ (1). If $T'TB = B'T'T$, let $E = TBT^{-1} = T'^{-1}B'T' = E'$.

(1) ⟺ (3). By Theorem 1.5, A has the form $M(\underline{\alpha})J(\theta)M(\underline{\alpha})^{-1}$, where $\underline{\alpha}$ is an mbv for $\mathfrak{a}$ and a characteristic vector for A. Since A has distinct roots $\theta^{(i)}$, its characteristic vectors are $\underline{\alpha}^{(i)}$ $(1 \leq i \leq n)$. Since a matrix with distinct characteristic roots is symmetric if and only if its characteristic vectors are orthogonal, we have $A = A'$ if and only if $M(\underline{\alpha})'M(\underline{\alpha}) = J((\underline{\alpha},\underline{\alpha})) = J(\mu)$. From $M(\underline{\alpha}) = M(\underline{\alpha})'^{-1}J(\mu)$ and Theorem 1.4 (4), we have $\mathfrak{a} = \mu\mathfrak{a}^{\circ}$. Since $\mu = \Sigma\alpha_i^2$, Krakowski's theorem completes the proof.

(3) ⟺ (4) Both statements are equivalent to $M(\underline{\alpha})^{-1} = J(\lambda)M(\underline{\alpha})'$.

(4) ⟺ (5) The mbv's for $\mathfrak{a}$ are related by $n \times n$ D unimodular matrices according to Theorem 1.4 (2). Hence if $M(\underline{\alpha})J(\lambda)M(\underline{\alpha})' = I$ and $\underline{\beta}$ is another mbv, then $\underline{\beta} = T\underline{\alpha}$ for some D unimodular T and $M(\underline{\beta})J(\lambda)M(\underline{\beta})' = TT'$. Conversely, if $M(\underline{\beta})J(\lambda)M(\underline{\beta})' = TT'$ we set $\underline{\alpha} = T^{-1}\underline{\beta}$.

The replacement of "every" by "some" follows from the proof of (2) ⇒ (1) and (5) ⇒ (4).

<u>Corollary 2.2.1</u>. (Generalizes a result of Faddeev [3].) If F does not have characteristic 2 and if A is a Δ/D rep with $C(A) \longleftrightarrow C(\mathfrak{a})$ and if $\underline{\alpha}$ is an mbv for $\mathfrak{a}$, then there is a Δ/D symrep in $C(A)$ if and only if there is a $\lambda \in G$ such that the quadratic form $\mathrm{tr}_{G/F}\lambda(\underline{x},\underline{\alpha})^2$, where $\underline{x}$ is an indeterminate, is

equivalent over D to a sum of n squares.

Proof. We may write the quadratic form condition as $\underline{x}'M(\underline{\alpha})J(\lambda)M(\underline{\alpha})'\underline{x} = \underline{y}'\underline{y}$ where $\underline{y} = T'\underline{x}$ and T is a D unimodular matrix. Hence $M(\underline{\alpha})J(\lambda)M(\underline{\alpha})' = TT'$ is equivalent to the quadratic form condition. Now apply (1) and (5) of the theorem.

Corollary 2.2.2. Assume that $S(G,D)$ holds and that A is a Δ/D rep with $C(A)$ corresponding to $C(\mathfrak{A})$. The following conditions are equivalent.

(1) $C(A)$ contains a Δ/D symrep.

(2) There is an mbv $\underline{\alpha}$ for $\mathfrak{A}$ and a $\lambda \in G$ which is totally positive if F is formally real such that $M(\underline{\alpha})J(\lambda)M(\underline{\alpha})'$ is a D matrix whose determinant is the square of a D unit.

Proof. (1) $\Rightarrow$ (2) Use parts (1), (5), and (3) of the theorem. (2) $\Rightarrow$ (1) We use Definition 2.1 with $W = M(\underline{\alpha})J(\lambda)M(\underline{\alpha})'$ and $T = M(\underline{\alpha})\sqrt{J(\lambda)}$. Suppose F is formally real, then T is over the real closure of F and $\underline{x}'W\underline{x} = (T'\underline{x}, T'\underline{x}) > 0$ if $\underline{x} \neq \underline{0}$.

Corollary 2.2.3. If $S(G,D)$ holds and every D unit (totally positive D unit if F is formally real) is a square in D, then there is a Δ/D symrep whose class corresponds to $C(\mathfrak{A})$ if and only if $\mathfrak{A}^{\circ} = \lambda\mathfrak{A}$ for some $\lambda \in G$ (with G totally real and λ totally positive if F is formally real).

Proof. In matrix notation $\mathfrak{a}^{\circ} = \lambda \mathfrak{a}$ gives $TM(\underline{\alpha})'^{-1} = M(\underline{\alpha})J(\lambda)$ where $\underline{\alpha}$ is an mbv for $\mathfrak{a}$ and T is a D unimodular matrix. This is $T = M(\underline{\alpha})J(\lambda)M(\underline{\alpha})'$. Use the previous corollary.

Corollary 2.2.4. (Generalizes a theorem of Gorshkov [4].) There is a G/F symrep if and only if for some $\alpha_1,\ldots,\alpha_n \in G$ we have $(\underline{\alpha}^{(i)},\underline{\alpha}^{(j)}) = 0$ for $i \neq j$ and $(\underline{\alpha},\underline{\alpha}) \neq 0$. If F is formally real, $(\underline{\alpha},\underline{\alpha}) \neq 0$ may be weakened to $\underline{\alpha} \neq \underline{0}$.

Proof. The first part follows from (1) and (3) in the theorem. To prove the weakened form it suffices to show that G is formally real. Suppose G is not formally real. Let R be a real closure of F such that $R(i)$ contains G. Since R does not contain G, we cannot have $\Theta \in R$. Thus $\bar{\Theta} \neq \Theta$ where $^{-}$ denotes conjugate in $R(i)$ over R. Since $F \subseteq R$ we have that Θ and $\bar{\Theta}$ are conjugate over F. By assumption $(\bar{\underline{\alpha}},\underline{\alpha}) = 0$. Thus $\underline{\alpha} = \underline{0}$.

We have been dealing exclusively with a field extension of F; however, similar problems exist when $\mathfrak{G}$ is an algebra over F. When $\mathfrak{G}$ is a direct sum of fields, we can work componentwise to some extent. Let $p(x)$ be an F polynomial with distinct roots and let $\mathfrak{G} = F[x]/(p(x))$. Then $\mathfrak{G}$ is a direct sum of fields. Using this Sapiro [14, Lemma 1.1] has generalized Corollary 2.2.1 when $D = F$. Latimer and MacDuffee [11] have established the equivalent of Theorem 1.5 when $D = Z$.

The next theorem deals with the existence of symreps corresponding to the principal ideal class.

Lemma 2.1. If $\Delta = D[\theta]$ and θ satisfies a monic F irreducible D polynomial f, then $(1) = f'(\theta)(1)^\circ$.

Proof. Let $X = (x_j^{i-1})$. Then $|X|$ is a vander Monde determinant and will be written $\mathrm{vdm}(x_1,\ldots,x_n)$. We wish to consider X'^{-1}. Notice that the cofactor X_{i1} vanishes whenever $x_k = x_m$ and $k \neq m$ and $k,m \neq 1$. Thus $\mathrm{vdm}(x_2,\ldots,x_n)$ divides X_{i1}. Since $X_{n1} = \pm\, \mathrm{vdm}(x_2,\ldots,x_n)$ we have that X_{n1} divides X_{i1}. Now let $x_j = \theta^{(j)}$. By Theorem 1.4 (4) we have that
$(1)^\circ = (\mathrm{vdm}(\theta^{(2)},\ldots,\theta^{(n)})/\mathrm{vdm}(\theta^{(1)},\ldots,\theta^{(n)})) = (1/f'(\theta))$.

Theorem 2.3. Assume $\Delta = D[\theta]$. If $C((1))$ corresponds to a class with a Δ/D symrep, then there is a Δ unit η with $(-1)^{n(n-1)/2}N\eta$ a square in D and, if F is formally real, G is totally real and $f'(\theta)\eta$ totally positive where f is the monic irreducible F polynomial for θ. If $S(G,D)$ holds, the converse is true.

Proof. By Theorem 2.2 (3) and the previous lemma we have $(1) = \mu(1)^\circ = (\mu/f'(\theta))$ for a $\mu \in G$ with G totally real and μ totally positive if F is formally real. Write $\mu = \eta f'(\theta)$. By Theorem 2.2 (5) we have $M(\underline{\alpha})J(\mu^{-1})M(\underline{\alpha})' = TT'$ for some D unimodular T with $\underline{\alpha} = (1,\theta,\ldots,\theta^{n-1})'$. Thus

$$|T|^2 = |M(\underline{\alpha})|^2/N\mu = (-1)^{n(n-1)/2}N(f'(\theta)/\mu) = (-1)^{n(n-1)/2}/N\eta.$$

We must show that η is a Δ unit. Since $(1) = (\mu/f'(\theta)) = \eta(1)$ we have that η and η^{-1} lie in $(1) = \Delta$.

Suppose $S(G,D)$ holds. Let $\lambda^{-1} = \eta f'(\theta)$. We may use Corollary 2.2.2 since $|M(\underline{\alpha})|^2 \cdot |J(\lambda)| = (-1)^{n(n-1)/2}/N\eta$, a square in D, and $\lambda(1) = (1)^\circ$ whence $M(\underline{\alpha})\ J(\lambda) = T\ M(\underline{\alpha})'^{-1}$ for a D unimodular matrix T by Theorem 1.4 (2) and (4).

Corollary 2.3.1. (See [20, Theorem 3] for a more general result.) If $n \equiv 2 \pmod 4$ and a G/F symrep exists, there is an $\eta \in G$ and a $k \in F$ such that $-1 = k^2 N\eta$.

Proof. We have $G = F[\theta]$. Take η as in the theorem.

If we consider other values of n, the result is trivial: for odd n, we replace -1 by $(-1)^{(n-1)/2}$ and let $k = 1$ and $\eta = (-1)^{(n-1)/2}$; for $n \equiv 0(4)$, we replace -1 by $+1$ and let $k = \eta = 1$.

The following result gives a method for finding all G/F symreps when $n = 2$. For general n we cannot do this.

Theorem 2.4. Let $n = 2$. If the characteristic of F is not 2, then we may assume that $G = F(\sqrt{c}\ )$ for some $c \in F$. There are G/F symreps if and only if c is the sum of two squares in F. All G/F symreps then have the form

$$\begin{pmatrix} -u & v \\ v & u \end{pmatrix} \longleftrightarrow \sqrt{c} \quad \text{where} \quad c = u^2 + v^2 .$$

If F has characteristic 2 and $\theta^2 + a\theta + b = 0$, where $a,b \in F$, then there is a G/F symrep if and only if $a \neq 0$. All G/F symreps then have the form

$$\begin{pmatrix} (v^2 + b)/a & v + (v^2 + b)/a \\ v + (v^2 + b)/a & a + (v^2 + b)/a \end{pmatrix} \longleftrightarrow \theta \quad \text{where } v \in F \text{ is arbitrary} .$$

Proof. Assume the characteristic of F is not 2. Let $A \longleftrightarrow \sqrt{c}$. Then $|A - \lambda I| = \lambda^2 - \mathrm{tr}A\cdot\lambda + |A|$. By Lemma 1.2, $A^2 - cI = 0$. Thus $a_{11} = -a_{22}$. Put $u = a_{22} = -a_{11}$ and $v = a_{12} = a_{21}$. Then $c = u^2 + v^2$. Now assume F has characteristic 2. If $a = 0$, we may apply the above analysis and conclude that if there are G/F symreps then $b = u^2 + v^2$. But then $\theta = \sqrt{b} = u + v \in F$, a contradiction. Let $A \longleftrightarrow \theta$. As in the above case, $\mathrm{tr}A = \mathrm{tr}\theta = a$ and $|A| = -N\theta = b$. Thus we have the equations $a_{11} + a_{22} = a$ and $a_{11}a_{22} + a_{21}a_{12} = b$ and $a_{12} = a_{21}$. Let $a_{11} = u$ and $a_{12} = u + v$. Then $a_{22} = u + a$ and $u(u + a) + (u + v)^2 = b$ so that $u = (b + v^2)/a$ since $a \neq 0$.

The remainder of this section is devoted to structure properties rather than existence questions. The next theorem bounds the number of symreps in a given class. We begin by defining a concept which is necessary here and in the study of conjugators in Section VI.

Definition 2.2. Let $A = \Phi(\Theta)$ be a Δ/D rep which has been extended to a G/F rep. Let $\mathfrak{R}(A)$ be the inverse image of the set of D matrices in $\Phi(G)$. In other words, $\mathfrak{R}(A)$ is the largest subset of G for which A is an $\mathfrak{R}(A)/D$ rep.

Lemma 2.2. $\mathfrak{R}(A)$ is an integral domain containing Δ. If $C(\mathfrak{a})$ corresponds to $C(A)$, then $\mathfrak{R}(A) = (\mathfrak{a}:\mathfrak{a})$ where $(\mathfrak{a}:\mathfrak{b}) = \{\lambda \in G : \lambda\mathfrak{b} \subseteq \mathfrak{a}\}$. If $B \in C(A)$, then $\mathfrak{R}(A) = \mathfrak{R}(B)$.

Proof. Clearly $\mathfrak{R}(A)$ contains Δ and is a subring of G. Observe that $(\mathfrak{a}:\mathfrak{a})$ is a class invariant. By Theorem 1.5, we may choose $\underline{\alpha}$ to be a characteristic vector for A and an mbv for $\mathfrak{a}$. Then $(\mathfrak{a}:\mathfrak{a}) = \{\lambda \in G : \lambda\alpha_i \in \mathfrak{a}$ for $1 \leq i \leq n\} = \{\lambda \in G : \lambda\underline{\alpha} = T\underline{\alpha}$ for some D matrix $T\}$. Since $\Theta\underline{\alpha} = A\underline{\alpha}$, we have $\Phi(\lambda) = T$ where Φ is the rep corresponding to A. Hence $(\mathfrak{a}:\mathfrak{a}) = \{\lambda \in G : \Phi(\lambda)$ is a D matrix$\} = \mathfrak{R}(A)$. Since $\mathfrak{R}(A) = (\mathfrak{a}:\mathfrak{a})$ it is clear that $B \in C(A)$ implies $\mathfrak{R}(A) = \mathfrak{R}(B)$.

We shall make a brief observation before proceeding to the theorem. The correspondence between rep classes and M-ideal classes depends on characteristic vectors and mbv's. However, all equivalent matrices arise through D unimodular transformations of one characteristic vector and all equivalent M-ideals arise through multiples over G of one mbv. Hence all equivalent M-ideals are generated by taking the characteristic vectors of a fixed rep and all equivalent reps by taking all bases of a fixed M-ideal. The proof of the theorem takes a fixed M-ideal and studies the set of bases giving symreps after partitioning it in a suitable fashion.

Theorem 2.5. Let A be a Δ/D symrep, $\mathfrak{U}^+$ the group of those units in $\mathfrak{R}(A)$ which (1) have norms that are squares in D and (2) are totally positive if F is formally real. Let $\mathfrak{U}^2$ be the subgroup consisting of the squares of the units in $\mathfrak{R}(A)$. If $O_n(D)$ is the (possibly infinite) group of D unimodular $n \times n$ matrices T such that $TT' = I_n$, let $g = |O_n(D)|$ if F has characteristic 2 and let $g = |O_n(D)|/2$ otherwise. Then the number of Δ/D symreps in $C(A)$ is a multiple of g and is bounded above by $g \cdot [\mathfrak{U}^+ : \mathfrak{U}^2]$. If $S(G,D)$ holds, the bound is actually equal to the number of Δ/D symreps in $C(A)$.

Proof. Fix an $\mathfrak{a}$ such that $C(A)$ corresponds to $C(\mathfrak{a})$. By the remark preceding the theorm it suffices to study the mbv's of $\mathfrak{a}$. With each $\mu \in G$ we may associate the (possibly empty) set $\mathfrak{m}(\mu) = \{$mbv's $\underline{\alpha}$ for $\mathfrak{a}$: $M(\underline{\alpha})'\, M(\underline{\alpha}) = J(\mu)\}$. By the proof of (1) $\Longleftrightarrow$ (3) in Theorem 2.2, it is clear that $\underline{\alpha} \rightarrow M(\underline{\alpha})\, J(\theta)\, M(\underline{\alpha})^{-1}$ maps elements of $\bigcup \mathfrak{m}(\mu)$ $(0 \neq \mu \in G)$ onto the Δ/D symreps in $C(A)$. Define the function $f(\mu) = \{M(\underline{\alpha})\, J(\theta)\, M(\underline{\alpha})^{-1} : \underline{\alpha} \in \mathfrak{m}(\mu)\}$. Let $x = \mu_0$ be a solution of $A \in f(x)$. We will show

(1) $f(\mu) \cap f(\lambda)$ is nonempty if and only if $\mu \in \lambda\mathfrak{U}^2$,

(2) $f(\mu)$ and $f(\lambda)$ are equal or disjoint,

(3) $|f(\mu)| = 0$ or g,

(4) if $\mathfrak{m}(\mu)$ is nonempty, then $\mu \in \mu_0 \mathfrak{U}^+$; if $S(G,D)$ holds, the converse is true.

The theorem easily follows from these four results.

(1). Assume $\underline{\alpha} \in \mathfrak{m}(\mu)$ and $\underline{\beta} \in \mathfrak{m}(\lambda)$ and $M(\underline{\alpha})\ J(\theta)\ M(\underline{\alpha})^{-1} = M(\underline{\beta})\ J(\theta)\ M(\underline{\beta})^{-1} = B$. By Theorem 1.4 (2) there is a D unimodular matrix T such that $\underline{\alpha} = T\underline{\beta}$. Since $TB = BT$ and B is an F matrix with distinct characteristic roots, $T = p(B)$ where p is some F polynomial. Let $\eta = p(\theta)$. Since T is D unimodular, η is a unit in $\mathfrak{R}(A)$. Since $BM(\underline{\beta}) = M(\underline{\beta})\ J(\theta)$, we have $TM(\underline{\beta}) = M(\underline{\beta})\ J(\eta)$. Thus

$$\begin{aligned} J(\mu) &= M(\underline{\alpha})'\ M(\underline{\alpha}) = (TM(\underline{\beta}))'\ (TM(\underline{\beta})) \\ &= (M(\underline{\beta})\ J(\eta))'\ (M(\underline{\beta})\ J(\eta)) = J(\eta)\ M(\underline{\beta})'\ M(\underline{\beta})\ J(\eta) \\ &= J(\eta)\ J(\lambda)\ J(\eta) \\ &= J(\lambda\eta^2)\ . \end{aligned}$$

Conversely, if $\mu \in \lambda\mathfrak{U}^2$ we may write $\mu = \lambda\eta^2$ where η is a unit in $\mathfrak{R}(A)$. Let $\underline{\beta} \in \mathfrak{m}(\lambda)$ and T correspond to η under the Δ/D symrep $B = M(\underline{\beta})\ J(\theta)\ M(\underline{\beta})^{-1}$. Then T is D unimodular and $\underline{\alpha} = T\underline{\beta}$ satisfies

(i) $\underline{\alpha}$ is an mbv,

(ii) $M(\underline{\alpha})'\ M(\underline{\alpha}) = (TM(\underline{\beta}))'\ (TM(\underline{\beta})) = (M(\underline{\beta})\ J(\eta))'\ (M(\underline{\beta})\ J(\eta)) =$
$J(\eta\lambda\eta) = J(\mu)$, and

(iii)
$$\begin{aligned} M(\underline{\alpha})\ J(\theta)\ M(\underline{\alpha})^{-1} &= TM(\underline{\beta})\ J(\theta)\ M(\underline{\alpha})^{-1} \\ &= M(\underline{\beta})\ J(\eta)\ J(\theta)\ M(\underline{\alpha})^{-1} \\ &= M(\underline{\beta})\ J(\theta)\ (M(\underline{\alpha})\ J(\eta)^{-1})^{-1} \\ &= M(\underline{\beta})\ J(\theta)\ M(\underline{\beta})^{-1}\ . \end{aligned}$$

(2). If $f(\lambda)$ and $f(\mu)$ are not disjoint, then $\mu \in \lambda\mathcal{U}^2$. In the second half of the proof of (1) we constructed for <u>any</u> $\underline{\beta} \in \mathfrak{m}(\lambda)$ an $\underline{\alpha} \in \mathfrak{m}(\mu)$ such that $M(\underline{\alpha})\ J(\theta)\ M(\underline{\alpha})^{-1} = M(\underline{\beta})\ J(\theta)\ M(\underline{\beta})^{-1}$. Hence $f(\lambda) \subseteq f(\mu)$. By symmetry $f(\mu) \subseteq f(\lambda)$.

(3). Let $\underline{\alpha} \in \mathfrak{m}(\mu)$ and let T be a D unimodular matrix. Then $T\underline{\alpha} \in \mathfrak{m}(\mu)$ if and only if $(TM(\underline{\alpha}))'\ (TM(\underline{\alpha})) = J(\mu) = M(\underline{\alpha})'\ M(\underline{\alpha})$. Hence, for a D matrix T, the equation $TT' = I_n$ is equivalent to $T\underline{\alpha} \in \mathfrak{m}(\mu)$. Since $\underline{\alpha}$ is an mbv, $T\underline{\alpha} = S\underline{\alpha}$ if and only if $T = S$. Thus we have that $|\mathfrak{m}(\lambda)| = |O_n(D)|$. Suppose that $\underline{\alpha},\underline{\beta} \in \mathfrak{m}(\mu)$ yield the same symrep under the correspondence of Theorem 1.5. By the first part of the proof of (1) we see that $\underline{\beta} = T\underline{\alpha}$ and $\eta^2\mu = \mu$ where η is the preimage of T under the symrep corresponding to $\underline{\alpha}$ and $\underline{\beta}$. Thus $\eta = \pm 1$ and so $T = \pm I_n$. When F has characteristic 2 we have $I_n = -I_n$. Thus $|f(\mu)| = g$.

