71-16,696

PONOMAREV, Paul, 1944-
CLASS NUMBERS OF POSITIVE DEFINITE QUATERNARY FORMS.

Yale University, Ph.D., 1970
Mathematics

University Microfilms, A XEROX Company, Ann Arbor, Michigan

© 1971

PAUL PONOMAREV

ALL RIGHTS RESERVED

THIS DISSERTATION HAS BEEN MICROFILMED EXACTLY AS RECEIVED

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

CLASS NUMBERS OF POSITIVE DEFINITE QUATERNARY FORMS

By

Paul Ponomarev

1970

A Dissertation Presented to the Faculty of the Graduate School of Yale University in Candidacy for the Degree of Doctor of Philosophy.

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

Summary

Let V be a quadratic vector space of dimension four over the field of rational numbers $\mathbb{Q}$. Suppose that the associated quadratic form q is positive definite with square discriminant. Hence we may assume that $V = \mathcal{A}$, a positive definite quaternion algebra over $\mathbb{Q}$, and $q = N$, the norm form of $\mathcal{A}$. All maximal integral lattices of $\mathcal{A}$ have the same discriminant $D = d^2$, where d is a positive square-free integer. The main result of this dissertation is Theorem 2.1, which gives an explicit formula for H, the number of proper classes in the genus of maximal integral lattices of $\mathcal{A}$. This formula is analogous to the known formulas for h_d, the ideal class number of $\mathcal{A}$ (cf.[5]), and t_d, the type number of $\mathcal{A}$ (cf.[7]). It depends directly on h_d and on the class numbers of those imaginary quadratic extensions $\mathbb{Q}(\sqrt{-m})$ which can be embedded in $\mathcal{A}$ and for which m divides d. The formula is derived by applying the Selberg Trace Formula in an appropriate manner.

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

Acknowledgements

The author wishes to express his deep gratitude to Professor Tsuneo Tamagawa for his invaluable advice and encouragement before and during the preparation of this thesis.

The author also wishes to thank Professors Robert P. Langlands and George B. Seligman for their many helpful suggestions having to do with the improvement of the exposition.

He would also like to thank Dante M. Giarrusso for several informative conversations concerning the integration theory of locally compact groups.

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

Table of contents

Chapter I. Preliminaries

1. Basic notions 1

2. Arithmetic of rational quadratic forms 2

3. Rational quaternion algebras 6

4. The Selberg Trace Formula 12

Chapter II. Statement of results

1. The main theorem 14

2. Outline of the proof 16

Chapter III. Proof of the theorem

1. Preparatory discussion 18

2. Structure of isotropy groups 20

3. The adelized setting 23

4. Application of the Selberg Trace Formula 26

5. The principal term $\delta \equiv (\pm 1, 1)$ 29

6. The term $\delta \equiv (1, u)$ 35

7. The term $\delta \equiv (u, v)$ 38

8. The term $\delta \equiv (\mu, \nu)$ 40

9. Evaluation of the trace sum 45

Chapter IV. Concluding discussion and tables

1. Comparison with the classical theory 51

2. Generalizations 55

3. The non-square discriminant case 56

4. Tables 57

References 61

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

Chapter I. Preliminaries

§1. Basic notions (cf.[9],Chap.IV)

Let V be a finite dimensional vector space over a field F having characteristic $\neq 2$.

Definition 1.1: A mapping $q:V \to F$ is called a quadratic form on V if it satisfies the following two conditions:

(i) $q(ax) = a^2 q(x)$ for all $a \in F, x \in V$.

(ii) The mapping $(x,y) \to B(x,y) = q(x + y) - q(x) - q(y)$ is a bilinear form on $V \times V$.

One calls the pair (V,q) a quadratic vector space over F. Whenever q is implicitly known, we shall simply say that V is a quadratic vector space over F. The form B is called the bilinear form associated to q. Clearly, B is a symmetric bilinear form and q is uniquely determined by B, since $q(x) = \frac{1}{2}B(x,x)$ for all $x \in V$. Thus we have a one-to-one correspondence between symmetric bilinear forms on $V \times V$ and quadratic forms on V. We call q degenerate or non-degenerate according as B is degenerate or non-degenerate, respectively. We shall assume throughout that q is non-degenerate.

For a quadratic vector space V we define $O(V)$, the orthogonal group of V, to be the subgroup of $GL(V)$ consisting of all σ such that $q(\sigma(x)) = q(x)$ for all $x \in V$. The elements of $O(V)$ are called orthogonal transformations. An orthogonal transformation must have determinant equal to ± 1. We define $O^+(V)$, the proper (or special) orthogonal group , to be the subgroup of $O(V)$

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

consisting of all those orthogonal transformations which have determinant +1. One easily sees that $O^+(V)$ is a normal subgroup of $O(V)$ of index 2. The elements of $O^+(V)$ are called proper orthogonal transformations (or rotations).

If K/F is an extension field, then q extends uniquely, in the obvious manner, to a quadratic form on $V_K = V \otimes_F K$. This extension of q gives natural embeddings: $O(V) \subset O(V_K)$ and $O^+(V) \subset O^+(V_K)$.

§2. Arithmetic of rational quadratic forms

The basic reference for the material covered in this section is O'Meara [9], Chapters VIII-X.

From now on we assume that V is a quadratic vector space over the field of rational numbers $\mathbb{Q}$. For each rational prime p denote by $\mathbb{Q}_p$ the field of p-adic numbers and by V_p the quadratic vector space $V \otimes_{\mathbb{Q}} \mathbb{Q}_p$.

By a lattice M in V we mean a finitely generated $\mathbb{Z}$-submodule of V which contains a basis of V over $\mathbb{Q}$. Clearly, this is equivalent to: there exists a basis $x_1, \ldots, x_n$ of V over $\mathbb{Q}$ such that $M = \mathbb{Z}x_1 + \ldots + \mathbb{Z}x_n$. A lattice in V_p is defined in the same manner: M(p) is a lattice in $V_p \iff$ M(p) is a finitely generated $\mathbb{Z}_p$-submodule of V_p containing a basis of V_p over $\mathbb{Q}_p$ $\iff$ $M(p) = \mathbb{Z}_p x_1^{(p)} + \ldots + \mathbb{Z}_p x_n^{(p)}$ for some basis $x_1^{(p)}, \ldots, x_n^{(p)}$ of V_p over $\mathbb{Q}_p$. Here $\mathbb{Z}_p$ is, of course, the ring of p-adic integers. If M is a lattice in V, then $M_p = M \otimes_{\mathbb{Z}} \mathbb{Z}_p$ is clearly a lattice in V_p for each rational prime p. If M is a lattice in

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

V, then $O(M)$ is the subgroup of $O(V)$ consisting of all σ such that $\sigma M \subset M$. We set $O^+(M) = O(M) \cap O^+(V)$. Similarly, we can define $O(M(p))$ and $O^+(M(p))$ for any local lattice $M(p)$, where p is a prime.

We say that two lattices M and M' in V are of the same class and write $M \simeq M'$ if there exists $\sigma \in O(V)$ such that $\sigma M = M'$. Two lattices M, M' in V are of the same proper class if there exists $\sigma \in O^+(V)$ such that $\sigma M = M'$. Clearly, every class of lattices in V consists of at most two proper classes. We say that two lattices M and M' in V are of the same genus and write $M \sim M'$ if for every prime p there exists $\sigma_p \in O(V_p)$ such that $\sigma_p M_p = M'_p$. There is no distinct notion of proper genus for lattices in V, since there always exists $\sigma_p \in O(M_p)$ such that $\det \sigma_p = -1$, p any finite prime. (cf. [9], p. 241)

For a lattice M in V, the discriminant $D(M)$ of M is defined to be: $D(M) = (-1)^{[\frac{n}{2}]} |B(x_i, x_j)|$, where $x_1, \ldots, x_n$ is a basis of M. It is easily seen that $D(M)$ is independent of the choice of basis. Moreover, for any two lattices M and M', $D(M)$ and $D(M')$ differ only by a square multiple. A lattice M in V is said to be integral if $q(x) \in \mathbb{Z}$ for all $x \in M$. One then has:

Proposition 1.2: If $M \sim M'$, then:

(i) $D(M) = D(M')$

(ii) M integral $\Leftrightarrow$ M' integral (cf. [9], p. 299)

A lattice M in V is maximal integral if it is maximal with respect to the property of being integral. It is easy to show that maximal integral lattices exist and, in fact, that any

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

integral lattice is contained in a maximal integral lattice. It is well-known that the maximal integral lattices are all of the same genus (cf.[9], p.240). Conversely, by Proposition 1.2, any lattice which is of the same genus as a maximal integral lattice must itself be maximal integral. Hence the collection of maximal integral lattices forms a genus. In particular, by Proposition 1.2, all maximal integral lattices have the same discriminant D. We shall call D the fundamental discriminant of q.

Obviously, $M \simeq M' \Rightarrow M \sim M'$. Hence each genus of lattices in V decomposes into a disjoint union of classes. The fundamental result in the arithmetic theory of quadratic forms then is:

Theorem 1.3: Every genus consists of a finite number of classes. (cf.[9], p.309)

By this theorem, we can attach to each non-degenerate quadratic vector space V over $\mathbb{Q}$ a certain number H = the number of proper classes of maximal integral lattices in V. It is easy to see that any integral lattice M with D(M) = D must be a maximal integral lattice. Therefore, H = the number of proper classes of integral lattices with discriminant D.

Let us review some of the known results for H in case dimV is 2 or 3, the so-called "binary" and "ternary" cases, respectively. If q is a binary form and if D is a square, then q must have a null vector, that is, a vector $x \in V$, $x \neq 0$, such that $q(x) = 0$. It follows that H must be 1. If D is not a square, but q represents 1, then q is essentially the norm form of the

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

quadratic number field $\mathbb{Q}(\sqrt{D})$ and $H = 2^{1-e}h^+(\sqrt{D})$, where $h^+(\sqrt{D})$ = the ideal class number of $\mathbb{Q}(\sqrt{D})$ in the narrow sense and e = the number of distinct primes dividing the discriminant of $\mathbb{Q}(\sqrt{D})$.

We say that q is an indefinite form if $V_{\mathbb{R}}$ contains a null vector. Otherwise, q is said to be definite. If q is definite, then $q(x)$ is either always positive or always negative for $x \in V$, $x \neq 0$. In the former case, we call q positive definite; in the latter case, we call q negative definite. Using the approximation theorem of Watson [12] for indefinite quadratic forms, one can show that H = 1 for any indefinite form of dimension > 2. In view of this and the fact that H is unaffected by replacing q by $-q$, we can restrict ourselves to positive definite quadratic forms in case dimV > 2.

If q is a positive definite ternary form with -D = a square, then V can be thought of as the subspace of trace 0 elements in a positive definite quaternion algebra $\mathcal{A}$ over $\mathbb{Q}$ with q given by the restriction to V of the norm form N of $\mathcal{A}$ (cf.[4], p.29). One can then show that H = the type number of $\mathcal{A}$ = the number of conjugacy classes of maximal orders in $\mathcal{A}$. The type number of $\mathcal{A}$ can be expressed in terms of the class numbers of certain complex quadratic extensions inside $\mathcal{A}$ and the ideal class number of $\mathcal{A}$ (cf.[3] and [7]). These class numbers in turn can be expressed in terms of the Kronecker symbol, in the quadratic case by the classical formula of Dirichlet, in the other case by the formula of Eichler [5].

Thus H can be effectively computed for the binary and ternary

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

cases mentioned above, where we made certain assumptions on the discriminant and on the representability of q. The question naturally arises whether similar formulas can be obtained for H in the case of quaternary forms, that is, forms of dimension 4. In this dissertation we answer this question affirmatively for the square discriminant case. By an earlier remark, we may assume that q is positive definite. In the quaternary case there are essentially two distinct possibilities, depending on whether D is a square or a non-square (cf.[4], pp.31-33). In this dissertation we shall restrict ourselves to the square discriminant case. For a discussion of the non-square discriminant case, see Section IV.3. It is a standard result in the theory of Clifford algebras that a positive definite quadratic vector space (V,q) over $\mathbb{Q}$ having square discriminant is isometric to a quadratic vector space $(\mathcal{A},N)$, where $\mathcal{A}$ is a positive definite quaternion algebra over $\mathbb{Q}$ and N is its norm form. In view of this, let us review some of the basic results in the theory of rational quaternion algebras.

§3. Rational quaternion algebras

The basic references for this section are: for the algebraic theory, O'Meara [9], pp. 142-149; for the arithmetic theory, Deuring [2], Chapter VI.

Definition 1.4: A rational quaternion algebra is a central simple algebra over $\mathbb{Q}$ of dimension 4.

Let $\mathcal{A}$ be a rational quaternion algebra. Since $\mathcal{A}$ can be

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

split by a quadratic extension of $\mathbb{Q}$, $\mathcal{A}$ must be a cyclic algebra, that is, there exist $w,z \in \mathcal{A}$ and $a,b \in \mathbb{Q}^*$, such that $\mathcal{A} = \mathbb{Q} + \mathbb{Q}w + \mathbb{Q}z + \mathbb{Q}wz$, $w^2 = a$, $z^2 = b$ and $wz = -zw$. We denote by ι the canonical involution of $\mathcal{A}$: $\iota(a_0 + a_1w + a_2z + a_3wz) = a_0 - a_1w - a_2z - a_3wz$, where $a_0,a_1,a_2,a_3 \in \mathbb{Q}$. Then we have the norm mapping N and the trace mapping T defined in the usual way: $N(\alpha) = \alpha \cdot \iota(\alpha) = \iota(\alpha)\cdot\alpha$, $T(\alpha) = \alpha + \iota(\alpha)$ for all $\alpha \in \mathcal{A}$. If $\alpha \in \mathcal{A}$, $\alpha \notin \mathbb{Q}$, then the minimal polynomial of α is: $X^2 - T(\alpha)X + N(\alpha)$.

For each finite prime p, $\mathcal{A}_p = \mathcal{A} \otimes_{\mathbb{Q}} \mathbb{Q}_p$ is a central simple algebra over $\mathbb{Q}_p$ with the same defining relations as $\mathcal{A}$. It is well-known that, up to isomorphism, there are only two central simple algebras over $\mathbb{Q}_p$ of dimension 4: either $M(2,\mathbb{Q}_p)$ or the unique division algebra of dimension 4 over $\mathbb{Q}_p$. One calls $\mathcal{A}_p$ the "split" quaternions if it is $M(2,\mathbb{Q}_p)$. Otherwise, $\mathcal{A}_p$ is said to be "non-split" or "ramified". By class field theory, $\mathcal{A}_p$ is split $\Leftrightarrow (a,b)_p = 1$, where $a,b \in \mathbb{Q}^*$ are as above and $(a,b)_p$ is the Hilbert norm residue symbol. In particular, $\mathcal{A}_p$ is split for almost all primes p. The same sort of considerations are valid for the infinite prime ∞, where $\mathcal{A}_\infty = \mathcal{A}_{\mathbb{R}} = \mathcal{A} \otimes_{\mathbb{Q}} \mathbb{R}$. Namely, $\mathcal{A}_\infty = \mathbb{H}$, the usual Hamilton quaternions $\Leftrightarrow$ $(a,b)_\infty = -1 \Leftrightarrow a < 0$ and $b < 0$. We note that $(\mathcal{A},N)$ is positive definite as a quadratic vector space $\Leftrightarrow \mathcal{A}_\infty = \mathbb{H}$. The finite set $\{p_1,\ldots,p_e\}$ of non-archimedean primes at which $\mathcal{A}$ is non-split will be called the "non-split primes" of $\mathcal{A}$. By the product formula for the norm residue symbol, we see that e must be odd if $\mathcal{A}$ is positive definite, but e must be even if $\mathcal{A}$ is indefinite.

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

Moreover, it can be shown that, given any finite set of distinct non-archimedean primes $\{p_1,\ldots,p_e\}$, there exists a unique (up to isomorphism) quaternion algebra $\mathcal{A}$ whose non-split primes are $p_1,\ldots,p_e$. This gives a one-to-one correspondence between rational quaternion algebras and finite sets of rational primes.

Definition 1.5: A subset $\mathcal{O}$ of $\mathcal{A}$ is called an order if:

(i) $\mathcal{O}$ is a lattice in $\mathcal{A}$ and

(ii) $\mathcal{O}$ is a subring of $\mathcal{A}$ containing 1.

Orders in $\mathcal{A}_p$ are defined in exactly the same manner. Then, given an order $\mathcal{O}$ in $\mathcal{A}$, $\mathcal{O}_p = \mathcal{O} \otimes_{\mathbb{Z}} \mathbb{Z}_p$ is an order in $\mathcal{A}_p$ for every finite p. If $\mathcal{O}$ is an order in $\mathcal{A}$, then any $\alpha \in \mathcal{O}$ must be integral over $\mathbb{Z}$, from which it follows that $N(\alpha), T(\alpha) \in \mathbb{Z}$. An order in $\mathcal{A}$ (or in $\mathcal{A}_p$) is said to be maximal if it is not contained properly in any other order. One can easily show: $\mathcal{O}$ is a maximal order in $\mathcal{A} \Leftrightarrow \mathcal{O}_p$ is a maximal order in $\mathcal{A}_p$ for every p. The classification of maximal orders in $\mathcal{A}_p$ is very easy. If $\mathcal{A}_p$ is split, then any maximal order is isomorphic to $M(2,\mathbb{Z}_p)$ and any two maximal orders in $\mathcal{A}_p$ are conjugate by an invertible element in $\mathcal{A}_p$. If $\mathcal{A}_p$ is non-split, then there is a unique maximal order $\mathcal{O}_p = \{\alpha \in \mathcal{A}_p \mid N(\alpha) \in \mathbb{Z}_p\}$. If $\mathcal{O}$ is an order in $\mathcal{A}$, then we define:

$$\hat{\mathcal{O}} = \{\alpha \in \mathcal{A} \mid T(\alpha\mathcal{O}) \subset \mathbb{Z}\}$$

It turns out that the discriminant $D(\mathcal{O}) = [\hat{\mathcal{O}} : \mathcal{O}]$, just as in the case of number fields. Using this, one can easily show that any order in $\mathcal{A}$ is contained within a maximal order of $\mathcal{A}$. Any maximal order of $\mathcal{A}$ is necessarily a maximal integral lattice

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

with respect to N. Hence the fundamental discriminant D must equal $[\hat{\mathcal{O}} : \mathcal{O}]$ for any maximal order $\mathcal{O}$ of $\mathcal{A}$. Using this fact, one easily shows by elementary local computations that $D = (p_1 \ldots p_e)^2$, where $\{p_1, \ldots p_e\}$ is the set of non-split primes of $\mathcal{A}$. Combining this fact with an earlier discussion, it follows that the quaternary forms of square discriminant are completely classified by their fundamental discriminants. Thus we can rightfully expect any formula for H to depend only on D. For convenience, let us write $D = d^2$, where $d = p_1 \ldots p_e$.

