ISRAEL JOURNAL OF MATHEMATICS, Vol. 24, No. 2, 1976

CONSTRUCTION OF MODULAR FORMS

BY

JOSEPH LEWITTES[†]

ABSTRACT

Modular forms arising from lattices are constructed and their transformation properties under the full modular group are obtained in explicit form suitable for calculation. The forms are obtained via specialization of the several variable theta function.

Introduction

Theta series associated with positive integral quadratic forms have a long history. Among the classical papers concerned with this topic we cite Hurwitz [4], Hecke [3] and Schoeneberg [7]. In these and others one obtains a function f of the complex variable τ in the upper half plane and studies its behavior under the mappings $\tau \to \tau + 1$ and $\tau \to -1/\tau$ which generate the modular group Γ. One then deduces that f is a modular form for a suitable subgroup G of Γ. However there seems to be no systematic investigation as to how f transforms under a general element of Γ. Knowledge of this type is indispensable though when one wishes to obtain the appropriate expansions at all the cusps of G. Our attitude here is to be as explicit as possible in all constructions so that in any given case calculations should actually be feasible.

The functions that we consider are a generalization of those of Hecke and Schoeneberg but we approach them via specialization of the theta function of several variables. Use of the 'characteristic' notation of this function is amenable to our purposes. Also the methods developed here may be found useful in the study of modular functions of several variables. Rather than working with a quadratic form we start with a lattice in $\boldsymbol{R}^n$ and certain related spaces. This appears to be a natural point of view and allows for greater flexibility and generality.

By way of illustration of what is to be discussed, let $\mathscr{L}$ be a lattice in $\boldsymbol{R}^n$ such that $\|\lambda\|^2$ ($= \lambda \cdot \lambda$, usual norm and inner-product) is an even integer for every

[†] The author gratefully acknowledges the support of N.S.F. Grant GP-42874.

Received October 28, 1975

$\lambda \in \mathscr{L}$. Define the integer $L = \text{g.c.d.}\{(1/2)\|\lambda\|^2 : \lambda \in \mathscr{L}\}$ and with $x, y \in \boldsymbol{R}^n$ and τ as above, set

$$\psi_{\mathscr{L}}\begin{bmatrix} x \\ y \end{bmatrix}(\tau) = \sum_{\lambda \in \mathscr{L}} \exp\left(2\pi i(\lambda + x)\cdot y + \pi i \frac{\tau}{L}\|\lambda + x\|^2\right).$$

Then we obtain the transformation formula for $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$,

$$\frac{\psi_{\mathscr{L}}\begin{bmatrix} x \\ y \end{bmatrix}(M(\tau))}{(c\tau + d)^{n/2}} = e^{\pi i \nu(x, y, M_{(L)})} \sum_{\beta \in J} t(M, \beta)\psi_{\mathscr{L}}\begin{bmatrix} ax + Lcy + \beta \\ bx/L + dy \end{bmatrix}(\tau).$$

Here $\nu(x, y, M_{(L)}) = -(ab/L)\|x\|^2 - Lcd\|y\|^2 - 2bcx \cdot y$ and J is the finite abelian group $L\mathscr{L}^*/\mathscr{L}$, $\mathscr{L}^*$ the dual lattice of $\mathscr{L}$. $\beta \in J$ means β ranges over a set of coset representatives of $L\mathscr{L}^*$ mod $\mathscr{L}$. The coefficients $t(M, \beta)$ depend on M, $\mathscr{L}$ and β mod $\mathscr{L}$ but not x, y or τ. Considering $\beta \to t(M, \beta)$ as a complex valued function $t(M)$ on the group J we find that the $t(M)$ all have the same norm, as elements of the finite dimensional Hilbert space of functions on J, and that $t(MS)$, $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$, is up to an eighth root of unity the Fourier transform of $t(M)$. The $t(M)$ are known initially only for S and $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, generators of Γ, but by iteration we obtain them for all $M \in \Gamma$. The final result involves the group structure of J and we get explicit formulas at least for the case where Δ, the order of J, is odd. To get these formulas we must evaluate a Gauss-like sum

$$\sum_{k_1, \cdots, k_r \bmod m} \zeta^{u_1 k_1^2 + \cdots + u_r k_r^2 - 2k_1 k_2 - \cdots - 2k_r k};$$

here ζ is a primitive mth root of unity, m odd, $r \geqq 1$ and $u_1, \cdots, u_r, k$ are arbitrary integers.

In Section 1 we discuss lattices and introduce the class of lattices which are our main concern.

Section 2 introduces the theta function and develops the transformation theory as needed. At the end of this section we reach our first main theorem. The coefficients $t(M)$ are investigated systematically in Section 3. Along the way we discover two invariants $W = \pm 1$ and ε, a fourth root of unity, of our lattices and the relation between them is found. It will be evident throughout that the number 2 plays a special role and our results are complete only in case Δ is odd. An analysis of the even Δ is left to the future but the general picture should be the same. Finally in Section 4 we give examples arising from number fields, particular attention being given to the imaginary quadratic fields.

We must admit that our treatment is incomplete in that the functions we study have not been integrated into the framework of the general theory of modular forms. Presentations of this theory from various viewpoints are given in the books of Eichler [2], Lehner [5] and Shimura [8]. Thus we must defer until later such questions as the relations among these functions and the Eisenstein and Poincaré series, Petersson inner product, Hecke operators and so on. Ultimately it is hoped that a careful cataloguing of the various modular forms obtained by these methods will enable one to write down explicitly a basis for the cusp forms of weight two (= abelian differentials of first kind) for the groups $\Gamma_0(m)$ and $\Gamma(m)$. Some progress has been made in this direction but a discussion of this program is outside the scope of this paper.

1. Lattices

Let n be a positive integer and $\boldsymbol{C}^n$ the space of n-tuples of complex numbers, taken as column vectors. The entries (or coordinates) of $z \in \boldsymbol{C}^n$ are usually denoted $z_1, \cdots, z_n$; thus ${}^t z$ is the row $(z_1, \cdots, z_n)$, 't' indicating the transpose. The dot product for $z, w \in \boldsymbol{C}^n$ is $z \cdot w = {}^t z w = \Sigma_{k=1}^n z_k w_k$ and the length of z, $\| z \|$, is given by $\| z \|^2 = z \cdot \bar{z}$, the bar indicating complex conjugate. If M is an $n \times n$ matrix the notation $M[z] = z \cdot Mz = {}^t zMz$ is convenient and will be used.

Let r_1, r_2 be non-negative integers with $r_1 + 2r_2 = n$. $\mathcal{M}^{r_1, r_2}$ is the set of vectors in $\boldsymbol{C}^n$ whose first r_1 entries are real and whose last r_2 entries are the complex conjugates of the preceding r_2. Thus $z \in \mathcal{M}^{r_1, r_2}$ if and only if $z_k = \bar{z}_k$, $1 \leqq k \leqq r_1$, and $z_{r_1+r_2+k} = \bar{z}_{r_1+k}$, $1 \leqq k \leqq r_2$. If one of r_1 or r_2 is zero the obvious modifications must be made in the previous sentence. If $r_1 = n$, $r_2 = 0$, $\mathcal{M}^{n,0}$ is just $\boldsymbol{R}^n$, the space of real vectors. From now on we consider n, r_1, r_2 as fixed and write simply $\mathcal{M}$ for $\mathcal{M}^{r_1, r_2}$. Note that $z \in \mathcal{M}$ implies $\bar{z} \in \mathcal{M}$ and for $z, w \in \mathcal{M}$, $z \cdot w$ is real and

$$(1) \qquad \| z + w \|^2 = \| z \|^2 + \| w \|^2 + 2z \cdot \bar{w}.$$

$\mathcal{M}$ is a real vector space of (real) dimension n with a basis given by the columns of the $n \times n$ matrix

$$(2) \qquad \Phi = \Phi^{r_1, r_2} = \begin{pmatrix} E_1 & 0 & 0 \\ 0 & E_2 & iE_2 \\ 0 & E_2 & -iE_2 \end{pmatrix}.$$

Here E_j is the identity matrix of size r_j ($j = 1, 2,$) and each 0 is a zero matrix of appropriate size. Any $n \times n$ matrix whose columns form a basis of $\mathcal{M}$ will be called a basic matrix for $\mathcal{M}$. Another important matrix is

$$(3) \qquad R = R^{r_1, r_2} = \begin{pmatrix} E_1 & 0 & 0 \\ 0 & 0 & E_2 \\ 0 & E_2 & 0 \end{pmatrix}.$$

If A is a nonsingular matrix we set $A^* = {}'A^{-1}$ so that, when defined, $(AB)^* = A^*B^*$.

PROPOSITION 1.

i) $\det \Phi = (-2i)^{r_2}$ *and* $\Phi^* = \Phi H$,

$$H = \begin{pmatrix} E_1 & 0 & 0 \\ 0 & \tfrac{1}{2}E_2 & 0 \\ 0 & 0 & -\tfrac{1}{2}E_2 \end{pmatrix}.$$

ii) Λ *is a basic matrix for* $\mathcal{M}$ *if and only if* $\Lambda = \Phi G$, G *an* $n \times n$ *real nonsingular matrix.*

iii) *If* Λ *is a basic matrix for* $\mathcal{M}$ *then so is* Λ^*.

iv) $R = {}'R = R^{-1} = R^*$, $\det R = (-1)^{r_2}$. *If* $x, y \in \mathcal{M}$ *and* Λ *is a basic matrix for* $\mathcal{M}$ *then* $Rx = \bar{x}$, $R\Lambda = \bar{\Lambda}$, $x \cdot \bar{y} = {}'xRy$, *and* $\| x \|^2 = R[x]$.

PROOF. (i), (ii), (iv) are straightforward linear algebra. For (iii), note that, by (ii), $\Lambda = \Phi G$ so $\Lambda^* = \Phi^* G^* = \Phi(HG^*)$ whence, by (ii) again, Λ^* is a basic matrix.

A lattice in $\mathcal{M}$ is a free abelian group (under vector addition) generated by a basis of $\mathcal{M}$. Thus every lattice, as a free abelian group of rank n, has a basis which at the same time is a vector space basis for $\mathcal{M}$. If the vectors $\lambda_1, \cdots, \lambda_n$ of $\mathcal{M}$ are a basis for the lattice $\mathcal{L}$ the matrix Λ whose columns are $\lambda_1, \cdots, \lambda_n$ is called a basic matrix for $\mathcal{L}$. Λ is then a basic matrix for $\mathcal{M}$ also. Conversely if Λ is a basic matrix for $\mathcal{M}$ it is also a basic matrix for the lattice $\mathcal{L}$ consisting of all integral linear combinations of the columns of Λ. The simplest example of a lattice is $\boldsymbol{Z}^n$, the lattice of integral vectors in $\mathcal{M}^{n,0} = \boldsymbol{R}^n$.

Let $\mathcal{L}$ be a lattice in $\mathcal{M}$ with basic matrix Λ. Then, by the above remarks, every $z \in \mathcal{M}$ has a unique expression as $z = \Lambda\xi$, $\xi \in \boldsymbol{R}^n$, and $z \in \mathcal{L}$ if and only if $\xi \in \boldsymbol{Z}^n$. The totality of basic matrices for $\mathcal{L}$ is $\{\Lambda U\}$, U ranging over all $n \times n$ unimodular matrices (integral matrices of determinant ± 1). $\bar{\mathcal{L}} = \{\bar{\lambda} : \lambda \in \mathcal{L}\}$ is a lattice with basic matrix $\bar{\Lambda}$ and for c a nonzero real number $c\mathcal{L} = \{c\lambda : \lambda \in \mathcal{L}\}$ is a lattice with basic matrix $c\Lambda$. If c is an integer then $c\mathscr{L}$ is a sublattice of $\mathscr{L}$ with index (in the sense of group theory) $[\mathscr{L}: c\mathscr{L}] = |c|^n$. In the following proposition we give two basic definitions.

Proposition 2. *Let $\mathscr{L}$ be a lattice in $\mathscr{M}$ with basic matrix Λ.*

i) *The discriminant of $\mathscr{L}$, $D(\mathscr{L})$, is defined by $D(\mathscr{L}) = (\det\Lambda)^2$. It depends only on $\mathscr{L}$ and not the choice of Λ. $D(\mathscr{L})$ is a real number, positive if r_2 is even, negative if r_2 is odd. $|D(\mathscr{L})| = (-1)^{r_2}D(\mathscr{L})$. $D(\bar{\mathscr{L}}) = D(\mathscr{L})$ and $D(c\mathscr{L}) = c^{2n}D(\mathscr{L})$.*

ii) *Let $\mathscr{L}_1$ be a lattice with basic matrix Λ_1. Then $\mathscr{L}_1$ is a sublattice of $\mathscr{L}$ if and only if $\Lambda_1 = \Lambda G$, G a nonsingular integral matrix. It this case then, $[\mathscr{L}: \mathscr{L}_1] = |\det G|$ and $D(\mathscr{L}_1) = [\mathscr{L}: \mathscr{L}_1]^2 D(\mathscr{L})$.*

iii) *$\mathscr{L}^* = \{z \in \mathscr{M};\ z \cdot \lambda \in \boldsymbol{Z}$ for every $\lambda \in \mathscr{L}\}$ is a lattice, called the dual lattice of $\mathscr{L}$. Λ^* is a basic matrix for $\mathscr{L}^*$ and $D(\mathscr{L}^*) = D(\mathscr{L})^{-1}$, $(\mathscr{L}^*)^* = \mathscr{L}$, $(\bar{\mathscr{L}})^* = \overline{(\mathscr{L}^*)}$, $(c\mathscr{L})^* = c^{-1}\mathscr{L}^*$.*

Proof. If U is unimodular, $(\det\Lambda U)^2 = (\det\Lambda)^2$, which shows $D(\mathscr{L})$ is well defined independent of the choice of the basic matrix Λ. By Proposititon 1 we may write $\Lambda = \Phi G$, $D(\mathscr{L}) = (\det\Lambda)^2 = (\det\Phi)^2(\det G)^2 = (-2i)^{2r_2}(\det G)^2 = (-1)^{r_2}p$, p a positive real number. The rest of (i) is clear. (ii) is standard matrix and group theory, for details see [1, p. 125]. For (iii) it is clear that $\mathscr{L}^*$ is a subgroup of $\mathscr{M}$. By Proposition 1 (iii), Λ^* is a basic matrix for $\mathscr{M}$ along with Λ, so we can express $z \in \mathscr{M}$ as $z = \Lambda^*\xi$, $\xi \in \boldsymbol{R}^n$, and $\lambda \in \mathscr{L}$ as Λu, $u \in \boldsymbol{Z}^n$. Then $z \cdot \lambda = \xi \cdot u$ is an integer for all $u \in \boldsymbol{Z}^n$ if and only if $\xi \in \boldsymbol{Z}^n$, i.e., z is an integral linear combination of the columns of Λ^*. Thus $\mathscr{L}^*$ is the lattice generated by the columns of Λ^*. The rest is obvious.

We are interested in lattices $\mathscr{L}$ with the property:

(4) $\lambda \cdot \bar{\mu}$ is an integer for all $\lambda, \mu \in \mathscr{L}$.

It follows then that $\|\lambda\|^2 = \lambda \cdot \bar{\lambda}$ is an integer. However, for the purpose of the functions to be constructed it is more convenient to have $\|\lambda\|^2$ an even integer. Thus we define: A lattice $\mathscr{L}$ satisfying (4) is odd if for some $\lambda \in \mathscr{L}$, $\|\lambda\|^2$ is an odd integer and is even if $\|\lambda\|^2$ is an even integer for all $\lambda \in \mathscr{L}$. For example, $\boldsymbol{Z}^n$ is odd. If $\mathscr{L}$ is an odd lattice, then it is easily verified, using (1) and (4), that $\mathscr{L}_0 = \{\lambda \in \mathscr{L}: \|\lambda\|^2$ is even$\}$ is an even lattice of index 2 in $\mathscr{L}$. Note also that every sublattice of an even lattice is even and if $\mathscr{L}$ is even so is $\bar{\mathscr{L}}$. The condition (4) is equivalent to $\mathscr{L} \subset \bar{\mathscr{L}}^*$, and in the next propostion we obtain a refinement of this.

Proposition 3. *Let $\mathscr{L}$ be an even lattice. Define the positive integer $L = L(\mathscr{L}) =$ g.c.d.$\{(1/2)\|\lambda\|^2: \lambda \in \mathscr{L}\}$.*

i) *For all* $\lambda, \mu \in \mathscr{L}$, $\lambda \cdot \bar{\mu} \equiv 0 (\operatorname{mod} L)$.

ii) $\mathscr{L}$ *is a sublattice of* $L\bar{\mathscr{L}}^*$. *If* $\Delta = \Delta(\mathscr{L})$ *is the index* $[L\bar{\mathscr{L}}^*: \mathscr{L}|$ *then* $|D(\mathscr{L})| = L^n\Delta$.

iii) $L(\bar{\mathscr{L}}) = L(\mathscr{L})$, $\Delta(\bar{\mathscr{L}}) = \Delta(\mathscr{L})$. *If c is a nonzero integer* $L(c\mathscr{L}) = c^2L(\mathscr{L})$, $\Delta(c\mathscr{L}) = \Delta(\mathscr{L})$.

Proof. For all $\lambda \in \mathscr{L}$, $\|\lambda\|^2 \equiv 0 (\operatorname{mod} 2L)$ whence by (1), with z, w replaced by λ, μ, $2\lambda \cdot \bar{\mu} \equiv 0 (\operatorname{mod} 2L)$ which gives (i). (i) can be restated as $\lambda \cdot \bar{\mu} / L \in \boldsymbol{Z}$ so that $\bar{\mu}/L \in \mathscr{L}^*$, $\mu \in L\bar{\mathscr{L}}^*$, i.e., $\mathscr{L}$ is a sublattice of $L\bar{\mathscr{L}}^*$. Since $\mathscr{L} \subset \bar{\mathscr{L}}^*$, Proposition 2, (ii), (iii) show that $[\bar{\mathscr{L}}^*: \mathscr{L}]^2 = D(\mathscr{L})/D(\bar{\mathscr{L}}^*) = D(\mathscr{L})^2$ so that taking (positive) square roots, $|D(\mathscr{L})| = [\bar{\mathscr{L}}^*: \mathscr{L}] = [\bar{\mathscr{L}}^*: L\bar{\mathscr{L}}^*][L\bar{\mathscr{L}}^*: \mathscr{L}] = L^n\Delta$ which proves (ii). (iii) is easy.

