ADVANCES IN MATHEMATICS 43, 122–172 (1982)

Hecke's Theorem in Quadratic Reciprocity, Finite Nilpotent Groups and the Cooley–Tukey Algorithm

L. AUSLANDER, R. TOLIMIERI, AND S. WINOGRAD

IBM T. J. Watson Research Center, Yorktown Heights, New York 10598

INTRODUCTION

Although Gauss's theorem on quadratic reciprocity and its relation to Gauss sums is well known, there is a generalization due to Hecke that is less well known. Hecke's theorem holds for general number fields and has at its core the evaluation of certain trigonometric sums that we will call Hecke sums. Hecke's original proof involved modular forms (theta constants) and the transformation theory of these forms. There is a combinatorial proof of Hecke's result due to Milgram in [6]. Milgram's result had a strong antecedent in the work of Braun [3].

We now know many ways of evaluating Gauss sums and a fairly complete discussion of this problem is given in [1]. It was Schur [7] who first observed that one can use the fact that Gauss sums are the trace of certain finite Fourier transforms to evaluate Gauss sums. In this paper, we will show that Hecke sums are also the trace of certain finite Fourier transforms and use this fact to derive the usual results about Hecke sums.

Weil's work in [8] centered on the problem of understanding Hecke's results on quadratic reciprocity. In Weil's work the unitary representations of certain locally compact nilpotent groups play an essential role. From this work of Weil, Brezin derived the Weil–Brezin mapping as discussed in [2]. Now the Weil–Brezin mapping and the Cooley–Tukey algorithm [4] for evaluating the finite Fourier transform are intimately related. Thus it is reasonable to try to use finite Fourier transforms to study Hecke sums.

In our approach to evaluating Hecke sums, the central role is played by the induced representation theory of certain finite nilpotent groups, called finite Heisenberg groups, that are intimately related to the finite Fourier transforms. This will enable us to determine matrices similar to the finite Fourier transforms for which it is easier to evaluate the trace. This construction is based on induced representations, and certain intertwining operators.

The Cooley–Tukey algorithm or the FFT (fast Fourier transform), as we have mentioned, is analogous to the Weil–Brezin mapping. This suggests that

0001-8708/82/020122-51$05.00/0

the Cooley–Tukey algorithm should be related to our finite nilpotent group constructions. This is indeed the case. But in order to see this relation one has to determine a multidimensional version of the FFT. We do this in Section V of this paper. In Section VI we relate it to nilpotent group theory. We have presented the results in the FFT in such a way as to provide a purely combinatorial proof of the results on Hecke trigonometric sums, logically independent of the finite nilpotent group theory.

The results of this paper give another example of the importance of communication between pure and applied mathematics—in our case, number theory and digital signal processing. For, because of this exchange of ideas, we have enriched our understanding of Hecke's work, while stimulating the need for obtaining a truly multidimensional Cooley–Tukey algorithm that may have important practical applications, and gained deeper insight into the structure of the finite Fourier transform.

I. The Finite Fourier Transform

Let A be a finite abelian group of order m. The group law of A will be written additively. In this section, the Fourier transform of A will be defined and its basic properties will be examined. We will begin with an exposition of some fundamental results about finite abelian group theory.

Let U_m be the set consisting of all mth roots of unity in C. Then, U_m becomes under multiplication, a cyclic group of order m, generated by any element of the form $e^{2\pi i(j/m)}$, where j and m are relatively prime. We will denote by A^*, the set of all homomorphisms a^* of A into U_m and call this set, the dual of A. The dual, A^*, becomes an abelian group relative to the group law:

$$(a^* + b^*)(a) = a^*(a)\, b^*(a), \qquad a^*, b^* \in A^*,\ a \in A.$$

A basic result states that A and A^* are isomorphic. Indeed, if $A = B \oplus C$, the direct sum of the groups B and C, then $A^* = B^* \oplus C^*$. The fundamental structure theorem for finite abelian groups implies that we may write A as the direct sum of cyclic groups,

$$A = \mathbb{Z}/m_1 \oplus \cdots \oplus \mathbb{Z}/m_r, \qquad m = m_1 \cdots m_r.$$

Thus, $A^* = (\mathbb{Z}/m_1)^* \oplus \cdots \oplus (\mathbb{Z}/m_r)^*$ and an isomorphism between A and A^* will be established once we specify an isomorphism between $\mathbb{Z}/m_i$ and $(\mathbb{Z}/m_i)^*$, $i = 1,..., r$. However, for any integer $n > 0$, there can be found an $a^* \in (\mathbb{Z}/n)^*$ with the property that $a^*(1) = e^{2\pi i(1/n)}$. The mapping

$$j \to ja^*: \mathbb{Z}/n \to (\mathbb{Z}/n)^*$$

is a well defined isomorphism of $\mathbb{Z}/n$ onto $(\mathbb{Z}/n)^*$. Observe that the resulting isomorphism between A and A^* depends upon the initial decomposition into cyclic subgroups as well as the choice of an isomorphism between corresponding factors.

Consider the pairing

$$A \times A^* \to U_m$$

given by $\langle a, a^* \rangle = a^*(a)$, $a \in A$, $a^* \in A^*$. We call this a bilinear pairing between A and its dual, since it satisfies $\langle a + b, a^* \rangle = \langle a, a^* \rangle \langle b, a^* \rangle$ and $\langle a, a^* + b^* \rangle = \langle a, a^* \rangle \langle a, b^* \rangle$, for all $a, b \in A$ and $a^*, b^* \in A^*$. Let A^{**} be the dual of A^*. The bilinear pairing determines a canonical isomorphism between A and A^{**}; namely, for $a \in A$ we define $\chi_a \in A^{**}$ by the formula $\chi_a(a^*) = \langle a, a^* \rangle$, $a^* \in A^*$. The mapping, $a \to \chi_a : A \to A^{**}$, is the canonical isomorphism.

The set, $C = \{\langle a, a^* \rangle : a \in A, a^* \in A^*\}$, is a subgroup of U_m. In fact, in terms of the decomposition $A = \mathbb{Z}/m_1 \oplus \cdots \oplus \mathbb{Z}/m_r$ we have that C is the group generated by $e^{2\pi i(d/m)}$, where d is the greatest common divisor of $m/m_1, \ldots, m/m_r$.

Let $L^2(A)$ be the Hilbert space of complex valued functions on A, with respect to the inner product

$$\langle f, g \rangle = \sum_{a \in A} f(a)\, \bar{g}(a), \qquad f, g \in L^2(A).$$

$L^2(A)$ is an m dimensional complex vector space. The set of functions $\{e_a : a \in A\}$, where

$$\begin{aligned} e_a(b) &= 1, \qquad b = a, \\ &= 0, \qquad b \neq a, \end{aligned}$$

is an orthonormal basis of $L^2(A)$. Consider $L^2(A^*)$ as a Hilbert space in exactly the same way. The character orthogonality condition

$$\begin{aligned} \sum_{a^* \in A^*} \langle a, a^* \rangle &= m, \qquad a = 0, \\ &= 0, \qquad a \neq 0, \end{aligned}$$

immediately implies that the set of functions $\{(1/\sqrt{m})\, \chi_a : a \in A\}$, defined above, is an orthonormal basis of $L^2(A^*)$.

The Fourier transform, $\mathcal{F} = \mathcal{F}_A$, is the unique linear operator satisfying

$$\mathcal{F}(e_a) = 1/\sqrt{m}\, \chi_a, \qquad a \in A.$$

Clearly, since $\mathscr{F}$ takes an orthonormal basis onto an orthonormal basis, it must be an isometry. Moreover, the general formula describing $\mathscr{F}$ is given by

$$\mathscr{F}(f)(a^*) = 1/\sqrt{m} \sum_{a \in A} \langle a, a^* \rangle f(a), \qquad a^* \in A^*, f \in L^2(A).$$

To see this, simply observe that the mapping $f \to \mathscr{F}(f)$ is linear and compute $\mathscr{F}(e_a)$, $a \in A$.

In the following sections, we will study finite abelian group A which arise as quotients of finitely generated, torsion free abelian groups. Along with the group A, there will be given an isomorphism D: $A \to A^*$ which satisfies the condition

$$\langle a, D(b) \rangle = \langle b, D(a) \rangle, \qquad a, b \in A.$$

We will call such an isomorphism D, a symmetric isomorphism.

Let D be a symmetric isomorphism of A and A^*. Let $D^{\#}$: $L^2(A^*) \to L^2(A)$ be the linear isometry given by $D^{\#}(f^*) = f^* \cdot D$, $f^* \in L^2(A^*)$. We will study the unitary operator $D^{\#} \cdot \mathscr{F}_A$ of $L^2(A)$. For $a, b \in A$,

$$D^{\#} \cdot \mathscr{F}_A(e_a)(b) = \mathscr{F}_A(e_a)(D(b)) = 1/\sqrt{m} \sum_{c \in A} \langle c, D(b) \rangle e_a(c)$$

$$= 1/\sqrt{m} \langle a, D(b) \rangle.$$

Since D is symmetric and $D(a) = \sum_{c \in A} D(a)(c) e_c$ we have

$$D^{\#} \cdot \mathscr{F}_A(e_a)(b) = 1/\sqrt{m} \sum_{c \in A} D(a)(c)\, e_c(b).$$

Thus,

$$D^{\#} \cdot \mathscr{F}_A(e_a) = 1/\sqrt{m} \sum_{c \in A} D(a)(c) e_c.$$

When D: $A \to A^*$, the symmetric isomorphism is given, we will refer to the unitary operations $D^{\#} \cdot \mathscr{F}_A$ of $L^2(A)$ as the Fourier transform of A. It depends obviously on D. The above expression for $D^{\#} \cdot \mathscr{F}_A(e_a)$, $a \in A$, determines $D^{\#} \cdot \mathscr{F}_A$ on the basis $\{e_a : a \in A\}$. The corresponding matrix is given by

$$1/\sqrt{m}(D(a)(c)) = 1/\sqrt{m}(\langle c, D(a) \rangle)_{a,c \in A}$$

and its trace is given by

$$1/\sqrt{m} \sum_{a \in A} \langle a, D(a) \rangle.$$

Consider the following example. Take $A = \mathbb{Z}/m$, the additive group of integers mod m. For $l \in \mathbb{Z}$, let $\chi(l)$ be the character of $\mathbb{Z}$ defined by $\chi(l)(r) = e^{2\pi i(lr/m)}$. Clearly, $\chi(l)$ acts trivially on $m \cdot \mathbb{Z}$ and hence induces a character $D(l)$ on $A = \mathbb{Z}/m$. Also, the mapping D: $\mathbb{Z} \to A^*$ satisfies the short exact sequence

$$0 \to m\mathbb{Z} \to \mathbb{Z} \xrightarrow{D} A^* \to 1.$$

Thus, D induces an isomorphism, which we also denote by D, from A onto A^*. Clearly, D is a symmetric isomorphism. By the discussion above

$$D^{\#} \cdot \mathscr{F}_A(e_a) = 1/\sqrt{m} \sum_{c \in A} e^{2\pi i(ac/m)} e_c$$

and the trace of $D^{\#} \cdot \mathscr{F}_A$ is

$$1/\sqrt{m} \sum_{c \in A} e^{2\pi i(a^2/m)}.$$

Such sums were studied by Gauss and play an important role in quadratic reciprocity over $\mathbb{Q}$. In the next section, we will study generalizations of these sums to general number fields and show how they enter into the quadratic reciprocity of such number fields.

II. The Trigonometric Sums of Hecke

Let $\mathfrak{k}$ be a number field of degree h over $\mathbb{Q}$. Consider $\mathfrak{k}$ as a $\mathbb{Q}$-vector space. Let $\mathrm{end}(\mathfrak{k})$ be the $\mathbb{Q}$-algebra of endomorphisms of $\mathfrak{k}$; and $\mathfrak{k}' = \mathrm{Hom}(\mathfrak{k}, \mathbb{Q})$ be the dual $\mathbb{Q}$-vector space. We will now see how the field structures of $\mathfrak{k}$ determine a $T \in \mathfrak{k}'$ and an isomorphism d: $\mathfrak{k} \to \mathfrak{k}'$.

To each $\alpha \in \mathfrak{k}$, let $r(\alpha) \in \mathrm{end}(\mathfrak{k})$ be defined by $r(\alpha)(\beta) = \alpha\beta$, $\beta \in \mathfrak{k}$. The mapping r: $k \to \mathrm{end}(\mathfrak{k})$ is a $\mathbb{Q}$-algebra isomorphism. We call r, the regular representation of $\mathfrak{k}$ over $\mathbb{Q}$. Let $\mathrm{tr}(\bar{X})$ denote the trace of $\bar{X} \in \mathrm{end}(\mathfrak{k})$. The mapping T: $\mathfrak{k} \to \mathbb{Q}$ given by $T(\alpha) = \mathrm{tr}(r(\alpha))$, $\alpha \in \mathfrak{k}$, is in $\mathfrak{k}'$. It is called the trace mapping of $\mathfrak{k}$ over Q. It is well known that the bilinear form t: $\mathfrak{k} \times \mathfrak{k} \to \mathbb{Q}$ defined by $t(\alpha, \beta) = T(\alpha\beta)$, $\alpha, \beta \in \mathfrak{k}$, is a non-degenerative, symmetric $\mathbb{Q}$-bilinear form. Thus, the corresponding mapping d: $\mathfrak{k} \to \mathfrak{k}'$ given by $d(\alpha)(\beta) = t(\alpha, \beta)$, $\alpha, \beta \in \mathfrak{k}$, is a $\mathbb{Q}$-linear isomorphism. In this way, the field structures of $\mathfrak{k}$, determine an identification of $\mathfrak{k}$ with $\mathfrak{k}'$.

The action of a group character, as considered in Section I, occurs here as well. Let U be the multiplicative group of complex numbers of absolute value 1. Consider $\mathfrak{k}$ as a group with respect to its addition and put $\mathfrak{k}^* = \mathrm{Hom}(\mathfrak{k}, U)$. We call $\mathfrak{k}^*$, the dual group of $\mathfrak{k}$. To each $\alpha' \in \mathfrak{k}'$, let $\alpha^* \in \mathfrak{k}^*$ be

given by $\alpha^*(\alpha) = e^{2\pi i \alpha'(\alpha)}$, $\alpha \in \mathfrak{k}$. The mapping $\alpha' \to \alpha^*$ is a monomorphism from the additive group of $\mathfrak{k}'$ into $\mathfrak{k}^*$.

Let M be a full module in $\mathfrak{k}$. Then, a basis $\alpha_1, \ldots, \alpha_h$ of $\mathfrak{k}$ over $\mathbb{Q}$ can be found such that $M = \oplus \sum_{i=1}^{h} \mathbb{Z}\alpha_i$. We will call this basis an integral basic relative to M. The dual of M with respect to T is the set M' defined by

$$M' = \{\alpha \in \ : T(\alpha M) \subset \mathbb{Z}\}.$$

For the remainder of this section, M will denote a full module in $\mathfrak{k}$. We will now establish certain basic properties of M'.

Let $\{\alpha_i\}$ be any basis of $\mathfrak{k}$ over $\mathbb{Q}$. The isomorphism $d: \mathfrak{k} \to \mathfrak{k}'$ implies the existence and uniqueness of a basis $\{\alpha_j'\}$ of $\mathfrak{k}$ over $\mathbb{Q}$, called the dual of $\{\alpha_i\}$, satisfying

$$\begin{aligned} T\{\alpha_i \alpha_j'\} &= 1, \qquad i = j, \\ &= 0, \qquad i \neq j. \end{aligned}$$

It follows that, if $\{\alpha_i\}$ is an integral basis for M then M' is a full module in $\mathfrak{k}$ having $\{\alpha_j'\}$ as an integral basis. We can immediately infer that $M'' = M$.