We recall that if L,M are lattices in $\mathcal{A}$, then $L \cdot M = \left\{ \sum_{i=1}^{k_i} \ell_i m_i \mid \ell_i \in L, m_i \in M \right\}$. Clearly L·M is a lattice in $\mathcal{A}$.

Definition 1.6: Let $\mathcal{O}$ be an order of $\mathcal{A}$. A subset I of $\mathcal{A}$ is said to be a left ideal of $\mathcal{O}$ if:

(i) I is a lattice in $\mathcal{A}$ and

(ii) $\mathcal{O} \cdot I = I$.

One defines the notion of a right ideal J of $\mathcal{O}$ by replacing (ii) with (ii)' $J \cdot \mathcal{O} = J$. For an order $\mathcal{O}(p)$ in $\mathcal{A}_p$, p a finite prime, the notions of left and right ideals of $\mathcal{O}(p)$ are defined in exactly the same manner as for $\mathcal{O}$. If $\mathcal{O}(p)$ is a maximal order of $\mathcal{A}_p$, then all ideals of $\mathcal{O}(p)$, left or right, are principal. In other words, given a left ideal I(p) of $\mathcal{O}(p)$ and a right ideal J(p) of $\mathcal{O}(p)$, there exist invertible elements α_p, β_p in $\mathcal{A}_p$ such that $I(p) = \mathcal{O}(p)\alpha_p$, $J(p) = \beta_p \mathcal{O}(p)$ (cf. [2], p.100).

Let us fix a maximal order $\mathcal{O}$ in $\mathcal{A}$. We say that two left ideals I,J of $\mathcal{O}$ are of the same ideal class if there exists an invertible element $\alpha \in \mathcal{A}$ such that $I\alpha = J$. It is well-known that

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

the number of ideal classes of left ideals of $\mathcal{O}$ is finite (cf.[2], p.90). In fact, this can be derived from the finiteness of H. Moreover, if we define the corresponding notion of ideal class for right ideals of $\mathcal{O}$, then the number of left ideal classes = the number of right ideal classes and this number is independent of the choice of maximal order $\mathcal{O}$. We may therefore speak of the ideal class number of the quaternion algebra $\mathcal{A}$. The ideal class number of $\mathcal{A}$ depends only on d, so we denote it by h_d. We then have the following formula for h_d, due to Eichler [5]:

Theorem 1.7:

$$h_d = \frac{1}{12}\phi(d) + \frac{1}{4}\prod_{p|d}\left(1 - \left(\frac{-4}{p}\right)\right) + \frac{1}{3}\prod_{p|d}\left(1 - \left(\frac{-3}{p}\right)\right)$$

where ϕ = the Euler ϕ-function and $\left(\frac{-4}{p}\right)$, $\left(\frac{-3}{p}\right)$ are Kronecker symbols.

If L is any lattice in $\mathcal{A}$, then the set $\mathcal{O}_\ell = \{\alpha \in \mathcal{A} \mid \alpha L \subset L\}$ is an order of $\mathcal{A}$ having L as a left ideal. Clearly, if $\mathcal{O}$ is an order of $\mathcal{A}$ such that L is a left $\mathcal{O}$-ideal, then $\mathcal{O} \subset \mathcal{O}_\ell$. The set $\mathcal{O}_r = \{\alpha \in \mathcal{A} \mid L\alpha \subset L\}$ is an order of $\mathcal{A}$ having L as a right ideal which contains any other order of $\mathcal{A}$ having L as a right ideal. We call $\mathcal{O}_\ell$ and $\mathcal{O}_r$ the left and right order, respectively, of the lattice L. Using the fact that all ideals of a maximal order in $\mathcal{A}_p$ are principal for any rational prime p, one can show that: $\mathcal{O}_\ell$ is a maximal order $\Leftrightarrow$ $\mathcal{O}_r$ is a maximal order. In accordance with this we define:

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

Definition 1.8: A lattice I in $\mathcal{A}$ is said to be a normal ideal if its left (hence its right) order is maximal (cf.[1]).

A local normal ideal I(p) in $\mathcal{A}_p$ is defined in the same way. Using again the fact that in the local case the ideals of maximal orders are all principal, one can show: If I(p),J(p) are normal ideals in $\mathcal{A}_p$, p a finite prime, then there exist $\alpha_p, \beta_p \in \mathcal{A}_p$, necessarily invertible, such that $\alpha_p I(p) \beta_p = J(p)$. If I is a normal ideal of $\mathcal{A}$, we define its norm N(I) as follows: Let $\mathcal{O}$ = the left order of I. Then, for every finite prime p, $I_p = \mathcal{O}_p \alpha_p$ for some invertible $\alpha_p \in \mathcal{A}_p$. Of course, α_p is a unit of $\mathcal{O}_p$ for almost all p.

We then set: $N(I) = \prod_p p^{v_p(N(\alpha_p))}$, where v_p = the normalized valuation on $\mathbb{Q}_p$.

The set of all normal ideals of $\mathcal{A}$ can be given the structure of a groupoid, with an associative composition $I \circ J$ defined to be $I \cdot J$ whenever the right order of I = the left order of J. Of course, the left identity of a normal ideal I is its left order and the right identity of I is its right order. Whenever $I \circ J$ is defined, we have: $N(I \circ J) = N(I)N(J)$.

Definition 1.9: Two normal ideals I,J of $\mathcal{A}$ are said to be equivalent if there exist $\alpha, \beta \in \mathcal{A}$ (necessarily invertible) such that $\alpha I \beta = J$ (cf.[1]).

One can show that the number of equivalence classes of normal ideals is finite. In fact, we will see in Section III.1 that the number of equivalence classes of normal ideals is equal to H.

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

§4. The Selberg Trace Formula

Our intention is to obtain a formula for H in the case of a positive definite quaternion algebra $\mathcal{A}$ over $\mathbb{Q}$ having fundamental discriminant $D = d^2$. We would like this formula to be of the same kind as the known ones for the type number t_d of $\mathcal{A}$ and the ideal class number h_d of $\mathcal{A}$. Tamagawa has successfully employed the Selberg Trace Formula to derive the known formulas for both t_d (unpublished) and h_d [11]. Inspired by this, we shall apply the Selberg Trace Formula in a suitable manner to obtain an expression for H which will closely resemble the one for t_d.

Let us review the statement of the Selberg Trace Formula. We do not need the most general version, as given, for example, by Tamagawa in [10] and [11]. For our purposes the following version will suffice:

Let G be a locally compact unimodular group and U a compact subgroup of G. We denote by L(G,U) the set of complex-valued continuous functions F on G such that:

(i) F has compact support and

(ii) $F(ugu') = F(g)$ for all $g \in G$, $u, u' \in U$.

Let Γ be a discrete subgroup of G such that G/Γ is compact and suppose, in addition, that G decomposes into finitely many double cosets $U g \Gamma$. Denote by $L^2(U\backslash G/\Gamma)$ the finite dimensional complex vector space of all complex-valued functions f on G such that $f(ug\gamma) = f(g)$ for all $g \in G$, $u \in U$, $\gamma \in \Gamma$. Then $L^2(U\backslash G/\Gamma)$ is a Hilbert space equipped with the inner product:

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

$$\langle f,g\rangle = \int_{G/\Gamma} f(x)\overline{g(x)}\,dx \quad \text{for} \quad f,g \in L^2(U\backslash G/\Gamma).$$

Any $F \in L(G,U)$ induces a linear endomorphism of $L^2(U\backslash G/\Gamma)$ by convolution: $f \to F*f$. More precisely, for $f \in L^2(U\backslash G/\Gamma)$ and $F \in L(G,U)$ we define $F(f) \in L^2(U\backslash G/\Gamma)$ by:

$$(F(f))(x) = \int_G F(xy^{-1})f(y)\,dy = \int_G F(y)f(y^{-1}x)\,dy$$

For any $\gamma \in \Gamma$, we define $\{\gamma\}$ = the conjugacy class of γ in Γ. For each conjugacy class $\{\gamma\}$ we fix a representative γ. Let $\Gamma(\gamma)$ = the centralizer of γ in Γ. We denote by $d_\gamma x$ the invariant measure on the homogeneous space $G/\Gamma(\gamma)$. We then have:

Theorem 1.10: (Selberg Trace Formula)

$$Tr(F) = \sum_{\{\gamma\}} \int_{G/\Gamma(\gamma)} \Psi_\gamma(x)\,d_\gamma x$$

where $\Psi_\gamma(x) = F(x\gamma x^{-1})$ for all $x \in G$.

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

In this chapter we state the main results and give an indication of the proof. The actual details of the proof will be presented in Chapter III.

§1. The main theorem

Using the notation of Chapter I, assume we have a positive definite quaternion algebra $\mathcal{A}$ over $\mathbb{Q}$ with fundamental discriminant $D = d^2$. For any positive integer n, denote by $h(\sqrt{-n})$ the ideal class number of the imaginary quadratic field $\mathbb{Q}(\sqrt{-n})$. Set $\lambda(n)$ = the number of distinct primes which divide n. In particular, $\lambda(d) = e$. Define $\delta(\sqrt{-n})$ to be 1 if $n|d$ and there exists $x \in \mathcal{A}$ such that $x^2 + n = 0$. Otherwise define $\delta(\sqrt{-n}) = 0$.

Theorem 2.1: (a) If D is odd, then:

$$H = 2^{-e}\left(h_d^2 + \sum_{m>2} A_m^2 \right)$$

where $A_3 = 2^{e-1}\,\delta(\sqrt{-3})$, $A_m = 2^{e-\lambda(m)-\sigma(m)}\,\delta(\sqrt{-m})h(\sqrt{-m})$ for $m > 3$.

and $$\sigma(m) = \begin{cases} -1 & \text{if } m \equiv 3 \pmod 8 \\ 0 & \text{if } m \equiv 7 \pmod 8 \\ 1 & \text{if } m \equiv 1 \pmod 4 \end{cases}$$

(b) If D is even, then:

$$H = 2^{-e}\left(h_d^2 + \sum_{m>1} A_m^2 \right)$$

where $A_2 = 2^{e-2}\left(\delta(\sqrt{-1}) + \delta(\sqrt{-2}) \right)$ and

$A_m = 2^{e-\lambda(m)-\sigma(m)}\,\delta(\sqrt{-m})h(\sqrt{-m})$ for $m > 2$, but now:

$$\sigma(m) = \begin{cases} 1 & \text{if } m \equiv 2,3 \pmod 4 \\ 2 & \text{if } m \equiv 1 \pmod 4 \end{cases}$$

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

Remark: Using the Brauer-Hasse-Noether Theorem on splitting fields of central simple algebras over global fields, it is easy to interpret the condition $\delta(\sqrt{-m}) = 1$ in terms of the Kronecker symbol. Namely, let Δ_m = the discriminant of $\mathbb{Q}(\sqrt{-m})$. Then:

$$\delta(\sqrt{-m}) = 1 \iff \left(\frac{\Delta_m}{p_i}\right) = -1 \text{ for all } p_i \nmid \Delta_m,\ i = 1,\ldots,e$$

Applying this, one can rephrase Theorem 2.1 in terms of the Kronecker symbol, in a form similar to that of Theorem 1.7.

As a special case of Theorem 2.1 we have the following:

Corollary 2.2: Suppose $D = p^2$, p a prime > 3. Then:

$$H = \frac{1}{2}\left(h_p^2 + 4^{f(p)} h(\sqrt{-p})^2\right)$$

where $f(p) = \begin{cases} -1 & \text{if } p \equiv 1 \pmod 4 \\ 0 & \text{if } p \equiv 7 \pmod 8 \\ 1 & \text{if } p \equiv 3 \pmod 8 \end{cases}$

We note the close resemblance of this formula to the following one for t_p, due to Deuring [3]:

Proposition 2.3: Let p be a prime > 3. Then:

$$t_p = \frac{1}{2}\left(h_p + 2^{f(p)} h(\sqrt{-p})\right), \text{ where } f(p) \text{ is as}$$

in Corollary 2.2.

One should keep in mind that h_p is very easy to compute. In fact, as a direct application of Theorem 1.7, we have:

$$h_p = \begin{cases} \frac{1}{12}(p-1) & \text{if } p \equiv 1 \pmod{12} \\ \frac{1}{12}(p+7) & \text{if } p \equiv 5 \pmod{12} \\ \frac{1}{12}(p+5) & \text{if } p \equiv 7 \pmod{12} \\ \frac{1}{12}(p+13) & \text{if } p \equiv 11 \pmod{12} \end{cases}$$

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

§2. Outline of the proof

We do not apply the Selberg Trace Formula to the setting afforded by the orthogonal groups which appear in the usual definition of the class number H (cf. I.2). The reason is that the definitions of these groups involve a norm condition which makes integration unmanageable and which also complicates conjugacy considerations. To avoid these difficulties, we replace the usual definition of H by the one mentioned at the end of I.3:

H = the number of equivalence classes of normal ideals in $\mathcal{O}$.

Notation: (a) For any associative ring R with an identity element, let R^* = the group of all invertible elements in R.

(b) For any group S, let $\Delta(S)$ be the diagonal subgroup of $S\times S$, that is, let $\Delta(S) = \{(s,s) \mid s \in S\}$.

We set $G = (\mathcal{O}^*\times \mathcal{O}^*)/\Delta(\mathbb{Q}^*)$. Then G acts on the set of normal ideals, two normal ideals being equivalent if and only if they are in the same orbit. Let $J_{\mathcal{O}}$ be the idele group of $\mathcal{O}$ and let $J_{\mathbb{Q}}$ be the idele group of $\mathbb{Q}$. We then define subgroups:

$$J_{\mathcal{O}}^1 = \left\{(\alpha_p) \in J_{\mathcal{O}} \mid \prod_p |N(\alpha_p)|_p = 1\right\}, \quad J_{\mathbb{Q}}^1 = \left\{(r_p) \in J_{\mathbb{Q}} \mid \prod_p |r_p|_p = 1\right\}.$$

Set $G_A = (J_{\mathcal{O}}^1 \times J_{\mathcal{O}}^1)/\Delta(J_{\mathbb{Q}}^1)$. Then G_A acts transitively on the set of normal ideals of $\mathcal{O}$. If Θ is a maximal order in $\mathcal{O}$, we set $G_{\tilde{\Theta}}$ = the isotropy group of Θ under this action. One easily verifies that G_A is a locally compact unimodular group, $G_{\tilde{\Theta}}$ is an open compact subgroup and G is a discrete subgroup such that G_A/G is compact. Then $G_{\tilde{\Theta}}\backslash G_A/G$ must be a finite set, in fact, of cardinality = H. We then apply the Selberg Trace Formula to

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

$F_{\tilde{\theta}}$, the characteristic function of $G_{\tilde{\theta}}$, to obtain:

$$H = \mathrm{Tr}(F_{\tilde{\theta}}) = \sum_{\{\delta\}} \int_{G_A/G(\delta)} \Psi_\delta(\rho)\, d_\delta\rho$$

where $\Psi_\delta(\rho) = F(\rho\delta\rho^{-1})$ for $\delta \in G$, $\rho \in G_A$.

In this trace sum the only conjugacy classes which make a non-zero contribution are those containing the following elements:

(i) $\delta \equiv (\pm 1, 1) \pmod{\Delta(\mathbb{Q}^*)}$

(ii) $\delta \equiv (1,u)$ or $(u,1)$, where $u^2 + 1 = 0$ or $u^2 \pm u + 1 = 0$

(iii) $\delta \equiv (u,u')$, where u,u' are as in (ii).

(iv) $\delta \equiv (\mu,\nu)$, where μ,ν are integral, $N(\mu) = N(\nu) = m$ and $m \neq 1$ divides d.

The contributions to the trace of the conjugacy classes represented by cases (i),(ii) and (iii) give the term $2^{-e} h_d^2$ in our formula. The remaining terms are contributed by the conjugacy classes represented by case (iv).

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

§1. Preparatory discussion

Let (V,q) be a quadratic vector space over $\mathbb{Q}$. We denote by $O^+(V_A)$ the adelization of the group $O^+(V)$, that is, the restricted direct product of the groups $O^+(V_p)$, p finite or $p = \infty$, with respect to the compact subgroups $O^+(M_p)$, p finite, where M is a lattice in V (cf.[11] and [13]). As usual, this definition of $O^+(V_A)$ does not depend on the choice of lattice M. For any lattice M we define: $O^+(\tilde{M}) = \prod_{p\neq\infty} O^+(M_p) \times O^+(V_{\mathbb{R}})$.

Then $O^+(V_A)$ becomes a locally compact topological group with respect to the unique topology such that $O^+(\tilde{M})$ (with the product topology) is an open subgroup. This topology is, of course, independent of the choice of M. One can show that $O^+(V)$ is a discrete subgroup of $O^+(V_A)$ such that the homogeneous space $O^+(V_A)/O^+(V)$ has a finite left-invariant measure. In particular, $O^+(V_A)$ must be unimodular. If M is a maximal integral lattice, then it follows directly from the definition of H that we have a double coset decomposition: $O^+(V_A) = \bigcup_{k=1}^{H} O^+(\tilde{M})\xi_k O^+(V)$.

Moreover, if q is definite, then $O^+(\tilde{M})$ is compact. It would seem natural, therefore, to apply the Selberg Trace Formula to the characteristic function of $O^+(\tilde{M})$ in order to obtain a formula for H. In fact, this can be done in both the binary and ternary cases, at least under the restrictions mentioned in I.2. However, there are certain difficulties which arise in trying to do it for the case of a positive definite quaternion algebra $(\mathcal{A},N)$ over $\mathbb{Q}$.

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

In this case it is known that $O^+(\mathcal{O})$ is completely represented by all mappings of the type: $x \to \alpha x \beta^{-1}$, where $N(\alpha) = N(\beta)$ and $\alpha, \beta \in \mathcal{O}^*$. It follows that $O^+(\mathcal{O}) \cong (\mathcal{O}^* \times \mathcal{O}^*)^1 / \Delta(\mathbb{Q}^*)$, where $(\mathcal{O}^* \times \mathcal{O}^*)^1 = \{(\alpha, \beta) \in \mathcal{O}^* \times \mathcal{O}^* \mid N(\alpha) = N(\beta)\}$. The groups $O^+(\mathcal{O}_A)$ and $O^+(\tilde{M})$ can be described by similar norm conditions. These norm conditions are what cause the difficulties alluded to above. In the first place, since we sum over conjugacy classes inside $O^+(\mathcal{O})$, we must be able to settle the question of conjugacy inside $(\mathcal{O}^* \times \mathcal{O}^*)^1$, which seems to be a complicated matter. It would be extremely helpful if we could replace $(\mathcal{O}^* \times \mathcal{O}^*)^1$ somehow by $\mathcal{O}^* \times \mathcal{O}^*$, where questions of conjugacy are easily settled.