If $\mathscr{L}$ is a lattice satisfying (4), and Λ a basic matrix for $\mathscr{L}$ with columns $\lambda_1, \cdots, \lambda_n$ then every $\lambda \in \mathscr{L}$ is $\lambda = \Lambda u$, $u \in \boldsymbol{Z}^n$ and $\|\lambda\|^2 = \Sigma_{j,k=1}^n a_{jk}u_ju_k$ is a positive definite quadratic form $Q(u)$ in $u_1, \cdots, u_n$ with integral coefficients $a_{jk} = \lambda_j \cdot \bar{\lambda}_k = a_{kj}$. The matrix $(a_{jk}) = {}^t\Lambda\bar{\Lambda}$ is a positive definite integral symmetric matrix, with even diagonal coefficients if $\mathscr{L}$ is even. In this latter case it is clear that $L = L(\mathscr{L})$ is the largest positive integer such that ${}^t\Lambda\bar{\Lambda} = LA$, A an integral symmetric matrix with even diagonal entries. Then $\det({}^t\Lambda\bar{\Lambda}) = L^n \det A$ while on the other hand $\det({}^t\Lambda\bar{\Lambda}) = |D(\mathscr{L})| = L^n\Delta$. Thus $\Delta = \det A$ and if n is odd it is not difficult to see that $\det A$ must be even so we deduce that

$$\text{if } \Delta \text{ is odd } n \text{ must be even}. \tag{5}$$

Example of lattices arising from algebraic number fields and the related quadratic forms will be discussed in Section 5. We only point out here that two different lattices may give rise to the same quadratic form Q. For example, let $\mathscr{L}$ be the even lattice in $\mathscr{M}^{2,0}$ consisting of all $\lambda \in \boldsymbol{Z}^2$ such that $\|\lambda\|^2$ is even. Then

$$\Lambda = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

is a basic matric for $\mathscr{L}$ and $D(\mathscr{L}) = 4$. Let $\mathscr{L}'$ be the even lattice in $\mathscr{M}^{0,1}$ with basic matrix

$$\Lambda' = \begin{pmatrix} 1 & i \\ 1 & -i \end{pmatrix}.$$

Then $D(\mathscr{L}') = -4$ and both $\mathscr{L}$ and $\mathscr{L}'$ give rise to the same quadratic form $Q(u_1, u_2) = 2(u_1^2 + u_2^2)$.

2. The Theta function

The generalized upper half plane of degree n, $\mathcal{H}^n$, is the set of $n \times n$ complex symmetric matrices with positive definite imaginary part. In particular $\mathcal{H}^1$, or simply $\mathcal{H}$, is the usual upper half plane. For $x, y, z \in \boldsymbol{C}^n$ and $Z \in \mathcal{H}^n$ the series

$$\sum_{m \in \boldsymbol{Z}^n} e^{2\pi i(m+x)\cdot(z+y)+\pi i Z[m+x]} \tag{6}$$

is absolutely convergent and uniformly convergent on compact subsets of $\boldsymbol{C}^n \times \boldsymbol{C}^n \times \boldsymbol{C}^n \times \mathcal{H}^n$. The function defined by (6) — analytic in x, y, z, Z — is called the θ function, denoted $\theta[{x \atop y}](z, Z)$. x, y are usually taken as fixed and $[{x \atop y}]$ is then called the characteristic of the θ function. Note that $\theta[{x \atop y}](z, Z) = \theta[{x \atop 0}](y + z, Z)$ so that y or z might be dispensed with, but our notation is more or less traditional and has its advantages. There is a vast literature devoted to the θ function but we shall be able to develop here most of those properties that we intend to use. References to the classical literature along with detailed development of the theory from the point of view of applications to Riemann surfaces will be found in the book by Rauch and Farkas [6]. A concise introduction to the θ function is presented by Eichler [2]. The reader should be forewarned that the notation in this subject has never been standardized and one must exercise some caution when using different sources.

Now we associate a θ function with each lattice $\mathcal{L}$, essentially by replacing in (6) the sum over $\boldsymbol{Z}^n$ by a sum over the vectors in $\mathcal{L}$. First though we must define $\mathcal{H}^{r_1, r_2}$ the analogue of $\mathcal{H}^n$. The condition that a symmetric matrix Z be in $\mathcal{H}^n$ is $(\operatorname{Im} Z)[\xi] > 0$ for all $\xi \in \boldsymbol{R}^n$, $\xi \neq 0$, which can also be expressed as $\operatorname{Im}(Z[\xi]) > 0$. We define now $\mathcal{H}^{r_1, r_2}$ as the set of $n \times n$ complex symmetric matrices V satisfying $\operatorname{Im}(V[x]) > 0$ for all $x \in \mathcal{M}^{r_1, r_2}$, $x \neq 0$. Thus $\mathcal{H}^{n,0}$ is the original $\mathcal{H}^n$. If Λ is a basic matrix for $\mathcal{M}$ setting $x = \Lambda\xi$, $\xi \in \boldsymbol{R}^n$, we see that $V \in \mathcal{H}^{r_1, r_2}$ if and only if ${}'\Lambda V \Lambda \in \mathcal{H}^n$. In particular, as it is known that $-Z^{-1} \in \mathcal{H}^n$ if $Z \in \mathcal{H}^n$ it follows that $-V^{-1} \in \mathcal{H}^{r_1, r_2}$ whenever $V \in \mathcal{H}^{r_1, r_2}$. Indeed, $V \in \mathcal{H}^{r_1, r_2}$ implies $-({}'\Lambda V \Lambda)^{-1} = {}'\Lambda^*(-V^{-1})\Lambda^* \in \mathcal{H}^n$ and since Λ^* is also a basic matrix for $\mathcal{M}$ the result follows. Every matrix of the form

$$V = \begin{pmatrix} U & 0 & 0 \\ 0 & S & T \\ 0 & T & \bar{S} \end{pmatrix}$$

with $U \in \mathcal{H}^{r_1}$, $T \in \mathcal{H}^{r_2}$ and S an arbitrary $r_2 \times r_2$ symmetric matrix is in $\mathcal{H}^{r_1, r_2}$. For, any $x \in \mathcal{M}^{r_1, r_2}$ is

$$x = \begin{pmatrix} a \\ b+ic \\ b-ic \end{pmatrix},$$

$a \in \boldsymbol{R}^{r_1}$, $b, c \in \boldsymbol{R}^{r_2}$ and a calculation shows

$$\operatorname{Im}(V[x]) = \operatorname{Im} U[a] + 2\operatorname{Im} T[b] + 2\operatorname{Im} T[c]$$

which is positive unless $a = 0$, $b = c = 0$, i.e. $x = 0$. In particular, if $\tau \in \mathcal{H}$ then $V = \tau R$ (R as in (3)) is in $\mathcal{H}^{r_1, r_2}$ and $-V^{-1} = (-1/\tau)R$.

Now let $\mathcal{L}$ be a lattice in $\mathcal{M} = \mathcal{M}^{r_1, r_2}$, $x, y, z \in \boldsymbol{C}^n$, $V \in \mathcal{H}^{r_1, r_2}$ and define the function $\theta_{\mathcal{L}}$ by

$$\theta_{\mathcal{L}}\begin{bmatrix} x \\ y \end{bmatrix}(z, V) = \sum_{\lambda \in \mathcal{L}} e^{2\pi i(\lambda + x)\cdot(z+y) + \pi i V[\lambda + x]}. \tag{7}$$

In case $\mathcal{L} = \boldsymbol{Z}^n$ this coincides with the original θ defined by (6). If Λ is a basic matrix for $\mathcal{L}$ we see that

$$\theta_{\mathcal{L}}\begin{bmatrix} x \\ y \end{bmatrix}(z, V) = \theta\begin{bmatrix} \Lambda^{-1}x \\ {}^t\Lambda y \end{bmatrix}({}^t\Lambda z, {}^t\Lambda V \Lambda) \tag{8}$$

so that there is no problem as to convergence in (7) and analyticity in x, y, z, V. However the great advantage in working with $\theta_{\mathcal{L}}$ as defined by (7) rather than with the right side of (8) is that one can deal directly with a lattice and there is no need to specify any particular basic matrix. Along with $\theta_{\mathcal{L}}$ we consider the functions obtained by differentiating with respect to the coordinates z_j of z. Let $s = (s_1, s_2, \cdots, s_l)$ be a finite sequence of integers, $1 \leqq s_j \leqq n$ for each j, and define

$$\theta_{\mathcal{L}}^{(s)}\begin{bmatrix} x \\ y \end{bmatrix}(z, V) = \frac{\partial^l}{\partial z_{s_1}\partial z_{s_2}\cdots\partial z_{s_l}}\theta_{\mathcal{L}}\begin{bmatrix} x \\ y \end{bmatrix}(z, V). \tag{9}$$

l is the length of the sequence s and we agree to allow also $s = (0)$, the empty sequence of length $l = 0$ with the usual convention $\theta_{\mathcal{L}}^{(0)} = \theta_{\mathcal{L}}$. The series (7) can be differentiated term by term and we obtain

$$\begin{aligned} \theta_{\mathcal{L}}^{(s)}\begin{bmatrix} x \\ y \end{bmatrix}(z, V) &= (2\pi i)^l \sum_{\lambda \in \mathcal{L}} c^{(s)}(\lambda, x) e^{2\pi i(\lambda + x)\cdot(z+y) + \pi i V[\lambda + x]} \\ c^{(s)}(\lambda, x) &= \prod_{k=1}^{l} (\lambda_{s_k} + x_{s_k}) \end{aligned} \tag{10}$$

where λ_{s_k}, x_{s_k} is the s_kth component of the vector λ, x, respectively.

Proposition 4.

i) *For* $\mu \in \mathscr{L}$, $\nu \in \mathscr{L}^*$

$$\theta_{\mathscr{L}}^{(s)}\begin{bmatrix} x+\mu \\ y+\nu \end{bmatrix}(z, V) = e^{2\pi i x\cdot\nu}\theta_{\mathscr{L}}^{(s)}\begin{bmatrix} x \\ y \end{bmatrix}(z, V).$$

In particular, $\theta_{\mathscr{L}}^{(s)}[{}^{x+\mu}_{\ y}](z, V) = \theta_{\mathscr{L}}^{(s)}[{}^{x}_{y}](z, V)$.

ii) *If* $\mathscr{L}$ *is a sublattice of* $\mathscr{L}_1$ *of index* Δ *and* $\beta_1, \cdots, \beta_\Delta$ *is a set of coset representatives of* $\mathscr{L}_1 \bmod \mathscr{L} - \mathscr{L}_1 = \bigcup_{j=1}^{\Delta}(\beta_j + \mathscr{L})$*—then*

$$\theta_{\mathscr{L}_1}^{(s)}\begin{bmatrix} x \\ y \end{bmatrix}(z, V) = \sum_{j=1}^{\Delta} \theta_{\mathscr{L}}^{(s)}\begin{bmatrix} x+\beta_j \\ y \end{bmatrix}(z, V).$$

iii) *If* $\mathscr{L}'$ *is a lattice in* $\mathscr{M}^{r_1'+2r_2'}$, $r_1' + 2r_2' = n$, Λ, Λ' *are basic matrices for* $\mathscr{L}$, $\mathscr{L}'$ *respectively, and* $W = (W_{jk})_{1\leqq j,k\leqq n} = \Lambda'\Lambda^{-1}$ *then*

$$\theta_{\mathscr{L}'}\begin{bmatrix} x \\ y \end{bmatrix}(z, V) = \theta_{\mathscr{L}}\begin{bmatrix} W^{-1}x \\ {}^tWy \end{bmatrix}({}^tWz, {}^tWVW). \tag{11}$$

If s *is any sequence with length* $l > 0$ *then*

$$\theta_{\mathscr{L}'}^{(s)}\begin{bmatrix} x \\ y \end{bmatrix}(z, V) = \sum_{k_1,\cdots,k_l=1}^{n} W_{s_1k_1} W_{s_2k_2} \cdots W_{s_lk_l}\theta_{\mathscr{L}}^{(k_1,\cdots,k_l)}\begin{bmatrix} W^{-1}x \\ {}^tWy \end{bmatrix}({}^tWz, {}^tWVW). \tag{12}$$

Proof. (i) follows by direct substitution in (10) noting that as λ ranges over $\mathscr{L}$ so does $\lambda + \mu$ and $e^{2\pi i\lambda\cdot\nu} = 1$. (ii) is proved similarly. The first part of (iii) follows from (7) upon replacing $\mathscr{L}$ by $\mathscr{L}'$ and noting that as λ ranges over $\mathscr{L}$, $\lambda' = W\lambda$ ranges over $\mathscr{L}'$. Successive differentiation of (11) yields (12).

A special case worth mentioning is: If $\mathscr{L}' = c\mathscr{L}$, c a nonzero real number, we can take $\Lambda' = c\Lambda$, $W = cE$, E the $n \times n$ identity matrix, and obtain for $l \geqq 0$,

$$\theta_{c\mathscr{L}}^{(s)}\begin{bmatrix} x \\ y \end{bmatrix}(z, V) = c^l\theta_{\mathscr{L}}^{(s)}\begin{bmatrix} c^{-1}x \\ cy \end{bmatrix}(cz, c^2V). \tag{13}$$

Taking $c = -1$, $c\mathscr{L} = \mathscr{L}$ and

$$\theta_{\mathscr{L}}^{(s)}\begin{bmatrix} x \\ y \end{bmatrix}(z, V) = (-1)^l\theta_{\mathscr{L}}^{(s)}\begin{bmatrix} -x \\ -y \end{bmatrix}(-z, V). \tag{14}$$

If furthermore $2x \in \mathscr{L}$, $2y \in \mathscr{L}^*$ and $2x \cdot 2y = k \in \boldsymbol{Z}$ then

$$\theta_{\mathscr{L}}^{(s)}\begin{bmatrix} x \\ y \end{bmatrix}(-z, V) = \theta_{\mathscr{L}}^{(s)}\begin{bmatrix} -x+2x \\ -y+2y \end{bmatrix}(-z, V) = (-1)^k\theta_{\mathscr{L}}^{(s)}\begin{bmatrix} -x \\ -y \end{bmatrix}(-z, V)$$

(by (i) of the proposition) $= (-1)^{k+l}\theta_{\mathscr{L}}^{(s)}[{}^{x}_{y}](z, V)$ (by (14)). In this case then $\theta_{\mathscr{L}}^{(s)}[{}^{x}_{y}](z, V)$ is an even or odd function of z. When odd, $\theta_{\mathscr{L}}^{(s)}[{}^{x}_{y}](0, V)$ is identically zero as a function of V. In particular $\theta^{(s)}_{\mathscr{L}}[{}^0_0](0, V)$ vanishes identically in V when l is odd.

The next step is to carry over to $\theta^{(s)}_{\mathscr{L}}$ part of the transformation theory of the θ function. For our purposes we take as our starting point the known formula

$$(15)\qquad \theta\begin{bmatrix} x \\ y \end{bmatrix}(z, -Z^{-1}) = e^{2\pi i x\cdot y + \pi i Z[z]}\sqrt{\det(-iZ)}\,\theta\begin{bmatrix} y \\ -x \end{bmatrix}(Zz, Z).$$

We claim that for $\theta_{\mathscr{L}}$ this becomes

$$(16)\qquad \theta_{\mathscr{L}}\begin{bmatrix} x \\ y \end{bmatrix}(z, -V^{-1}) = e^{2\pi i x\cdot y + \pi i V[z]}\sqrt{\frac{\det(-iV)}{D(\mathscr{L})}}\,\theta_{\mathscr{L}^*}\begin{bmatrix} y \\ -x \end{bmatrix}(Vz, V).$$

This is deduced by expressing the left side of (16) as an ordinary θ via (8), $-V^{-1}$ is thus replaced by ${}^t\Lambda(-V^{-1})\Lambda = -({}^t\Lambda^* V\Lambda^*)^{-1}$, then apply (15) with $Z = {}^t\Lambda^* V\Lambda^*$ and recalling that Λ^* is a basic matrix for $\mathscr{L}^*$ a reverse application of (8) brings us to $\theta_{\mathscr{L}^*}$. The discriminant $D(\mathscr{L})$ enters from $\det(-i{}^t\Lambda^* V\Lambda^*) = \det(-iV)(\det\Lambda)^{-2} = \det(-iV)/D(\mathscr{L})$. The square root in (15) is determined uniquely by the condition that for $Z = iE$ $\sqrt{\det(-iZ)} = 1$ and then by analytic continuation, since $\mathscr{H}^n$ is simply connected.

If both sides of (16) are differentiated successively with respect to $z_{s_1}, z_{s_2}, \cdots$ as before the formulas become quite complicated, so henceforth we shall restrict ourselves to the case which finds immediate application in this paper. From now on we consider only $x, y \in \mathscr{M}$ and $V = \tau R$. Furthermore we write $\theta^{(s)}_{\mathscr{L}}[{}^x_y](z, \tau)$ in place of $\theta^{(s)}_{\mathscr{L}}[{}^x_y](z, \tau R)$ and $\theta^{(s)}_{\mathscr{L}}[{}^x_y](\tau)$ in place of $\theta^{(s)}_{\mathscr{L}}[{}^x_y](0, \tau)$. We have then — noting Proposition 1(iv) and (10) —

$$(17)\qquad \theta^{(s)}_{\mathscr{L}}\begin{bmatrix} x \\ y \end{bmatrix}(z, \tau) = (2\pi i)^l \sum_{\lambda\in\mathscr{L}} c^{(s)}(\lambda, x)\, e^{2\pi i(\lambda+x)\cdot(z+y) + \pi i\tau\|\lambda+x\|^2}$$

and (16) specializes to — using Proposition 1(iv) and Proposition 2(i) —

$$(18)\qquad \theta_{\mathscr{L}}\begin{bmatrix} x \\ y \end{bmatrix}\left(z, -\frac{1}{\tau}\right) = e^{2\pi i x\cdot y + \pi i\tau R[z]}\sqrt{\frac{(-i\tau)^n}{|D(\mathscr{L})|}}\,\theta_{\mathscr{L}^*}\begin{bmatrix} y \\ -x \end{bmatrix}(\tau Rz, \tau).$$

The linear transformation $z \to z' = Rz$ permutes the coordinates of z. Carrying over this permutation to the indices $1, \cdots, n$ we set $k' = k$, $1 \leqq k \leqq r_1$, $k' = k + r_2$, $r_1 + 1 \leqq k \leqq r_1 + r_2$, and $k' = k - r_2$, $r_1 + r_2 + 1 \leqq k \leqq n$. Then the kth coordinate of z' is $z'_k = z_{k'}$, $(k')' = k$, the j, k entry of R is $R_{j,k} = \delta_{jk'}$ (Kronecker δ), $R[z] = \sum_{k=1}^n z_k z_{k'}$ and $(\partial/\partial z_k)R[z] = 2z_{k'}$. For the moment let us write (18) as $F(z) = A(z)B(z)$ where $F(z)$ is the left side,

$$A(z)=\sqrt{\frac{(-i\tau)^n}{|D(\mathscr{L})|}}\,e^{2\pi i x\cdot y}e^{\pi i\tau R[z]}\quad\text{and}\quad B(z)=C(\tau Rz)$$

where $C(z)=\theta_{\mathscr{L}^*}[{}^{\;y}_{-x}](z,\tau)$. Then $(\partial A/\partial z_k)(z)=2\pi i\tau z_{k'}A(z)$, $(\partial B/\partial z_k)(z)=\tau(\partial C/\partial z_{k'})(\tau Rz)$ and $(\partial F/\partial z_k)(z)=2\pi i\tau z_{k'}A(z)B(z)+A(z)\tau(\partial C/\partial z_{k'})(\tau Rz)$. A second differentiation with respect to z_j then yields

$$\frac{\partial^2 F}{\partial z_k\partial z_j}(z)=2\pi i\tau\frac{\partial z_{k'}}{\partial z_j}A(z)B(z)+2\pi i\tau z_{k'}\frac{\partial}{\partial z_j}(A(z)B(z))$$
$$+2\pi i\tau^2 z_{j'}A(z)\frac{\partial C}{\partial z_{k'}}(\tau Rz)+A(z)\tau^2\frac{\partial^2 C}{\partial z_{k'}\partial z_{j'}}(\tau Rz).$$

In the formula for $\partial F/\partial z_k$ we see that setting $z=0$ leaves only one nonzero term on the right side, the one on the extreme right. The same is true for $\partial^2 F/\partial z_k\partial z_j$ provided $\partial z_{k'}/\partial z_j=0$, i.e., $k'\neq j$. We thus define a sequence $s=(s_1,s_2,\cdots,s_l)$ to be admissible if for every k which occurs as a term of the sequence k' does not occur as another term of the sequence. For example, if $n=3$, $r_1=r_2=1$, the sequences $(2,1,2,2)$, $(3,3,3)$ are admissible while $(1,2,3)$ and $(1,2,1)$ are not. Note that every subsequence of an admissible sequence is admissible (including by convention the empty sequence of length 0) and that if s is admissible so is $s'=(s_1',s_2',\cdots,s_l')$. Clearly if $r_2=0$ an admissible s must have $l\leqq n$ while if $r_2>0$, l can be arbitrarily large. An inductive argument now shows that if $s=(s_1,\cdots,s_l)$ is an admissible sequence then

$$\frac{\partial^l F}{\partial z_{s_1}\cdots\partial z_{s_l}}(z)=\Sigma+A(z)\tau^l\frac{\partial^l C}{\partial z_{s_1'}\cdots\partial z_{s_l'}}(\tau Rz)$$

where Σ is a sum of terms each having some z_j as a factor so that $z=0$ gives $\Sigma=0$. It follows that on differentiating (18) l times and setting $z=0$ we get

$$\text{(19)}\qquad \theta_{\mathscr{L}}^{(s)}\begin{bmatrix}x\\y\end{bmatrix}\left(-\frac{1}{\tau}\right)=e^{2\pi i x\cdot y}\sqrt{\frac{(-i\tau)^n}{|D(\mathscr{L})|}}\,\tau^l\theta_{\mathscr{L}^*}^{(s')}\begin{bmatrix}y\\-x\end{bmatrix}(\tau).$$

We now have to be explicit about the square root. We make the convention that for any complex number $b\neq 0$, $\arg b$ is that value of the argument satisfying $-\pi<\arg b\leqq\pi$, $\log b=\log|b|+i\arg b$ and $b^c=e^{c\log b}$.