(4). Let $\mathfrak{M}(\mu)$ be nonempty. Then $\mu^{-1}\mathfrak{a} = \mathfrak{a}^{o} = \mu_0^{-1}\mathfrak{a}$ by Theorem 2.2 (3). Thus $(\mu/\mu_0)\mathfrak{a} = \mathfrak{a}$ and so μ/μ_0 is a unit of $(\mathfrak{a} : \mathfrak{a}) = \mathfrak{R}(A)$. If G is totally real, μ and μ_0 are totally positive since they are sums of squares in $F(\theta^{(1)}, \dots, \theta^{(n)})$. Furthermore, if $\underline{\alpha} \in \mathfrak{M}(\mu)$ and $\underline{\beta} \in \mathfrak{M}(\mu_0)$, there is a D matrix T such that $\underline{\alpha} = T\underline{\beta}$ and then

$$\frac{N\mu}{N\mu_0} = \frac{|M(\underline{\alpha})'\ M(\underline{\alpha})|}{|M(\underline{\beta})'\ M(\underline{\beta})|} = |T|^2 .$$

Hence $\mu \in \mu_0\mathcal{U}^+$.

Now suppose $S(G,D)$ holds and $\mu \in \mu_0\mathcal{U}^+$. Let $\underline{\alpha} \in \mathfrak{M}(\mu_0)$ and let $W = M(\underline{\alpha})\ J(\mu^{-1})\ M(\underline{\alpha})'$. Then

(i) W is a D unimodular matrix since μ_0/μ corresponds to a D unimodular matrix T under the rep $M(\underline{\alpha})\ J(\theta)\ M(\underline{\alpha})^{-1}$ and then $W = M(\underline{\alpha})\ J(\mu_0/\mu)\ J(\mu_0^{-1})\ M(\underline{\alpha})' =$ $TM(\underline{\alpha})\ J(\mu_0^{-1})\ M(\underline{\alpha})' = T$;

(ii) $|W| = |T| = N(\mu_0/\mu)$ which is a square in D;

(iii) if G is totally real, then W is positive definite since μ is totally positive and $\underline{x}'W\underline{x} = (V'\underline{x}, V'\underline{x}) > 0$ when $\underline{x} \neq \underline{0}$ where $V = M(\underline{\alpha})\sqrt{J(\mu^{-1})}$ lies over the real closure of G;

(iv) $W = VV'$ where V is as in (iii).

By $S(G,D)$, there is a D unimodular matrix U such that $M(\underline{\alpha})\, J(\mu^{-1})\, M(\underline{\alpha})' = UU'$. Let $\underline{\beta} = U^{-1}\underline{\alpha}$. Then $\underline{\beta}$ is an mbv for $\mathfrak{a}$ and $M(\underline{\beta})'\, M(\underline{\beta}) = J(\mu)$.

Corollary 2.5.1. If $x^2 + y^2 = 1$ has infinitely many solutions in D or $n \geq 4$ and $x^2 + y^2 + u^2 + v^2 = 1$ has infinitely many solutions in D, then every Δ/D rep class has no symreps or infinitely many.

Proof. Since

$$\begin{pmatrix} x & y \\ -y & x \end{pmatrix} \oplus I_{n-2} \quad \text{or} \quad \begin{vmatrix} x & y & u & v \\ y & -x & v & -u \\ u & -v & -x & y \\ v & u & -y & -x \end{vmatrix} \oplus I_{n-4}$$

lies in $O_n(D)$, we have $g = \infty$.

The previous theorem studies the number of symreps in a given class. In the next theorem we shall establish some results on the different classes of symreps. We actually study a set of ideal classes under the assumption that inverses exist. A group operation is introduced with identity $C(\mathfrak{h})$ where $\mathfrak{h}$ is somewhat arbitrary. The arbitrariness of $\mathfrak{h}$ is useful in Corollary 2.6.2. These results prove useful in studying the case $D = Z$. These results do not depend on the existence of M-ideals.

Lemma 2.3. Let $\mathfrak{a}$ and $\mathfrak{b}$ be ideals in Δ which have inverses. Then

(1) $(\mathfrak{a}\mathfrak{b})^\circ = \mathfrak{a}^\circ\mathfrak{b}^{-1} = \mathfrak{a}^{-1}\mathfrak{b}^\circ$ and so $\mathfrak{a}\mathfrak{a}^\circ = \mathfrak{b}\mathfrak{b}^\circ$ and $(\mathfrak{a}\mathfrak{b}^{-1})^{-1} = \mathfrak{a}^\circ(\mathfrak{b}^\circ)^{-1}$;

(2) if $\mathfrak{c} \in C(\mathfrak{a})$ and $\mathfrak{a}^\circ = \alpha\mathfrak{a}$, then for some $\tau \in G$ we have $\mathfrak{c}^\circ = \tau\alpha\mathfrak{c}$ and if G is totally real we may take τ to be totally positive.

Proof. Recall that $\mathfrak{c}^\circ = \{\lambda \in G : \mathrm{tr}\,\lambda\gamma \in D \text{ for all } \gamma \in \mathfrak{c}\}$. Thus

$$\begin{aligned}(\mathfrak{a}\mathfrak{b})^\circ\mathfrak{b} &= (\beta\lambda : \beta \in \mathfrak{b} \text{ and } \lambda \in G \text{ and } \mathrm{tr}(\Sigma\alpha_i\beta_i\lambda) \in D \\ &\qquad\qquad \text{for all } \alpha_i \in \mathfrak{a} \text{ and } \beta_i \in \mathfrak{b}) \\ &\subseteq (\beta\lambda : \lambda \in G \text{ and } \mathrm{tr}\,\alpha\beta\lambda \in D \text{ for all } \alpha \in \mathfrak{a}) \\ &= (\mu : \mu \in G \text{ and } \mathrm{tr}\,\alpha\mu \in D \text{ for all } \alpha \in \mathfrak{a}) = \mathfrak{a}^\circ.\end{aligned}$$

Furthermore $\mathfrak{a}^\circ\mathfrak{b}^{-1} = (\mathfrak{a}\mathfrak{b}\mathfrak{b}^{-1})^\circ\mathfrak{b}^{-1} \subseteq (\mathfrak{a}\mathfrak{b})^\circ$ by the above. Hence (1) is true. To prove (2) let $\mathfrak{a} = \lambda\mathfrak{c}$ and $\tau = \lambda^2$. Then $\tau\alpha\mathfrak{c} = \lambda\alpha\mathfrak{a} = \lambda\mathfrak{a}^\circ = (\lambda^{-1}\mathfrak{a})^\circ = \mathfrak{c}^\circ$ by (1).

Theorem 2.6. Assume that whenever $\mathfrak{a}$ is an ideal in Δ with $\mathfrak{a}^\circ \sim \mathfrak{a}$, then $\mathfrak{a}^{-1}$ exists. Fix an $\mathfrak{n}$ such that $\mathfrak{n} \sim \mathfrak{n}^\circ$. Let

(1) $\mathfrak{J} = \{C(\mathfrak{a}) : \mathfrak{a} \sim \mathfrak{a}^\circ\}$ and

(2) $C(\mathfrak{a}) \circ C(\mathfrak{b}) = C(\mathfrak{a}\mathfrak{b}\mathfrak{n}^{-1})$.

The operation "$\circ$" makes $\mathfrak{J}$ into an abelian group of exponent 2 in the semigroup of all ideal classes of Δ under "$\circ$". If the ideal classes of Δ form a group under ordinary product, they do so under "$\circ$". If G is totally real, define

$\mathfrak{P} = \{C(\mathfrak{a}) : \mathfrak{a}^\circ = \tau\mathfrak{a}$ for some totally positive $\tau \in G\}$ (by Lemma 2.3 (2), if $\mathfrak{b} \in C(\mathfrak{a}) \in \mathfrak{P}$, then $\mathfrak{b}^\circ = \sigma\mathfrak{b}$ for some totally positive σ). If $\mathfrak{P}$ is nonempty let

(1) $\mathfrak{S}$ be a maximal subset of $\{\mathfrak{a} : \mathfrak{a}^2 \sim (1)\}$ such that $\mathfrak{a}, \mathfrak{b} \in \mathfrak{S}$ and $\mathfrak{a}^2 = \tau\mathfrak{b}^2$ for some totally positive $\tau \in G$ implies $\mathfrak{a} = \mathfrak{b}$,

(2) $C(\mathfrak{a})\,\mathfrak{P} = \{C(\mathfrak{a}\mathfrak{b}) : C(\mathfrak{b}) \in \mathfrak{P}\}$.

Then $\mathfrak{J} = \bigcup_{\mathfrak{a} \in \mathfrak{S}} C(\mathfrak{a})\,\mathfrak{P}$ where the components are disjoint, the square under "$\circ$" of any component lies in that component containing $C(\mathfrak{n})$, and this component is a subgroup of $\mathfrak{J}$.

Proof. The group properties are easily proved:

(i) associativity by ordinary ideal class product associativity

(ii) closure follows since if $C(\mathfrak{a}), C(\mathfrak{b}) \in \mathfrak{J}$, we have

$\mathfrak{a} \sim \mathfrak{a}^\circ$ and $\mathfrak{b} \sim \mathfrak{b}^\circ$ and

$$\begin{aligned}(\mathfrak{a}\,\mathfrak{b}\mathfrak{n}^{-1})^\circ &= \mathfrak{a}^\circ(\mathfrak{b}\mathfrak{n}^{-1})^{-1} \quad \text{by Lemma 2.3 (1)}\\ &= \mathfrak{a}^\circ(\mathfrak{b}^\circ(\mathfrak{n}^\circ)^{-1}) \quad \text{by Lemma 2.3 (1)}\\ &\sim \mathfrak{a}(\mathfrak{b}\mathfrak{n}^{-1}).\end{aligned}$$

(iii) identity - clearly $C(\mathfrak{n})$ works

(iv) inverse - $C(\mathfrak{a}^{-1}\mathfrak{n}^2) \circ C(\mathfrak{a}) = C(\mathfrak{n})$

(v) abelian - clear

(vi) exponent - $C(\mathfrak{a}) \circ C(\mathfrak{a}) = C(\mathfrak{a}^2\mathfrak{n}^{-1})$ and $\mathfrak{a}^2\mathfrak{n}^{-1} \sim (\mathfrak{a}\mathfrak{a}^\circ)\mathfrak{n}^{-1} = (\mathfrak{n}\mathfrak{n}^\circ)\mathfrak{n}^{-1} = \mathfrak{n}^\circ \sim \mathfrak{n}$ (by Lemma 2.3 (1)).

We now assume that G is totally real and $\mathcal{P}$ is nonempty. Let us show that the components are disjoint. Suppose $\mathfrak{a}_1, \mathfrak{a}_2 \in \mathfrak{S}$ and $C(\mathfrak{b}_1)$, $C(\mathfrak{b}_2) \in \mathcal{P}$ and $C(\mathfrak{a}_1\mathfrak{b}_1) = C(\mathfrak{a}_2\mathfrak{b}_2)$. Let $\beta_1, \beta_2 \in G$ be totally positive and $\mathfrak{b}_i^\circ = \beta_i \mathfrak{b}_i$. Choose ε so that $\mathfrak{n} = \varepsilon\mathfrak{n}^\circ$. Then by assumption and by (vi) we have $(\mathfrak{a}_1\mathfrak{b}_1)(\mathfrak{a}_2\mathfrak{b}_2)\mathfrak{n}^{-1} \sim (\mathfrak{a}_1\mathfrak{b}_1)^2\mathfrak{n}^{-1} \sim \mathfrak{n}$ whence $\mathfrak{a}_1^2\mathfrak{a}_2^2\,\mathfrak{b}_1^2\,\mathfrak{b}_2^2 = (\lambda\mathfrak{n}^2)^2$ for some $\lambda \in G$. However

$$\mathfrak{n}^4 = \varepsilon^2(\mathfrak{n}\mathfrak{n}^\circ)^2 = \varepsilon^2(\mathfrak{b}_1\mathfrak{b}_1^\circ)\,(\mathfrak{b}_2\mathfrak{b}_2^\circ) \text{ by Lemma 2.3 (1)}$$
$$= \varepsilon^2\beta_1\beta_2\,\mathfrak{b}_1^2\mathfrak{b}_2^2.$$

Thus $\mathfrak{a}_1^2\mathfrak{a}_2^2 = \beta_1\beta_2(\lambda\varepsilon)^2$, a totally positive element of G. By the definition of $\mathfrak{S}$ we have $\mathfrak{a}_1 = \mathfrak{a}_2$. Hence $C(\mathfrak{b}_1) = C(\mathfrak{b}_2)$.

The union is contained in $\mathfrak{J}$ since if $C(\mathfrak{b}) \in \mathcal{P}$ and $\mathfrak{a} \in \mathfrak{S}$ we have $(\mathfrak{a}\mathfrak{b})^\circ = \mathfrak{a}^{-1}\mathfrak{b}^\circ \sim \mathfrak{a}^{-1}\mathfrak{b} \sim \mathfrak{a}\mathfrak{b}$. The reverse inclusion is more complicated. We first show that if $\mathfrak{b}^\circ = \beta\mathfrak{b}$, then $\mathfrak{a}^2 = (\beta\tau)$ for some $\mathfrak{a} \in \mathfrak{S}$ and some totally positive τ. Let $C(\mathfrak{c}) \in \mathcal{P}$ and $\mathfrak{c}^\circ = \gamma\mathfrak{c}$ where γ is totally positive. Then $(\mathfrak{b}\mathfrak{c}^{-1})^2 = (\gamma/\beta)(\mathfrak{b}\mathfrak{b}^\circ)/(\mathfrak{c}\mathfrak{c}^\circ) = (\gamma/\beta)$ by Lemma 2.3 (1). By the definition of $\mathfrak{S}$, we have $\mathfrak{a} \in \mathfrak{S}$ with $\mathfrak{a}^2 = (\beta\tau)$ for some totally positive τ. Now $C(\mathfrak{b}\mathfrak{a}^{-1}) \in \mathcal{P}$ since $(\mathfrak{b}\mathfrak{a}^{-1})^\circ = \mathfrak{b}^\circ\mathfrak{a} = \beta^2\tau\,\mathfrak{b}\mathfrak{a}^{-1}$. Thus $C(\mathfrak{b}) = C(\mathfrak{a})\,C(\mathfrak{b}\mathfrak{a}^{-1})$ is in the union.

We now suppose that $\mathfrak{a} \in \mathfrak{S}$ is such that $C(\mathfrak{n}) \in C(\mathfrak{a})\,\mathcal{P}$. Let $C(\mathfrak{b}_1)$, $C(\mathfrak{b}_2) \in \mathcal{P}$ and $\mathfrak{a}' \in \mathfrak{S}$. We must show that $C(\mathfrak{a}'\mathfrak{b}_1) \circ C(\mathfrak{a}'\mathfrak{b}_2) \in C(\mathfrak{a})\mathcal{P}$. Thus we must show that $(C(\mathfrak{a}'\mathfrak{b}_1) \circ C(\mathfrak{a}'\mathfrak{b}_2))\,C(\mathfrak{a}^{-1}) \in \mathcal{P}$. Let $\mathfrak{n} = \mathfrak{a}\mathfrak{b}_3$ where

$C(\mathfrak{b}_3) \in \mathcal{P}$. Choose β_i totally positive so that $\beta_i \mathfrak{b}_i = \mathfrak{b}_i^\circ$ for $i = 1,2,3$. Let $\mathfrak{a}^2 = (\alpha)$ and $\mathfrak{a}'^2 = (\alpha')$. We have $(C(\mathfrak{a}'\mathfrak{b}_1) \circ C(\mathfrak{a}'\mathfrak{b}_2))\, C(\mathfrak{a}^{-1}) = C(\alpha'\mathfrak{b}_1\mathfrak{b}_2\mathfrak{b}_3^{-1}/\alpha)$ and

$$\begin{aligned}
(\mathfrak{b}_1\mathfrak{b}_2\mathfrak{b}_3^{-1})^\circ &= \mathfrak{b}_1^\circ \mathfrak{b}_2^{-1}\mathfrak{b}_3 && \text{by Lemma 2.3 (1)} \\
&= \mathfrak{b}_1^\circ\,(\mathfrak{b}_2^\circ(\mathfrak{b}_3^\circ)^{-1}) && \text{by Lemma 2.3 (1)} \\
&= \beta_1\beta_2\beta_3^{-1}(\mathfrak{b}_1\mathfrak{b}_2\mathfrak{b}_3^{-1}) && \text{and the } \beta_i\text{'s are totally positive by assumption.}
\end{aligned}$$

Clearly $C(\mathfrak{a})\,\mathcal{P}$ is a group under "$\circ$" if $C(\mathfrak{h}) \in C(\mathfrak{a})\,\mathcal{P}$ since $\mathfrak{J}$ is of exponent 2.

Corollary 2.6.1. Assume the classes in $\mathfrak{J}$ have ordinary inverses, G is totally real, and $\mathcal{P}$ is nonempty. A component in the expression for $\mathfrak{J}$ is a group under ideal class product if and only if it contains $C((1))$.

Proof. We have $C((1)) \in \mathfrak{J}$. Since all concepts in the corollary are independent of $\mathfrak{h}$, we may let $\mathfrak{h} = (1)$.

Corollary 2.6.2. Let $\mathfrak{H}$ be the set of ideal classes with ordinary inverses. Then $\mathfrak{H}$ is a group under ideal class product. Let $\mathfrak{K}$ be a maximal subgroup of exponent 2 of $\mathfrak{H}$. Then $|\mathfrak{K}| = |\mathfrak{J}|$.

Proof. We can also make the classes in $\mathfrak{H}$ into a group under "$\circ$". Then $\mathfrak{J}$ is a subgroup of exponent 2 of $\mathfrak{H}$. We show that it is maximal. Assume $C(\mathfrak{a}) \circ C(\mathfrak{a}) = C(\mathfrak{h})$. Thus $\mathfrak{a}^2\mathfrak{h}^{-1} \sim \mathfrak{h}$

and so $\mathfrak{a}^2 \sim \mathfrak{h}^2$. Finally $\mathfrak{a}^\circ = \mathfrak{h}\mathfrak{h}^\circ\mathfrak{a}^{-1}$ by Lemma 2.3 (1)

$$\sim \mathfrak{h}^2\mathfrak{a}^{-1} \sim \mathfrak{a}.$$

Define $\varphi(C(\mathfrak{a})) = C(\mathfrak{a}\mathfrak{h})$. We shall show that φ is an isomorphism from $\mathfrak{H}$ under ideal class product to $\mathfrak{H}$ under "$\circ$". Clearly φ is one-to-one onto. We have $\varphi(C(\mathfrak{a}\mathfrak{b})) = C(\mathfrak{a}\mathfrak{b}\mathfrak{h}) = C((\mathfrak{a}\mathfrak{h})(\mathfrak{b}\mathfrak{h})\mathfrak{h}^{-1})$ $= \varphi(C(\mathfrak{a})) \circ \varphi(C(\mathfrak{b}))$. Since φ is an isomorphism it maps $\mathfrak{K}$ onto $\mathfrak{J}$.

III. THE FINITE FIELD CASE

When F is a finite field, $D = F$ and so there can be only one class of symreps. The two main questions when $D = F$ are

(1) do G/F symreps exist?

(2) If G/F symreps exist, how many are there?

The next theorem answers both questions.

Theorem 3.1. Let F be a finite field. If $|F|$ is even let $\varepsilon = 0$; otherwise let $\varepsilon = \pm 1 \equiv |F| \pmod 4$. The number of G/F symreps is exactly $|F|(|F|^2 - 1)|F|^3(|F|^4 - 1)\dots(|F|^{n-1} - 1)$ for n odd and $|F|(|F|^2 - 1)\dots|F|^{n-3}(|F|^{n-1} - 1)(|F|^{n-1} - \varepsilon^{n/2}|F|^{(n/2-1)})$ for n even.

Proof. The existence of G/F symreps. By Theorem 2.1 (1) and Theorem 2.3, it suffices to find $\eta \in G$ for which $(-1)^{n(n-1)/2}\, N\eta$ is a nonzero square in F. Suppose α generates the multiplicative group of G. Let $|F| = q$, then $N\alpha = \alpha \cdot \alpha^q \alpha^{q^2} \dots \alpha^{q^{n-1}} = \alpha^{(q^n-1)/(q-1)}$. Thus $N\alpha$ has order $q - 1$ and so generates the multiplicative group of F. Let $(-1)^{n(n-1)/2} = (N\alpha)^k$. It suffices to take $\eta = \alpha^k$.

The number of G/F symreps. We shall use Theorem 2.5. There is only one class of G/F reps and $S(G,F)$ holds. Hence there are $g[\mathcal{U}^+ : \mathcal{U}^2]$ symreps. We shall show that $[\mathcal{U}^+ : \mathcal{U}^2] = 1$. Let α be as above. We have

$$\begin{aligned} \mathcal{U}^+ &= \{\alpha^k : (N\alpha)^k \text{ is a square in } F\} \\ &= \{\alpha^{2k}\} \quad \text{since } N\alpha \text{ generates the multiplcative group of } F \\ &= \mathcal{U}^2. \end{aligned}$$

When $|F|$ is odd, the value of $|O_n(F)|$ can be found in Dickson [2, p.160] and leads to the expression stated in the theorem.