In the second place, the norm conditions are also inherited by the centralizers $(O^+(\mathcal{O}))(\delta)$, $(O^+(\mathcal{O}_A))(\delta)$ and $(O^+(\tilde{M}))(\delta)$ for $\delta \in O^+(\mathcal{O})$. The fact that these groups can have very complicated structures comes from the possibility that $(O^+(\mathcal{O}))(\delta)$ may be isomorphic to a group of the type: $(E^* \times F^*)^1 / \Delta(\mathbb{Q}^*)$, where E and F are certain imaginary quadratic extensions within $\mathcal{O}$ and $(E^* \times F^*)^1 = \{(x,y) \in E^* \times F^* \mid N(x) = N(y)\}$. This rather unpleasant possibility for $(O^+(\mathcal{O}))(\delta)$ makes the evaluation of the integrals occurring in the trace formula unmanageable. The way to avoid both these difficulties simultaneously is provided in the following:

Proposition 3.1: H = the number of equivalence classes of normal ideals of $\mathcal{O}$.

Proof

Let I be a normal ideal. Since N represents all positive

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

rationals, there exists $\alpha \in \mathcal{O}^*$ such that $N(\alpha) = N(I)$. Then $I\alpha^{-1}$ is equivalent to I and $N(I\alpha^{-1}) = 1$. Hence any equivalence class of normal ideals can be represented by a normal ideal of norm 1. Furthermore, it is almost trivial to see that the set of normal ideals having norm 1 is precisely the set of all maximal integral lattices in $\mathcal{O}$ (cf. p.11). Suppose I and J are normal ideals of norm 1. Then: I and J are equivalent as normal ideals $\iff$ there exist $\alpha,\beta \in \mathcal{O}^*$ such that $\alpha I\beta = J \iff \alpha I\beta = J$ and $N(\alpha\beta) = N(\alpha I\beta) = N(J) = 1 \iff \alpha I\beta = J$ and $N(\alpha) = N(\beta^{-1}) \iff I \sim J$. [QED]

It is this definition of H which we shall utilize throughout the remainder of this dissertation.

We have a homomorphism $\psi: \mathcal{O}^* \times \mathcal{O}^* \longrightarrow GL(\mathcal{O})$ defined by: $(\psi(\alpha,\beta))x = \alpha x \beta^{-1}$, $x \in \mathcal{O}$, $\alpha,\beta \in \mathcal{O}^*$. Then $\mathrm{Ker}(\psi) = \Delta(\mathbb{Q}^*)$, so we have an embedding of $G = \mathcal{O}^* \times \mathcal{O}^*/\Delta(\mathbb{Q}^*)$ in $GL(\mathcal{O})$. If $\delta \in G$ and $\alpha,\beta \in \mathcal{O}^*$, $\delta \equiv (\alpha,\beta)$ will mean $\delta \equiv (\alpha,\beta) \bmod \Delta(\mathbb{Q}^*)$. Then G acts on the set of normal ideals by: $\delta \equiv (\alpha,\beta): I \longrightarrow \alpha I \beta^{-1}$. Two normal ideals are equivalent if and only if they lie in the same orbit under this action of G.

§2. Structure of isotropy groups

For any normal ideal I we set G_I = the isotropy group of I under G. Suppose $\delta \in G_I$, $\delta \equiv (\alpha,\beta)$, $\alpha,\beta \in \mathcal{O}^*$. Then $\alpha I\beta^{-1} = I \implies N(\alpha\beta^{-1}) = 1 \implies N(\alpha) = N(\beta)$. Therefore $G_I \subset O^+(I)$. The reverse inclusion is obvious. We conclude that $G_I = O^+(I)$. Let us examine the structure of $O^+(I)$. We let $\mathcal{O}_\ell$ = the left order of I, $\mathcal{O}_r$ = the right order of I. Suppose $\delta \equiv (\alpha,\beta) \in O^+(I)$. Then

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

$\alpha I \beta^{-1} = I \Rightarrow \alpha \mathcal{O}_\ell \alpha^{-1} = \mathcal{O}_\ell$ and $\beta \mathcal{O}_r \beta^{-1} = \mathcal{O}_r$. In other words, α normalizes the order $\mathcal{O}_\ell$ and β normalizes the order $\mathcal{O}_r$. If $\mathcal{O}$ is any maximal order of $\mathcal{A}$, let $\mathcal{N}(\mathcal{O})$ = the group of all those elements in $\mathcal{A}^*$ which normalize $\mathcal{O}$. We proceed now to investigate the structure of $\mathcal{N}(\mathcal{O})$.

Given a lattice L in a finite dimensional vector space V over $\mathbb{Q}$, we set $\tilde{L} = \prod_{p \neq \infty} L_p$. Then the <u>local-global correspondence</u> for lattices in V says the following: (cf.[9], p.218)

(i) If L and M are lattices in V, then $L_p = M_p$ for almost all p.

(ii) Let L be a lattice in V. Suppose a local lattice M(p) is given at each $p \neq \infty$ and suppose $M(p) = L_p$ for almost all p. Then there exists a <u>unique</u> lattice M in V such that $\tilde{M} = \prod_{p \neq \infty} M(p)$.

The group $J^1_{\mathcal{A}}$ then acts by conjugation on the set of maximal orders as follows: If $\tilde{\alpha} = (\alpha_p) \in J^1_{\mathcal{A}}$ and $\mathcal{O}$ is a maximal order of $\mathcal{A}$, then, by the local-global correspondence for lattices in $\mathcal{A}$, there exists a unique maximal order $\mathcal{O}'$ of $\mathcal{A}$ such that $\tilde{\mathcal{O}}' = \tilde{\alpha} \tilde{\mathcal{O}} \tilde{\alpha}^{-1} = \prod_{p \neq \infty} \alpha_p \mathcal{O}_p \alpha_p^{-1}$. For any maximal order $\mathcal{O}$ of $\mathcal{A}$, we define $\mathcal{N}(\tilde{\mathcal{O}}) = \{\tilde{\alpha} \in J^1_{\mathcal{A}} \mid \tilde{\alpha} \tilde{\mathcal{O}} \tilde{\alpha}^{-1} = \tilde{\mathcal{O}}\}$. Obviously, $\mathcal{N}(\mathcal{O}) = \mathcal{N}(\tilde{\mathcal{O}}) \cap \mathcal{A}^*$, where $\mathcal{A}^*$ is viewed as a subgroup of $J^1_{\mathcal{A}}$ under the canonical diagonal embedding. If $\tilde{\alpha} = (\alpha_p) \in \mathcal{N}(\tilde{\mathcal{O}})$, we set $I^{\tilde{\alpha}}$ = the unique lattice in $\mathcal{A}$ such that $I^{\tilde{\alpha}}_p = \mathcal{O}_p \alpha_p$ for all finite p. Then $I^{\tilde{\alpha}}$ is clearly a two-sided ideal of $\mathcal{O}$. Moreover, any two-sided ideal of $\mathcal{O}$ is obtained in this way. Let $\mathcal{I}(\mathcal{O})$ = the group of all two-sided ideals of $\mathcal{O}$; $P(\mathcal{O})$ = the subgroup of $\mathcal{I}(\mathcal{O})$ of rational principal ideals, that is, ideals I such that $I = \mathcal{O} r$, $r \in \mathbb{Q}^*$.

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

Let $U(\mathfrak{O}_p)$ = the unit group of $\mathfrak{O}_p$ for $p \neq \infty$ and let $U_\infty = \{x \in \mathfrak{o}_\infty^* | N(x) = 1\}$. We then set $U^1(\tilde{\mathfrak{O}}) = \prod_{p \neq \infty} U(\mathfrak{O}_p) \times U_\infty$.

One easily sees that the mapping $\tilde{\alpha} \to I^{\tilde{\alpha}}$ is a homomorphism which induces a canonical isomorphism: $\mathcal{N}(\tilde{\mathfrak{O}})/J_{\mathbb{Q}}^1 U^1(\tilde{\mathfrak{O}}) \cong \mathcal{I}(\mathfrak{O})/P(\mathfrak{O})$.

It is known that $\mathcal{I}(\mathfrak{O})/P(\mathfrak{O})$ is an elementary abelian 2-group of order 2^e. In fact, we may choose the set of coset representatives modulo $P(\mathfrak{O})$ to be: $\mathcal{P}(\mathfrak{O}) = \{\mathfrak{p}_1^{\varepsilon_1} \cdots \mathfrak{p}_e^{\varepsilon_e} | \varepsilon_i = 0 \text{ or } 1\}$, where $\mathfrak{p}_i$, $i = 1,\ldots,e$ is the unique two-sided prime ideal of $\mathfrak{O}$ such that $N(\mathfrak{p}_i) = p_i$. We note in particular that the norm mapping induces an isomorphism: $\mathcal{I}(\mathfrak{O})/P(\mathfrak{O}) \cong \Phi(d)$, where $\Phi(d)$ = the subgroup of $\mathbb{Q}^*/(\mathbb{Q}^*)^2$ generated by $\{p_1,\ldots,p_e\}$. The group $\Pi(\mathfrak{O})$ of <u>principal</u> two-sided ideals of $\mathfrak{O}$ modulo rational principal ones must then be an elementary abelian 2-group of order 2^f, where $f \leq e$. Let $W(\mathfrak{O})$ = the unit group of $\mathfrak{O}$, $w(\mathfrak{O}) = |W(\mathfrak{O})|$. Clearly, $\alpha \in \mathcal{N}(\mathfrak{O}) \iff \mathfrak{O}\alpha = \alpha\mathfrak{O}$ is a principal two-sided ideal of $\mathfrak{O}$. Therefore, the mapping: $\mathcal{N}(\mathfrak{O}) \ni \alpha \to \mathfrak{O}\cdot\alpha$ induces an isomorphism: $\mathcal{N}(\mathfrak{O})/\mathbb{Q}^* W(\mathfrak{O}) \cong \Pi(\mathfrak{O})$. Using this and the fact that representatives for $\Pi(\mathfrak{O})$ may be chosen from $\mathcal{P}(\mathfrak{O})$, it is easily seen that $\alpha \in \mathfrak{o}^*$ normalizes $\mathfrak{O} \iff \alpha$ is a rational multiple of an element $\alpha' \in \mathfrak{O}$ such that $N(\alpha')$ is an integer dividing d.

From above we have: $\mathcal{N}(\mathfrak{O})/\mathbb{Q}^* \Big/ \mathbb{Q}^* W(\mathfrak{O})/\mathbb{Q}^* \cong \Pi(\mathfrak{O})$. Hence $[\mathcal{N}(\mathfrak{O}) : \mathbb{Q}^*] = 2^f [W(\mathfrak{O}) : W(\mathfrak{O}) \cap \mathbb{Q}^*] = 2^{f-1} w(\mathfrak{O})$. Let $N(\Pi(\mathfrak{O}))$ denote the image of $\Pi(\mathfrak{O})$ under the isomorphism $\mathcal{I}(\mathfrak{O})/P(\mathfrak{O}) \cong \Phi(d)$. Then, returning to our investigation of $O^+(I)$, we let $\Pi(\mathfrak{O}_\ell) = \Pi_\ell$, $\Pi(\mathfrak{O}_r) = \Pi_r$, $w(\mathfrak{O}_\ell) = w_\ell$, $w(\mathfrak{O}_r) = w_r$, $2^{f_\ell} = |\Pi_\ell|$,

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

$2^{f_r} = |\Pi_r|$. We write $|N(\Pi_\ell) \cap N(\Pi_r)| = 2^{f_{\ell r}}$ for some $f_{\ell r} \leq \mathrm{Min}(f_\ell, f_r)$. Set $(\mathcal{N}(\mathcal{O}_\ell) \times \mathcal{N}(\mathcal{O}_r))^1 = \mathcal{N}(\mathcal{O}_\ell) \times \mathcal{N}(\mathcal{O}_r) \cap (\mathcal{A}^* \times \mathcal{A}^*)^1$ We have a surjection $\tilde{N}: (\mathcal{N}(\mathcal{O}_\ell) \times \mathcal{N}(\mathcal{O}_r))^1 \longrightarrow N(\Pi_\ell) \cap N(\Pi_r)$ defined by: $\tilde{N}(\alpha,\beta) = N(\alpha) \bmod (\mathbb{Q}^*)^2$ for $(\alpha,\beta) \in (\mathcal{N}(\mathcal{O}_\ell) \times \mathcal{N}(\mathcal{O}_r))^1$ One easily verifies that $\mathrm{Ker}(\tilde{N}) = (W(\mathcal{O}_\ell) \times W(\mathcal{O}_r)) \Delta(\mathbb{Q}^*)$. Using this, and arguing exactly as above, we conclude that $|O^+(I)| = [(\mathcal{N}(\mathcal{O}_\ell) \times \mathcal{N}(\mathcal{O}_r))^1 : \Delta(\mathbb{Q}^*)] = 2^{f_{\ell r}-1} w_\ell w_r$. Moreover, from our discussion it is evident that there are essentially only four types of elements inside $O^+(I)$:

(i) $\delta \equiv (\pm 1, 1)$

(ii) $\delta \equiv (u,1)$ or $(1,u)$, where $u \notin \mathbb{Q}$ is a unit of $\mathcal{O}_\ell$ or $\mathcal{O}_r$, respectively.

(iii) $\delta \equiv (u,v)$, where $u \notin \mathbb{Q}$, $v \notin \mathbb{Q}$ and u,v are units of $\mathcal{O}_\ell$, $\mathcal{O}_r$, respectively.

(iv) $\delta \equiv (\mu,\nu)$, where $\mu \notin \mathbb{Q}$, $\nu \notin \mathbb{Q}$; $\mu \in \mathcal{O}_\ell$, $\nu \in \mathcal{O}_r$; $N(\mu) = N(\nu) = m$ and $m \neq 1$ divides d.

§3. The adelized setting

We recall from III.1 that there is an action of G on the set of normal ideals of $\mathcal{A}$, two normal ideals being equivalent if and only if they are in the same orbit under G. We also have an action of $G_A = J^1_{\mathcal{A}} \times J^1_{\mathcal{A}} / \Delta(J^1_{\mathbb{Q}})$ on the set of normal ideals as follows: by the local-global correspondence for lattices, we may identify each normal ideal I with its corresponding $\tilde{I} = \prod_{p \neq \infty} I_p$; if $\delta \in G_A$, $\delta \equiv ((\alpha_p),(\beta_p))$ takes $\tilde{I}$ to $\prod_{p \neq \infty} \alpha_p I_p \beta_p^{-1} = \tilde{J}$ for some normal ideal J of $\mathcal{A}$. By the discussion in I.3, this action of

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

G_A is transitive. If I is a normal ideal of $\mathfrak{a}$, we set G_I = the isotropy group of I under G_A. Since $\Delta(J_{\mathbb{Q}}^1) \cap \mathfrak{a}^* \times \mathfrak{a}^* = \Delta(\mathbb{Q}^*)$, G may be considered as a subgroup of G_A. This identification is consistent with the group actions already defined. It follows that, under this identification, $G_I = G_{\tilde{I}} \cap G$.

Let us fix a maximal order $\mathfrak{o}$ of $\mathfrak{a}$. We then have a double coset decomposition: $G_A = \bigcup_{k=1}^{H} G_{\tilde{\mathfrak{o}}} \tilde{\delta}_k G = \bigcup_{k=1}^{H} G \tilde{\delta}_k^{-1} G_{\tilde{\mathfrak{o}}}$, where the double coset $G \tilde{\delta}_k^{-1} G_{\tilde{\mathfrak{o}}}$ corresponds to the equivalence class of the normal ideal $\tilde{\delta}_k^{-1} \tilde{\mathfrak{o}} = \tilde{M}_k$, $k = 1, \ldots, H$. For convenience, we set $\tilde{\delta}_1 = 1$, $M_1 = \mathfrak{o}$. Let $G_p = \mathfrak{a}_p^* \times \mathfrak{a}_p^* / \Delta(\mathbb{Q}_p^*)$ for p finite and let $G_\infty = \mathfrak{a}_\infty^* \times \mathfrak{a}_\infty^* / \Delta(\mathbb{R}^*)$. We define $\mathcal{G}_A$ to be the restricted direct product of the groups G_p, p finite or infinite, with respect to the compact groups $U(\mathfrak{o}_p) \times U(\mathfrak{o}_p) / \Delta(U_p)$, where U_p is, of course, the group of p-adic units. This definition is meaningful, since $\Delta(\mathbb{Q}_p^*) \cap U(\mathfrak{o}_p) \times U(\mathfrak{o}_p) = \Delta(U_p)$ for all finite p, giving an embedding: $U(\mathfrak{o}_p) \times U(\mathfrak{o}_p) / \Delta(U_p) \subset \mathfrak{a}_p^* \times \mathfrak{a}_p^* / \Delta(\mathbb{Q}_p^*)$. We can immediately conclude that $\mathcal{G}_A$ is a locally compact unimodular group, G is a discrete subgroup of $\mathcal{G}_A$, and $U(\tilde{\mathfrak{o}}) \times U(\tilde{\mathfrak{o}}) / \Delta(U_{\mathbb{Q}})$ is an open subgroup of $\mathcal{G}_A$, where $U(\tilde{\mathfrak{o}}) = \prod_{p \neq \infty} U(\mathfrak{o}_p) \times \mathfrak{a}_\infty^*$, $U_{\mathbb{Q}} = \prod_{p \neq \infty} U_p \times \mathbb{R}^*$.

Since G_A is a closed subgroup of $\mathcal{G}_A$, it follows that G_A is a locally compact topological group. Moreover, G is a discrete subgroup of G_A and $U^1(\tilde{\mathfrak{o}}) \times U^1(\tilde{\mathfrak{o}}) / \Delta(U_{\mathbb{Q}}^1)$ is a compact open subgroup of G_A, where $U_{\mathbb{Q}}^1 = J_{\mathbb{Q}}^1 \cap U_{\mathbb{Q}} = \prod_{p \neq \infty} U_p \times \{\pm 1\}$. One easily sees that $U^1(\tilde{\mathfrak{o}}) \times U^1(\tilde{\mathfrak{o}}) / \Delta(U_{\mathbb{Q}}^1)$ is contained in $G_{\tilde{\mathfrak{o}}}$; in fact, we have:

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

Proposition 3.2: $[G_{\tilde{\delta}} : U^1(\tilde{\mathcal{O}})\times U^1(\tilde{\mathcal{O}})/\Delta(U^1_{\mathbb{Q}})] = 2^e$.

Proof

Let us write $G_{\mathcal{O}_p} = \{\delta_p \in G_p \mid \delta_p(\mathcal{O}_p) = \mathcal{O}_p\}$ for p finite. If p is finite and split, it is well-known (and implicit in our discussion in III.2) that the group of all elements in $\mathcal{O}_p^*$ which normalize $\mathcal{O}_p$ is precisely: $U(\mathcal{O}_p)\mathbb{Q}_p^*$. Using this, one can easily show that $G_{\mathcal{O}_p} = (U(\mathcal{O}_p)\times U(\mathcal{O}_p))\Delta(\mathbb{Q}_p^*)/\Delta(\mathbb{Q}_p^*) = U(\mathcal{O}_p)\times U(\mathcal{O}_p)/\Delta(\mathbb{Q}_p^*) \cap U(\mathcal{O}_p)\times U(\mathcal{O}_p) = U(\mathcal{O}_p)\times U(\mathcal{O}_p)/\Delta(U_p)$.

