HECKE THEORY OVER COMPLEX QUADRATIC FIELDS

by Robert Alan Styer

Submitted to the Department of Mathematics on May 1, 1981 in partial fulfillment of the requirements for the degree of Doctor of Philosophy.

ABSTRACT

This thesis generalizes work of Stark and Patterson-Goldfeld to complex quadratic fields of class number greater than one. We first define a vector Hecke operator which has a classical-looking multiplicative relation. We then define vector forms on the quaternionic upper half space, and examine their Fourier expansions and the effect of the Hecke operators on these coefficients. Then we examine eigenforms of the Hecke operators, and Dirichlet series formed out of these vector forms. One obtains both Euler products and functional equations for the Dirichlet series. Finally, we define quaternionic Eisenstein series and study their Fourier expansions and Dirichlet series. We obtain results that are remarkably close to the classical analogs.

Thesis supervisor: Harold M. Stark
Title: Professor of Mathematics

TABLE OF CONTENTS

ACKNOWLEDGMENTS

"A student is not above his teacher, but everyone who is fully trained will be like his teacher" (Luke 6.40, NIV). God has surely blessed me with tremendous teachers. Miss Slater interested me in math in seventh grade, Ruth Delcamp encouraged me in ninth, Prof. Sigler in twelfth, Prof. Shatz at Penn, and now Prof. Stark for the last few years. I also owe many debts to Prof. Ankeny and Prof. Goldfeld for teaching me a large part of what little I know of number theory. I am also grateful for colleagues and friends who have taught me a great deal not only about number theory but also about life. Special thanks belong to Ram Murty, Bob Rumely, Prof. Patterson, Prof. Terras, Sol Friedberg, and Jon Sands. Again, I want to specifically acknowledge Dorian Goldfeld and Harold Stark as the chief brain trusts behind this thesis, and to thank Prof. Stark for his continual patience and generosity during the last two years.

I. Introduction

From the time of Gauss and Ramanujan, people have been interested in the coefficients of modular forms. One of the most useful tools used to study these coefficients is the Hecke algebra. Hecke's theory enables one to see the connections between the modular forms and the associated Dirichlet series.

The classical modular forms were quickly generalized to Hilbert modular forms, defined over totally real fields. Whenever the class number of the field was greater than one, however, people found obstacles to extending Hecke theory to Hilbert modular forms. Oskar Hermann [5] finally overcame these difficulties by introducing the idea of a vector of modular forms, each component of the vector form corresponding to an ideal class of the field. He uses ideal numbers to essentially introduce a principal generator for each ideal. Eichler [1] has defined vector forms without using ideal numbers, but only by replacing the ideal numbers by complicated conditions on the ideals involved.

Ideal numbers are very appealing; essentially their origins go back to Kummer. Hecke [4] developed them fully in 1920 in order to replace ideals by specific elements. Ideal numbers behave like algebraic integers except for an important restriction on addition. One can only add ideal numbers within a given class, and this forces one to consider classes of matrices and classes of forms. This is why Hermann introduces vector forms and vector Hecke operators.

Hilbert modular forms are only defined over totally real fields. Recently, several people have considered the complex field analogs for modular forms. One introduces the quaternionic upper half space which supports an action by $SL(2, \mathbb{C})$. One also introduces representations of the quaternions in order to guarantee the needed transformation properties. For fields of class number one, Patterson-Goldfeld [8] have developed Eisenstein series defined on the quaternionic upper half space. Stark [10] has extended Hecke operators to the complex case if the field has class number one.

This thesis extends the work of Patterson-Goldfeld and of Stark to complex quadratic fields of class number greater than one. The concepts used parallel those of Hermann, so we also introduce vector forms and vector Hecke operators. In the complex case, however, even when the class number is one, the forms are vectors, so we will actually need to consider vectors of vectors, which makes the notation slightly awkward. Nevertheless, the basic results parallel the classical cases. In Chapter II we introduce ideal numbers and develop the needed properties. One can then develop the Hecke operators, which look remarkably similar to the classical case. Chapter III begins with a short discussion of the quaternionic upper half space and of quaternionic representations. We now have all of the preliminaries.

Now one can develop the theory of modular forms. As mentioned before, we actually have a vector of forms, one component for each ideal class. These components in turn are vectors, each a modular form with respect to a fixed class of matrix operators. One can introduce Fourier expansions in a very general setting — the example of the Eisenstein series in Chapter IV shows the reasonableness of our definition. After suitably renormalizing the Hecke operators, one considers simultaneous eigenforms and finds analogs to many of the classical results. For instance, the Fourier coefficients correspond closely to the eigenvalues of the Hecke operators. They are not equal, however, which would be impossible since the Fourier coefficients actually are a vector themselves, while the eigenvalues are scalars. Nevertheless, the correspondence is very close, and one can show that the multiplicativity of the coefficients is related to the vector form being an eigenform for the Hecke operators.

Dirichlet series are found via two techniques. The Mellin transform defines a Dirichlet series which has a functional equation. The eigenvalues of the Hecke operators define another Dirichlet series which has an Euler product. These Dirichlet series are not the same, however, since the Fourier coefficients are not exactly equal to the eigenvalues. One suitably twists the series, therefore, to create a new Dirichlet series which has both an Euler product and a functional equation.

After wrestling with the complications of vectors of forms and vector Hecke operators, one could wish that the principal component corresponding to the principal ideal class might contain enough information to reconstruct the entire form. If so, then one would be able to eliminate ideal numbers and the complicated vectors of vectors. The principal theorem in Chapter III Section 8 shows that one's wish can be fulfilled. If a function f is an eigenform for "principal" Hecke operators and is modular with respect to the "principal" matrices, then one can find a vector eigenform which has f as its principal component.

The final chapter illustrates the results of Chapter III by defining quaternionic Eisenstein series. We explicitly find the

Fourier coefficients and the Hecke eigenvalues, which are remarkably similar to the results one gets in the classical cases. We explicitly evaluate the matrix integral which appears in the Fourier expansion, and show that one gets a matrix with sums of Bessel functions. This is slightly surprising, but a consideration of the differential equations satisfied by the integrals confirms that one gets Bessel functions. In case the weight is one, a quaternion-valued Eisenstein series can be defined for which an interesting differential equation can be found, but for other weights this equation does not seem to have an obvious analogy. Finally, we develop an example of Eisenstein series over $K = Q(\sqrt{-23})$.

In conclusion, the complications of class number greater than one are relatively minor. The broad outlines are precisely those found in the classical analogs. Furthermore, since the principal components determine the entire form, one need not even consider ideal numbers nor a vector of vectors, with a separate component for each ideal class.

II. 1 Ideal Numbers

Ideal numbers are an appealing concept, underlying the original ideas of Kummer. Hecke [4] developed a full theory of ideal numbers in 1920, which is summarized in Hermann [5]. In this section I will establish the notation and basic properties of ideal numbers.

Let K be an algebraic number field, and let O(K) be the algebraic integers of K, and let U be the units of O(K). Let $\underline{I}$ be the group of ideals over O(K), and $\underline{P}$ the subgroup of principal ideals. Then classical algebraic number theory shows that $\underline{I}/\underline{P}$ is a finite abelian group of order h, called the ideal class number. We can decompose $\underline{I}/\underline{P}$ into a direct product of cyclic subgroups, say $G_1 \times G_2 \times \cdots \times G_r$. Let N_s = order (G_s), $s = 1, 2, \ldots, r$.

For any ideal $\underline{a}$, let $[\underline{a}]$ denote the class of $\underline{a}$ in $\underline{I}/\underline{P}$. Choose ideals $\underline{b}_s$ so that $[\underline{b}_s]$ generates G_s, $s = 1, 2, \ldots, r$. Then $\underline{b}_s^{N_s}$ is a principal ideal, so let $\underline{b}_s^{N_s} = c_s \cdot O(K) = (c_s)$ for some $c_s \in K$. Let $\beta_s = \sqrt[N_s]{c_s}$ where we fix some N^{th} root of c_s, with $N = \ell.c.m\,(N_1, N_2, \ldots, N_r)$.

Suppose $\underline{a}$ is any ideal. Then $\underline{a} = (c)\underline{b}_1^{P_1} \cdot \underline{b}_2^{P_2} \cdots b_r^{P_r}$ for some integer powers P_s mod N_s and for some $c \in K$. Define $\alpha = c \cdot \beta_1^{P_1} \cdots \beta_r^{P_r}$. Then α is said to be an ideal number associated to the ideal $\underline{a}$. Let $K[\underline{a}] = \{d\alpha \mid d \in K\}$.

Before proceeding, I must comment on the arbitrary choices we have made in defining α. Firstly, the decomposition $\underline{I}/\underline{P} = G_1 \times G_2 \times \cdots \times G_r$ is not unique, nor the choice of generators $\underline{b}_s$. Secondly, the choices of c_s and c are only determined modulo U, and also the N^{th} root is fixed arbitrarily. Fortunately, however, N is the same for any decomposition $G_1 \times \cdots \times G_r$. Changing the generators $\underline{b}_s$ changes α by a principal element (up to an arbitrary N^{th} root of unity) so $K[\underline{a}]$ is unchanged. The arbitrary N^{th} root is more critical. Changing the choice of c_s generating $\underline{b}_s$ and changing the branch of the root will change α by an arbitrary N^{th} root of a unit $u \in U$. In particular, for a complex quadratic field with $h > 1$, $U = \{1, -1\}$ so the ideal numbers are unique only up to an arbitrary $2N^{th}$ root of unity.

Notation. Small underlined Latin letters will denote ideals of $\underline{I}$. Small Greek letters will be reserved for ideal numbers. Propositions and theorems will be numbered, and in case they have several parts, a second number will denote the specific part. For instance, Prop. 4.3 means Proposition 4, part number 3.

II.2 Properties of Ideal Numbers

Let $\underline{a}_1, \underline{a}_2, \ldots, \underline{a}_h$ be ideal class representatives. Define the set of ideal numbers to be $Z = \bigcup_{m=1}^{h} K[\underline{a}_m]$. If $[\underline{a}] = [\underline{a}_m]$ then $K[\underline{a}] = K[\underline{a}_m]$. Notice that if $[\underline{a}] \neq [\underline{a}_m]$ then $K[\underline{a}] \cap K[\underline{a}_m] = \{0\}$.

The multiplication of K extends to Z, and in fact $K[\underline{a}] \cdot K[\underline{b}] = K[\underline{a} \cdot \underline{b}]$, so Z is a multiplicative group. Given $\alpha \in Z$, we have $\alpha = c \cdot \beta_1^{P_1} \beta_2^{P_2} \cdots \beta_r^{P_r}$ for some $c \in K$, $P_s \bmod N_s$, so we can associate an ideal $\underline{a} = (c)\underline{b}_1^{P_1} \underline{b}_2^{P_2} \cdots \underline{b}_r^{P_r}$. This association is a surjective homomorphism $(-): Z \to \underline{I}$ given by $\alpha \to (\alpha) = \underline{a}$. The kernel is U.