We now suppose that $|F|$ is even. Then F has characteristic 2. Clearly the number of solutions to $XX' = I$ is the number of orthonormal bases (counting order) for the n dimensional vector space over F with inner product $(\underline{\alpha},\underline{\beta}) = \Sigma\, \alpha_i \beta_i$. We shall count the number of bases by an inductive process. Assume $\underline{\alpha}_1,\ldots,\underline{\alpha}_{k-1}$ are orthonormal. How many $\underline{\alpha}_k$'s can be found which preserve orthonormality? Let $\underline{e} = (1,1,\ldots,1)'$. Since $\sqrt{\Sigma\, a_i^2} = \sqrt{(\Sigma\, a_i)^2} = \Sigma\, a_i$, the vector $\underline{\alpha}_k$ preserves orthonormality if and only if

$$(\underline{\alpha}_i,\underline{\alpha}_k) = 0 \quad \text{for} \quad 1 \leq i \leq k-1$$

and

$$(\underline{e},\underline{\alpha}_k) = 1 .$$

Since $\underline{\alpha}_1,\ldots,\underline{\alpha}_{k-1}$ are independent, these equations are independent if they are consistent. The equations are inconsistent if and only if $\underline{e} = \Sigma_{i=1}^{k-1} \lambda_i \underline{\alpha}_i$ for some $\lambda_i \in F$. This gives $\lambda_i = (\underline{e},\underline{\alpha}_i) = 1$ by orthonormality. Thus the equations are inconsistent if and only if

$\underline{e} = \Sigma_{i=1}^{k-1} \underline{\alpha}_i$. From this discussion it follows that if any such $\underline{\alpha}_k$ exists, exactly $|F|^{n-k}$ exist. Furthermore, we can have inconsistency only if

$$n = (\underline{e},\underline{e}) = \sum_{i=1}^{k-1} (\underline{\alpha}_i,\underline{\alpha}_i) = k - 1 \quad \text{in} \quad F \ ;$$

i.e. only if $n \equiv k - 1 (\text{mod } 2)$. In this case we have

$$(\underline{e} + \sum_{i=1}^{k-2} \underline{\alpha}_i,\underline{\alpha}_i) = (\underline{e},\underline{\alpha}_i) + (\underline{\alpha}_i,\underline{\alpha}_i) = 0 \quad \text{for} \quad 1 \leq i \leq k - 2$$

and

$$(\underline{e} + \sum_{i=1}^{k-2} \underline{\alpha}_i,\underline{e}) = (\underline{e},\underline{e}) + \sum_{i=1}^{k-2} (\underline{e},\underline{\alpha}_i) = n + k - 2 = 1 \ .$$

Hence, if $\underline{\alpha}_1,\ldots,\underline{\alpha}_{k-2}$ are orthonormal and $n \equiv k - 1 \ (\text{mod } 2)$, there is exactly one $\underline{\alpha}_{k-1}$ such that $\underline{\alpha}_1,\ldots,\underline{\alpha}_{k-1}$ are orthonormal and the equations for $\underline{\alpha}_k$ are inconsistent. Let A_k^n be the number of sequences $\underline{\alpha}_1,\ldots,\underline{\alpha}_k$ of n dimensional orthonormal vectors over F. We have shown that A_k^n satisfies the recursion

$$A_k^n = A_{k-1}^n \ |F|^{n-k} \quad \text{if} \quad n \equiv k \ (\text{mod } 2) \ ;$$

$$A_k^n = (A_{k-1}^n - A_{k-2}^n) \ |F|^{n-k} \quad \text{if} \quad n \equiv k - 1 \ (\text{mod } 2) \ .$$

Since $A_1^n = |F|^{n-1}$ and, for n odd, $A_2^n = (|F|^{n-1} - 1) \ |F|^{n-2}$, the recursion leads to the result stated in the theorem.

IV. THE ALGEBRAIC NUMBER FIELD CASE

We now assume that F is an algebraic number field. Of the two basic questions - existence of symreps and number of symreps - it is far easier to find the number when at least one symrep exists. By Corollary 2.5.1 and the fact the F has $\aleph_0$ elements, we see that if any G/F symreps exist, then there are exactly $\aleph_0$ symreps. We make the following conjecture regarding existence.

> When F is an algebraic number field, G/F symreps exist if and only if
>
> (i) if F is formally real, G is totally real and,
>
> (ii) if $n \equiv 2 \pmod 4$, there is a $\lambda \in G$ and a $k \in F$ such that $-1 = k^2 N\lambda$.

The necessity of these conditions follows easily from Theorem 2.2 (3) and Corollary 2.3.1. We now show that condition (ii) is sufficient when $n = 2$. By Theorem 2.4 we have $G = F(\sqrt{c})$ and G/F symreps exist if $c = x^2 + y^2$ for some $x, y \in F$. The condition $x^2 + y^2 = c$ is equivalent to $(1/y)^2 N(x - \sqrt{c}) = -1$ since we cannot have $y = 0$. Sapiro [14] established our conjecture for $n = 3$. The remainder of this section is devoted to establishing the conjecture for all odd n.

One of the major difficulties with the study of the algebraic number field case is that, unlike the study of the finite field case, it is not clear how to choose λ in Theorem 2.2. When n is odd, a slight generalization of Sapiro's method [14] enables us to reduce the problem to $\mathfrak{p}$-adic considerations for all spots $\mathfrak{p}$ on F. The choice of λ is easier in the local case than in the global; however, spots which divide 2 present difficulties. These can be disposed of by considering cases.

We shall make use of quadratic form theory, local field theory, and local class field theory. Needed theorems can be found in the Appendix and are referred to with roman capitals, e.g. Theorem B. To read the remainder of this section it suffices to have a basic knowledge of local fields such as that found in [12, Part One].

Definition 4.1. The following notation is to be used for the rest of this section.

(1) f,g,h are quadratic forms.

(2) A,B,C are the symmetric matrices associated with quadratic forms, thus $f = \underline{x}'A\underline{x}$.

(3) $\cdot \cong \cdot \ (\cdot)$ is equivalence of forms. Thus $A \cong B(F)$ means that for some nonsingular F matrix P we have $PAP' = B$. We may omit $(\cdot)$ if the meaning is clear.

(4) $(\cdot,\cdot/\cdot) = \pm 1$, the Hilbert symbol. Thus $(\alpha,\beta/H) = +1$ if and only if $\alpha x^2 + \beta y^2 = 1$ has a solution $x,y \in H$. We may omit $/\cdot$ if the meaning is clear.

(5) $c(\cdot/\cdot)$ is the Hasse symbol. Thus $c(A/H)$ is $\Pi_{i \leq j} \ (\alpha_i,\alpha_j/H)$

where $A \cong \Sigma \oplus \alpha_i \ (H)$. We may omit $/\cdot$ if the meaning is clear.

(6) $\alpha W^2 = \{\alpha w^2 : w \in W\}$.

(7) $W^* = \{w \in W : w \neq 0\}$.

(8) $N(\cdot^*/\cdot)$ is the norm group. Thus $N(K^*/H) = \{N_{K/H}\,\alpha : \alpha \in K^*\}$.

(9) $\mathfrak{D}(\cdot/\cdot)$ is the discriminant. Thus for an algebraic number field H we have $\mathfrak{D}(K/H)$ is the ideal generated by all $|M(\underline{\alpha})|^2$ where $\underline{\alpha}$ is an mbv for K over H and $\underline{\alpha}$ has algebraic integers for components.

(10) $f = f(\cdot/\cdot)$ is the index of inertia of an extension of one local field over another and $e = e(\cdot/\cdot)$ is the index of ramification.

(11) If H is an algebraic number field with prime spot $\mathfrak{p}$, then $H_{\mathfrak{p}}$ is the completion of H at $\mathfrak{p}$. Further, if ρ is a zero of an irreducible H polynomial $p(x)$, then $H(\rho;\mathfrak{p}) = H_{\mathfrak{p}}[x]/(p(x))$.

We shall now generalize Sapiro's technique for reduction to the local case. The main points of the proof follow [14].

Theorem 4.1. Let F be an algebraic number field. Assume that n is odd. There is a G/F symrep if and only if

(i) for every local prime spot $\mathfrak{p}$ on F there is a $\lambda(\mathfrak{p}) \in F(\theta;\mathfrak{p})$ and a basis $\alpha_1,\ldots,\alpha_n$ for $F(\theta;\mathfrak{p})$ over F such that for an indeterminate $\underline{x}$ we have

$$\mathrm{tr}(\lambda(\mathfrak{p})(\underline{\alpha},\underline{x})^2) \cong (\underline{x},\underline{x}) \ (F_{\mathfrak{p}})$$

where the trace is from $F(\theta;\mathfrak{p})$ to $F_{\mathfrak{p}}$;

(ii) if F is formally real, G is totally real.

Proof. The necessity is clear since we may take $\lambda(\mathfrak{p})$ to be the λ of Corollary 2.2.1.

The proof of sufficiency involves three main parts:

(1) preliminary remarks,

(2) choice of λ for Corollary 2.2.1,

(3) proof that λ has the required property.

(1). Without loss of generality, we may assume that θ is an algebraic integer. Let $p(x) = 0$ be the monic irreducible F polynomial for θ. All mbv's for $F(\theta;\mathfrak{p})$ over $F_{\mathfrak{p}}$ are related by nonsingular $F_{\mathfrak{p}}$ transformations. Hence we can choose for $\underline{\alpha}$ in (i) of the theorem any mbv for $F(\theta;\mathfrak{p})$ over $F_{\mathfrak{p}}$. One such mbv is $\alpha_i \equiv x^{i-1} \pmod{p(x)}$, which corresponds to the mbv $(1,\theta,\ldots,\theta^{n-1})$' for G over F. Thus we can choose the same $\underline{\alpha}$ for all $\mathfrak{p}$ and in such a way that the components are algebraic integers. Fix $\underline{\alpha}$ to be as above.

Let $A(\nu)$ correspond to the form $\mathrm{tr}(\nu(\underline{\alpha},\underline{x})^2)$ where ν is in G or $F(\theta;\mathfrak{p})$. If $\mathfrak{P}$ is a prime divisor of $\mathfrak{p}$ over G, let $\lambda(\mathfrak{P})$ be the component of $\lambda(\mathfrak{p})$ in the $L(\mathfrak{P})$ of Theorem G. Let $(\pi) = \mathfrak{p}$. Since (i) holds for $\lambda(\mathfrak{p})$ if and only if it holds for $\pi^{2c}\lambda(\mathfrak{p})$ for every integer c, we may assume that $\lambda(\mathfrak{P})$ is a $\mathfrak{P}$-adic integer for all $\mathfrak{P}$ dividing $\mathfrak{p}$.

Since every quadratic form over $F_{\mathfrak{p}}$ is equivalent to a diagonal form, we can choose a nonsingular matrix $T(\mathfrak{p})$ with $\mathfrak{p}$-adic integer components in $F_{\mathfrak{p}}$ such that $T(\mathfrak{p})\, A(\lambda(\mathfrak{p}))\, T(\mathfrak{p})' = \Sigma \oplus \beta_i$ for some nonzero β_i's in $F_{\mathfrak{p}}$. Let j be such that $4\mathfrak{p}\Pi\, \beta_i$ divides $\mathfrak{p}^j$. Let $\mathfrak{P}$ be a prime spot on G dividing $\mathfrak{p}$. Define $k(\mathfrak{P}) = j \cdot e(L(\mathfrak{P})/F_{\mathfrak{p}})$. We will show that if for all prime spots $\mathfrak{P}$ on G dividing $\mathfrak{p}$ we have

$$(*) \qquad \begin{aligned} &\mu(\mathfrak{P}) \equiv \lambda(\mathfrak{P}) \pmod{\mathfrak{P}^{k(\mathfrak{P})}}, \quad \text{then} \\ &c(A(\mu(\mathfrak{p}))/F_{\mathfrak{p}}) = +1 . \end{aligned}$$

Let $T(\mathfrak{p})$ be as above. Then we have that

$$\begin{aligned} c(A(\mu(\mathfrak{p}))/F_{\mathfrak{p}}) &= c(T(\mathfrak{p})A(\mu(\mathfrak{p}))T(\mathfrak{p})') \quad \text{by Theorem B (1)} \\ &= c(T(\mathfrak{p})A(\lambda(\mathfrak{p}))T(\mathfrak{p})') \quad \text{by Theorems B (6) and} \\ &\qquad \text{A (6) and the fact that } \alpha_1,\ldots,\alpha_n,\ \lambda(\mathfrak{P}) \text{ are} \\ &\qquad \mathfrak{P}\text{-adic integers and } \mu(\mathfrak{p}) \equiv \lambda(\mathfrak{p}) \pmod{\mathfrak{p}^j} \\ &= c(A(\lambda(\mathfrak{p}))) = +1 \quad \text{by condition (i) of the} \\ &\qquad \text{theorem.} \end{aligned}$$

(2). Let $d = |M(\underline{\alpha})|^2$ and $\Omega = \{\mathfrak{Q} : \mathfrak{Q}$ is a prime divisor of $(2d)$ over $G\}$. Let $m = \max_{\Omega} k(\mathfrak{Q})$ where k is as defined in the previous paragraph. Let $\mathfrak{B} = (\Pi_{\Omega}\, \mathfrak{Q})^m$. By Theorem H there is a

$\mu_0 \in G$ such that

$$(**) \qquad \mu_0 \equiv \lambda(\mathfrak{D}) \pmod{\mathfrak{D}^m} \quad \text{for all} \quad \mathfrak{D} \in \Omega .$$

Any $\mu \in G$ with $\mu \equiv \mu_0 \pmod{\mathfrak{B}}$ is also a solution. If G is totally real, there is a $\beta \in G$ such that $\beta \equiv 1 \pmod{\mathfrak{B}}$ and $\mu_0\beta$ is totally positive. By condition (ii) of the theorem we may assume that μ_0 is totally positive whenever F is formally real.

Let $\ell(\mathfrak{D})$ be the highest power of $\mathfrak{D}$ dividing μ_0. Let $\mathfrak{C} = \Pi_\Omega \mathfrak{D}^{\ell(\mathfrak{D})}$. Apply Theorem M with $\mathfrak{A} = (\mu_0)/\mathfrak{C}$ and $\mathfrak{B}$ as above. Let $\mu = \mu_0/\alpha$. Then $\mu \equiv \mu_0 \pmod{\mathfrak{B}}$ and $(\mu) = \mathfrak{C}\,\mathfrak{P}_0$ and μ is totally positive if F is formally real. Let $\lambda = \mu d\, N\mu$.

(3). We have $|A(\lambda)| = |M(\underline{\alpha})|^2\, |J(\lambda)| = d\, N\lambda$. Since n is odd, $d\, N\lambda = (d\, N\mu)^{n+1} \in F^{*2}$.

If F is formally real, μ and $d = |M(\underline{\alpha})|^2$ are totally positive. Thus $c(A(\lambda)/F_{\mathfrak{p}}) = +1$ whenever $\mathfrak{p}$ is an infinite prime spot on F.

Let $\mathfrak{p}$ be a finite prime spot on F which is prime to $2d\,\mathfrak{P}_0$. Then $\mathfrak{p}$ is prime to $2(d\,N(\mathfrak{C}\,\mathfrak{P}_0))^{n+1} = 2(|A(\lambda)|)$. By Theorem B (5) we have $c(A(\lambda)/F_{\mathfrak{p}}) = +1$ for such $\mathfrak{p}$.

Assume that $\mathfrak{p}$ is not prime to 2d. Thus $\mathfrak{p}$ divides 2d. By equation (**) and the definition of μ, it follows that $\mu \equiv \lambda(\mathfrak{P}) \pmod{\mathfrak{P}^m}$ for all prime spots $\mathfrak{P}$ on G which divide $\mathfrak{p}$.

Thus we have $c(A(\mu)/F_{\mathfrak{p}}) = +1$ by the result (*). Also $N\mu/N\lambda(\mathfrak{p}) \equiv 1 \pmod{4\mathfrak{p}}$. Since $d\ N\lambda(\mathfrak{p}) = |A(\lambda(\mathfrak{p}))| \in F^{*2}$ by (i) of the theorem, it follows that $d\ N\mu \in F^{*2}$ by Theorem A (6). Hence $c(A(\lambda)/F_{\mathfrak{p}}) = c(A(\mu d\ N\mu)) = c(A(\mu)) = +1$.

We have shown that $|A(\lambda)| \in F^{*2}$ and that $c(A(\lambda)/F_{\mathfrak{p}}) = +1$ for all prime spots $\mathfrak{p}$ on F except possibly the one which $\mathfrak{P}_0$ divides. By Theorems C and D, we have $A(\lambda) \cong I_n(F)$. Application of Corollary 2.2.1 completes the proof.

We shall now deal with the local problems that arise as a result of Theorem 4.1 (i). The division into cases is as follows.

I. $(\mathfrak{p}, 2) = 1$. Done in Lemma 4.2.

II. $(\mathfrak{p}, 2) = \mathfrak{p}$.

   A. For $\mathfrak{P}_1$ and $\mathfrak{P}_2$ distinct prime divisors of $\mathfrak{p}$ we have $N(L(\mathfrak{P}_i)^*/F_{\mathfrak{p}}) \not\subseteq F_{\mathfrak{p}}^{*2}$. Done in Lemma 4.3.

   B. For at most one prime $\mathfrak{P}$ dividing $\mathfrak{p}$ we have $N(L(\mathfrak{P})^*/F_{\mathfrak{p}}) \not\subseteq F_{\mathfrak{p}}^{*2}$. Reduced to II C by Lemma 4.5.

   C. The field H is a local field with prime spot $\mathfrak{p}$ and extension K of odd degree. By Theorem F it suffices to consider the following cases.

      1. $e(K/H) = 1$. Done in Lemma 4.6.

      2. $f(K/H) = 1$. Let $a = (e(K/H)^2 - 1)/8$.

         a. $(-1,-1/H)^a = +1$. Done in Lemma 4.7.

         b. $(-1,-1/H)^a = -1$. Done in Lemma 4.8.

Lemma 4.1. Let H be a local field at the spot $\mathfrak{p}$ and let K be a finite extension of H. There is a $\lambda \in K$ and an mbv $\underline{\alpha}$ for K over H such that $M(\underline{\alpha})\ J(\lambda)\ M(\underline{\alpha})' = A(\lambda)$ has $\mathfrak{p}$-adic integer entries and $\mathfrak{p}$-adic unit determinant.

Proof. By Theorem F, there is an mbv $\underline{\alpha}$ for the integers in K over the integers in H. Let (Π) be the prime spot on K. Since every ideal of K is a power of (Π) we have $(1)^\circ = \Pi^m(1)$ for some integer m. Since $\underline{\alpha}$ is an mbv for (1), the matrix $M(\underline{\alpha})\ J(\Pi^m)\ M(\underline{\alpha})'$ has the desired form by Theorem 1.4 (2) and (4).

Lemma 4.2. Condition (i) of Theorem 4.1 can be satisfied when $\mathfrak{p}$ is prime to 2.

Proof. Let $F(\theta;\mathfrak{p}) = \Sigma \oplus L(\mathfrak{P})$ be the decomposition by Theorem G and let $A = \Sigma \oplus A(\lambda_{\mathfrak{P}})$ where $A(\lambda_{\mathfrak{P}})$ is the matrix over $F_{\mathfrak{p}}$ derived by applying Lemma 4.1 to $L(\mathfrak{P})$ and $F_{\mathfrak{p}}$. Then $c(A/F_{\mathfrak{p}}) = +1$ by Theorem B (5). Let $B = |A|\ A$. Then $|B| \in F_{\mathfrak{p}}^{*2}$ and $c(B) = (|A|, \pm 1) = +1$ by Theorems B (3) and A (5).

We now turn to the case in which $\mathfrak{p}$ divides 2. The following lemma, however, does not require this restriction on $\mathfrak{p}$ for its method of proof.

Lemma 4.3. If $F(\theta;\mathfrak{p}) = H \oplus K \oplus \mathfrak{A}$ where H and K are fields, $\mathfrak{A}$ is a (possibly empty) algebra, $[H : F_{\mathfrak{p}}]$ is odd, and $N(K^*/F_{\mathfrak{p}}) \not\subseteq F_{\mathfrak{p}}^{*2}$; then condition (i) of Theorem 4.1 can be satisfied.

Proof. Let (i) $m = (n - [H : F_{\mathfrak{p}}])/2$,

(ii) $\underline{\alpha}$ be an mbv for $\mathfrak{A}$ over $F_{\mathfrak{p}}$,

(iii) $\underline{\beta}$ be an mbv for K over $F_{\mathfrak{p}}$, and

(iv) $\underline{\gamma}$ be an mbv for H over $F_{\mathfrak{p}}$.

Let A correspond to $tr_{\mathfrak{A}/F} (\underline{\alpha},\underline{x})^2$. Let $\kappa \in K$ be such that $N\kappa \notin F_{\mathfrak{p}}^{*2}$. If $(-1)^m |A|\cdot|M(\underline{\beta})|^2 \in F_{\mathfrak{p}}^{*2}$, let $\mu = \kappa$; otherwise let $\mu = 1$. Let B correspond to $tr_{K/F_{\mathfrak{p}}} (\mu(\underline{\beta},\underline{x})^2)$. Then $(-1)^m |A|\cdot|B| \notin F^{*2}$. Let $c = |A|\cdot|B|\cdot|M(\underline{\gamma})|^2$ and let C correspond to $c\, tr_{H/F_{\mathfrak{p}}} (\underline{\gamma},\underline{x})^2$ and let $D(a) = aA \oplus aB \oplus C$ where $a \in F_{\mathfrak{p}}^*$. Then $|D(a)| = |A|\cdot|B|\cdot a^{2m}\cdot|M(\underline{\gamma})|^2 c^h$ where $h = [H : F_{\mathfrak{p}}]$ is odd. Hence $|D(a)| \in F_{\mathfrak{p}}^{*2}$. We have

$$\begin{aligned} c(D(a)) &= c(aA \oplus aB)\, c(C)\, (|C|,\ |D(a)|/|C|) \quad \text{by Theorem B (2)} \\ &= c(A \oplus B)\, c(C)\, (|C|,\ |C|)\, (a,(-1)^m |A|\cdot|B|) \end{aligned}$$

by Theorem B (3). Theorem A (3) shows that an appropriate choice of a will make $c(D(a)) = +1$.

We now wish to study a field H for which $N(H^*/F_{\mathfrak{p}}) \subseteq F_{\mathfrak{p}}^2$. This will then be applied in Lemma 4.5.

Lemma 4.4. Let $\mathfrak{p}$ be a prime spot on F which divides 2. Let H be an extension of $F_{\mathfrak{p}}$ such that $N(H^*/F_{\mathfrak{p}}) \subseteq F_{\mathfrak{p}}^2$. Then

(i) there is a field $E = F_{\mathfrak{p}}(\sqrt{\alpha}, \sqrt{\beta}, \sqrt{\gamma})$ for some $\alpha, \beta, \gamma \in F_{\mathfrak{p}}$ such that $H \supseteq E$ and $e(H/F_{\mathfrak{p}}) = 4$ and $f(E/F_{\mathfrak{p}}) = 2$, and

(ii) for any mbv $\underline{\alpha}$ of H over $F_{\mathfrak{p}}$ we have $|M(\underline{\alpha})|^2 \in F_{\mathfrak{p}}^{*2}$.