For p finite and non-split it is easy to see that $G_{\mathcal{O}_p} = \{(\alpha_p,\beta_p) \in \mathcal{O}_p^*\times\mathcal{O}_p^* \mid \alpha_p\beta_p^{-1} \in U(\mathcal{O}_p)\}/\Delta(\mathbb{Q}_p^*)$. Consider the mapping: $G_{\mathcal{O}_p} \ni \delta_p \equiv (\alpha_p,\beta_p) \to N(\alpha_p) \bmod U_p(\mathbb{Q}_p^*)^2$. This is a surjective homomorphism with kernel $= (U(\mathcal{O}_p)\times U(\mathcal{O}_p))\Delta(\mathbb{Q}_p^*)/\Delta(\mathbb{Q}_p^*) = U(\mathcal{O}_p)\times U(\mathcal{O}_p)/\Delta(U_p)$. Thus $[G_{\mathcal{O}_p} : U(\mathcal{O}_p)\times U(\mathcal{O}_p)/\Delta(U_p)] = [\mathbb{Q}_p^* : U_p(\mathbb{Q}_p^*)^2] = 2$ for p non-split. If $\tilde{\delta} = (\delta_p) \in G_{\tilde{\mathcal{O}}}$, with $\delta_p \equiv (\alpha_p,\beta_p)$, then from the preceding discussion we know that $|N(\alpha_p)|_p = |N(\beta_p)|_p$ for all $p \neq \infty$. Therefore, $\prod_{p\neq\infty}|N(\alpha_p)|_p = \prod_{p\neq\infty}|N(\beta_p)|_p \iff |N(\alpha_\infty)|_\infty = |N(\beta_\infty)|_\infty \iff N(\alpha_\infty) = N(\beta_\infty)$. It follows that $G_{\tilde{\delta}} = \prod_{p\neq\infty} G_{\mathcal{O}_p} \times G^1_\infty$, where $G^1_\infty = (\mathcal{O}_\infty^*\times\mathcal{O}_\infty^*)^1/\Delta(\mathbb{R}^*)$, which can be identified with $U_\infty\times U_\infty/\Delta(\pm 1)$. We conclude that $[G_{\tilde{\delta}} : U^1(\tilde{\mathcal{O}})\times U^1(\tilde{\mathcal{O}})/\Delta(U^1_{\mathbb{Q}})] = 2^e$. [QED]

Corollary 3.3: $G_{\tilde{\delta}}$ is an open compact subgroup of G_A and the quotient space G_A/G is compact.

Proof

The first statement is an obvious consequence of the preceding proposition. The second follows trivially from the finite

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

decomposition: $G_A = \bigcup_{k=1}^{H} G_{\tilde{\mathcal{O}}}\, \tilde{\delta}_k G$. [QED]

As an immediate consequence of this corollary we may conclude that G_A is unimodular.

§4. Application of the Selberg Trace Formula

We are now in a position to apply the Selberg Trace Formula to the setting: $(G_{\tilde{\mathcal{O}}}, G_A, G)$, where $\mathcal{O}$ is a maximal order of $\mathcal{A}$. We normalize the Haar measure μ on G_A so that $\mu(G_{\tilde{\mathcal{O}}}) = 1$. Then $L^2(G_{\tilde{\mathcal{O}}} \backslash G_A / G)$ is a Hilbert space of dimension H over $\mathbb{C}$. Let f_k = the characteristic function of the double coset $G_{\tilde{\mathcal{O}}}\, \tilde{\delta}_k G$, $k = 1,\ldots,H$. Clearly, $f_1,\ldots,f_H$ is a basis of $L^2(G_{\tilde{\mathcal{O}}} \backslash G_A / G)$ over $\mathbb{C}$. We set $E(M_k) = |G_{M_k}|$. Then we have:

$$\|f_k\|^2 = \langle f_k, f_k \rangle = \int_{G_{\tilde{\mathcal{O}}} \tilde{\delta}_k G / G} d\rho = \int_{\tilde{\delta}_k^{-1} G_{\tilde{\mathcal{O}}} \tilde{\delta}_k G / G} d\rho = \int_{G_{\tilde{M}_k} G / G} d\rho =$$

$$\int_{G_{\tilde{M}_k} / G_{M_k}} d\rho = \frac{1}{E(M_k)} \int_{G_{\tilde{M}_k}} d\rho = \frac{1}{E(M_k)} .$$ Clearly, $\langle f_j, f_k \rangle = 0$ if $j \neq k$.

Therefore, $\|f\|^2 = \sum_{k=1}^{H} |c_k|^2 \cdot \frac{1}{E(M_k)}$ if $f = \sum_{k=1}^{H} c_k f_k$, $c_k \in \mathbb{C}$.

In particular, if f = the characteristic function of G_A, then:

$$\|f\|^2 = v(G_A/G) = \sum_{k=1}^{H} \frac{1}{E(M_k)} .$$

We apply the Selberg Trace Formula to the operator defined by $F_{\tilde{\mathcal{O}}}$ = the characteristic function of $G_{\tilde{\mathcal{O}}}$. If $f \in L^2(G_{\tilde{\mathcal{O}}} \backslash G_A / G)$,

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

then $(F_{\tilde{\theta}}(f))(\rho) = \int_{G_A} F_{\tilde{\theta}}(\sigma) f(\sigma^{-1}\rho)\, d\sigma = \int_{G_{\tilde{\theta}}} f(\sigma^{-1}\rho)\, d\sigma = \int_{G_{\tilde{\theta}}} f(\rho)\, d\sigma$

$= f(\rho)$. Therefore, $F_{\tilde{\theta}}$ induces the identity operator on the Hilbert space $L^2(G_{\tilde{\theta}}\backslash G_A/G)$. Then, by the Selberg Trace Formula,

$$H = \mathrm{Tr}(F_{\tilde{\theta}}) = \sum_{\{\delta\}} \int_{G_A/G(\delta)} \Psi_\delta(\rho)\, d_\delta\rho$$

where $\Psi_\delta(\rho) = F_{\tilde{\theta}}(\rho\delta\rho^{-1})$ for all $\rho \in G_A$.

For $\delta \in G$, the conjugacy class $\{\delta\}$ needs to be considered in this sum only if there exists $\rho \in G_A$ such that $\rho\delta\rho^{-1} \in G_{\tilde{\theta}} \Longrightarrow$ $\delta \in \rho^{-1}G_{\tilde{\theta}}\rho = G_{\rho^{-1}\tilde{\theta}}$. But $\rho^{-1}\tilde{\theta}$ is equivalent to $\tilde{M}_k$ for some k, so $G_{\rho^{-1}\tilde{\theta}}$ is conjugate to some $G_{\tilde{M}_k}$ by an element of G. Thus we need only consider the conjugacy classes of those δ in G which lie in $G_{\tilde{M}_k}$ for $k = 1,\ldots,H$. In other words, we need only consider the conjugacy classes of elements in $G_{\tilde{M}_k} \cap G = G_{M_k}$, $k = 1,\ldots,H$. This shows explicitly the finiteness of the trace sum.

Let $\mathcal{O}_\ell$, $\mathcal{O}_r$ be the left and right orders, respectively, of the fixed normal ideal M_k. If $\delta \in G_{M_k}$, then δ must be represented by one of the cases (i) - (iv) mentioned at the end of III.2. The remainder of Chapter III will be devoted to computing the contributions to the trace sum of the conjugacy classes lying in each of the cases (i) - (iv). Before proceeding to compute these contributions, we need the following elementary discussion:

Definition 3.4: An element $x \in \mathcal{O}$ is said to be pure if $x \notin Q$, but $x^2 \in Q$.

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

This definition is clearly equivalent to: $T(x) = 0$, $x \neq 0$. If $\mathcal{A} = \langle w,z \rangle$ is a representation of $\mathcal{A}$ as a cyclic algebra, then x is pure $\iff$ $x = aw + bz + cwz$, $a,b,c \in \mathbb{Q}$, $x \neq 0$.

Definition 3.5: An element $g \in G$ is said to be pure if $g \equiv (x,y)$, where both x and y are pure.

This definition does not depend on the choice of x and y. An element of $\mathcal{A}$ or G which is not pure is said to be impure.

Lemma 3.6: Suppose $x \in \mathcal{A}$. There exists $\alpha \in \mathcal{A}^*$ such that $\alpha x \alpha^{-1} = cx$, $1 \neq c \in \mathbb{Q} \iff$ x is pure and $c = -1$.

Proof

There exists $\alpha \in \mathcal{A}^*$ such that $\alpha x \alpha^{-1} = cx$, $c \neq 1 \iff x \notin \mathbb{Q}$ and $x \to cx$ gives a non-trivial automorphism of the quadratic extension $\mathbb{Q}(x)$ over $\mathbb{Q} \iff$ x is pure and $c = -1$. [QED]

For any $x \in \mathcal{A}^*$, define $C(x)$ = the centralizer of x in $\mathcal{A}^*$. If $G \ni \delta \equiv (x,y)$, then obviously $G(\delta) \supset C(x) \times C(y)/\Delta(\mathbb{Q}^*)$.

Proposition 3.7: If δ is impure, then $G(\delta) = C(x) \times C(y)/\Delta(\mathbb{Q}^*)$ If δ is pure, then $C(x) = \mathbb{Q}(x)^*$, $C(y) = \mathbb{Q}(y)^*$ and we have: $[G(\delta) : \mathbb{Q}(x)^* \times \mathbb{Q}(y)^*/\Delta(\mathbb{Q}^*)] = 2$.

Proof

Suppose $g \equiv (\xi,\omega) \in \mathcal{A}^* \times \mathcal{A}^*$ and there exists a $q \equiv (c,c)$ in $\Delta(\mathbb{Q}^*)$ such that $g(x,y)g^{-1} = q(x,y)$. Hence $\xi x \xi^{-1} = cx$, $\omega y \omega^{-1} = cy$. If either x or y is impure, then, by the preceding lemma, $c = 1$. In other words, $\xi \in C(x)$ and $\omega \in C(y)$. If both x and y are pure, then we have automorphisms $\sigma \in G(\mathbb{Q}(x)/\mathbb{Q})$ (the Galois group of $\mathbb{Q}(x)$ over $\mathbb{Q}$) and $\tau \in G(\mathbb{Q}(y)/\mathbb{Q})$ such that $\sigma(x) = -x$, $\tau(y) = -y$. Hence there exist $\xi_0, \omega_0 \in \mathcal{A}^*$ such that $\xi_0 x \xi_0^{-1} = -x$, $\omega_0 y \omega_0^{-1} = -y$.

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

Moreover, it is clear that the set $\{\xi \mid \xi x \xi^{-1} = -x\}$ is just $\mathbb{Q}(x)^*\xi_0 = \xi_0 \mathbb{Q}(x)^*$ and $\{\omega \mid \omega y \omega^{-1} = -y\} = \mathbb{Q}(y)^*\omega_0 = \omega_0 \mathbb{Q}(y)^*$. Thus $G(\delta) = \mathbb{Q}(x)^* \times \mathbb{Q}(y)^*/\Delta(\mathbb{Q}^*) \cup g_0\left(\mathbb{Q}(x)^* \times \mathbb{Q}(y)^*/\Delta(\mathbb{Q}^*)\right)$, where $g_0 \equiv (\xi_0, \omega_0)$. [QED]

§5. The principal term $\delta \equiv (\pm 1, 1)$

If $\delta \equiv (\pm 1, 1)$, then $G(\delta) = G$, so the contribution of δ is $v(G_A/G) = \sum_{k=1}^{H} \frac{1}{E(M_k)}$. By the theory of Tamagawa numbers (cf.[13] and [14]) we know that $\prod_p \alpha(\mathcal{O}_p) \cdot \left(\sum_{k=1}^{H} \frac{1}{E(M_k)}\right) = \tau(O^+(\mathcal{A})) = 2$, where $\alpha(\mathcal{O}_p) = \mu_p(O^+(\mathcal{O}_p))$ for p finite, with μ_p = the canonical invariant measure on $O^+(\mathcal{O}_p)$; $\alpha(\mathcal{O}_\infty) = \mu_\infty(O^+(\mathcal{A}_\infty))$, μ_∞ = the canonical invariant measure on $O^+(\mathcal{A}_\infty)$. It is easy to see that $O^+(\mathcal{O}_p) = \{(x_p, y_p) \in U(\mathcal{O}_p) \times U(\mathcal{O}_p) \mid N(x_p) = N(y_p)\}/\Delta(U_p)$ for p split ; $O^+(\mathcal{O}_p) = \{(x_p, y_p) \ \mathcal{A}_p^* \times \mathcal{A}_p^* \mid N(x_p) = N(y_p)\}/\Delta(\mathbb{Q}_p^*)$ for p non-split.

If p is a split prime, then $\mathcal{O}_p \cong M(2, \mathbb{Z}_p)$ and there is an obvious mapping $\theta: SL(2, \mathbb{Z}_p) \times SL(2, \mathbb{Z}_p) \longrightarrow O^+(\mathcal{O}_p)$ with $\mathrm{Ker}(\theta) = \{(1,1),(-1,-1)\}$. θ is a continuous open homomorphism. One easily sees that $[O^+(\mathcal{O}_p) : \mathrm{Im}(\theta)] = [U_p : (U_p)^2] = 2$ if $p \neq 2$, $= 4$ if $p = 2$. Therefore, $\alpha(\mathcal{O}_p) = (1 - p^{-2})^2$ if $p \neq 2$ is split, $\alpha(\mathcal{O}_2) = 2(1 - 2^{-2})^2$ if 2 is split.

If p is a non-split prime and $U^1(\mathcal{O}_p) = \{x_p \in \mathcal{O}_p \mid N(x_p) = 1\}$, we have an obvious mapping $\theta: U^1(\mathcal{O}_p) \times U^1(\mathcal{O}_p) \longrightarrow O^+(\mathcal{O}_p)$ with $\mathrm{Ker}(\theta) = \{(1,1),(-1,-1)\}$. Once again, θ is a continuous open homomorphism. This time, however, $[O^+(\mathcal{O}_p) : \mathrm{Im}(\theta)] =$

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

$[\mathcal{O}_p^* : U^1(\mathcal{O}_p)\mathbb{Q}_p^*] = [\mathbb{Q}_p^* : (\mathbb{Q}_p^*)^2] = 4$ if $p \neq 2$, 8 if $p = 2$. Hence it suffices to compute $\alpha(U^1(\mathcal{O}_p))$. Let $\mathcal{P}$ be the unique two-sided prime ideal of $\mathcal{O}_p$. Then $\mathcal{O}_p/\mathcal{P}$ is the finite field with p^2 elements $\Rightarrow \mu_p(\mathcal{P}) = p^{-2} \Rightarrow \mu_p(U(\mathcal{O}_p)) = p^{-2}(p^2 - 1)$. Therefore, $\mu_p(U^1(\mathcal{O}_p)) = \lim_{n\to\infty} p^n \mu_p\left(\{x_p \in U(\mathcal{O}_p) \mid N(x_p) \equiv 1 \bmod p^n\}\right)$

$= p^n \frac{p^{-2}(p^2 - 1)}{(p-1)p^{n-1}} = p^{-1}(p+1) = (1 + p^{-1})$. We conclude that $\alpha(\mathcal{O}_p) = 2(1 + p^{-1})^2$ if $p \neq 2$ is non-split; $\alpha(\mathcal{O}_2) = 4(1 + 2^{-1})^2$ if 2 is non-split.

For the infinite prime we have a surjective mapping $\theta: U_\infty \times U_\infty \longrightarrow O^+(\mathcal{O}_\infty)$ with $\mathrm{Ker}(\theta) = \{(1,1),(-1,-1)\}$. The volume of the ellipsoid $\Sigma_T = \{x \in \mathcal{O}_\infty \mid N(x) \leq T\}$ is $\frac{2\pi^2 T^2}{\sqrt{D}}$. Therefore, $\mu_\infty(\Sigma_T) = \frac{4\pi^2 T}{\sqrt{D}}$. In particular, $\mu_\infty(U_\infty) = \mu_\infty(\Sigma_1) = \frac{4\pi^2}{\sqrt{D}}$. We conclude that $\alpha(\mathcal{O}_\infty) = \frac{1}{2}\left(\frac{4\pi^2}{\sqrt{D}}\right)^2 = \frac{1}{2}\left(\frac{16}{D}\right)\pi^4$.

Then $\prod_p \alpha(\mathcal{O}_p) = 2^e \prod_{p \nmid D}(1 - p^{-2})^2 \cdot \prod_{p \mid D}(1 + p^{-1})^2 \cdot \frac{16\pi^4}{D} =$

$2^e \zeta(2)^{-2} \prod_{p \mid D}\left(\frac{1}{1 - p^{-1}}\right)^2 \cdot \frac{16\pi^4}{D} = 2^e \left(\frac{6}{\pi^2}\right)^2 \cdot \prod_{p \mid D}(p-1)^{-2} \cdot (4\pi^2)^2 =$

$2^e \left(\frac{1}{24} \prod_{p \mid D}(p-1)\right)^2$. We conclude that $\sum_{k=1}^{H} \frac{1}{E(M_k)} = 2\left(\prod_p \alpha(\mathcal{O}_p)\right)^{-1}$

$= 2^{1-e}\left(\frac{1}{24} \prod_{p \mid D}(p-1)\right)^2 = 2^{1-e}\left(\frac{1}{24}\phi(d)\right)^2$.

Remark: There is yet another, more direct way of showing that $\sum_{k=1}^{H} \frac{1}{E(M_k)} = 2^{1-e}\left(\frac{1}{24}\phi(d)\right)^2$. Let $I_1, \ldots, I_h$ be a complete set of representatives for the left ideal classes of $\mathcal{O}$, where $h = h_d$. Let $\mathcal{O}_1, \ldots, \mathcal{O}_h$ be the right orders of $I_1, \ldots, I_h$, resp-

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

ectively, and let $w_1,\ldots,w_h$ be the orders of the groups of units of $\mathcal{O}_1,\ldots,\mathcal{O}_h$, respectively. Then, by evaluating the residue of the zeta function $\zeta_{\mathcal{A}}(z)$ of $\mathcal{A}$ at $z = 2$, one can easily verify that:

$$\sum_{j=1}^{h} \frac{1}{w_j} = \frac{1}{24}\phi(d)$$

After a suitable rearrangement, if necessary, we may assume that $\mathcal{O}_1,\ldots,\mathcal{O}_t$ is a complete set of representatives for the type classes of maximal orders in $\mathcal{A}$, where $t = t_d$. One can easily show that among the orders $\mathcal{O}_1,\ldots,\mathcal{O}_h$ there are exactly 2^{e-f_i} of type $\mathcal{O}_i$, where $2^{f_i} = |\Pi(\mathcal{O}_i)|$, $i = 1,\ldots,t$ (cf. III.2). From our discussion in III.2 we know that $O^+(M_k)$, $k = 1,\ldots,H$, depends only on the left and right orders of M_k. We say that M_k is of type (i,j) if its left order is of type $\mathcal{O}_i$ and its right order is of type $\mathcal{O}_j$. We set $2^{f_{ij}} = |N(\Pi(\mathcal{O}_i)) \cap N(\Pi(\mathcal{O}_j))|$, $i,j = 1,\ldots,t$. It is then a simple matter to show that there are precisely $2^{e-f_i-f_j+f_{ij}}$ distinct M_k of type (i,j). Therefore,

$$\sum_{k=1}^{H} \frac{1}{E(M_k)} = \sum_{i,j=1}^{t} \frac{2^{e-f_i-f_j+f_{ij}}}{w_i w_j 2^{f_{ij}-1}} = 2^{1-e}\sum_{i,j=1}^{t} \frac{2^{e-f_i}2^{e-f_j}}{w_i w_j} =$$

$$2^{1-e}\sum_{j=1}^{t}\left(\frac{2^{e-f_j}}{w_j}\right)^2 = 2^{1-e}\left(\sum_{j=1}^{h}\frac{1}{w_j}\right)^2 = 2^{1-e}\left(\frac{1}{24}\phi(d)\right)^2.$$

It is interesting to note that, assuming the Minkowski-Siegel Theorem, these two different ways of computing $\sum_{k=1}^{H} \frac{1}{E(M_k)}$ give a direct proof that $\tau(O^+(V)) = 2$ for a positive definite quadratic vector space V of dimension 4 having square discriminant.