For any fixed $[\underline{a}]$, the addition of K extends to $K[\underline{a}]$, so $K[\underline{a}]$ is an additive group. One cannot, however, add two ideal numbers from different $K[\underline{a}]$. In other words, $\alpha + \beta$ is defined iff $[(\alpha)] = [(\beta)]$.

For convenience, define $[\alpha] = [(\alpha)]$ and $[\alpha\underline{a}] = [(\alpha)\underline{a}]$ for any $\alpha \in Z$ and $\underline{a} \in \underline{I}$. One has that $[\alpha]^{-1} = [\alpha^{-1}]$.

We define $\alpha \in Z$ to be an integral ideal number if α is an algebraic integer which happens iff (α) is an integral ideal. Let $O[\underline{a}]$ be the integral elements of $K[\underline{a}]$ and $O(Z) = \bigcup_{m=1}^{h} O[\underline{a}_m]$ be the integral elements of Z. If $\alpha, \beta \in Z$, we say that α divides

β, written $\alpha \mid \beta$, if β/α is an integral ideal number. Note that $\alpha \mid \beta$ in Z iff $(\alpha) \mid (\beta)$ in $\underline{I}$. From this observation immediately follow the multiplicative properties of greatest common divisors and least common multiples for ideal numbers. We can also define congruences: if $\alpha, \beta, \gamma \in Z$, we say $\alpha \equiv \beta \bmod \gamma$ when $(\alpha - \beta)/\gamma$ is integral. In particular, $[\alpha] = [\beta]$ so that $\alpha - \beta$ will be defined. The properties of congruences in K extend to Z. In particular, for $\alpha \in O(Z)$, define $N(\alpha) = N((\alpha))$ where $N((\alpha))$ is the norm of the ideal (α) which is also the number of incongruent representatives mod (α) in K. The following proposition summarizes useful facts we will need later.

<u>Proposition 1</u>. Define (α, β) = greatest common divisor (α, β).

1) Let $[\underline{c}]$ be any ideal class, $\alpha, \beta \in Z$, and $\alpha \mid \beta$. Then there exists $\gamma \in K[\underline{c}]$ so that $\alpha = (\beta, \gamma)$.

2) Let $\gamma = (\alpha, \beta)$. Then there exists $\mu, \nu \in O(Z)$ so that $\gamma = \alpha\mu + \beta\nu$.

3) Given $\alpha, \beta, \gamma \in Z$, $\alpha\mu \equiv \beta \bmod \gamma$ has an integral solution $\mu \in O(Z)$ iff $(\alpha, \gamma) \mid \beta$.

4) Let $[\underline{a}]$ be any ideal class, $\beta, \gamma \in O(Z)$. Then in $K[\underline{a}]$ there are $N(\beta)$ residue classes mod β, and furthermore we can choose representatives $\beta_1, \beta_2, \ldots, \beta_{N(\beta)} \in O[\underline{a}]$ so that $(\beta_n, \gamma) = 1$

for all $n = 1, 2, \ldots, N(\beta)$. Finally if $\delta \in O(Z)$ with $(\delta, \beta) = 1$, then $\delta\beta_1, \delta\beta_2, \ldots, \delta\beta_{N(\beta)}$ is a complete residue system mod β in $K[\underline{a}\,\delta]$.

5) Let $(\alpha, \delta) = 1$ and suppose $\alpha\beta \equiv \alpha\gamma \bmod \delta$. Then $\beta \equiv \gamma \bmod \delta$.

6) Define $\pi \in O(Z)$ to be prime if (π) is a prime ideal. Then for any $\alpha \in Z$, $\alpha = u\pi_1^{p_1}\pi_2^{p_2} \cdots \pi_k^{p_k}$ where $u \in U$, each π_n is prime, and each p_n is a rational integer.

Proof. The proofs for 1) and 6) follow from the corresponding properties for ideals. The proof of 2) is essentially the Euclidean algorithm, except that one must be careful to add numbers only when they lie in the same $K[\underline{a}]$. The crucial point that allows the algorithm to work is that zero is in $O[\underline{a}]$ for every $[\underline{a}]$. The proofs for 3) and 4) follow from the corresponding properties in $O(K)$, once one multiplies by an appropriate ideal number to put everything into the principal class. Then the proof of 5) follows since 3) implies that an inverse exists. QED

II. 3 Ideal Number Matrices

Let $GL(2, \mathbb{C})$ denote all 2×2 invertible complex matrices. Let $[\underline{a}], [\underline{c}]$ be ideal classes, and $\mu \in O(Z)$. Define a set of matrices

$$\Gamma^{\underline{a}}_{\underline{c}}(\mu) = \left\{ \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in GL(2, \mathbb{C}) \;\middle|\; \alpha\delta - \beta\gamma = \mu , \right.$$

$$\left. \alpha \in O[\underline{a}],\ \gamma \in O[\underline{c}],\ \beta \in O[\mu \underline{c}^{-1}],\ \delta \in O[\mu \underline{a}^{-1}] \right\} .$$

Note that $\Gamma^{\underline{a}}_{\underline{c}}(\mu) = \Gamma^{\underline{b}}_{\underline{d}}(\mu)$ iff $[\underline{a}] = [\underline{b}]$ and $[\underline{c}] = [\underline{d}]$.

For convenience we will write

$$\Gamma_{\underline{c}}(\mu) = \Gamma^{(1)}_{\underline{c}}(\mu) , \quad \Gamma^{\underline{a}}_{\underline{c}} = \Gamma^{\underline{a}}_{\underline{c}}(1), \text{ and } \Gamma_{\underline{c}} = \Gamma^{(1)}_{\underline{c}}(1) .$$

We now fix a representative of each $\Gamma^{\underline{a}_m}_{\underline{a}_n}$.

Choose some $C^{\underline{a}_m}_{\underline{a}_n} \in C^{\underline{a}_m}_{\underline{a}_n}$ for all $m, n = 1, 2, \ldots, h$. As usual, we let $C^{\underline{a}}_{\underline{b}} = C^{\underline{a}_m}_{\underline{a}_n}$ whenever $[\underline{a}] = [\underline{a}_m]$ and $[\underline{b}] = [\underline{a}_n]$. For convenience we may choose $C^{(1)}_{\underline{a}_m} = I$ for $m = 1, 2, \ldots, h$.

Proposition 2

1) (the consistency rule). Let $A \in \Gamma^{\underline{a}}_{\underline{c}}(\mu)$ and $B \in \Gamma^{\underline{b}}_{\underline{d}}(\nu)$. Then $A \cdot B$ is defined iff $[\underline{d}] = [\underline{a}\,\underline{b}\,\underline{c}\,\mu^{-1}]$. We have

$$\Gamma^{\underline{a}}_{\underline{c}}(\mu)\ \Gamma^{\underline{b}}_{\underline{a}\,\underline{b}\,\underline{c}\,\mu^{-1}}(\nu) = \Gamma^{\underline{a}\,\underline{b}}_{\underline{c}\,\underline{b}}(\mu\nu) .$$

2) $$\Gamma^{\underline{a}}_{\underline{c}}(\mu) \cdot C^{\underline{b}}_{\underline{a}\,\underline{b}\,\underline{c}\,\mu^{-1}} = \Gamma^{\underline{a}\,\underline{b}}_{\underline{c}\,\underline{b}}(\mu) .$$

3) $$C^{\underline{b}}_{\underline{c}\underline{a}^{-1}\underline{b}^{-1}} \Gamma^{\underline{a}}_{\underline{c}}(\mu) = \Gamma^{\underline{a}\underline{b}}_{\underline{c}\underline{b}^{-1}}(\mu) .$$

4) $$C^{\underline{b}}_{\underline{c}\underline{a}^{-1}\underline{b}^{-1}} C^{\underline{a}}_{\underline{c}} = A \cdot C^{\underline{a}\underline{b}}_{\underline{c}\underline{b}^{-1}} \text{ for some } A \in \Gamma_{\underline{a}^{-1}\underline{b}^{-2}\underline{c}} .$$

5) Given $A \in \Gamma_{\underline{a}\underline{c}}$ there is $A' \in \Gamma_{\underline{a}^{-1}\underline{c}}$ so that $C^{\underline{a}}_{\underline{c}} A = A' C^{\underline{a}}_{\underline{c}}$.

6) If $B \in \Gamma^{\underline{a}}_{\underline{c}}$ then $B^{-1} \in \Gamma^{\underline{a}^{-1}}_{\underline{c}}$.

Proof. These follow from straightforward matrix manipulation. QED

Remarks. It is impossible to overemphasize the importance of the consistency rule Prop. 2.1. We wish to develop Hecke theory, so we must require that the determinant of a matrix be defined. But as noted above, addition is only defined within a fixed $K[\underline{a}]$. Thus, one must take care that one multiplies matrices where the additions will be defined.

Later it will be convenient to identify matrices that differ only by elements of $\Gamma_{\underline{a}_m}$. We will say that $B \sim B'$ whenever there is an $A \in \Gamma_{\underline{a}_m}$ for some $m = 1, 2, \ldots, h$ so that $B = AB'$. We extend this to formal sums of matrices by saying that $B + D \sim B' + D'$ whenever $B \sim B'$ and $D \sim D'$.

II.4 Vectors of Matrix Operators

In the next chapter, I will define vector modular forms, and now I will define the vectors of matrices that will act on these forms. One should think of these vectors of matrices as operators, so in particular addition will be formal operator addition rather than matrix addition.

Let $\mu \in O(Z)$ and $[\underline{b}]$ be an ideal class. Choose representatives $\underline{a}_1, \underline{a}_2, \ldots, \underline{a}_h$ from each ideal class, with $\underline{a}_1 = (1)$ representing the principal class. This choice will remain fixed for the remainder of the thesis. Define a vector operator

$$A = A(\mu, \underline{b}) = \left(A_{[\underline{a}_m]}\right)_{m=1,2,\ldots,h} = \begin{pmatrix} A_{[\underline{a}_1]} \\ A_{[\underline{a}_2]} \\ \vdots \\ A_{[\underline{a}_h]} \end{pmatrix}$$

where $A_{[\underline{a}_m]} \in \Gamma^{\underline{b}}_{\underline{b}\,\underline{a}_m}(\mu)$ for $m = 1, 2, \ldots, h$.

For the remainder of this chapter, we will be dealing with many vectors of length h. I will reserve the letter m to run through the set $1, 2, \ldots, h$. I will also drop the subscripting index from vectors, and one must infer from the context and from the undetermined m that a vector of length h is indicated. For instance, $\left(A_{[\underline{a}_m]}\right)_{m=1,2,\ldots,h}$ will be written $\left(A_{[\underline{a}_m]}\right)$.

Let $B = B(\mu, \underline{b}) = \left(B_{[\underline{a}_m]}\right)$ be another vector of matrices $B_{[\underline{a}_m]} \in \Gamma^{\underline{b}}_{\underline{b}\,\underline{a}_m}(\mu)$. Then we define a formal addition by $A + B = \left(A_{[\underline{a}_m]} + B_{[\underline{a}_m]}\right)$, where the addition is formal addition of operators, not as matrices. We do not define addition of vectors $A(\mu, \underline{a})$ and $B(\nu, \underline{b})$, not even formally, unless $\mu = \nu$ and $[\underline{a}] = [\underline{b}]$.