PROPOSITION 5. *Let $\mathscr{L}$ be a lattice in $\mathscr{M}$, $x,y,\in\mathscr{M}$, and s an admissible sequence of length $l\geqq 0$.*

$$\text{(i)}\quad \theta_{\mathscr{L}}^{(s)}\begin{bmatrix}x\\y\end{bmatrix}\left(-\frac{1}{\tau}\right)=e^{2\pi i x\cdot y}\frac{(-i)^{n/2}}{\sqrt{|D(\mathscr{L})|}}\,\tau^{n/2+l}\theta_{\mathscr{L}^*}^{(s')}\begin{bmatrix}y\\-x\end{bmatrix}(\tau).$$

(ii) $\theta^{(s)}_{\bar{\mathscr{L}}}\begin{bmatrix} x \\ y \end{bmatrix}(\tau) = \theta^{(s')}_{\mathscr{L}}\begin{bmatrix} \bar{x} \\ \bar{y} \end{bmatrix}(\tau)$.

Proof. In (19) let $s = (0)$, $x = y = 0$ and obtain

$$\theta_{\mathscr{L}}\begin{bmatrix} 0 \\ 0 \end{bmatrix}\left(-\frac{1}{\tau}\right) = \sqrt{\frac{(-i\tau)^n}{|D(\mathscr{L})|}}\,\theta_{\mathscr{L}^*}\begin{bmatrix} 0 \\ 0 \end{bmatrix}(\tau)$$

which for $\tau = i$ becomes

$$\sum_{\lambda \in \mathscr{L}} e^{-\pi \|\lambda\|^2} = \sqrt{\frac{1}{|D(\mathscr{L})|}} \sum_{\lambda \in \mathscr{L}} e^{-\pi \|\lambda\|^2}.$$

As both series are sums of positive terms we see that $f(\tau) = \sqrt{(-i\tau)^n / |D(\mathscr{L})|}$ is the unique analytic function of $\tau \in \mathscr{H}$ whose square is $f(\tau)^2$ and satisfies $f(i) > 0$. According to our conventions $(-i)^{n/2}\tau^{n/2}/\sqrt{|D(\mathscr{L})|}$ has these properties, hence is $f(\tau)$, which proves (i). If Λ is a basic matrix for $\mathscr{L}$ then $\bar{\Lambda} = R\Lambda$ is basic for $\bar{\mathscr{L}}$ so that in Proposition 4(iii) we can take $W = R$ and (ii) then follows from (12) with $z = 0$, $V = \tau R$.

Keeping the hypotheses as in the above proposition let us further assume that $\mathscr{L}$ is an even lattice, $L = L(\mathscr{L})$, $\Delta = \Delta(L)$ as defined in Proposition 3. We define

$$\mathscr{J} = L\bar{\mathscr{L}}^* \quad \text{and} \quad J = \mathscr{J}/\mathscr{L}. \tag{20}$$

J is a finite abelian group of order Δ whose elements are cosets $\alpha + \mathscr{L}$, $\alpha \in \mathscr{J}$. Allowing a slight abuse of language we also speak of the element $\alpha \in J$ meaning the coset $\alpha + \mathscr{L}$. Also, for $\alpha, \beta \in \mathscr{J}$ or, more generally, $\alpha, \beta \in \mathscr{M}$ we write $\alpha \equiv \beta \bmod \mathscr{L}$ for $\alpha - \beta \in \mathscr{L}$. Now $\mathscr{L}^* = (1/L)\bar{\mathscr{J}}$ so application of (13) and Proposition 5(ii) shows that Proposition 5(i) can be written

$$\theta^{(s)}_{\mathscr{L}}\begin{bmatrix} x \\ y \end{bmatrix}\left(-\frac{1}{\tau}\right) = e^{2\pi i x \cdot y}\frac{(-i)^{n/2}}{\sqrt{|D(\mathscr{L})|}}\frac{\tau^{n/2+l}}{L^l}\theta^{(s)}_{\mathscr{J}}\begin{bmatrix} L\bar{y} \\ -(1/L)\bar{x} \end{bmatrix}(\tau/L^2). \tag{21}$$

By Proposition 4(ii),

$$\theta^{(s)}_{\mathscr{J}}\begin{bmatrix} L\bar{y} \\ -(1/L)\bar{x} \end{bmatrix}(\tau/L^2) = \sum_{\beta \in J}\theta^{(s)}_{\mathscr{L}}\begin{bmatrix} L\bar{y}+\beta \\ -(1/L)\bar{x} \end{bmatrix}(\tau/L^2),$$

the sum over $\beta \in J$ meaning that β ranges over a set of coset representatives of $\mathscr{J} \bmod \mathscr{L}$. Putting this in (21), then replacing τ by $L^2\tau$, recalling $|D(\mathscr{L})| = L^n\Delta$, a slight manipulation yields

$$\frac{\theta^{(s)}_{\mathscr{L}}\begin{bmatrix} x \\ y \end{bmatrix}(-1/(L^2\tau))}{(L\tau)^{n/2+l}} = e^{2\pi i x \cdot y}\frac{(-i)^{n/2}}{\sqrt{\Delta}}\sum_{\beta \in J}\theta^{(s)}_{\mathscr{L}}\begin{bmatrix} L\bar{y}+\beta \\ -(1/L)\bar{x} \end{bmatrix}(\tau). \tag{22}$$

We have now achieved that functions of the same type $\theta_{\mathscr{L}}^{(s)}$ appear on both sides of the equation. The reason for writing (22) with the extra power of $L\tau$ on the left will appear below. Now we consider the effect of replacing τ by $\tau + u/L$, $u \in Z$ in $\theta_{\mathscr{L}}^{(s)}[{}^{x}_{y}](\tau)$. The typical exponential term in (17), with $z = 0$, is then

$$e^{2\pi i(\lambda+x)\cdot y+\pi i\tau\|\lambda+x\|^2+\pi i(u/L)\|\lambda+x\|^2}.$$

But

$$e^{\pi i(u/L)\|\lambda+x|^2}=e^{\pi iu(\|\lambda\|^2/L)}e^{\pi i(u/L)\|x\|^2}e^{2\pi i\lambda\cdot(u\bar{x})/L}.$$

Since $\|\lambda\|^2/L$ is an even integer the first factor is 1. It is at this point that crucial use is made of the fact that $\mathscr{L}$ is even. The second factor is independent of λ and we can write

$$e^{2\pi i(\lambda+x)\cdot y+\pi i(\tau+(u/L))\|\lambda+x\|^2}=e^{-\pi i(u/L)\|x\|^2}e^{2\pi i(\lambda+x)\cdot(y+(u/L)\bar{x})+\pi i\tau\|\lambda+x\|^2}.$$

Finally,

$$\theta_{\mathscr{L}}^{(s)}\begin{bmatrix} x \\ y \end{bmatrix}(\tau+u/L)=e^{-\pi i(u/L)\|x\|^2}\theta_{\mathscr{L}}^{(s)}\begin{bmatrix} x \\ (u/L)\bar{x}+y \end{bmatrix}(\tau). \tag{23}$$

To put these formulas in proper perspective we recall briefly some notions from the theory of modular forms. Let $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}(2, \boldsymbol{R})$, the group of real 2×2 matrices of determinant one, $f = f(\tau)$ a function of $\tau \in \mathscr{H}$ and let $w \in \boldsymbol{C}$. The 'stroke operator' of weight (or degree) w is defined by

$$f \underset{w}{|}_M(\tau)=\frac{f(M\tau)}{(c\tau+d)^w},\quad M\tau=M(\tau)=\frac{a\tau+b}{c\tau+d}. \tag{24}$$

$(c\tau + d)^w$ is defined by our general convention on powers. Note that $c\tau + d$ is never zero and $\arg(c\tau + d)$ is a continuous function of τ in $\mathscr{H}$. For fixed w we write simply $f|_M$ in place of $f \underset{w}{|}_M$. For fixed w and $M f \rightarrow f|_M$ is linear in f and if f is analytic so is $f|_M$. If $M_k = \begin{pmatrix} a_k & b_k \\ c_k & d_k \end{pmatrix}$, $k = 1, 2$, and $M = M_1M_2$ then

$$(c\tau+d)=(c_1(M_2\tau)+d_1)(c_2\tau+d_2),\quad f|_M=v(M_1,M_2)(f|_{M_1})|_{M_2} \tag{25}$$

where

$$v(M_1,M_2)=v_w(M_1,M_2)=\frac{(c_1(M_2\tau)+d_1)^w(c_2\tau+d_2)^w}{(c\tau+d)^w}.$$

We claim that v depends only on w, M_1, M_2 but is constant in τ. In fact, by the first equation of (25) and properties of the argument,

$$\arg(c\tau + d) = \arg(c_1(M_2\tau) + d_1) + \arg(c_2\tau + d_2) + 2\pi k \tag{26}$$

where k is an integer depending on M_1, M_2 and continuous in τ, whence it is a constant in τ. Thus $k = k(M_1, M_2)$ can be computed by using any particular convenient value $\tau = \tau_0$ in (26). It follows from (26) that

$$v_w(M_1, M_2) = e^{-2\pi i k w}, \quad k = k(M_1, M_2). \tag{27}$$

In particular, $v_w = 1$ if $w \in \boldsymbol{Z}$, $v_w = v_{w'}$ if $w - w' \in \boldsymbol{Z}$ and $f|_{M_1M_2} = f|_{M_1}|_{M_2}$ if $w \in \boldsymbol{Z}$. Actually we shall always have $2w \in \boldsymbol{Z}$ so that $v_w = \pm 1$ in our applications.

The (homogeneous) modular group $\Gamma = \mathrm{SL}(2, \boldsymbol{Z})$ is the group of all $M \in \mathrm{SL}(2, \boldsymbol{R})$ whose coefficients a, b, c, d, are integers. The inhomogeneous modular group is the corresponding group of Möbius transformations $\tau \to M(\tau)$. It is well known that Γ is generated by $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$, $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. With E the 2×2 identity matrix, we have $S^2 = -E$, $S^3 = S^{-1}$, $S^4 = E$, $(ST)^3 = -E$, $T^u = \begin{pmatrix} 1 & u \\ 0 & 1 \end{pmatrix}$, $u \in \boldsymbol{Z}$. It is easily seen from (26) and (27) that for all $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}(2, \boldsymbol{R})$

$$k(M, T^u) = k(T^u, M) = 0, \quad k(M, S) = \begin{cases} -1 & \text{if } c \geqq 0,\ d < 0 \\ 0 & \text{otherwise} \end{cases} \tag{28}$$

Thus for any w, $v_w(M, T^u) = v_w(T^u, M) = v_w(M, S) = 1$ except in case $c \geqq 0$, $d < 0$ where $v_w(M, S) = e^{2\pi i w}$.

For any real $r > 0$ and $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL(2, \boldsymbol{R})$ let

$$M_{(r)} = \begin{pmatrix} a & b/r \\ rc & d \end{pmatrix} \in \mathrm{SL}(2, \boldsymbol{R}); M \to M_{(r)}$$

is an automorphism of $\mathrm{SL}(2, \boldsymbol{R})$. Then one has

$$k(M_{1(r)}, M_{2(r)}) = k(M_1, M_2), \quad v_w(M_{1(r)}, M_{2(r)}) = v_w(M_1, M_2). \tag{29}$$

We now observe that using the stroke operator of weight $n/2 + l$ equations (22) and (23) can be written upon suppressing the τ as functional equations

$$\theta_{\mathscr{L}}^{(s)}\begin{bmatrix} x \\ y \end{bmatrix}\Bigg|_M = e^{\pi i v(x, y, M)} \sum_{\beta \in J} t(M, \beta)\theta_{\mathscr{L}}^{(s)}\begin{bmatrix} ax + c\bar{y} + \beta \\ b\bar{x} + dy \end{bmatrix} \tag{30}$$

where $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ is $S_{(L)}$ or $T^u_{(L)}$, $\nu(x, y, S_{(L)}) = 2x \cdot y$, $\nu(x, y, T^u_{(L)}) = -(u/L)\| x \|^2$, $t(S_{(L)}, \beta) = (-i)^{n/2}/\sqrt{\Delta}$ for all β and $t(T^u_{(L)}, \beta) = 0$ or 1 according as $\beta \not\equiv 0 \bmod \mathcal{L}$ or $\beta \equiv 0 \bmod \mathcal{L}$. Since every $M \in \Gamma$ can be expressed in terms of S and T the same is true for every $M \in \Gamma_{(L)}$ in terms of $S_{(L)}$ and $T_{(L)}$ and successive applications of (30) should yield a formula for every $M \in \Gamma_{(L)}$. The question is what are the $\nu(x, y, M)$ and the $t(M, \beta)$. Suitable experimentation leads one to introduce the following notions. For $(x, y) \in \mathcal{M} \times \mathcal{M}$, $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}(2, \boldsymbol{R})$ define

$$(x, y) \circ M = (ax + c\bar{y},\ b\bar{x} + dy). \tag{31}$$

This is clearly an $\boldsymbol{R}$-linear action on $\mathcal{M} \times \mathcal{M}$, but more interesting is that it is a group action, as is easily checked:

$$(x, y) \circ M_1 M_2 = ((x, y) \circ M_1) \circ M_2. \tag{32}$$

Now with $(X, Y) = (x, y) \circ M$ define

$$\nu(x, y, M) = x \cdot y - X \cdot Y = -ab\| x \|^2 - cd\| y \|^2 - 2bc\, x \cdot y \tag{33}$$

where we have used $ad - bc = 1$. Note that for $M = S_{(L)}$ or $T^u_{(L)}$ this $\nu(x, y, M)$ coincides with that used in (30) above. $\nu(x, y, M)$ satisfies a 'cocycle' condition:

$$\nu(x, y, M_1 M_2) = \nu(x, y, M_1) + \nu((x, y) \circ M_1, M_2). \tag{34}$$

The proof is easy: let $(X, Y) = (x, y) \circ M_1$, $(\xi, \eta) = (X, Y) \circ M_2 = (x, y) \circ M_1 M_2$ by (32), then $\nu(x, y, M_1 M_2) = x \cdot y - \xi \cdot \eta = (x \cdot y - X \cdot Y) + (X \cdot Y - \xi \cdot \eta) = \nu(x, y, M_1) + \nu((x, y) \circ M_1, M_2)$. We now state our basic theorem using the terminology and results developed above.

THEOREM 1. *Let $\mathcal{L}$ be an even lattice in $\mathcal{M}$. For each $M \in \Gamma_{(L)}$ there is a complex valued function $t(M)$ defined on J such that for every $x, y \in \mathcal{M}$ and admissible sequence s*

$$\theta^{(s)}_{\mathcal{L}}\begin{bmatrix} x \\ y \end{bmatrix}\Bigg|_M = e^{\pi i \nu(x, y, M)} \sum_{\beta \in J} t(M, \beta)\, \theta^{(s)}_{\mathcal{L}}\begin{bmatrix} ax + c\bar{y} + \beta \\ b\bar{x} + dy \end{bmatrix}.$$

NOTE. We write $t(M, \beta)$ for the value of the function $t(M)$ at β rather than $t(M)(\beta)$.