Proof. Let K be the maximum abelian subextension of H and let L be the maximum abelian subextension of H of type $(2,2,\ldots,2)$. Let $\mathcal{K}$ be the Galois group of K over $F_{\mathfrak{p}}$ and $\mathcal{L}$ the Galois group of L over $F_{\mathfrak{p}}$. We shall show that $\mathcal{L} \simeq F_{\mathfrak{p}}^*/F_{\mathfrak{p}}^{*2}$ where $\simeq$ is group isomorphism. By Theorem L we have $\mathcal{K} \simeq F_{\mathfrak{p}}^*/N(K^*/F_{\mathfrak{p}})$. Theorem K gives $N(K^*/F_{\mathfrak{p}}) = N(H^*/F_{\mathfrak{p}})$. Thus

$$\mathcal{L} \simeq \mathcal{K}/\mathcal{K}^2 \simeq (F_{\mathfrak{p}}^*/N(K^*/F_{\mathfrak{p}}))/(F_{\mathfrak{p}}^*/N(K^*/F_{\mathfrak{p}}))^2$$
$$= (F_{\mathfrak{p}}^*/N(H^*/F_{\mathfrak{p}}))/(F_{\mathfrak{p}}^*/N(H^*/F_{\mathfrak{p}}))^2 \simeq F_{\mathfrak{p}}^*/F_{\mathfrak{p}}^{*2}$$

since $N(H^*/F_{\mathfrak{p}}) \subseteq F_{\mathfrak{p}}^{*2}$ by assumption. We shall show that $f(L^*/F_{\mathfrak{p}}) = 2$ and $e(L^*/F_{\mathfrak{p}}) \geq 4$. From this (i) will follow by taking for E an appropriate subfield of L. Since inertial extensions are cyclic and $\mathcal{L}$ is of type $(2,2,\ldots,2)$, we have that f is 1 or 2. We also have $F_{\mathfrak{p}}^*/N(L^*/F_{\mathfrak{p}}) \simeq \mathcal{L}$ by Theorem L so that $N(L^*/F_{\mathfrak{p}}) = F_{\mathfrak{p}}^{*2}$ and we cannot have $f = 1$. Hence $f = 2$. Since $ef = [L : F_{\mathfrak{p}}] = |\mathcal{L}| = [F_{\mathfrak{p}}^* : F_{\mathfrak{p}}^{*2}] \geq 8$ by Theorem J, it follows that $e \geq 4$.

To establish (ii) it suffices by Theorem 1.4 (2) to choose a particular $\underline{\alpha}$. Let $H = F_{\mathfrak{p}}(\varphi)$ and $k = [H : F_{\mathfrak{p}}]$ and $p(x)$ be the monic irreducible $F_{\mathfrak{p}}$ polynomial for φ and $\underline{\alpha} = (1,\varphi,\ldots,\varphi^{k-1})'$. Then we have

$$|M(\underline{\alpha})|^2 = (-1)^{k(k-1)/2} N_{H/F_{\mathfrak{p}}}\ p'(\varphi) \quad \text{by the formula for a van der Monde determinant}$$

$$= N_{H/F_{\mathfrak{p}}}\ p'(\varphi)$$

$$\in F_{\mathfrak{p}}^{*2} \quad \text{since } 4 \text{ divides } [E : F_{\mathfrak{p}}] \text{ which divides } [H : F_{\mathfrak{p}}] \text{ by (i) and } N(H^*/F_{\mathfrak{p}}) \subseteq F_{\mathfrak{p}}^{*2} \text{ by assumption.}$$

Lemma 4.5. Let $\mathfrak{p}$ be a prime spot of F which divides 2. Assume that $F(\theta;\mathfrak{p}) = \mathfrak{A} \oplus K$ where $\mathfrak{A}$ is an algebra and K is a field such that $N(K^*/F_{\mathfrak{p}}) \subseteq F_{\mathfrak{p}}^2$. To satisfy (i) of Theorem 4.1 it suffices to find an mbv $\underline{\alpha}$ for $\mathfrak{A}$ over $F_{\mathfrak{p}}$ and a $\lambda \in \mathfrak{A}$ such that $tr_{\mathfrak{A}/F_{\mathfrak{p}}}(\lambda(\underline{\alpha},\underline{x})^2) \simeq (\underline{x},\underline{x})$ $(F_{\mathfrak{p}})$.

Proof. Let A be the matrix of the form $tr_{\mathfrak{A}/F_{\mathfrak{p}}}(\lambda(\underline{\alpha},\underline{x})^2)$ mentioned in the statement of the lemma. Let $\omega \in K^*$, let $\underline{\xi}$ be an mbv for K over $F_{\mathfrak{p}}$, and let B correspond to $tr_{K/F_{\mathfrak{p}}}(\omega(\underline{\xi},\underline{x})^2)$. Then $c(A \oplus B) = c(A)\ c(B)\ (|A|, |B|) = c(B)$ by Theorem B (2) since $A \simeq I$. Also $|A \oplus B| = |A|\cdot|B| \in F_{\mathfrak{p}}^{*2}$ since $A \simeq I$ and since $|B| \in F_{\mathfrak{p}}^{*2}$ by Lemma 4.4 (ii). Thus it suffices to choose ω so that $c(B) = +1$. We do not know enough about the structure of K over $F_{\mathfrak{p}}$ to do this directly. The idea of the proof is to apply the structure properties given in Lemma 4.4 and Theorem F and the formulas for calculation of the Hasse invariant given in Theorems A and B to reduce the problem to fields between K and $F_{\mathfrak{p}}$ with simpler structure.

Let T be the inertial field of K over $F_{\mathfrak{p}}$. Since the Galois group of T over $F_{\mathfrak{p}}$ is cyclic (Theorem F), we may construct the tower $F_{\mathfrak{p}} = T_0 \subset T_1 \subset \cdots \subset T_k \subseteq T$ where $[T_j : T_{j-1}] = 2$ for $1 \leq j \leq k$ and $[T : T_k]$ is odd. By Lemma 4.4 (i) we have $N(K^*/T_k) \not\subseteq T_k^2$. Hence we can choose $i < k$ such that $N(K^*/T_i) \subseteq T_i^2$ and $N(K^*/T_{i+1}) \not\subseteq T_{i+1}^2$. Let $\underline{\sigma}$ be an mbv for K over T_i and $\underline{\tau}$ an mbv for T_i over $F_{\mathfrak{p}}$. Then $\underline{\xi} = \underline{\sigma} \otimes \underline{\tau}$ is an mbv for K over $F_{\mathfrak{p}}$. If $tr_{K/T_i}(\omega(\underline{\sigma},\underline{x})^2) \cong (\underline{x},\underline{x})\ (T_i)$, then let B correspond to $tr_{K/F_{\mathfrak{p}}}(\omega(\underline{\xi},\underline{y})^2)$. As $tr_{K/F_{\mathfrak{p}}}(\omega\sigma_\ell\tau_k\sigma_q\tau_r) = tr_{T_i/F_{\mathfrak{p}}}(\tau_k\tau_r(tr_{K/T_i}\omega\sigma_\ell\sigma_q))$, we have $B \cong I_m \otimes B_1$ where B_1 corresponds to $tr_{T_i/F_{\mathfrak{p}}}(\underline{\tau},\underline{z})^2$ and $m = [K : T_i]$. Since 8 divides m by Lemma 4.4 (i), an application of Theorem B (4) gives $c(B) = +1$ since the only factors which can have odd powers are $c(I_m) = +1$ and $(-1,|I_m|) = +1$ and $(|I_m|,|B_1|) = +1$. This shows that $F_{\mathfrak{p}}$ can be replaced by T_i to prove the lemma.

Let $\underline{\beta}$ be an mbv for K over T_{i+1}. Since $N(K^*/T_{i+1}) \not\subseteq T_{i+1}^2$, we can choose $\nu \in K$ so that the matrix C associated with $tr_{K/T_{i+1}}(\nu(\underline{\beta},\underline{x})^2)$ satisfies $|C| \notin T_{i+1}^2$. (The reasoning is like that used in choosing B in Lemma 4.3.) By Theorem E we have $C \cong C_1 \oplus s \oplus t$ where $s,t \in T_{i+1}^*$ and $C_1 = I \oplus -1$. Let $e \in T_i^*$ be such that $T_{i+1} = T_i(\sqrt{e})$. Let $\underline{\gamma} = (1, \sqrt{e})'$ and $\underline{\sigma} = \underline{\beta} \otimes \underline{\gamma}$. Let $\omega = r\nu$ where $r \in T^*_{i+1}$ will be chosen later. For $q \in T_{i+1}$ let $E(q)$ correspond to $tr_{T_{i+1}/T_i}(q(\underline{\gamma},\underline{x})^2)$. Then $tr_{K/T_i}(\omega(\underline{\sigma},\underline{y})^2)$ corresponds to

$$(C_1 \otimes E(r)) \oplus E(rs) \oplus E(rt) .$$

Call this $D(r)$. We will show how to choose r so as to make $c(D(r)) = +1$.

We now compute $c(D(r))$ in terms of simpler expressions. This requires Theorem B in many places. $c(D(r)) = c(C_1 \otimes E(r))$ $c(E(rs) \oplus E(rt))$ $(|C_1 \otimes E(r)|, |E(rs) \oplus E(rt)|)$. Since $\dim C_1 = \dim C - 2$ and $\dim C \equiv 0$ (4) by Lemma 4.4 (i), we have $|C_1 \otimes E(r)| \in T_i^{*2}$. It therefore follows that $c(D(r)) = c(C_1 \otimes E(r))\ c(E(rs) \oplus E(rt))$. From $\dim C_1 \equiv 2$ (4) and Theorem B (4) we have

$$\begin{aligned} c(C_1 \otimes E(r)) &= (-1,|C_1|)\ (-1,|E(r)|)\ (|C_1|,|E(r)|) \\ &= (-1,-1)\ (-1,|E(r)|)\ (-1,|E(r)|) \\ &= (-1,-1). \end{aligned}$$

Thus $c(D(r)) = (-1,-1)\ c(E(rs))\ c(E(rt))\ (|E(rs)|, |E(rt)|)$. Furthermore $|E(rt)| \in |E(rs)|\ T_i^{*2}$ since $|D(r)| \in T_i^{*2}$ by Lemma 4.4 (ii) and $|C_1 \otimes E(r)| \in T_i^{*2}$.

Any $p \in T_i$ has the form $a + b\sqrt{e}$. Write $p_1 = a$ and $p_2 = b$. Suppose $p_1 \neq 0$. Then by Theorem B (6) we have

$c(E(p)) = (2p_1, -|E(p)|)\ (-1, |E(p)|)$. If $(rs)_1 \neq 0$ and $(rt)_1 \neq 0$, then

$$\begin{aligned} c(D(r)) &= (-1,-1)\ (2(rs)_1, -|E(rs)|)\ (-1, |E(rs)|) \\ &\qquad \cdot (2(rt)_1, -|E(rs)|)\ (-1, |E(rs)|) \\ &\qquad \cdot (|E(rs)|, |E(rs)|) \\ &= (-1,-1)\ ((rs)_1\ (rt)_1, -|E(rs)|)\ (|E(rs)|, -1) \\ &= (-(rs)_1\ (rt)_1, -|E(rs)|). \end{aligned}$$

To make $c(D(r)) = +1$ it suffices to show how to choose r so that $(rs)_1\ (rt)_1 \neq 0$ and $-|E(rs)| \in T_i^2$. Let $v(a) = s^{-1}\ (a^2 + \sqrt{e})^2 \sqrt{e}$ for $a \in T_i$. Then $-|E(v(a)s))| = 4e^2(a^4 - e)^2 \in T_i^2$. We show that $v(a)/v(b) \in T_i$ if and only if $a^2 = b^2$. Clearly

$$v(a)/v(b) = ((a^4 + e) + 2a^2 \sqrt{e}\ )/((b^4 + e) + 2b^2 \sqrt{e}\ )$$

which lies in T_i if and only if $2a^2 \cdot (b^4 + e) = 2b^2 \cdot (a^4 + e)$. This gives $a^2b^2(a^2 - b^2) = (a^2 - b^2)e$ and so $a^2 = b^2$ since $e \notin T_i^2$. This will be used to prove the existence of the desired r. By the above, $(s \cdot v(a))_1 \neq 0$ for at least two of $a = 0,1,2$ and $(t \cdot v(a))_1 \neq 0$ for at least two of $a = 0,1,2$. Thus $(s \cdot v(a))_1\ (t \cdot v(a))_1 \neq 0$ for at least one of $a = 0,1,2$.

This lemma reduces us to the situation in which $\mathfrak{p}$ divides 2 and K is an extension of odd degree of $F_{\mathfrak{p}}$. We break the extension into interial and ramified parts. First we consider the inertial case.

Lemma 4.6. Let $\mathscr{P}$ be a prime spot on F which divides 2. Let H be an inertial extension of $F_{\mathscr{P}}$ of odd degree. There is an $H/F_{\mathscr{P}}$ symrep.

Proof. Let $\underline{\alpha}$ be an mbv for H over $F_{\mathscr{P}}$. Define $A = |M(\underline{\alpha})|^2 M(\underline{\alpha})M(\underline{\alpha})'$. Clearly $|A| \in F_{\mathscr{P}}^{*2}$. Since inertial extensions are cyclic, $\underline{\alpha}^{(i)} \in H$. Thus $A \cong I(H)$. By Theorem B (7) we have $c(A/F_{\mathscr{P}}) = c(A/H) = +1$. By Corollary 2.2.1 there is an $H/F_{\mathscr{P}}$ symrep.

Lemma 4.7. If $\mathscr{P}$ divides 2 and H is local at $\mathscr{P}$, and K is a pure ramified extension of H of odd degree e, and $(-1,-1/H)^a = +1$ where $a = (e^2 - 1)/8$; then there is a K/H symrep.

Proof. By Theorem F we can choose $\Pi \in K$ such that (Π) is the prime spot on K and $\Pi^e = \pi \in H$. Let $\underline{\alpha} = (1, \Pi, \ldots, \Pi^{e-1})$ and let $A = e^{-1}M(\underline{\alpha})\, M(\underline{\alpha})'$. Then

$$A = \left(\begin{array}{c|ccc} 1 & & 0 & \\ \hline & 0 & & \pi \\ 0 & & \cdot^{\cdot^{\cdot}} & \\ & \pi & & 0 \end{array}\right) \cong 1 \oplus (I_k \otimes (1 \oplus -1)) \quad \text{where} \quad k = (e - 1)/2$$

since $2\pi xy = x'^2 - y'^2$ under the substitution $x = (x' + y')/2\pi$ and $y = x' - y'$. Let $B = (-1)^k A$. Then $|B| \in H^{*2}$ and

$$\begin{aligned} c(B/H) &= c(A)\ ((-1)^k, (-1)^{(e+1)/2}) \quad \text{by Theorem B (3)} \\ &= c(-I_k)\ (-1,-1)^{k(e+1)/2} \\ &= c(I_k)\ (-1,\ (-1)^{k(k+1)/2})\ (-1,-1)^{k(e+1)/2} \\ &= (-1,-1)^b \quad \text{where we have} \end{aligned}$$

$b = k(k+1)/2 + k(e+1)/2 = a + 2a = 3a$. Thus $B \cong I(H)$ and we apply Corollary 2.2.1.

Lemma 4.8. Let $\mathscr{G}$, H, K, e, a be as in the previous lemma. If $(-1,-1/H)^a = -1$, then there is a K/H symrep.

Proof. Since a is odd, $e \equiv \pm 3(8)$. Since $(-1,-1/H) = -1$ and $-((1-\sqrt{-3})/2)^2 - ((1+\sqrt{-3})/2)^2 = 1$, it follows that $\sqrt{5} \notin H$ by Theorem A (6). Let π, Π, $\underline{\alpha}$ be as in the previous lemma and let $\lambda = (1 + \Pi^{-1} + 4\Pi^{-2})/e$. Put $A = M(\underline{\alpha})\ J(\lambda)\ M(\underline{\alpha})'$. We have

$$A = \begin{pmatrix} 1 & 1 & 4 & & & 0 \\ 1 & 4 & & 0 & & \pi \\ 4 & & & & & \pi \\ & & & & & 4\pi \\ 0 & \pi & \pi & 4\pi & & 0 \end{pmatrix} .$$

Let $B = |A| \cdot A$. Clearly $|B| \in H^{*2}$. It suffices to show that $c(B) = +1$. We have $c(B) = (|A|, (-1)^{(e+1)/2})\ c(A)$. We shall use Theorem B (6) to evaluate $c(B)$. The cases $e = 3, 5$ will be considered separately. If E is a matrix, let $E_i = (e_{jk})$ $1 \le j,k \le i$.

When $e = 3$ we have

$$A = \begin{vmatrix} 1 & 1 & 4 \\ 1 & 4 & \pi \\ 4 & \pi & \pi \end{vmatrix} , \quad |A_1| = 1, \quad |A_2| = 3, \quad |A_3| = \pi(11 - \pi - 4^3/\pi) .$$

Thus $c(B) = c(A) = (1,-3)\ (3,-\pi\varepsilon)\ (\pi\varepsilon,-1)$

where $\varepsilon = 11 - \pi - 4^3/\pi$ is a $\mathfrak{p}$-adic unit

$= (-5,-\pi\varepsilon)(-1,-\pi\varepsilon)\ (-1,-1)$ by Theorem A (6)

$= (5,-\pi\varepsilon)\ (-1,-1)$

$= +1$ since $(5,-\pi\varepsilon) = -1$ by Theorem A (4).

When $e = 5$ we have

$$A = \begin{pmatrix} 1 & 1 & 4 & 0 & 0 \\ 1 & 4 & 0 & 0 & \pi \\ 4 & 0 & 0 & \pi & \pi \\ 0 & 0 & \pi & \pi & 4\pi \\ 0 & \pi & \pi & 4\pi & 0 \end{pmatrix}, \quad |A_1| = 1, \quad |A_2| = 3, \quad |A_3| = -4^3,$$

$$|A_4| = -3\pi^2(1 + 4^3/3\pi), \quad |A_5| = \pi^3\varepsilon \text{ for a } \mathfrak{p}\text{-adic unit } \varepsilon.$$

Hence $c(B) = (|A|,-1)\ c(A)$

$= (-1,|A|)^2(1,-3)\ (3,4^3)\ (-4^3,-|A_4|)(|A_4|, -|A|)$

$= (-1,-|A_4|)\ (|A_4|, -|A|) = (-1,-1)(|A_4|,|A|)$

$= -\ (5,|A|)$ by Theorem A (6)

$= +1$ by Theorem A (4).

Assume that $e > 5$. Since $e \equiv \pm 3(8)$, we have $e \geq 11$. Let $e = 8b + 3$ or $8b + 5$ determine the integer b. Let X be the $e \times e$ transformation such that premultiplication by X adds π^{-1} times the $(e - k + 2)^{nd}$ row to the k^{th} row for $k = 4,6,8,\ldots,$ $4b + 2$ and leaves the remaining rows unchanged. Then

$$XAX' = \left(\begin{array}{ccc|ccccccccc}
1 & 1 & 4 & & & & & & & & & 0\\
1 & 4 & 0 & & & & & & & & & \pi\\
4 & 0 & 0 & & & & & & & \mathbf{0} & & \pi\\
\hline
 & & & 2 & 1 & 4 & & & & & & 4\pi\\
 & & & 1 & 0 & 0 & & & & & \iddots & \\
 & & & 4 & 0 & 2 & 1 & 4 & & & & \\
 & & & & & 1 & 0 & 0 & & & & \\
 & & & & & 4 & 0 & 2 & & & & \\
 & \mathbf{0} & & & & & & & \ddots & & & \\
 & & & & & & & & & C & & \\
 & & \iddots & & & & & & & & \mathbf{0} & \\
0 & \pi & \pi & 4\pi & & & & & & & &
\end{array}\right),$$

where the block C is given by ($*$ indicates the center element of XAX')

(a) $$C = \begin{vmatrix} 2 & 1 & 4\\ 1 & 0^* & \pi\\ 4 & \pi & \pi \end{vmatrix} \qquad \text{if} \quad e = 8b + 5 ,$$

(b) $$C = \begin{pmatrix} 2 & 1 & 4 & 0 & 0\\ 1 & 0 & 0 & 0 & \pi\\ 4 & 0 & (2+\pi^{-1})^* & \pi+1 & \pi+4\\ 0 & 0 & \pi+1 & \pi & 4\pi\\ 0 & \pi & \pi+4 & 4\pi & 0 \end{pmatrix} \qquad \text{if} \quad e = 8b + 3 .$$

Let $d_i = |(XAX')_i|$. We now show that each $d_i \in H^*$ and evaluate certain of the d_i. We easily have

(i) $a_1 = 1$,

(ii) $a_2 = 3$,

(iii) $a_3 = -4^3 \in -H^{*2}$,

(iv) $a_{2k+1} = -a_{2k-1} \in (-1)^k H^{*2}$ for $5 \leq 2k + 1 \leq (e + 1)/2$,

(v) $a_{2k} = 2a_{2k-1} \neq 0$ for $4 \leq 2k < (e + 1)/2$,

(vi) $a_{4b+2} = (2 + \pi^{-1})\, a_{4b+1} \neq 0$ for $e = 8b + 3$.

When $e - 2 \geq 2i + 1 > (e + 1)/2$ we have

$(X_{2i+1})^{-1}(XAX')_{2i+1}(X'_{2i+1})^{-1} =$

$$\begin{array}{r} \\ \\ (e-2i)^{th} \text{ row} - - - - - - \\ \\ \end{array}
\left(\begin{array}{cccc}
\begin{array}{ccc|}1&1&4\\1&4&0\\4&0&0\\\hline\end{array} & & & \text{\Large 0}\\
& \ddots & & \\
& & \begin{array}{|ccc}\hline 2&1&4\\1&0&0\\4&0&\end{array} & \\
\text{\Large 0} & & & \begin{array}{|cccc}\hline 0 & & & \pi\\ & & \diagup & \pi\\ & \diagup & & 4\pi\\ \pi & \pi & 4\pi & 0\end{array}
\end{array}\right)$$

(vii) Thus $d_{2i+1} = d_{e-2i}\,(-\pi^2)^{(4i-e+1)/2} \in (-1)^i H^{*2}$.