Let $M(\mu, \underline{b})$ be the set of all formal sums of vector operators $A(\mu, \underline{b})$. Note that $[\underline{a}] = [\underline{b}]$ implies that $M(\mu, \underline{a}) = M(\mu, \underline{b})$. For convenience, we set $M = M(1, (1))$, $M(\mu, \underline{I}) = \bigcup_{m=1}^{h} M(\mu, \underline{a}_m)$, and $M(Z, \underline{I}) = \bigcup_{\mu \in Z} M(\mu, \underline{I})$. We can define multiplication in $M(Z, \underline{I})$ as follows:

$$A(\mu, \underline{a}) \cdot B(\nu, \underline{b}) = D(\mu\nu, \underline{a}\,\underline{b}) = \left(D_{[\underline{a}_m]}\right)$$

where

$$D_{[\underline{a}_m]} = A_{[\underline{a}_m]} \cdot B_{[\underline{a}^2 \underline{a}_m \mu^{-1}]} \; .$$

In light of the consistency rule Prop. 2.1, this is legitimate.

Choose $C(\underline{b}) = \left(C^{\underline{b}}_{\underline{b}\,\underline{a}_m}\right)$ where we fix some choice of

$C^{\underline{b}}_{\underline{b}\,\underline{a}_m} \in \Gamma^{\underline{b}}_{\underline{b}\,\underline{a}_m}$ for all $[\underline{b}]$ and $m = 1, 2, \ldots, h$. I will reserve the letter C to be these fixed representatives throughout this chapter. For convenience, fix $C^{(1)}_{\underline{a}_m} = I$ for all m so that

$$C((1)) = \begin{pmatrix} I \\ I \\ \vdots \\ I \end{pmatrix}$$ will be the multiplicative identity in $M(Z, \underline{I})$.

$M(Z, \underline{I})$ has the following properties.

<u>Proposition 3</u>

1) (Distributive Law). Let $A, B, D \in M(Z, \underline{I})$ and suppose $A + B$ is defined. Then

$$(A + B)D = AD + BD \quad \text{and}$$

$$D(A + B) = DA + DB \text{ .}$$

2) $M(Z, I)$ and M are multiplicative semigroups.

3) $M(\mu, \underline{b}) = C(\underline{b}) \cdot M(\mu, (1)) = M(\mu, (1)) \cdot C(\underline{b})$.

4) $M(\mu, \underline{b}) = M \cdot M(\mu, \underline{b}) = M(\mu, \underline{b}) \cdot M$.

5) $M \cdot C(\underline{b}) = C(\underline{b}) \cdot M$.

6) $C(\underline{a})\, C(\underline{b}) = A\, C(\underline{a}\,\underline{b})$ for some $A \in M$.

<u>Proof.</u> Everything follows from Prop. 2 along with the definition of multiplication. <u>QED</u>

When we define vector modular forms, they will be invariant under M. Hence it is convenient to define equivalence of operators. We say that $B \sim B'$ if there exists $A \in M$ so that $B = AB'$. In particular, B and B' are in the same $M(\mu, \underline{b})$. We extend this to formal sums by defining $B + D \sim B' + D'$ whenever $B \sim B'$ and $D \sim D'$. Notice that if

$B = \left(B_{[\underline{a}_m]}\right)$ and $D = \left(D_{[\underline{a}_m]}\right)$, then $B \sim D$ iff

$B_{[\underline{a}_m]} \sim D_{[\underline{a}_m]}$ for $m = 1, 2, \ldots, h$. Thus there should be no confusion between equivalence of vector operators and equivalence of matrices defined earlier.

Proposition 4

1) $\sim$ is an equivalence relation.

2) For any D, $B \sim B'$ implies $BD \sim B'D$.

3) Suppose that $D \in M(Z, \underline{I})$ satisfies $D \sim DA$ for all $A \in M$. Then $B \sim B'$ implies $DB \sim DB'$.

Conversely, suppose that $B \sim B'$ implies $DB \sim DB'$. Then $D \sim DA$ for all $A \in M$.

Proof. 1) follows since M has multiplicative inverses. 2) and 3) are obvious from the definitions. QED

II. 5 Hecke Operators

Before defining Hecke operators, we will prove a lemma which underlies the definition of Hecke operators, and which is essential to what follows.

<u>Lemma 1</u> (Standard Decomposition)

1) Let $\begin{pmatrix}\pi & \rho \\ \psi & \tau\end{pmatrix} \in \Gamma_{\underline{c}}^{\underline{a}}(\mu)$. Then there exists $A \in \Gamma_{\underline{c}\,\underline{a}^{-1}}$ such that

$$\begin{pmatrix}\pi & \rho \\ \psi & \tau\end{pmatrix} = A \cdot C_{\underline{c}\,\kappa^{-1}}^{\underline{a}\,\kappa^{-1}} \cdot \begin{pmatrix}\kappa & \sigma \\ 0 & \lambda\end{pmatrix}$$

with $\kappa, \sigma, \lambda \in O(Z)$, $\kappa\lambda = \mu$, (κ) unique, σ mod λ unique, and $[\sigma] = [\underline{a}^{-1}\underline{c}^{-1}\kappa^2\lambda]$.

2) If we choose particular κ generating (κ) for all $(\kappa) \mid (\mu)$, and if we choose particular σ mod λ for λ such that $\kappa\lambda = \mu$, then A is unique.

<u>Proof.</u> Let $\kappa = (\pi, \psi)$, so (κ) is unique and we can choose a particular generator κ. Let $\gamma = -\psi/\kappa$ and $\delta = \pi/\kappa$ so that $(\gamma, \delta) = 1$. By Prop. 1.2 we can find $\alpha, \beta \in O(Z)$ such that $\alpha\delta - \beta\gamma = 1$. Thus,

$$\begin{pmatrix}\alpha & \beta \\ \gamma & \delta\end{pmatrix}\begin{pmatrix}\pi & \rho \\ \psi & \tau\end{pmatrix} = \begin{pmatrix}\kappa & \sigma' \\ 0 & \lambda\end{pmatrix}$$

where $\kappa\lambda = \mu$.

Choose $\nu \in O(Z)$ such that $\sigma' + \nu\lambda = \sigma$, where σ is some chosen representative mod λ. Then

$$\begin{pmatrix}1 & \nu \\ 0 & 1\end{pmatrix}\begin{pmatrix}\alpha & \beta \\ \gamma & \delta\end{pmatrix}\begin{pmatrix}\pi & \rho \\ \psi & \tau\end{pmatrix} = \begin{pmatrix}\kappa & \sigma \\ 0 & \lambda\end{pmatrix}$$

so

$$\begin{pmatrix}\pi & \rho \\ \psi & \tau\end{pmatrix} = \begin{pmatrix}\alpha + \nu\gamma & \beta + \nu\delta \\ \gamma & \delta\end{pmatrix}^{-1}\begin{pmatrix}\kappa & \sigma \\ 0 & \lambda\end{pmatrix} .$$

Using Prop. 2.2 we find that

$$\begin{pmatrix}\pi & \rho \\ \psi & \tau\end{pmatrix} = A \cdot C^{\underline{a}\,\kappa^{-1}}_{\underline{c}\,\kappa^{-1}} \cdot \begin{pmatrix}\kappa & \sigma \\ 0 & \lambda\end{pmatrix} \quad \text{for some} \quad A \in \Gamma_{\underline{a}^{-1}\underline{c}} .$$

To show the uniqueness of A, suppose that

$$A_1 \cdot C^{\underline{a}\,\kappa_1^{-1}}_{\underline{c}\,\kappa_1^{-1}} \cdot \begin{pmatrix}\kappa_1 & \sigma_1 \\ 0 & \lambda_1\end{pmatrix} = A_2 \cdot C^{\underline{a}\,\kappa_2^{-1}}_{\underline{c}\,\kappa_2^{-1}} \cdot \begin{pmatrix}\kappa_2 & \sigma_2 \\ 0 & \lambda_2\end{pmatrix} .$$

If we let

$$\begin{pmatrix}\alpha & \beta \\ \gamma & \delta\end{pmatrix} = \left(C^{\underline{a}\,\kappa_2^{-1}}_{\underline{c}\,\kappa_2^{-1}}\right)^{-1} \cdot A_2^{-1} \cdot A_1 \cdot C^{\underline{a}\,\kappa_1^{-1}}_{\underline{c}\,\kappa_1^{-1}}$$

then

$$\begin{pmatrix}\alpha & \beta \\ \gamma & \delta\end{pmatrix}\begin{pmatrix}\kappa_1 & \sigma_1 \\ 0 & \lambda_1\end{pmatrix} = \begin{pmatrix}\kappa_2 & \sigma_2 \\ 0 & \lambda_2\end{pmatrix} .$$

Thus $\gamma\kappa_1 = 0$ so $\gamma = 0$. Then $\alpha\delta = 1$ so $\alpha, \delta \in U$. Now $\alpha\kappa_1 = \kappa_2$ so $(\kappa_1) = (\kappa_2)$. By uniqueness of generator $\kappa_1 = \kappa_2$ which implies that $\alpha = 1$ and $\delta = 1$, as well as showing that

$\lambda_1 = \lambda_2$. One now sees that $\sigma_1 + \beta\lambda_1 = \sigma_2$ so $\sigma_1 \equiv \sigma_2 \bmod \lambda_1$, but by uniqueness of choice of representative, $\sigma_1 = \sigma_2$. One concludes that $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} = I$ and thus $A_1 = A_2$, which verifies statement 2) of the lemma. QED

We are now almost ready to define Hecke operators. Let $\mu \in O(Z)$. Choose $\alpha_1 = 1, \alpha_2, \ldots, \alpha_h$ such that $\alpha_m \in O[\underline{a}_m]$ and $(\alpha_m, \mu) = 1$ for $m = 1, 2, \ldots, h$. This is possible by Prop. 1.1. For each (κ) with $\kappa\lambda = \mu$, choose a particular generator κ. From each $O[\lambda]$, fix a complete set of representatives $\sigma_n \bmod \lambda$, $n = 1, 2, \ldots, N(\lambda)$.

For convenience, define the vector operator $\left(\begin{pmatrix} \kappa & \sigma_n \\ 0 & \lambda \end{pmatrix}\right)$ to be $\left(B_{[\underline{a}_m]}\right)$ where

$$B_{[\underline{a}_m]} = \begin{pmatrix} \kappa & \alpha_m \sigma_n \\ 0 & \lambda \end{pmatrix} \in \Gamma^{\kappa}_{\kappa \underline{a}_m} .$$

Proposition 5

1) $\left(\begin{pmatrix} \kappa & \sigma \\ 0 & \lambda \end{pmatrix}\right) \cdot \left(\begin{pmatrix} \zeta & \omega \\ 0 & \xi \end{pmatrix}\right) \approx \left(\begin{pmatrix} \kappa\zeta & \kappa\omega + \xi\sigma \\ 0 & \lambda\xi \end{pmatrix}\right)$.