Now, take $\alpha \in \mathfrak{k}^x$ and form $(\alpha M)'$. If $\beta \in (\alpha M)'$ then $T(\beta(\alpha M)) = T((\beta\alpha)M) \subset \mathbb{Z}$ and $\beta\alpha \in M'$. Hence, $\beta \in (1/\alpha)M'$ and $(\alpha M)' \subset (1/\alpha)M'$. The reverse inclusion $(1/\alpha)M' \subset (\alpha M)'$ is established by reversing the argument. Thus, we may conclude that $(\alpha M)' = (1/\alpha)M'$.

Let M^2 be the group generated by all products mn, $m, n \in M$. Now, M^2 is a full lattice in $\mathfrak{k}$ since it is finitely generated and contains the full submodule mM, where m is any fixed non-zero element in M. Take $0 \neq \alpha \in (M^2)'$ and form $(\alpha M)'$. Since $\beta \in M$ implies

$$T(\beta(\alpha M)) \subset T(\alpha M^2) \subset \mathbb{Z}$$

it follows that $M \subset (\alpha M)'$. Thus, we can construct the abelian group

$$A = A(M, \alpha) = (\alpha M)'/M.$$

Observe, that M and $(\alpha M)'$ are full module in $\mathfrak{k}$ and hence A is a finite abelian group.

We want to define a symmetric isomorphism $D: A \to A^*$. For $\beta \in (\alpha M)'$, let $\chi(\beta)$: $(\alpha M)' \to U$ be the mapping defined by $\chi(\beta)(\gamma) = e^{2\pi i T(\alpha\beta\gamma)}$, $\gamma \in (\alpha M)'$. Clearly, $\chi(\beta)$ is a homomorphism and acts trivially on M. Thus, $\chi(\beta)$ induces a character $D(\beta)$ of $(\alpha M)'/M = A$. The mapping D: $(\alpha M)' \to A^*$ is a homomorphism which satisfies the short exact sequence

$$0 \to M \to (\alpha M)' \xrightarrow{D} A^* \to 1.$$

This can be seen as follows. Clearly, D is a homomorphism and $M \subset \ker D$. Take $\beta \in \ker D$ which implies $D(\beta)(c) = 1$ for all $c \in A$. Thus, $\chi(\beta)(\gamma) = e^{2\pi i T(\alpha\beta\gamma)} = 1$ for all $\gamma \in (\alpha M)'$ and $T(\beta\alpha(\alpha M)') \subset \mathbb{Z}$. Since $(\alpha M)' = 1/\alpha M'$, we have $\beta \in M'' = M$ and $\ker D \subset M$. We have established that $M = \ker D$. Since A and A^* have equal finite order the rest follows.

The short exact sequence implies that D induces an isomorphism, which we also denote by D, from A to A^*. This isomorphism$D$: $A \to A^*$ is clearly symmetric.

The selection of a full module M in $\mathcal{k}$ and a $0 \neq \alpha \in (M^2)'$ determines a finite abelian group $A = (\alpha M)'/M$ and a symmetric isomorphism D: $A \to A^*$. We are in the situation considered in Section I. Before we apply the results of Section I, observe that, if $b = \beta + M$, $c = \gamma + M$ are in A, where β, γ are in $(\alpha M)'$, we may unambiguously define $e^{2\pi i T(abc)} = e^{2\pi i T(\alpha\beta\gamma)}$. Then $\langle c, D(b)\rangle = e^{2\pi i T(abc)}$.

Let $\mathcal{F} = \mathcal{F}_A : L^2(A) \to L^2(A^*)$ be the Fourier transform of A and consider the unitary operator $D^{\#} \cdot \mathcal{F}$ of $L^2(A)$. By Section I,

$$D^{\#} \cdot \mathcal{F}(e_b) = 1/\sqrt{m} \sum_{c \in A} \langle b, D(c)\rangle e_c = 1/\sqrt{m} \sum_{c \in A} e^{2\pi i T(abc)} e_c, \qquad b \in A.$$

The trace of the unitary operator $D^{\#} \cdot \mathcal{F}$ is given by

$$G(M, \alpha) = 1/\sqrt{m} \sum_{b \in A} \langle b, D(b)\rangle = 1/\sqrt{m} \sum_{b \in A} e^{2\pi i T(ab^2)}.$$

Hecke considered trigonometric sums of this type (see [5]) and used them in the proof of the quadratic reciprocity law for the number field $\mathcal{k}$. The crucial step is a formula which evaluates certain sums of this type. For more recent derivations of closely related formulas, see Mlnor and Husemoller [6, especially Appendix 4]. There, a formula of Milgram, is discussed as well as the application of this formula to quadratic reciprocity laws. In the next section, we will assume a variant of the Milgram formula (see Theorem A below) and derive the quadratic reciprocity law for the number field $\mathcal{k}$.

Let $\mathcal{k}$ be our number field of degree h over $\mathbb{Q}$. As is well known, there are exactly h homomorphisms σ of $\mathcal{k}$ into $\mathbb{C}$ over $\mathbb{Q}$. Let these isomorphisms be $\sigma_1, \ldots, \sigma_s; \sigma_{s+1}, \bar{\sigma}_{s+1}, \ldots, \sigma_{s+t}, \bar{\sigma}_{s+t}$, $h = s + 2t$, where $\{\sigma_i : 1 \leqslant i \leqslant s\}$ consists of all those isomorphisms σ satisfying $\sigma(\mathcal{k}) \subset \mathbb{R}$ and $\bar{\sigma}_{s+j}$ is the complex conjugate of σ_{s+j}, $1 \leqslant j \leqslant t$. For $\beta \in \mathcal{k}^x$ and $1 \leqslant i \leqslant s$, let

$$\begin{aligned} \operatorname{sgn}_i(\beta) &= 1, \qquad \sigma_i(\beta) > 0, \\ &= -1, \qquad \sigma_i(\beta) < 0, \end{aligned}$$

and

$$S(\beta) = \sum_{i=1}^{s} \operatorname{sign}_i(\beta).$$

Let M be our full module in $\mathscr{k}$ and $0 \neq \alpha \in (M^2)'$. Then $4\alpha \in (M^2)'$ and we consider $G(M, 4\alpha)$.

THEOREM A. $G(M, 4\alpha) = 2^h e^{2\pi i S(\alpha)/8}$.

In Section IV, we will prove this result and see how it arises out of an understanding of the finite Fourier transform as an object related to the representation theory of finite nilpotent groups, especially the notion of an intertwining operator. In Section V, we will explicitly describe these intertwining operators and see how they can be derived from the multidimensional Cooley–Tukey algorithm [4] for computing the finite Fourier transform.

III. QUADRATIC RECIPROCITY

Let $\mathscr{k}$ be a number field of degree h over $\mathbb{Q}$. The ring $\mathscr{O}$ of algebraic integers in $\mathscr{k}$ is a full module in $\mathscr{k}$ and $\mathscr{O}^2 = \mathscr{O}$. For each non-zero $\alpha \in \mathscr{O}'$ consider the finite abelian group

$$A(\alpha) = A(\mathscr{O}, \alpha) = (\alpha\mathscr{O})'/\mathscr{O}$$

and the symmetries isomorphism

$$D(\alpha): A(\alpha) \to A(\alpha)^*$$

determined by the equation $\langle b, D(\alpha)(c)\rangle = e^{2\pi i T(\alpha bc)}$, $b, c \in A(\alpha)$, where T is the trace mapping of $\mathscr{k}$ over $\mathbb{Q}$. Let $D(\alpha)^{\#}$: $L^2(A^*(\alpha)) \to L^2(A(\alpha))$ be the linear isometry given by $D(\alpha)^{\#}(f^*) = f^* \cdot D(\alpha)$, $f^* \in L^2(A^*(\alpha))$ and consider this unitary operator

$$F(\alpha) = D(\alpha)^{\#} \cdot \mathscr{F}_{A(\alpha)}: L^2(A(\alpha)) \to L^2(A(\alpha)),$$

where $\mathscr{F}_{A(\alpha)}$ is the Fourier transform of $A(\alpha)$. Denote by

$$\sigma(\alpha) = \operatorname{tr}(F(\alpha)).$$

By the remarks of Section II,

$$F(\alpha)(e_b) = \frac{1}{\sqrt{m(\alpha)}} \sum_{c \in A(\alpha)} e^{2\pi i T(\alpha bc)} e_c, \qquad b \in A(\alpha),$$

$$G(\alpha) = \frac{1}{\sqrt{m(\alpha)}} \sum_{b \in A(\alpha)} e^{2\pi i T(\alpha b^2)},$$

where $m(\alpha) = o(A(\alpha))$ and $T: \mathcal{k} \to \mathbb{Q}$ is the trace mapping. Although, we do not have an explicit formula for $G(\alpha)$, by Theorem A, which we will assume throughout this section,

$$G(4\alpha) = 2^h e^{2\pi i S(\alpha)/8}.$$

Let $\mathcal{O}'$ be the dual of $\mathcal{O}$ with respect to T. To begin with, we will assume that

$$\mathcal{O}' = \delta \cdot \mathcal{O}, \qquad \delta \in \mathcal{k}.$$

This condition will be removed eventually.

Let $\alpha \in \mathcal{O}'$, $\alpha \neq 0$, be fixed. We will now introduce a group of unitary operators of $L^2(A(\alpha))$. Firstly, take $\beta/\delta \in \mathcal{O}$ relatively prime to α/δ in $\mathcal{O}$. Thus, $\mathcal{O} = (\alpha/\delta)\mathcal{O} + (\beta/\delta)\mathcal{O}$. Since $(\alpha\mathcal{O})'$ is an $\mathcal{O}$-module, the mapping, $\gamma \to (\beta/\delta)\gamma$, $\gamma \in (\alpha\mathcal{O})'$, is easily seen to be an isomorphism of $(\alpha\mathcal{O})'$ into itself. Moreover, it maps $\mathcal{O}$ into itself and hence, induces a homomorphism, denoted by $\zeta_\alpha(\beta)$, of $A(\alpha)$. We will show that it is an automorphism. Since $A(\alpha)$ has finite order, it suffices to show that, if $\gamma \in (\alpha\mathcal{O})'$ and $(\beta/\delta)\gamma \in \mathcal{O}$ then $\gamma \in \mathcal{O}$. Choose $u, v \in \mathcal{O}$ such that $(\alpha/\delta)u + (\beta/\delta)v = 1$. Then

$$(1 - (\alpha/\delta)u)\gamma = v(\beta/\delta)\gamma \in v \cdot \mathcal{O},$$

$$\gamma \in v\mathcal{O} + (\alpha/\delta)\, u\gamma \subset v\mathcal{O} + u(\alpha/\delta)(\alpha\mathcal{O})' = v\mathcal{O} + u\mathcal{O} = \mathcal{O}.$$

Thus, $\zeta_\alpha(\beta)$ is an automorphism of $A(\alpha)$.

LEMMA 3.1. *Let $(\mathcal{O}/(\alpha/\delta)\mathcal{O})^x$ denote the multiplicative group of units in the ring $\mathcal{O}/(\alpha/\delta)\mathcal{O}$ and $U(L^2(A(\alpha)))$ denote the group of unitary operators of $L^2(A(\alpha))$. Then there exists a faithful representation $\zeta_\alpha^{\#}$: $(\mathcal{O}/(\alpha/\delta)\mathcal{O})^x \to U(L^2(A(\alpha)))$ satisfying the condition*

$$\zeta_\alpha^{\#}(b) f = f \cdot \zeta_\alpha(\beta),$$

where

$$f \in L^2(A(\alpha)), \qquad b \in (\mathcal{O}/(\alpha/\delta)\mathcal{O})^x,$$

and

$$b = \beta/\delta + (\alpha/\delta)\mathcal{O}$$

in any coset representation.

Proof. For $b \in \mathcal{O}/(\alpha/\delta)\mathcal{O}$, we have $b \in (\mathcal{O}/(\alpha/\delta)\mathcal{O})^x$ if and only if whenever we represent $b = \beta/\delta + a/\delta\mathcal{O}$, it follows that β/δ is relatively prime to α/δ in $\mathcal{O}$. Also, observe that $\zeta_\alpha(\beta) = \zeta_\alpha(\beta + \alpha u)$, for all $u \in \mathcal{O}$. Thus, if $b \in (\mathcal{O}/(\alpha/\delta)\mathcal{O})^x$ we may, without ambiguity, define $\zeta_\alpha(b) = \zeta_\alpha(\beta)$, where

$b = \beta/\delta + (\alpha/\delta)\mathcal{O}$ is any representation. The resulting mapping, ζ_α: $(\mathcal{O}/(\alpha/\delta)\mathcal{O})^x \to \mathrm{aut}(A(\alpha))$ is clearly an isomorphism.

Now, let $\zeta_\alpha^{\#}$: $(\mathcal{O}/(\alpha/\delta)\mathcal{O})^x \to U(L^2(A(\alpha)))$ be defined by $\zeta_\alpha^{\#}(b)f = f \cdot \zeta_\alpha(b)$, $f \in L^2(A(\alpha))$ and $b \in (\mathcal{O}/(\alpha/\delta)\mathcal{O})^x$. The lemma follows.

Remarks. Let $b \in (\mathcal{O}/(\alpha/\delta)\mathcal{O})^x$ and $c \in A(\alpha)$. Put $bc = \zeta_\alpha(b)(c)$. Then, $\zeta_\alpha^{\#}(b)\, f(c) = f(bc)$.

We will now study the relationship between the unitary operator $F(\alpha)$ of $L_2(A(\alpha))$ and the group representation $\zeta_\alpha^{\#}$: $(\mathcal{O}/(\alpha/\delta)\mathcal{O})^x \to U(L^2(A(\alpha)))$.

LEMMA 3.2. *Let $b \in (\mathcal{O}/(\alpha/\delta)\mathcal{O})^x$. Then*

$$F(\alpha)\, \zeta_\alpha(b) = \zeta_\alpha(b)^{-1}\, F(\alpha).$$

Proof. Choose $b^{-1} \in (\mathcal{O}/(\alpha/\delta)\mathcal{O})^x$. Then, for $c \in A(\alpha)$,

$$\zeta_\alpha(b^{-1})\, F(\alpha)(e_c) = \frac{1}{\sqrt{m(\alpha)}} \sum_{d' \in A(\alpha)} e^{2\pi i T(\alpha c d')}\, e_{b^{-1}d'}.$$

The mapping $d' \to \zeta_\alpha(b)^{-1}d' = b^{-1}d'$ is an automorphism of $A(\alpha)$. Thus, we can replace $b^{-1}d'$ by d and sum over $d \in A(\alpha)$ in the last sum. The result is

$$\frac{1}{\sqrt{m(\alpha)}} \sum_{d \in A(\alpha)} e^{2\pi i T(\alpha b c d)}\, e_d,$$

which is easily seen to be $F(\alpha)\, \zeta_\alpha(b)(e_c)$ and the lemma has been verified.

COROLLARY 3.2.1. *Let $b \in (\mathcal{O}/(\alpha/\delta)\mathcal{O})^x$ be a perfect square, i.e., $b = x^2$, for some $x \in (\mathcal{O}/(\alpha/\delta)\mathcal{O})^x$. Then*

$$F(\alpha)\, \zeta_\alpha(b) = \zeta_\alpha(x)^{-1}\, F(\alpha)\, \zeta_\alpha(x).$$

Proof. Simply observe, using the lemma, that

$$F(\alpha)\, \zeta_\alpha(b) = F(\alpha)\, \zeta_\alpha(x^2) = F(\alpha)\, \zeta_\alpha(x)^2 = \zeta_\alpha(x)^{-1}\, F(\alpha)\, \zeta_\alpha(x).$$

COROLLARY 3.2.2. *Let $b \in (\mathcal{O}/(\alpha/\delta)\mathcal{O})^x$. Then*

$$\mathrm{tr}(F(\alpha)\, \zeta_\alpha(b)) = \frac{1}{\sqrt{m(\alpha)}} \sum_{c \in A(\alpha)} e^{2\pi i T(\alpha b c^2)}.$$

Proof. The proof of Lemma 3.2 implies this result.