PROOF. We already know the result is true for $M = S_{(L)}$, $T^u_{(L)}$ so the theorem will be proven if we show that whenever the result holds for $M_k =$

$\begin{pmatrix} a_k & b_k \\ c_k & d_k \end{pmatrix} \in \Gamma_{(L)}$, $k = 1, 2$ then it holds for $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} = M_1 M_2$ also. Let $v = v(M_1, M_2) = v_{n/2}(M_1, M_2)$, $(X, Y) = (x, y) \circ M_1$, $(\xi, \eta) = (X, Y) \circ M_2 = (x, y) \circ M$; then

$$\begin{aligned} \theta_{\mathscr{L}}^{(s)} \begin{bmatrix} x \\ y \end{bmatrix} \Bigg|_M &= v \theta_{\mathscr{L}}^{(s)} \begin{bmatrix} x \\ y \end{bmatrix} \Bigg|_{M_1} \Bigg|_{M_2} \\ &= v e^{\pi i \nu(x, y, M_1)} \sum_{\beta \in J} t(M_1, \beta)\, \theta_{\mathscr{L}}^{(s)} \begin{bmatrix} X + \beta \\ Y \end{bmatrix} \Bigg|_{M_2} \\ &= v e^{\pi i \nu(x, y, M_1)} \sum_{\alpha, \beta \in J} e^{\pi i \nu(X + \beta, Y, M_2)} t(M_1, \beta) t(M_2, \alpha)\, \theta_{\mathscr{L}}^{(s)} \begin{bmatrix} a_2(X + \beta) + c_2 \bar{Y} + \alpha \\ b_2(\bar{X} + \bar{\beta}) + d_2 Y \end{bmatrix}. \end{aligned}$$

A little calculation shows

$$\nu(X + \beta, Y, M_2) = \nu(X, Y, M_2) - 2a_1 b_2 X \cdot \bar{\beta} - 2b_2 c_2 Y \cdot \beta - a_2 b_2 \| \beta \|^2.$$

Furthermore since $M_2 \in \Gamma_{(L)}$, $Lb_2 \in \boldsymbol{Z}$ and $\beta \in \mathscr{J} = L\bar{\mathscr{L}}^*$ whence $b_2 \bar{\beta} \in \mathscr{L}^*$ so that the term $b_2 \bar{\beta}$ can be removed from the bottom of the characteristic by Proposition 4(i) introducing an exponential factor. Finally collecting terms,

$$\begin{aligned} \theta_{\mathscr{L}}^{(s)} \begin{bmatrix} x \\ y \end{bmatrix} \Bigg|_M = v e^{\pi i \nu(x, y, M)} \sum_{\alpha, \beta \in J} t(M_1, \beta) t(M_2, \alpha) \exp(\pi i a_2 b_2 \| \beta \|^2 \\ + 2\pi i b_2 \beta \cdot \bar{\alpha})\, \theta_{\mathscr{L}}^{(s)} \begin{bmatrix} \xi + a_2 \beta + \alpha \\ \eta \end{bmatrix}. \end{aligned}$$

Since in the last characteristic all that matters is $a_2 \beta + \alpha \bmod \mathscr{L}$ the formula can be rewritten as

$$\theta_{\mathscr{L}}^{(s)} \begin{bmatrix} x \\ y \end{bmatrix} \Bigg|_M = e^{\pi i \nu(x, y, M)} \sum_{\gamma \in J} t(M, \gamma)\, \theta_{\mathscr{L}}^{(s)} \begin{bmatrix} ax + c\bar{y} + \gamma \\ b\bar{x} + dy \end{bmatrix}$$

with

$$t(M, \gamma) = v(M_1, M_2) \sum\nolimits^* t(M_1, \beta) t(M_2, \alpha) \exp(\pi i a_2 b_2 \| \beta \|^2 + 2\pi i b_2 \beta \cdot \bar{\alpha}) \tag{35}$$

where Σ^* is the sum over all ordered pairs (β, α) in $J \times J$ such that $a_2 \beta + \alpha \equiv \gamma \bmod \mathscr{L}$. This completes the proof.

The function $t(M)$ — which we consider simultaneously as a function on J and as a function on $\mathscr{J}$ constant on cosets of $\mathscr{L}$ — is not necessarily uniquely determined, for $M \in \Gamma_{(L)}$ does not have a unique expression as a word in $S_{(L)}$ and $T_{(L)}$ and furthermore, the functions $\theta_{\mathscr{L}}^{(s)}[{}^{x+\beta}_{\ y}](\tau)$, $\beta \in J$, are not necessarily linearly independent for fixed x, y. Thus $t(M)$ is potentially a multi-valued symbol but this will not matter as long as we take it to mean any $t(M)$ obtained by expressing M as a word in $S_{(L)}$ and $T_{(L)}$ and iterating, using (35) and the initial values of $t(S_{(L)})$, $t(T^u_{(L)})$ given after (30). Theorem 1 involves the group $\Gamma_{(L)}$ which depends on $\mathscr{L}$ while it would be preferable to have the single fixed group Γ. This can be achieved by a change of variable in τ (but then unfortunately L's begin to proliferate in the formulas). It is easily verified that if $f, f_1, \cdots, f_N$ are functions of τ and $f\,|_{M_{(L)}} = \Sigma_{k=1}^{N} c_k f_k$, for certain constants c_k, then the functions $g(\tau) = f(\tau/L)$, $g_1(\tau) = f_1(\tau/L), \cdots$ satisfy $g\,|_M = \Sigma_{k=1}^{N} c_k g_k$. Thus, writing the matrices $M \in \Gamma_{(L)}$ as $M_{(L)}$, $M \in \Gamma$, and noting (29), we can reformulate the theorem as follows, along with a summary of the basic formulas.

THEOREM 1'. *Let $\mathscr{L}$ be an even lattice in $\mathscr{M}$ and define the functions*

$$\psi^{(s)}_{\mathscr{L}}\begin{bmatrix} x \\ y \end{bmatrix}(\tau) = \theta^{(s)}_{\mathscr{L}}\begin{bmatrix} x \\ y \end{bmatrix}\left(\frac{\tau}{L}\right). \tag{36}$$

For each $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$ there is a complex valued function $t(M)$ on J such that for any $x, y \in \mathscr{M}$ and admissible sequence s,

$$\psi^{(s)}_{\mathscr{L}}\begin{bmatrix} x \\ y \end{bmatrix}\Bigg|_M = e^{\pi i \nu(x, y, M_{(L)})} \sum_{\beta \in J} t(M, \beta) \psi^{(s)}_{\mathscr{L}}\begin{bmatrix} ax + Lc\bar{y} + \beta \\ \dfrac{b}{L}\bar{x} + dy \end{bmatrix}. \tag{37}$$

$\nu(x, y, M_{(L)}) = -(ab/L)\| x \|^2 - Lcd \| y \|^2 - 2bcx \cdot y$. The $t(M)$ satisfy: $t(S, \beta) = (-i)^{n/2}/\sqrt{\Delta}$ for all β, $t(T^u, \beta) = 1$ if $\beta \equiv 0 \mod \mathscr{L}$ and $t(T^u, \beta) = 0$ if $\beta \not\equiv 0 \mod \mathscr{L}$, and

$$t(M_1 M_2, \gamma) = v(M_1, M_2) \sum{}^{*}\, t(M_1, \beta) t(M_2, \alpha) \times \exp\left(\pi i\left(\frac{a_2 b_2}{L}\right)\| \beta \|^2 + 2\pi i\left(\frac{b_2}{L}\right)\beta \cdot \bar{\alpha}\right), \tag{38}$$

the sum being over all $(\beta, \alpha) \in J \times J$ such that $a_2\beta + \alpha \equiv \gamma \mod \mathscr{L}$ and $v(M_1, M_2) = v_{n/2}(M_1, M_2)$.

3. Evaluation of $t(M)$

The problem at hand is to find an explicit expression for $t(M, \beta)$. Considering (38) suggests introducing

$$\Phi(\alpha) = e^{(\pi i/L)\| \alpha \|^2}, \quad \Omega(\alpha, \beta) = e^{(2\pi i/L)\alpha \cdot \bar{\beta}}$$

for $\alpha, \beta \in \mathscr{J}$. (Note: this Φ has nothing to do with the matrix Φ of Section 1).

PROPOSITION 6.

i) $\Omega(\alpha,\beta)=\Omega(\beta,\alpha)$, $\Phi(\alpha+\beta)=\Phi(\alpha)\Phi(\beta)\Omega(\alpha,\beta)$;

ii) $\Omega(\alpha_1+\alpha_2,\beta)=\Omega(\alpha_1,\beta)\Omega(\alpha_2,\beta)$;

iii) *$\Phi(\alpha)$ and $\Omega(\alpha,\beta)$ depend only on α and β* $\bmod \mathscr{L}$.

Thus they define functions (still denoted) Φ and Ω on J and $J\times J$ respectively;

iv) *for each $\beta\in J$ the function $\alpha\to\Omega(\alpha,\beta)$ is a character of J, call it χ_β. The mapping $\beta\to\chi_\beta$ is an isomorphism of J onto its character group $\hat{J}$.*

PROOF. (i) and (ii) are clear. If $\lambda\in\mathscr{L}$, $\|\lambda\|^2\equiv 0 \bmod 2L$ so that $\Phi(\lambda)=1$ and $(1/L)\lambda\cdot\bar{\beta}=\lambda\cdot(\bar{\beta}/L)\in Z$, since $(\bar{\beta}/L)\in\mathscr{L}^*$, so that $\Omega(\lambda,\beta)=1$. (i), (ii) then give $\Phi(\alpha+\lambda)=\Phi(\alpha)$ and $\Omega(\alpha+\lambda,\beta)=\Omega(\alpha,\beta)=\Omega(\alpha,\beta+\lambda)$ which is (iii). It is now clear that χ_β is a character and $\beta\to\chi_\beta$ is a homomorphism. As both J and $\hat{J}$ are finite groups of order Δ to show this is an isomorphism it suffices to prove that if χ_β is the identity character — i.e., $\chi_\beta(\alpha)=1$ for all α — then $\beta\equiv 0 \bmod \mathscr{L}$. But if $\beta\not\equiv 0 \bmod\mathscr{L}$ then $\beta\notin\mathscr{L}=(\mathscr{L}^*)^*$ so there is some $\mu\in\mathscr{L}^*$ such that $\beta\cdot\mu\notin Z$, or, with $\alpha=L\bar{\mu}$, $\alpha\in\mathscr{J}$ and $(1/L)\beta\cdot\bar{\alpha}\notin Z$, hence $\chi_\beta(\alpha)=\Omega(\alpha,\beta)\neq 1$.

COROLLARY. *Let $\alpha,\beta\in J$. If the order of α is a and the order of β is b and $c=(a,b)$ then $\Omega(\alpha,\beta)$ is a cth root of unity. Furthermore there is some $\gamma\in J$ such that $\Omega(\alpha,\gamma)$ is a primitive ath root of unity — in which case the order of γ is a multiple of a.*

This follows from standard results of the character theory of finite abelian groups.

Again, let $\beta\in J$ have order b so that $\Omega(\beta,\beta)$ is a bth root of unity. Then $\Phi(\beta)^2=\Omega(\beta,\beta)$ whence $\Phi(\beta)$ is a $2b$th root of unity. Now we have the crucial fact that:

(39) If $\beta\in J$ has odd order b then $\Phi(\beta)$ is a bth root of unity.

PROOF. $\Phi(\beta)=\exp((\pi i/L)\|\beta\|^2)$ so we must show $(1/L)\|\beta\|^2=2w/b$ for some integer w. But on the one hand $(1/L)\|\beta\|^2=(1/b)(b\beta\cdot(\bar{\beta}/L))\in(1/b)\mathscr{L}$. $\mathscr{L}^*=(1/b)Z$ so $(1/L)\|\beta\|^2=(u/b)$ for some integer u, while on the other hand $(1/L)\|\beta\|^2=(1/b^2L)\|b\beta\|^2=(1/b^2L)2Lv$ for some integer v, since $\lambda=b\beta\in\mathscr{L}$ and $\|\lambda\|^2\equiv 0 \bmod 2L$. Thus $(1/L)\|\beta\|^2=u/b=2v/b^2$, $u=2v/b$ and since b is odd, $b\mid v$, $u=2w$ where $w=v/b$.

A noteworthy corollary is

(40) *If $\beta\in J$ has odd order b and $\Omega(\beta,\beta)$ is a primitive bth root of unity then so is $\Phi(\beta)$.*

Returning now to (38) let $M_2 = T^u$ so $t(M_2, \alpha) = 0$ unless $\alpha \equiv 0 \bmod \mathcal{L}$, $a_2 = 1$, $b_2 = u$ and noting the remark after (28) we obtain

$$t(M_1T^u, \gamma) = t(M_1, \gamma)\exp(\pi i(u/L)\|\gamma\|^2) = t(M_1, \gamma)\Phi^u(\gamma).$$

In a similar way we deduce $t(T^uM_2, \gamma) = t(M_2, \gamma)$ and

$$t(M_1, S, \gamma) = v(M_1, S)\frac{(-i)^{n/2}}{\sqrt{\Delta}}\sum_{\beta \in J} t(M_1, \beta)\exp(-(2\pi i/L)\beta \cdot \bar{\gamma})$$

$$= v(M_1, S)\frac{(-i)^{n/2}}{\sqrt{\Delta}}\sum_{\beta \in J} t(M_1, \beta)\bar{\Omega}(\beta, \gamma).$$

It is interesting to observe that this last formula can be understood as a Fourier transform in the context of finite abelian groups. We digress a bit to discuss the situation in general.

Let A be a finite abelian group (under addition) of order N. Furthermore suppose there is on A a function W pairing A with its character group $\hat{A}$ as our Ω above. That is, we assume given $W: A \times A \to C$ such that $W(x, y) = W(y, x) \neq 0$ for all $x, y \in A$ and for each $y \in A$, $x \to W(x, y)$ is a character of A, call it χ_y such that $y \to \chi_y$ is an isomorphism of A onto $\hat{A}$. Let $F = F(A)$ be the set of all complex valued functions on A. Clearly F is an N dimensional complex vector space and can be made into a Hilbert space with the inner product $(f, g) = (1/N)\Sigma_{x\in A}f(x)\overline{g(x)}$. The norm of f is then $\|f\|^2 = (1/N)\Sigma_{x\in A}|f(x)|^2$. The character relation $(\chi, \chi') = (1/N)\Sigma_{x\in A}\chi(x)\overline{\chi'(x)} = 1$ or 0 according as $\chi = \chi'$ or $\chi \neq \chi'$ shows that $\{\chi\}_{x\in \hat{A}}$ is an orthonormal basis for F. Every $f \in F$ then has a 'Fourier expansion' $f = \Sigma_{\chi\in\hat{A}}c_\chi\chi$ with $c_\chi = (f, \chi)$. The function $\hat{f}$ on $\hat{A}$ defined by $\hat{f}(\chi) = \sqrt{N}(f, \chi)$ is the Fourier transform of f. The factor $\sqrt{N}$ will appear to be a convenient normalization. In our case with the above identification of $\hat{A}$ with A via W, $\hat{f}$ can be considered as a function on A. Then $\hat{f}(y) = \sqrt{N}(f, \chi_y) = (1/\sqrt{N})\Sigma_{x\in A}f(x)\bar{W}(x, y)$. The following are easy to prove: (a) $f \to \hat{f}$ is an isometry of F, i.e., $(\hat{f}, \hat{g}) = (f, g)$ for all $f, g \in F$, in particular $\|\hat{f}\| = \|f\|$; (b) if $h \in F$ and $|h(x)| = 1$ for all $x \in A$ then $f \to fh$ is an isometry of F, $(fh, gh) = (f, g)$ and $\|fh\| = \|f\|$; (c) if f is an even function, i.e. $f(-x) = f(x)$ for all $x \in A$, then so is $\hat{f}$.

In particular, reverting to our case where $A = J$, $W = \Omega$, $N = \Delta$, we see that the formulas obtained before the above paragraph can be stated in terms of the $t(M) \in F(J)$ as

(41) $t(T^uM) = t(M)$, $\quad t(MT^u) = t(M)\Phi^u$, $\quad t(MS) = v(M, S)(-i)^{n/2}\widehat{t(M)}$.

It is easily verified that $t(T^u)$, $t(S)$ are even functions with norm $1/\sqrt{\Delta}$ in $F(J)$, Φ^u is even, $|\Phi^u(\beta)| = 1$ and $|v(M,S)(-i)^{n/2}| = 1$. Hence our discussion shows that, considering the $t(M)$ as elements of $F(J)$:

$$\text{(42)} \qquad \text{for all } M \in \Gamma,\ t(M) \text{ is an even function and } \|t(M)\| = \frac{1}{\sqrt{\Delta}}.$$

We see that $t(M)$ is computed from the given $t(T^u)$ and $t(S)$ by successively multiplying by a function and taking the Fourier transform. Looking again first at the general case with A, W as before let $f_1, f_2, \cdots$ be functions in $F(A)$, $c_0, c_1, \cdots$ constants and define $g_0 = c_0$, $g_r = c_r\widehat{g_{r-1}f_r}$ for $r = 1, 2, \cdots$. Then

$$g_r(y) = \frac{c_r}{\sqrt{N}} \sum_{x \in A} g_{r-1}(x) f_r(x) \bar{W}(x, y).$$

Inserting the similar expression for $g_{r-1}(x)$ in this sum, continuing this way, we eventually get an r-fold sum

$$\text{(43)} \quad g_r(y) = \frac{c_0 c_1 \cdots c_r}{(\sqrt{N})^r} \sum_{x_1, \cdots, x_r \in A} f_1(x_1) \cdots f_r(x_r) \bar{W}(x_1, x_2) \cdots \bar{W}(x_{r-1}, x_r) \bar{W}(x_r, y).$$

$W(x, y)$ is like an inner product on A except that its values are in the multiplicative group of nonzero complex numbers rather than the additive group of all complex numbers. Nevertheless one can mimic the procedure of choosing an orthonormal basis. We say x is orthogonal to y (in A, with respect to W) if $W(x, y) = 1$ and two subsets B, C of A are orthogonal if $W(x, y) = 1$ for all $x \in B$, $y \in C$. We indicate orthogonality by the usual symbol $x \perp y$, $B \perp C$. We first observe that if the orders of x and y are relatively prime then $x \perp y$. From this it follows that if $A = \bigoplus_{p \mid N} A^{(p)}$ is the decomposition of A as the direct sum of its p Sylow subgroups then this is an orthogonal decomposition, each $A^{(p)}$ is orthogonal to all the others. Each $A^{(p)}$ is a direct sum of cyclic groups (each having order a power of p) but these in general are not uniquely determined. If $A = B \oplus C$ and the subgroups B and C are orthogonal then W restricted to $B \times B$ is seen to be a pairing of B with its character group $\hat{B}$ with the same properties as postulated for W on A. Thus for each prime p we restrict W to $A^{(p)}$ and deduce that for each $x \in A^{(p)}$ of order p^e there is some $y \in A^{(p)}$ such that $W(x, y)$ is a primitive $p^{e\text{th}}$ root of unity. Let p^{e_1} be the maximum of the orders of the elements of $A^{(p)}$. We claim that if $p \neq 2$ then for some $x \in A^{(p)}$, $W(x, x)$ is a primitive $p^{e_1\text{th}}$ root of unity. For, choose some $y \in A^{(p)}$ of order p^{e_1} and then $z \in A^{(p)}$ such that $W(y, z)$ is a primitive $p^{e_1\text{th}}$ root of unity. Then the order of z must also be p^{e_1}, by the maximum condition on p^{e_1}. Now if $w = y + z$

we have $W(y,z)^2 = W(w,w)\bar{W}(y,y)\bar{W}(z,z)$. If $p \neq 2$, $W(y,z)^2$ is also a primitive p^{e_1}th root of unity while the three numbers on the right side are p^{e_1}th roots of unity, hence for x equal to one of y, z or w, $W(x,x)$ must be a primitive p^{e_1}th root of unity. Now let $B = \{y \in A^{(p)}: W(x,y) = 1\}$, i.e., B is the kernel of the character χ_x. Then $A^{(p)}$ is the direct sum of $\langle x \rangle$, the cyclic group of order p^{e_1} generated by x, and B; and this sum is orthogonal, $A^{(p)} = \langle x \rangle \oplus B$, $x \perp B$. Then restricting W to B we can split off in the same way a cyclic orthogonal direct summand of maximal order in B. Continuing in this way we obtain finally the analogue of an orthonormal basis. Explicitly — and to fix notation —

$$\text{for} \quad p \neq 2, \; A^{(p)} = \langle \alpha^{(p,1)} \rangle \oplus \cdots \oplus \langle \alpha^{(p,h)} \rangle \tag{44}$$

where each cyclic group $\langle \alpha^{(p,i)} \rangle$ is orthogonal to all the others and $W(\alpha^{(p,i)}, \alpha^{(p,i)})$ is a primitive p^{e_i}th root of unity, where p^{e_i} is the order of $\alpha^{(p,i)}$. Furthermore, $e_1 \geqq e_2 \geqq \cdots \geqq e_h \geqq 1$, $h = h_p$, $e_1 = e_1(p)$ are invariants of $A^{(p)}$ and A.