2) $\left(\begin{pmatrix} \kappa & \sigma \\ 0 & \lambda \end{pmatrix}\right) \sim \left(\begin{pmatrix} \kappa & \sigma' \\ 0 & \lambda \end{pmatrix}\right)$ whenever $\sigma \equiv \sigma' \bmod \lambda$.

3) Given $B \in M(Z, \underline{I})$, $\lambda \in O(Z)$, we have

$$\left(\begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix}\right) \cdot B = B \cdot \left(\begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix}\right) .$$

Proof. 1) One needs to observe that the consistency rule Prop. 2.1 is not violated; otherwise the proof is straightforward.

2) follows from 1), and 3) is elementary. QED

We can now define the unnormalized Hecke operators $t(\mu)$. In the next chapter, we will renormalize $t(\mu)$ but for this chapter it is convenient to ignore the normalizing constants.

Definition. The unnormalized Hecke operator $t(\mu)$ for $\mu \in O(Z)$ is given by

$$t(\mu) = \left(t_{[\underline{a}_m]}(\mu)\right) = \left(\sum_{\substack{(\kappa) \\ \kappa\lambda = \mu}} C^{\kappa^{-1}}_{\kappa^{-1}\underline{a}_m} \sum_{n=1}^{N(\lambda)} \begin{pmatrix} \kappa & \alpha_p \sigma_n \\ 0 & \lambda \end{pmatrix} \right)$$

$$= \sum_{\substack{(\kappa) \\ \kappa\lambda = \mu}} C(\kappa^{-1}) \cdot \sum_{n=1}^{N(\lambda)} \left(\begin{pmatrix} \kappa & \sigma_n \\ 0 & \lambda \end{pmatrix}\right)$$

where $\sigma_n \bmod \lambda$ is a fixed complete set of representatives and where $[\alpha_p] = [\underline{a}_m^{-1} \kappa^2]$.

Remark. Notice that $t(\mu) \in M(\mu, (1))$. We could also define a more general Hecke operator $t(\mu, \underline{b}) = C(\underline{b})\, t(\mu) \in M(\mu, \underline{b})$, but we will not need this generalization.

The following lemma shows that up to equivalence, $t(\mu)$ does not depend on the particular choices above.

Lemma 2

1) Replace $C^{\underline{b}}_{\underline{b}\,\underline{a}_m} \in \Gamma^{\underline{b}}_{\underline{b}\,\underline{a}_m}$ by $C'^{\underline{b}}_{\underline{b}\,\underline{a}_m} \in \Gamma^{\underline{b}}_{\underline{b}\,\underline{a}_m}$ for all $[\underline{b}]$ and $m = 1, 2, \ldots, h$. Call the new Hecke operator $t'(\mu)$. Then $C(\underline{b}) \sim C'(\underline{b})$ and $t(\mu) \sim t'(\mu)$.

2) Replace $\sigma_n \bmod \lambda$ by $\sigma_n' \bmod \lambda$, with σ_n' in $O[\lambda]$ also a complete set of residues. Call the new Hecke operator $t'(\mu)$. Then

$$\sum_{n=1}^{N(\lambda)} \left(\!\!\begin{pmatrix} \kappa & \sigma_n \\ 0 & \lambda \end{pmatrix}\!\!\right) \sim \sum_{n=1}^{N(\lambda)} \left(\!\!\begin{pmatrix} \kappa & \sigma_n' \\ 0 & \lambda \end{pmatrix}\!\!\right)$$

and $t(\mu) \sim t'(\mu)$.

3) Replace α_m by β_m with $\beta_m \in O[\underline{a}_m]$ and $(\beta_m, \mu) = 1$, $m = 1, 2, \ldots, h$. Call the new Hecke operator $t'(\mu)$. Then

$$\sum_{n=1}^{N(\lambda)} \begin{pmatrix} \kappa & \alpha_m \sigma_n \\ 0 & \lambda \end{pmatrix} \sim \sum_{n=1}^{N(\lambda)} \begin{pmatrix} \kappa & \beta_m \sigma_n \\ 0 & \lambda \end{pmatrix}$$

for $m = 1, 2, \ldots h$. Also, $t(\mu) \sim t'(\mu)$.

4) Replace κ by κ' where $(\kappa) = (\kappa')$ and $\kappa\lambda = \mu$ and $\kappa'\lambda' = \mu$. Let $\sigma_n \bmod \lambda$ and $\sigma_n' \bmod \lambda'$ be complete sets of representatives. Call the new Hecke operator (defined in terms of $\kappa', \lambda', \sigma_n'$) $t'(\mu)$. Then

$$\sum_{n=1}^{N(\lambda)} \left(\begin{pmatrix} \kappa & \sigma_n \\ 0 & \lambda \end{pmatrix} \right) \sim \sum_{n=1}^{N(\lambda)} \left(\begin{pmatrix} \kappa' & \sigma'_n \\ 0 & \lambda' \end{pmatrix} \right)$$

and $t(\mu) \sim t'(\mu)$.

Proof. 1) Prop. 2 shows that $C'^{\underline{b}}_{\underline{b}\,\underline{a}_m} = A_{[\underline{a}_m]} C^{\underline{b}}_{\underline{b}\,\underline{a}_m}$ for some $A_{[\underline{a}_m]} \in \Gamma_{\underline{a}_m}$. Thus $C(\underline{b}) \sim C'(\underline{b})$. Using Prop. 4.2, $t(\mu) \sim t'(\mu)$.

2) For each $n = 1, 2, \ldots, N(\lambda)$, there is a unique $p(n)$ such that $\sigma_n \equiv \sigma'_{p(n)} \bmod \lambda$. Using Prop. 5.1 and reordering the sum, we get the first equivalence. Then Prop. 4.3 with Prop. 3.5 shows that $t(\mu) \sim t'(\mu)$.

3) Fix any $m = 1, 2, \ldots, h$. By Lemma 2, there exists $A \in \Gamma_{\underline{a}_m}$ such that

$$A \cdot \begin{pmatrix} \kappa & \alpha_m \sigma_n \\ 0 & \lambda \end{pmatrix} = \begin{pmatrix} \kappa' & \beta_m \sigma'_{p(n)} \\ 0 & \lambda' \end{pmatrix}$$

Uniqueness of the decomposition implies that

$$\kappa = \kappa', \quad \lambda = \lambda', \quad \text{and} \quad \{\sigma_n\}_{n=1,2,\ldots,N(\lambda)} = \{\sigma_{p(n)}\}_{n=1,2,\ldots,N(\lambda)} .$$

We also find that $\alpha_m \sigma_n \equiv \beta_m \sigma_{p(n)} \bmod \lambda$, hence we can apply 2) above.

4) By hypothesis, $\kappa = \eta\kappa'$ for some $\eta \in U$, so $\lambda = \eta^{-1} \lambda'$. Using Prop. 5.1,

$$\left(\begin{pmatrix} \kappa & \sigma_n \\ 0 & \lambda \end{pmatrix}\right) = \left(\begin{pmatrix} \eta & 0 \\ 0 & \eta^{-1} \end{pmatrix}\right)\left(\begin{pmatrix} \kappa' & \eta^{-1}\sigma_n \\ 0 & \lambda' \end{pmatrix}\right) \sim \left(\begin{pmatrix} \kappa' & \eta^{-1}\sigma_n \\ 0 & \lambda' \end{pmatrix}\right)$$

Now $(\eta, \lambda) = 1$ for any $\eta \in U$, so Prop. 1.4 says that $\eta^{-1}\sigma_n$ is a complete set of representatives mod λ'. Applying 3) above, we are done. QED

Theorem 1 (Invariance of the Hecke operator).

$$B \cdot t(\mu) \sim t(\mu) \cdot B \quad \text{for any } B \in M(1, \underline{I}) .$$

Proof. Recall that $t(\mu) = \left(t_{[\underline{a}_m]}(\mu)\right)$ where

$$t_{[\underline{a}_m]}(\mu) = \sum_{\substack{(\kappa) \\ \kappa\lambda = \mu}} C^{\kappa^{-1}}_{\kappa^{-1}\underline{a}_m} \sum_{n=1}^{N(\lambda)} \begin{pmatrix} \kappa & \alpha_p \sigma_n \\ 0 & \lambda \end{pmatrix}$$

where $[\alpha_p] = [\kappa^2 \underline{a}_m^{-1}]$. Let $D \in \Gamma^{\underline{b}}_{\underline{b}\,\underline{a}_m \mu^{-1}}$. We want to show that multiplying $t_{[\underline{a}_m]}(\mu)$ on the right by D will effectively permute the matrices $\begin{pmatrix} \kappa & \alpha_p \sigma_n \\ 0 & \lambda \end{pmatrix}$.

$$\text{Set } \begin{pmatrix} \pi & \rho \\ \psi & \tau \end{pmatrix} = C^{\kappa^{-1}}_{\kappa^{-1}\underline{a}_m} \begin{pmatrix} \kappa & \alpha_p \sigma_n \\ 0 & \lambda \end{pmatrix} \cdot D \quad \text{so } \begin{pmatrix} \pi & \rho \\ \psi & \tau \end{pmatrix} \in \Gamma^{\underline{b}}_{\underline{b}\,\underline{a}_m}(\mu).$$

By Lemma 1 there exists a unique $A \in \Gamma_{\underline{a}_m}$ such that

$$\begin{pmatrix} \pi & \rho \\ \psi & \tau \end{pmatrix} = A \cdot C^{\underline{b}\,\kappa'^{-1}}_{\underline{b}\,\underline{a}_m \kappa'^{-1}} \cdot \begin{pmatrix} \kappa' & \alpha_r \sigma'_s \\ 0 & \lambda' \end{pmatrix}$$

where we fix representatives σ'_s mod λ' and where $[\alpha_r] = [\underline{b}^{-1} \underline{a}_m^{-1} \kappa'^2]$. I claim that each term $\begin{pmatrix} \kappa & \alpha_p \sigma_n \\ 0 & \lambda \end{pmatrix}$ of $t_{[\underline{a}_m]}$ gives rise to a distinct term $\begin{pmatrix} \kappa' & \alpha_r \sigma'_s \\ 0 & \lambda' \end{pmatrix}$. If this is true, then Prop. 2.4 shows that

$$t_{[\underline{a}_m]}(\mu) \cdot D \sim C^{\underline{b}}_{\underline{b}\,\underline{a}_m} \sum_{\substack{(\kappa') \\ \kappa'\lambda' = \mu}} C^{\kappa'^{-1}}_{\kappa'^{-1} \underline{a}_m} \cdot \sum_{s=1}^{N(\lambda')} \begin{pmatrix} \kappa' & \alpha_r \sigma'_s \\ 0 & \lambda' \end{pmatrix}$$

and using Prop. 2.2 we may conclude that

$$t_{[\underline{a}_m]}(\mu) \cdot D \sim D' \cdot t_{[\underline{a}_m]}(\mu) \quad \text{for any } D' \in \Gamma^{\underline{b}}_{\underline{b}\,\underline{a}_m} .$$