Combining (i), (iii), (iv), and (vii) gives

(viii) $d_{2k+1} \in (-1)^k H^{*2}$ for $1 \leq 2k + 1 \leq e - 2$.

In a similar fashion to the derivation of (vii),

(ix) $d_{2i+2} \neq 0$ when $(e + 1)/2 < 2i + 2 \leq e - 3$.

We also have

(x) $d_e = |A_e| = \pi^{e-2}\varepsilon$ for some $\mathfrak{p}$-adic unit ε.

Finally, $d_{e-1} = |A_{e-1}| = \begin{vmatrix} 1 & 1 & 4 & & & 0 \\ 1 & 4 & & \text{\Large 0} & & 0 \\ 4 & & & & & \pi \\ & & & & \iddots & \pi \\ & & & \iddots & \iddots & 4\pi \\ 0 & 0 & \pi & \pi & 4\pi & \text{\Large 0} \end{vmatrix}$

$= 3(-\pi^2)^{(e-3)/2} + m4^3\,\pi^{e-4}$ for some integer m.

(xi) Thus $d_{e-1} \in (-1)^{(e-1)/2}\,5\,H^{*2}$ by Theorem A (6).

We now evaluate $c(B)$ from the above. Since $((-1)^k,-b)(b,-(-1)^{k+1}) = ((-1)^k,-1) = (-1)^k$ when $b \in H^*$, Theorem B (6) gives

$$c(B) = (d_e,-1)^{(e+1)/2}.\prod_{k=0}^{(e-5)/2} (-1)^k\cdot(d_{e-2},-d_{e-1})(d_{e-1},-d_e)(d_e,-1)\ .$$

However,

$$\begin{aligned}(d_{e-2},-d_{e-1}) &= ((-1)^{(e-3)/2},(-1)^{(e-3)/2}5) \\ &= (-1,-1)^{(e-3)/2}\ (-1,5)^{(e-3)/2} \\ &= (-1)^{(e-3)/2}\quad \text{since}\ \ -(1/2)^2 + 5(1/2)^2 = 1,\ \text{and}\end{aligned}$$

$$\begin{aligned}(d_{e-1}, -d_e) &= ((-1)^{(e-1)/2}5, -d_e) \\ &= ((-1)^{(e-1)/2}5, -1)\ (-1, d_e)^{(e-1)/2}\ (5, d_e) \\ &= (-1,-1)^{(e-1)/2}\ (5,-1)\ (-1,d_e)^{(e-1)/2}\ (5, \varepsilon\pi) \\ &= (-1)^{(e-1)/2}\ (-1,d_e)^{(e-1)/2}\ (-1) \quad \text{by Theorem A (4).}\end{aligned}$$

Thus $c(B) = (-1)^{(e-5)(e-3)/8}\ (-1)^{(e-3)/2}\ (-1)^{(e-1)/2}\ (-1)$

$= +1$ since $(e - 5)(e - 3)/8 \equiv 0 \pmod 2$.

We shall now establish the result mentioned at the beginning of this section.

<u>Theorem 4.2</u>. Let F be an algebraic number field and let n be odd. There is a G/F symrep if and only if

(i) F is not formally real, or

(ii) F is formally real and G is totally real.

<u>Proof</u>. It suffices to consider (i) of Theorem 4.1. Let $\mathfrak{p}$ be a local prime spot of F. If $\mathfrak{p}$ is prime to 2, then Theorem 4.1 (i) can be satisfied by Lemma 4.2. Suppose $\mathfrak{p}$ divides 2. If Lemma 4.3 does not apply, it suffices, by Lemma 4.5, to find a $K/F_{\mathfrak{p}}$ symrep whenever $[K : F_{\mathfrak{p}}]$ is odd. As remarked before Theorem 1.1, if $K \supseteq H \supseteq F_{\mathfrak{p}}$ and K/H and $H/F_{\mathfrak{p}}$ symreps exist, then there is a $K/F_{\mathfrak{p}}$ symrep. Let H be the maximal inertial subextension of $F_{\mathfrak{p}}$. Apply Lemmas 4.6, 4.7, and 4.8.

V. THE RATIONAL INTEGRAL CASE

We now assume that $D = Z$, the integers. This case is more complex than the two previous special cases since D is no longer a field. Even when $n = 2$ many interesting questions arise. These are taken up in the next section.

Theorem 5.1. Let $\mathcal{U}^+$ and $\mathcal{U}^2$ be defined as in Theorem 2.5. The number of Δ/Z symreps in any given class is a multiple of $n!2^{n-1}$ and is bounded above by $n!2^{n-1}[\mathcal{U}^+ : \mathcal{U}^2] \leq n!4^{n-1}$. If $n \leq 7$ and a given class contains a Δ/Z symrep, then it contains exactly $n!2^{n-1}[\mathcal{U}^+ : \mathcal{U}^2]$. The total number of Δ/Z symreps is a finite multiple of $n!2^{n-1}$.

Proof. We shall apply Theorem 2.5. Let us determine $O_n(Z)$. Since $X \in O_n(Z)$ if and only if $XX' = I_n = X'X$, we have $\Sigma\, x_{ij}^2 = 1$ where the sum is over i or j. Since the elements of X lie in Z, every row and column of X has one nonzero entry, and this is ± 1. Clearly every such X is in $O_n(Z)$. Hence $|O_n(Z)| = n!2^n$. If m is the number of generators of infinite order of $\mathcal{U}$, the group of units of $\mathcal{R}(A)$, then $[\mathcal{U}^+ : \mathcal{U}^2] \leq 2^m$. By the Dirichelet Unit Theorem, $m \leq n - 1$. If $n \leq 7$, then $S(G,Z)$ holds (Theorem 2.1 (2)) and we may apply Theorem 2.5. The final statement is a consequence of the following:

(i) the number of symreps in each class is a finite multiple of $n!2^{n-1}$,

(ii) the number of symrep classes does not exceed the number of ideal classes in the order Δ,

(iii) the number of ideal classes in Δ is finite [1].

Let Γ be the ring of integers in G. When $n = 2$ there is a Γ/Z symrep if and only if there is a G/Q symrep (Corollary 6.1.1). It is natural to ask if this is true for all n. We do not know. Faddeev [3] has derived a partial result in this direction. (We rederive it below with a bound on the number of symreps.) The previous theory provides some tools for seeking a counterexample. Suppose that n is odd, G is totally real, the class number is odd, and $\Gamma = Z[\theta]$. By Theorem 4.2 a G/Q symrep exists. By Corollary 2.6.2 we have $|\mathfrak{J}| = 1$. By Lemma 2.1 it follows that $C((1)) \in \mathfrak{J}$. There is a Γ/Z symrep if and only if $C((1)) \in \mathfrak{P}$. By Theorem 2.3 the existence of a Γ/Z symrep implies that there is a unit $\eta \in \Gamma$ with $\eta f'(\theta)$ totally positive where $f(x)$ is the monic irreducible Q polynomial for θ.

<u>Theorem 5.2</u>. Assume that G is totally real, that Δ is the ring of integers in G, that $n \leq 7$, and that for any nonzero $\alpha \in \Delta$ we have a totally positive τ and an ideal $\mathfrak{a}$ with $\mathfrak{a}^2 = (\alpha\,\tau)$. Then the number of Δ/Z symreps is $n!2^{n+k-1}$ where $k \geq 0$ and 2^k divides the class number.

Proof. We shall use the notation of Theorems 2.5 and 2.6. Since the class of the field different has a square root [7, Thm. 176], we have $(\mathfrak{a}^{-1})^2 \sim (\mathfrak{a}^\circ \mathfrak{a})^{-1}$ for some ideal $\mathfrak{a}$. Thus $\mathfrak{a}^2 \sim \mathfrak{a}^\circ \mathfrak{a}$ and so $\mathfrak{a} \sim \mathfrak{a}^\circ$. Let $\mathfrak{a}^\circ = \alpha\mathfrak{a}$. Choose $\mathfrak{b}$ and τ such that τ is totally positive and $\mathfrak{b}^2 = (\alpha\,\tau)$. Then $C(\mathfrak{a}\mathfrak{b}) \in \mathfrak{P}$ since $(\mathfrak{a}\mathfrak{b})^\circ = \mathfrak{a}^\circ \mathfrak{b}^{-1} = \mathfrak{a}\mathfrak{b}/\tau$ by Lemma 2.3 (1). Since every ideal is an M-ideal and since $S(G,Z)$ holds (Theorem 2.1 (2)), it follows from Corollary 2.2.3 that every class in $\mathfrak{P}$ corresponds to a Δ/Z rep class containing symreps. For any Δ/Z rep A we have $\mathfrak{R}(A) = \Delta$. Since $|\mathfrak{P}| = |\mathfrak{J}|/|\mathfrak{S}|$, application of Theorem 4.1 shows that the number of symreps is $n!2^{n-1}\,[\mathfrak{U}^+ : \mathfrak{U}^2]\cdot|\mathfrak{J}|/|\mathfrak{S}|$. By Corollary 2.6.2 we have $|\mathfrak{J}| = 2^k$, the order of the maximum subgroup of type $(2,2,\ldots,2)$ of the ideal class group. Thus 2^k divides the class number.

We must show that $[\mathfrak{U}^+ : \mathfrak{U}^2] = |\mathfrak{S}|$. Let $\operatorname{sgn}\gamma$ be the vector whose i^{th} component lies in $GF(2)$ and is 0 if and only if $\gamma^{(i)} > 0$. Since the units $\mathfrak{U}$ of Δ form a group, $\operatorname{sgn}\mathfrak{U}$ is a subspace of $GF(2)^n$, say of dimension m. If t is the maximum number of generators of $\mathfrak{U}$ which can be chosen totally positive, then $2^t = [\mathfrak{U}^+ : \mathfrak{U}^2]$. However, $t + m$ is the number of generators of $\mathfrak{U}$, namely n by the Dirichelet Unit Theorem. Hence $[\mathfrak{U}^+ : \mathfrak{U}^2] = 2^{n-m}$. For a principal ideal (γ) let $\operatorname{sgn}(\gamma) = \{\operatorname{sgn}\delta : (\delta) = (\gamma)\}$. By the assumption of this theorem,

$$\bigcup_{\mathfrak{a} \in \mathfrak{S}} \operatorname{sgn}(\mathfrak{a}^2) = GF(2)^n .$$

If $\mathfrak{a}, \mathfrak{b} \in \mathfrak{S}$ and $\operatorname{sgn}(\mathfrak{a}^2) \cap \operatorname{sgn}(\mathfrak{b}^2) \neq \emptyset$, then $\mathfrak{a}^2 = \tau\mathfrak{b}^2$ for some totally positive τ and so $\mathfrak{a} = \mathfrak{b}$. Hence $2^n = |GF(2)^n| = \Sigma_{\mathfrak{a} \in \mathfrak{S}} |\operatorname{sgn}(\mathfrak{a}^2)| = |\mathfrak{S}| \cdot |\operatorname{sgn}\mathfrak{U}|$ since $\operatorname{sgn}(\gamma) = \{\operatorname{sgn}\gamma + \operatorname{sgn}\eta : \eta \in \mathfrak{U}\}$. This gives $|\mathfrak{S}| = 2^{n-m} = [\mathfrak{U}^+ : \mathfrak{U}^2]$.

VI. THE 2×2 RATIONAL INTEGRAL CASE

In view of Theorem 2.1 and Theorem 2.4, it is to be expected that when $D = Z$ and $n = 2$ the theory would be simpler. This is correct; in fact, completely new tools are available. One of these is continued fractions which can be used to study equivalence of ideals. By this means, previous results can be rederived for this special case. Our main use has been in a computer program, some results of which are given at the end of this section. A more fruitful tool is the Gaussian integers. They are suggested by the equation $c = u^2 + v^2$ in Theorem 2.4 and turn out to be a convenient device for stating results developed at the end of this section.

The first part of this section deals with concepts developed earlier and their application in the present case. Next Theorem 6.4 answers the following question. Let $\Delta_1 \subseteq \Delta_2$ both have the same quotient field, quadratic over the rational numbers. Let A be a Δ_1/Z symrep and $C_1(\mathfrak{a})$ the corresponding ideal class. Extending $\mathfrak{a}$ to a Δ_2 ideal gives a new class C_2 $(\mathfrak{A})$. Let $C_2(\mathfrak{A})$ correspond to $C_2(B)$. Does $C_2(B)$ contain a Δ_2/D symrep? If so, how does it relate to A? The final part of this section deals with a related problem: Let A be a Δ/D symrep. Find all symreps in $C(A)$. A complete answer is not known, but some general results are given which reduce the necessary calculations.

Lemma 6.1. If Δ/Z reps exist, then we may choose θ so that $\Delta = Z[\theta]$ and θ is a real algebraic integer.

Proof. The ring of integers in G has 1 and ω as a module basis with $\omega = \sqrt{m}$ or $\frac{1}{2} + \frac{1}{2}\sqrt{m}$. If any Δ/Z reps exist, $\Delta \subseteq Z[\omega]$ by Corollary 1.5.2. If no Δ/Z reps exist there is nothing to study. For any $\alpha \in \Delta$, $\alpha = a + b\omega$ where a and b are integers. Thus $a + b\omega \in \Delta$ if and only if $b\omega \in \Delta$. Let k be the greatest common divisor of all b's such that $b\omega \in \Delta$. We have $\Delta = Z[k\omega]$. Let $\theta = k\omega$. By Krakowski's condition, θ is real.

Because of this we shall assume that $\Delta = Z[\theta]$ where θ is a real algebraic integer.

Definition 6.1. Let $\tau(c)$ be the number of ordered pairs of integers (u,v) such that $u^2 + v^2 = c$.

The value of $\tau(c)$ is well known in elementary number theory. Assume c is a nonsquare. Write $c = 2^j \ell k$ where $\ell = \Pi\, p_i^{a_i}$ and the p_i are distinct primes congruent to 1 mod 4 and k is a product of primes congruent to 3 mod 4. If k is a nonsquare, $\tau(c) = 0$. If k is a square, $\tau(c) = 4\Pi(a_i + 1)$.

Theorem 6.1. Let θ satisfy $x^2 + ax + b = 0$. The number of Δ/Z symreps is

$\tau(a^2 - 4b)$ if a is even $\qquad \tau(a^2 - 4b)/2$ if a is odd.

Proof. Write $m = a^2 - 4b$. Since θ is a real integer, $m > 0$ and $a,b \in Z$. By Theorem 2.4 there are $\tau(m)$ $Z[\sqrt{m}\,]/Z$ symreps. Since $\Delta \supseteq Z[\sqrt{m}\,]$ it suffices to determine which $Z[\sqrt{m}\,]/Z$ symreps can be extended to Δ/Z symreps. Let the Z matrix $A \longleftrightarrow \sqrt{m}$. Then $B = (A - aI)/2 \longleftrightarrow \theta$. It suffices to determine when B has integer entries. If a is even, $a^2 - 4b$ is a multiple of 4. By Theorem 2.4, A has even entries. Thus B is a Z matrix. If a is odd so is $a^2 - 4b$. Then B is integral if and only if A has even off-diagonal elements. Since $u^2 + v^2 = v^2 + u^2$, this is true for exactly half of the $Z[\sqrt{m}\,]/Z$ symreps.

If existence is the only question we may use the following.

Corollary 6.1.1. There is a Δ/Z symrep if and only if there is a G/Q symrep.

Proof. Necessity follows from Theorem 1.1. To prove sufficiency let m be as above. By Theorem 2.4, m is the sum of two rational squares. It is known by elementary number theory that if an integer is the sum of two rational squares, then it is the sum of two integral squares. Hence $\tau(m) \neq 0$.

We now turn our attention to the number of symreps in a given class. This uses the concept of $\mathcal{R}(A)$ given in Definition 2.2.

Theorem 6.2. Let $C(A)$ be a class of Δ/Z reps such that $A' \in C(A)$.

(1) If $\mathfrak{R}(A)$ has a unit of norm -1, then $C(A)$ contains four symreps.

(2) If $\mathfrak{R}(A)$ has no unit of norm -1, then $C(A)$ contains zero or eight symreps.

Proof. Recalling that the units group is the direct product of a group of order 2 and an infinite cyclic group, and using Theorem 5.1 we see that it suffices to show that $C(A)$ contains at least one symrep in case (1). Let η be a unit of norm -1 in $\mathfrak{R}(A)$. Let $C(\mathfrak{a})$ correspond to $C(A)$. Since η is a unit in $\mathfrak{R}(A) = (\mathfrak{a} : \mathfrak{a})$, we have $\eta\mathfrak{a} = \mathfrak{a}$. Since $A' \in C(A)$, it follows by Theorem 1.5 that $\mathfrak{a} = \lambda\mathfrak{a}^\circ$ where $\lambda \in G$. One of $\pm\lambda$, $\pm\eta\lambda$ is totally positive. Call it τ. Then $\mathfrak{a} = \tau\mathfrak{a}^\circ$. By Corollary 2.2.3, $C(A)$ contains a Δ/Z symrep.

When Δ is the ring of integers in G we can characterize the classes containing Δ/Z symreps since Theorem 2.6 applies. This is done in the following theorem, which can be found in Taussky's work [18,19].

Theorem 6.3. Assume Δ is the ring of integers in G. Let $\mathfrak{J}$ and $\mathfrak{P}$ be as in Theorem 2.6. Every class in $\mathfrak{P}$ corresponds to a class containing a Δ/Z symrep. The set $\mathfrak{J}$ is a group under ideal class product.

(1) If Δ has a unit of norm -1, then $\mathfrak{J} = \mathfrak{P}$.

(2) If Δ has no unit of norm -1, then $\mathfrak{P} = \emptyset$ or $\mathfrak{J} - \mathfrak{P}$ is a subgroup of $\mathfrak{J}$ of index 2. In fact $\mathfrak{J} - \mathfrak{P}$ consists precisely of those classes containing self conjugate ideals.

Proof. By Corollary 2.2.3 every class in $\mathfrak{P}$ corresponds to a class with a Δ/Z symrep. By Lemmas 6.1 and 2.1, we have $C((1)) \in \mathfrak{J}$. Letting $\mathfrak{n} = (1)$ in Theorem 2.6 shows that $\mathfrak{J}$ is a group under ideal class product. By Theorem 1.5, we may apply the previous theorem to get that $\mathfrak{J} = \mathfrak{P}$ if there is a unit of norm -1.

Suppose Δ has no unit of norm -1. Assume that $\mathfrak{P} \neq \emptyset$. By Theorem 2.3 it follows that $C((1)) \notin \mathfrak{P}$. Since $|\mathfrak{S}|$ in Theorem 2.6 cannot exceed the number of distinct signatures of elements of G beginning $+$, we have $|\mathfrak{S}| \leq 2$ as $(+, +)$ and $(+, -)$ are the only possible such signatures. As $\mathfrak{P} \neq \mathfrak{J}$ we have $|\mathfrak{S}| > 1$. Hence $|\mathfrak{S}| = 2$. By the union expression of Theorem 2.6 and by Corollary 2.6.1, the properties of $\mathfrak{J} - \mathfrak{P}$ follow except the last.

Assume that $\mathfrak{R}(A)$ has no unit of norm -1. If $\mathfrak{a} = \overline{\mathfrak{a}}$, then $\mathfrak{a}^2 = \mathfrak{a}\overline{\mathfrak{a}} = N\mathfrak{a} \sim (1)$. Thus we have

$$\mathfrak{a} = (\mathfrak{a}\,\mathfrak{a}^\circ/(1)^\circ) \qquad \text{by Lemma 2.3 (1)}$$

$$= (N\mathfrak{a}/(1)^\circ)\ \mathfrak{a}^\circ = ((\theta - \overline{\theta})N\mathfrak{a})\ \mathfrak{a}^\circ \qquad \text{by Lemma 2.1.}$$

Since $N((\theta - \overline{\theta})N\mathfrak{a}) = -(\theta - \overline{\theta})^2(N\mathfrak{a})^2 < 0$ and Δ contains no unit of norm -1, it follows that $C(\mathfrak{a}) \in \mathfrak{J} - \mathfrak{P}$. Conversely, suppose $C(\mathfrak{a}) \in \mathfrak{J} - \mathfrak{P}$. Let $\mathfrak{a} = \lambda \mathfrak{a}^{\circ}$. Then

$$\mathfrak{a}/\bar{\mathfrak{a}} = \mathfrak{a}^2/\mathfrak{a}\bar{\mathfrak{a}} = \mathfrak{a}\lambda\mathfrak{a}^{\circ}/N\mathfrak{a} = (\lambda/N\mathfrak{a})\ (1)^{\circ} \quad \text{by Lemma 2.3 (1)}$$
$$= \lambda/((\theta - \bar{\theta})N\mathfrak{a}) \quad \text{by Lemma 2.1.}$$

Since G is real and $C(\mathfrak{a}) \in \mathfrak{J} - \mathfrak{P}$, we have $N\lambda < 0$ and $N(\theta - \bar{\theta}) = -(\theta - \bar{\theta})^2 < 0$. Hence for some totally positive $\mu \in G$, we have $\mathfrak{a}/\bar{\mathfrak{a}} = (\mu)$. Since $N\mathfrak{a} = N\bar{\mathfrak{a}}$, it follows that $N\mu = +1$. Let $G = Q(\sqrt{c}\,)$. Let $\bar{\alpha} = \sqrt{c}\,(1 - \mu)$, then $\bar{\alpha}/\alpha = -(1 - \mu)/(1 - \mu) = \mu$. Let $\mathfrak{b} = \alpha\mathfrak{a}$. Since $\mathfrak{a}/\bar{\mathfrak{a}} = \mu = \bar{\alpha}/\alpha$, it follows that $\mathfrak{b} = \bar{\mathfrak{b}}$. Clearly $\mathfrak{b} \in C(\mathfrak{a})$.