Note that the cyclic groups occurring in (44) are still not necessarily uniquely determined. Also, the assumption $p \neq 2$ was essential in our proof and an easy example shows the result can fail for $p = 2$. Take $A = \boldsymbol{Z}_2 \oplus \boldsymbol{Z}_2$, so $A = A^{(2)}$, each $x \in A$ is $x = (x_1, x_2)$, $x_1, x_2 = 0$ or 1. Define $W(x,y) = (-1)^{x_1y_2 + x_2y_1}$. Then $W(x,x) = 1$ for all x and no orthonormal basis as in (44) exists. Thus $p = 2$ needs an individual treatment in any particular case.

Reverting to (43) the r-fold sum can be simplified using an orthogonal decomposition of A provided some assumption is made on the functions f_i. In our applications each f_i is of the form Φ^u ($u \in \boldsymbol{Z}$) on J and we observe that if $\Omega(\alpha,\beta) = 1$ then by Proposition 6(i), $\Phi^u(\alpha+\beta) = \Phi^u(\alpha)\Phi^u(\beta)$. Thus let us assume that each f_i is a W-function. A W-function — for lack of a better name — is an $f \in F(A)$ such that $f(x+y) = f(x)f(y)$ whenever $x \perp y$. Thus $\Phi^u \in F(J)$ is an Ω-function. For each $p \mid N$, let N_p be the order $A^{(p)}$, this being the highest power of p dividing N and $N = \Pi_{p \mid N} N_p$. Each $x \in A$ has a unique expression as $x = \Sigma_{p \mid N} x^{(p)}$, $x^{(p)} \in A^{(p)}$. For any W-function f, $f(x) = \Pi_p f(x^{(p)})$ and $W(x,y) = \Pi_p W(x^{(p)}, y^{(p)})$ — p always ranging over primes dividing N. Using such a decomposition for each x_i ranging over A in (43) along with the distributive law we obtain

$$\begin{aligned} g_r(y) &= (c_0 c_1 \cdots c_r) \prod_p g_r^{(p)}(y) \\ g_r^{(p)}(y) &= \frac{1}{(\sqrt{N_p})^r} \sum_{\substack{x_i^{(p)} \in A^{(p)} \\ i = 1, 2, \cdots, r}} f_1(x_r^{(p)}) \cdots f_r(x_r^{(p)}) \bar{W}(x_1^{(p)}, x_2^{(p)}) \cdots \bar{W}(x_r^{(p)}, y^{(p)}). \end{aligned} \tag{45}$$

For any p such that $A^{(p)}$ has an orthonormal basis as in (44) — which includes all $p \neq 2$ — we have $N_p = \Pi_{j=1}^{h_p} p^{e_j}$, and each $x^{(p)} \in A^{(p)}$ has a unique expression $x^{(p)} = \Sigma_{j=1}^{h} x^{(p,j)}$, $x^{(p,j)} \in \langle \alpha^{(p,j)} \rangle$. The elements of this cyclic group are $k\alpha^{(p,j)}$, k running over a complete set of residues $\bmod p^{e_j}$. Arguing as before we deduce that if $y^{(p)} = \Sigma_{j=1}^{h} k^{(p,j)} \alpha^{(p,j)}$ then

$$g_r^{(p)}(y) = \prod_{j=1}^{h} g_r^{(p,j)}(y) \tag{46}$$

$$g_r^{(p,j)}(y) = \frac{1}{(\sqrt{p^{e_j}})^r} \sum_{k_1, \cdots, k_r \bmod p^{e_j}} f_1(k_1\alpha^{(p,j)}) \cdots f_r(k_r\alpha^{(p,j)}) \times \bar{W}^{k_1 k_2 + \cdots + k_r k^{(p,j)}}(\alpha^{(p,j)}, \alpha^{(p,j)}).$$

We now return to the case $A = J$, $N = \Delta$, $W = \Omega$. Let $r \geqq 1$, $u_1, \cdots, u_r \in \boldsymbol{Z}$ and set $M = M(u_1, \cdots, u_r) = ST^{u_1}S \cdots T^{u_r}S$. There are r powers of T and $r + 1$ S's. Let $c_0 = (-i)^{n/2}/\sqrt{\Delta}$, $c_j = v(ST^{u_1} \cdots ST^{u_j}, S)(-i)^{n/2}$, $f_j = \Phi^{u_j}$, $j = 1, 2, \cdots, r$, then by (41) $g_0 = c_0 = t(S)$, $g_1 = c_1\widehat{g_0 f_1}, \cdots, g_r = c_r\widehat{g_{r-1} f_r}$ gives $g_r = t(M)$. Let

$$v(u_1, \cdots, u_r) = \prod_{j=1}^{r} v(ST^{u_1} \cdots ST^{u_j}, S), \tag{47}$$

$\Delta = \Pi_{p|\Delta} \Delta_p$, Δ_p being the highest power of p dividing Δ, and for $p \neq 2$ let $J^{(p)} = \bigoplus_{j=1}^{h_p} \langle \alpha^{(p,j)} \rangle$ be the orthogonal decomposition for $J^{(p)}$ as in (44) with the notation used there. By (40) each $\Phi(\alpha^{(p,j)})$ is a primitive p^{e_j}th root of unity, say

$$\zeta_{p,j} = \exp(2\pi i w^{(p,j)}/p^{e_j}) \quad \text{where} \quad \frac{1}{L}\|\alpha^{(p,j)}\|^2 = \frac{2w^{(p,j)}}{p^{e_j}}. \tag{48}$$

Equations (45) and (46), taking into account the nature of c_0, imply, for $M = M(u_1, \cdots, u_r)$, $\beta \in J$,

$$t(M, \beta) = v(u_1, \cdots, u_r)(-i)^{(n/2)(r+1)} \prod_{p|\Delta} t^{(p)}(M, \beta) \tag{49}$$

$$t^{(p)}(M, \beta) = \frac{1}{(\sqrt{\Delta_p})^{r+1}} \sum_{\alpha_1, \cdots, \alpha_r \in J^{(p)}} \Phi^{u_1}(\alpha_1) \cdots \Phi^{u_r}(\alpha_r) \bar{\Omega}(\alpha_1, \alpha_2) \cdots \bar{\Omega}(\alpha_r, \beta^{(p)})$$

and for $p \neq 2$, $t^{(p)}(M, \beta) = \Pi_{j=1}^{h_p} t^{(p,j)}(M, \beta)$

$$t^{(p,j)}(M, \beta) = \frac{1}{(\sqrt{p^{e_j}})^{r+1}} \sum_{k_1, \cdots, k_r \bmod p^{e_j}} \zeta_{p,j}^{u_1 k_1^2 + \cdots + u_r k_r^2 - 2k_1 k_2 \cdots - 2k_r k^{(p,j)}}$$

where $\beta^{(p)}$ is the component of β in $J^{(p)}$ and $k^{(p,j)}\alpha^{(p,j)}$ the component of $\beta^{(p)}$ in $\langle \alpha^{(p,j)} \rangle$.

The sum in the formula for $t^{(p,j)}(M,\beta)$ is like a Gaussian sum but its evaluation is not immediately obvious. Let m be a positive odd integer, $\zeta = e^{2\pi i w/m}$ a primitive mth root of unity, $u_1, \cdots, u_r, k$ a sequence of integers and define

$$G(u_1, \cdots, u_r, k, \zeta) = \sum_{k_1, \cdots, k_r \bmod m} \zeta^{u_1 k_1^2 + \cdots + u_r k_r^2 - 2k_1 k_2 - \cdots - 2k_r k}. \tag{50}$$

The sum in (49) is of this type with $m = p^{e_j}$, $\zeta = \zeta_{p,j}$, $w = w^{(p,j)}$ and $k = k^{(p,j)}$. Before giving the evaluation of G we need some more notation. Let $B_0 = 1$, $B_1 = u_1$ and for $j \geqq 2$ $B_j = u_j B_{j-1} - B_{j-2}$, let $d_j = (B_j, m)$, $j = 0, 1, 2, \cdots$ and define B'_j by $B'_j B_j \equiv d_j \bmod m$. This last equation has at least one solution mod m and it may have more, in any case B'_j is any solution, it will not matter. Note that $M(u_1, \cdots, u_j) = \begin{pmatrix} * & * \\ B_j & -B_{j-1} \end{pmatrix}$ for $j = 1, 2, \cdots$. This is true for $j = 1$ and if true for $j \geqq 1$ then

$$M(u_1, \cdots, u_j, u_{j+1}) = \begin{pmatrix} * & * \\ B_j & -B_{j-1} \end{pmatrix} \begin{pmatrix} u_{j+1} & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} * & * \\ B_{j+1} & -B_j \end{pmatrix}.$$

In particular $(B_j, B_{j-1}) = 1 = (d_j, d_{j-1})$ always.

THEOREM 2. *Let $G = G(u_1, \cdots, u_r, k, \zeta)$. With the above notation*

$$G = 0 \textit{ if } d_r \nmid k \textit{ and if } d_r \mid k \textit{ then} \tag{51}$$

$$G = (\sqrt{m})^r \sqrt{d_r} \left(\frac{w}{m}\right)^r \left(\frac{w}{d_r}\right) \eta_r \zeta^{-d_r B_{r-1} B'_r (k/d_r)^2}.$$

The symbols $\left(\dfrac{w}{m}\right)$, $\left(\dfrac{w}{d_r}\right)$

are Jacobi symbols and $\eta_r = \eta(u_1, \cdots, u_r, m)$ is a fourth root of unity not depending on w or k whose value is given below in (52).

PROOF. By induction. Take first $r = 1$ and to simplify we momentarily drop the subscript 1. Consider then

$$G(u, k, \zeta) = \sum_{j \bmod m} \zeta^{uj^2 - 2jk}$$

and let $d = (u, m)$. If $d = 1$ let $u'u \equiv 1 \bmod m$, write $uj^2 - 2jk \equiv u(j^2 - 2u'jk) \equiv u(j - u'k)^2 - u'k^2 \bmod m$ and as j goes over a set of residues mod m so does

$j - u'k$. Thus $G(u,k,\zeta) = G(1,0,\zeta^{u'})\zeta^{-u'k^2}$. The classical result on the Gaussian sum is that if $z = e^{2\pi i a/m}$ is a primitive mth root of unity, m odd, then

$$G(1,0,z) = \sum_{j \bmod m} z^{j^2} \quad \text{is} \quad \sqrt{m}\left(\frac{a}{m}\right)\varepsilon(m) \quad \text{where} \quad \varepsilon(m) = \sqrt{(-1)^{(m-1)/2}}$$

which is 1 if $m \equiv 1 \pmod 4$ and i if $m \equiv 3 \pmod 4$. So

$$G(u,k,\zeta) = \sqrt{m}\left(\frac{w}{m}\right)\eta_1\zeta^{-u'k^2} \quad \text{where} \quad \eta_1 = \left(\frac{u}{m}\right)\varepsilon(m).$$

Say now $(u,m) = d > 1$. Set $u = du_0$, $m = dm_0$, $(u_0,m_0) = 1$ and as $j \bmod m$ take $j \equiv hm_0 + f$, $h \bmod d$, $f \bmod m_0$. Then

$$G(u,k,\zeta) = \sum_{\substack{h \bmod d \\ f \bmod m_0}} \zeta^{u(hm_0+f)^2 - 2(hm_0+f)k} = \sum_{f \bmod m_0} \zeta^{uf^2-2fk} \sum_{h \bmod d} \zeta^{-2m_0kh}$$

since $um_0 \equiv 0 \bmod m$. With $z = \zeta^{-2m_0k}$ which is a dth root of unity the inner sum is $\Sigma_{h \bmod d} z^h$ which is 0 unless $z = 1$ where its value is d. But $z = 1$ if and only if $2m_0k \equiv 0 \bmod m$ and since m is odd this is exactly when $k \equiv 0 \bmod d$. Thus $G(u,k,\zeta) = 0$ if $d \nmid k$ while if $d \mid k$ let $k = dk_0$ so $G(u,k,\zeta) = d\,\Sigma_{f \bmod m_0}\zeta^{uf^2-2fk} = dG(u_0,k_0,\zeta^d)$. ζ^d is a primitive m_0th root of unity and $(u_0,m_0) = 1$ so by our initial result

$$dG(u_0,k_0,\zeta^d) = d\sqrt{m_0}\left(\frac{w}{m_0}\right)\eta_1(\zeta^d)^{-u_0'k_0^2}$$

where $\quad u_0'u_0 \equiv 1 \bmod m_0 \quad$ and $\quad \eta_1 = \left(\frac{u_0}{m_0}\right)\varepsilon(m_0)$.

Now $d\sqrt{m_0} = d\sqrt{m/d} = \sqrt{m}\sqrt{d}$ and $(\zeta^d)^{-u_0'k_0^2} = \zeta^{-du'(k/d)^2}$ where $u'u \equiv d \bmod m$. Also

$$\left(\frac{w}{m_0}\right) = \left(\frac{w}{m/d}\right) = \left(\frac{w}{m}\right)\left(\frac{w}{d}\right),$$

a fact about the Jacobi symbol that we shall frequently use. We see now that (51) is true for $r = 1$ and

$$\eta_1 = \eta(u,m) = \left(\frac{u_0}{m_0}\right)\varepsilon(m_0) = \left(\frac{u/d}{m/d}\right)\varepsilon\left(\frac{m}{d}\right).$$

Suppose now that the theorem is true for positive integers $\leqq r$ where r is a positive integer and that furthermore

$$(52)\qquad \eta_r = \eta(u_1,\cdots,u_r,m) = \prod_{j=1}^{r}\left(\frac{B_{j-1}/d_{j-1}}{m/(d_{j-1}d_j)}\right)\left(\frac{B_j/d_j}{m/(d_{j-1}d_j)}\right)\varepsilon\left(\frac{m}{d_{j-1}d_j}\right),$$

this coinciding with the result obtained for η_1 above. Consider

$$G(u_1,\cdots,u_r,u_{r+1},k,\zeta) = \sum_{j \bmod m} \zeta^{u_{r+1}j^2-2jk}G(u_1,\cdots,u_r,j,\zeta).$$

By the induction hypothesis the inner sum is 0 unless $j \equiv 0 \bmod d_r$ whereupon writing $j \equiv d_rh$, $h \bmod m/d_r$ we obtain

$$G(u_1,\cdots,u_r,u_{r+1},k,\zeta) = (\sqrt{m})^r\sqrt{d_r}\left(\frac{w}{m}\right)^r\left(\frac{w}{d_r}\right)\eta_r \sum_{h \bmod (m/d_r)} (\zeta^{d_r})^{u_{r+1}d_rh^2-2hk-B_{r-1}B'_rh^2}$$
$$= CG(u_{r+1}d_r - B_{r-1}B'_r,k,\zeta^{d_r})$$

where C is the product of the terms to the left of the summation. Let $U = u_{r+1}d_r - B_{r-1}B'_r$, $z = \zeta^{d_r}$ so by our initial result for $r=1$ $G(U,k,z)$ is 0 unless $d = (U, m/d_r)$ divides k where

$$G(U,k,z) = \sqrt{m/d_r}\sqrt{d}\left(\frac{w}{m/d_r}\right)\left(\frac{w}{d}\right)\eta(U,m/d_r)(\zeta^{d_r})^{-dU'(k/d)^2}$$

Here

$$U'U \equiv d \bmod m/d_r \quad\text{and}\quad \eta(U,m/d_r) = \left(\frac{U/d}{m/(d_rd)}\right)\varepsilon\left(\frac{m}{d_rd}\right).$$

Now by definition $B'_r(B_r/d_r) \equiv 1 \bmod m/d_r$ so

$$U \equiv B'_r(B_r/d_r)U \equiv B'_rB_ru_{r+1} - B_{r-1}B'_r \bmod m/d_r \equiv B'_rB_{r+1}$$

by definition of $B_{r+1} = u_{r+1}B_r - B_{r-1}$. Then $d = (U, m/d_r) = (B'_rB_{r+1}, m/d_r) = (B_{r+1}, m/d_r)$ (since $(B'_r, m/d_r) = 1) = (B_{r+1}, m)$ (since $(B_{r+1}, d_r) = 1) = d_{r+1}$. Thus we have $U \equiv B'_rB_{r+1} \bmod m/d_r$, $d = d_{r+1}$ so

$$U/d \equiv B'_rB_{r+1}/d_{r+1} \bmod m/(d_rd_{r+1}),$$

$$\left(\frac{U/d}{m/(d_rd)}\right) = \left(\frac{B'_r}{m/(d_rd_{r+1})}\right)\left(\frac{B_{r+1}/d_{r+1}}{m/(d_rd_{r+1})}\right) \quad\text{and}\quad \left(\frac{B'_r}{m/(d_rd_{r+1})}\right) = \left(\frac{B_r/d_r}{m/(d_rd_{r+1})}\right)$$

since $B'_rB_r/d_r \equiv 1 \bmod m/d_r$, a fortiori $\bmod m/(d_rd_{r+1})$. Finally U' is a number satisfying $U'U/d_{r+1} \equiv 1 \bmod m/(d_rd_{r+1})$ but

$$(B'_{r+1}(B_r/d_r))U/d_{r+1} \equiv B'_{r+1}(B_r/d_r)B'_r(B_{r+1}/d_{r+1}) \equiv 1 \bmod m/(d_rd_{r+1})$$

so one can take $U' \equiv B'_{r+1}(B_r/d_r) \bmod m/(d_rd_{r+1})$ and then $d_rd_{r+1}U' \equiv$

$d_{r+1}B_rB'_{r+1} \bmod m$. Putting these values into the above formula for $G(U, k, z)$ and noting the value of C the proof is finished.