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

Summarizing, we have deduced the following:

Lemma 3.8: The contribution to the trace sum of the conjugacy class of an element $\delta \equiv (\pm 1, 1)$ is:

$$2^{1-e}\left(\frac{1}{24}\,\phi(d)\right)^2$$

Before we can proceed to evaluate the contributions of cases (ii) - (iv), we need the following discussion. Let k be the quotient field of a complete discrete valuation ring 0. Let K be a maximal commutative semi-simple subalgebra of M(n,k). In other words, K is a commutative semi-simple subalgebra of M(n,k) with $[K : k] = n$. K must be a direct sum of finite extensions of k. We let 0_K = the ring of integers in K = the unique maximal order of K. Then 0_K is a finite direct sum of complete discrete valuation rings. The next result has the rather impressive title "The Hasse-Noether-Chevalley Theorem."

Theorem 3.9: Suppose Θ and Θ' are maximal orders of M(n,k) and $\Theta \cap K = 0_K = \Theta' \cap K$. Then there exists $\alpha \in K^*$ such that $\Theta' = \alpha \Theta \alpha^{-1}$.

Proof

Though it is very elementary, we present the following proof, due to Tamagawa, if only to deflate the pomposity of the theorem's title. Identify M(n,k) with $\mathrm{Hom}_k(K,K)$. One can easily show that it suffices to prove the theorem for but one particular embedding of K in M(n,k). For convenience, we choose the embedding of K in $\mathrm{Hom}_k(K,K)$ given by the regular representation. By general theory we know that $\Theta = \mathrm{Hom}_0(M,M)$, $\Theta' = \mathrm{Hom}_0(M',M')$, where M and M'

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

are lattices in K. By assumption, $\mathcal{O}_K M \subset M$ and $\mathcal{O}_K M' \subset M'$. That is, M and M' are fractional $\mathcal{O}_K$-ideals. Hence there exists $\alpha \in K^*$ such that $M' = M\alpha$. Therefore, $\Theta' = \alpha \Theta \alpha^{-1}$. [QED]

The preceding theorem, in the special case n = 2, can be used to compute the contributions of cases (ii) and (iii). However, it is not quite strong enough to be applied to case (iv), because in that case there is the possibility that $\Theta \cap K$ may not be $\mathcal{O}_K$. To handle this possibility, we need the following strengthening of Theorem 3.9 for the case n = 2:

Theorem 3.10: Let K be a maximal commutative semi-simple subalgebra of M(2,k). Suppose Θ, Θ' are maximal orders of M(2,k) and $\Theta \cap K = \Theta' \cap K$. Then there exists $\alpha \in K^*$ such that $\Theta' = \alpha \Theta \alpha^{-1}$.

Proof

Once again we identify M(2,k) with $\mathrm{Hom}_K(K,K)$ and embed K in $\mathrm{Hom}_K(K,K)$ via its regular representation. We again have $\Theta = \mathrm{Hom}_{\mathcal{O}}(M,M)$, $\Theta' = \mathrm{Hom}_{\mathcal{O}}(M',M')$ for certain lattices M,M' in K. Let $\mathcal{O}'_K = \Theta \cap K = \Theta' \cap K$. Then, by assumption, $\mathcal{O}'_K = \{\alpha \in K \mid \alpha M \subset M\} = \{\alpha \in K \mid \alpha M' \subset M'\}$. It suffices, therefore, to prove:

Lemma 3.11: Let K be as in Theorem 3.10. Let $M \subset K$ be any lattice and set $\mathcal{O}'_K = \{\alpha \in K \mid \alpha M \subset M\}$. Then there exists $\gamma \in K^*$ such that $M = \mathcal{O}'_K \gamma$.

Proof (Tamagawa)

There are two cases:

1) K is a field. Then $M = \mathcal{O}\beta + \mathcal{O}\gamma$ for certain $\beta, \gamma \in K^*$. Either γ/β or β/γ is in $\mathcal{O}_K$, the ring of integers in K. Without

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

loss of generality, we may assume that $\beta/\gamma \in \mathcal{O}_K$. Of course, β/γ is not in k. It follows that $\mathcal{O}''_K = \mathcal{O} + \mathcal{O}(\beta/\gamma)$ is an order of K. Clearly, $M = \mathcal{O}''_K\gamma \Longrightarrow \mathcal{O}''_K = \{\alpha \in K \mid \alpha M \subset M\} = \mathcal{O}'_K$. Thus, $M = \mathcal{O}'_K\gamma$.

2) $K = k \oplus k$. Let e_1, e_2 be the orthogonal idempotents of K. We denote a basis of M over $\mathcal{O}$ by: $m_1 = ae_1 + be_2$

where $a,b,c,d \in k$ and $ad - bc \neq 0$. $m_2 = ce_1 + de_2$

Let p be a prime element in $\mathcal{O}$. Then we can write: $\begin{pmatrix} a \\ c \end{pmatrix} = p^i \begin{pmatrix} a' \\ c' \end{pmatrix}$

where $a',c' \in \mathcal{O}$ and $(a',c') = 1$.

Hence there exist $b',d' \in \mathcal{O}$ such that $a'd' - b'c' = 1$. Then

$$\begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}^{-1} \begin{pmatrix} m_1 \\ m_2 \end{pmatrix} = \begin{pmatrix} d' & -b' \\ -c' & a' \end{pmatrix} \begin{pmatrix} ae_1 + be_2 \\ ce_1 + de_2 \end{pmatrix} = \begin{pmatrix} p^i e_1 + (bd' - b'd)e_2 \\ (a'd - bc')e_2 \end{pmatrix}$$

Thus, multiplying m_2 by a unit of $\mathcal{O}$ if necessary, we may assume $m_1 = p^i e_1 + be_2$, $m_2 = p^j e_2$. If the lemma is true for $p^k M$, then it is certainly true for M. Consequently, we may further assume that $i,j \geq 0$, $b \in \mathcal{O}$. If $b = 0$, then $\mathcal{O}'_K = \mathcal{O}e_1 + \mathcal{O}e_2$ and $M = \mathcal{O}'_K(p^i e_1 + p^j e_2)$. Assume $b \neq 0$ and let ℓ = the p-order of b. By adding m_2 to m_1, if necessary, we may assume $\ell \leq j$. Suppose $x,y \in k$ and $(xe_1 + ye_2)M \subset M \Longleftrightarrow (xe_1 + ye_2)(p^i e_1 + be_2)$ and $(xe_1 + ye_2)p^j e_2$ are in M. Therefore, $xp^i e_1 + ybe_2$, $yp^j e_2 \in M$. In particular, $y \in \mathcal{O}$. Moreover, $xp^i e_1 + ybe_2 = w(p^i e_1 + be_2) + zp^j e_2$ for certain $w,z \in \mathcal{O} \Rightarrow x \in \mathcal{O} \Longrightarrow x(p^i e_1 + be_2) \in M \Longrightarrow (yb - xb)e_2 \in M \Longrightarrow (y - x)b \equiv 0 \pmod{p^j}$. Conversely, if x,y are in $\mathcal{O}$ and $(y - x)b \equiv 0 \pmod{p^j}$, then $xe_1 + ye_2 \in \mathcal{O}'_K$. Thus, $\mathcal{O}'_K = \{xe_1 + ye_2 \mid x,y \in \mathcal{O}, x \equiv y \pmod{p^{j-\ell}}\}$. We conclude that $M = \mathcal{O}'_K m_1$, since $p^{j-\ell}e_2 \in \mathcal{O}'_K$ implies that $p^{j-\ell}be_2 = \varepsilon p^j e_2 \in M$, where ε is a unit of $\mathcal{O}$. [QED]

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

We note that no such discussion is needed in the case where $\mathcal{A}$ is a quaternion algebra over k, since in that case there is a unique maximal order $\mathcal{O}$ of $\mathcal{A}$, and $\mathcal{O} \cap K = \mathcal{O}_K$ for any subfield K of $\mathcal{A}$. (N.B. Here $\mathcal{A}$ is meant to be a division algebra, of course.)

§6. The term $\delta \equiv (1,u)$

Notation: Suppose x and y are elements of two (possibly distinct) associative algebras over $\mathbb{Q}$. Then $x \simeq y$ will mean that x and y are algebraic over $\mathbb{Q}$ and have the same minimal polynomial over $\mathbb{Q}$. If $x,y \in \mathcal{A}$ then $x \simeq y \iff y$ and x are conjugate.

Suppose $\delta \equiv (1,u)$, where $u \notin \mathbb{Q}$ is a unit of $\mathcal{O}_R$, the right order of M_k. We define $K_u = \mathbb{Q}(u)$, J_u = the idele group of K_u. Since δ is impure, we have by Proposition 3.7 that $G(\delta) = \mathcal{A}^* \times K_u^* / \Delta(\mathbb{Q}^*)$. Since u is integral and $N(u) = 1$, u must be a root of a polynomial $X^2 + tX + 1$, where $t \in \mathbb{Z}$. Suppose u is real. Then the fact that K_u splits $\mathcal{A}$ would imply that $\mathbb{R}$ must split $\mathcal{A}$, contradicting our assumption that $\mathcal{A}$ is positive definite. Therefore, u must be imaginary; that is, $t^2 - 4 < 0 \implies |t| < 2 \implies t = 0, \pm 1$. Hence the only possibilities for u are: $u \simeq \sqrt{-1}$ or $u \simeq \pm\zeta$, where $\zeta = \frac{-1 + \sqrt{-3}}{2}$. If such an element u lies inside $\mathcal{A}$, then some conjugate of u lies in the right order $\mathcal{O}_R$ of some M_k, $k = 1,\ldots,H$. Without loss of generality, we may assume $u \in \mathcal{O}_R$. In that case, there exists $\tilde{\gamma}_0 \in G_A$, $\tilde{\gamma}_0 \equiv (\alpha_0, \beta_0) \bmod \Delta(J_{\mathbb{Q}}^1)$ such that $\tilde{\gamma}_0 \delta \tilde{\gamma}_0^{-1} \equiv (1, \beta_0 u \beta_0^{-1}) \in G_{\tilde{\mathcal{O}}}$, where $\beta_0^{-1} \tilde{\mathcal{O}} \beta_0 = \tilde{\mathcal{O}}_R$.

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

Let us write $\beta_0 = (\beta_{0p})$. Since the lattice generated by $\{1,u\}$ in K_u is the maximal order $\mathcal{O}_u$ of K_u, we must have $\mathcal{O}_\mathcal{R} \cap K_u = \mathcal{O}_u$. For every finite prime p let $K_{u,p} = K_u \otimes_\mathbb{Q} \mathbb{Q}_p$, $\mathcal{O}_{u,p} = \mathcal{O}_u \otimes_\mathbb{Z} \mathbb{Z}_p$. Then $K_{u,p}$ is a maximal commutative semi-simple subalgebra of $\mathcal{A}_p$ and $\mathcal{O}_{\mathcal{R},p} \cap K_{u,p} = \mathcal{O}_{u,p}$ for every p. Suppose $\beta_p \in \mathcal{A}_p^*$ is another element such that $\beta_p^{-1} \mathcal{O}_p \beta_p \cap K_{u,p} = \mathcal{O}_{u,p} = \beta_{0p}^{-1} \mathcal{O}_p \beta_{0p} \cap K_{u,p}$. Then, by Theorem 3.9, there exists $z_p \in K_{u,p}^*$ such that $\beta_p^{-1} \mathcal{O}_p \beta_p = z_p^{-1} \beta_{0p}^{-1} \mathcal{O}_p \beta_{0p} z_p \Rightarrow \beta_{0p} z_p \beta_p^{-1} \in \mathcal{N}(\mathcal{O}_p)$, the normalizer of $\mathcal{O}_p$. Thus, $\beta_p \in \mathcal{N}(\mathcal{O}_p) \beta_{0p} z_p = \beta_{0p} \mathcal{N}(\mathcal{O}_{\mathcal{R},p}) z_p$. Doing this for each p, it follows that $<\beta>$, the set of all β such that $(1, \beta u \beta^{-1}) \in G_\mathcal{Z}$, is equal to $\beta_0 \mathcal{N}(\tilde{\mathcal{O}}_\mathcal{R}) J_u^1$. By our discussion in III.2, we have:

$\mathcal{N}(\tilde{\mathcal{O}}_\mathcal{R}) = \bigcup_{\kappa=1}^{2^e} n_\kappa U^1(\tilde{\mathcal{O}}_\mathcal{R}) J_\mathbb{Q}^1$ for certain $n_\kappa \in J_\mathcal{A}^1$, where this is a disjoint union of cosets. Hence $<\beta> = \bigcup_{\kappa=1}^{2^e} \beta_0 n_\kappa U^1(\tilde{\mathcal{O}}_\mathcal{R}) J_u^1$, but now this union may not be disjoint, since it may be possible that some $n_\kappa \in U^1(\tilde{\mathcal{O}}_\mathcal{R}) J_u^1$ though $n_\kappa \notin U^1(\tilde{\mathcal{O}}_\mathcal{R}) J_\mathbb{Q}^1$. Looking at this locally, it is easily seen that this can occur if and only if for some $p|d$ there is an $n_p \in U(\mathcal{O}_p) K_{u,p}^*$, $n_p \notin U(\mathcal{O}_p) \mathbb{Q}_p^* \Leftrightarrow K_{u,p}$ is a ramified field extension of $\mathbb{Q}_p$ for some $p|d$. In fact, if ε = the number of primes p which divide d and ramify in K_u, then there are exactly $2^{e-\varepsilon}$ distinct cosets $\beta_0 n_\kappa U^1(\tilde{\mathcal{O}}_\mathcal{R}) J_u^1$. In the present case ε is at most equal to 1. Then, renumbering the n_κ if necessary, we see that: $<\beta> = \bigcup_{\kappa=1}^{2^{e-\varepsilon}} \beta_0 n_\kappa U^1(\tilde{\mathcal{O}}_\mathcal{R}) J_u^1$, where this is now a disjoint union. Of course there is no condition on the

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

element α of $\tilde{\gamma} = (\alpha,\beta)$ such that $\tilde{\gamma}\delta\tilde{\gamma}^{-1} \in G_{\tilde{\theta}}$. We conclude that $\langle\tilde{\gamma}\rangle$, the set of all $\tilde{\gamma}$ such that $\tilde{\gamma}\delta\tilde{\gamma}^{-1} \in G_{\tilde{\theta}}$, is equal to:

$$\bigcup_{\kappa=1}^{2^{e-\varepsilon}} (J^1_{\mathcal{O}} \times \beta_0 n_\kappa U^1(\tilde{\theta}_r) J^1_u)/\Delta(J^1_{\mathcal{Q}})$$

Let $Y_\delta = J^1_{\mathcal{O}} \times U^1(\tilde{\theta}_r) J^1_u/\Delta(J^1_{\mathcal{Q}})$. Then the support of Ψ_δ is equal to $2^{e-\varepsilon}$ disjoint translates of $Y_\delta/G(\delta)$, so we have:

$$\int_{G_A/G(\delta)} \Psi_\delta(\rho)\, d_\delta\rho = 2^{e-\varepsilon} \int_{Y_\delta/G(\delta)} d_\delta\rho = 2^{e-\varepsilon} v(Y_\delta/G(\delta)).$$

Our embedding of G in G_A is such, that $\mathcal{O}^* \times K^*_u/\Delta(\mathcal{Q}^*)$ is identified with $(\mathcal{O}^* \times K^*_u)\Delta(J^1_{\mathcal{Q}})/\Delta(J^1_{\mathcal{Q}})$. Hence $v(Y_\delta/G(\delta)) =$

$$v\left(J^1_{\mathcal{O}} \times U^1(\tilde{\theta}_r) J^1_u/\Delta(J^1_{\mathcal{Q}})(\mathcal{O}^* \times K^*_u)\right) = v\left(J^1_{\mathcal{O}} \times U^1(\tilde{\theta}_r) J^1_u/\Delta(U^1_{\mathcal{Q}})(\mathcal{O}^* \times K^*_u)\right), \quad (*)$$

since $\Delta(J^1_{\mathcal{Q}}) = \Delta(U^1_{\mathcal{Q}})\Delta(\mathcal{Q}^*)$. As in III.5, we let h = the ideal class number of $\mathcal{O}$. Then we have a disjoint coset decomposition:

$J^1_{\mathcal{O}} = \bigcup_{j=1}^{h} U^1(\tilde{\theta})\delta_j \mathcal{O}^*$ for certain $\delta_j \in J^1_{\mathcal{O}}$. $J^1_u = U^1_u \cdot K^*_u$, since K_u has class number equal to 1, where, of course, $U^1_u = U^1(\tilde{\theta}_r) \cap J_u$.

Thus, $(*) = \sum_{j=1}^{h} v\left(U^1(\tilde{\theta})\delta_j \mathcal{O}^* \times U^1(\tilde{\theta}_r) K^*_u/\Delta(U^1_{\mathcal{Q}})(\mathcal{O}^* \times K^*_u)\right)$.

For every j we have: $v\left(U^1(\tilde{\theta})\delta_j \mathcal{O}^* \times U^1(\tilde{\theta}_r) K^*_u/\Delta(U^1_{\mathcal{Q}})(\mathcal{O}^* \times K^*_u)\right) =$

$v\left(\delta_j^{-1} U^1(\tilde{\theta})\delta_j \mathcal{O}^* \times U^1(\tilde{\theta}_r) K^*_u/\Delta(U^1_{\mathcal{Q}})(\mathcal{O}^* \times K^*_u)\right)$. But $\delta_j^{-1} U^1(\tilde{\theta})\delta_j = U^1(\tilde{\theta}_j)$, where θ_j = the right order of an ideal representing the ideal class associated to the coset $U^1(\tilde{\theta})\delta_j \mathcal{O}^*$. Thereby, $(*) =$

$$\sum_{j=1}^{h} v\left(U^1(\tilde{\theta}_j) \mathcal{O}^* \times U^1(\tilde{\theta}_r) K^*_u/\Delta(U^1_{\mathcal{Q}})(\mathcal{O}^* \times K^*_u)\right)$$

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

Let W_j = the unit group of $\mathcal{O}_j$, W_u = the unit group of $\mathcal{O}_u$; $w_j = |W_j|$, $w_u = |W_u|$.