This means that if $B = \left(B_{[\underline{a}_m]}\right)$ and if we let $D = B_{[\underline{a}_m \mu^{-1}]}$, $D' = B_{[\underline{a}_m]}$, then

$$t(\mu) \cdot B \sim B \cdot t(\mu) .$$

We need to show that the matrices $\begin{pmatrix} \kappa' & \alpha_r \sigma'_s \\ 0 & \lambda' \end{pmatrix}$ are distinct. Suppose we have

$$C_{\kappa_1^{-1}\underline{a}_m}^{\kappa_1^{-1}} \cdot \begin{pmatrix} \kappa_1 & \alpha_p \sigma_1 \\ 0 & \lambda_1 \end{pmatrix} \cdot D = A_1 \cdot C_{\underline{b}\underline{a}_m \kappa^{-1}}^{\underline{b}\kappa^{-1}} \cdot \begin{pmatrix} \kappa & \alpha_r \sigma_s \\ 0 & \lambda \end{pmatrix}$$

and also

$$C_{\kappa_2^{-1}\underline{a}_m}^{\kappa_2^{-1}} \cdot \begin{pmatrix} \kappa_2 & \alpha_q \sigma_2 \\ 0 & \lambda_2 \end{pmatrix} \cdot D = A_2 \cdot C_{\underline{b}\underline{a}_m \kappa^{-1}}^{\underline{b}\kappa^{-1}} \cdot \begin{pmatrix} \kappa & \alpha_r \sigma_s \\ 0 & \lambda \end{pmatrix} .$$

We wish to show that $\kappa_1 = \kappa_2$, $\lambda_1 = \lambda_2$, and $\alpha_p \sigma_1 = \alpha_q \sigma_2$. Simple matrix manipulation shows that

$$\begin{pmatrix} \kappa_1 & \alpha_p \sigma_1 \\ 0 & \lambda_1 \end{pmatrix} = \left(C_{\kappa_1^{-1}\underline{a}_m}^{\kappa_1^{-1}} \right)^{-1} \cdot A_1 \cdot A_2^{-1} \cdot C_{\kappa_2^{-1}\underline{a}_m}^{\kappa_2^{-1}} \begin{pmatrix} \kappa_2 & \alpha_q \sigma_2 \\ 0 & \lambda_2 \end{pmatrix} .$$

Using Prop. 2.4, 2.5, and 2.6, there exists $A_3 \in \Gamma_{\underline{a}_m \kappa_1^{-1}}$ such that

$$\begin{pmatrix} \kappa_1 & \alpha_p \sigma_1 \\ 0 & \lambda_1 \end{pmatrix} = A_3 \cdot C_{\kappa_1^{-1}\kappa_2^{-1}\underline{a}_m}^{\kappa_1 \kappa_2^{-1}} \cdot \begin{pmatrix} \kappa_2 & \alpha_q \sigma_2 \\ 0 & \lambda_2 \end{pmatrix} .$$

Both sides are in the standard form of Lemma 1, so by the uniqueness statements of Lemma 1,

$$\begin{pmatrix} \kappa_1 & \alpha_p \sigma_1 \\ 0 & \lambda_1 \end{pmatrix} = \begin{pmatrix} \kappa_2 & \alpha_q \sigma_2 \\ 0 & \lambda_2 \end{pmatrix} .$$

QED

We are now ready for the key theorem of this chapter.

Theorem 2 (Multiplicative relations of Hecke operators).

$$t(\mu)\, t(\nu) = \sum_{\substack{(\theta) \\ \theta \mid (\mu,\, \nu)}} N(\theta)\, C(\theta^{-1}) \left(\begin{pmatrix} \theta & 0 \\ 0 & \theta \end{pmatrix}\right) t\left(\frac{\mu\nu}{\theta^2}\right) .$$

Proof. First we will show that this relation holds for all $(\mu, \nu) = 1$, then for prime powers, and finally for arbitrary μ and ν in $O(Z)$.

Suppose $(\mu, \nu) = 1$. We wish to show that $t(\mu)\, t(\nu) = t(\mu\nu)$.

Let

$$t(\mu) = \sum_{\substack{(\kappa) \\ \kappa\lambda = \mu}} C(\kappa^{-1}) \sum_{n=1}^{N(\lambda)} \left(\begin{pmatrix} \kappa & \sigma_n \\ 0 & \lambda \end{pmatrix}\right)$$

and

$$t(\nu) = \sum_{\substack{(\zeta) \\ \zeta\xi = \nu}} C(\zeta^{-1}) \sum_{r=1}^{N(\xi)} \left(\begin{pmatrix} \zeta & \omega_r \\ 0 & \xi \end{pmatrix}\right) .$$

Then

$$t(\mu)\, t(\nu) = t(\mu) \sum_{(\zeta)} C(\zeta^{-1}) \sum_{r=1}^{N(\xi)} \left(\begin{pmatrix} \zeta & \omega_r \\ 0 & \xi \end{pmatrix}\right)$$

$$\sim \sum C(\zeta^{-1})\, t(\mu) \sum \left(\begin{pmatrix} \zeta & \omega_r \\ 0 & \xi \end{pmatrix}\right)$$

using Theorem 1. Note that I have also used Prop. 4.2. I will be using Prop. 4.2 and 4.3 continually throughout this proof, and will generally not mention their use.

$$t(\mu)\,t(\nu) \sim \sum_{\substack{(\kappa) \\ \kappa\lambda=\mu}} \sum_{\substack{(\zeta) \\ \zeta\xi=\nu}} C(\kappa^{-1}) \cdot C(\zeta^{-1}) \cdot \sum_{n=1}^{N(\lambda)} \sum_{r=1}^{N(\xi)} \left(\!\!\begin{pmatrix} \kappa & \sigma_n \\ 0 & \lambda \end{pmatrix}\!\!\right)\left(\!\!\begin{pmatrix} \zeta & \omega_r \\ 0 & \xi \end{pmatrix}\!\!\right).$$

Using Prop. 3.6 and Prop. 5.1 we find that

$$t(\mu)\,t(\nu) \sim \sum_{(\kappa)} \sum_{(\zeta)} C((\kappa\zeta)^{-1}) \sum_n \sum_r \left(\!\!\begin{pmatrix} \kappa\zeta & \kappa\omega_r + \sigma_n\xi \\ 0 & \lambda\xi \end{pmatrix}\!\!\right)$$

I claim that $\kappa\omega_r + \sigma_n\xi$ is a complete set of representatives mod $(\lambda\xi)$ if σ_n mod λ and ω_r mod ξ are complete. Further, note that $[\kappa\omega_r + \sigma_n\xi] = [\lambda\xi]$. Assuming that my claim is true, Lemma 2 shows that the right side is $t(\mu\nu)$ and we are done.

Suppose σ_n mod λ and ω_r mod ξ are complete sets of representatives, with $[\sigma_n] = [\lambda]$ and $[\omega_r] = [\xi]$. There are $N(\lambda\xi)$ representatives mod $\lambda\xi$ and I want to show that if $\kappa\omega_r + \sigma_n\xi \equiv \kappa\omega_s + \sigma_p\xi$ mod $\lambda\xi$ then $\omega_r = \omega_s$ and $\sigma_n = \sigma_p$.

Clearly $\kappa\omega_r \equiv \kappa\omega_s$ mod ξ. By hypothesis, $(\mu, \nu) = 1$ so $(\kappa, \xi) = 1$. Using Prop. 1.5, $\omega_r \equiv \omega_s$ mod ξ hence $\omega_r = \omega_s$. Then $\sigma_n\xi \equiv \sigma_p\xi$ mod $\lambda\xi$ so $\sigma_n \equiv \sigma_p$ mod λ which says that $\sigma_n = \sigma_p$.

Thus we have finished showing that $t(\mu)t(\nu) \sim t(\mu\nu)$ whenever $(\mu, \nu) = 1$. Now we wish tc show that for π prime, $t(\pi)\,t(\pi^r)$ $\sim t(\pi^{r+1}) + N(\pi)\,C(\pi^{-1})\left(\!\begin{pmatrix}\pi & 0\\ 0 & \pi\end{pmatrix}\!\right) t(\pi^{r-1})$ for any r a positive integer.

Let

$$t(\pi) = C(\pi^{-1})\left(\!\begin{pmatrix}\pi & 0\\ 0 & 1\end{pmatrix}\!\right) + \sum_{n=1}^{N(\pi)} \left(\!\begin{pmatrix}1 & \sigma_n\\ 0 & \pi\end{pmatrix}\!\right)$$

and

$$t(\pi^r) = \sum_{s=0}^{r} C(\pi^{-s}) \sum_{u=1}^{N(\pi^{r-s})} \left(\!\begin{pmatrix}\pi^s & \omega_u\\ 0 & \pi^{r-s}\end{pmatrix}\!\right)$$

By Theorem 1,

$$t(\pi)\,t(\pi^r) \sim \sum_{s=0}^{r} C(\pi^{-s})\,t(\pi) \sum_{u=1}^{N(\pi^{r-s})} \left(\!\begin{pmatrix}\pi^s & \omega_u\\ 0 & \pi^{r-s}\end{pmatrix}\!\right)$$

$$= \sum_{s=0}^{r} C(\pi^{-s})\,C(\pi^{-1}) \sum_{u=1}^{N(\pi^{r-s})} \left(\!\begin{pmatrix}\pi & 0\\ 0 & 1\end{pmatrix}\!\right)\left(\!\begin{pmatrix}\pi^s & \omega_u\\ 0 & \pi^{r-s}\end{pmatrix}\!\right)$$

$$+ \sum_{s=0}^{r} C(\pi^{-s}) \sum_{n=1}^{N(\pi)} \sum_{u=1}^{N(\pi^{r-s})} \left(\!\begin{pmatrix}1 & \sigma_n\\ 0 & \pi\end{pmatrix}\!\right)\left(\!\begin{pmatrix}\pi^s & \omega_u\\ 0 & \pi^{r-s}\end{pmatrix}\!\right)$$

$$\sim \sum_{s=0}^{r-1} C(\pi^{-s})\, C(\pi^{-1}) \sum_{u=1}^{N(\pi^{r-s})} \left(\begin{pmatrix} \pi^{s+1} & \pi\omega_u \\ 0 & \pi^{r-s} \end{pmatrix}\right)$$

$$+\ C(\pi^{r+1}) \left(\begin{pmatrix} \pi^{r+1} & 0 \\ 0 & 1 \end{pmatrix}\right)$$

$$+ \sum_{s=0}^{r} C(\pi^{-s}) \sum_{n=1}^{N(\pi)} \sum_{u=1}^{N(\pi^{r-s})} \left(\begin{pmatrix} \pi^{s} & \omega_u + \sigma_n \pi^{r-s} \\ 0 & \pi^{r-s+1} \end{pmatrix}\right)$$

Just as above, we find that there are $N(\pi^{r-s+1})$ distinct $\omega_u + \sigma_n \pi^{r-s} \bmod \pi^{r-s+1}$. Thus Lemma 2.2 allows us to combine the last two expressions, and we conclude that

$$t(\pi)\, t(\pi^r) \sim \sum_{s=0}^{r-1} C(\pi^{-s})\, C(\pi^{-1}) \sum_{u=1}^{N(\pi^{r-s})} \left(\begin{pmatrix} \pi^{s+1} & \pi\omega_u \\ 0 & \pi^{r-s} \end{pmatrix}\right) + t(\pi^{r+1}).$$