The proof also shows that (52) is indeed the correct formula for η_r. Let us try to simplify it. Employing the appropriate multiplicativity of the Jacobi symbol in both numerator and denominator the first factor in the jth term of (52) can be expressed as

$$\left(\frac{B_{j-1}/d_{j-1}}{m/(d_{j-1}d_j)}\right)=\left(\frac{B_{j-1}/d_{j-1}}{m/d_{j-1}}\right)\left(\frac{B_{j-1}/d_{j-1}}{d_j}\right)=\left(\frac{B_{j-1}/d_{j-1}}{m/d_{j-1}}\right)\left(\frac{B_{j-1}}{d_j}\right)\left(\frac{d_{j-1}}{d_j}\right)$$

and a similar result holds for the second factor. Regrouping,

$$\eta_r=\prod_{j=1}^{r}\left(\frac{B_{j-1}/d_{j-1}}{m/d_{j-1}}\right)\left(\frac{B_j/d_j}{m/d_j}\right)\left(\frac{B_{j-1}}{d_j}\right)\left(\frac{B_j}{d_{j-1}}\right)\left(\frac{d_{j-1}}{d_j}\right)\left(\frac{d_j}{d_{j-1}}\right)\varepsilon\left(\frac{m}{d_{j-1}d_j}\right).$$

We see that each term $((B_{j-1}/d_{j-1})/(m/d_{j-1}))$ will occur twice, once in the $(j-1)$st and then in the jth term of the product, hence gives $(\pm 1)^2=1$, except for $((B_0/d_0)/(m/d_0))$ which occurs only in the first term, but has the value $(1/m)=1$ anyway, and the term $((B_r/d_r)/(m/d_r))$ which occurs only in the rth term. Also for $j\geqq 2$, $B_j=u_jB_{j-1}-B_{j-2}\equiv -B_{j-2} \bmod d_{j-1}$ so that

$$\left(\frac{B_j}{d_{j-1}}\right)=\left(\frac{-1}{d_{j-1}}\right)\left(\frac{B_{j-2}}{d_{j-1}}\right)\quad\text{for}\quad j=2,\cdots,r,$$

and this is true for $j=1$ also if we set $(B_{-1}/d_0)=1$. Thus

$$\eta_r=\left(\frac{B_r/d_r}{m/d_r}\right)\prod_{j=1}^{r}\left(\frac{B_{j-1}}{d_j}\right)\left(\frac{B_{j-2}}{d_{j-1}}\right)\left(\frac{-1}{d_{j-1}}\right)\left(\frac{d_{j-1}}{d_j}\right)\left(\frac{d_j}{d_{j-1}}\right)\varepsilon\left(\frac{m}{d_{j-1}d_j}\right)$$

$$=\left(\frac{B_r/d_r}{m/d_r}\right)\left(\frac{-B_{r-1}}{d_r}\right)\prod_{j=1}^{r}\left(\frac{-1}{d_j}\right)\left(\frac{d_{j-1}}{d_j}\right)\left(\frac{d_j}{d_{j-1}}\right)\varepsilon\left(\frac{m}{d_{j-1}d_j}\right).$$

By quadratic reciprocity

$$\left(\frac{-1}{d_j}\right)\left(\frac{d_{j-1}}{d_j}\right)\left(\frac{d_j}{d_{j-1}}\right)=1$$

except if $d_{j-1}\equiv 1\ (\mathrm{mod}\ 4)$ and $d_j\equiv 3\ (\mathrm{mod}\ 4)$ when it is -1. Also $\varepsilon(m/d_{j-1}d_j)=\varepsilon(m)$ if $d_{j-1}d_j\equiv 1\ (\mathrm{mod}\ 4)$ and $=\varepsilon(-m)$ if $d_{j-1}d_j\equiv 3\ (\mathrm{mod}\ 4)$. Hence

$$\left(\frac{-1}{d_j}\right)\left(\frac{d_{j-1}}{d_j}\right)\left(\frac{d_j}{d_{j-1}}\right)\varepsilon\left(\frac{m}{d_{j-1}d_j}\right)=\varepsilon(m)$$

if $d_{j-1}\equiv d_j\ (\mathrm{mod}\ 4)$, $=\varepsilon(-m)$ if $d_{j-1}\equiv 3$, $d_j\equiv 1\ (\mathrm{mod}\ 4)$ and $=-\varepsilon(-m)$ if $d_{j-1}\equiv 1$, $d_j\equiv 3\ (\mathrm{mod}\ 4)$. Thus

$$\eta_r = \left(\frac{B_r / d_r}{m / d_r}\right)\left(\frac{-B_{r-1}}{d_r}\right)\varepsilon(m)^a \varepsilon(-m)^b(-\varepsilon(-m))^c \tag{53}$$

where a is the number of j, $1 \leqq j \leqq r$, such that $d_{j-1} \equiv d_j \pmod 4$, b the number of j such that $d_{j-1} \equiv 3$, $d_j \equiv 1 \pmod 4$ and c is the number of j where $d_{j-1} \equiv 1$, $d_j \equiv 3 \pmod 4$. Clearly $a + b + c = r$.

In our applications we shall have m a power of an odd prime. Assuming this so, since $(d_{j-1}, d_j) = 1$ and d_{j-1}, d_j divide m one of d_{j-1}, d_j is always 1, so if for some j, $d_j \equiv 3 \pmod 4$ then $d_{j-1} \equiv d_{j+1} \equiv 1 \pmod 4$. Let $j_1, \cdots, j_c$ be those indices j in $1, \cdots, r$ where $d_j \equiv 3 \pmod 4$; then $j_1 + 1 < j_2, j_2 + 1 < j_3, \cdots, c$ thus having the same meaning as in the previous paragraph. The corresponding b indices are $j_1 + 1, j_2 + 1, \cdots, j_{c-1} + 1$, and also $j_c + 1$ if $j_c < r$, i.e., $b = c - 1$ if $d_r \equiv 3 \pmod 4$ and $b = c$ if $d_r \equiv 1 \pmod 4$, $a = r - b - c$ is $r - 2c + 1$, $r - 2c$, respectively. A little calculation yields $\varepsilon(m)^a \varepsilon(-m)^b(-\varepsilon(-m))^c = \varepsilon(m)^{r+1} / \varepsilon(d_r m)$ in all cases. Thus for $m = p^e$, $p \neq 2$,

$$\eta_r = \left(\frac{B_r / d_r}{m / d_r}\right)\left(\frac{-B_{r-1}}{d_r}\right)\frac{\varepsilon(m)^{r+1}}{\varepsilon(d_r m)}. \tag{54}$$

After this diversion let us return to the modular group and the notation of (48) and (49). Note that every element of Γ has an expression as some $M(u_1, \cdots, u_r)$. For example, $E = M(0,0,0)$, $S = M(0,0,0,0)$, $T^u = M(0,u,0)$ and

$$M(u_1, \cdots, u_r) M(u_1', \cdots, u_r') = M(u_1, \cdots, u_r, 0, u_1', \cdots, u_r').$$

Given now $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$ fix a representation $M = M(u_1, \cdots, u_r) = \begin{pmatrix} * & * \\ B_r & -B_{r-1} \end{pmatrix}$ so $B_r = c$, $-B_{r-1} = d$. Applying Theorem 2 and (54) to the last equation of (49) with $m = p^{e_j}$ $(p \neq 2)$ and setting $c^{(p,j)} = (B_r, p^{e_j}) = (c, p^{e_j})$ in place of d_r, we deduce:

$$t^{(p,j)}(M, \beta) = 0 \quad \text{if} \quad c^{(p,j)} \nmid k^{(p,j)}$$

and

$$t^{(p,j)}(M, \beta) = \sqrt{\frac{c^{(p,j)}}{p^{e_j}}}\left(\frac{w^{(p,j)}}{p^{e_j}}\right)^r \left(\frac{w^{(p,j)}}{c^{(p,j)}}\right)\left(\frac{c / c^{(p,j)}}{p^{e_j} / c^{(p,j)}}\right)\left(\frac{d}{c^{(p,j)}}\right) \tag{55}$$
$$\times \frac{\varepsilon(p^{e_j})^{r+1}}{\varepsilon(c^{(p,j)} p^{e_j})} \zeta_{p,j}^{c^{(p,j)} d c' (k^{(p,j)} / c^{(p,j)})^2}$$

if $c^{(p,j)} \mid k^{(p,j)}$.

Here c' satisfies $c'c \equiv c^{(p,j)} \bmod p^{e_j}$.

Define $\Gamma(\mathscr{L})=\{M: t(M,\beta)=0 \text{ for all } \beta\not\equiv 0 \bmod \mathscr{L}\}$. Define the function $\chi=\chi_{\mathscr{L}}$ on $\Gamma(\mathscr{L})$ by $\chi_{\mathscr{L}}(M)=t(M,0)$. Since $\|t(M)\|=1/\sqrt{\Delta}$ it is clear that $|\chi(M)|=1$. Note that $T^u\in\Gamma(\mathscr{L})$ and $\chi(T^u)=1$. (38) with $M_1=M\in\Gamma(\mathscr{L})$ and $M_2=M^{-1}$ shows that $M^{-1}\in\Gamma(\mathscr{L})$ also. Furthermore if $M_1, M_2\in\Gamma(\mathscr{L})$, $M_1M_2\in\Gamma(\mathscr{L})$ also and $\chi(M_1M_2)=v(M_1,M_2)\chi(M_1)\chi(M_2)$.Thus $\Gamma(\mathscr{L})$ is a subgroup of Γ and χ is almost a character of $\Gamma(\mathscr{L})$ except for the factor $v(M_1,M_2)=\pm 1$. If n is even then $v(M_1,M_2)=1$ always and in this case χ is a character of $\Gamma(\mathscr{L})$. (38) shows in general that if $M'=M_0M$, $M_0\in\Gamma(\mathscr{L})$, then

$$t(M')=v(M_0,M)\chi(M_0)t(M). \tag{56}$$

If $\mathscr{L}$ has Δ odd — we have remarked in (5) that n is then even — we can identify $\Gamma(\mathscr{L})$ and the character $\chi_{\mathscr{L}}$.

Theorem 3. *Suppose the even lattice $\mathscr{L}$ has Δ odd and n even. Set $\Delta_1=\Pi_{p\mid\Delta}p^{e_1}$, the least positive integer such that $\Delta_1\mathscr{J}\subset\mathscr{L}$. Then $\Gamma(\mathscr{L})$ is*

$$\Gamma_0(\Delta_1)=\left\{M=\begin{pmatrix} a & b\\ c & d\end{pmatrix}:\ c\equiv \bmod \Delta_1\right\}$$

and $\chi_{\mathscr{L}}$ is the character of $\Gamma_0(\Delta_1)$ given by $\chi_{\mathscr{L}}(M)=(d/\Delta)$.

Proof. It is clear that Δ_1 has the stated property as p^{e_1} is the maximum of the orders of elements of $J^{(p)}$ and $J=\bigoplus_{p\mid\Delta}J^{(p)}$. Note that $\Delta_1\mid\Delta$, uses the same primes as Δ and $\Delta_1=\Delta$ if and only if J is cyclic. Say $M=\begin{pmatrix} a & b\\ c & d\end{pmatrix}\in\Gamma_0(\Delta_1)$; then $c\equiv 0 \bmod p^{e_j}$ for all p and j and (55) shows that $t^{(p,j)}(M,\beta)=0$ unless $k^{(p,j)}\equiv 0 \bmod p^{e_j}$. By (49), $t(M,\beta)=(-i)^{(n/2)(r+1)}\Pi_{p,j}t^{(p,j)}(M,\beta)$ is then 0 unless the component $\beta^{(p,j)}$ of β in the cyclic group $\langle\alpha^{(p,j)}\rangle$ is 0 for all p,j, i.e., $t(M,\beta)=0$ unless $\beta=0$ in J. This shows $\Gamma_0(\Delta_1)\subset\Gamma(\mathscr{L})$. On the other hand, if $M\notin\Gamma_0(\Delta_1)$ then for some $p, c\not\equiv 0 \bmod p^{e_1}$, $c^{(p,j)}\mid p^{e_1-1}$ and the element $\beta=p^{e_1-1}\alpha^{(p,1)}\not\equiv 0 \bmod \mathscr{L}$. But clearly by (49) and (55) $t(M,\beta)\neq 0$ so $M\notin\Gamma(\mathscr{L})$. Thus $\Gamma(\mathscr{L})=\Gamma_0(\Delta_1)$. Now returning to $M\in\Gamma_0(\Delta_1)$ let us compute $\chi(M)=t(M,0)=(-i)^{(n/2)(r+1)}\Pi_{p\mid\Delta}\Pi_{j=1}^{h_p}t^{(p,j)}(M,0)$. By (55), since now $c^{(p,j)}=p^{e_j}$,

$$t^{(p,j)}(M,0)=\left(\frac{d}{p^{e_j}}\right)\left(\frac{w^{(p,j)}}{p^{e_j}}\right)^{r+1}\varepsilon(p^{e_j})^{r+1}.$$

Define

$$W=W(\mathscr{L})=\prod_{p\mid\Delta}\prod_{j=1}^{h_p}\left(\frac{w^{(p,j)}}{p^{e_j}}\right),\quad \varepsilon=\varepsilon(\mathscr{L})=\prod_{p\mid\Delta}\prod_{j=1}^{h_p}\varepsilon(p^{e_j}). \tag{57}$$

It is not immediately apparent that W is an invariant of $\mathscr{L}$ since it depends on the orthogonal basis chosen in each $J^{(p)}$ but we shall express W in terms of ε which is clearly an invariant of $\mathscr{L}$ which shows W is also. We have now that

$$\chi(M) = \left(\frac{d}{\Delta}\right)((-i)^{n/2} W\varepsilon)^{r+1}$$

and the proof will be complete if we show that

$$(-i)^{n/2} W\varepsilon = 1\,, \tag{58}$$

the promised fundamental relation between W, ε and n. Consider the element $M = -E = ST^0S = M(0) \in \Gamma_0(\Delta_1)$ so that our above formulas give

$$\chi(-E) = \left(\frac{-1}{\Delta}\right)((-i)^{n/2} W\varepsilon)^2 = \left(\frac{-1}{\Delta}\right)(-i)^n\varepsilon^2$$

since $W = \pm 1$, $W^2 = 1$. On the other hand for any function $f(\tau)$,

$$f \underset{n/2}{|}_{-E} = (-1)^{n/2} f$$

by definition of the stroke operator. Thus $\psi_{\mathscr{L}}\left[\begin{smallmatrix}0\\0\end{smallmatrix}\right]|_{-E} = (-1)^{n/2}\psi_{\mathscr{L}}\left[\begin{smallmatrix}0\\0\end{smallmatrix}\right]$, but $\psi_{\mathscr{L}}\left[\begin{smallmatrix}0\\0\end{smallmatrix}\right]|_{-E} = \chi(-E)\psi_{\mathscr{L}}\left[\begin{smallmatrix}0\\0\end{smallmatrix}\right]$ by Theorem 1′ and the definition of $\chi(-E) = t(-E, 0)$. So we have $\chi(-E) = (-1)^{n/2}$ which upon comparison with the previous expression for $\chi(-E)$ gives

$$\left(\frac{-1}{\Delta}\right)\varepsilon^2 = 1\,. \tag{59}$$

Next consider $M = \begin{pmatrix} -1 & 1 \\ 0 & -1 \end{pmatrix} = STSTS = M(1,1) \in \Gamma_0(\Delta_1)$. Then

$$\chi(M) = \left(\frac{-1}{\Delta}\right)((-i)^{n/2} W\varepsilon)^3 = (-i)^{3n/2} W\varepsilon\,,$$

where we have made use of (59). But $M = (-E)T^{-1}$ so that $\chi(M) = \chi(-E)\chi(T^{-1}) = \chi(-E) = (-1)^{n/2}$.

Comparing the two values for $\chi(M)$ gives (58) and the proof is finished.

COROLLARY. *The following table relates n, Δ, W and ε:*

(60)

n mod 8	Δ mod 4	W
0	1	ε
2	3	$-i\varepsilon$
4	1	$-\varepsilon$
6	3	$i\varepsilon$

Proof. Since $W = W^{-1} = \pm 1$ (58) shows $W = (-i)^{n/2}\varepsilon$ which is the last column. Squaring, $1 = W^2 = (-1)^{n/2}\varepsilon^2$ and (59) show $(-1)^{n/2} = (-1/\Delta) = (-1)^{(\Delta-1)/2}$ which is the middle column.

Note that $\varepsilon = i^H$ where H is the number of cyclic summands of J of order p^e with $p \equiv 3 \bmod 4$ and e odd. W has a much more complicated definition and the above relation between them was unexpected. The character $\chi_{\mathscr{L}}$ is identically one only in case Δ is a square.

Keeping from now on $\mathscr{L}$ as in Theorem 3, Theorem 1′ yields: if $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(\Delta_1)$, then for every $x, y \in \mathscr{M}$ and admissible sequence s,

$$\psi_{\mathscr{L}}^{(s)}\begin{bmatrix} x \\ y \end{bmatrix}\Bigg|_M = \exp(\pi i \nu(x, y, M_{(L)})\left(\frac{d}{\Delta}\right)\psi_{\mathscr{L}}^{(s)}\begin{bmatrix} ax + Lc\bar{y} \\ (b/L)\bar{x} + dy \end{bmatrix}. \tag{61}$$

For any $M \in \Gamma$ we can compute $t(M)$ via (56) if it has been computed for a set of coset representatives of the right cosets of $\Gamma \bmod \Gamma_0(\Delta_1)$. It can be shown that these may be chosen of the form E, ST^k and ST^kST^j for suitable integers k and j. By (41) and $t(S,\beta) = (-i)^{n/2}/\sqrt{\Delta}$ we have $t(ST^k) = ((-i)^{n/2}/\sqrt{\Delta})\Phi^k$ and $t(ST^kST^j) = t(ST^kS)\Phi^j$ so one has only to compute $t(ST^kS)$ which can be done using (49) and (55). It is precisely in this computation that something must be known about the $w^{(p,j)}$. However, if $\Delta_1 = p$ this situation does not arise and the calculations simplify. $\Delta_1 = p$ if and only if $\Delta = p^h$ and J is a direct sum of cyclic groups each of order p, i.e., J is an elementary abelian p group. It is easy to see that $[\Gamma : \Gamma_0(p)] = p + 1$ and $\Gamma = \Gamma_0(p) \cup (\bigcup_k \Gamma_0(p)ST^k)$, k going over a complete set of residues $\bmod p$. In fact, if $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \notin \Gamma_0(p)$ then $M = M_0ST^k$ where $M_0 = \begin{pmatrix} ak - b & a \\ ck - d & c \end{pmatrix} \in \Gamma_0(p)$ where k satisfies $ck \equiv d \bmod p$, i.e., $k \equiv c^*d$, $c^*c \equiv 1 \bmod p$. $\chi(M_0) = (c/\Delta)$ and (56) shows

$$t(M,\beta) = (c/\Delta)t(ST^k,\beta) = (c/\Delta)((-i)^{n/2}/\sqrt{\Delta})\Phi^k(\beta).$$

Thus if $\Delta = p^h$, $\Delta_1 = p$ then for every $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ with $c \not\equiv 0 \bmod p$,

$$\begin{aligned} \psi_{\mathscr{L}}^{(s)}\begin{bmatrix} x \\ y \end{bmatrix}\Bigg|_M &= \exp(\pi i \nu(x, y, M_{(L)})\left(\frac{c}{\Delta}\right)\frac{(-i)^{n/2}}{\sqrt{\Delta}} \\ &\times \sum_{\beta \in J} \exp\left(\frac{\pi i c^* d}{L}\|\beta\|^2\right)\psi_{\mathscr{L}}^{(s)}\begin{bmatrix} ax + Lc\bar{y} + \beta \\ (b/L)\bar{x} + dy \end{bmatrix}. \end{aligned} \tag{62}$$

Equation (61) shows that $\psi^{(s)}_{\mathscr{L}}[{}^x_y](\tau)$ is in general not a modular form for $\Gamma_0(\Delta_1)$ since besides the multiplier the transformed function has a new characteristic. If certain algebraic conditions are put on x and y one does obtain modular forms for some subgroup of $\Gamma_0(\Delta_1)$.