The trigonometric sum in this corollary is called a generalized Hecke sum. We will write

$$G(a, b) = \mathrm{tr}(F(a)\,\zeta_a(b)).$$

Corollary 3.2.1 easily implies the next corollary.

COROLLARY 3.2.3. *If* $b \in (\mathcal{O}/(a/\delta)\mathcal{O})^x$ *is a perfect square, then*

$$G(a, b) = G(a).$$

The same argument shows the following generalization.

COROLLARY 3.2.4. *Let* $c, b \in (\mathcal{O}/(a/\delta)\mathcal{O})^x$, b *a perfect square. Then*

$$G(a, bc) = G(a, c).$$

We will now piece together the various operators $F(a)$, $a \in \mathcal{O}'$. The basic tool in the process is the tensor product.

Let a/δ and β/δ be relatively prime elements in $\mathcal{O}$. Then, $(a\mathcal{O})' \subset ((a\beta/\delta)\mathcal{O})'$ and $(\beta\mathcal{O})' \subset ((a\beta/\delta)\mathcal{O})'$ and if follows that $A(a) \subset A(a\beta/\delta)$ and $A(\beta) \subset A(a\beta/\delta)$.

LEMMA 3.3. $A(a\beta/\delta) = A(a) \oplus A(\beta)$.

Proof. If suffices to show that $A(a) \cap A(\beta) = (0)$ or equivalently $(a\mathcal{O})' \cap (\beta\mathcal{O})' = \mathcal{O}$, since $o(A(a\beta/\delta)) = o(A(a))\, o(A(\beta))$. Let $\gamma \in (a\mathcal{O})' \cap (\beta\mathcal{O})'$ and write $\gamma = (\delta/a)u = (\delta/\beta)v$, $u, v \in \mathcal{O}$. Find $r, s \in \mathcal{O}$ such that $(a/\delta)r + (\beta/\delta)s = 1$. Then,

$$s\frac{\beta}{\delta}u = s\frac{a}{\delta}v = \left(1 - \frac{a}{\delta}r\right)u.$$

If follows that $\gamma = (\delta/a)u = vs + ur \in \mathcal{O}$, which is what we intended to prove.

For $f \in L^2(A(a))$ and $g \in L^2(A(\beta))$, consider $\pi(f, g) \in L^2(A(a\beta/\delta))$ defined by $\pi(f, g)(a + b) = f(a)\, g(b)$, $a \in A(a)$, $b \in A(\beta)$. The mapping

$$\pi: L^2(A(a)) \times L^2(A(\beta)) \to L^2(A(a\beta/\delta))$$

is $\mathbb{C}$-bilinear and hence defines, by definition, a $\mathbb{C}$-linear homomorphism

$$\pi^{\#}: L^2(A(a)) \otimes L^2(A(\beta)) \to L^2(A(a\beta/\delta))$$

uniquely determined by the condition $\pi^{\#}(f \otimes g) = \pi(f, g)$.

LEMMA 3.4. *There is a* $\mathbb{C}$*-linear isomorphism*

$$\pi^{\#}: L^2(A(\alpha)) \otimes L^2(A(\beta)) \to L^2(A(\alpha\beta/\delta))$$

uniquely determined by the condition $\pi^{\#}(f \otimes g) = \pi(f, g)$.

Proof. It remains to show that $\pi^{\#}$ is an isomorphism. Let

$$e_a \in L^2(A(\alpha)), a \in A(\alpha) \qquad \text{and} \qquad e_b \in L^2(A(\beta)), b \in A(\beta).$$

Then, $\pi^{\#}(e_a \otimes e_b)(x + y) = e_a(x)\, e_b(y)$. Hence, the basis $\{e_a \otimes e_b\}$ of $L^2(A(\alpha)) \otimes L^2(A(\beta))$ is taken by $\pi^{\#}$ onto the basis $\{e_{a+b}\}$ of $L^2(A(\alpha\beta/\delta))$.

By abuse of language, we will write $f \otimes g = \pi^{\#}(f \otimes g)$.

Let V and W be arbitrary vector spaces over a field F and $V \otimes W$ their tensor product. Then

$$\mathrm{End}(V) \otimes \mathrm{End}(W) \cong \mathrm{End}(V \otimes W),$$

where, by abuse of language, we put $X \otimes Y \in \mathrm{End}(V \otimes W)$ defined by $X \otimes Y(v \otimes w) = X(v) \otimes X(w)$.

LEMMA 3.5. *Let* α/δ *and* β/δ *be relatively prime elements in* $\mathcal{O}$. *Then*

$$F\left(\frac{\alpha\beta}{\delta}\right) = F(\alpha)\, \zeta_\alpha(b) \otimes F(\beta)\, \zeta_\beta(\alpha),$$

where

$$a = \frac{\alpha}{\delta} + \frac{\beta}{\delta}\mathcal{O} \in \left(\mathcal{O}\Big/\frac{\beta}{\delta}\mathcal{O}\right)^{\times} \qquad \text{and} \qquad b = \frac{\beta}{\delta} + \frac{\alpha}{\delta}\mathcal{O} \in \left(\mathcal{O}\Big/\frac{\alpha}{\delta}\mathcal{O}\right)^{\times}.$$

Proof. Let $a' \in A(\alpha)$ and $b' \in A(\beta)$. Then $e_{a'+b'} = e_{a'} \otimes e_{b'}$ and

$$F\left(\frac{\alpha\beta}{\delta}\right)(e_{a'+b'}) = \frac{1}{\sqrt{m(\alpha\beta/\delta)}} \sum_{c'' \in A(\alpha\beta/\delta)} e^{2\pi i T((\alpha\beta/\delta)(a'+b')c'')}\, e_{c''}.$$

$$F(\alpha)\, \zeta_\alpha(b) \otimes F(\beta)\, \zeta_\beta(a)(z_{a'} \otimes e_{b'}) = F(\alpha)\, \zeta_\alpha(b)(e_{a'}) \otimes F(\beta)\, \zeta_\beta(a)(e_{b'})$$

$$= \frac{1}{\sqrt{m(\alpha)}} \sum_{c \in A(\alpha)} e^{2\pi i T(\alpha a' b c)}\, e_c \otimes \frac{1}{\sqrt{m(\beta)}} \sum_{c' \in A(\beta)} e^{2\pi i T(\beta b' a c')}\, e_{c'}$$

$$= \frac{1}{\sqrt{m(\alpha)}\sqrt{m(\beta)}} \sum_{\substack{c \in A(\alpha) \\ c' \in A(\beta)}} e^{2\pi i T(\alpha a' b c + \beta b' a c')}\, e_c \otimes e_{c'}.$$

As can be checked,

$$T(\alpha a'bc + \beta b'ac') = T((\alpha a'b + \beta b'a)(c + c')) = T((\alpha b + \beta a)(a' + b')(c + c'))$$
$$= T((\alpha\beta/\delta)(a' + b')(c + c')).$$

Thus, since $e_c \otimes e_{c'} = e_{c+c'}$ and $m(\alpha\beta/\delta) = m(\alpha)\, m(\beta)$, we can write

$$F(\alpha)\, \zeta_\alpha(b) \otimes F(\beta)\, \zeta_\beta(a)(e_{a'} \otimes e_{b'})$$
$$= \frac{1}{\sqrt{m(\alpha\beta/\delta)}} \sum_{\substack{c \in A(\alpha) \\ c' \in A(\beta)}} e^{2\pi i T((\alpha\beta/\delta)(a'+b')(c+c'))} e_{c+c'}.$$

Letting $c'' = c + c'$, by Lemma 3.3, the lemma follows.

COROLLARY 3.5.1. *If α/δ and β/δ are relatively prime in $\mathcal{O}$, then*

$$G\left(\frac{\alpha\beta}{\delta}\right) = G(\alpha, b) \cdot G(\beta, a),$$

where

$$a = \alpha/\beta + \beta/\delta\mathcal{O} \in \left(\mathcal{O}\Big/\frac{\beta}{\delta}\mathcal{O}\right)^x \qquad \text{and} \qquad b = \beta/\delta + \alpha/\delta\mathcal{O} \in \left(\mathcal{O}\Big/\frac{\alpha}{\delta}\mathcal{O}\right)^x.$$

The above results, especially Corollary 3.5.1, will now be applied to the problem of evaluating $G(\alpha)$, for general $\alpha \in \mathcal{O}'$. We will still assume the formula for $G(4\alpha)$, given by Theorem A. Also, we will use the notation $G(\alpha; \beta)$, where $\beta \in \mathcal{O}$ is relatively prime to α/δ, to mean $G(\alpha; b)$, where $b = \beta + \alpha/\delta\mathcal{O} \in (\mathcal{O}/\alpha/\delta\mathcal{O})^x$.

An element $\gamma \in \mathcal{O}$ will be called odd, if γ and 2 are relatively prime in $\mathcal{O}$. If $\gamma \in \mathcal{O}$ is odd then γ and 4 are relatively prime as well. We may see this as follows. Suppose γ is odd and find $u, v \in \mathcal{O}$ such that $\gamma u + 2v = 1$. Then,

$$\gamma(\gamma u^2 + 4uv) + 4v^2 = 1, \qquad \gamma u^2 + 4uv \in \mathcal{O},\ v^2 \in \mathcal{O}.$$

LEMMA 3.6. *Let α/δ be odd. Then*

$$G(4\alpha) = G(\alpha; 4)\, G(4\delta, \alpha/\delta) = G(\alpha)\, G(4\delta, \alpha/\delta).$$

Proof. Apply Corollary 3.5.1, with $\beta = 4\delta$ and Corollary 3.2.3.

Theorem A implies $G(4\alpha) \neq 0$; thus neither factor on the right vanishes. This gives us an expression for $G(\alpha)$; namely,

$$G(\alpha) = \frac{G(4\alpha)}{G(4\delta, \alpha/\delta)}.$$

Since, by Theorem A, $G(4\alpha)$ is known, we know $G(\alpha)$ once we evaluate $G(4\delta, \alpha/\delta)$. In general,

$$G(4\delta, \alpha/\delta) = 2^{-h} \sum_{c \in (1/4)\mathcal{O}/\mathcal{O}} e^{2\pi i T(4\alpha c^2)} = 2^{-h} \sum_{c \in \mathcal{O}/4\mathcal{O}} e^{\pi i T(\alpha c^2)/2}.$$

COROLLARY 3.6.1. *Let α/δ be odd and a perfect square* mod $4\mathcal{O}$. *Then* $G(4\delta, \alpha/\delta) = G(4\delta)$. *Moreover,*

$$G(\alpha) = \frac{G(4\alpha)}{G(4\delta)} = e^{\pi i/4(S(\alpha)-S(\delta))},$$

where $S(\alpha) = \sum_{i=1}^{s} \operatorname{sgn}_i(\alpha)$.

Let P be a prime ideal in $\mathcal{O}$. $\mathcal{O}/P = F$ is a finite field and the multiplicative subgroup F^x of non-zero elements of F is cyclic. For $a \in F^x$, define

$$\begin{aligned} (a/P) &= 1 \qquad \text{if } a = x^2 \text{ for some } x \in F^x \\ &= -1 \qquad \text{otherwise.} \end{aligned}$$

We call (a/P), the Legendre symbol of a with respect to P. It is easy to see that the mapping

$$a \to (a/P)\colon\ F^x \to \{+1, -1\}$$

is a character of F^x. We may extend this notation as follows. Let $\alpha \in \mathcal{O}$ and $\alpha \notin P$. Then $a = \alpha + P \in F^x$ and we put $(\alpha/P) = (a/P)$ and observe that (α/P) is well defined.

In particular, we shall apply these definitions to an odd prime element α/δ in $\mathcal{O}$. Then, we have the following relationship between the Legendre symbol with respect to $P = \alpha/\delta\mathcal{O}$ and Hecke sums. Let $a = \alpha/\delta$ be an odd prime in $\mathcal{O}$ in what follows and write $(b/a) = (b/a\mathcal{O})$, $b \notin a \cdot \mathcal{O}$.

LEMMA 3.7. *Let $b \notin a \cdot \mathcal{O}$. Then*

$$\left(\frac{b}{a}\right) = \frac{G(\alpha; b)}{G(\alpha)}.$$

Proof. Let b_1 be a generator of $(\mathcal{O}/a\mathcal{O})^x$ and suppose its order is m. Then

$$\left(\frac{b_1^j}{a}\right) = (-1)^j.$$

On the other hand, by Corollary 3.2.4, $G(\alpha; b_1^j) = G(\alpha)$, j is even, and $G(\alpha; b_1^j) = G(\alpha; b_1)$, j is odd. Thus, to prove the lemma is sufficient to show $G(\alpha; b_1) = -G(\alpha)$. Now,

$$\sqrt{m(\alpha)}\, G(\alpha) = \sum_{c \in A(\alpha)} e^{2\pi i T(\alpha c^2)} = 1 \sum_{j=0}^{m-1} e^{2\pi i T((\delta/a) b_1^{2j})},$$

$$\sqrt{m(\alpha)}\, G(\alpha; b_1) = \sum_{c \in A(\alpha)} e^{2\pi i T(\alpha b_1 c^2)} = 1 + \sum_{j=0}^{m-1} e^{2\pi i T((\delta/a) b_1^{2j+1})},$$

$$\begin{aligned}\sqrt{m(\alpha)}(G(\alpha) + G(\alpha; b_1)) &= 2 + 2 \sum_{b \in (\mathcal{O}/a\mathcal{O})^x} e^{2\pi i T((\delta/a)b)} \\ &= 2 \cdot \sum_{b \in \mathcal{O}/a\mathcal{O}} e^{2\pi i T((\delta/a)b)} = 0\end{aligned}$$

since the mapping, $b \to e^{2\pi i T((\delta/a)b)}$, is a non-trivial character of $\mathcal{O}/a\mathcal{O}$.