Decompose $\omega_u = \tau_v + \sigma_n \pi^{r-s-1}$ where $\tau_v \bmod \pi^{r-s-1}$ and $\sigma_n \bmod \pi$ are unique. Since $N(\pi^{r-s}) = N(\pi^{r-s-1})\, N(\pi)$, we see that $\tau_v \bmod \pi^{r-s-1}$ and $\sigma_n \bmod \pi$ are complete sets of representatives. Thus

$$t(\pi)\, t(\pi^r) \sim t(\pi^{r+1}) + \sum_{s=1}^{r-1} C(\pi^{-s})\, C(\pi^{-1}) \left(\begin{pmatrix} \pi & 0 \\ 0 & \pi \end{pmatrix}\right).$$

$$\cdot \sum_{n=1}^{N(\pi)} \sum_{v=1}^{N(\pi^{r-s-1})} \left(\begin{pmatrix} \pi^s & \tau_v + \sigma_n \pi^{r-s-1} \\ 0 & \pi^{r-s-1} \end{pmatrix}\right)$$

Using Prop. 5.3 and 3.6, we can interchange terms and apply Lemma 2.2 to get

$$t(\pi)\, t(\pi^r) \sim t(\pi^{r+1}) +$$

$$+ \sum_{n=1}^{N(\pi)} C(\pi^{-1}) \left(\begin{pmatrix} \pi & 0 \\ 0 & \pi \end{pmatrix}\right) \sum_{s=0}^{r-1} C(\pi^{-s}) \sum_{v=1}^{N(\pi^{r-s-1})} \left(\begin{pmatrix} \pi^s & \tau_v \\ 0 & \pi^{r-s-1} \end{pmatrix}\right)$$

$$\sim t(\pi^{r+1}) + N(\pi)\, C(\pi^{-1}) \left(\begin{pmatrix} \pi & 0 \\ 0 & \pi \end{pmatrix}\right) t(\pi^{r-1}) \quad .$$

Now we will use induction to show that

$$t(\pi^q)\, t(\pi^r) \sim \sum_{s=0}^{\min(q,r)} N(\pi^s)\, C(\pi^{-s}) \left(\begin{pmatrix} \pi^s & 0 \\ 0 & \pi^s \end{pmatrix}\right) t(\pi^{q+r-2s}) \quad .$$

Assume this is true for $q-1$ and all r, with $q \geq 2$. We have just shown that it is true for $q=1$.

$$t(\pi^q)\, t(\pi^r) \sim \left[t(\pi)\, t(\pi^{q-1}) - N(\pi)\, C(\pi^{-1}) \left(\begin{pmatrix} \pi & 0 \\ 0 & \pi \end{pmatrix}\right) \cdot t(\pi^{q-2}) \right] \cdot t(\pi^r)$$

by the above. Applying the inductive hypothesis,

$$t(\pi^q)\, t(\pi^r) \sim t(\pi) \cdot \sum_{s=0}^{\min(q-1,r)}$$

$$\cdot\ N(\pi^s)\, C(\pi^{-s}) \left(\begin{pmatrix} \pi^s & 0 \\ 0 & \pi^s \end{pmatrix}\right) t(\pi^{q+r-1-2s})$$

$$-\ N(\pi)\, C(\pi^{-1}) \left(\begin{pmatrix} \pi & 0 \\ 0 & \pi \end{pmatrix}\right) \sum_{s=0}^{\min(q-2,r)} N(\pi^s)\, C(\pi^{-s}) \left(\begin{pmatrix} \pi^s & 0 \\ 0 & \pi^s \end{pmatrix}\right) \cdot$$

$$\cdot\ t(\pi^{q+r-2-2s})$$

$$\sim \sum_{s=0}^{\min(q-1,r)} N(\pi^s)\, C(\pi^{-s}) \left(\begin{pmatrix} \pi^s & 0 \\ 0 & \pi^s \end{pmatrix}\right) \Big[t(\pi^{q+r-2s})$$

$$+\ N(\pi)\, C(\pi^{-1}) \left(\begin{pmatrix} \pi & 0 \\ 0 & \pi \end{pmatrix}\right) t(\pi^{q+r-2-2s}) \Big]$$

$$-\sum_{s=0}^{\min(q-2,r)} N(\pi^{s+1})\, C(\pi^{-s-1}) \left(\begin{pmatrix} \pi^{s+1} & 0 \\ 0 & \pi^{s+1} \end{pmatrix}\right) \cdot t(\pi^{q+r-2-2s})$$

where I have used Prop. 5.3 and Prop. 4 and Prop. 3.6 several times.

Finally, define $f(q, r) = 1$ if $r \geq q - 1$ and $f(q, r) = 0$ if $r < q - 1$. Then the above becomes

$$t(\pi^{q})\,t(\pi^{r}) \sim \sum_{s=0}^{\min(q-1,\,r)} N(\pi^{s})\,C(\pi^{-s})\left(\!\!\begin{pmatrix}\pi^{s} & 0\\ 0 & \pi^{s}\end{pmatrix}\!\!\right) t(\pi^{q+r-2s})$$

$$+\, f(q,r)\; N(\pi^{q})\,C(\pi^{-q})\left(\!\!\begin{pmatrix}\pi^{q} & 0\\ 0 & \pi^{q}\end{pmatrix}\!\!\right) t(\pi^{r-q}) \;.$$

This implies that

$$t(\pi^{q})\,t(\pi^{r}) \sim \sum_{s=0}^{\min(q,\,r)} N(\pi^{s})\,C(\pi^{-s})\left(\!\!\begin{pmatrix}\pi^{s} & 0\\ 0 & \pi^{s}\end{pmatrix}\!\!\right) t(\pi^{q+r-2s})$$

which is the desired result.

We still need to consider the general case of μ and ν with $(\mu, \nu) > 1$. First we notice that the expressions we have already shown imply commutativity. By Prop. 1.6 we can factor μ and ν into prime factors, where we can fix a particular generator π for any prime ideal (π) dividing (μ) and (ν). We have just finished showing that the result is true for each prime factor, and then we can use our statement about relatively prime $t(\mu)$ and $t(\nu)$ to conclude the proof. QED

II. 6 Example: Hecke Operators for $K = \mathbb{Q}(\sqrt{-23})$

First we will define a set of ideal numbers. It is well known that $\mathbb{Q}(\sqrt{-23})$ has class number 3 and that either prime ideal dividing (2) generates the ideal class group. We can easily calculate a set of ideal numbers Z corresponding to $\mathbb{Q}(\sqrt{-23})$.

Let $\underline{p}_2 = \left(\frac{1 - \sqrt{-23}}{2}, 2\right)$ and $\underline{p}_2 = \left(\frac{1 + \sqrt{-23}}{2}, 2\right)$. We will choose $\underline{p}_2$ as the generator of the ideal class group. Now $\underline{p}_2^3 = \left(\frac{3 + \sqrt{-23}}{2}\right)$ so we choose some branch of the cube root and define an ideal number $\pi_2 = \sqrt[3]{\frac{3 + \sqrt{-23}}{2}}$ which corresponds to the ideal $\underline{p}_2$. Because the choice of generator of $\left(\frac{3 + \sqrt{-23}}{2}\right)$ has an ambiguity of sign, and because the choice of cube root is arbitrary, π_2 contains an arbitrary sixth root of unity. We fix this choice, however, so the rest of the ideal numbers are determined.

For any ideal $\underline{a}$, if $\underline{a} = (a)$ is principal, then the corresponding ideal numbers are $\pm a$. If $\underline{p}_2\underline{a} = (a)$ is principal, then the ideal numbers corresponding to $\underline{a}$ are $\pm a/\pi_2$. If $\underline{p}_2^2\underline{a} = (a)$ is principal, then the ideal numbers corresponding to $\underline{a}$ are $\pm a/\pi_2^2 = \pm a \cdot \pi_2 \Big/ \left(\frac{3 + \sqrt{-23}}{2}\right)$.

For convenience, let $b = \sqrt{-23}$. One can verify the following facts.

$$\left(\frac{1 + b}{2}\right) = \overline{\underline{p}}_2\underline{p}_3 \qquad \left(\frac{1 - b}{2}\right) = \underline{p}_2\overline{\underline{p}}_3$$

$$\left(\frac{9 + b}{2}\right) = \overline{\underline{p}}_2\underline{p}_{13} \qquad \left(\frac{9 - b}{2}\right) = \underline{p}_2\overline{\underline{p}}_{13}$$

$$\left(\frac{5-3b}{2}\right) = \underline{\overline{p}}_2\underline{p}_{29} \qquad \left(\frac{5+3b}{2}\right) = \underline{p}_2\underline{\overline{p}}_{29}$$

$$\left(\frac{15-b}{2}\right) = \underline{\overline{p}}_2\underline{p}_{31} \qquad \left(\frac{15+b}{2}\right) = \underline{p}_2\underline{\overline{p}}_{31}$$

$$\left(\frac{11+3b}{2}\right) = \underline{\overline{p}}_2\underline{p}_{41} \qquad \left(\frac{11-3b}{2}\right) = \underline{p}_2\underline{\overline{p}}_{41}$$

where $\underline{p}_q$ are defined consistent with the following table:

q	$\sqrt{-23} \bmod \underline{p}_q$	$\sqrt{-23} \bmod \underline{\overline{p}}_q$
3	-1	1
13	4	9
29	21	8
31	15	16
41	10	31

Now we can define corresponding ideal numbers. Define the following:

$$\pi_2 = \sqrt[3]{\frac{3+b}{2}} \qquad \overline{\pi}_2 = \frac{2}{\pi_2}$$

$$\pi_3 = \frac{1+b}{4} \cdot \pi_2 \qquad \overline{\pi}_3 = \frac{1-b}{2\pi_2}$$

$$\pi_{13} = \frac{9+b}{4} \cdot \pi_2 \qquad \overline{\pi}_{13} = \frac{9-b}{2\pi_2}$$

$$\pi_{29} = \frac{5 - 3b}{4} \cdot \pi_2 \qquad \bar{\pi}_{29} = \frac{5 + 3b}{2\pi_2}$$

$$\pi_{31} = \frac{15 - b}{4} \cdot \pi_2 \qquad \bar{\pi}_{31} = \frac{15 + b}{2\pi_2}$$

$$\pi_{41} = \frac{11 + 3b}{4} \cdot \pi_2 \qquad \bar{\pi}_{41} = \frac{11 - 3b}{2\pi_2}$$

Here π_q corresponds to $\underline{p}_q$ and $\bar{\pi}_q$ corresponds to $\bar{\underline{p}}_q$.