This concludes our specialization of the general theory. We now develop the Gaussian integers as a tool. They provide a more detailed correspondence than ideals - instead of class correspondence we have a correspondence of individual symreps to individual complex numbers which are Gaussian integers or half integers.

<u>Definition 6.2</u>. Let G be generated by $\sqrt{r}$ over Q where r is a nonsquare rational number. Assume that $\eta = q + \sqrt{r}$, with $q \in Q$, is an integer in G. Assume that a $Z[\eta]/Z$ symrep exists and let $\sqrt{r} \longleftrightarrow \begin{pmatrix} -b & a \\ a & b \end{pmatrix}$ in the extension of this representation. Then we say that the symrep corresponds to $\alpha = a + bi$.

For example, if $\eta = (1 + \sqrt{5}\,)/2 \longleftrightarrow \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$, then $\sqrt{5}/2 \longleftrightarrow \begin{pmatrix} -\frac{1}{2} & 1 \\ 1 & \frac{1}{2} \end{pmatrix}$ and $\alpha = 1 + i/2$. Note that the correspondence is one-to-one since specification of α determines the image of $\sqrt{r}$ and hence the symrep.

Lemma 6.2. The complex number α corresponds to a $Z[\eta]/Z$ symrep for some η if and only if

(1) $Re(\alpha) \in Z$,

(2) $2Im(\alpha) \in Z$, and

(3) $N\alpha$ is not a rational square. We have

We have that $\eta = k + 2N(\alpha) + \sqrt{N(\alpha)}$ for some $k \in Z$.

Proof. If $\alpha = a + bi$ satisfies (1) - (3), then $\begin{pmatrix} 0 & a \\ a & 2b \end{pmatrix}$ is a Z matrix corresponding to $b + \sqrt{N\alpha}$. It determines a symrep. Conversely, suppose $\eta = q + \sqrt{r}$. Then $2\sqrt{r} \in Z[\eta]$ and so $2Im(\alpha) \in Z$. Since $\eta = q + \sqrt{r}$ and $q \longleftrightarrow qI_2$, we have $Re(\alpha) \in Z$. Finally, $N\alpha = r$ so $N\alpha$ cannot be a rational square. Since $N\alpha = r$, we have $\eta = q + \sqrt{N\alpha}$. Since η is an integer, $q - 2N(\alpha) \in Z$.

Lemma 6.3. Let α correspond to a Δ/Z symrep A. The symreps equivalent to A under the elements of $O_2(Z)$ correspond to $\alpha, -\alpha, \bar{\alpha}, -\bar{\alpha}$. To get these symreps we may use $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, and $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ respectively.

Proof. By Theorem 5.1 we have $|O_2(Z)| = 8$.

Theorem 6.4. Let θ be a nonrational integer in G and $p \cdot a$

rational prime. Let $\Delta_1 = Z[\theta]$ and $\Delta_2 = Z[p\theta]$. Assume A is a Δ_2/Z symrep and let it correspond to α. Determine β as follows.

(i) If $\mathrm{Re}(\alpha/p) \in Z$, then $\beta = \alpha/p$.

(ii) If (i) does not apply, then there is a Gaussian prime π such that $N\pi = p$ and $\mathrm{Re}(\alpha/\pi^2) \in Z$. Let $\beta = \alpha/\pi^2$.

This β corresponds to a Δ_1/Z symrep B. Furthermore, if $C(A) \longleftrightarrow C(\mathfrak{a})$ and $C(B) \longleftrightarrow C(\mathfrak{B})$, then $C(\mathfrak{B})$ is the extension of $C(\mathfrak{a})$ to a Δ_1 ideal class.

Proof. We shall use small German letters for ideals in Δ_2 and capitals for ideals in Δ_1. Let $\mathfrak{A}$ be the extension of $\mathfrak{a}$ to a Δ_1 ideal. We shall let $\alpha = x + iy$ and $\beta = u + iv$ and $\theta = t + \sqrt{s}$ where $x,y,u,v,s,t \in Q$. If (i) applies, the theorem is clear. Assume that $\mathrm{Re}(\alpha/p) \notin Z$. We shall consider $p = 2$ and p odd separately.

Assume $p = 2$. Since (i) does not apply, $x \equiv 1(2)$ by Lemma 6.2 (1). Since θ is an algebraic integer, $4s \equiv 1$ or $0(4)$. However, $4s = N\alpha \equiv 1 + y^2(4)$. Thus y is even and $4s$ is odd. Then $\alpha/2i$ satisfies Lemma 6.2 (1) - (3) and so corresponds to a Δ_1/Z symrep. Since $2i = (1 + i)^2$, we have that $\beta = \pm\, \alpha/2i$. By Lemma 6.3 we may assume $\beta = \alpha/2i = (y - ix)/2$. Under the symrep A we have $2\sqrt{s} \longleftrightarrow \begin{pmatrix} -y & x \\ x & y \end{pmatrix}$. A characteristic vector for this matrix is $(x, y + 2\sqrt{s})$. By Theorem 1.5 we may assume $\mathfrak{a} = (x, y + 2\sqrt{s})$. In a similar fashion we have $\mathfrak{B} = (y, -x + 2\sqrt{s})$. Since

$\sqrt{s} + (x + y)/2 \in \Delta_1$, it follows that

$$\begin{aligned}\mathfrak{A} &= (x,(\sqrt{s} + (x + y)/2)2) = (x, \sqrt{s} + (x + y)/2) \quad \text{as } x \text{ is odd} \\ &\sim (x(x + y - 2\sqrt{s}), (N(x + y + 2\sqrt{s}))/2) \\ &= (x(x + y - 2\sqrt{s}),xy) \quad \text{since } x^2 + y^2 = 4s \\ &\sim (y,x + y - 2\sqrt{2}) = (y, -x + \sqrt{s}) = \mathfrak{B} .\end{aligned}$$

Assume that $p \neq 2$. We will show that π as described in (ii) exists. Since 2α is a Gaussian integer and $N(2\alpha) = 4s\cdot p^2$, there is a Gaussian integer γ such that $2\alpha/\gamma$ is a Gaussian integer and $N\gamma = p^2$. We may assume that $\gamma \equiv 1(2)$ since $N\gamma$ is odd. Then $2\alpha/\gamma \equiv 2\alpha(2)$. By Lemma 6.2 we have that $\beta = \alpha/\gamma$ corresponds to a Δ_1/Z symrep. Since $\gamma \equiv 1(2)$ and (i) does not apply, $\gamma \neq pi^k$ for any $k \in Z$. Thus, for some Gaussian prime π, we have $\gamma = \pi^2 i^k$ for some $k \in Z$. Since $\pi^2 \equiv 1(2)$, either $\gamma = \pi^2$ or $\gamma = -\pi^2$. By Lemma 6.3 we may assume that $\gamma = \pi^2$.

We must show that $C(\mathfrak{B}) = C(\mathfrak{A})$. As in the case $p = 2$, we have $\mathfrak{A} = (x,y + p\sqrt{s})$ and $\mathfrak{B} = (u,v + \sqrt{s})$. Our first goal is to show that we may assume $(x,2y) = 1$. It is known [8, p.v] that if ω is a quadratic integer over Q and $a,b,c \in Z$, then $(a,b + c\omega)'$ is an mbv for a $Z[\omega]$ ideal over Z if and only if $N(b + c\omega) \equiv 0(ac)$ and c divides (a,b). We shall use this below. Since (i) does not apply and $p \neq 2$, we can choose $\ell,m \in Z$ such that $\ell p + 2mx = 1$. Then $(x,\ell y + \sqrt{s})'$ is an mbv for $\mathfrak{A}$ since

(1) $\ell y + \sqrt{s} = m(2\sqrt{s})x + \ell(y + p\sqrt{s})$

(2) $y + p\sqrt{s} = p(\ell y + \sqrt{s}) + m(2y)x$

(3) $(\ell y)^2 - s \in Z$

(4)
$$\begin{aligned}(\ell y)^2 - s &= (1 - 2mx)^2 y^2/p^2 - s \\ &= (y^2 - p^2 s + mx(mx - 1)(2y)^2)/p^2 \\ &= (-x^2 + mx(mx - 1)(2y)^2)/p^2 \\ &\equiv 0 \pmod{x} \quad \text{as} \quad (x,p) = 1 \quad \text{and} \quad 2y, x \in Z .\end{aligned}$$

Let $k = (x,2y)$ and $c = s/k^2$. Since $c = (x/k)^2 + (y/k)^2$, the sum of two squares, and $4c \in Z$, one of $\sqrt{c}$ and $\sqrt{c} + 1/2$ is integral. Call it φ. Then $\underline{z} = (x/k, \ell y/k + \sqrt{c})'$ is an mbv for a $Z[\varphi]$ ideal since $(\ell y/k)^2 - c \in Z$ and

$$\begin{aligned}(\ell y/k)^2 - c &= (-(x/k)^2 + m(x/k)(m(x/k)-1)(2y)^2/p^2 \quad \text{by (4)} \\ &\equiv 0 \pmod{x/k}.\end{aligned}$$

We shall show that $\underline{w} = (u/k, v/k + \sqrt{c})'$ is an mbv for a $Z[\varphi]$ ideal. Since α/k satisfies Lemma 6.2 (1) - (3) and $(k,p) = 1$, it follows that β/k satisfies Lemma 6.2 (1) - (3). Thus β/k corresponds to a $Z[\varphi]/Z$ symrep E. A characteristic vector of E is $\underline{w}$. By Theorem 1.5 we have that $\underline{w}$ is an mbv for a $Z[\varphi]$ ideal. Since $\underline{z}$ and $\underline{w}$ are mbv's, the corresponding ideals are equivalent over $Z[\varphi]$ if and only if $\underline{z} = \mu T\underline{w}$ for some $\mu \in G$ and some Z unimodular matrix T. Multiplying by k we see that this implies the result stated in the theorem. Hence, it suffices to consider the case $(x,2y) = 1$.

Assume $(x,2y) = 1$. Clearly $(u,2v) = 1$ also. We will show that $\mathfrak{A}\,\overline{\mathfrak{A}} \sim (1)$ and $\mathfrak{B}\,\overline{\mathfrak{A}} \sim (1)$. Then $\mathfrak{B} \sim \mathfrak{B}\,\mathfrak{A}\,\overline{\mathfrak{A}} \sim \mathfrak{A}$, which will prove the theorem. First,

$$\begin{aligned}\mathfrak{A}\,\overline{\mathfrak{A}} &= (x^2, xy + xp\sqrt{s},\ xy - xp\sqrt{s},\ y^2 - p^2 s = -x^2)\\ &= x(x,2y,y + p\sqrt{s}\ ) = x(1,y + p\sqrt{s}\ )\\ &= (x) \quad \text{since} \quad y + p\sqrt{s} \in \Delta_1.\end{aligned}$$

Let $\pi = c + di$ and $\pi\beta = a + bi$ where $a,b,c,d \in Q$. Define $\lambda = a - d\sqrt{s}$. Since $a = uc - vd \equiv vd \pmod 1$ and $d^2 s = d^2(u^2 + v^2) \equiv (dv)^2 \pmod 1$ and $d \in Z$, we have $\lambda \in \Delta_1$. We shall show that $\mathfrak{B}\,\overline{\mathfrak{A}} = (\lambda)$. We have

$$\begin{aligned}\mathfrak{B}\,\overline{\mathfrak{A}} &= (x,y - p\sqrt{s}\ )(u,v + \sqrt{s}\ )\\ &= (xu,x(v + \sqrt{s}\ ),\ u(y - p\sqrt{s}\ ),\ (y - p\sqrt{s}\ )(v + \sqrt{s}\ ))\\ &= (\lambda\bar{\lambda},\lambda(b + c\sqrt{s}\ ),\lambda(b - c\sqrt{s}\ ),-\lambda^2).\end{aligned}$$

In a similar fashion to showing $\lambda \in \Delta_1$, we can show that $b + c\sqrt{s} \in \Delta_1$. Let $\mathfrak{C} = \mathfrak{B}\,\mathfrak{A}/\lambda$. Then

$$\begin{aligned}(1) \supseteq \mathfrak{C} &\supseteq ((2a,2b),a + d\sqrt{s},\ b + c\sqrt{s}\ )\\ &\supseteq ((2,2y),a + d\sqrt{s},\ b + c\sqrt{s}\ ) \quad \text{since } \pi(2\pi\beta) = 2\alpha \text{ shows}\\ &\qquad \text{that } (2a,2b) \text{ divides } (2x,2y) = (2,2y).\\ \text{(a)} &\quad = (1) \quad \text{if} \quad y \notin Z\\ \text{(b)} &\quad \supseteq (2,a + d\sqrt{s},\ b + c\sqrt{s}\ ) \quad \text{if} \quad y \in Z.\end{aligned}$$

We consider case (b). Since $\alpha = x + iy$ is a Gaussian integer and $p \neq 2$, it follows by assumption that $\beta = \alpha/\pi^2$ is a Gaussian integer.

Since $1 = (u,2v)$, we have that u is odd. Since $N\pi$ is odd, exactly one of c and d is odd.

(b-1) If c is odd, $b \equiv ud \equiv d \equiv 1 \pmod 2$ and so $\mathfrak{C} \supseteq (2,b) = (1)$.

(b-2) If d is odd, $a \equiv uc \equiv c \equiv 1 \pmod 2$ and so $\mathfrak{C} \supseteq (2,a) = (1)$.

Thus $\mathfrak{C} = (1)$.

We now turn our attention to the problem of find equivalent symreps.

Definition 6.3. If $B = TAT^{-1}$ for some $T \in O_2(Z)$, we say that A and B are *trivially equivalent*.

Let A be a symrep. There are four symreps trivially equivalent to A. They are given by Lemma 6.3. Let $\mathfrak{R}(A)$ be as in Definition 2.2. If $\mathfrak{R}(A)$ has a unit of norm -1, there are only these four trivial solutions to our problem by Theorem 6.2. On the other hand, if $\mathfrak{R}(A)$ has no unit of norm -1, there are eight symreps equivalent to A. We may divide these into two sets $\mathfrak{m}_1$ and $\mathfrak{m}_2$ such that $A \in \mathfrak{m}_1$ and the symreps in $\mathfrak{m}_i$ are all trivially equivalent for $i = 1,2$. Thus it suffices to find a $B \in \mathfrak{m}_2$. For this purpose we will introduce an $\mathfrak{R}(A)$ invariant called the conjugator. At present no method is known for finding it in all cases, except by solving the original problem. We shall list properties of the conjugator which make its speedy determination possible in many cases. A table of conjugators would be useful when a digital computor is not available.

The fact that the correspondence $A \longleftrightarrow \alpha$ does not always lead to Gaussian integers is somewhat troublesome. We can eliminate the problem by the following lemma.

Lemma 6.4. Let A and B be symreps corresponding to α and β respectively. Assume that $\mathcal{R}(A) = Z[(1+\sqrt{s}\,)k]$ where $s \in Z$. Then $\alpha_0 = 2i\alpha$ and $\beta_0 = 2i\beta$ determine symreps A_0 and B_0 which are equivalent if and only if A and B are equivalent and one equivalence is trivial if and only if the other is. Furthermore, $\mathcal{R}(A_0) = Z[\sqrt{s}\,]$.

Proof. We can assume A and B are images of $(1+\sqrt{s}\,)/2$. Since $\mathcal{R}(A) = Z[(1+\sqrt{s}\,)/2]$ we must have $Im(\alpha) \notin Z$. Hence $Re(2i\alpha)$ is odd. Thus $\mathcal{R}(C) = Z[\sqrt{s}\,]$. By Lemma 6.3, the trivial equivalences arise from multiplication by $+1$ and -1 and conjugation followed by such multiplication. Since $\pm 2i\delta = 2i(\pm\delta)$ and $\pm\overline{2i\delta} = 2i(\mp\overline{\delta})$ we see that $A \sim B$ is a trivial equivalence if and only if $A_0 \sim B_0$ is. If $A_0 \sim B_0$, then application of Theorem 6.4 gives $A \sim B$.

It remains to eliminate one possibility: $A \sim B$ is nontrivial and $A_0 \not\sim B_0$. Suppose this is the case. By Theorem 6.2, $\mathcal{R}(A)$ has no unit of norm -1. Since $\mathcal{R}(A_0) \subsetneqq \mathcal{R}(A)$, it follows that $\mathcal{R}(A_0)$ has no unit of norm -1. Thus there is a symrep E_0 which is nontrivially equivalent to A_0. If E_0 corresponds to ε_0, then by

Theorem 6.4 $\varepsilon_0/2i$ corresponds to a symrep. E equivalent to A. Since $A_0 \sim E_0$ is nontrivial, $A \sim E$ is nontrivial by the previous paragraph. Hence $B \sim E$ is trivial. Thus $B_0 \sim E_0$ and so $A_0 \sim E_0 \sim B_0$, a contradiction.

The method of applying Theorem 6.4 which we used above will prove useful in discussing the conjugator later. We now develop what is nearly a canonical form for α.

Lemma 6.5. Assume that the symrep A corresponds to a Gaussian integer α. If $\mathcal{R}(A)$ has no unit of norm -1, there are Gaussian integers μ and ν and a rational integer k such that

(i) $\alpha = k\mu\nu$,

(ii) $(N\mu, N\nu) = 1$,

(iii) $k\mu\bar{\nu}$ corresponds to a symrep nontrivially equivalent to A,

(iv) no rational prime divides $\mu\nu$.

If $k'\mu'\nu'$ is another such decomposition, then $k = \pm k'$ and either μ/μ' and ν/ν' are Gaussian units or μ/ν' and ν/μ' are Gaussian units.

Proof. Let $\alpha = i^a k \cdot \Pi\, \pi_j^{a_j}$ where $N\pi_j$ are distinct rational primes and $k \in Z$. Let $A \sim B$ be a nontrivial equivalence and let B correspond to $\beta = i^b m\, \Pi\, \pi_j'^{b_j}$. Without loss of generality $m,k > 0$. If $N\pi_j = 2$, we can assume $a_j = 0$ or 1 since $(1 + i)^2 = 2i$. The same remark applies to β. Under these conditions we shall show that

$k = m$. Since $(1/k)A$ is a Z matrix equivalent to $(1/k)B$, we have that β/k is a Gaussian integer. As $\Pi\, \pi_j'^{\,b_j}$ is divisible by no rational prime, k divides m. Similarly m divides k. Hence $k = m$. Since $N\alpha = -|A| = -|B| = N\beta$, it follows that the π_j' can be arranged so that $N\pi_j = N\pi_j'$ and $a_j = b_j$. Since the Gaussian units are powers of i, we may adjust b so that $\pi_j' = \pi_j$ or $\overline{\pi}_j$. Now let

$$\mu = i^a \prod_{\pi_j = \pi_j'} \pi_j^{a_j} \quad \text{and} \quad \nu = \prod_{\overline{\pi}_j = \pi_j'} \pi_j^{a_j} .$$

Then all properties but (iii) are satisfied. We have $k\mu\overline{\nu} = i^{a-b}\beta = i^c\beta$. Since $\nu \equiv \overline{\nu} \pmod 2$ we have that $i^{a-b}\beta/k \equiv \alpha/k \not\equiv 0 \pmod 2$. As $\Re(A) = \Re(B)$, an application of Lemma 6.2 to $\alpha/2k$ and $\beta/2k$ gives $\alpha/k \equiv \beta/k \pmod 2$. Thus we have two possibilities:

(a) $a - b \equiv 0$ (2)

(b) $a - b \equiv 1$ (2) and $\alpha \equiv 1 + i \pmod 2$.

We temporarily assume that the latter occurs. Then $1 + i$ divides $\mu\nu$ and hence μ or ν. If $1 + i$ divides μ, replace μ by $\mu/(1 + i)$ and ν by $\nu(1 + i)$. Since $\overline{(1 + i)} = i^3(1 + i)$, this reduces case (b) to case (a). If $1 + i$ divides ν, the situation is similar. In case (b) we have $k\mu\overline{\nu} = \pm\beta$ and we are done by Lemma 6.3.

The uniqueness question remains. By using (iv) and an argument similar to the one on m and k above, we see that k' divides k and k divides k'. Hence $k = \pm k'$. Thus $\mu'\overline{\nu}'$ is one of $\pm\,\mu\overline{\nu}$ and $\pm\,\overline{\mu\overline{\nu}}$ by Lemma 6.3 since there are only eight symreps equivalent to A.

Suppose $\mu'\overline{\nu}' = \pm\,\mu\overline{\nu}$. Since $\mu'\nu' = \pm\,\mu\nu$, we have $\mu'^2 N\nu' = \pm\,\mu^2 N\nu$. By (iv) no rational primes divide μ or μ'. Hence no odd rational primes divide μ^2 or μ'^2. Thus $r = N\nu'/N\nu$ is a power of two. By (iv), we have $r = 2^t$ for $t = -1, 0,$ or $+1$. Suppose $N\nu$ is odd and $N\nu'$ is even. Then $N\mu'$ is odd and we have

$$\begin{aligned} 1 &\equiv \mu'^2 \pmod 2 \\ &= \mu^2/2 = (\mu/(1+i))^2\, i \equiv i \pmod 2, \quad \text{a contradiction.} \end{aligned}$$

Similarly, $t \neq -1$. Hence $t = 0$. Thus $\mu^2 = \pm\,\mu'^2$ and so μ/μ' is a unit. Also, $\nu/\nu' = \pm\,\mu'/\mu$ is a unit.

Suppose $\mu'\overline{\nu}' = \pm\,\overline{\mu\overline{\nu}} = \pm\,\overline{\mu}\nu$, then the roles of μ and ν are reversed and we get that $\mu/\nu' = \pm\,\mu'/\nu$, a unit.

The following lemma makes it possible to define the conjugator.

Lemma 6.6. Let A and B be inequivalent Δ/Z symreps such that $\Re(A) = \Re(B)$, a ring with no unit of norm -1, and A corresponds to a Gaussian integer $\alpha = k\mu\nu$ where k, μ, ν are as in the previous lemma. Let B correspond to β. Then we may write $\beta = k\mu_0\nu_0$ where $N\mu = N\mu_0$ and $N\nu = N\nu_0$ and k, μ_0, ν_0 satisfy the previous lemma.