THEOREM 3.1. *Assume $\mathcal{O}' = \delta\mathcal{O}$. Let a, b be non-associative odd primes in $\mathcal{O}$. Then*

$$\left(\frac{a}{b}\right)\left(\frac{b}{a}\right) = e^{\pi i/4 T(\delta(ab-a-b))} \frac{G(4; a)\, G(4; b)}{G(4; ab)}.$$

Moreover, if a is a square mod $4\mathcal{O}$, *then*

$$\left(\frac{a}{b}\right)\left(\frac{b}{a}\right) = e^{\pi i \sum_{i=1}^{q} ((\operatorname{sgn}_i(a)-1)/2)((\operatorname{sgn}_i(b)-1)/2)}$$

Proof. By Lemma 3.7,

$$\left(\frac{a}{b}\right)\left(\frac{b}{a}\right) = \frac{G(b \cdot \delta; a)}{G(b \cdot \delta)} \frac{G(a \cdot \delta; b)}{G(a \cdot \delta)}.$$

Applying Corollary 3.5.1, to the numerator,

$$\left(\frac{a}{b}\right)\left(\frac{b}{a}\right) = \frac{G(ab \cdot \delta)}{G(b\delta)\, G(a\delta)}.$$

Corollary 3.6.1 implies

$$G(ab\delta) = \frac{G(4ab\delta)}{G(4\delta; ab)},$$

$$G(b\delta) = \frac{G(4b\delta)}{G(4\delta; b)},$$

$$G(a\delta) = \frac{G(4a\delta)}{G(4\delta; a)}$$

from which it follows,

$$\left(\frac{a}{b}\right)\left(\frac{b}{a}\right)=\frac{G(4ab\delta)}{G(4\delta;ab)}\frac{G(4\delta;a)\,G(4\delta;b)}{G(4b\delta)\,G(4a\delta)},$$

$$\left(\frac{a}{b}\right)\left(\frac{b}{a}\right)=\frac{G(4ab\delta)}{G(4b\delta)\,G(a\delta)}\frac{G(4\delta;b)\,G(4\delta;a)}{G(4\delta;ab)}.$$

By Theorem A,

$$G(4ab\delta)=2^h e^{\pi i/4S(ab\delta)},$$

$$G(4b\delta)=2^h e^{\pi i/4S(b\delta)},$$

$$G(4a\delta)=2^h e^{\pi i/4S(a\delta)}.$$

Thus,

$$\left(\frac{a}{b}\right)\left(\frac{b}{a}\right)=2^{-h}e^{\pi i/4S(ab\delta-b\delta-a\delta)}\frac{G(4\delta;b)\,G(4\delta;a)}{G(4\delta;ab)},$$

proving the first assertion. Suppose a is a perfect square mod $4\mathcal{O}$. Then

$$G(4\delta;ab)=G(4\delta;b),$$

$$G(4\delta;a)=G(4\delta).$$

The formula now becomes

$$\left(\frac{a}{b}\right)\left(\frac{b}{a}\right)=e^{\pi i/4S(ab\delta-b\delta-a\delta+\delta)}.$$

Now, $\operatorname{sgn}_i(rs)=\operatorname{sgn}_i(r)\operatorname{sgn}_i(s)$, from which it follows,

$$\operatorname{sgn}_i(ab\delta)-\operatorname{sgn}_i(b\delta)-\operatorname{sgn}_i(a\delta)+\operatorname{sgn}_i(\delta)=\operatorname{sgn}_i(\delta)((\operatorname{sgn}_i(a)-1)(\operatorname{sgn}_i(b)-1)).$$

Thus,

$$\left(\frac{a}{b}\right)\left(\frac{b}{a}\right)=(-1)^{\sum_{i=1}^{\bar{l}}\operatorname{sgn}_i(\delta)((\operatorname{sgn}_i(a)-1)/2)((\operatorname{sgn}_i(b)-1)/2)}$$

and since $(\operatorname{sgn}_i(a)-1)/2$ and $(\operatorname{sgn}_i(b)-1)/2$ are integers. The theorem follows.

The condition $\mathcal{O}'=\delta\mathcal{O}$ was convenient to assume, in that, it provided a framework in which to carry out the required computations. We will now remove this condition, but will have to introduce certain auxiliary ideals to assist in ensuring sufficient structures for those computations which must now be treated. Also, the ideal theory of $\mathcal{O}$ will have to be examined more closely. In particular, the structure theory of the set of non-trivial fractional

ideals will play a central role. For the most part, we will assume that the elementary contents of the theory are known. Especially that, this set is a group under ideal multiplication and is freely generated by the prime ideals in $\mathcal{O}$. To the depth required, this theory can be found in [5, pp. 41–50]. Let a and b be relatively prime elements in $\mathcal{O}$. Since $\mathcal{O}'$ is a fractional ideal, we can find an integral ideal C satisfying the following two conditions:

(i) $C + (ab)\mathcal{O} = \mathcal{O}$,

(ii) $C\mathcal{O}' = \delta\mathcal{O}$ for some $\delta \in \mathcal{O}'$.

Let C be specified satisfying these conditions. $\mathcal{O}'$ as an $\mathcal{O}$-module can be generated by two elements, one of which can be chosen in C. Thus,

$$\mathcal{O}' = \omega\mathcal{O} + \zeta\mathcal{O}, \qquad \omega \in \mathcal{O}',\ \zeta \in C.$$

Consider the mapping

$$\gamma \to \omega\gamma\colon \mathcal{O} \to \mathcal{O}'.$$

Clearly, the mapping is an $\mathcal{O}$-module homomorphism taking C into $C\mathcal{O}'$ and hence, induces an $\mathcal{O}$-module homomorphism

$$\mathcal{O}/C \to \mathcal{O}'/C\mathcal{O}.$$

Let $\gamma' \in \mathcal{O}'$ and write $\gamma' = \omega\gamma + \zeta C$, γ, $C \in \mathcal{O}$. Then $\gamma' = \omega\gamma \bmod C\mathcal{O}'$, since $\zeta \in C$, implying that this latter $\mathcal{O}$-module homomorphism is surjective. Let

$$K = \{\gamma \in \mathcal{O}\colon \omega\gamma \in C\mathcal{O}'\}.$$

K is an ideal of $\mathcal{O}$ containing C. Also,

$$K\mathcal{O}' = \omega K + \zeta K \subset C\mathcal{O}' + C = C\mathcal{O}'$$

and since $C\mathcal{O}' \subset K\mathcal{O}'$ as well, we have $C\mathcal{O}' = K\mathcal{O}' = \delta \cdot \mathcal{O}$. Thus, the mapping, $\gamma \to \omega\gamma$, induces an isomorphism of $\mathcal{O}/K$ onto $\mathcal{O}'/K\mathcal{O}'$, where K is an integral ideal satisfying conditions (i) and (ii). We organize this discussion in the following lemma.

LEMMA 3.8. *Let a and b be relatively prime elements in $\mathcal{O}$. Then there exist an integral ideal K and a decomposition $\mathcal{O}' = \omega\mathcal{O} + \zeta\mathcal{O}$, where $\zeta \in K$, satisfying the following conditions*:

(i) *$K\mathcal{O}' = \delta \cdot \mathcal{O}$ for some $\delta \in \mathcal{O}'$,*

(ii) *$K + (ab)\mathcal{O} = \mathcal{O}$,*

(iii) *the mapping, $\gamma \to \omega\gamma$: $\mathcal{O} \to \mathcal{O}'$, induces an isomorphism of $\mathcal{O}/K$ onto $\mathcal{O}'/K\mathcal{O}'$.*

The application of the lemma, in subsequent work, will be to permit the writing of a trigonometric sum indexed over $\mathcal{O}'/K\mathcal{O}'$ as a trigonometric sum indexed over $\mathcal{O}/K$.

For the remainder of this work, we will assume that the relatively prime elements a and b on $\mathcal{O}$, the integral ideal K and decomposition $\mathcal{O}' = \omega\mathcal{O} + \zeta\mathcal{O}$, where $\zeta \in K$, have been chosen, once and for all, satisfying the conditions of the lemma. Let $\alpha = a\delta$ and $\beta = b\delta$. Consider the group $A(\alpha) = (\alpha\mathcal{O})'/\mathcal{O}$. Since $(\alpha\mathcal{O})'$ is an $\mathcal{O}$-module, we can consider the mapping

$$\gamma \to b_1\gamma\colon (\alpha\mathcal{O})' \to (\alpha\mathcal{O})',$$

where $b_1 \in \mathcal{O}$. This mapping is an $\mathcal{O}$-module homomorphism taking $\mathcal{O}'$ into itself. Thus, it induces a homomorphism

$$\zeta_\alpha(b_1)\colon A(\alpha) \to A(\alpha).$$

Assume now that b_1 is chosen relatively prime to both a and K, or equivalently, relatively prime to aK. We will show in this case $\zeta_\alpha(b_1)$ is an automorphism of $A(\alpha)$. Since $A(\alpha)$ has finite order it suffices to carry out the proof injectively. This will follow if we can show that $\gamma \in (\alpha\mathcal{O})'$ and $b_1\gamma \in \mathcal{O}$ implies $\gamma \in \mathcal{O}$. Write

$$1 = b_1x + ak, \qquad x \in \mathcal{O},\ k \in K.$$

Then $\gamma = b_1\gamma x + a\gamma k \in \mathcal{O} + a(1/\alpha)\,k\mathcal{O}' \subset \mathcal{O} + (1/\delta)\,K\mathcal{O}' = \mathcal{O}$ as we needed to prove.

For $x \in \mathcal{O}$, denote the image of x in $\mathcal{O}/aK$ by $\mathbf{x}$. Then, x is relatively prime to aK if and only if $\mathbf{x} \in (\mathcal{O}/aK)^x$. Suppose $\mathbf{x} = \mathbf{y}$ and hence $x = y + ak$, $k \in K$. For $\gamma \in (\alpha\mathcal{O})'$,

$$\gamma x = \gamma y + \gamma ak \equiv \gamma y \bmod \mathcal{O}$$

since $\gamma ak \in (1/\alpha)ak\mathcal{O}' = (1/\delta)\,K\mathcal{O}' = \mathcal{O}$. Thus $\zeta_\alpha(x) = \zeta_\alpha(y)$ and we can, unambiguously, define

$$\zeta_\alpha(\mathbf{x}) = \zeta_\alpha(x), \qquad \mathbf{x} \in (\mathcal{O}/aK)^x.$$

Consider, now, the mapping $\mathbf{x} \to \zeta_\alpha(\mathbf{x})$. Let $\mathbf{x}, \mathbf{y} \in (\mathcal{O}/aK)^x$ and $\gamma \in (\alpha\mathcal{O})'$. Clearly, $x(y\gamma) = (xy)\gamma$ and it follows that

$$\zeta_\alpha(\mathbf{x})\,\zeta_\alpha(\mathbf{y}) = \zeta_\alpha(\mathbf{xy}).$$

We summarize this discussion in the next lemma.

LEMMA 3.9. *The mapping*

$$\mathbf{x} \to \zeta_\alpha(\mathbf{x})\colon (\mathcal{O}/aK)^x \to \mathrm{aut}(A(\alpha))$$

is a homomorphism.

For $\mathbf{x} \in (\mathcal{O}/aK)^x$, let $\zeta_\alpha^\#(\mathbf{x})$ denote the unitary operator of $L^2(A(\alpha))$ defined by

$$\zeta_\alpha^\#(\mathbf{x}) f = f \cdot \zeta_\alpha^\#(\mathbf{x}), \qquad f \in L^2(A(\alpha)).$$

The following corollary is now obvious.

COROLLARY 3.9.1. *The mapping*

$$\mathbf{x} \to {}^\#_\alpha(\mathbf{x})\colon (\mathcal{O}/aK)^x \to \mathrm{aut}(L^2(A(\alpha)))$$

is a unitary representation of the group $(\mathcal{O}/aK)^x$ *on* $L^2(A(\alpha))$.

As before, we will study the relationship between the unitary representation $\zeta_\alpha^\#$ and the unitary operator $F(\alpha)$. The following results, Lemma 3.10 and its corollaries, can be proved in exactly the same way as the analogous results considered in the beginning of this section. We will state them without proof.

Consider $F(\alpha)\, \zeta_\alpha^\#(\mathbf{x})$, with $\mathbf{x} \in (\mathcal{O}/aK)^x$, and define

$$G(\alpha; \mathbf{x}) = \mathrm{tr}(F(\alpha)\, \zeta_\alpha^\#(\mathbf{x})).$$

LEMMA 3.10. *For* $\mathbf{x} \in (\mathcal{O}'aK)^x$,

$$F(\alpha)\, \zeta_\alpha^\#(\mathbf{x}) = \zeta_\alpha^\#(\mathbf{x})^{-1} F(\alpha).$$

COROLLARY 3.10.1. *For* $c \in A(\alpha)$,

$$F(\alpha)\, \zeta_\alpha(\mathbf{x})(e_c) = m(\alpha)^{-1/2} \sum_{c' \in A(\alpha)} e^{2\pi i T(\alpha x c c')} e_{c'}.$$

COROLLARY 3.10.2. $G(\alpha; \mathbf{x}) = m(\alpha)^{-1/2} \sum_{c \in A(\alpha)} e^{2\pi i T(\alpha x c^2)}$.

COROLLARY 3.10.3. *If* $\mathbf{x}$ *is a perfect square on* $(\mathcal{O}/aK)^x$ *then*

$$G(\alpha; \mathbf{xy}) = G(\alpha; \mathbf{y})$$

for all $\mathbf{y} \in (\mathcal{O}/aK)^x$.

The tensor product formula expressed by Lemma 3.5 and its corollaries

does not exactly generalize. Although, $A(\alpha)$ and $A(\beta)$ are both subgroups of $A(\alpha\beta/\delta)$ and

$$A(\alpha\beta/\delta) = A(\alpha) + A(\beta),$$

the sum is not a direct sum. Indeed,

$$A(\alpha) \cap A(\beta) = A(\delta).$$

However, we do have the following result.

LEMMA 3.11. $A(\alpha) = (1/a)\mathcal{O}/\mathcal{O} \oplus A(\delta)$.

Proof. Observe that both $A(\delta)$ and $(1/a)\mathcal{O}/\mathcal{O}$ are subgroups of $A(\alpha)$. Since $o(A(\alpha)) = o(A(\delta))\, o((1/a)\mathcal{O}/\mathcal{O})$, the lemma will be proved once we show $A(\delta) \cap (1/a)\mathcal{O}/\mathcal{O} = (0)$. It is equivalent to showing $(1/a)\mathcal{O} \cap (\delta\mathcal{O})' = \mathcal{O}$. Take $\gamma \in (1/a)\mathcal{O} \cap (\delta\mathcal{O})'$. Since $a\mathcal{O} + K = \mathcal{O}$, we can write $1 = ax + k$, $x \in \mathcal{O}$, $k \in K$. Thus

$$\gamma = a\gamma x + \gamma k \subset a \cdot \frac{1}{a}\mathcal{O} + \frac{1}{\delta} K\mathcal{O}' = \mathcal{O}.$$

Let $A_1(a) = (1/a)\mathcal{O}/\mathcal{O}$. We will now consider $\mathcal{F}_1(a)$, the Fourier transform of $A_1(a)$. Consider the mapping, $D_1(a)$: $A_1(a) \to A_1(a)^*$, given by the formula

$$\langle c, D_1(a)c' \rangle = e^{2\pi i T(acc')}, \qquad c, c' \in A_1(a).$$

It is easy to verify that $D_1(a)$ is well defined and that it is a symmetric isomorphism, in the sense of Section I. Set

$$F_1(a) = D_1^* \cdot \mathcal{F}_1(a).$$

By the comments in Section I,

$$F_1(a)e_c = |N(a)|^{-1/2} \sum_{c' \in A_1(a)} e^{2\pi i T(acc')} e_{c'},$$

where $e_c \in L^2(A_1(a))$. The context should make clear where e_c lies. As in Section II, it is easy to see that

$$L^2(A(\alpha)) \cong L^2(A_1(a)) \otimes L^2(A(\delta)).$$

The identification given by $e_{c+c'} \cong e_c \otimes e_{c'}$.

The arguments used in the beginning of this section, for example, those leading up to Lemma 3.1, may be carried over to show that the formula

$$\zeta_a^{\#}(\mathbf{x})\, f(c) = f(xc)\mathbf{x} = x + a\mathcal{O} \in (\mathcal{O}/a\mathcal{O})^{\times}, \qquad c \in A_1(a),\ f \in L^2(A_1(a)),$$

defines a unitary representation of $(\mathcal{O}/a\mathcal{O})^{\times}$ on $L^2(A_1(a))$.

LEMMA 3.12. $F(\alpha)\,\zeta_\alpha^{\#}(b) = F_1(a)\,\zeta_a^{\#}(b) \otimes F(\delta)\,\zeta_\delta^{\#}(ab)$.