Then $v\left(U^1(\tilde{\mathcal{O}}_j)\mathfrak{a}^*\times U^1(\tilde{\mathcal{O}}_r)K_u^*/\Delta(U^1_{\mathbb{Q}})(\mathfrak{a}^*\times K_u^*)\right)$ =

$v\left(U^1(\tilde{\mathcal{O}}_j)\mathfrak{a}^*\times U^1(\tilde{\mathcal{O}}_r)K_u^*/\mathfrak{a}^*\times K_u^* \Big/ \Delta(U^1_{\mathbb{Q}})(\mathfrak{a}^*\times K_u^*)/\mathfrak{a}^*\times K_u^*\right)$ =

$v\left(U^1(\tilde{\mathcal{O}}_j)\times U^1(\tilde{\mathcal{O}}_r)/\mathfrak{a}^*\times K_u^* \cap U^1(\tilde{\mathcal{O}}_j)\times U^1(\tilde{\mathcal{O}}_r) \Big/ \Delta(U^1_{\mathbb{Q}})/\Delta(U^1_{\mathbb{Q}}) \cap \mathfrak{a}^*\times K_u^*\right)$

$= v\left(U^1(\tilde{\mathcal{O}}_j)\times U^1(\tilde{\mathcal{O}}_r)/W_j\times W_u \Big/ \Delta(U^1_{\mathbb{Q}})/\{\pm 1\}\right)$ =

$\frac{2}{w_j w_u}\, v\left(U^1(\tilde{\mathcal{O}}_j)\times U^1(\tilde{\mathcal{O}}_r)/\Delta(U^1_{\mathbb{Q}})\right) = \frac{2^{1-e}}{w_j w_u}$, by Proposition 3.2.

Hence $(*) = \sum_{j=1}^{h} \frac{2^{1-e}}{w_j w_u} = \frac{2^{1-e}}{w_u}\sum_{j=1}^{h}\frac{1}{w_j} = \frac{2^{1-e}}{w_u}\left(\frac{1}{24}\phi(d)\right)$ (cf.p.31)

Multiplying this result by $2^{e-\varepsilon}$, we conclude:

Lemma 3.12: The contribution to the trace sum of the conjugacy class of an element $\delta \equiv (1,u)$ is:

$$\frac{2^{1-\varepsilon}}{w_u}\left(\frac{1}{24}\phi(d)\right)$$

By symmetry, the contribution of $\delta \equiv (u,1)$ is the same as that of $\delta \equiv (1,u)$.

§7. The term $\delta \equiv (u,v)$

Now suppose that $\delta \equiv (u,v)$, where $u,v \notin \mathbb{Q}$ are units of $\mathcal{O}_\ell$, $\mathcal{O}_r$, respectively, the left and right orders of M_k. Let $K_u = \mathbb{Q}(u)$, $K_v = \mathbb{Q}(v)$ and let J_u, J_v be the idele groups of K_u, K_v, respectively. By Proposition 3.7, $G(\delta) = K_u^*\times K_v^*/\Delta(\mathbb{Q}^*)$ or $[G(\delta) : K_u^*\times K_v^*/\Delta(\mathbb{Q}^*)] = 2$, the latter being possible if and only

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

if $u \simeq v \simeq \sqrt{-1}$. By assumption, there exists $\tilde{\gamma}_0 \equiv (\alpha_0, \beta_0) \in G_A$ such that $\tilde{\gamma}_0 \delta \tilde{\gamma}_0^{-1} \equiv (\alpha_0 u \alpha_0^{-1}, \beta_0 v \beta_0^{-1}) \in G_{\tilde{\theta}}$, with $\alpha_0^{-1} \tilde{\theta} \alpha_0 = \tilde{\theta}_\ell$, $\beta_0^{-1} \tilde{\theta} \beta_0 = \tilde{\theta}_\kappa$. Just as in III.6, we have:

$$<\alpha> = \bigcup_{\iota=1}^{2^{e-\varepsilon_1}} \alpha_0 m_\iota U^1(\tilde{\theta}_\ell) J_u^1, \quad <\beta> = \bigcup_{\kappa=1}^{2^{e-\varepsilon_2}} \beta_0 n_\kappa U^1(\tilde{\theta}_\kappa) J_v^1, \text{ where:}$$

$$\mathcal{N}(\tilde{\theta}_\ell) = \bigcup_{\iota=1}^{2^e} m_\iota U^1(\tilde{\theta}_\ell) J_{\mathbb{Q}}^1, \quad \mathcal{N}(\tilde{\theta}_\kappa) = \bigcup_{\kappa=1}^{2^e} n_\kappa U^1(\tilde{\theta}_\kappa) J_{\mathbb{Q}}^1 \text{ and } \varepsilon_1 = 1,0$$

($\varepsilon_2 = 1,0$) according as the unique ramified prime of K_u divides d or not (respectively, the unique ramified prime of K_v divides d or not). As an immediate consequence we have:

$$<\tilde{\gamma}> = \bigcup_{\iota=1}^{2^{e-\varepsilon_1}} \bigcup_{\kappa=1}^{2^{e-\varepsilon_2}} \left(\alpha_0 m_\iota U^1(\tilde{\theta}_\ell) J_u^1 \times \beta_0 n_\kappa U^1(\tilde{\theta}_\kappa) J_v^1 / \Delta(J_{\mathbb{Q}}^1) \right).$$

Setting $Y_\delta = U^1(\tilde{\theta}_\ell) J_u^1 \times U^1(\tilde{\theta}_\kappa) J_v^1 / \Delta(J_{\mathbb{Q}}^1)$, it is easily seen that the support of Ψ_δ is equal to $2^{2e-\varepsilon_1-\varepsilon_2}$ disjoint translates of $Y_\delta / G(\delta)$. It follows that:

$$\int_{G_A/G(\delta)} \Psi_\delta(\rho)\, d_\delta \rho = 2^{2e-\varepsilon_1-\varepsilon_2} v(Y_\delta / G(\delta)).$$

In order to compute $v(Y_\delta / G(\delta))$, it suffices to first compute $v(Y_\delta / (K_u^* \times K_v^* / \Delta(\mathbb{Q}^*)))$. Let $\mathcal{O}_u$, $\mathcal{O}_v$ be the rings of integers of K_u, K_v, respectively. Let W_u = the unit group of $\mathcal{O}_u$, W_v = the unit group of $\mathcal{O}_v$; $w_u = |W_u|$, $w_v = |W_v|$. Then, arguing exactly the same way as we did in III.6, we conclude:

$$v(Y_\delta / (K_u^* \times K_v^* / \Delta(\mathbb{Q}^*))) = v\left(U^1(\tilde{\theta}_\ell) \times U^1(\tilde{\theta}_\kappa) / W_u \times W_v \Big/ \Delta(U_{\mathbb{Q}}^1) / \{\pm 1\} \right) = \frac{2^{1-e}}{w_u w_v}.$$

This immediately yields the following result:

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

Lemma 3.13: The contribution to the trace sum of the conjugacy class of an element $\delta \equiv (u,v)$ is:

(i) $\dfrac{2^{e-\varepsilon_1-\varepsilon_2}}{w_u w_v}$ if δ is pure.

(ii) $\dfrac{2^{e-\varepsilon_1-\varepsilon_2+1}}{w_u w_v}$ if δ is impure.

§8. The term $\delta \equiv (\mu,\nu)$

Now we have $\delta \equiv (\mu,\nu)$, where $\mu,\nu \notin \mathbb{Q}$ and $\mu \in \mathcal{O}_\ell$, $\nu \in \mathcal{O}_r$, the left and right orders, respectively, of some M_k, and $N(\mu) = N(\nu) = m$, with $m > 1$, $m|d$. We let $K_\mu = \mathbb{Q}(\mu)$, $K_\nu = \mathbb{Q}(\nu)$ and let J_μ, J_ν be the idele groups of K_μ, K_ν, respectively. Then μ satisfies some quadratic equation: $X^2 + tX + m = 0$, $t \in \mathbb{Z}$. Since K_μ splits $\mathcal{A}$, and $\mathcal{A}$ is positive definite, we know that μ must be complex, i.e. $t^2 - 4m < 0$. Moreover, μ has to satisfy the condition that p does not split in K_μ for any $p|d$. In other words, $K_\mu \otimes_{\mathbb{Q}} \mathbb{Q}_p = K_{\mu,p}$ has to be a field for every $p|d$. The same sort of conditions must also be satisfied by ν. Conversely, by the Brauer-Hasse-Noether Theorem, if $\mu,\nu \in \mathcal{A}$ satisfy quadratic equations: $X^2 + tX + m = 0$, $X^2 + t'X + m = 0$, respectively, with $t,t' \in \mathbb{Z}$ and $t^2 - 4m < 0$, $(t')^2 - 4m < 0$ and if $K_{\mu,p}, K_{\nu,p}$ are fields for every $p|d$, then some conjugate of $\delta \equiv (\mu,\nu)$ by an element of G lies in G_{M_k} for some $k = 1,\ldots,H$. Let us examine these conditions. By Hensel's Lemma, t must have the property that $p|m$ implies $p|t$ for every p which divides d. In other words, m must divide t. So let $t = mb$, $b \in \mathbb{Z}$. Then $m^2b^2 - 4m < 0$

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

$\Leftrightarrow mb^2 - 4 < 0 \Leftrightarrow b^2 < 4/m \Leftrightarrow |b| < 2/\sqrt{m}$. Therefore, if m = 2 or 3, the only possibilities for t are: $0, \pm m$. If $m > 3$, the only possibility is $t = 0$. In other words, if $m = 2$, then $\mu \simeq \pm 1 + \sqrt{-1}$ or $\mu \simeq \sqrt{-2}$; if $m = 3$, then $\mu \simeq \frac{\pm 3 + \sqrt{-3}}{2}$ or $\mu \simeq \sqrt{-3}$; if $m > 3$, then $\mu \simeq \sqrt{-m}$. We have exactly the same range of possibilities for ν.

For any element $\alpha \in \mathcal{O}^*$, let $\{\alpha\}$ denote the conjugacy class of α in $\mathcal{O}^*$. For each integer $m > 1$, $m|d$, let $T(m)$ denote the set of all α in $\mathcal{O}^*$ such that α is integral and $N(\alpha) = m$. From the preceding discussion, we conclude that the only possibilities for $T(m)$ are:

1) $T(2) = \emptyset, \{\sqrt{-2}\}, \{1 + \sqrt{-1}\} \cup \{-1 + \sqrt{-1}\}$, or
$\{\sqrt{-2}\} \cup \{1 + \sqrt{-1}\} \cup \{-1 + \sqrt{-1}\}$.

2) $T(3) = \emptyset, \{\sqrt{-3}\} \cup \left\{\frac{3 + \sqrt{-3}}{2}\right\} \cup \left\{\frac{-3 + \sqrt{-3}}{2}\right\}$.

3) $T(m) = \emptyset, \{\sqrt{-m}\}$ for $m > 3$.

Clearly, $\mu \in T(m) \Leftrightarrow \nu \in T(m)$.

By assumption, we have $\tilde{\gamma}_0 \equiv (\alpha_0, \beta_0) \in G_A$ such that $\tilde{\gamma}_0 \delta \tilde{\gamma}_0^{-1} \equiv (\alpha_0 \mu \alpha_0^{-1}, \beta_0 \nu \beta_0^{-1}) \in G_{\tilde{\delta}}$, with $\alpha_0^{-1} \tilde{\Theta} \alpha_0 = \tilde{\Theta}_\ell$, $\beta_0^{-1} \tilde{\Theta} \beta_0 = \tilde{\Theta}_r$. Then $\mu \in \Theta_\ell \cap K_\mu = \mathcal{O}'$, an order of K_μ. This order $\mathcal{O}'$ has the property that its conductor is prime to d, since $\mathcal{O}'_p = \Theta_{\ell,p} \cap K_{\mu,p}$ = the maximal order of $K_{\mu,p}$ for every $p|d$. But, from the preceding discussion, the conductor always equals 1 or 2. Hence if $2|d$, then $\mathcal{O}'$ has to be the unique maximal order of K_μ. We have similar considerations for $\nu \in \Theta_r \cap K_\nu = \mathcal{O}''$. Since the orders $\mathcal{O}', \mathcal{O}''$ may not be maximal in this case, we can not apply Theorem 3.9,

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

rather, we must apply the stronger Theorem 3.10. Doing so, we obtain:

$$\langle\alpha\rangle = \bigcup_{\iota=1}^{2} \alpha_0 m_\iota U^1(\tilde{\Theta}_\ell) J_\mu^{1\,e-f_\mu}, \quad \langle\beta\rangle = \bigcup_{\kappa=1}^{2} \beta_0 n_\kappa U^1(\tilde{\Theta}_r) J_\nu^{1\,e-f_\nu}, \text{ where:}$$

$$\mathcal{N}(\tilde{\Theta}_\ell) = \bigcup_{\iota=1}^{2} m_\iota U^1(\tilde{\Theta}_\ell) J_{\mathfrak{Q}}^{1\,e}, \quad \mathcal{N}(\tilde{\Theta}_r) = \bigcup_{\kappa=1}^{2} n_\kappa U^1(\tilde{\Theta}_r) J_{\mathfrak{Q}}^{1\,e}, \text{ and where:}$$

f_μ, f_ν = the number of primes dividing d and ramifying in K_μ, K_ν, respectively. As an immediate consequence, we have:

$$\langle\tilde{\gamma}\rangle = \bigcup_{\iota=1}^{2} \bigcup_{\kappa=1}^{2} \left(\alpha_0 m_\iota U^1(\tilde{\Theta}_\ell) J_\mu^{1\,e-f_\mu} \times \beta_0 n_\kappa U^1(\tilde{\Theta}_r) J_\nu^{1\,e-f_\nu} / \Delta(J_{\mathfrak{Q}}^1)\right).$$

In the present case, however, $\langle\tilde{\gamma}\rangle/G(\delta)$ is not necessarily the whole support of Ψ_δ, since there may be several distinct possibilities for the pair $(\mathcal{O}', \mathcal{O}'')$. Accordingly, we should write: $\langle\tilde{\gamma}\rangle = \langle\tilde{\gamma}(\mathcal{O}', \mathcal{O}'')\rangle$. It is easy to show that any order in $K_{\mu,p}$ or $K_{\nu,p}$, for p split, is the intersection of some <u>maximal</u> order in $\mathcal{A}_p$ with $K_{\mu,p}$ or $K_{\nu,p}$, respectively. It follows that any orders $\mathcal{O}', \mathcal{O}''$ in K_μ, K_ν, respectively, which are possible from our above considerations will indeed be realized as intersections $\Theta_\ell \cap K_\mu$, $\Theta_r \cap K_\nu$, respectively, for certain maximal orders Θ_ℓ, Θ_r of $\mathcal{A}$. Hence the contribution of $\{\delta\}$ to the trace sum equals:

$$\sum_{(\mathcal{O}', \mathcal{O}'')} v\left(\langle\tilde{\gamma}(\mathcal{O}', \mathcal{O}'')\rangle / G(\delta)\right)$$

Since the conductors of $\mathcal{O}', \mathcal{O}''$ are always either 1 or 2, there are at most two possibilities for each, hence at most four possibilities for the ordered pair $(\mathcal{O}', \mathcal{O}'')$.

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

As in II.1, we define $\lambda(m)$ = "the length of m" = the number of (distinct) primes dividing m. Then, from the well-known ramification theory of quadratic number fields, we easily see that:

$$f_\mu = f_\nu = \begin{cases} \lambda(m) & \text{if } m \equiv 2,3 \pmod 4 \\ \lambda(m) & \text{if } m \equiv 1 \pmod 4,\ 2 \nmid d \\ \lambda(m)+1 & \text{if } m \equiv 1 \pmod 4,\ 2 \mid d \end{cases}$$

Since f_μ and f_ν evidently depend only on m, let us write $f_\mu = f_\nu = f_m$. Proceeding exactly as in III.7, we see that the contribution of $(0',0'')$ to the trace sum is equal to:

$$2^{2e-2f_m}\, v(Y_\delta(0',0'')/G(\delta));\ Y_\delta(0',0'') = U^1(\tilde{\mathcal{O}}_\ell)J_\mu^1 \times U^1(\tilde{\mathcal{O}}_r)J_\nu^1/\Delta(J_{\mathbb{Q}}^1)$$

To compute this contribution, we first evaluate the quantity $v(Y_\delta(0',0'')/(K_\mu^* \times K_\nu^*/\Delta(\mathbb{Q}^*)))$ by using the coset decompositions:

$$J_\mu^1 = \bigcup_{\rho=1}^{h'} U^1(0')K_\mu^* x_\rho,\quad J_\nu^1 = \bigcup_{\sigma=1}^{h''} U^1(0'')K_\nu^* y_\sigma \quad (\dagger) \quad \text{for certain } x_\rho \in J_\mu^1,$$

$y_\sigma \in J_\nu^1$; where $U^1(0') = \prod_{p \neq \infty} U(0'_p) \times K^1_{\mu,\infty}$, $U^1(0'') = \prod_{p \neq \infty} U(0''_p) \times K^1_{\nu,\infty}$

with $U(0'_p)$ = the unit group of $0'_p$, $U(0''_p)$ = the unit group of $0''_p$; $K^1_{\mu,\infty} = \{x \in K_{\mu,\infty} \mid N(x) = 1\}$, $K^1_{\nu,\infty} = \{x \in K_{\nu,\infty} \mid N(x) = 1\}$. Here h' = the class number of $0'$ and h" = the class number of $0''$. These are not class numbers in the usual sense, since $0'$ and $0''$ may not be Dedekind domains. In the present context the class number is the order of the group of "locally principal" fractional ideals modulo principal fractional ideals.

Let w' = the number of units in $0'$, w'' = the number of units in $0''$; w_μ = the number of units in the maximal order 0_μ of K_μ, w_ν = the number of units in the maximal order 0_ν of K_ν. We set

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

$h(\mu), h(\nu)$ = the ideal class numbers of $\mathcal{O}_\mu, \mathcal{O}_\nu$, respectively. It is easy to see that the following relations hold:

$$\frac{h'}{w'} = \frac{h(\mu)[U_\mu^1 : U^1(\mathcal{O}')]}{w_\mu}, \quad \frac{h''}{w''} = \frac{h(\nu)[U_\nu^1 : U^1(\mathcal{O}'')]}{w_\nu} \qquad (\dagger\dagger)$$

where, of course, $U_\mu^1 = U^1(\mathcal{O}_\mu)$, $U_\nu^1 = U^1(\mathcal{O}_\nu)$.