Suppose m is a positive integer and $[{}^x_y]$ a characteristic with $x \in (1/m)\mathscr{J}$, $y \in (1/m)\mathscr{L}^*$. Since $\mathscr{J} = L\bar{\mathscr{L}}^*$ one has $(1/L)\bar{x} \in (1/m)\mathscr{L}^*$ and $L\bar{y} \in (1/m)\mathscr{J}$. Then for any $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$ and $\beta \in \mathscr{J}$ the characteristic

$$\begin{bmatrix} X \\ Y \end{bmatrix} = \begin{bmatrix} ax + Lc\bar{y} + \beta \\ (b/L)\bar{x} + dy \end{bmatrix}$$

has $X \in (1/m)\mathscr{J}$, $Y \in (1/m)\mathscr{L}^*$. Define $F^{(s)}(\mathscr{L}, m)$ as the space of functions $f(\tau)$ spanned by all complex linear combinations of $\psi^{(s)}_{\mathscr{L}}[{}^x_y](\tau)$ with $x \in (1/m)\mathscr{J}$, $y \in (1/m)\mathscr{L}^*$, (s) a fixed admissible sequence. By Theorem 1′, our above remarks and Proposition 4(i), it follows that $F^{(s)}(\mathscr{L}, m)$ is a finite dimensional, complex vector space and $f \to f|_M$ is an automorphism of $F^{(s)}(\mathscr{L}, m)$ for each $M \in \Gamma$, giving a representation of Γ by nonsingular linear transformations of $F^{(s)}(\mathscr{L}, m)$. Actually one obtains only a finite group of linear tranformations as there is a subgroup of finite index, say G, such that $f|_M = f$ for all $M \in G$. Thus the $f \in F^{(s)}(\mathscr{L}, m)$ are all modular forms of weight $(n/2) + l$ for G. Determination of the group G depends on algebraic properties of $\mathscr{L}$ and m but we can make a general summary as follows:

THEOREM 4. *Let $\mathscr{L}, \Delta$, n, Δ_1 be as in Theorem 3 and $F^{(s)}(\mathscr{L}, m)$ as defined above. Assigning to $M \in \Gamma$ the linear transformation $f \to f|_M$ of $F^{(s)}(\mathscr{L}, m)$ gives a representation of Γ by a finite group of linear transformations. The kernel of the representation $G^{(s)}(\mathscr{L}, m)$ is a normal subgroup of finite index in Γ. All $f \in F^{(s)}(\mathscr{L}, m)$ are modular forms of weight $(n/2) + l$ for $G^{(s)}(\mathscr{L}, m)$:*

$$f|_M = f, \quad M \in G^{(s)}(\mathscr{L}, m).$$

The group $G^{(s)}(\mathscr{L}, m)$ contains the principal congruence subgroup

$$\Gamma(m^2\Delta_1) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \operatorname{mod} m^2\Delta_1 \right\}.$$

PROOF. Clearly the kernel of the representation is a normal subgroup and everything follows if we show that $G^{(s)}(\mathscr{L}, m)$ contains $\Gamma(m^2\Delta_1)$ since this latter group has finite index. Now for $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(\Delta_1)$ we have (61), $\nu(x, y, M_{(L)})$ as in (37), $x = (1/m)\xi$ and $y = (1/Lm)\bar{\eta}$ with $\xi, \eta \in \mathscr{J}$. By (39),

$$\exp\left(\frac{\pi i}{L}\| \xi \|^2\right), \ \exp\left(\frac{\pi i}{L}\| \eta \|^2\right)$$

are Δ_1th roots of unity whence

$$\zeta_x = \exp\left(\frac{\pi i}{L}\| x \|^2\right) \quad \text{and} \quad \zeta_y = \exp(\pi i L \| y \|^2)$$

are $m^2\Delta_1$th roots of unity. Since $\Delta_1 \xi \cdot (\bar{\eta} / L) \in \mathscr{L} \cdot \mathscr{L}^* = \boldsymbol{Z}$, $\zeta_{x,y} = e^{2\pi i x \cdot y}$ is also an $m^2\Delta_1$th root of unity. Then

$$e^{\pi i \nu(x, y, M_{(L)})} = \zeta_x^{-ab} \zeta_y^{-cd} \zeta_{x,y}^{-bc}$$

is an $m^2\Delta_1$th root of unity. The transformed characteristic in (61) may be written as

$$\begin{bmatrix} x + (a-1)x + cL\bar{y} \\ y + (b/L)\bar{x} + (d-1)y \end{bmatrix} = \begin{bmatrix} x + \mu \\ y + \nu \end{bmatrix},$$

say. If $a - 1 \equiv c \equiv 0 \bmod m\Delta_1$ and $b \equiv d - 1 \equiv 0 \bmod m$ then $\mu \in \mathscr{L}$, $\nu \in \mathscr{L}^*$ and Proposition 4(i) gives

$$\begin{aligned} \psi_{\mathscr{L}}^{(s)}\begin{bmatrix} x + \mu \\ y + \nu \end{bmatrix} &= e^{2\pi i x \cdot \nu} \psi_{\mathscr{L}}^{(s)}\begin{bmatrix} x \\ y \end{bmatrix} \\ &= \zeta_x^{2b} \zeta_{x,y}^{d-1} \psi_{\mathscr{L}}^{(s)}\begin{bmatrix} x \\ y \end{bmatrix}. \end{aligned}$$

Note that our congruence condition along with $ad - bc = 1$ implies $d \equiv 1 \bmod m\Delta_1$. Let then $G(\Delta_1, m)$ be all those M satisfying $a - 1 \equiv d - 1 \equiv c \equiv 0 \bmod m\Delta_1$ and $b \equiv 0 \bmod m$. Clearly $G(\Delta_1, m)$ is a subgroup of Γ and is contained in $\Gamma_0(\Delta_1) \cap \Gamma(m)$. For all $M \in G(\Delta_1, m)$ we have now:

$$\psi_{\mathscr{L}}^{(s)}\begin{bmatrix} x \\ y \end{bmatrix}\Bigg|_M = \left(\frac{d}{\Delta}\right) \zeta_x^{(2-a)b} \zeta_y^{-cd} \zeta_{x,y}^{d-1-bc} \psi_{\mathscr{L}}^{(s)}\begin{bmatrix} x \\ y \end{bmatrix}.$$

Since Δ_1 and Δ have the same prime divisors $d \equiv 1 \bmod m\Delta_1$ implies $d \equiv 1 \bmod p$ for each $p \mid \Delta$ whence $(d/p) = 1$, $(d/\Delta) = 1$. As $(2-a)b = b + (1-a)b \equiv b \bmod m^2\Delta_1$, $cd = c + (d-1)c \equiv c \bmod m^2\Delta_1$, $bc \equiv 0 \bmod m^2\Delta_1$ and all the ζ's are $m^2\Delta_1$th roots of unity, the above equation becomes:

$$\psi_{\mathscr{L}}^{(s)}\begin{bmatrix} x \\ y \end{bmatrix}\Bigg|_M = \zeta_x^{b} \zeta_y^{-c} \zeta_{x,y}^{d-1} \psi_{\mathscr{L}}^{(s)}\begin{bmatrix} x \\ y \end{bmatrix}, \quad M \in G(\Delta_1, m). \tag{63}$$

If now $b \equiv c \equiv d - 1 \equiv 0 \bmod m^2\Delta_1$ all the powers of the ζ's are 1. Thus for all $M \in \Gamma(m^2\Delta_1)$, $\psi_{\mathscr{L}}^{(s)}[{}^x_y]|_M = \psi_{\mathscr{L}}^{(s)}[{}^x_y]$, as asserted.

4. Examples

Let K be an algebraic number field of degree n over the rational field $\boldsymbol{Q}$. An isomorphism σ of $K/\boldsymbol{Q}$ into $\boldsymbol{C}/\boldsymbol{Q}$ is called real if $\sigma(K)\subset\boldsymbol{R}$ and otherwise complex. If σ is complex then $\bar{\sigma}$ given by $\bar{\sigma}(\alpha)=\overline{\sigma(\alpha)}$, $\alpha\in K$, is an isomorphism distinct from σ. It follows — as K has n distinct isomorphisms — that these can be arranged as $\sigma_1,\cdots,\sigma_n$ with $\sigma_1,\cdots,\sigma_{r_1}$ real and the remaining $2r_2$ complex with $\sigma_{r_1+r_2+k}=\bar{\sigma}_{r_1+k}$, $1\leqq k\leqq r_2$. r_1, r_2 are nonnegative integers and $r_1+2r_2=n$. The map $\sigma\colon K\to\mathcal{M}=\mathcal{M}^{r_1,r_2}$ given by

$$\sigma(\alpha)=\begin{pmatrix}\sigma_1(\alpha)\\ \cdot\\ \cdot\\ \cdot\\ \sigma_n(\alpha)\end{pmatrix}$$

is a one-one map linear over $\boldsymbol{Q}$. For this and further points of number theory quoted in the sequel we refer to Borevich and Shafarevich [1], especially chapters 2, 3 and 5. According to their terminology a full module in K is a finitely generated subgroup of the additive group of K which contains a basis of K. Equivalently a full module in K is a subgroup of the additive group of K which is a free abelian group of rank n. If A is a full module in K with basis $\alpha_1,\cdots,\alpha_n$ then $\sigma(A)$ is a lattice in $\mathcal{M}$ with basic matrix $\Lambda=(\sigma(\alpha_1),\cdots,\sigma(\alpha_n))$. The discriminant $D(\sigma(A))=(\det\Lambda)^2=\det{}^t\Lambda\Lambda=\det(\sigma(\alpha_i)\cdot\sigma(\alpha_j))=D(A)$, the discriminant of A. Observe that for $\alpha,\beta\in K$, $\sigma(\alpha)\cdot\sigma(\beta)=\sum_{j=1}^{n}\sigma_j(\alpha)\sigma_j(\beta)=\sum_{j=1}^{n}\sigma_j(\alpha\beta)=\operatorname{tr}(\alpha\beta)$ where tr is the trace of $K/\boldsymbol{Q}$. In particular, $\sigma(\alpha)\cdot\sigma(\beta)\in\boldsymbol{Q}$ for $\alpha,\beta\in K$ and $\sigma(\alpha)\cdot\sigma(\beta)\in\boldsymbol{Z}$ for $\alpha,\beta\in I_K$, the ring of algebraic integers in K.

For our purposes we seek fields K where $\sigma(\alpha)\cdot\overline{\sigma(\beta)}\in\boldsymbol{Q}$ for $\alpha,\beta\in K$. Unfortunately $\sigma(\alpha)\cdot\overline{\sigma(\beta)}$ need not be rational, for $\overline{\sigma(\beta)}=\sigma(\bar{\beta})$ is not true in general. For example if $\alpha=\sqrt[3]{2}>0$, $\omega=e^{2\pi i/3}$, $K=\boldsymbol{Q}(\alpha)$ has $n=3$, $r_1=r_2=1$,

$$\sigma(\alpha)=\begin{pmatrix}\alpha\\ \omega\alpha\\ \bar{\omega}\alpha\end{pmatrix}$$

but $\overline{\sigma(\alpha)}\neq\sigma(\bar{\alpha})$. Also $\|\sigma(\alpha)\|^2=\sigma(\alpha)\cdot\overline{\sigma(\alpha)}=3\alpha^2$ is irrational. There are two cases where $\overline{\sigma(\alpha)}=\sigma(\bar{\alpha})$ is true. First, if K is totally real, i.e., $r_2=0$, $n=r_1$, in which case $\overline{\sigma(\alpha)}=\sigma(\bar{\alpha})=\sigma(\alpha)$ as all quantities are real. Second, suppose K_0 is a totally real field of degree n_0 and $\mu\in K_0$ is totally negative: $\sigma_j^{(0)}(\mu)<0$, $j=1,2,\cdots,n_0$, the $\sigma_j^{(0)}$ being the isomorphisms of K_0. Then $K=K_0(\sqrt{\mu})$ is a totally complex field of degree $n = 2n_0$, $r_1 = 0$, $r_2 = n_0$ and $\overline{\sigma(\alpha)} = \sigma(\bar{\alpha})$ holds in K. Verification of this is left to the reader. A normal extension K of $\boldsymbol{Q}$ with $\{1, c\}$, c complex conjugation, a normal subgroup of the Galois group of K is of this type for then $\sigma_j(\bar{\alpha}) = \sigma_j(c\alpha) = c\sigma_j(\alpha) = \overline{\sigma_j(\alpha)}$ for every automorphism σ_j of K. In particular every cyclotomic or quadratic field falls into these categories.

Let now K satisfy $\sigma(\bar{\alpha}) = \overline{\sigma(\alpha)}$ for all $\alpha \in K$. Then $\sigma(\alpha) \cdot \overline{\sigma(\beta)} = \sigma(\alpha) \cdot \sigma(\bar{\beta}) = \operatorname{tr}(\alpha\bar{\beta}) \in \boldsymbol{Q}$ for all $\alpha, \beta \in K$ and $\sigma(\alpha) \cdot \overline{\sigma(\beta)} \in \boldsymbol{Z}$ for $\alpha, \beta \in I_K$. Thus for any full module $A \subset I_K$, $\mathscr{L} = \sigma(A)$ is an even or odd lattice in $\mathscr{M}$ according as $\operatorname{tr}(\alpha\bar{\alpha})$ is an even integer for all $\alpha \in A$ or not. In the complex case $\sigma(I_K)$ itself is even for $\operatorname{tr}(\alpha\bar{\alpha}) = 2\operatorname{tr}_{K_0/Q}(\alpha\bar{\alpha})$ where $K_0 = K \cap \boldsymbol{R}$, whence every $\sigma(A)$ is an even lattice. In any case, if $\mathscr{L} = \sigma(A)$ is even, by the results of Section 1, $|D(\mathscr{L})| = L^n\Delta$ where $L = \text{g.c.d.}\{\frac{1}{2}\operatorname{tr}(\alpha\bar{\alpha}),\ \alpha \in A\}$ and $\Delta = [L\bar{\mathscr{L}}^*: \mathscr{L}] = [L\bar{A}^*: A]$, $\bar{A}^*$ being the complementary module (with respect to the trace) of $\bar{A}$. Determination of the number L in general appears to lead to some deep questions of number theory. For applications of our theory we are particularly interested in the case where Δ is odd. If L is unknown this can be achieved by requiring $D(A) = D(\mathscr{L}) = (-1)^{r_2}L^n\Delta$ to be odd. Since $D(A) = [I_K: A]^2 D_k$, where $D_k = D(I_K)$ is the discriminant of K, $D(A)$ will be odd exactly when D_k is odd and A has odd index in I_K. Recall also that Δ odd requires n even. Suppose K is totally real, A a full module in I_K such that $D(A)$ is odd and $\sigma(A)$ is an even lattice. Then $D(A) = |D(A)| = L^n\Delta \equiv \Delta \bmod 4$. But by Stickelberger's theorem of number theory, the discriminant of a full module of algebraic integers is $\equiv 0$ or $1 \bmod 4$, here then $D(A) \equiv 1 \bmod 4$ by (60), $\Delta \equiv 1 \bmod 4$ implies $n \equiv 0 \bmod 4$. Put another way, if K is totally real field of degree $n \equiv 2 \bmod 4$ and A is a full module in I_K with $D(A)$ odd then $\sigma(A)$ is an odd lattice, i.e., there is some $\alpha \in A$ such that $\operatorname{tr}(\alpha^2)$ is odd.

In somewhat greater detail consider the field $K = \boldsymbol{Q}(\zeta)$, ζ a primitive pth root of unity, p an odd prime. The degree of K is $n = p - 1$, $r_1 = 0$, $r_2 = (p-1)/2$ and the discriminant $D_K = (-1)^{(p-1)/2}p^{p-2}$. $\mathscr{L} = \sigma(I_K)$ is an even lattice in $\mathscr{M} = \mathscr{M}^{0, r_2}$. $L = L(\mathscr{L}) = 1$ here, since by Proposition 3(i), for any $\lambda, \mu \in \mathscr{L}$, $\lambda \cdot \bar{\mu} \equiv 0 \bmod L$ but for $\lambda = \sigma(\zeta)$, $\mu = \sigma(1)$, $\lambda \cdot \bar{\mu} = \operatorname{tr}\zeta = -1$. Then $\Delta = |D(\mathscr{L})| = |D_K| = p^{p-2}$ is odd and is the order of the group $\mathscr{J} \bmod \mathscr{L}$, $\mathscr{J} = \bar{\mathscr{L}}^*$. Here though $\mathscr{L} = \sigma(I_K) = \sigma(\bar{I}_K) = \bar{\mathscr{L}}$ and $\mathscr{L}^* = \sigma(I_K^*) = \sigma(\partial_K^{-1})$ where ∂_K is the different of K. Thus $\mathscr{J} = \sigma(\partial_K^{-1})$. With (α) denoting the principal ideal in K generated by the element α, it is known that $(1-\zeta)$ is a prime ideal and $(p) = (1-\zeta)^{p-1}$ is the prime factorization of p in K. Since $N\partial_K = |D_K|$ ($N\partial_K$ is the norm of the ideal ∂_K) and $N(1-\zeta) = p$, we must have $\partial_K = (1-\zeta)^{p-2}$, $\partial_K^{-1} = ((1-\zeta)/p) = ((1-\zeta)/p)I_K$. It follows that for all $\alpha \in \partial_K^{-1}$, $p\alpha \in I_K$. So ∂_K^{-1}/I_K is an elementary abelian p-group, a direct product of $p-2$ cyclic groups each of order p. Here then $\Delta = p^h$, $h = p-2$, $\Delta_1 = p$, $\varepsilon = \varepsilon(p)^{p-2} = 1$ or i according as $p \equiv 1$ or $p \equiv 3 \bmod 4$, $\Gamma(\mathscr{L}) = \Gamma_0(p)$ and the character $\chi_{\mathscr{L}}$ is $\chi_{\mathscr{L}}(d) = (d/\Delta) = (d/p)$, the Legendre symbol. Now by (60) we see that $W = 1$ if $p \equiv 1$ or $3 \bmod 8$ and $W = -1$ if $p \equiv 5$ or $7 \bmod 8$. By Theorem (3) and (62) we now know how the functions $\psi_{\mathscr{L}}^{(s)}[{x \atop y}](\tau)$ transform under any $M \in \Gamma$. One might now consider $\mathscr{L} = \sigma(A)$ for any full module A in I_K and also more general cyclotomic K but we do not pursue this topic any further here.