Proof. Let $c \in A(\alpha)$ be written $c = c_1 + c_2$, where $c_1 \in A_1(a)$ and $c_2 \in A(\delta)$. Then $e_c = e_{c_1} \otimes e_{c_2}$. Applying $F(\alpha)\,\zeta_\alpha^{\#}(b)$ to e_c gives

$$m(\alpha)^{-1/2} \sum_{c' \in A(\alpha)} e^{2\pi i T(\alpha b c c')} e_{c'}.$$

Applying $F_1(a)\,\zeta_a^{\#}(b) \otimes F(\delta)\,\zeta_\delta^{\#}(ab)$ to $e_{c_1} \otimes e_{c_2}$ gives

$$|N(a)|^{-1/2} \sum_{c_1' \in A_1(a)} e^{2\pi i T(\alpha b c_1 c_1')} e_{c_1'} \otimes |m(\delta)|^{-1/2} \sum_{c_2' \in A(\delta)} e^{2\pi i T(\delta a b c_2 c_2')} e_{c_2'}$$

$$= m(\alpha)^{-1/2} \sum_{c_1', c_2'} e^{2\pi i T(\alpha b (c_1 c_1' + c_2 c_2'))} e_{c_1'} \otimes e_{c_2'}.$$

Observe, $T(\alpha b(c_1 + c_2)(c_1' + c_2')) = T(\alpha b(c_1 c_1' + c_2 c_2'))$ since $T(\alpha b(c_1 c_2' + c_1' c_2)) \in Z$. The lemma follows. Let

$$C_1(\alpha; b) = |N(a)|^{-1/2} \operatorname{tr}(F_1(a)\,\zeta_a(b)) = |N(a)|^{-1/2} \sum_{c \in A_1(a)} e^{2\pi i T(\alpha b c^2)}.$$

COROLLARY 3.12.1. $G(\alpha; b) = C_1(\alpha; b)\, G(\delta; ab)$.

The unitary operators $F_1(a)$ can be handled exactly as the unitary operators $F(\alpha)$ were handled in Lemma 3.2 and its corollaries. We will state the results in the next lemma and its corollaries, without proof.

LEMMA 3.13. *Let $x \in (\mathcal{O}/a\mathcal{O})^{\times}$. Then*

$$F_1(a)\,\zeta_a(x) = \zeta_a(x)^{-1}\, F_1(a).$$

COROLLARY 3.13.1. *If x is a perfect square in $(\mathcal{O}/a\mathcal{O})^{\times}$ then*

$$C_1(\alpha; xy) = C_1(\alpha; y), \qquad y \in (\mathcal{O}/a\mathcal{O})^{\times}.$$

Also, the tensor product yields for the "Fourier transforms" $F_1(a)$, results analogous to those of Lemmas 3.3, 3.4 and 3.5. Again, we will state the results without proof.

LEMMA 3.14. $F_1(ab) = F_1(a)\,\zeta_a(b) \otimes F_1(b)\,\zeta_b(a)$.

COROLLARY 3.14.1. $C_1(ab) = C_1(a; b)\,C_1(b; a)$.

We will now use these results to investigate the Fourier transform $F(\alpha)$.

LEMMA 3.15. $F(\alpha)\,\zeta_\alpha^*(b) \otimes F(\beta)\,\zeta_\beta^*(a) = F(\alpha\beta/\delta) \otimes F(\delta)\,\zeta_\delta^*(ab)$.

Proof. Follows immediately from Lemmas 3.12 and 3.14.

COROLLARY 3.15.1. $G(\beta; a)\,G(\alpha; b) = G(\alpha\beta/\delta) \cdot G(\delta; ab)$.

In [5], Hecke introduced the following trigonometric sums. Let $\xi \in k$. Then, there exist integral ideals R and S such that $R + S = \mathcal{O}$ and

$$S^{-1}R\mathcal{O}' = \xi\mathcal{O}.$$

We will assign to ξ the trigonometric sum $C(\xi)$ defined by the formula

$$C(\xi) = \sum_{c \in \mathcal{O}/S} e^{2\pi i T(\xi c^2)}.$$

Also, if $\mathbf{x} \in (\mathcal{O}/S)^\times$, the trigonometric sum $C(\mathbf{x}\xi)$ is given by

$$C(\mathbf{x}\xi) = \sum_{c \in \mathcal{O}/S} e^{2\pi i T(\mathbf{x}\xi c^2)}.$$

We will now see how the trigonometric sums that we have been concerned with are related to these Hecke sums.

LEMMA 3.16. $C_1(a; b) = |N(a)|^{-1/2}\,C(\mathbf{b}(\delta/a))$.

Proof. Observe $(1/a)K\mathcal{O}' = (\delta/a)\mathcal{O}$.

LEMMA 3.17. $G(\delta; \mathbf{x}) = m(\delta)^{-1/2}\,C(\mathbf{x}(w^2/\delta))$, $\mathbf{x} \in (\mathcal{O}/K)^\times$.

Proof. Recall $\mathcal{O}' = w\mathcal{O} + \zeta\mathcal{O}$, $\zeta \in K$, and that the mapping, $\gamma \to w\gamma$, induces an isomorphism of $\mathcal{O}/K$ onto $A(\delta)$. Thus,

$$G(\delta; \mathbf{x}) = m(\delta)^{-1/2} \sum_{c \in \mathcal{O}/K} e^{2\pi i T((w^2/\delta)xc^2)}.$$

Consider $(w^2/\delta^2)K^2$. Observe $(w^2/\delta^2)K^2 \subset (K\mathcal{O}'/\delta)^2 = \mathcal{O}$. Thus, it is an integral ideal. Suppose we knew $K + (w^2/\delta^2)K^2 = \mathcal{O}$. Then, since, $(w^2/\delta^2)K^2K^{-1}\mathcal{O}' = (w^2/\delta)\mathcal{O}$, the lemma would follow. It remains to show $K + (w^2/\delta^2)K^2 = \mathcal{O}$. Since $\mathcal{O}' = w\mathcal{O} + \zeta\mathcal{O}$, $(1/\delta)K\mathcal{O}' = \mathcal{O} = (w/\delta)K +$

$(\zeta/\delta)K$. We must show $K + (w^2/\delta^2)K^2 \supset (w/\delta)K + (\zeta/\delta)K$. Since $\zeta/\delta \in K/\delta \subset \mathcal{O}$, $(\zeta/\delta)K \subset K$, and so we are done once we show $(w/\delta)K \subset K + (w^2/\delta^2)K$. From $\delta\mathcal{O} = K\mathcal{O}' = wK + \zeta K$, we can write $\delta = wk + \zeta k'$, k, $k' \in K$. It follows that $w/\delta = (w^2/\delta^2)k + (\zeta/\delta)(w/\delta)$, $k' \in (w^2/\delta^2)K' + \mathcal{O}$ and $(w/\delta)K \subset (w^2/\delta^2)K^2 + K$. The lemma is now proved.

We will now relate these trigonometric sums to the Legendre symbol. Let B be an odd ideal and write $B = \prod_{j=1}^{l} P_j$, its factorization into prime ideals P_j. For each $x \in \mathcal{O}$, relatively prime to B, we put

$$\left(\frac{x}{B}\right) = \prod_{j=1}^{l} \left(\frac{x}{P_j}\right).$$

From the previous discussion on the Legendre symbol (x/P_j), it follows that the mapping $x \to (x/B)$ induces a character of $(\mathcal{O}/B)^x$.

For convenience, we shall borrom the following result from Hecke [5, p. 223].

LEMMA 3.18. *Let R and S be relatively prime ideals, with S odd. Suppose $S^{-1}R\mathcal{O}' = \xi\mathcal{O}$. Then, for $\mathbf{x} \in (\mathcal{O}/S)^x$,*

$$C(\mathbf{x}\xi) = (x/S)\, C(\xi).$$

There is no loss in generality in assuming that K is odd.

COROLLARY 3.18.1. *Suppose a is odd. Then*

$$G(\alpha; b) = (b/aK)\, G(\alpha).$$

Proof. By Corollary 3.12.1, $G(\alpha; b) = C_1(\alpha; b)\, G(\delta; ab)$. Lemmas 3.16 and 3.17 imply $G(\alpha; b) = m(\alpha)^{-1/2} C(\mathbf{b}(\delta/a))\, G(\mathbf{ab}(w^2/\delta))$. By Lemma 3.18, $G(\alpha; b) = m(\alpha)^{-1/2}(b/a)(b/K)\, G(\alpha)$.

We will now consider the quadratic reciprocity law for $\mathcal{k}$. Let a and b be odd elements in $\mathcal{O}$. Then,

$$\left(\frac{a}{b}\right)\left(\frac{b}{a}\right) = \frac{G(\alpha; b)\, G(\beta; a)}{G(\alpha)\, G(\beta)} \left(\frac{ab}{K}\right)$$

by Corollary 3.18.1. Applying Lemma 3.15, especially its corollary, we have

$$\left(\frac{a}{b}\right)\left(\frac{b}{a}\right) = \frac{G(\alpha\beta/\delta)\, G(\delta; \mathbf{ab})}{G(\alpha)\, G(\beta)} \left(\frac{ab}{K}\right)$$

$$= \frac{G(\alpha\beta/\delta)\, G(\delta)}{G(\alpha)\, G(\beta)}.$$

Now, since a is odd, it is relatively prime to 4, and hence we can again apply Corollary 3.15.1 to assert

$$G(\alpha) = \frac{G(4\alpha)\, G(\delta; \mathbf{a})}{G(4\delta; \mathbf{a})}$$

with similar expressions for $G(\beta)$ and $G(\alpha\beta/\delta)$. Hence

$$\left(\frac{a}{b}\right)\left(\frac{b}{a}\right) = \frac{G(4(\alpha\beta/\delta))}{G(4\alpha)\, G(4\beta)} \frac{G(4\delta; \mathbf{a})\, G(4\delta; \mathbf{b})}{G(4\delta; \mathbf{ab})},$$

since $G(\delta)\, G(\delta; \mathbf{ab}) = G(\delta; \mathbf{a})\, G(\delta; \mathbf{b})$. We may now argue exactly as in Theorem 3.1 to prove the following theorem.

THEOREM 3.2. *Let a, b be odd relatively prime elements in $\mathcal{O}$. Then,*

$$\left(\frac{a}{b}\right)\left(\frac{b}{a}\right) = (-1)^{\sum_{j=1}^{\delta}((\operatorname{sgn}_j(a)-1)/2)((\operatorname{sgn}_j(b)-1)/2)} \frac{G(4\delta; \mathbf{a})\, G(4\delta; \mathbf{b})}{G(4\delta; \mathbf{ab})}.$$

Moreover, if a is a perfect square mod 4, *then*

$$\left(\frac{a}{b}\right)\left(\frac{b}{a}\right) = (-1)^{\sum_{j=1}^{\delta}((\operatorname{sgn}_j(a)-1)/2)((\operatorname{sgn}_j(b)-1)/2)}.$$

This is the generalized quadratic reciprocity law of Hecke.

IV. MILGRAM'S FORMULA AND INDUCED REPRESENTATIONS

Milgram's formula is the ultimate result needed in the quadratic reciprocity law of Hecke. However, the methods of Section III involve, primarily, results on the Fourier transform of several finite abelian groups. It is natural to speculate about the relationship between the Milgram formula and the theory of these Fourier transforms. In this section we will give a group theoretic setting for the conjoining of these ideas. Indeed, the notion of induced representation will provide the key. In order to make this work self-contained, we will begin by presenting a brief review of this theory as applied to finite dimensional representations of finite groups.

Let G be a subgroup of a finite group N. Let π_1 be a representation of G on the finite dimensional space V. We want to define a representation π of N, whose restrictions to G, will reflect the representation π_1. We will define π below and call it the representation of N induced from π_1.

Let $\mathcal{F}(N, V)$ be the space of functions $f\colon N \to V$. N acts on $\mathcal{F}(N, V)$ by

right and left translations. Denote by W, the space of all $f \in \mathcal{F}(N, V)$ satisfying

$$\pi_1(g)(f(n)) = f(g \cdot n), \qquad g \in G,\ n \in N.$$

Since right translations commute with left translations, W is invariant under right translations from N. Thus, we can define the representation π of N on W by

$$(\pi(n)f)(m) = f(m \cdot n), \qquad m, n \in N,\ f \in W.$$

$\mathcal{F}(N, V)$ may be viewed as the direct sum of $o(N)$ copies of V. We shall now see that W is the direct sum of $o(N/G)$ copies of V. Let $n_0, n_1, \ldots, n_{r-1}$ be a complete system of representations for the space of cosets N/G. Then, N is the disjoint union of Gn_0, $Gn_1, \ldots, Gn_{r-1}$. We will take $n_0 = 1$. A function $f \in W$ is uniquely determined by its values $f(n_0), f(n_1), \ldots, f(n_{r-1})$ since for every $n \in N$, there is a unique $g \in G$ such that $n = gn_i$, $0 \leqslant i < r$, and

$$f(n) = f(gn_i) = \pi_1(g)(f(n_i)).$$

Conversely, given a function f: $\{n_0, \ldots, n_{r-1}\} \to V$ we can extend f to a function of N into V by this formula: this extension being on W. Thus, under this identification

$$W = \mathcal{F}(\{n_0, n_1, \ldots, n_{r-1}\}, V) = \oplus \sum_{0 \leqslant i < r} W(i),$$

where

$$W(i) = \mathcal{F}(\{n_i\}, V) \sim V.$$

We will now study π_G, the representation π restricted to G. Also, we denote by $\pi_G \mid U$, the restriction of the space of the representation π_G to the π_G-invariant subspace U of W. We will assume, once and for all, G is a normal subgroup of N. Thus, if $n \in N$, the mapping, $g \to ngn^{-1}$, is an automorphism of G, which we denote by $\mathrm{ad}_G(n)$.

LEMMA 4.1. $\pi_G \mid W(i) = \pi_1 \circ \mathrm{ad}_G(n_i)$, $0 \leqslant i < r$.

Proof. For $g \in G$ and $f \in W$,

$$(\pi(g)f)(n_i) = f(n_i g) = f(n_i g n_i^{-1} n_i) = \pi_1(n_i g n_i^{-1}) f(n_i).$$

In particular, each subspace $W(i)$ is π_G-invariant and $\pi_G \mid W(i) = \pi_1(n_i g n_i^{-1})$.

COROLLARY 4.1.1. $\pi_G \mid W(0) = \pi_1$.

We will also need to determine $\pi(n_i)$, $1 \leqslant i < r$. Write $n_j n_i = g_{j,i} n_{j,i}$, where $g_{j,i} \in G$ and $n_{j,i} \in \{n_0, n_1, ..., n_{r-1}\}$. Then, if $f \in W$, $(\pi(n_i)f)(n_j) = f(n_j n_i) = f(g_{j,i} n_{j,i}) = \pi_1(g_{j,i}) f(n_{j,i})$. Thus, $\pi(n_i)$ permutes the factors $W(j)$ and then acts by some $\pi_1(g)$.

Let A be a finite abelian group of order m. Denote its dual by A^* and let $\langle , \rangle = \langle , \rangle_A : A \times A^* \to U_m$ be the bilinear pairing of A with A^*. Consider the subgroup of U_m, $C = C_A = \{\langle a, a^* \rangle : a \in A,\ a^* \in A^*\}$ and the set $N(A) = A \times A^* \times C$. We make $N(A)$ into a group by the following composition law:

$$(a_1, a_1^*, c_1)(a_2, a_2^*, c_2) = (a_1 + a_2, a_1^* + a_2^*, c_1 c_2 \langle a_1, a_2^* \rangle),$$

where $a_1, a_2 \in A$, $a_1^*, a_2^* \in A^*$, and $c_1, c_2 \in C$. In fact, $N(A)$ is easily seen to be a two-step nilpotent group with center $Z = Z_A$ given by

$$Z = [N(A), N(A)] = (0) \times (0) \times C$$

and

$$N(A)/Z \simeq A \oplus A^*.$$

We will show that the Fourier transform $\mathscr{F} = \mathscr{F}_A$ manifests itself in the representation theory of $N(A)$; namely, as an intertwining operator between two irreducible representations of $N(A)$.