Using the decompositions (†) and proceeding exactly as in III.6 and III.7, we conclude:

$$v(Y_\delta(\mathcal{O}', \mathcal{O}'')/(K_\mu^* \times K_\nu^*/\Delta(\mathbb{Q}^*))) = 2^{1-e} \frac{h'h''}{w'w''}$$

This immediately yields the following result:

Lemma 3.14: The contribution to the trace sum by the conjugacy class of an element $\delta \equiv (\mu, \nu)$ is:

(i) $\sum_{(\mathcal{O}', \mathcal{O}'')} 2^{e-2f_m} \frac{h'h''}{w'w''}$ if δ is pure.

(ii) $\sum_{(\mathcal{O}', \mathcal{O}'')} 2^{e-2f_m+1} \frac{h'h''}{w'w''}$ if δ is impure.

In the particular case where d is even, the orders $\mathcal{O}'$ and $\mathcal{O}''$ are always maximal. Hence the preceding lemma simplifies in this case to read:

Lemma 3.15: If d is even, then the contribution of $\{\delta\}$, for $\delta \equiv (\mu, \nu)$, is:

(i) $2^{e-2f_m} \frac{h(\mu)h(\nu)}{w_\mu w_\nu}$ if δ is pure.

(ii) $2^{e-2f_m+1} \frac{h(\mu)h(\nu)}{w_\mu w_\nu}$ if δ is impure.

In the next section we obtain our final formula for H.

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

§9. Evaluation of the trace sum

Let us now sum up the contributions of cases (i) - (iv) (cf. p.23) according to their multiplicities, that is, according to the number of conjugacy classes occurring in each case.

We first group cases (i), (ii) and (iii) according to their multiplicities.

In case (i) there are only two conjugacy classes: $\{(1,1)\}$ and $\{(-1,1)\}$. Hence, by Lemma 3.8, the total contribution of case (i) is: $$2\cdot 2^{1-e}\left(\frac{1}{24}\phi(d)\right)^2 = 2^{-e}\left(\frac{1}{12}\phi(d)\right)^2$$

In case (ii) the only possible conjugacy classes, if they occur, are: $\{(1,\sqrt{-1})\}$, $\{(\sqrt{-1},1)\}$, $\{(1,\zeta)\}$, $\{(1,-\zeta)\}$, $\{(\zeta,1)\}$ and $\{(-\zeta,1)\}$. Let $\varepsilon(\sqrt{-1}) = 0$ or 1, depending on whether $2\nmid d$ or $2|d$, respectively. Similarly, let $\varepsilon(\zeta) = 0,1$, depending on whether $3\nmid d$ or $3|d$, respectively. Then, by Lemma 3.12, the contribution of $\{(1,\sqrt{-1})\}$ and $\{(\sqrt{-1},1)\}$ is equal to:

$$2\cdot\frac{2^{1-\varepsilon(\sqrt{-1})}}{4}\,\delta(\sqrt{-1})\left(\frac{1}{24}\phi(d)\right) = 2^{-e}\left(\frac{2}{4}\prod_{p|d}\left(1-\left(\frac{-4}{p}\right)\right)\left(\frac{1}{12}\phi(d)\right)\right) \quad \text{since}$$

$$2^{e-\varepsilon(\sqrt{-1})}\,\delta(\sqrt{-1}) = \prod_{p|d}\left(1-\left(\frac{-4}{p}\right)\right), \text{ where } \left(\frac{-4}{p}\right) \text{ is the Kronecker}$$

symbol. Similarly, the contribution of $\{(1,\zeta)\}$, $\{(1,-\zeta)\}$, $\{(\zeta,1)\}$ and $\{(-\zeta,1)\}$ is equal to:

$$4\cdot\frac{2^{1-\varepsilon(\zeta)}}{6}\,\delta(\sqrt{-3})\left(\frac{1}{24}\phi(d)\right) = 2^{-e}\left(\frac{2}{3}\prod_{p|d}\left(1-\left(\frac{-3}{p}\right)\right)\left(\frac{1}{12}\phi(d)\right)\right)$$

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

In case (iii) the only possible conjugacy classes are: $\{(\sqrt{-1},\sqrt{-1})\}$, $\{(\sqrt{-1},\zeta)\}$, $\{(\zeta,\sqrt{-1})\}$, $\{(\zeta,\zeta)\}$ and $\{(-\zeta,\zeta)\}$. By (i) of Lemma 3.13, the contribution of $\{(\sqrt{-1},\sqrt{-1})\}$ is equal to:

$$\frac{2^{e-2\varepsilon(\sqrt{-1})}}{16}\delta(\sqrt{-1}) = 2^{-e}\left(\frac{1}{4}\prod_{p|d}\left(1-\left(\frac{-4}{p}\right)\right)\right)^2$$

By (ii) of Lemma 3.13, the contribution of $\{(\sqrt{-1},\zeta)\}$ and $\{(\zeta,\sqrt{-1})\}$ is equal to:

$$2\cdot\frac{2^{e-\varepsilon(\sqrt{-1})-\varepsilon(\zeta)+1}}{4\cdot 6}\delta(\sqrt{-1})\delta(\sqrt{-3}) =$$

$$2^{-e}\left(\frac{2}{4}\prod_{p|d}\left(1-\left(\frac{-4}{p}\right)\right)\cdot\frac{1}{3}\prod_{p|d}\left(1-\left(\frac{-3}{p}\right)\right)\right)^2;$$ the contribution of

$\{(\zeta,\zeta)\}$ and $\{(-\zeta,\zeta)\}$ is equal to: $$2^{-e}\left(\frac{1}{3}\prod_{p|d}\left(1-\left(\frac{-3}{p}\right)\right)\right)^2$$

Hence the total contribution of cases (i), (ii) and (iii) is equal to:

$$2^{-e}\left[\frac{1}{12}\phi(d)+\frac{1}{4}\prod_{p|d}\left(1-\left(\frac{-4}{p}\right)\right)+\frac{1}{3}\prod_{p|d}\left(1-\left(\frac{-3}{p}\right)\right)\right]^2 = 2^{-e}h_d^2,$$ by Theorem 1.7.

We now compute the contribution of case (iv). Let us first handle the easier case where d is even.

a) Suppose m = 2. Then the possible conjugacy classes are: $\{(\sqrt{-2},\sqrt{-2})\}$, $\{(\sqrt{-2},1+\sqrt{-1})\}$, $\{(1+\sqrt{-1},\sqrt{-2})\}$, $\{(1+\sqrt{-1},1+\sqrt{-1})\}$ and $\{(1+\sqrt{-1},-1+\sqrt{-1})\}$. By (i) of Lemma 3.15, the contribution of $\{(\sqrt{-2},\sqrt{-2})\}$ is: $\frac{2^{e-2}}{4}\delta(\sqrt{-2}) = 2^{e-4}\delta(\sqrt{-2})$. By (ii) of Lemma

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

3.15, the contribution of $\{(\sqrt{-2},1+\sqrt{-1})\}$ and $\{(1+\sqrt{-1},\sqrt{-2})\}$ is equal to: $\frac{2\cdot 2^{e-1}}{8}\delta(\sqrt{-1})\delta(\sqrt{-2}) = 2^{e-3}\delta(\sqrt{-1})\delta(\sqrt{-2})$; the contribution of $\{(1+\sqrt{-1},1+\sqrt{-1})\}$ and $\{(1+\sqrt{-1},-1+\sqrt{-1})\}$ is equal to: $\frac{2\cdot 2^{e-1}}{16}\delta(\sqrt{-1}) = 2^{e-4}\delta(\sqrt{-1})$. We conclude that the total contribution coming from (2) is: $2^{e-4}(\delta(\sqrt{-1})+\delta(\sqrt{-2}))^2$.

b) Suppose $m = 3$. Then the possible conjugacy classes are: $\{(\sqrt{-3},\sqrt{-3})\}$, $\left\{\left(\sqrt{-3},\frac{3+\sqrt{-3}}{2}\right)\right\}$, $\left\{\left(\frac{3+\sqrt{-3}}{2},\sqrt{-3}\right)\right\}$, $\left\{\left(\frac{3+\sqrt{-3}}{2},\frac{3+\sqrt{-3}}{2}\right)\right\}$ and $\left\{\left(\frac{-3+\sqrt{-3}}{2},\frac{3+\sqrt{-3}}{2}\right)\right\}$. Using Lemma 3.15, we see that the contribution of $\{(\sqrt{-3},\sqrt{-3})\}$ equals $\frac{2^{e-2}}{36}\delta(\sqrt{-3})$; that of $\left\{\left(\sqrt{-3},\frac{3+\sqrt{-3}}{2}\right)\right\}$ and $\left\{\left(\frac{3+\sqrt{-3}}{2},\sqrt{-3}\right)\right\}$ equals $\frac{2^{e}}{36}\delta(\sqrt{-3})$; that of $\left\{\left(\frac{3+\sqrt{-3}}{2},\frac{3+\sqrt{-3}}{2}\right)\right\}$ and $\left\{\left(\frac{-3+\sqrt{-3}}{2},\frac{3+\sqrt{-3}}{2}\right)\right\}$ equals $\frac{2^{e}}{36}\delta(\sqrt{-3})$ as well. Hence the total contribution coming from $T(3)$ is: $2^{e-4}\delta(\sqrt{-3})$.

c) Suppose $m > 3$. Then $w_\mu = w_\nu = 2$; the only conjugacy class is $\{(\sqrt{-m},\sqrt{-m})\}$ and its contribution is $\frac{2^{e-2f_m}}{4}\delta(\sqrt{-m})h(\sqrt{-m})^2$ $= 2^{e-2(\lambda(m)+\sigma(m))}\delta(\sqrt{-m})h(\sqrt{-m})^2$, where $\sigma(m) = 1$ if $m \equiv 2$ or $3 \pmod 4$; $\sigma(m) = 2$ if $m \equiv 1 \pmod 4$. Collecting all these terms contributed by cases (i) - (iv) for d even, we obtain:

$$2^{-e}\left[h_d^2 + \left(2^{e-2}\left(\delta(\sqrt{-1})+\delta(\sqrt{-2})\right)\right)^2 + \left(2^{e-2}\delta(\sqrt{-3})\right)^2 + \sum_{m>3}\left(2^{e-\lambda(m)-\sigma(m)}\delta(\sqrt{-m})h(\sqrt{-m})\right)^2\right],$$ proving (b) of Theorem 2.1.

We now consider the case where d is odd. The only way it

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

is possible for $\mathcal{O}'$ or $\mathcal{O}''$ not to be maximal is if $m \equiv 3 \pmod 4$ and $\mu \simeq \sqrt{-m}$ or $\nu \simeq \sqrt{-m}$. We would like an expression for $\frac{h'}{w'}$ assuming $\mathcal{O}'$ is not maximal. By (††) of III.8, it suffices to compute $[U_\mu^1 : U^1(\mathcal{O}')]$. This is done in the following elementary lemma, which we state without proof:

Lemma 3.16:

(i) If $m \equiv 3 \pmod 8$, then $[U_\mu^1 : U^1(\mathcal{O}')] = 3$

(ii) If $m \equiv 7 \pmod 8$, then $[U_\mu^1 : U^1(\mathcal{O}')] = 1$

We conclude that $\frac{h'}{w'} = \frac{1}{2}$ if $m = 3$; $\frac{h'}{w'} = \frac{3h(\mu)}{2} = \frac{3h(\sqrt{-m})}{2}$ if $m > 3$, $m \equiv 3 \pmod 8$; $\frac{h'}{w'} = \frac{h(\sqrt{-m})}{2}$ if $m \equiv 7 \pmod 8$, where we are assuming, of course, that $\mathcal{O}' = \langle 1, \sqrt{-m} \rangle$, the order generated by 1 and $\sqrt{-m}$. In particular, we deduce that: $h' = 1$ for $m = 3$; $h' = 3h(\sqrt{-m})$ for $m > 3$, $m \equiv 3 \pmod 8$; $h' = h(\sqrt{-m})$ for $m \equiv 7 \pmod 8$. These formulas are also valid for $\mathcal{O}''$ in case it is not the maximal order of K_ν.

We are now in a position to evaluate the contributions of the terms $\delta \equiv (\mu,\nu)$ when d is odd. For the sake of convenience, we will let $\mathcal{O}', \mathcal{O}''$ denote the aforementioned non-maximal orders of K_μ, K_ν, respectively; $\mathcal{O}$ will denote the generic maximal order of K_μ or K_ν.

a) Suppose $m = 3$. Then $\frac{h'}{w'} = \frac{h''}{w''} = \frac{1}{2}$, $\frac{h(\mu)}{w_\mu} = \frac{h(\nu)}{w_\nu} = \frac{1}{6}$.

(1) If $\mu \simeq \sqrt{-3} \simeq \nu$, then the only possibilities for the orders of K_μ and K_ν, respectively, are: $(\mathcal{O}', \mathcal{O}'')$, $(\mathcal{O}', \mathcal{O})$, $(\mathcal{O}, \mathcal{O}'')$ and $(\mathcal{O}, \mathcal{O})$. Hence by (i) of Lemma 3.14, the contribution of

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

$\{(\sqrt{-3},\sqrt{-3})\}$ is: $2^{e-2}\left(\left(\frac{1}{2}\right)^2 + \frac{1}{2}\cdot\frac{1}{6} + \frac{1}{6}\cdot\frac{1}{2} + \left(\frac{1}{6}\right)^2\right)\delta(\sqrt{-3}) = \frac{2^{e+2}}{36}\delta(\sqrt{-3})$

(2) If $\mu \simeq \sqrt{-3}$, $\nu \simeq \frac{3+\sqrt{-3}}{2}$, the only possibilities for orders are $(0',0)$ and $(0,0)$. Hence by (ii) of Lemma 3.14, the contribution is: $2^{e-1}\left(\frac{1}{2}\cdot\frac{1}{6} + \frac{1}{36}\right)\delta(\sqrt{-3}) = \frac{2^{e+1}}{36}\delta(\sqrt{-3})$.

(3) If $\mu \simeq \frac{3+\sqrt{-3}}{2}$, $\nu \simeq \sqrt{-3}$, then, by symmetry, the contribution is also $\frac{2^{e+1}}{36}\delta(\sqrt{-3})$.

(4) If $\mu \simeq \frac{\pm 3+\sqrt{-3}}{2}$, $\nu \simeq \frac{3+\sqrt{-3}}{2}$, then the only possibility is $(0,0)$ and the contribution is equal to: $\frac{2^{e-1}}{36}\delta(\sqrt{-3})$, by (ii) of Lemma 3.14. Therefore, the total contribution to the trace sum coming from T(3) is: $\frac{(2^{e+2} + 2^{e+1} + 2^{e+1} + 2^{e})}{36}\delta(\sqrt{-3}) = 2^{e-2}\delta(\sqrt{-3})$.

b) Suppose $m > 3$, so that $\mu \simeq \sqrt{-m} \simeq \nu$. In particular, $\delta \equiv (\mu,\nu)$ is pure, so we apply (i) of Lemma 3.14 repeatedly:

(1) If $m \equiv 1 \pmod 4$, then $(0,0)$ is the only possible pair and it contributes: $2^{e-2\lambda(m)}\delta(\sqrt{-m})\frac{h(\sqrt{-m})^2}{4} = 2^{e-2(\lambda(m)+1)}\delta(\sqrt{-m})h(\sqrt{-m})^2$.

(2) If $m \equiv 3 \pmod 8$, then all four possibilities occur: $(0,0)$, $(0,0'')$, $(0',0)$ and $(0',0'')$. Hence, by Lemma 3.16, their contribution equals: $2^{e-2\lambda(m)}\delta(\sqrt{-m})\left(\frac{h(\sqrt{-m})^2}{4} + \frac{h(\sqrt{-m})^2 3}{4} + \frac{h(\sqrt{-m})^2 3}{4} + \frac{h(\sqrt{-m})^2 9}{4}\right) = 2^{e-2(\lambda(m)-1)}\delta(\sqrt{-m})h(\sqrt{-m})^2$.

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

(3) If $m \equiv 7 \pmod 8$, then all four pairs of possible orders occur and they contribute: $2^{e-2\lambda(m)}\,\delta(\sqrt{-m})h(\sqrt{-m})^2$.

Summarizing, the total contribution of $T(m)$ to the trace sum for $m > 3$ is: $2^{e-2(\lambda(m)+\sigma(m))}\,\delta(\sqrt{-m})h(\sqrt{-m})^2$, where:

$$\sigma(m) = \begin{cases} -1 & \text{if } m \equiv 3 \pmod 8 \\ 0 & \text{if } m \equiv 7 \pmod 8 \\ 1 & \text{if } m \equiv 1 \pmod 8 \end{cases}$$

Collecting all the terms contributed by cases (i) - (iv) for d odd, we finally obtain:

$$2^{-e}\left(h_d^2 + \left(2^{e-1}\,\delta(\sqrt{-3})\right)^2 + \sum_{m>3}\left(2^{e-\lambda(m)-\sigma(m)}\,\delta(\sqrt{-m})h(\sqrt{-m})\right)^2\right), \text{ which}$$

completes the proof of Theorem 2.1.

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

§1. Comparison with the classical theory

In the classical theory of quadratic forms one proceeds as follows: A quadratic form in n variables over $\mathbb{Q}$ is defined to be a homogeneous polynomial $q(x_1,\ldots,x_n)$ of degree two with coefficients in $\mathbb{Q}$, i.e.:

$$q(x_1,\ldots,x_n) = \sum_{i=1}^{n} A_i x_i^2 + \sum_{i<j} B_{ij} x_i x_j, \text{ where } A_i, B_{ij}$$

are in $\mathbb{Q}$. We shall assume in addition that q is not negative definite (cf. p.5). The discriminant $D(q)$ of q is defined by: $D(q) = (-1)^{[n/2]} \left| \frac{\partial^2 q}{\partial x_i \partial x_j} \right|$. We shall always assume that $q(x_1,\ldots,x_n)$ is non-degenerate, i.e. $D(q) \neq 0$. A quadratic form $q(x_1,\ldots,x_n)$ is integral if $A_i, B_{ij} \in \mathbb{Z}$ for all $i,j = 1,\ldots,n$.

Two quadratic forms $q(x_1,\ldots,x_n), q'(x_1,\ldots,x_n)$ are said to be (properly) equivalent if there exists $\sigma \in SL(n,\mathbb{Z})$ such that $q'(x_1,\ldots,x_n) = q(\sigma x_1,\ldots,\sigma x_n)$, where $\sigma x_i = \sum_j a_{ij} x_j$ if $\sigma = (a_{ij})$. Clearly, if q and q' are equivalent, then: (i) $D(q) = D(q')$ and (ii) q integral $\Leftrightarrow$ q' integral. Fixing n for the remainder of the discussion, we say that an integer Δ is a discriminant if $\Delta \neq 0$ and there exists an integral quadratic form $q(x_1,\ldots,x_n)$ such that $D(q) = \Delta$. Then, using Hermite's reduction theory, one can prove:

Theorem 4.1: If Δ is a discriminant, there are only finitely many equivalence classes of integral quadratic forms q such that $D(q) = \Delta$.