We can now calculate some multiplicative relations we will use later.

$$\pi_q \cdot \bar{\pi}_q = q \quad \text{for} \quad q = 2, 3, 13, 29, 31, 41.$$

$$\pi_2^3 = \frac{3 + b}{2} \qquad \bar{\pi}_2^3 = \frac{3 - b}{2}$$

$$\pi_2 \pi_3^2 = -\frac{7 + b}{2} \qquad \bar{\pi}_2 \pi_3 = \frac{1 + b}{2}$$

$$\pi_3^3 = 2 - b \qquad \bar{\pi}_3^3 = 2 + b$$

$$\bar{\pi}_2^2 \pi_3^2 = \frac{-11 + b}{2} \qquad \pi_{13}^3 = 37 + 6b$$

$$\bar{\pi}_2 \pi_{13} = \frac{9 + b}{2} \qquad \pi_3 \pi_{13}^2 = -22 - b$$

$$\pi_2 \cdot \pi_3 \pi_{13} = \frac{-17 + d}{2}$$

For convenience, let $O_0 = O[(1)]$, $O_1 = O[\pi_2]$, and $O_2 = O[\pi_2^2]$.

As a typical example, we will find the Hecke operator $t(\pi_{13})$. To do this, we need to fix representatives mod π_{13} and also fix our "standard matrices" $C(\underset{\sim}{a})$. For convenience we will denote $\Gamma_{\pi_2^b}^{\pi_2^a}$ by Γ_b^a and $C_{\pi_2^b}^{\pi_2^a}$ by C_b^a, where a and b may be considered mod 3, since the class number is 3. We will also denote $t_{[\pi_2^a]}(\pi_{13})$ by $t_a(\pi_{13})$ so that

$$t(\pi_{13}) = \begin{pmatrix} t_0(\pi_{13}) \\ t_1(\pi_{13}) \\ t_2(\pi_{13}) \end{pmatrix} .$$

As a choice of representatives mod π_{13} in O_0, take $0, 1, 2, \ldots, 12$. In O_1, take representatives $0, \pi_2, 2\pi_2, \ldots, 12\pi_2$, and in O_2 take $0, \pi_2^2, 2\pi_2^2, \ldots, 12\pi_2^2$.

For the C_b^a, we can consider "variations" of the matrices $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ and $\begin{pmatrix} \pi_3 & \bar{\pi}_2 \\ \pi_2 & \bar{\pi}_3 \end{pmatrix}$. In particular, let $C_m^o = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ for $m = 0, 1, 2$, $C_0^m = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ for $m = 1, 2$,

$$C_1^1 = \begin{pmatrix} \pi_3 & \bar{\pi}_2 \\ \pi_2 & \bar{\pi}_3 \end{pmatrix}, \quad C_2^1 = \begin{pmatrix} \pi_3 & \pi_2 \\ \bar{\pi}_2 & \bar{\pi}_3 \end{pmatrix},$$

$$C_1^2 = \begin{pmatrix} \overline{\pi}_3 & \overline{\pi}_2 \\ \pi_2 & \pi_3 \end{pmatrix}, \quad \text{and} \quad C_2^2 = \begin{pmatrix} \overline{\pi}_3 & \pi_2 \\ \overline{\pi}_2 & \pi_3 \end{pmatrix}.$$

Now we can define $t(\pi_{13})$ by letting

$$t_0(\pi_{13}) = \begin{pmatrix} \overline{\pi}_3\pi_{13} & \pi_2 \\ \overline{\pi}_2\pi_{13} & \pi_3 \end{pmatrix} + \sum_{q=0}^{12} \begin{pmatrix} 1 & q\pi_2 \\ 0 & \pi_{13} \end{pmatrix}$$

and $$t_1(\pi_{13}) = \begin{pmatrix} 0 & -1 \\ \pi_{13} & 0 \end{pmatrix} + \sum_{s=0}^{12} \begin{pmatrix} 1 & s \\ 0 & \pi_{13} \end{pmatrix}$$

and $$t_2(\pi_{13}) = \begin{pmatrix} \overline{\pi}_3\pi_{13} & \overline{\pi}_2 \\ \pi_2\pi_{13} & \pi_3 \end{pmatrix} + \sum_{r=0}^{12} \begin{pmatrix} 1 & r\pi_2^2 \\ 0 & \pi_{13} \end{pmatrix}.$$

Consider the principal class component of $t(\pi_{13})^3$. This component is simply $t_0(\pi_{13}) \cdot t_2(\pi_{13})\, t_1(\pi_{13})$. Multiplying out the matrices directly yields the following expression:

$$\begin{pmatrix} \overline{\pi}_2\overline{\pi}_3\pi_{13}^2 + \pi_2\pi_3\pi_{13} & -(\overline{\pi}_3\pi_{13}^2 + \pi_2^2\pi_{13}) \\ \overline{\pi}_2^2\pi_{13}^2 + \pi_3^2\pi_{13} & -\overline{\pi}_2\overline{\pi}_3\pi_{13}^2 \end{pmatrix}$$

$$+ \sum_{q=0}^{12} \begin{pmatrix} \overline{\pi}_2\pi_{13} + q\pi_2\pi_3\pi_{13} & -(\overline{\pi}_3\pi_{13} + q\pi_2^2\pi_{13}) \\ \pi_3\pi_{13}^2 & -\pi_2\pi_{13}^2 \end{pmatrix}$$

$$+\sum_{r=0}^{12}\begin{pmatrix}\pi_2\pi_{13}^2+r\pi_2^2\bar{\pi}_3\pi_{13}^2 & -\bar{\pi}_3\pi_{13}\\ \pi_3\pi_{13}^2+2r\pi_2\pi_{13}^2 & -\bar{\pi}_2\pi_{13}\end{pmatrix}$$

$$+\sum_{s=0}^{12}\begin{pmatrix}\bar{\pi}_3^2\pi_{13}^2+\pi_2^2\pi_{13} & \bar{\pi}_2\bar{\pi}_3\pi_{13}^2+\pi_2\pi_3\pi_{13}+s(\bar{\pi}_3^2\pi_{13}^2+\pi_2^2\pi_{13})\\ \bar{\pi}_2\bar{\pi}_3\pi_{13}^2+\pi_2\pi_3\pi_{13} & \bar{\pi}_2^2\pi_{13}^2+\pi_3^3+s(\bar{\pi}_2\bar{\pi}_3\pi_{13}^2+\pi_2\pi_3\pi_{13})\end{pmatrix}$$

$$+\sum_{q=0}^{12}\sum_{r=0}^{12}\begin{pmatrix}q\pi_2\pi_{13}^2+r\pi_2^2\pi_{13} & -1\\ \pi_{13}^3 & 0\end{pmatrix}$$

$$+\sum_{q=0}^{12}\sum_{s=0}^{12}\begin{pmatrix}\bar{\pi}_3\pi_{13}+q\pi_2^2\pi_{13} & \bar{\pi}_2\pi_{13}+q\pi_2\pi_3\pi_{13}+s(\bar{\pi}_3\pi_{13}+q\pi_2^2\pi_{13})\\ \pi_2\pi_{13}^2 & \pi_3\pi_{13}^2+s\pi_2\pi_{13}^2\end{pmatrix}$$

$$+\sum_{r=0}^{12}\sum_{s=0}^{12}\begin{pmatrix}\bar{\pi}_3\pi_{13} & \pi_2\pi_{13}^2+r\pi_2^2\bar{\pi}_3\pi_{13}^2+s\bar{\pi}_3\pi_{13}\\ \bar{\pi}_2\pi_{13} & \pi_3\pi_{13}^2+2r\pi_2\pi_{13}^2+s\bar{\pi}_2\pi_{13}\end{pmatrix}$$

$$+\sum_{q=0}^{12}\sum_{r=0}^{12}\sum_{s=0}^{12}\begin{pmatrix}1 & q\pi_2\pi_{13}^2+r\pi_2^2\pi_{13}+s\\ 0 & \pi_{13}^3\end{pmatrix}$$

Notice that every entry is a principal element. In other words, ideal numbers are not needed to define the principal component of $t(\pi_{13})^3$.

III. 1 The Quaternionic Upper Half Space

The classical theory of modular forms considers functions defined on the upper half plane which is acted on by $SL(2, \mathbb{R})$. As one might expect, mathematicians quickly generalized the basic notions. One of the earliest generalizations was the Poincaré 3-space, also known as the quaternionic upper half space.

Let $i = \sqrt{-1}, j$, and $i \cdot j = k$ be the unit basis elements for the quaternion algebra Q. One defines conjugation as follows: $q = a + bi + cj + dk \in Q$ has conjugate $\overline{q} = a - bi - cj - dk \in Q$ for any $a, b, c, d \in \mathbb{R}$. One defines the norm of q to be $|q| = (a^2 + b^2 + c^2 + d^2)^{1/2}$. The following proposition summarizes trivial but useful properties of Q.

Proposition 6

1) $\overline{(q_1 q_2)} = \overline{q}_2 \overline{q}_1$ for any $q_1, q_2 \in Q$.

2) $q^{-1} = \overline{q}/|q|^2$ for any $q \in Q - \{0\}$.

3) $\alpha k = k\overline{\alpha}$ for any $\alpha \in \mathbb{C}$.

Proof. This is left to the reader. QED

Define the quaternionic upper half space H by $H = \{z \in Q \mid z = x + yk,\ x \in \mathbb{C},\ y > 0\}$. Thus $H \cong \mathbb{C} \times \mathbb{R}^+$. We define an action of $SL(2, \mathbb{C})$ on H by

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}(z) = (\alpha z + \beta)(\gamma z + \delta)^{-1}$$

for $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in SL(2, \mathbb{C})$ and $z \in H$.

Proposition 7

1) The action is well-defined, that is, if $A \in SL(2, \mathbb{C})$ and $z \in H$, then $A(z) \in H$.

2) For any $A, B \in SL(2, \mathbb{C})$, $A(B(z)) = (AB)(z)$.

3) The maximal subgroup of $SL(2, \mathbb{C})$ fixing $z = k$ is $SU(2)$.

4) $SL(2, \mathbb{C})$ acts transitively on H.

Proof. All of these have slick proofs (see Siegel [9]) but also follow from straightforward calculation using Prop. 6. I will not need 3) and 4) so will not prove them, and 1) and 2) are simple.

QED

III.2 Quaternionic Representations

Quaternions do not commute, which discourages consideration of quaternion-valued functions. Using representations, however, one can obtain complex-valued functions with a quaternion argument.

Let $Mat(n, \mathbb{C})$ be the algebra of all $n \times n$ complex matrices. The basic representation ρ of the quaternions Q is given by:

$$\rho : Q \to Mat(2, \mathbb{C})$$

$$\rho(x + yk) = \begin{pmatrix} x & y \\ -\bar{y} & \bar{x} \end{pmatrix} \quad \text{for } x, y \in \mathbb{C} .$$

We construct other representations of Q by considering symmetric powers. Let $A = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ be a matrix, and u, v variables. Then define u', v' by $\begin{pmatrix} u' \\ v' \end{pmatrix} = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \begin{pmatrix} u \\ v \end{pmatrix}$. Let the n-fold symmetric product of A be the $(n+1) \times (n+1)$ matrix $A^{(n)}$ given by

$$\begin{pmatrix} u'^n \\ u'^{n-1} v' \\ u'^{n-2} v'^2 \\ \vdots \\ v'^n \end{pmatrix} = A^{(n)} \begin{pmatrix} u^n \\ u^{n-1} v \\ u^{n-2} v^2 \\ \vdots \\ v^n \end{pmatrix}$$

Now we define the n-fold symmetric quaternion representation

$$\rho^n : Q \to \mathrm{Mat}(n+1, \mathbb{C}) \qquad \text{by}$$

$$\rho^n(x + yk) = \begin{pmatrix} x & y \\ -\bar{y} & \bar{x} \end{pmatrix}^{(n)} .$$

Notice that ρ^n is actually an abusive notation; for instance, ρ^2 has nothing to do with $\rho \cdot \rho$. To further abuse notation, let $\rho^{-n}(x + yk) = (\rho^n(x + yk))^{-1}$.