Let $\zeta = \zeta_A$ be the representation of $N(A)$ on $L^2(A)$ defined by

$$(\zeta(a_1, a_1^*, c_1)f)(a) = c_1 \langle a, a_1^* \rangle f(a + a_1),$$

where $a, a_1 \in A$, $a_1^* \in A^*$, $c_1 \in C$. Observe, that ζ may be viewed as an induced representation as follows. Let $M = (0) \times A^* \times C$ and let $x_0 : M \to U_m$ be the character defined by $x_0(0, a^*, c) = c$. Clearly, M is a maximal abelian subgroup of $N(A)$. Inducing x_0 to $N(A)$ gives ζ.

We will now describe $\zeta(N(A))$ and see how $\mathscr{F}$ enters into the theory. For this purpose, we will make the following definitions. Let r denote the regular representation of A on $L^2(A)$, namely,

$$(r(a)f)(a_1) = f(a_1 + a), \qquad a, a_1 \in A, f \in L^2(A).$$

Denote by r, again, the regular representation of A^* on $L^2(A^*)$. Consider $\chi_a \in L^2(A^*)$ defined by $\chi_a(a^*) = \langle a, a^* \rangle$, $a \in A$, $a^* \in A^*$. It is easy to see that

$$r(a^*)\chi_a = \langle a, a^* \rangle \chi_a, \qquad a \in A,\ a^* \in A.$$

We have previously considered the set $\{1/\sqrt{m}\,\chi_a : a \in A\}$, $m = o(A)$, and showed that it was an orthonormal basis of $L^2(A^*)$.

Let s denote the representation of A^* on $L^2(A)$ defined by

$$(s(a^*)f)(a) = \langle a, a^* \rangle f(a), \qquad a \in A, a^* \in A^*, f \in L^2(A).$$

Consider $e_a \in L^2(A)$ defined by

$$\begin{aligned} e_a(a_1) &= 1, \qquad a_1 \neq a, \\ &= 0, \qquad a_1 \neq a, \end{aligned} \qquad a, a_1 \in A.$$

The set $\{e_a : a \in A\}$ is an orthonormal basis of $L^2(A)$. Clearly,

$$s(a^*)e_a = \langle a, a^* \rangle e_a, \qquad a \in A, a^* \in A^*.$$

In Section I, we showed

$$\mathcal{F}(e_a) = \frac{1}{\sqrt{m}} \chi_a, \qquad a \in A.$$

LEMMA 4.2. $s(a^*) = \mathcal{F}^{-1} r(a^*) \mathcal{F}$, $a^* \in A^*$,

$$s(-a^*) = \mathcal{F}^{-1} s(a^*) \mathcal{F}, \qquad a^* \in A^*.$$

Proof. For $a \in A$ and $a^* \in A^*$,

$$(r(a^*)\mathcal{F})(e_a) = \frac{1}{\sqrt{m}} r(a^*)\chi_a = \frac{1}{\sqrt{m}} \langle a, a^* \rangle \chi_a = (\mathcal{F} s(a^*))(e_a).$$

Thus, the first assertion follows. The second is proved in exactly the same way.

LEMMA 4.3. *For $a \in A$, $a^* \in A^*$ and $c \in C$,*

$$\zeta(a, a^*, c) = cs(a^*)\, r(a),$$
$$\zeta(b, b^*, \langle a, a^* \rangle) = r(a)\, s(a^*).$$

Proof. For $f \in L^2(A)$,

$$c(s(a^*)\, r(a) f)(a_1) = c\langle a_1, a^* \rangle (r(a)f)(a_1) = c\langle a_1, a^* \rangle f(a_1 + a)$$

which is $(\zeta(a, a^*, c)f)(a_1)$ by definition. This proves the first assertion. The second follows in a similar way.

COROLLARY 4.3.1. *$\zeta(N(A))$ is the group of unitary operators of $L^2(N(A))$ generated by $r(A)$ and $s(A^*) = \mathcal{F}^{-1} f(A^*) \mathcal{F}$.*

In the presence of a fixed symmetric isomorphism $D = D_A : A \to A^*$, we will identify A and A^* as in the preceding discussion. The notation remains the same, except for replacing $\mathscr{F}$ by the unitary operator, $F = F_A$, given by $F(f) = \mathscr{F}(f) \cdot D, f \in L^2(A)$. We will assume, as will occur in practice, that D has been specified and the identifications made in the next discussion.

Consider the mapping, $J = J_A$, of $N(A)$ given by

$$J(a, b, c) = (-b, a, c\langle a, b\rangle^{-1}), \qquad a, b \in A_1,\ c \in C.$$

A direct verification shows J is an automorphism of $N(A)$ acting by the identity on the center Z. The general representation theory of two-step nilpotent groups implies ζ and $\zeta \cdot J$ are unitarily equivalent. Indeed, we have the next important result.

LEMMA 4.4. *$F^{-1}\zeta F = \zeta \cdot J$. Thus, F is an intertwining operator between ζ and $\zeta \cdot J$.*

Proof. Since $s(a) = F^{-1}r(a)F$ and $r(-a) = F^{-1}s(a)F$, we have

$$F^{-1}\zeta(a, b, c)F = cF^{-1}s(b)\, r(a)F = cr(-b)\, s(a).$$

By Lemma 4.3,

$$\zeta \cdot J(a, b, c) = \zeta(-b, a, c\langle a, b\rangle^{-1}) = cr(-b)\, s(a)$$

and the lemma follows.

We want to study F; in particular, in this section, its trace. The crucial observation is the following. Suppose π is another representation of $N(A)$, unitarily equivalent to ζ. Let

$$L^{-1}\pi L = \zeta.$$

Then, $L^{-1}\pi \cdot JL = \zeta \cdot J$ and

$$F^{-1}L^{-1}\pi LF = F^{-1}\zeta F = \zeta \cdot J = L^{-1}\pi \cdot JL.$$

Hence, $\mathscr{T} = LFL^{-1}$ is an intertwining operator between π and $\pi \cdot J$ since

$$\mathscr{T}^{-1}\pi\mathscr{T} = \pi \cdot J.$$

It follows that F is the conjugate of some intertwining operator $\mathscr{T}$ between π and $\pi \cdot J$, whenever π is unitarily equivalent to ζ. The importance of this comment is that if π is suitably chosen, the structure of $\mathscr{T}$ will be simpler than the structure of F. The essential property of π, that will accomplish this,

will be the specification of π as an induced representation form a representation of a subgroup C of $N(A)$ satisfying

$$J(C) = C.$$

Notice, ζ was induced from the subgroup M, but $J(M) \neq M$.

Let $\alpha \in \hat{k}$. A full module M in k satisfying $\alpha \in (M^2)'$ will be called an α-integral module. Let M be an α-integral module. Set $A = A(M, \alpha)$, $N = N(A)$, $\zeta = \zeta_A$, $F = F_A$ and $J = J_A$. Then, $F^{-1}\zeta F = \zeta \cdot J$ and F is an intertwining operator between ζ and $\zeta \cdot J$. In this action, we want to study $G = \mathrm{tr}(F) = G(M, \alpha)$.

Suppose M_1 is an α-integral module containing M. Then,

$$M \subset M_1 \subset (\alpha M_1)' \subset (\alpha M)'.$$

Let $A_1 = A(M_1, \alpha)$, $N_1 = N(A_1)$, $\zeta_1 = \zeta_{A_1}$, $F_1 = F_{A_1}$ and $J_1 = J_{A_1}$. Then, $F_1^{-1}\zeta_1 F_1 = \zeta_1 \cdot J$ and we may consider $G_1 = \mathrm{tr}(F_1) = G(M_1, \alpha)$. We will compare G and G_1 by using ζ_1 to induce a representation π of A which is unitarily equivalent to ζ.

Let $Z = (0) \times (0) \times C$ and $Z_1 = (0) \times (0) \times C_1$ be the centers of N and N_1, respectively. Then, $C_1 \subset C$. Let N_1 be the group defined as the set $A_1 \times A_1 \times C$ where the composition law is given by $(a, b, c)(a', b', c') = (a + a', b + b', c \cdot c' \langle a, b' \rangle)$, where $a, b \in A_1$ and $c, c' \in C$. Then, $N(A_1) \subset N(A_1)^{\#}$ as a subgroup and $N(A_1)^{\#}/N(A_1) \cong C/C_1$. Extend ζ_1 to a representation $\zeta_1^{\#}$ of $N_1^{\#}$ be requiring $\zeta_1^{\#}(0, 0, c) = c$, $c \in C$.

Let K and C be the subsets of N defined by

$$K = M_1/M \times M_1/M \times (1),$$
$$C = (\alpha M_1)'/M \times (\alpha M_1)'/M \times C.$$

LEMMA 4.5. *K is an abelian subgroup of N and C is its centralizer on N. Moreover, $J(K) = K$ and $J(C) = C$.*

Proof. Let $a, b' \in M_1$. Then $T(\alpha ab') \subset Z$ by definition. Thus, if $(a, b, 1)$ and $(a', b', 1)$ are in K, then

$$(a, b, 1)(a', b', 1) = (a + a', b + b', \langle a, b' \rangle) \in K$$

since $\langle a, b' \rangle = e^{2\pi i T(\alpha ab')} = 1$.

Now, let $(a', b', c') \in N$ be in the centralizer of K. Then, for all $(a, b, 1) \in K$,

$$(a, b, 1)(a', b', c') = (a', b', c')(a, b, 1)$$

which implies $\langle a, b' \rangle = \langle a', b \rangle$ for all $a, b \in M_1$. Thus, $e^{2\pi i T(\alpha(ab'-a'b))} = 1$, for all $a, b \in M_1$ and it follows that $b' \in (\alpha M_1)'$ and $a' \in (\alpha M_1)'$. Conversely, the same argument shows that C is contained in the centralizer of K and hence must be the centralizer of K.

The final assertion is obvious and the lemma is proved.

Consider the natural mapping $(\alpha M_1)'/M \to (\alpha M_1)'/M_1$. Denote, again, by p the mapping

$$p\colon C \to N(A_1)^{\#}$$

given by $p(a, b, c) = (p(a), p(b), c)$, $a, b \in (\alpha M_1)^{\#}$, $c \in C$.

The next result is obvious.

LEMMA 4.6. *The mapping $p\colon C \to N(A_1)^{\#}$ is a homomorphism satisfying the short exact sequence*

$$1 \to K \to C \xrightarrow{p} N(A_1)^{\#} \to 1.$$

Consider the representation of C on $L^2(A_1)$ given by

$$\pi_1 = \zeta_1^{\#} \cdot p.$$

Clearly, since $J(C) = C$, $\pi_1 \cdot J$ is also a representation of C. Since, $F_1^{-1}\zeta_1 F_1 = \zeta_1 \cdot J$, it follows that $F_1^{-1}\pi_1 F = \pi_1 \cdot J$, and F_1 is an intertwining operator between π_1 and $\pi_1 \cdot J$.

Let π be the representation of N defined by inducing π_1 to N. We will study π. By the general induced representation theory the representation space W of π is given as follows. Observe that $N(A)/C \cong (\alpha M_1)'/(\alpha M)' \oplus (\alpha N_1)'/(\alpha M)'$. Let $n_0 = 0, n_1, \ldots, n_{r-1}$ be a complete system of representations for $(\alpha M_1)'/(\alpha M)'$. Then, we can write

$$W = \bigoplus_{1 \leq i, j < r} W(i, j),$$

where $W(i, j) = \mathscr{F}(\{n_i, n_j, 1\}, L^2(A_1)) \cong L^2(A_1)$. Let π_C be the restiction of π to C. Then,

$$\pi_C \mid W(i, j) = \pi_1 \cdot \mathrm{ad}_C(n_i, n_j, 1).$$

LEMMA 4.7. *Using the notation above, for $(a, b, c) \in C$,*

$$\pi_C(a, b, c) \mid W(i, j) = \langle n_i, b \rangle \langle a, n_j \rangle^{-1} \pi_1(a, b, c).$$

Proof. Let $(a, b, c) \in C$. Then,

$$\mathrm{ad}_C(n, n_j, 1)(a, b, c) = (a, b, c \cdot \langle n_i, b\rangle\langle a, n_j\rangle^{-1}).$$

It follows that for $f \in W(i, j) \cong L^2(A_1)$ and $a' \in A_1$,

$$\begin{aligned}(\pi_C(a, b, c)f)(a') &= \pi_1(a, b, c\langle n_i, b\rangle\langle a, n_j\rangle^{-1})(f(a')) \\ &= \zeta_1(a, b, c\langle n_i, b\rangle\langle a, n_j\rangle^{-1})(f(a')) \\ &= c\langle n_i, b\rangle\langle a, n_j\rangle^{-1}\langle a', b\rangle f(a' + a) \\ &= \langle n_i, b\rangle\langle a, n_j\rangle^{-1}\pi_1(a, b, c)(f(a')).\end{aligned}$$

COROLLARY 4.7.1. *$\pi_C \mid W(i, j)$ is irreducible.*

COROLLARY 4.7.2. $\pi_C \mid W(0, 0) = \pi_1$.

COROLLARY 4.7.3. $\pi_k(a, b, 1) \mid W(i, j) = \langle n_i, b\rangle\langle a, n_j\rangle^{-1}$, $(a, b, 1) \in K$.

The last corollary implies that each of the spaces $W(i, j)$ is a character space for $\pi(K)$ with character

$$(a, b, 1) \to \langle n_i, b\rangle\langle a, n_j\rangle^{-1} = e^{2\pi i T(\alpha(n_i b - n_j a))}.$$

Since, $(M_1/M \oplus M_1/M)^* = (\alpha M_1)'/(\alpha M)' \oplus (\alpha M_1)^*/(\alpha M)'$, it follows that each $W(i, j)$ corresponds to a distinct character space and all characters are realized. From, the general theory of induced representations, we get the following results.

COROLLARY 4.7.4. *$\pi_C \mid W(i, j) \sim \pi_C \mid W(k, l)$ if and only if $i = k$ and $j = l$.*

COROLLARY 4.7.5. *π is irreducible.*

COROLLARY 4..6. *π is unitarily equivalent to ζ.*

Clearly, π and $\pi \cdot J$ are unitarily equivalent. Let $\mathscr{J}$ be an intertwining operator between π and $\pi \cdot J$ with $\mathscr{J}^{-1}\pi\mathscr{J} = \pi \cdot J$. $\mathscr{J}$ is determined only up to constant multiple λ where $|\lambda| = 1$. We will eventually want to choose a particular $\mathscr{J}$.

LEMMA 4.8. $\mathscr{J}(W(i, j)) = W(j, -i)$.

Proof. Let $f \in W(i, j)$ and $(a, b, 1) \in K$. Then,

$$(\pi \cdot J)(a, b, 1)f = \pi(-b, a, 1)f = \langle n_i, a\rangle\langle n_j, b\rangle f.$$

Since $\mathscr{J}^{-1}\pi\mathscr{J} = \pi \cdot J$, we have

$$((\mathscr{J}^{-1}\pi\mathscr{J})(a, b, 1))f = \langle n_i, a\rangle\langle n_j, b\rangle f.$$

By multiplying on the left by $\mathscr{J}$, we have

$$(\pi(a, b, 1))\,\mathscr{J}(f) = \langle n_i, a\rangle\langle n_j, b\rangle\,\mathscr{J}(f),$$

which by Corollary 4.7.3 implies $\mathscr{J}(f) \in W(j, -i)$.