Finally, we look more closely at an imaginary quadratic field K. Again we mention that our basic reference for this is [1, chap. 2]. Let $I = I_K$ be the ring of algebraic integers in K and $D = D(I) = D_K$ the discriminant of K. For K we have $n = 2$, $r_1 = 0$, $r_2 = 1$ and the embedding σ of K into $\mathscr{M} = \mathscr{M}^{0,1}$ is given by

$$\alpha \rightarrow \sigma(\alpha) = \begin{pmatrix} \alpha \\ \bar{\alpha} \end{pmatrix}, \quad \sigma(\alpha)\cdot\overline{\sigma(\beta)} = \mathrm{tr}_{K/Q}(\alpha\bar{\beta})$$

and $\|\sigma(\alpha)\|^2 = \mathrm{tr}_{K/Q}(\alpha\bar{\alpha}) = 2N_{K/Q}(\alpha)$. In this special case we see that the map σ does not really depend on K, that is, it extends to a map $\sigma: \boldsymbol{C} \rightarrow \mathscr{M}^{0,1}$, by $\sigma(\alpha) = \begin{pmatrix} \alpha \\ \bar{\alpha} \end{pmatrix}$ for all $\alpha \in \boldsymbol{C}$, coinciding with $\sigma(\alpha)$ as above for $\alpha \in K$. Furthermore, for $\alpha, \beta \in \boldsymbol{C}$,

$$\sigma(\alpha)\cdot\overline{\sigma(\beta)} = \alpha\bar{\beta} + \bar{\alpha}\beta = 2\,\mathrm{Re}(\alpha\bar{\beta}) = \mathrm{tr}_{\boldsymbol{C}/\boldsymbol{R}}(\alpha\bar{\beta})$$

and $\|\sigma(\alpha)\|^2 = 2|\alpha|^2 = 2N_{\boldsymbol{C}/\boldsymbol{R}}(\alpha)$. From now on we let tr stand for $\mathrm{tr}_{\boldsymbol{C}/\boldsymbol{R}}$ and N for $N_{\boldsymbol{C}/\boldsymbol{R}}$, so tr restricted to K is $\mathrm{tr}_{K/Q}$ and similarly for N. Every full module A of K has a coefficient ring $R = \{x \in K : xA \subset A\}$. This coefficient ring is both a ring and a full module, such an object is called an order in K. Every order in any field is contained in the ring of algebraic integers, this being the maximal order. In a quadratic field K the order is determined by its index in the maximal order I: for each integer $g \geqq 1$ there is a unique order R_g of index g in I. Let $D_g = D(R_g) = g^2D$. A full module A with coefficient ring R_g and which is contained in R_g will be referred to simply as an R_g ideal. The reader not used to these notions can take A simply as an integral ideal of K, i.e., $g = 1$. If A is an R_g ideal the index $[R_g : A]$ is called the norm of A, NA.

THEOREM 5. *Let A be an R_g ideal, $\mathscr{L} = \sigma(A)$ the corresponding even lattice in $\mathscr{M}^{0,1}$, $L = L(\mathscr{L})$, $\Delta = \Delta(\mathscr{L})$. Then $L = \mathrm{NA}$, $\Delta = |D_g|$, $\mathscr{J} = L\mathscr{L}^* = \sigma((1/\sqrt{D_g})A)$ and $J = \mathscr{J}/\mathscr{L}$ is (isomorphic to via σ) $(1/\sqrt{D_g})A/A$. Δ is odd if and only if g and D are odd. If Δ is odd and $(L, D_g) = 1$ then J is cyclic, $\Delta_1 = \Delta$, $\Gamma(\mathscr{L}) = \Gamma_0(g^2|D|)$ and the character $\chi_{\mathscr{L}}$ coincides essentially with character of the field K: $\chi_{\mathscr{L}}(M) =$*

$(d/|D|)$. The invariants W, ε of $\mathscr{L}$ then are $\varepsilon = i^H$ where H is the number of prime factors of D which are $\equiv 3 \bmod 4$, *$W = -i\varepsilon$ and furthermore* $(\mathrm{NA}/|\mathrm{D}|) = 1$.

Proof. It is known that for $\alpha, \beta \in A$, NA divides each of the numbers $N\alpha, N\beta$ and $\operatorname{tr} \alpha\bar{\beta}$. As L is the greatest common divisor of the numbers $\frac{1}{2}\|\sigma(\alpha)\|^2 = N\alpha$, $\alpha \in A$, one has $NA \mid L$. On the other hand if α_1, α_2 is a basis for A (as a free abelian group) — which we denote by $A = [\alpha_1, \alpha_2]$ — the fundamental correspondence between full modules and binary forms states that $\mathrm{N}(x_1\alpha_1 + x_2\alpha_2) = (\mathrm{N}\alpha_1)x_1^2 + (\operatorname{tr} \alpha_1\bar{\alpha}_2)x_1x_2 + (N\alpha_2)x_2^2$ has NA as the g.c.d. of its coefficients. But each of these coefficients is divisible by L so $L \mid NA$. Thus $L = NA$. Now $D(A) = (NA)^2 D_g$ while also $D(A) = D(\mathscr{L}) = -L^2\Delta$ by Proposition 3, thus $\Delta = |D_g|$. With $A = [\alpha_1, \alpha_2]$, a basic matrix for $\mathscr{L}$ is

$$\Lambda = (\sigma(\alpha_1),\ \sigma(\alpha_2)) = \begin{pmatrix} \alpha_1 & \alpha_2 \\ \bar{\alpha}_1 & \bar{\alpha}_2 \end{pmatrix};$$

$\Lambda^* = {}^t\Lambda^{-1}$ is then basic for $\mathscr{L}^*$ and $L\bar{\Lambda}^*$ is basic for $L\bar{\mathscr{L}}^* = \sigma(L\bar{A}^*)$. $\delta = \det \Lambda$ satisfies $\delta^2 = D(A) = L^2 D_g$ and without loss of generality we can assume $\delta = L\sqrt{D_g}$, since otherwise $\delta = -L\sqrt{D_g}$ and we can then interchange α_1 and α_2. A calculation then gives

$$L\bar{\Lambda}^* = \left(\sigma\left(\frac{-\alpha_2}{\sqrt{D_g}}\right),\ \sigma\left(\frac{\alpha_1}{\sqrt{D_g}}\right)\right)$$

which shows $L\bar{A}^* = (1/\sqrt{D_g})A$. Since $\Delta = |D_g| = g^2|D|$ clearly Δ is odd if and only if g and D are odd. If D is odd D is square free, $D \equiv 1 \bmod 4$, $\Delta \equiv |D| \equiv 3 \bmod 4$. Assuming this to be the case it follows that $I = [1, \omega]$, $\omega = (1 + \sqrt{D})/2$ and $R_g = [1, g\omega]$.

Since $L = NA = [R_g : A]$, for every $x \in R_g$, $Lx \in A$ which with $x = 1$ gives $L \in A$. To show $(1/\sqrt{D_g})A/A$ is cyclic it suffices to show that for $k \in \mathbf{Z}$, $(kL/\sqrt{D_g}) \in A$ only if $k \equiv 0 \bmod |D_g|$ since $\Delta = |D_g|$ is the order of the group. Say then $(kL/\sqrt{D_g}) = \alpha \in A$. Since $A \subset R_g$, α has a unique expression as $\alpha = a + bg\omega$, $a, b \in \mathbf{Z}$, or $kL = \alpha\sqrt{D_g} = (a + bg\omega)\sqrt{D_g} = (a + (bg/2))\sqrt{D_g} + (bD_g/2)$. Then $a + (bg/2) = 0$, $kL = bD_g/2$. Since g is odd, b must be even, $kL = (b/2)D_g$. With the extra assumption $(L, D_g) = 1$ this implies $D_g \mid k$ as required.

With J cyclic, $\Delta_1 = \Delta$ and Theorem 3 gives $\Gamma(\mathscr{L}) = \Gamma_0(\Delta) = \Gamma_0(g^2|D|)$ and the character

$$\chi_{\mathscr{L}}(M) = \left(\frac{d}{\Delta}\right) = \left(\frac{d}{g^2|D|}\right) = \left(\frac{d}{|D|}\right).$$

Since the $J^{(p)}$ for different p are mutually orthogonal (in the sense of Section 3) and each $J^{(p)}$ is cyclic an orthogonal basis of J is $\{\alpha^{(p)}\}_{p \mid D_g}$ where $\alpha^{(p)}$ is a generator of $J^{(p)}$. We write here $\alpha^{(p)}$ instead of the more correct $\sigma(\alpha^{(p)})$, taking the identification by σ for granted. Thus $\alpha^{(p)}$ here is the $\alpha^{(p,1)}$ of (48), the corresponding $w^{(p)}$ is defined by $(1/L)2N\alpha^{(p)} = 2w^{(p)}/p^e$ where $p^e = p^{e_1}$ is the order of $J^{(p)}$. We can take $\alpha^{(p)} = (L/\sqrt{D_g})(D_g/p^e)$, $w^{(p)} = L \mid D_g \mid / p^e$. By Definition (57)

$$W = \prod_{p \,\|\, D_g \mid} \left(\frac{w^{(p)}}{p^e}\right), \quad \varepsilon = \prod_{p \,\|\, D_g \mid} \varepsilon(p^e).$$

If the highest power of p dividing g is p^a then $e = 2a$ if $p \nmid D$ and $e = 2a + 1$ if $p \mid D$. So in the products for W and ε the only primes which can yield a factor different from 1 are the $p \mid D$ and for these

$$\left(\frac{w^{(p)}}{p^e}\right) = \left(\frac{w^{(p)}}{p}\right)$$

and $\varepsilon(p^e) = \varepsilon(p)$. Thus

$$W = \prod_{p \mid D} \left(\frac{w^{(p)}}{p}\right) = \prod_{p \mid D} \left(\frac{Lg^2 \mid D \mid / p^e}{p}\right) = \left(\frac{L}{\mid D \mid}\right) \prod_{p \mid D} \left(\frac{\mid D \mid / p}{p}\right).$$

This last product is clearly

$$\prod_{p \mid D} \prod_{\substack{q \mid D \\ q \neq p}} \left(\frac{q}{p}\right), \quad q \text{ prime},$$

$$= \prod_{\{p,q\}} \left(\frac{q}{p}\right)\left(\frac{p}{q}\right)$$

taken over all two element sets $\{p, q\}$ with $pq \mid D$. By quadratic reciprocity $(q/p)(p/q) = 1$ except if $p \equiv q \equiv 3 \bmod 4$ where it is -1. Thus the product is $(-1)^j$ where j is the number of two element sets $\{p, q\}$ with $p \equiv q \equiv 3 \bmod 4$ and $pq \mid D$. If H is the number of prime factors of D that are $\equiv 3 \bmod 4$ then $j = \binom{H}{2} = H(H-1)/2$. Thus $W = (L/\mid D \mid)(-1)^{H(H-1)/2}$. On the other hand $\varepsilon = i^H$ and since $\mid D \mid \equiv 3 \bmod 4$, H is odd, so $\varepsilon = ii^{H-1} = (-1)^{(H-1)/2} i$ and $W = (L/\mid D \mid)(-1)^{(H-1)/2}$. By (60) $W = -i\varepsilon$ gives $W = (-1)^{(H-1)/2}$ and so $(NA/\mid D \mid) = (L/\mid D \mid) = 1$. This completes the proof.

We note that $(NA/\mid D \mid) = 1$ immediately gives part of the theory as to how rational primes factor in K (with negative odd discriminant). Say P is a prime ideal of K dividing the rational prime (p). If $P \neq (p)$ general considerations show $NP = p$ so if $p \nmid D$, $(p/\mid D \mid) = (NP/\mid D \mid) = 1$ by the last result of the theorem. Thus if $(p/\mid D \mid) = -1$ (p) remains prime in K. We do not pursue this any further here as the question as to how a rational prime factors in K has a full classical answer. We mention it only to indicate that our development leads naturally to the correct circle of ideas and perhaps it is not unreasonable to expect that application of these concepts to other fields will yield new results.

With A an R_g ideal, $\mathscr{L} = \sigma(A)$ and $L = NA$ the associated functions in the notation of Sections 2 and 3 are $\psi_{\mathscr{L}}^{(s)}[{x \atop y}](\tau)$ with $x, y \in \mathscr{M}$, (s) an admissible sequence. Every vector in $\mathscr{M}$ we have seen is $\sigma(x) = \begin{pmatrix} x \\ \bar{x} \end{pmatrix}$ with $x \in \boldsymbol{C}$ and an admissible sequence is either empty or $(1, \cdots; 1)$ or $(2, \cdots, 2)$ of arbitrary length l. It is convenient here to designate these sequences as $(1, l)$ and $(2, l)$ respectively and write $\psi_A^{(s)}[{x \atop y}]$ for $\psi_{\sigma(A)}^{(s)}[{\sigma(x) \atop \sigma(y)}]$. We have then for $x, y \in \boldsymbol{C}$:

$$\psi_A\begin{bmatrix} x \\ y \end{bmatrix}(\tau) = \sum_{\alpha \in A} e^{2\pi i \operatorname{tr}(\alpha + x)y + 2\pi i(\tau/L)N(\alpha + x)}$$

$$\psi_A^{(1,l)}\begin{bmatrix} x \\ y \end{bmatrix}(\tau) = (2\pi i)^l \sum_{\alpha \in A} (\alpha + x)^l e^{2\pi i \operatorname{tr}(\alpha + x)y + 2\pi i(\tau/L)N(\alpha + x)}$$

$$\psi_A^{(2,l)}\begin{bmatrix} x \\ y \end{bmatrix}(\tau) = (2\pi i)^l \sum_{\alpha \in A} (\bar{\alpha} + \bar{x})^l e^{2\pi i \operatorname{tr}(\alpha + x)y + 2\pi i(\tau/L)N(\alpha + x)}.$$

In case g and D are odd, $(L, g^2D) = 1$; the above theorem and the previous theory give the complete transformation properties of these functions under Γ. Corresponding to the situation of Theorem 4, $F^{(s)}(A, m)$ would then be linear combinations of the functions $\psi_A^{(s)}[{x \atop y}](\tau)$ with $\sigma(x) \in (1/m)\mathscr{J}$, $\sigma(y) \in (1/m)\mathscr{L}^*$, $x \in (1/(m\sqrt{D_g}))A$, $y \in (1/(mL\sqrt{D_g}))\bar{A}$. The group $G(\Delta_1, m)$ of that section is $G(|D_g|, m)$ consisting of all $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ with $a - 1 \equiv d - 1 \equiv c \equiv 0 \bmod m\,|D_g|$ and $b \equiv 0 \bmod m$. For $M \in G(|D_g|, m)$ (63) gives

$$\psi_A^{(s)}\begin{bmatrix} x \\ y \end{bmatrix}\Bigg|_M = e^{2\pi i((b/L)Nx - cLNy + (d-1)\operatorname{tr} xy)}\, \psi_A^{(s)}\begin{bmatrix} x \\ y \end{bmatrix}.$$

The nature of this root of unity depends on m and K, as will be evident by the following considerations. For example, say p is a prime and $\xi \in K$ satisfies $p\xi \in I$ and has an ideal factorization $(\xi) = B/(p)$, B an integral ideal. If (p) is prime in K and $\xi \notin I$ then B and (p) are relatively prime, $N\xi = NB/p^2$, $(NB, p) = 1$ so $N\xi$ actually has denominator p^2. If (p) is not prime $(p) = P\bar{P}$, $NP = p$ so $\xi \in (1/p)I$ with factorization $(\xi) = (B/P)$, $(NB, p) = 1$ has $N\xi = NB/p$ with denominator p.

Returning to the above functions with $x \in (1/(m\sqrt{D_g}))A$ and setting $y = 0$ (61) gives for $M \in \Gamma_0(|D_g|)$,

$$\psi_A^{(s)}\begin{bmatrix} x \\ 0 \end{bmatrix}\Bigg|_M = e^{-2\pi i(ab/L)Nx}\left(\frac{d}{|D|}\right)\psi_A^{(s)}\begin{bmatrix} ax \\ \frac{b}{L}\bar{x} \end{bmatrix}.$$

If $b \equiv 0 \bmod m$, $(b/L)\bar{x} \in (1/(L\sqrt{D_g}))\bar{A} = A^*$ so using again Proposition 4(i),

$$\psi_A^{(s)}\begin{bmatrix} x \\ 0 \end{bmatrix}\Bigg|_M = e^{2\pi i(ab/L)Nx}\left(\frac{d}{|D|}\right)\psi_A^{(s)}\begin{bmatrix} ax \\ 0 \end{bmatrix}.$$

Then

$$M_{(m)} = \begin{pmatrix} a & \frac{b}{m} \\ mc & d \end{pmatrix} \in \Gamma_0(m\,|\,D_g\,|)$$

and every element of this group may be written this way. It follows that if we consider instead the functions $\varphi_A^{(s)}[{x \atop 0}](\tau) = \psi_A^{(s)}[{x \atop 0}](m\tau)$ — as in the transition from Theorem 1 to 1′ — these satisfy for

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} = M \in \Gamma_0(m\,|\,D_g\,|) \quad \varphi_A^{(s)}\begin{bmatrix} x \\ 0 \end{bmatrix}\Bigg|_M = e^{2\pi i(mab/L)Nx}\left(\frac{d}{|D|}\right)\varphi_A^{(s)}\begin{bmatrix} x \\ 0 \end{bmatrix}.$$

One sees with some change of notation that it is this class of functions from imaginary quadratic K considered by Hecke [3], see §3, (11) and §4 Satz 7 of that paper. However he studies only the case $g = 1$, so that A is an integral ideal of K. It is fitting that we end with this reference to Hecke as it was the attempt to understand this work of his that gave us the impetus and inspiration for this paper.

References

1. Z. I. Borevich and I. R. Shafarevich, *Number Theory*, Academic Press, New York, 1966.
2. Martin Eichler, *Introduction to the Theory of Algebraic Numbers and Functions*, Academic Press, New York, 1966.
3. Erich Hecke, *Zur Theorie der elliptischen Modulfunktionen*, Math. Ann. **97** (1926), 210–242.
4. Adolf Hurwitz, *Uber Endliche Gruppen linearer Substitutionen, welche in der Theorie der elliptischen Transzendenten auftreten*, Math. Ann. **27** (1886), 183–233.
5. Joseph Lehner, *Discontinuous Groups and Automorphic Functions: Mathematical Surveys Number VIII*, American Mathematical Society, Providence, 1964.
6. Harry E. Rauch and Hershel M. Farkas, *Theta Functions with Applications to Riemann Surfaces*, The Williams and Wilkins Co., Baltimore, 1974.
7. B. Schoeneberg, *Das Verhalten von mehrfachen Thetareihen bei Modulsubstitutionen*, Math. Ann. **116** (1939), 511–523.
8. Goro Shimura, *Introduction to the Arithmetic Theory of Automorphic Functions*, Publications of the Mathematical Society of Japan 11, Iwanami Shoten Publishers and Princeton University Press, 1971.

Lehman College (CUNY)
Bronx, N. Y. 10468, U.S.A.
and
The Graduate School and University Center (CUNY)
New York, N.Y. 10036, U.S.A.