Proposition 8

1) ρ^n is a representation, that is, for any $q_1, q_2 \in Q$,

$\rho^n(q_1 q_2) = \rho^n(q_1)\, \rho^n(q_2)$.

2) $\rho^{-n}(q) = \rho^n(q^{-1})$.

3) $\rho^n(rq) = r^n \rho^n(q)$ for any $r \in \mathbb{R}$.

4) $\rho^{-n}(q_1 q_2) = \rho^{-n}(q_2)\, \rho^{-n}(q_1)$.

Proof. 1) ρ^n will be a representation if both ρ and the n-fold symmetric product are representations. Simple calculation shows that ρ is a representation. If we let

$$\begin{pmatrix} u'' \\ v'' \end{pmatrix} = (AB)\begin{pmatrix} u \\ v \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} u' \\ v' \end{pmatrix} = B\begin{pmatrix} u \\ v \end{pmatrix}$$

then

$$\begin{pmatrix} u'' \\ v'' \end{pmatrix} = A\left(B\begin{pmatrix} u \\ v \end{pmatrix}\right) = A\begin{pmatrix} u' \\ v' \end{pmatrix}$$

so one sees that $A^{(n)} B^{(n)} = (AB)^{(n)}$, hence this is a representation.

The rest of the statements are straightforward deductions from 1) and Prop. 6. QED

Let $z = x + yk \in H$.

Proposition 9

1) For any $i, j = 1, 2, \ldots, n+1$, the $(ij)^{th}$ entry $(\rho^n(z))_{ij}$ is a polynomial in x, $\bar{x}$, and y with rational integer coefficients,

homogeneous of degree n.

2) The first row of $\rho^n(z)$ is given by

$$(\rho^n(z))_{1j} = \binom{n}{j-1} x^{n+1-j} y^{j-1} \quad .$$

3) Let $x \in \mathbb{C}$. Then $\rho^n(x)$ is a diagonal matrix

$$\operatorname{diag}(x^{n+1-i}\, \overline{x}^{i-1})_{i=1,2,\ldots,n+1} \quad .$$

Proof. 1) Looking at the definition of the n-fold symmetric product, one sees that the entries of $A^{(n)}$ are polynomials in the entries of A with rational integer coefficients. Homogeneity of degree n follows from Prop. 8.3.

The proofs of 2) and 3) also follow directly from the definition of the symmetric product. QED

The following two examples illustrate the typical form of the representations. In particular, notice how the "outside" entries are single terms, while one gets more complicated expressions as one approaches the "center" of the matrix. Let $x + yk \in H$.

$$\rho^{-2}(x + yk) = \left(\frac{1}{|x|^2 + y^2}\right)^2 \begin{pmatrix} \overline{x}^2 & -2\overline{x}y & y^2 \\ \overline{x}y & |x|^2 - y^2 & -xy \\ y^2 & 2xy & x^2 \end{pmatrix} \quad .$$

$$\rho^{-4}(x + yk) = \left(\frac{1}{|x|^2 + y^2}\right)^4 \quad .$$

$$\begin{pmatrix} \bar{x}^4 & -4\bar{x}^3 y & 6\bar{x}^2 y^2 & -4\bar{x}y^3 & y^4 \\ \bar{x}^3 y & \bar{x}^2|x|^2 - 3\bar{x}^2 y^2 & -3\bar{x}|x|^2 y + 3\bar{x}y^3 & -y^4 + 3|x|^2 y^2 & -xy^3 \\ \bar{x}^2 y^2 & 2\bar{x}|x|^2 y - 2\bar{x}y^3 & |x|^4 - 4|x|^2 y^2 + y^4 & -2|x|^2 xy + 2xy^3 & x^2 y^2 \\ \bar{x}y^3 & -y^4 + 3|x|^2 y^2 & -3xy^3 + 3|x|^2 xy & |x|^2 x^2 - 3x^2 y^2 & -x^3 y \\ y^4 & 4xy^3 & 6x^2 y^2 & 4x^3 y & x^4 \end{pmatrix}$$

III. 3 Vector Modular Forms

We will define modular forms consistent with the model of Eisenstein series which we will develop in the next chapter. Let ρ^n be the n-fold symmetric quaternion representation as before. Fix an imaginary quadratic field $K = \mathbb{Q}(\sqrt{d})$ with discriminant = $d < 0$.

In order to concentrate on the properties of modular forms with class number $= h > 1$, we make some simplifying assumptions. I will assume that the discriminant $d \neq -3, -4$ and that the weight n is even. These assumptions eliminate the need for multiplier systems and characters of the unit group. The reader interested in the more general case is urged to see

Hermann [5] or Patterson-Goldfeld [8] for an indication of the complications we are avoiding.

Notation. For the remainder of this thesis, we will be manipulating many matrices and vectors. To avoid specifying the subscripts each time, I will reserve the subscripts i and j to run through the set $\{1, 2, \ldots, n+1\}$. The only exception will be the few times when $i = \sqrt{-1}$ in which cases there should be no confusion. An $(n+1) \times (n+1)$ matrix $(c_{ij})_{i,j=1,2,\ldots,n+1}$ will be written (c_{ij}). An $(n+1)$-length column vector $(c_i)_{i=1,2,\ldots,n+1}$ will be denoted (c_i). Similarly, I will reserve the subscript m to run through the set $\{1, 2, \ldots, h\}$ where h is the class number of the fixed field $K = \mathbb{Q}(\sqrt{d})$. Let $\underline{a}_1, \underline{a}_2, \ldots, \underline{a}_h$ be a fixed set of representatives of the ideal class group, with $\underline{a}_1 = (1)$. Then we will also drop the subscripts from h-length vectors subscripted by m. For instance, the h-length vector $(f(z, \underline{a}_m))_{m=1,2,\ldots,h}$ will be denoted $(f(z, \underline{a}_m))$ and $\left(A_{[\underline{a}_m]}\right)_{m=1,2,\ldots,h}$ will be written $\left(A_{[\underline{a}_m]}\right)$.

Let $[\underline{a}]$ be any ideal class. Let $f(z, \underline{a})$ be an $(n+1)$-length vector of complex-valued functions, say $(f_i(z, \underline{a}))$.

Definition. $f(z, \underline{a})$ is an $[\underline{a}]$ component of a vector modular form of weight n if

1) each $f_i(z, \underline{a})$ is defined and continuous on H.

2) each $f_i(z, \underline{a})$ is bounded "near infinity," that is, on a subset of H given by $\{x + yk \mid y > 1\}$.

3) $f(A(z), \underline{a}) = \rho^{n}(\gamma z + \delta) f(z, \underline{a})$ for all $A = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \Gamma_{\underline{a}}$.

Definition. The $[\underline{a}]$ component of the vector slash operator of weight n is defined by

$$f(z, \underline{a}) \mid A = \rho^{-n}(\mu^{-1/2} (\gamma z + \delta))\, f(\mu^{-1/2} A(z), \underline{a})$$

where $A = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \Gamma^{\underline{b}}_{\underline{b}\,\underline{a}}(\mu)$ for any $[\underline{b}]$, where one fixes either square root of $\mu \in O(Z)$.

Proposition 10. Let $A \in \Gamma^{\underline{b}}_{\underline{b}\,\underline{a}}(\mu)$, and let $f(z, \underline{a})$ be an $[\underline{a}]$ component of a vector modular form.

1) Changing the choice of square root of μ does not change the slash operator.

2) $f(z, \underline{a}) \mid A$ is an $[\underline{a}\,\underline{b}^2 \mu^{-1}]$ component of a vector modular form. If $B \in \Gamma^{\underline{c}}_{\underline{c}\,\underline{a}\,\underline{b}^2 \mu^{-1}}(\nu)$, for any $[\underline{c}]$ and any $\nu \in O(Z)$, then $(f(z, \underline{a}) \mid A) \mid B = f(z, \underline{a}) \mid (AB)$.

Proof. 1) By assumption, n is even so $\rho^n(-1) = \rho^n(1)$. Also $-\mu^{1/2} A(z) = \mu^{1/2} A(z)$ so replacing $\mu^{1/2}$ by $-\mu^{-1/2}$ does not change the slash operator.

2) This will follow from the consistency rule, Prop. 2.1,

and a careful application of Props. 6, 7 and 8. Let

$$A = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \Gamma^{\underline{b}}_{\underline{b}\,\underline{a}}(\mu)$$

and

$$B = \begin{pmatrix} \pi & \rho \\ \psi & \tau \end{pmatrix} \in \Gamma^{\underline{c}}_{\underline{c}\,\underline{a}\,\underline{b}^2\mu^{-1}}(\nu) \ .$$

Then

$$f(z, \underline{a}) \mid A = \rho^{-n}(\mu^{-1/2}(\gamma z + \delta))\, f(\mu^{-1/2} A(z), \underline{a})$$

so

$$(f(z, \underline{a}) \mid A) \mid B = \rho^{-n}(\nu^{-1/2}(\psi z + \tau)) \cdot$$

$$\cdot\ \rho^{-n}(\mu^{-1/2}(\gamma[\nu^{-1/2} B(z)] + \delta))\, f(\mu^{-1/2} A \nu^{-1/2} B(z), \underline{a})$$

$$= \rho^{-n}(\nu^{-1/2}(\psi z + \tau)) \cdot \rho^{-n}(\mu^{-1/2}[\gamma \nu^{-1/2}(\pi z + \rho)$$

$$+ \delta \nu^{-1/2}(\psi z + \tau)] \cdot (\psi z + \tau)^{-1} \nu^{1/2}) \cdot f((\mu \nu)^{-1/2} AB(z), \underline{a})$$

$$= \rho^{-n}((\mu\nu)^{-1/2}[(\gamma\pi + \delta\psi)z + (\gamma\rho + \delta\tau)]) \cdot$$

$$\cdot\ f((\mu\nu)^{-1/2} AB(z), \underline{a})$$

$$= f(z, \underline{a}) \mid (AB) \ .$$

Notice that several times I have used 1) to replace $\mu^{1/2} \nu^{1/2}$ by $(\mu\nu)^{1/2}$. <u>QED</u>

<u>Definition.</u> $F(z)$ is a vector modular form of weight n, written $F \in \underline{F}(n)$, if F is an h-length vector of functions $F(z) = (f(z, \underline{a}_m))$