COROLLARY 4.8.1. $\mathscr{J}(W(0, 0)) = W(0, 0)$.

Let $\mathscr{J}(i, j) = \mathscr{J} \mid W(i, j)$: $W(i, j) \to W(j, -i)$. Now, since $\mathscr{J}^{-1} \cdot \pi \cdot \mathscr{J} = \pi \cdot J$ and $J(C) = C$, we have

$$\mathscr{J}^{-1} \cdot \pi_C \cdot \mathscr{J} = \pi_C \cdot J.$$

By Corollary 4.7.2, $\pi_C \mid W(0, 0) = \pi_1$ and it follows that if $\mathscr{J} \mid W(0, 0) = \mathscr{J}(0, 0)$,

$$\mathscr{J}(0, 0)^{-1} \cdot \pi_1 \cdot \mathscr{J}(0, 0) = \pi_1 \cdot J_1.$$

Thus, $\mathscr{J}(0, 0)$ is an intertwining operator between π_1 and $\pi_1 \cdot J_1$. But, F_1 is also, so $F_1 = \lambda\mathscr{J}(0, 0)$ for some $|\lambda| = 1$. Replace $\mathscr{J}$ by $\lambda\mathscr{J}$ as our specified intertwining operator above. Thus, we will assume $\mathscr{J}$ has been chosen so that

$$F_1 = \mathscr{J}(0, 0).$$

Clearly, $\mathscr{J}$ is uniquely determined by this condition. For the remainder of this section $\mathscr{J}$ will be fixed.

Consider $V(0, 0) = L^{-1}\pi L = \rho$. Thus, L is an intertwining operator for π and ρ. As we have seen LFL^{-1} is a intertwining operator for π and $\pi \cdot J$. Hence, $LFL^{-1} = \lambda\mathscr{J}$, $|\lambda| = 1$. We will now show $\lambda = 1$.

Consider $V(0, 0) = L^{-1}(W(0, 0))$. $V(0, 0)$ is a character one space for ρ_K. Hence, if $f \in V(0, 0)$ and $(a, b, 1) \in K$ we have $\rho(a, b, 1)f(a') = \langle a', b\rangle f(a' + a) = f(a')$, wherever $a' \in A$. This implies $f(a' + a) = f(a')$ and $\langle a', b\rangle f(a') = f(a')$ for all $a, b \in M_1/M$ and $a' \in A$. It follows that we may view f as a function on $(aM)'/M_1$ by the first condition and that f vanishes off of $(aM_1)'$ by the second condition. Thus, $f \in L^2(A_1)$. In this way, we may identify $V(0, 0)$ with $L^2(A_1)$ and we shall do so in the following discussion. Clearly, $\rho_C \mid V(0, 0) = \pi_C \mid W(0, 0)$ which implies $L^{-1} \mid W(0, 0)$ is a scalar multiple of the identiy. Now, $F \mid V(0, 0) = F_1$; thus from $\mathscr{J} = F_1$ on $W(0, 0)$ it follows that $L \cdot F \cdot L^{-1} = \mathscr{J}$ on $W(0, 0)$. Clearly, $\lambda = 1$. We organize this discussion in a lemma.

LEMMA 4.9. *Let $\mathcal{I}$ be the intertwining operator between π and $\pi \cdot J$, uniquely determined by the condition $\mathcal{I} \mid W(0,0) = F_1$. Let L be an intertwining operator between π and ρ with $L^{-1}\pi L = \rho$. Then, $F = L^{-1}\mathcal{I}L$.*

We will now consider the implications of this lemma for computing $G = \mathrm{tr}(F)$. Clearly, we need only compute $\mathrm{tr}(\mathcal{I})$. By Lemma 4.8, and our normalizing assumption on $\mathcal{I}$, we have

$$\mathrm{tr}(\mathcal{I}) = \mathrm{tr}(F_1) + \sum_{0 \neq 2n_i \in (\alpha M_1)'} \mathrm{tr}(\mathcal{I}(i,i)).$$

LEMMA 4.10. *Let $o(M_1/M)$ be odd. Then*

$$G = \mathrm{tr}(\mathcal{I}) = G_1.$$

Proof. Since $o((\alpha M)'/(\alpha M_1)') = o(M_1/M)$ we have that no element in $(\alpha M)'/(\alpha M_1)'$ has order 2. Thus, the right-hand sum is vacuous.

We shall consider the general case. Let $\mathcal{I}(i) = \mathcal{I}(i,i)$, $2n_i \in (\alpha M_1)'$. Since $\pi_C \mid W(i,i)$ and $\pi_C \cdot J \mid W(i,i)$ are irreducible and $\mathcal{I}(i)$ intertwines them, any intertwining operator between them will be a constant multiple of $\mathcal{I}(i)$. We shall construct a convenient one.

LEMMA 4.11. *$F_1 \cdot s(2n_i)$ is an intertwining operator between $\pi_C \mid W(i,i)$ and $\pi_C \cdot J \mid W(i,i)$.*

Proof. We will restrict our attention our attention solely to $W(i,i)$. Now,

$$\pi_C(a,b,c) = \langle n_i, b\rangle\langle a, n_i\rangle^{-1}\pi_1(a,b,c), \qquad (a,b,c) \in C.$$

$$\pi_C \cdot J(a,b,c) = \langle b, n_i\rangle\langle n_i, a\rangle\pi_1 \cdot J(a,b,c), \qquad (a,b,c) \in C.$$

From $F_1^{-1} \cdot \pi_1 \cdot F_1 = \pi_1 \cdot J$, it follows that

$$\pi_C \cdot J_1(a,b,c) = \langle b, n_i\rangle\langle a, n_i\rangle F_1^{-1} \cdot \pi_1(a,b,c) \cdot F_1 = \langle 2n_i, a\rangle F_1^{-1} \cdot \pi_C(a,b,c) \cdot F_1.$$

We defined $s(b_1)f(a_1) = \langle a_1, b_1\rangle f(a_1)$, $a_1, b_1 \in A_1$, from which it follows that we can write

$$s(2n_i)^{-1} \cdot \pi_C(a,b,c)\, s(2n_i) = \langle 2n_i, a\rangle\, \pi_C(a,b,c).$$

Placing this result in the preceding, gives

$$s(2n_i) \cdot F_1 \cdot \pi_C \cdot J(a,b,c) \cdot F_1^{-1} \cdot s(2n_i)^{-1} = \pi_C(a,b,c)$$

which proves the lemma.

COROLLARY 4.11.1. $\mathcal{J}(i) = \lambda s(2n_i) \cdot F_1$ *for some* $|\lambda| = 1$.

We will now compute $\operatorname{tr}(s(2n_i) \cdot F_1)$. Take $a, b \in A_1$. Then, $m_1 = o(A_1)$,

$$(s(2n_i) \cdot F)(e_a)(b) = \frac{1}{\sqrt{m_1}} \langle 2n_i, b\rangle \sum_C \langle a, c\rangle e_c(b)$$

$$= \frac{1}{\sqrt{m_1}} \langle 2n_i, b\rangle\langle a, b\rangle = 1/\sqrt{m}\langle 2n_i + a, b\rangle$$

$$= \frac{1}{\sqrt{m_1}} \sum_{c \in A_1} \langle 2n_i + a, c\rangle e_c(b)$$

from which we may deduce

$$\operatorname{tr}(s(2n_i) \cdot F) = \frac{1}{\sqrt{m_1}} \sum_{a \in A_1} \langle 2n_i + a, a\rangle.$$

LEMMA 4.12. *If* $\alpha/4 \in (M_1^2)'$ *then*

$$\operatorname{tr}(s(2n_i) \cdot F) = 0, \qquad i \neq 0.$$

Proof. Since $M_1 \subset \frac{1}{2}M_1 \subset (\alpha M_1)'$ we may write $a \in (\alpha M_1)'/M_1$ as $a = a' + a''$, where a'' runs over a complete set of representations in $(\alpha M_1)'/\frac{1}{2}M_1$ and $a' \in \frac{1}{2}M_1/M_1$. Then,

$$\operatorname{tr}(s(2n_i) \cdot F) = \frac{1}{\sqrt{m_1}} \sum_{a', a''} e^{2\pi i T(\alpha(a'^2 + 2a'a'' + a''^2 + 2n_i a' + 2n_i a''))}.$$

But $T(\alpha a'^2) \subset Z$ and $T(\alpha a' a'') \subset Z$. Thus, simplifying,

$$\operatorname{tr}(s(2n_i) \cdot F) = \frac{1}{\sqrt{m_1}} \sum_{a''} e^{2\pi i T(\alpha(a''^2 + 2n_i a''))} \sum_{a' \in (1/2)M_1/M_1} e^{2\pi i T(2\alpha n_i a')}.$$

Since $2n_i \notin (\alpha M_1)'$, the mapping

$$a' \to e^{2\pi i T(2\alpha n_i a')}$$

is a non-trivial character on $\frac{1}{2}M_1/M_1$ and the inner sum is 0.

COROLLARY 4.12.1. *Suppose* $M \subset M_1$ *satisfy* $\alpha/4 \in (M_1^2)'$. *Then*

$$G = G_1;$$

Recall, $G = G(M, \alpha)$ *and* $G_1 = G(M_1, \alpha)$.

COROLLARY 4.12.2. *Suppose $M \subset M_1$ are α-integral modules. Then*

$$G(M, 4\alpha) = G(M_1, 4\alpha).$$

Let M_1, M be two α-integral modules. Then $M_1 \cap M$ is an α-integral module. Thus, $M_1 \cap M_2 \subset M_1$ implies

$$G(M_1 \cap M_2, 4\alpha) = G(M_1, 4\alpha)$$

and $M_1 \cap M_2 \subset M_2$ implies

$$G(M_1 \cap M_2, 4\alpha).$$

Thus, $G(M_1, 4\alpha) = G(M_2, 4\alpha)$ and $G(M, 4\alpha)$ is independent of the α-integral module M in $\mathcal{k}$. Hence, unambiguously, we can write $G(4\alpha)$. We will now compute $G(4\alpha)$ assuming the one dimensional case; namely, for $l \in \mathbb{Z}^x$,

$$G(4l) = \frac{1}{\sqrt{4|l|}} \sum_{0 \leqslant k < 4|l|} e^{2\pi i k^2/4\pi} = \begin{cases} 1+i, & l > 0, \\ 1-i, & l < 0. \end{cases}$$

The evaluation of the classical Gauss sum $G(4l)$ can be found in many places. (See [1] or [5].)

Before we begin the proof of Theorem A, we will make some additional comments on the $\mathbb{Q}$-bilinear form of $\mathcal{k}$.

$$(u, v) \to T(\alpha uv), \qquad u, v \in k.$$

Denote this form by T_α. In particular, we will show that the signature of this form is

$$S(\alpha) = \sum_{i=1}^{s} \operatorname{sgn}_i(\alpha).$$

The geometric embedding of $\mathcal{k}$

$$\sigma: \mathcal{k} \to \mathbb{R}^s \oplus \mathbb{C}^t \cong \mathbb{R}^h, \qquad h = s + 2t,$$

(see Section II), is defined by

$$\sigma(\beta) = (\sigma_1(\beta), \ldots, \sigma_s(\beta); \sigma_{s+1}(\beta), \ldots, \sigma_{s+t}(\beta)), \qquad \beta \in \mathcal{k}.$$

As is well known, $\sigma(\mathcal{k})$ is a rational vector space and

$$\mathbb{R}^h = \sigma(\mathcal{k}) \otimes_{\mathbb{Q}} \mathbb{R}.$$

Component-wise addition and multiplication makes $\mathbb{R}^e \oplus \mathbb{C}^t$ into a ring and

the mapping $\sigma: k \to \mathbb{R}^s \oplus \mathbb{C}^t$ is a ring injection homomorphism. Define the $\mathbb{R}$-linear form T': $\mathbb{R}^s \times \mathbb{C}^t \to \mathbb{R}$ by setting

$$T'(\beta_1,\ldots,\beta_s;\beta_{s+1},\ldots,\beta_{s+t}) = \sum_{l=1}^{s} \beta_l + 2 \cdot \text{real part}\left(\sum_{j=1}^{t} \beta_{s+j}\right).$$

Then, $T'(\sigma(\beta)) = T(\beta)$ whenever $\beta \in \mathfrak{k}$. Consider the $\mathbb{R}$-bilinear form on $\mathbb{R}^s \times \mathbb{C}^t$, viewing $\mathbb{R}^s \times \mathbb{C}^t$ as the $\mathbb{R}$-vector space $\mathbb{R}^h$,

$$(u, v) \to T'(\alpha \cdot u \cdot v), \qquad u, v \in \mathbb{R}^s \times \mathbb{C}^t.$$

This is clearly the $\mathbb{R}$-linear extension of the $\mathbb{Q}$-bilinear form T_α to $\mathbb{R}^s \times \mathbb{C}^t$ and hence the signature of the two forms are identical. By identifying $\mathbb{R}^s \times \mathbb{C}^t$ with $\mathbb{R}^h$ and choosing the standard basis for $\mathbb{R}^h$, the matrix of, $(u, v) \to T'(\alpha u v)$, is given by

$$\begin{bmatrix} \sigma_1(\alpha) & & & & & & \\ & \ddots & & & & & \\ & & \sigma_s(\alpha) & & & & \\ & & & a_{s+1} & -_{s+1} & & \\ & & & -b_{s+1} & -a_{s+1} & & \\ & & & & & \ddots & \\ & & & & & a_{s+t} & -b_{s+t} \\ & & & & & -b_{s+t} & -a_{s+t} \end{bmatrix},$$

where $a_{s+j} = 2$ real part of $\sigma_{s+j}(\alpha)$ and $b_{s+j} = 2$ imaginary part of $\sigma_{s+j}(\alpha)$. The signature is clearly $S(\alpha)$.

THEOREM A. $G(4\alpha) = 2^{h/2} e^{2\pi i S(\alpha)/8}$.

Proof. The $\mathbb{Q}$-bilinear form of $\mathfrak{k}$

$$(\beta_1, \beta_2) \to T(\alpha\beta_1\beta_2), \qquad \beta_1, \beta_2 \in \mathfrak{k},$$

diagonalizes. Thus, there exists a basis $v_1,\ldots, v_h$ of $\mathfrak{k}$ over $\mathbb{Q}$ such that

$$\begin{aligned} T(\alpha v_i v_j) &= l_i, \quad i = j, \\ &= 0, \quad i \neq j, \end{aligned} \qquad i \leqslant i,\ j \leqslant h,$$

where $l \in \mathbb{Z}^x$ and $\operatorname{sgn}_j(\alpha) = \operatorname{sgn}(l_j)$, $j = 1,\ldots, s$. Let M be the full module spanned by $v_1,\ldots, v_h$. The dual M' is then spanned by $\alpha v_1/l_1,\ldots, \alpha v_h/l_h$. A typical point $\gamma \in (4\alpha M)'/M$ can be written

$$\gamma = \sum_{j=1}^{h} m_j \frac{v_j}{4l_j}, \qquad \text{where} \quad 0 \leqslant m_j < 4\,|l_j|.$$

Thus,

$$G(4\alpha) = 1/\sqrt{m} \sum_{\gamma \in (4\alpha M)^{-1}/M} e^{2\pi i T(4\alpha\gamma^2)} = 1/\sqrt{m} \sum_{j=1} \sum_{0 \leqslant m_j < 4|l_j|} e^{2\pi i (m_j^2/4l_j)},$$

$$G(4\alpha) = \prod_{j=1}^{h} G(4l_j)$$

and the theorem is proved.