<u>Proof</u>. In general $\beta = k_0\mu_0\nu_0$. Since $\mathcal{R}(A) = \mathcal{R}(B)$, we may take $k_0 = k$ by combining the ± with μ_0. We may work with A/k and B/k, so it can be assumed that $k = 1$. Let $\mu = \lambda\eta$ and $\nu = \sigma\tau$ be such that $\beta = i^a\lambda\bar{\eta}\sigma\bar{\tau}$ (This can be done since $N\alpha = N\beta$.). By an argument like that of the previous lemma's proof we can show that λ,η,σ,τ can be chosen so that $i^a = \pm 1$. Since $\mathcal{R}(A) = \mathcal{R}(B)$, the norms of λ,η,σ,τ are pairwise prime.

By (γ,ε) we shall mean that for two symreps C and E corresponding to γ and ε we have $C \sim E$. We shall show that if ρ,φ,ψ are Gaussian integers with pairwise prime norms then $(\rho\varphi\psi,\rho\varphi\bar{\psi})$ implies $(\rho\bar{\varphi}\psi,\rho\overline{\varphi\psi})$. The desired result follows since $(\mu\nu,\mu\bar{\nu})$ implies $(\lambda\bar{\eta}\nu,\lambda\overline{\bar{\eta}\nu})$ implies $(\lambda\bar{\eta}\nu,\overline{\lambda\overline{\bar{\eta}\nu}} = \eta\nu\bar{\lambda})$ implies $(\lambda\bar{\eta}\sigma\bar{\tau},\eta\sigma\overline{\tau\lambda})$ implies $(\pm\lambda\bar{\eta}\sigma\bar{\tau}, \pm\lambda\overline{\eta\sigma}\tau)$ and we may let $\mu_0 = \pm\lambda\bar{\eta}$ and $\nu_0 = \sigma\bar{\tau}$. Define

$$f(\sigma) = \begin{pmatrix} \mathrm{Re}\,\sigma & -\mathrm{Im}\,\sigma \\ \mathrm{Im}\,\sigma & \mathrm{Re}\,\sigma \end{pmatrix} \text{ and } K = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

The matrix $f(\sigma)$ is a common means of representing the complex number σ. The following properties are easily shown.

(a) $f(\sigma\tau) = f(\sigma)f(\tau)$ and $f(\bar{\sigma}) = f(\sigma)'$

(b) $f(\sigma)K = Kf(\bar{\sigma})$

(c) $K^2 = I$

(d) $f(\sigma)K = \begin{pmatrix} -\mathrm{Im}\,\sigma & \mathrm{Re}\,\sigma \\ \mathrm{Re}\,\sigma & \mathrm{Im}\,\sigma \end{pmatrix}$.

Properties (a) - (c) will be used to establish identities. Property (d) links K and f to the correspondence between Gaussian integers and symreps (Definition 6.2). In terms of f and K our goal becomes:

> if ρ,φ,ψ are Gaussian integers with pairwise prime norms and T is a Z unimodular matrix and
>
> $$(*) \qquad Tf(\rho\varphi\psi)K = f(\rho\varphi\bar{\psi})KT \ ,$$
>
> then for some Z unimodular matrix S we have
>
> $$Sf(\rho\bar{\varphi}\psi)K = f(\rho\overline{\varphi\psi})KS \ .$$

We shall show that $S = f(\bar{\varphi})Tf(\varphi)/N\varphi$ is a solution. Clearly $|S| = |T| = \pm 1$ and

$$\begin{aligned} N\varphi \cdot Sf(\rho\bar{\varphi}\psi)K &= f(\bar{\varphi})Tf(\varphi)f(\rho\bar{\varphi}\psi)K \\ &= f(\bar{\varphi})Tf(\rho\varphi\psi)Kf(\varphi) \quad \text{by (a) and (b)} \\ &= f(\bar{\varphi})f(\rho\varphi\bar{\psi})KTf(\varphi) \quad \text{by } (*) \\ &= N\varphi \cdot f(\rho\overline{\varphi\psi})KS \quad \text{by (a) and (b).} \end{aligned}$$

We must show that S is a Z matrix. We have

$$\begin{aligned} N(\rho\psi)S &= N(\rho\psi)f(\bar{\varphi})Tf(\varphi)/N\varphi \\ &= f(\bar{\varphi})Tf(\rho\varphi\psi)f(\overline{\rho\psi})/N\varphi \quad \text{by (a)} \\ &= f(\bar{\varphi})Tf(\rho\varphi\psi)KKf(\overline{\rho\psi})/N\varphi \quad \text{by (c)} \\ &= f(\bar{\varphi})f(\rho\varphi\bar{\psi})KTKf(\overline{\rho\psi})/N\varphi \quad \text{by } (*) \\ &= f(\rho\bar{\psi})KTKf(\overline{\rho\psi}) \quad \text{by (a).} \end{aligned}$$

Thus $N(\rho\psi)S$ and $N(\varphi)S$ are Z matrices. Since $N(\rho\psi)$ and $N\varphi$ are relatively prime, S is a Z matrix.

Suppose that $s \in Z$ and that for some symrep A we have $Z[\sqrt{s}\,] = \mathfrak{R}(A)$. Assume that $\mathfrak{R}(A)$ has no unit of norm -1. Let $A \longleftrightarrow \alpha = k\mu\nu$ where k,μ,ν satisfy Lemma 6.5 (i) - (iv). Then $s = -N\sqrt{s} = -|A/k| = N\mu\nu$. By Lemmas 6.5 and 6.6, the set $\{N\mu, N\nu\}$ is a unique function of s. Since $(N\mu, N\nu) = 1$, this set is determined by s and the primes dividing $N\mu$. We are thus led to make the following definition.

<u>Definition 6.4.</u> Let $s \in Z$ and suppose $Z[\sqrt{s}\,] = \mathfrak{R}(A)$ for some symrep A. Then the <u>conjugator of</u> s, written $\kappa(s)$, is defined as follows. Write $s = \Pi\, p_i^{a_i}$ where $a_i > 0$ and the p_i are distinct rational primes. Let $c = \Pi\, p_i$.

(1) If $\mathfrak{R}(A)$ has a unit of norm -1, then $\kappa(s)$ is the set $\{1,c\}$.

(2) If $\mathfrak{R}(A)$ has no unit of norm -1, let $A \longleftrightarrow \alpha = k\mu\nu$ where k,μ,ν satisfy Lemma 6.5 (i) - (iv). Then $\kappa(s)$ is the set $\{(c,N\mu),(c,N\nu)\}$.

By the discussion preceding the definition, $\kappa(s)$ depends only on s and not on A. We wish to know when $\kappa(s)$ is defined. By Lemma 6.5 (iv) and the fact that $s = N\mu\nu$, it is clear that $\kappa(s)$ is defined if and only if s is the sum of two relatively prime squares. As $(1 + i)^2 = 2i$ and rational primes congruent to 3 modulo 4 are

Gaussian primes, it follows that $\kappa(s)$ is defined if and only if s is a product of primes congruent to 1 modulo 4 or twice such a product.

If a table of $\kappa(s)$ were available for s of the above form, then for a given symrep A one could find all equivalent symreps. Later we shall determine properties of $\kappa(s)$ which would be useful in the construction and extension of such tables.

The following procedure illustrates the use of such tables. Let A be the given symrep.

1. Let $t = \operatorname{tr} A$ and $h = (2a_{12}, a_{11} - a_{22})$ and $B = (2A - tI)/h$. (We have that $\mathfrak{R}(A)$ is isomorphic to $Z[B]$ or $Z[(B + I)/2]$. In the latter case, Lemma 6.4 can be used.)
2. Let $s = -|B|$ and $\alpha = b_{12} + ib_{22}$.
3. If $1 \in \kappa(s)$, the only equivalences are the trivial ones. These are given by Lemma 6.3.
4. Assume $1 \notin \kappa(s)$. Let $p_1 \ldots p_k \in \kappa(s)$. It is usually best to choose the element of $\kappa(s)$ with the lesser number of prime factors.
5. For each p_j find $x, y \in Z$ with $x^2 + y^2 = p_j$. If p_j divides $xb_{12} + yb_{11}$, let $\pi_j = x + iy$; otherwise, let $\pi_j = x - iy$. If the highest power of p_j dividing s is the n_jth, define $f + ig = \alpha \Pi \pi_j^{2n_j} / \Pi p_j^{n_j}$.
6. Let $E = \begin{pmatrix} -g & f \\ f & g \end{pmatrix}$. Then $(hE + tI)/2$ is nontrivially

equivalent to A.

A knowledge of the conjugator and the factorization of α into Gaussian primes is sufficient to find equivalent symreps. In order to find the unimodular transformation used to achieve the equivalence, it is also necessary to solve a diophantine equation. The next theorem proves this.

Theorem 6.5. Let A be a symrep corresponding to a Gaussian integer $\alpha = k\mu\nu$ where k,μ,ν satisfy Lemma 6.5 (i), (ii), and (iv). Condition (iii) of Lemma 6.5 is satisfied if and only if

$$(N\mu)x^2 - (N\nu)y^2 = \pm t^2 \quad \text{for some} \quad x,y \in Z ,$$

where $t = 1$ if $\mathcal{R}(A)$ is of the form $Z[\sqrt{s}\,]$, and $t = 2$ otherwise. The matrix

$$T = \frac{x}{t}\begin{pmatrix} -\operatorname{Im}\mu & \operatorname{Re}\mu \\ \operatorname{Re}\mu & \operatorname{Im}\mu \end{pmatrix} + \frac{y}{t}\begin{pmatrix} \operatorname{Re}\nu & \operatorname{Im}\nu \\ -\operatorname{Im}\nu & \operatorname{Re}\nu \end{pmatrix}$$

is Z unimodular and TAT^{-1} corresponds to $k\mu\overline{\nu}$.

Proof. Let f and K be as in the proof of Lemma 6.6. Then $A = f(k\mu\nu)K$. Let T be a nonsingular Q matrix. We have

$$(*) \qquad TAT^{-1} = kf(\mu\overline{\nu})K$$

if and only if $(f(\nu)T)A = f(\nu)kf(\mu)Kf(\nu)T = A(f(\nu)T)$. Thus $(*)$ holds if and only if $f(\nu)T$ is a polynomial in A. Let A correspond to $r + \sqrt{q}$ where $r,q \in Q$. Then $(A - rI)^2$ is scalar. Hence (*) holds if and only if $f(\nu)T = uA + vI$ for some $u,v \in Q$. This is equivalent to

$$\begin{aligned} T &= (ku)f(\mu)K + (v/N\nu)f(\bar{\nu}) \\ &= wf(\mu)K + zf(\bar{\nu}) \quad \text{for some } w,z \in Q. \end{aligned}$$

We have $|T| = (N\nu)z^2 - (N\mu)w^2$. Thus T is a Z unimodular matrix such that TAT^{-1} corresponds to $k\mu\bar{\nu}$ if and only if

(i) $T = xf(\mu)K/t + yf(\bar{\nu})/t$,

(ii) $(N\mu)x^2 - (N\nu)y^2 = \pm t^2$, and

(iii) $x,y \in Q$ and T is a Z matrix.

We must show that (iii) is equivalent to $x,y \in Z$.

Suppose $x,y \in Z$. If $t = 1$, then (iii) holds. If $t = 2$, then $\mathfrak{R}(A)$ is of the form $Z[(1 + \sqrt{s})/2]$. By Lemma 6.2 and $(\mu\nu,2) = 1$ (Lemma 6.5 (iv)) we have $\mu\nu \equiv i(2)$. Hence $\mu\nu^2 \equiv i\nu(2)$. Since $\nu^2 \equiv N\nu \equiv 1\ (2)$, we have $\mu \equiv i\nu(2)$. As $N\mu$ and $N\nu$ are odd, (ii) gives $x \equiv y\ (2)$. Thus $2T \equiv 0\ (2)$ and so (iii) holds.

Suppose (iii) holds. Then

$$(\pm\, x\cdot\text{Im}\,\mu + y\cdot\text{Re}\,\nu)/t \in Z \quad\text{and}\quad (x\cdot\text{Re}\,\mu \pm y\cdot\text{Im}\,\nu)/t \in Z\ .$$

Hence $2x\cdot\text{Im}\,\mu/t \in Z$ and $2x\cdot\text{Re}\,\mu/t \in Z$. By Lemma 6.5 (iv), we have $2x/t \in Z$. Similarly, $2y/t \in Z$. If $t = 2$, we are done. Suppose

$t = 1$. Then $2x, 2y \in Z$. If $x \in Z$, then $y \cdot \mathrm{Re}\,\nu \in Z$ and $y \cdot \mathrm{Im}\,\nu \in Z$ and so $y \in Z$. Similarly, if $y \in Z$ then $x \in Z$. Assume $x, y \notin Z$. Then $0 \equiv 2\,(x \cdot \mathrm{Im}\,\mu + y \cdot \mathrm{Re}\,\nu) \pmod 2 \equiv \mathrm{Im}\,\mu + \mathrm{Re}\,\nu$ and $0 \equiv \mathrm{Re}\,\mu + \mathrm{Im}\,\nu \pmod 2$. Thus $\mathrm{Re}(\mu\nu) = \mathrm{Re}\,\mu \cdot \mathrm{Re}\,\nu - \mathrm{Im}\,\mu \cdot \mathrm{Im}\,\nu \equiv 0 \pmod 2$. Hence by Lemma 6.5 (iv) we have $\mu\nu \equiv i(2)$. Thus $\mathcal{R}(A)$ is of the form $Z[(1+\sqrt{s}\,)/2]$ by Lemma 6.2. This contradicts $t = 1$.

It is interesting to note that the uniqueness of $\kappa(s)$ shows that $x^2 d - y^2(s/d) = \pm t^2$ with t as in the theorem and d a divisor of s with $d < \sqrt{s}$ is solvable for $d = 1$ and at most one other d. Actually, it can be shown (by means of the fact that $1 \in \kappa(s)$ if and only if there is a unit of norm -1 in $Z[\sqrt{s}\,]$) that exactly two of $x^2 d - y^2(s/d) = +1$ are solvable where d ranges over all divisors of s.

This theorem provides one means of finding the conjugator, but it seems rather hard to use. The next theorem lists some properties of $\kappa(s)$ which would be useful in generating a table of s versus $\kappa(s)$.

<u>Theorem 6.6</u>. Let $m, s \in Z$ be such that $\kappa(m^2 s)$ and $\kappa(s)$ are defined.

(1) If $1 \in \kappa(m^2 s)$, then $1 \in \kappa(s)$.

(2) $\kappa(m^3 s) = \kappa(ms)$.

(3) If p is a prime congruent to 1 modulo 4 and p does not divide s and $\kappa(s) = \{a, b\}$, then $\kappa(p^2 s)$ is one of $\{ab, p\}$, $\{a, pb\}$, $\{b, ap\}$.

(4) If $\kappa(s) = \{ab,c\}$ where the prime factors of a divide s exactly to an odd power and those of b divide s exactly to an even power, then $(a|p) = +1$ for all odd primes p dividing c.

(5) $1 \in \kappa(s)$ if and only if the continued fraction for $\sqrt{s}$ has odd period.

<u>Proof</u>. (1). Since $1 \in \kappa(t)$ if and only if $Z[\sqrt{t}\,]$ has a unit of norm -1 and since $Z[\sqrt{m^2 s}\,] \subseteq Z[\sqrt{s}\,]$, the result is clear.

We shall apply Theorem 6.4. Suppose $\kappa(p^2 s) = \{a,bp\}$ with $a \neq 1$. If p divides s, Theorem 6.4 shows that $\{a,bp\} = \kappa(s)$. If p is prime to s, then $\kappa(s) = \{a,b\}$ or $b = 1$.

(2). If $1 \in \kappa(a^3 s)$, use (1). If $1 \notin \kappa(a^3 s)$, the previous paragraph applies.

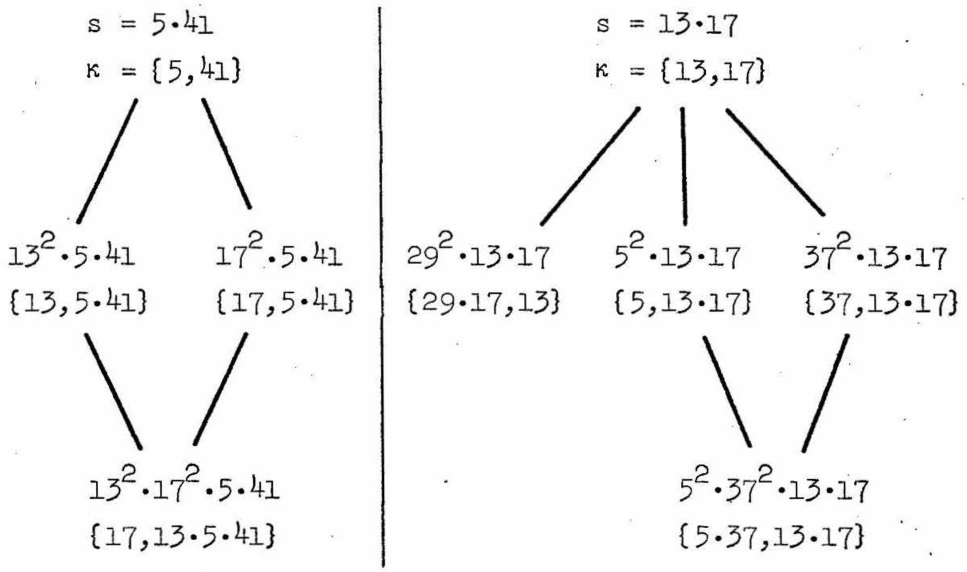
(3). If $1 \in \kappa(p^2 s)$, use (1). If $1 \notin \kappa(p^2 s)$, the above paragraph applies.

(4). We use Theorem 6.5. Since $(N\mu,N\nu) = 1$ and $(-1|p) = +1$ the result easily follows.

(5). It is well known that the continued fraction for $\sqrt{s}$ has odd period if and only if $Z[\sqrt{s}\,]$ has a unit of norm -1.

When $s < 10{,}000$, a table of the continued fraction expansion for $\sqrt{s}$ is available [13]. By this table and (5) of the theorem, it can be determined if $1 \in \kappa(s)$.

Let $p_1,\ldots,p_k$ be distinct primes congruent to 1 modulo 4 and prime to $s \in Z$. Assume $\kappa(s)$ is defined. We shall discuss the possibility of determining $\kappa(p_1^2\ldots p_\ell^2 s)$ in terms of the ℓ sets $\kappa(p_1^2\ldots p_\ell^2 s/p_i^2)$ $(1 \leq i \leq \ell)$. The discussion relies on (1) - (3) of the theorem. When $\ell = 3$ (and hence when $\ell > 3$), the value of $\kappa(p_1^2\ldots p_\ell^2 s)$ can be uniquely determined. As a matter of fact, two of $\kappa(p_1^2 p_2^2 s)$, $\kappa(p_1^2 p_3^2 s)$ and $\kappa(p_2^2 p_3^2 s)$, appropriately chosen, suffice to determine $\kappa(p_1^2 p_2^2 p_3^2 s)$. Our table is organized accordingly. When $\ell = 2$, an ambiguity arises in one of the six possible cases. An example shows that this ambiguity cannot be resolved only by knowing the form of $\kappa(p_1^2 s)$ and $\kappa(p_2^2 s)$. When $\ell = 1$, we cannot decide any of the cases. Examples are given. At times Theorem 6.6 (4) may be used to resolve such ambiguities; for example, since $(17/29) = -1$ and $\kappa(13\cdot17) = \{13,17\}$, we have $\kappa(29^2\cdot13\cdot17) = \{29\cdot17,13\}$. Theorem 6.6 (5) can also be used; for example, we see from [13] that the continued fraction for $\sqrt{5^2\cdot29}$ has even period and so $\kappa(5^2\cdot29) = \{5,29\}$. Many of the examples given below were found by an IBM 7094 using the continued fraction approach to ideal equivalence (see [8]). The program's running time per case is on the order of one second or less. Our main examples come from two distinct G's in which various integral domains were used. They are



In what follows we shall let $p_1 = p$, $p_2 = q$, and $p_3 = r$. We shall assume that a,b,c are all different from 1.

$\ell = 1$

$\kappa(s)$	$\kappa(p^2s)$	example
$\{1,a\}$	$\{1,pa\}$	$5^2\cdot 13$
	$\{p,a\}$	$5^2\cdot 29$
$\{a,b\}$	$\{p,ab\}$	$5^2\cdot 13\cdot 17$
	$\{pa,b\}$	$29^2\cdot 13\cdot 17$
	$\{pb,a\}$	

$\ell = 2$

$\kappa(p^2s)$	$\kappa(q^2s)$	$\kappa(p^2q^2s)$	
{1,pa}	{1,qa}	{1,pqa}	
{1,pa}	{q,a}	{pa,q}	
{p,a}	{q,a}	{pq,a}	ex. $5^2 \cdot 37^2 \cdot 13 \cdot 17$
		{p,qa}	ex. $13^2 \cdot 17^2 \cdot 5 \cdot 41$
		{q,pa}	
{p,a}	{qb,c}	{p,qa}	bc = a
{pa,b}	{qa,b}	{pqa,b}	
{pa,b}	{qb,a}	{pa,qb}	

The table for $\kappa(p^2s)$ clearly lists all possibilities which agree with Theorem 6.6(3). The table for $\kappa(p^2q^2s)$ lists all possible $\kappa(p^2s)$, $\kappa(q^2s)$ pairs except $\kappa(p^2s) = \{qb,c\}$ with bc = a. This cannot occur; for suppose $\kappa(p^2q^2s) = \{qx,y\}$. Then $\{x,y\} = \kappa(p^2s)$ or {1,pa} by Theorem 6.6 (3). Since $\kappa(p^2s) = \{1,pa\}$, we have $x = 1$, $y = pa$ or $x = pa$, $y = 1$. The former gives $\kappa(p^2q^2s) = \{q,pa\}$, so $\kappa(q^2s) = \{q,a\}$ which is impossible. The latter gives $\kappa(p^2q^2s) = \{pqa,1\}$ which is impossible by Theorem 6.6 (1). To evaluate $\kappa(p^2q^2s)$ for the remaining entries proceed as in the following example. Let $\kappa(p^2s) = \{1,pa\}$, $\kappa(q^2s) = \{q,a\}$. By Theorem 6.6 (3) one of the elements in $\kappa(p^2q^2s)$ is divisible by pa. Thus $\kappa(p^2q^2s) = \{1,pqa\}$ or $\{pa,q\}$. The former contradicts Theorem 6.6 (1).