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

We denote this number by $H(\Delta)$. It is this notion of class number which is of interest from the classical point of view. The relationship between the classical approach and the modern lattice-theoretic approach which we have adopted in this thesis will now be described.

We enumerate all the isometry classes of non-degenerate quadratic vector spaces of dimension n over $\mathbb{Q}$ and choose representatives: $V^1, V^2, \ldots, V^k, \ldots$. For each V^k we enumerate the collection of genera of integral lattices within V^k: $\mathcal{G}_1^k, \mathcal{G}_2^k, \ldots, \mathcal{G}_\ell^k, \ldots$. Each $\mathcal{G}_\ell^k$ decomposes into a finite disjoint union of proper classes: $\mathcal{G}_\ell^k = \bigcup_{m=1}^{H_{k\ell}} \mathcal{C}_{\ell m}^k$. We denote by $D(\mathcal{G}_\ell^k)$ the discriminant of $\mathcal{G}_\ell^k$.

Let us set $V = \mathbb{Q}^n$, $M = \mathbb{Z}^n$. Then M has the canonical base $e_1, \ldots, e_n$, where $e_i = (\ldots, 0, \overset{\hat{i}}{1}, 0, \ldots)$, $1 \leq i \leq n$. If $q(x_1, \ldots, x_n)$ is a non-degenerate integral quadratic form, we associate to it a non-degenerate quadratic vector space (V,q) in the obvious manner: if $\alpha = a_1 e_1 + \ldots + a_n e_n \in V$, then $q(\alpha) = q(a_1, \ldots, a_n)$. With respect to this structure of quadratic vector space M becomes an integral lattice, which we denote by (M,q). (V,q) is isometric to V^k for some k by an isometry σ. However, we can not choose σ arbitrarily, since we are interested in <u>proper</u> equivalences. To insure that we do not have any difficulties in this regard, we fix an <u>ordered</u> basis $v_1^k, \ldots, v_n^k$ of V^k for each k, and insist that the linear endomorphism of V^k which takes the ordered basis $\sigma e_1, \ldots, \sigma e_n$ to the ordered basis $v_1^k, \ldots, v_n^k$ have <u>positive</u> determinant.

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

Then, via the isometry σ, $(M,q) \in \mathcal{C}^k_{\ell m}$, for certain ℓ and m. One can show quite easily that $\mathcal{C}^k_{\ell m}$ does not depend on the choice of σ, so we set $\mathcal{C}(q) = \mathcal{C}^k_{\ell m}$. Moreover, $\mathcal{C}^k_{\ell m}$ depends only on the equivalence class $\{q\}$ of q, so we may write: $\mathcal{C}(\{q\}) = \mathcal{C}^k_{\ell m}$.

Conversely, given $\mathcal{C}^k_{\ell m}$ for certain k,ℓ and m, we choose an integral lattice $M^k_{\ell m}$ in V^k which represents $\mathcal{C}^k_{\ell m}$. If $\varepsilon_1,\ldots,\varepsilon_n$ is a base of $M^k_{\ell m}$ such that the endomorphism of V^k taking $\varepsilon_1,\ldots,\varepsilon_n$ to $v^k_1,\ldots,v^k_n$ has positive determinant, then we can define an integral quadratic form q by: $q(x_1,\ldots,x_n) = q_k(x_1\varepsilon_1 + \ldots + x_n\varepsilon_n)$, where q_k is the quadratic form on V^k. We write $\mathcal{Q}(M^k_{\ell m}) = \{q\}$. It is easily seen that $\mathcal{Q}(M^k_{\ell m})$ is independent of the choice of basis $\varepsilon_1,\ldots,\varepsilon_n$ and of the representative $M^k_{\ell m}$. Hence we may write $\mathcal{Q}(\mathcal{C}^k_{\ell m}) = \{q\}$.

It is not difficult to verify that the mappings $\mathcal{C}$ and $\mathcal{Q}$ are mutual inverses, thereby yielding a one-to-one correspondence $\mathcal{C}^k_{\ell m} \longleftrightarrow \{q\}$. This correspondence preserves discriminants, in the sense that $D(M^k_{\ell m}) = D(q)$ if $\mathcal{C}^k_{\ell m} \longleftrightarrow \{q\}$ and $M^k_{\ell m} \in \mathcal{C}^k_{\ell m}$. In particular, if Δ is a discriminant, the set of equivalence classes of integral quadratic forms of discriminant Δ decomposes into a disjoint union of subsets of the form $\mathcal{Q}(\mathcal{O}^k_\ell)$. Accordingly, we say that two integral quadratic forms q and q' are of the same <u>genus</u> if $q,q' \in \mathcal{Q}(\mathcal{O}^k_\ell)$ for some k and ℓ. This definition is equivalent to: there exist $\sigma_p \in SL(n,\mathbb{Z}_p)$ for $p \neq \infty$, $\sigma_\infty \in GL(n,\mathbb{R})$, such that $q'(x_1,\ldots,x_n) = q(\sigma_p x_1,\ldots,\sigma_p x_n)$. In other words, two integral quadratic forms are of the same genus if and only if

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

they are "locally equivalent".

Let D be a fundamental discriminant in the sense of I.2. Then the set of equivalence classes of integral forms having discriminant D decomposes into a finite union of genera. If n = 2, the set of equivalence classes forms an abelian group with one of the genera, called the principal genus, as a subgroup in such a manner that the other genera are cosets with respect to the principal genus. In fact, using the notation of I.2, we have: $H(D) = h^+(\sqrt{D}) = 2^{e-1}H$. For $n > 2$, however, there is no such group structure, so the decomposition into genera need not be uniform. In our particular case, where $n = 4$, $D = d^2$, $d = p_1 \ldots p_e$ with e odd, in order to compute H(D) we need to determine all the possible quaternion algebras $\mathcal{A}$ which have genera of integral lattices with discriminant D. Clearly, any such $\mathcal{A}$ must have fundamental discriminant dividing D. Hence we need only consider the 2^e distinct quaternion algebras $\{\mathcal{A}_m\}$, where $m|d$ and $\mathcal{A}_m$ has fundamental discriminant m^2. Then $\mathcal{A}_d$ contains a unique genus of integral lattices having discriminant D, namely the genus of maximal integral lattices. Using the special kind of non-maximal orders investigated by Eichler in [6], it is a simple matter to show that each $\mathcal{A}_m$, for $m < d$, contains at least one genus of (non-maximal) integral lattices with discriminant D. We conclude that $H(D) = H + \sum_{m<d} H_m$, where H_m = the number of proper classes of integral lattices within $\mathcal{A}_m$ having discriminant equal to D.

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

§2. Generalizations

There are essentially two ways that one could generalize the results we have presented. On the one hand, one could try to extend the results to non-maximal integral lattices. Such a generalization would not be an idle academic exercise because, as we have just seen, in order to compute H(D), one must be able to compute class numbers of certain special genera of non-maximal integral lattices. These are the genera having discriminant m^2 for m a square-free integer. One of these genera is the one containing the non-maximal orders of "Eichler type" (cf.[6]). The fact that Eichler [6] obtained a formula for the ideal class number of such orders which extends the known formula for h_d (Theorem 1.7) strongly suggests that we should be able to extend Theorem 2.1 to include this genus of "Eichler lattices". It is not clear whether such an extension is possible for the other genera having discriminant m^2, m square-free. If it were, one would then obtain a formula for H(D) which would be very similar to the one we derived for H.

On the other hand, one could also attempt to extend the results to quaternary forms of square discriminant over arbitrary algebraic number fields F, which would have to be totally real in order to insure positive definiteness. The difficulty in this case arises from the fact that in our derivation we replaced the usual definition of H by: H = the number of equivalence classes of normal ideals of $\mathcal{O}$ (Proposition 3.1). If

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

one looks closely at our proof of Proposition 3.1, one will notice that we made use of the fact that N(I) is an element of $\mathbb{Q}^*$ for any normal ideal I of $\mathcal{O}$. In the general case, however, N(I) is only a fractional ideal which need not be principal. Hence our proof will carry over only if the base field F has class number equal to one. Moreover, in our derivation of the formula for H we used the fact that $\Delta(J^1_{\mathbb{Q}}) = \Delta(U^1_{\mathbb{Q}})\Delta(\mathbb{Q}^*)$, which is equivalent to $\mathbb{Q}$ having class number equal to one.

§3. The non-square discriminant case

It is natural to ask whether our methods can be extended to the essentially different case of a positive definite quaternary form having non-square discriminant. Using the theory of Clifford algebras, one can show that any such quadratic vector space is isometric to a quadratic vector space (Λ, N) obtained as follows: Let $\mathcal{O}$ be a positive definite quaternion algebra with norm form N. Let K be a real quadratic extension $\mathbb{Q}(\sqrt{\Delta})$, where $\Delta > 0$ is square-free. We then have a canonical involution ι defined on $\mathcal{O}$ and a conjugation $a \to \bar{a}$ defined on K. If we set $\mathcal{O}_K = \mathcal{O} \otimes_{\mathbb{Q}} K$, then ι extends naturally to the canonical involution of $\mathcal{O}_K$ and the conjugation extends coefficientwise to $\mathcal{O}_K$. Then $\Lambda = \{\alpha \in \mathcal{O}_K \mid \iota(\alpha) = \bar{\alpha}\}$ is a four-dimensional $\mathbb{Q}$-subspace of $\mathcal{O}_K$ which, by restriction of N, becomes a quadratic vector space whose discriminant has square-free kernel = Δ. Moreover, all proper orthogonal transformations of (Λ, N) are given by mappings of the type: $x \to \alpha x \bar{\alpha}^{-1}$, where $x \in \Lambda$, $\alpha \in \mathcal{O}_K^*$ with $N(\alpha) \in \mathbb{Q}^*$.

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

In this case, matters are complicated first by the fact that Λ does not have as nice an algebraic structure to be exploited as in the square discriminant case. Secondly, we can not work with $O^+(\Lambda)$ for reasons similar to those in the square discriminant case and it is even less clear what to replace $O^+(\Lambda)$ by. Using some ideas of Tamagawa, it is possible to circumvent the first difficulty by utilizing the structure of $\mathcal{O}_K$ and establishing a nice correspondence between integral lattices in Λ and certain special kinds of normal ideals of $\mathcal{O}_K$. These are the "symmetric normal ideals" of $\mathcal{O}_K$, namely, those which satisfy the condition: $\iota(I) = \bar{I}$. The symmetric normal ideals are operated upon by "similarity" transformations: $x \longrightarrow c \cdot \alpha x \overline{\iota(\alpha)}$, where $c \in \mathbb{Q}^*$ and $\alpha \in \mathcal{O}_K^*$. The second difficulty is then circumvented by replacing $O^+(\Lambda)$ with the group of similarity transformations. Using this approach in the special case where D = p, a prime (necessarily congruent to 1 (mod 4)), Tamagawa has obtained:

Theorem 4.2:

$$H = \frac{h(\mathcal{O}_K)}{h(\sqrt{p})}$$

, where $h(\mathcal{O}_K)$ = the ideal class number of $\mathcal{O}_K$.

§4. Tables

In the following tables we will list h_d and H for all the possible $d < 400$. Within this range there are only two possibilities for e: e = 1 or e = 3. Since H is much larger with respect to d for e = 1 than for e = 3, we list the two cases

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

separately. This disparity would probably diminish if we were to compute H(D) instead of H, since the number of genera having discriminant D increases with e. Table 1 lists the case e = 1, d = p, a positive prime. Table 2 lists the case e = 3, d = $p_1p_2p_3$, where p_1, p_2, p_3 are positive primes and $p_1 < p_2 < p_3$. The values for $h(\sqrt{-m})$ are taken from Gauss [8]. In using Gauss's tables, one must be careful to divide the listed value by 3 for $m \equiv 3 \pmod 8$. The reason is that the listed value is the ideal class number of the non-maximal order mentioned in Lemma 3.16.

Notice: The author can not guarantee the infallibility of these tables. However, it is interesting to note that we have the following partial check of the values of H listed in Table 1: From Corollary 2.2 it is easily seen that H must be a sum of two squares for d = p, a prime. Consequently, the square-free kernel of H can be divisible only by the following kinds of primes: p = 2 or $p \equiv 1 \pmod 4$.

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

Table 1

p	h_p	$h(\sqrt{-p})$	H	p	h_p	$h(\sqrt{-p})$	H
2	1	1	1	173	15	14	137
3	1	1	1	179	16	5	178
5	1	2	1	181	15	10	125
7	1	1	1	191	17	13	229
11	2	1	4	193	16	4	130
13	1	2	1	197	17	10	157
17	2	4	4	199	17	9	185
19	2	1	4	211	18	3	180
23	3	3	9	223	19	7	205
29	3	6	9	227	20	5	250
31	3	3	9	229	19	10	193
37	3	2	5	233	20	12	218
41	4	8	16	239	21	15	333
43	4	1	10	241	20	12	218
47	5	5	25	251	22	7	340
53	5	6	17	257	22	16	274
59	6	3	36	263	23	13	349
61	5	6	17	269	23	22	325
67	6	1	20	271	23	11	325
71	7	7	49	277	23	6	269
73	6	4	20	281	24	20	338
79	7	5	37	283	24	3	306
83	8	3	50	293	25	18	353
89	8	12	50	307	26	3	356
97	8	4	34	311	27	19	545
101	9	14	65	313	26	8	346
103	9	5	53	317	27	10	377
107	10	3	68	331	28	3	410
109	9	6	45	337	28	8	400
113	10	8	58	347	30	5	500
127	11	5	73	349	29	14	445
131	12	5	122	353	30	16	482
137	12	8	80	359	31	19	661
139	12	3	90	367	31	9	521
149	13	14	109	373	31	10	493
151	13	7	109	379	32	3	530
157	13	6	89	383	33	17	689
163	14	1	100	389	33	22	605
167	15	11	173	397	33	6	549

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

Table 2

d	$p_1 \cdot p_2 \cdot p_3$	h_d	A_{p_1}	A_{p_2}	A_{p_3}	$A_{p_1p_2}$	$A_{p_2p_3}$	$A_{p_1p_3}$	A_d	H
30	2·3·5	2	0	2	0	0	0	2	2	2
42	2·3·7	2	2	0	0	0	2	0	2	2
66	2·3·11	4	2	2	0	0	2	2	4	6
70	2·5·7	2	2	0	0	0	2	0	2	2
78	2·3·13	2	0	0	2	2	0	0	2	2
102	2·3·17	4	0	2	0	2	2	4	2	6
105	3·5·7	4	0	0	4	4	0	0	4	8
110	2·5·11	6	0	2	0	0	0	2	6	10
114	2·3·19	4	2	0	2	2	2	0	4	6
130	2·5·13	4	2	2	2	0	4	0	2	6
138	2·3·23	6	2	2	0	2	4	4	4	12
154	2·7·11	6	2	0	2	4	4	2	4	12
165	3·5·11	8	4	0	0	4	8	4	4	24
170	2·5·17	8	0	2	4	2	2	0	6	16
174	2·3·29	6	0	2	0	0	0	2	6	10
182	2·7·13	6	2	0	0	0	2	0	6	10
186	2·3·31	6	2	0	0	0	2	0	6	10
190	2·5·19	6	0	2	0	0	0	6	2	10
195	3·5·13	8	0	0	4	4	0	0	8	20
222	2·3·37	6	0	0	2	2	0	0	6	10
230	2·5·23	10	2	0	0	0	2	0	10	26
231	3·7·11	12	0	0	0	0	0	0	12	36
238	2·7·17	8	0	0	0	4	0	0	4	12
246	2·3·41	8	0	2	0	2	2	4	6	16
255	3·5·17	12	4	0	0	0	4	0	12	40
258	2·3·43	8	2	0	2	2	6	0	4	16
266	2·7·19	10	2	0	0	0	2	0	10	26
273	3·7·13	12	0	4	0	4	8	8	4	40
282	2·3·47	10	2	2	0	2	4	8	4	26
285	3·5·19	12	0	0	0	0	0	4	8	28
286	2·11·13	10	0	2	0	0	0	6	6	22
290	2·5·29	12	2	0	0	2	4	2	10	34
310	2·5·31	10	2	2	0	2	4	8	4	26
318	2·3·53	10	0	2	0	0	0	6	6	22
322	2·7·23	12	4	0	0	0	8	4	4	32
345	3·5·23	16	4	0	0	0	8	0	4	44
354	2·3·59	12	2	2	0	0	2	6	8	32
357	3·7·17	16	0	4	0	0	0	8	4	44
366	2·3·61	10	0	0	6	2	0	0	6	22
370	2·5·37	12	2	2	2	0	8	0	6	32
374	2·11·17	16	0	2	0	2	2	4	14	60
385	5·7·11	20	0	0	0	0	8	0	4	60
399	3·7·19	20	0	4	0	0	4	4	16	88

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

References

1. H. Brandt, Idealtheorie in Quaternionenalgebren, Math. Ann. 99 (1928), 1-29.

2. M. Deuring, Algebren, Ergebnisse der Mathematik und ihrer Grenzgebiete, Band 4, Springer-Verlag, Berlin and New York, 1935.

3. _____, Die Anzahl der Typen von Maximalordnungen einer definiten Quaternionenalgebra mit primer Grundzahl, Jber. Deutsch. Math. Verein. 54 (1950), 24-41.

4. M. Eichler, Quadratische Formen und orthogonale Gruppen, Springer-Verlag, Berlin, 1952.

5. _____, Über die Idealklassenzahl total definiter Quaternionenalgebren, Math. Z. 43 (1937), 102-109.

6. _____, Zur Zahlentheorie der Quaternionen-Algebren, J. Reine Angew. Math. 195 (1955), 127-151.

7. _____, Über die Darstellbarkeit von Modulformen durch Thetareihen, J. Reine Angew. Math. 195 (1955), 156-171.

8. C. F. Gauss, Werke, Band II, Göttingen, 1876, Tafel der Anzahl der Classen binärer quadratischer Formen, pp.449-476.

9. O. T. O'Meara, Introduction to quadratic forms, Springer-Verlag, Berlin, 1963.

10. T. Tamagawa, On Selberg's trace formula, J. Fac. Sci. Univ. Tokyo Sect. I 8 (1960), 363-386.

11. _____, Harmonic analysis on adele groups, mimeographed notes taken by L. Goldstein, Advanced Science Seminar in Algebraic Groups, Bowdoin College, Me., 1968.

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

12. G. L. Watson, Representations of integers by indefinite quadratic forms, Mathematika 2 (1955), 32-38.

13. A. Weil, Adeles and algebraic groups, lecture notes, Princeton Univ., 1961.

14. _____, Sur la théorie des formes quadratiques, Colloque sur la Théorie des Groupes Algébriques, Bruxelles, 1962, pp. 9-22.

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.