$\ell = 3$

$\kappa(p^2q^2s)$	$\kappa(p^2r^2s)$	$\kappa(p^2q^2r^2s)$	$\kappa(q^2r^2s)$*	Case
$\{1,pqa\}$	$\{1,pra\}$	$\{1,pqra\}$	$\{1,qra\}$	I
$\{1,pqa\}$	$\{pa,r\}$	$\{r,pqa\}$	$\{r,qa\}$	I
$\{p,qa\}$	$\{p,ra\}$	$\{p,qra\}$	——	II
$\{p,qa\}$	$\{pr,a\}$	$\{pr,qa\}$	$\{r,qa\}$	II
$\{p,qa\}$	$\{pa,r\}$	$\{pqa,r\}$	$\{r,qa\}$	II
$\{pa,qb\}$	$\{pa,rb\}$	$\{pa,qrb\}$	$\{a,qrb\}$	V
$\{pa,qb\}$	$\{pra,b\}$	$\{pra,qb\}$	$\{ra,qb\}$	IV
$\{pq,a\}$	$\{pr,a\}$	$\{pqr,a\}$	$\{qr,a\}$	III
$\{pqa,b\}$	$\{pra,b\}$	$\{pqra,b\}$	$\{qra,b\}$	IV

* determined from $\kappa(p^2q^2r^2s)$

The calculations for $\ell = 3$ are more complicated than for $\ell = 1,2$; therefore they are presented in detail. The procedure is to use Theorem 6.6 and $\kappa(p^2q^2s)$ to determine all possible values for $\kappa(p^2r^2s)$. Those values which can be listed under a previous case by permuting p, q, and r are then rejected. For each value of $\kappa(p^2r^2s)$ that results, Theorem 6.6 is used to determine $\kappa(p^2q^2r^2s)$.

I $1 \in \kappa(p^2q^2s)$.

Let $\kappa((pqr)^2s) = \{rx,y\}$. Then $1 \in \{x,y\}$ by Theorem 6.6 (3). If $y = 1$, then $1 \in \kappa(p^2r^2s)$ by Theorem 6.6 (1). If $y \neq 1$, then

$x = 1$ and $\kappa(p^2q^2r^2s) = \{r,pqa\}$ and so $\kappa(p^2r^2s) = \{r,pa\}$.

II $\kappa(p^2q^2s) = \{p,qa\}$.

Let $\kappa(p^2r^2s) = \{px,y\}$. Since $\kappa(p^2s) = \{p,a\}$, dividing r out of $\{px,y\}$ gives $\{1,pa\}$ or $\{p,a\}$. In the former case, $y = 1$ (cas I) or r. In the latter case $y = a$ or ra. Let $\kappa(pqr)^2s) = \{pu,v\}$. Using $\kappa(p^2q^2s)$ gives $v = 1$ (impossible), r, qa, or qra. This gives the following array of $\kappa((pqr)^2s)$ possibilities versus $\kappa(p^2r^2s)$ possibilities.

		$\kappa((pqr)^2s)$		
		$\{pqa,r\}$	$\{pr,qa\}$	$\{p,qra\}$
$\kappa(p^2r^2s)$	$\{pa,r\}$		out	out
	$\{pr,a\}$	out		out
	$\{p,ra\}$	out	out	

We have eliminated cases by using $\kappa((pqr)^2s)$ to get $\kappa(p^2r^2s)$. The remaining cases are listed in the table for $\ell = 3$.

III $\kappa(p^2q^2s) = \{pq,a\}$.

Let $\kappa(p^2r^2s) = \{px,y\}$. Since $\kappa(p^2s) = \{p,a\}$ we have $y = 1$ (case I), r (case II), a, or ra (case II). Thus $\kappa(p^2r^2s) = \{pr,a\}$. Let $\kappa((pqr)^2s) = \{pu,v\}$. Using $\kappa(p^2q^2s)$ gives $v = 1$ (impossible), a, r, ra. Using $\kappa(p^2r^2s)$ similarly gives $v = a,q$, or qa. Thus $v = a$ and so $\kappa((pqr)^2s) = \{pqr,a\}$.

IV $\kappa(p^2q^2s) = \{pqa,b\}$.

Let $\kappa(p^2r^2s) = \{px,y\}$. Using $\kappa(p^2s) = \{pa,b\}$ gives $y = 1$ (case I), r (case II), b, rb. Let $\kappa(pqr)^2s) = \{pu,v\}$. Using $\kappa(p^2q^2s)$ gives $v = 1$ (impossible), r,b,rb.

A. If $\kappa(p^2r^2s) = \{pra,b\}$, then $v = 1,q,b,qb$. By the above values for v, we have $v = b$.

B. If $\kappa(p^2r^2s) = \{pa,rb\}$, then $v = 1,q,rb,qrb$. By the above values for v, we have $v = rb$.

V $\kappa(p^2q^2s) = \{pa,qb\}$.

Let $\kappa(p^2r^2s) = \{px,y\}$. We get $y = 1$ (case I), r (case II), b (case IV), or rb. Thus $\kappa(p^2r^2s) = \{pa,rb\}$. Let $\kappa(p^2q^2r^2s) = \{pu,v\}$. Then $v = 1$ (impossible), r,qb, or rqb and also $v = 1$, q,rb, or rqb. Thus $y = rqb$.

APPENDIX

The notation is that given in Definition 4.1. The purpose of the Appendix is to collect the theorems needed in Section IV. In all cases proofs or references are given; however, the results can be found in other places as they are rather well known in the areas to which they belong.

Theorem A (Hilbert symbol). Let H be a local field at the prime spot $\mathfrak{p} = (\pi)$ and let $a,b,c \in H^*$. Then

(1) $(a,bc) = (a,b)(a,c)$ by [12,57:10];

(2) $(a,ab) = (a,-b)$ by [12,57:10];

(3) if $a \notin H^2$, there is an $x \in H^*$ such that $(a,x) = -1$ by [12,63:13];

(4) if $f(H(\sqrt{a})/H) = 2$, then $(a,\pi) = -1$ by [12,63:3 and 63:11a];

(5) if π is prime to 2 and a and b are local units then $(a,b) = +1$ by [12,63:12];

(6) if $a/b \equiv 1 \pmod{4\pi}$, then $a \in bH^2$ and $(a,c) = (b,c)$ by [12,63:1].

Theorem B (Hasse symbol). Let A and B be nonsingular symmetric matrices over a local field H. Let A be $a \times a$ and B be $b \times b$. Then

(1) $A \cong B$ if and only if $c(A) = c(B)$ and $a = b$ and $|AB| \in H^2$ by [12, 63:20];

(2) $c(A \oplus B) = c(A)c(B)(|A|,|B|)$ by [12,58:3];

(3) $c(cA) = c(A)(c,(-1)^{a(a+1)/2}|A|^{a+1})$ when $c \in H^*$ by [12,58:3];

(4) $c(A \otimes B) = c(A)^b c(B)^a (-1,|A|)^{b(b-1)/2}(-1,|B|)^{a(a-1)/2} \cdot$
$(|A|,|B|)^{ab+1}$;

(5) if the prime spot of the field does not divide $2|A|$ and the elements of A are local integers, then $c(A) = +1$ by [12,92:1];

(6) if $A_i = (a_{jk})$, $1 \leq j, k \leq i$, then $c(A) = \Pi_{i<a} (|A_i|,-|A_{i+1}|) \cdot$ $(|A_a|,-1)$ if no $|A_i| = 0$ by [9, p.32];

(7) if K is an extension of H of odd degree and $|A| \in H^{*2}$, then $c(A/H) = c(A/K)$.

Proof. (4). Write $(i,j) \leq (i',j')$ if $i < i'$, or $i = i'$ and $j \leq j'$. Then $c(A \otimes B) = \Pi_{(i,j) \leq (k,\ell)} (a_i b_j, a_k b_\ell)$ where $A \cong \Sigma \oplus a_i$ and $B \cong \Sigma \oplus b_i$. By Theorem A (1) we have $(a_i b_j, a_k b_\ell) =$ $(a_i,a_k)(a_i,b_\ell)(a_k,b_j)(b_j,b_\ell)$. Splitting the product into the parts $i < k$ and $i = k$ gives

$$c(A \otimes B) = \Big(c(A) \prod_i (a_i,a_i)\Big)^{b^2} \Big(\prod_{i<k} (a_i,|B|)\,(a_k,|B|)\Big)^b$$

$$(|B|,|B|)^{a(a-1)/2}$$

$$\prod_i (a_i,a_i)^{b(b+1)/2} \cdot \prod_{j \leq \ell} (|A|,b_\ell)(|A|,b_j) \cdot c(B)^a .$$

By Theorem A (2) we get

$$c(A \otimes B) = c(A)^{b}\ (-1,|A|)^{b}\ (|A|,|B|)^{(a-1)b}\ (-1,|B|)^{a(a-1)/2}$$

$$(-1,|A|)^{b(b+1)/2}\ (|A|,|B|)^{b+1}\ c(B)^{a}\ .$$

(7). Let $B = A \oplus I_3$. By (2) of this theorem, $c(A) = c(B)$. By Theorem E we have two possibilities:

(i) $B \cong I \oplus -\varepsilon \oplus \pi \oplus -\varepsilon\,\pi\ (H)$ where $(\pi) = \mathfrak{p}$ is the prime ideal of H and ε is a $\mathfrak{p}$-adic unit with $H(\sqrt{\varepsilon}\,)$ quadratic unramified over H;

(ii) $B \cong I \oplus -1 \oplus 1 \oplus -1\ (H)$.

In these cases we have over any field containing H

(i) $c(B) = (-\varepsilon,\varepsilon\,\pi)(-\varepsilon\,\pi,-1)(1,-1) = (-1,-1)(\varepsilon,-\pi)$;

(ii) $c(B) = (-1,-1)$.

By Theorem A (4) we have $(\varepsilon,-\pi/H) = -1$. Since $f(K/H)$ is odd, $f(K(\sqrt{\varepsilon}\,)/K) = 2$. Let $e = e(K/H)$ and let Π be a prime of K, then $(\pi) = (\Pi)^{e}$ over K. By Theorem A (4) we have $(\varepsilon,-\pi/K) = (\varepsilon,\Pi/K)^{e} = (-1)^{e} = -1$ since e is odd. Thus

(i) $c(B/H) = -\ (-1,-1)$ $\qquad$ $c(B/K) = -\ (-1,-1)$;

(ii) $c(B/H) = \ \ (-1,-1)$ $\qquad$ $c(B/K) = \ \ (-1,-1)$.

Since $c(I_4) = +\ 1$, whichever of (i) and (ii) covers $B = I_4$ shows that $(-1,-1/H) = (-1,-1/K)$.

Theorem C. Let A be a symmetric matrix over a global field H. Assume $|A| \neq 0$. Then $\Pi\, c(A/H_{\mathfrak{p}}) = +1$ where the product runs over all prime spots $\mathfrak{p}$ on H (including the infinite ones). [12, p.190].

Theorem D (Hasse-Minkowski). Let A and B be symmetric matrices over a global field H. Assume A and B have the same dimensions and $|AB| \neq 0$. Then $A \cong B\ (H)$ if and only if

(1) $|AB| \in H^2$,

(2) $c(A/H_{\mathfrak{p}}) = c(B/H_{\mathfrak{p}})$ for all local prime spots $\mathfrak{p}$ on H,

(3) $\text{ind}(A/H_{\mathfrak{p}}) = \text{ind}(B/H_{\mathfrak{p}})$ at all real prime spots $\mathfrak{p}$ on H where $\text{ind}(A/H_{\mathfrak{p}})$ is the number of $a_i > 0$ in $A \cong \Sigma \oplus a_i (H_{\mathfrak{p}})$. [12, p.189].

Theorem E. Let H be a local field with prime spot $\mathfrak{p} = (\pi)$. Let ε be a unit in H such that $f(H(\sqrt{\varepsilon}\,)/H) = 2$. Exactly one of the following holds for a nonsingular symmetric H matrix A of dimension at least 3.

(1) $A \cong I \oplus -\varepsilon \oplus -\pi \oplus \varepsilon\pi$.

(2) $A \cong I \oplus -1 \oplus \alpha \oplus \beta$ for some $\alpha, \beta \in H^*$.

If (2) applies and $|A| \in H^2$, it may be assumed that $\alpha = 1$, $\beta = -1$.

Proof. We have $c(I \oplus -1 \oplus \alpha \oplus \beta) = (-1,\alpha)(-\alpha,\alpha\beta)(-\alpha\beta,-1) = (-1,-1)(\alpha,-\alpha\beta)$. By Theorems A (3) and B (1), we can put A in the form (2) unless $-\alpha\beta = |A| \in H^2$. Suppose $|A| \in H^2$. It is easily seen that $c(I \oplus -1 \oplus 1 \oplus -1) = (-1,-1)$ and $c(I \oplus -\varepsilon \oplus -\pi \oplus \varepsilon\pi) = (-\varepsilon, -\varepsilon\pi)(\varepsilon\pi, -1) = (-1,-1)(\varepsilon, -\varepsilon\pi) = -(-1,-1)$. An application of Theorem B (1) completes the proof.

Theorem F. Let H be a local field with prime spot $\mathfrak{p}$ and let K be a finite algebraic extension of H. Then $e(K/H)f(K/H) = [K : H]$. Further, K is a pure ramified extension of $H(\omega)$ where ω is a primitive $(p^g - 1)$st root of unity, $\mathfrak{p}$ divides the rational prime p, and $g = f(K/Q_p)$. If (e) is prime to $\mathfrak{p}$, then for ω as above and some prime π of $H(\omega)$ we have $K = H(\omega, \pi^{1/e})$. There is a basis for the integers of K over those of H. [5, p.241, 365].

Theorem G. Let H be a global field with finite algebraic extension $K = H(\varphi)$ and local prime spot $\mathfrak{p}$. Suppose $\mathfrak{p} = \Pi\, \mathfrak{P}^{e(\mathfrak{P})}$ is the decomposition of $\mathfrak{p}$ as powers of distinct primes over K. Determine $f(\mathfrak{P})$ by $N_{K/H}\, \mathfrak{P} = \mathfrak{p}^{f(\mathfrak{P})}$. Then $H(\varphi;\mathfrak{p}) = \Sigma_{\mathfrak{P}} \oplus L(\mathfrak{P})$ where $L(\mathfrak{P})$ is complete at $\mathfrak{P}$, and $e(L(\mathfrak{P})/H_{\mathfrak{p}}) = e(\mathfrak{P})$, and $f(L(\mathfrak{P})/H_{\mathfrak{p}}) = f(\mathfrak{P})$ and $\Sigma_{\mathfrak{P}}\, e(\mathfrak{P})f(\mathfrak{P}) = [K : H]$. Furthermore $\mathfrak{D}(L(\mathfrak{P})/H_{\mathfrak{p}}) = \mathfrak{p}^{a(\mathfrak{P})}$ and

$$\mathfrak{D}(K/H) = \prod_{\mathfrak{q}} \prod_{\mathfrak{Q}|\mathfrak{q}} \mathfrak{D}(L(\mathfrak{Q})/H_{\mathfrak{q}}) ,$$

where $a(\mathfrak{P}) = e'(\mathfrak{P})f(\mathfrak{P})$, and $e'(\mathfrak{P}) = e(\mathfrak{P}) - 1$ if $e(\mathfrak{P})$ is prime to $\mathfrak{P}$, and $e'(\mathfrak{P}) \geq e(\mathfrak{P})$ otherwise. [5 pp.429,431].

Theorem H. Let $\mathfrak{p}_1,\ldots,\mathfrak{p}_k$ be distinct local prime spots on a global field H. Let $a_1,\ldots,a_k$ be integers and let $\alpha_1,\ldots,\alpha_k \in H$. The k congruences

$$x \equiv \alpha_i (\mathrm{mod}\ \mathfrak{p}_i^{a_i}) \qquad 1 \leq i \leq k$$

have a solution $x \in H$. [12, 11:8].

Theorem J. Let H be a local field with prime spot $\mathfrak{p}$. If $\mathfrak{p}$ is prime to 2, then $[H^* : H^{*2}] = 4$. If $\mathfrak{p}$ is not prime to 2, then $[H^* : H^{*2}] = 4 \cdot 2^a$ where $a = [H : Q_2]$. [12, 63:9].

Theorem K (Limitation Theorem). If K is a finite separable extension of the local field H and L is the maximum abelian subextension, then $N(K^*/H) = N(L^*/H)$. [15, p.180].

Theorem L (Reciprocity Theorem). If K is a finite abelian extension of the local field H, then the Galois group of K over H is isomorphic to $H^*/N(K^*/H)$. [15, p.177].

Theorem M' (Generalized Arithmetic Progression Theorem). Let H be an algebraic number field with two relatively prime ideals $\mathfrak{A}$ and $\mathfrak{B}$. There is a prime ideal $\mathfrak{P}_0$ of H and an $\alpha \in H^*$ such that $\mathfrak{A} = \alpha\, \mathfrak{P}_0$ and $\alpha \equiv 1\ (\mathrm{mod}\ \mathfrak{B})$. If H is formally real, we may choose α to be totally positive. [6, Satz 13].

NOTATION

A	a matrix with entries a_{ij}; $A = (a_{ij})$
$\underline{\alpha}$	a vector with components α_i
N	norm
Q	rational numbers
Z	rational integers
Im	imaginary part
Re	real part
tr	trace
$\mathfrak{a}^\circ$	complement of the ideal $\mathfrak{a}$; $\mathfrak{a}^\circ = \{\lambda \in G : \text{tr}\,\lambda\alpha \in D$ for all $\alpha \in \mathfrak{a}\}$
$C(\ )$	class of
$J(\lambda)$	diag $(\lambda^{(1)},\lambda^{(2)},\ldots,\lambda^{(n)})$; see Theorem 1.5
$M(\underline{\alpha})$	the matrix $(\underline{\alpha}^{(1)},\ldots,\underline{\alpha}^{(n)})$; see Theorem 1.4
$\mathfrak{R}(\ )$	see Definition 2.3
$\lambda^{(i)}$	the i^{th} conjugate of λ
$S(\ ,\ )$	see Definition 2.1
$\oplus$	direct sum
$\otimes$	direct product
$\overline{}$	complex conjugate
$'$	transpose
$\lvert\ \rvert$	determinant, absolute value, cardinality
$\{\ \}$	set

$\sim$	ideal equivalence
$(\underline{\alpha},\underline{\beta})$	$\Sigma \alpha_i \beta_i$
[K : H]	index of H in K
mbv	module basis vector; see Theorem 1.4
M-ideal	see Definition 1.3
rep	see Definition 1.1
symrep	see Definition 1.1

The symbols D, Δ, F, G, θ, n have a special meaning throughout the thesis. See the beginning of Section I. The special notation used in Section IV is not listed here. See Definition 4.1.

BIBLIOGRAPHY

1. R. Dedekind, Gesammelte mathematische Werke I, Friedr. Vieweg & Sohn, Braunschweig, 1930, 105-157.

2. L. E. Dickson, Linear groups, Dover, New York, 1958.

3. D. K. Faddeev, On the characteristic equations of rational symmetric matrices (Russian), Dokl. Akad. Nauk SSSR 58 (1947), 753-754.

4. D. S. Gorshkov, Kubische Körper und symmetrische Matrizen, Dokl. Akad. Nauk SSSR 31 (1941), 842-844.

5. H. Hasse, Zahlentheorie, 2nd ed., Akademie-Verlag, Berlin, 1963.

6. ________, Bericht über neure Untersuchen und Probleme aus der Theorie der algebraischen Zahlkörper I, Jber. Deutsch. Math.-Verein. 35 (1926), 1-55.

7. E. Hecke, Vorlesungen über die Theorie der algebraischen Zahlen, Akademische Verlagsgesellschaft, Leipzig, 1923.

8. E. L. Ince, Cycles of reduced ideals in quadratic fields, BAAS Math. Tables 4, Office of the British Assn., London, 1934.

9. B. W. Jones, The arithmetic theory of quadratic forms, Carus Monographs 10, Math. Assn. Amer., 1950.

10. F. Krakowski, Eigenwerte und Minimalpolynome symmetrischer Matrizen in kommutativen Körpern, Comment. Math. Helv. 32 (1958), 224-240.

11. C. G. Latimer and C. C. MacDuffee, *A correspondence between classes of ideals and classes of matrices*, Ann. of Math. 34 (1933), 313-316.

12. O. T. O'Meara, *Introduction to quadratic forms*, Grund. Math. Wiss. 117, Academic Press Inc., New York, 1963.

13. W. Patz, *Tafel der regelmässigen Kettenbrüche und ihrer vollständigen Quotienten für die Quadratwurzelen aus den natürlichen Zahlen von 1-10,000*, Akademie-Verlag, Berlin, 1955.

14. A. P. Sapiro, *Characteristic polynomials of symmetric matrices* (Russian), Sibirsk. Mat. Ž. 3 (1962), 280-291.

15. J. P. Serre, *Corps locaux*, Hermann, Paris, 1962.

16. O. Taussky, *On a theorem of Latimer and MacDuffee*, Canad. J. Math. 1 (1949), 300-302.

17. ________, *Classes of matrices and quadratic fields*, Pacific J. Math. 1 (1951), 127-131.

18. ________, *Classes of matrices and quadratic fields II*, J. London Math. Soc. 27 (1952), 237-239.

19. ________, *On matrix classes corresponding to an ideal and its inverse*, Illinois J. Math. 1 (1957), 108-113.

20. ________, *Ideal Matrices I*, Arch. Math. 13 (1962), 275-282.

21. J. Williamson, *The latent roots of a matrix of special type*, Bull. Amer. Math. Soc. 37 (1931), 585-590.