V. Generalized Cooley–Tukey Algorithm and Hecke Trigonometric Sums

This section is totally self-contained and draws no material form Section IV. Indeed, we will re-prove all the results of Section IV in a slightly more general setting. Our work in this section has been modelled on the approach of Cooley and Tukey [4].

Let us begin by recalling the Cooley–Tukey algorithm. In order to get the flavour of their thinking, we will quote from their original paper [4].

> Consider the problem of calculating the complex Fourier series
>
> (1) $$X(j) = \sum_{k=0}^{N-1} A(k)\, W^{jk} \qquad j = 0, 1, \ldots, N-1$$
>
> where the given Fourier coefficients $A(k)$ are complex and W is the principal Nth root of unity
>
> (2) $$W = e^{2\pi i/N}.$$
>
> ... Suppose N is a composite, i.e., $N = r_1 r_2$. Then let the indices in (1) be expressed
>
> (3) $$\begin{aligned} j &= j_1 r_1 + j_0 \qquad j_0 = 0, 1, \ldots, r_1 - 1 \qquad j_1 = 0, 1, \ldots, r_2 - 1 \\ k &= k_1 r_2 + k_0 \qquad k_0 = 0, 1, \ldots, r_2 - 1 \qquad k_1 = 0, 1, \ldots, r_1 - 1 \end{aligned}$$
>
> Then, one can write
>
> (4) $$X(j_1, j_0) = \sum_{k_0} \sum_{k_1} A(k_1, k_0)\, W^{jk_1 r_2}\, W^{jk_0}$$
>
> Since
>
> (5) $$W^{jk_1 r_2} = W^{j_0 k_1 k_2}$$
>
> the inner sum, over k_1, depends only on j_0 and k_0 and can be defined as a new array,
>
> (6) $$A_1(j_0, k_0) = \sum_{k_1} A(k_1, k_0)\, W^{j_0 k_1 r_2}$$

The result can then be written

$$X(j_1, j_0) = \sum A_1(j_0, k_0)\, W^{(j_1 r_1 + j_0)k_0} \tag{7}$$

There are N elements in the array A_1, each requiring r_1 operations, giving a total of Nr_1 operations to obtain A_1. Similarly, it takes Nr_2 operations to calculate X from A. Therefore, this two step algorithm, given by (6) and (7), requires a total $T = N(r_1 + r_2)$ operations.

We see that Cooley and Tukey looked at their algorithm as a "divide and conquer" algorithm and they arrived at their algorithm combinatorially.

We will now see how the Cooley–Tukey algorithm can be structured in a different way. (For further discussion of this type of restructuring see [9].) Let $F(n)$ denote the Fourier transform matrix on n points and let $A(i)$, $i = 0,..., n-1$, be the inputs that we think of as a column vector A. Our problem then becomes to evaluate $F(n)A = X$. Using the above notation, let (k_1, k_0) be ordered anti-lexicographically and let P_0 be the permutation matrix that takes $0,..., n-1$ into (k_1, k_0) in this ordering operating on columns. Then

$$F(N)\, P_0^t P_0 A = X$$

and

$$P_0 F(N)\, P_0^t P_0 A = P_0 X.$$

Let $F_0(N) = P_0 F(N)\, P_0^t$, $A_0 = P_0 A$, and $X_0 = P_0 X$. Our task becomes to compute $F_0(N)A_0 = X_0$.

Equation (6) in this notation can be rewritten as

$$A_1 = L_1 A_0,$$

where

$$L_1 = \begin{pmatrix} F(r_1) & & 0 \\ & \ddots & \\ 0 & & F(r_1) \end{pmatrix},$$

where $F(r_1)$ is the Fourier transform matrix on r_1 points and L_1 is an $r_1 r_2 \times r_1 r_2$ matrix.

We next separate (7) into two steps.

Step 1. Define $A_2 = DA_1$, where D is a diagonal matrix with diagonal terms $e^{2\pi i j_0 k_0 / N}$ ordered anti-lexicographically in (j_0, k_0).

Step 2. Let P_1 be the permutation matrix that reorders (j_0, k_0) from anti-lexicographical to lexicographical ordering again operating on columns. Then

$$P_1 X_0 = L_2 P_1 A_2,$$

where

$$L_2 = \begin{pmatrix} F(r_2) & & 0 \\ & \ddots & \\ 0 & & F(r_2) \end{pmatrix}$$

and $F(r_2)$ is the $r_2 \times r_2$ Fourier transform matrix. Thus

$$X_0 = P_1^t L_2 P_1 D L_1 A_0$$

or

$$F_0(N) = (P_1^t L_2 P_1) D L_1 .$$

Thus the Cooley–Tukey algorithm can be considered as a factorization of the finite Fourier transform matrix by matrices that are either diagonal or built from the finite Fourier transforms $F(r_1)$ and $F(r_2)$ and permutation matrices.

Now the matrix factorization

$$F = L^{-1} \mathcal{J} L$$

that was so important in our study of Hecke trigonometric sums has the property that each of the matrices $\mathcal{J}$ and L were built from the Fourier transform and diagonal matrices in much the same way as $F(N)$ was factored in the Cooley–Tukey algorithm. This suggests that we try to find a multidimensional Cooley–Tukey of algorithm that would yield an evaluation of $G(M, 4\alpha)$ by combinatorial means. If we could succeed, we would be able to able to obtain a combinatorial proof of Hecke's result, see how to formulate a multidimensional Cooley–Tukey algorithm, and, perhaps, help build a bridge between "pure" and "applied" mathematics.

One of the crucial ingredients in the Cooley–Tukey algorithm is a choice of coset representatives for quotient group $\mathbb{Z}/N\mathbb{Z}$. For $n \in \mathbb{Z}^+$, consider the coset representatives $0, 1, \ldots, n-1$ of the cosets $\mathbb{Z}/n\mathbb{Z}$. We notice that we can describe $0, \ldots, n-1$ as those elements $a \in \mathbb{Z}$ such that $0 \leqslant a/n < 1$.

Consider V as column k-vectors with rational entries and let $Z \subset V$ be an additive subgroup of k-vectors all of whose entries are integers. The non-singular $k \times k$ matrices with integer integer entries will be denoted by $GL(k, \mathbb{Z})$. For $A \in GL(k, \mathbb{Z})$, $Z \supset AZ$ and

$$Z/AZ$$

is a finite abelian group. We need to be able to describe coset representatives for Z/AZ in much the same way as we did for $\mathbb{Z}/n\mathbb{Z}$. To do this, let us define $I \subset V$ as the set of all vectors v all of whose coordinates v_i satisfy the

condition $0 \leqslant a_i < 1$, $i = 1,\ldots, k$. Now let $S_A = \{a \in Z \mid A^{-1}a \in I\}$. We claim that S_A is a set of coset representatives for Z/AZ. To verify this, first notice that if $a \in Z$ and

$$A^{-1}a = \delta + \xi, \qquad \delta \in I,\ \xi \in Z,$$

then $A\delta \in Z$ because both a and $A\xi$ are in Z. Thus S_A has sufficiently many elements. Next, let $a, a' \in S$ be in the same coset or let

$$a = a' + A\xi, \qquad \xi \in Z.$$

Then $A^{-1}a = A^{-1}a' + \xi$. Since $A^{-1}a$ and $A^{-1}a'$ are in I and $\xi \in Z$, we have $\xi = 0$ and $a = a'$. This completes the proof of our assertion.

Let V^t be the row k-vectors and consider V^t as the dual space to V with the pairing given by matrix multiplication. We will let $Z^t \subset V^t$ be the additive subgroups of row R-vectors all of whose coordinates are integral. Let $A \in GL(k, \mathbb{Z})$ and let $\widehat{(Z/AZ)}$ denote the dual group to Z/AZ. We want a good working description of $\widehat{(Z/AZ)}$. For $a \in Z^t$ and $a \in Z$ define

$$B(a, a) = e^{2\pi i a A^{-1} a}.$$

To simplify notation, we will henceforth denote $e^{2\pi i(\,)}$ by $E(\,)$. We claim that B induces a pairing

$$B^*: Z^t/Z^tA \times Z/AZ \to \mathbb{C}.$$

To see this, notice that if $a \in Z$

$$B(a', Aa) = 1, \qquad a' \in Z^t.$$

Similarly, if $a' \in Z^t$

$$B(a'A, a) = 1, \qquad a \in Z^*.$$

Hence B factors through $Z^t/Z^tA \times Z/AZ$ and so we have defined B^*. The rest of the argument is straightforward.

With this pairing of Z/AZ with its dual group, we may write the Fourier transform as

$$F(f)(a) = \frac{1}{\sqrt{\mathcal{O}}} \sum_{a \in S_A} E(a'A^{-1}a) f(a),$$

where $\mathcal{O}$ = order Z/AZ and $a' \in Z^t/Z^tA$. We let

$$F(A) = (E(a'A^{-1}a)), \qquad a' \in Z^t/Z^tA,\ a \in S_A.$$

Since Z^t/Z^tA can be identified with Z/A^tZ we may form S_{A^t} and view $a' \in (S_{A^t})^t$. We will henceforth do precisely this.

We may now introduce the analogue of $\mathbb{Z}/r_1r_2\mathbb{Z}$. Let $A, B \in GL(k, \mathbb{Z})$ and consider Z/ABZ. We will now construct a generalized Cooley–Tukey algorithm for evaluating $F(AB)X$.

We first choose

$$Z \supset AZ \supset ABZ.$$

We next choose a set of coset representatives of Z/ABZ that respects the above diagram. To do this define

$$S(AB) = \{Ab + a \mid b \in S_B, a \in S_A\}.$$

We assert that $S(AB)$ is a set of coset representatives of Z/ABZ. (In general, $S(AB) \neq S_{AB}$.) This assertion may be verified as follows: First, the elements of $S(AB)$ belong to distinct cosets. For if

$$Ab + a = Ab' + a' + ABz, \qquad z \in Z,\ a, a' \in {}_A,\ b, b' \in S_B,$$

then $b + A^{-1}a = b' + A^{-1}a' + Bz$. Equating fractional parts, yields $a = a'$. But since b and $b' \in S_B$, $b = b' + Bz$, implies that $b = b'$.

To see that $S(AB)$ has enough elements, let $z \in Z$. Then $A^{-1}z = \delta + \xi$, $\xi \in Z$, $\delta \in I$. Because $A\delta \in Z$, $a = A\delta \in S_A$. Now $z - a = A\xi$. But, there exists a unique $b \in S_B$ such that $\xi = b + B\xi'$, $\xi' \in Z$. Hence

$$z - a = Ab + AB'\xi'$$

or

$$z = (Ab + a) + AB\xi'$$

and so $S(AB)$ has enough elements.

We have, of course, that $(Z/ABZ)\hat{}$ may be identified with Z^t/Z^tAB which may be identified with A/B^tA^tZ. It is easily verified that

$$S(B^tA^t) = \{\alpha B + \beta \mid \alpha \in (S_{A_t})^t,\ \beta \in (S_{B^t})^t\}.$$

We will let $|C| =$ order Z/CZ. Then

$$F(AB)(f)(\alpha B + \beta)$$

$$= \frac{1}{|A|^{1/2}|B|^{1/2}} \sum_{a \in S_A,\, b \in S_B} E((\alpha B + \beta)B^{-1}A^{-1}(Ab + a) f(Aa + b))$$

$$= \frac{1}{|A|^{1/2}} \sum_{a \in S_A} E(\alpha A^{-1}a)\, E(\beta B^{-1}A^{-1}a)$$

$$\times \frac{1}{|B|^{1/2}} \sum_{b \in S_B} E(\beta B^{-1}b) f(Ab + a).$$

These formulas are exact analogues of formulas (6) and (7) of the Cooley–Tukey algorithm and, of course, may also be interpreted as factoring the Fourier transform matrix $F(AB)$. Again, there exist permutation matrices P_0 and P_1 such that

$$P_0^t F(AB) P_0 = (P_1^t L_2 P_1)\, DL_1,$$

where

$$L_1 = \begin{pmatrix} F(B) & & 0 \\ & \ddots & \\ 0 & & F(B) \end{pmatrix} \quad \text{and} \quad L_2 = \begin{pmatrix} F(A) & & 0 \\ & \ddots & \\ 0 & & F(A) \end{pmatrix}.$$

We could now go through a counting argument exactly as Cooley and Tukey did in their classical paper. But rather than doing this, we will use a modification of the above construction to obtain $F(ABA^t) = L^{-1}\mathscr{T}L$ which specializes to the construction of our previous section.

We begin by looking again at S_A, $A \in GL(k, \mathbb{Z})$. We want to define a group law of composition on S_A and analogous to working modulo n. Thus if $a_1, a_2 \in S_A$, define

$$a_1 + a_2 = A((A^{-1}a + A^{-1}a_2) \bmod Z),$$

where mod Z denotes taking the fractional parts of all components. One verifies that this operation makes S_A into an abelian group isomorphic to Z/AZ and that the inverse of $a \in S_A$, denoted by $-a$ is given by the formula

$$-a = A((\mathbf{1} - A^{-1}a) \bmod Z)$$

when $\mathbf{1} = (1,..., 1)^t$.

We will henceforth assume that $B = B^t$; i.e., that B is equal to its transpose. This really simplifies the formulas and it is the only case needed in Hecke's work. Hence we want to compute $F(ABA^t)$ by twice applying the generalized Cooley–Tukey algorithm. Of course if $C = AB$, we may consider $Z \supset CZ \supset CA^tZ$ and $Z \supset AZ \supset ABZ$ which combine to yield $Z \supset AZ \supset ABZ \supset ABA^tZ$. Similarly, by twice applying generalized Cooley–Tukey methods for choosing factor sets, we obtain

$$S(ABA^t) = \{ABc + Ab + a \mid c \in S_{A^t}, b \in S_B, a \in S_A\}.$$

Since $(ABA)^t = ABA^t$, we can identify the dual group of Z/ABA^tZ with itself or with Z^t/Z^tABA^t. Let $c' \in (S_{A^t})^t$, $b' \in (S_B)^t$, $a' \in (S_A)^t$ and $(C^{-1})^t = C^*$ for any matrix C. The factor set for the dual group to Z/ABA^tZ is $\{c'BA^t + b'A^t + a'\}$. Further, let

$$g(c, b, a) = f(ABc + Ab + a),$$
$$\hat{g}(c', b', a') = F(ABA^t)(f)(c'BA^t + b'A^t + a').$$

Then by the formula for the Fourier transform, we have

$$\begin{aligned}\hat{g}(c', b', a') &= \sum_a \sum_b \sum_c E((c'VA^t + b'A^t + a')A^*B^{-1}A^{-1}(ABc + Ab + a)) \\ &\quad \times g(c,b,a) \\ &= \sum_a E((c'BA^t + b'A^t + a')\,A^*B^{-1}A^{-1}a) \\ &\quad \times \sum_b E((c'BA^t + b'A^t + a')\,A^*B^{-1}a) \\ &\quad \times \sum_c E((c'BA^t + b'A^t + a')\,A^*c)\,g(c, b, a) \\ &= \mathrm{I} \times \mathrm{II} \times \mathrm{III}.\end{aligned}$$

Now III reduces to

$$\sum_c E(a'A^*c)\; g(c, b, a)$$

which is the Fourier transform $F(A^t)$, because Z/A^tZ is dually paired to Z/AZ. (Recall, that if $c \in S_{A^t}$ the coset representations of the dual group may be taken as $(S_A)^t$.) We now apply a permutation matrix and write

$$\sum_c E(a'A^*c)\; g(c, b, a) = h_0(a', a, b).$$

Next notice that II has a factor $E(a'A^*B^{-1}b)$ and so we may form

$$h_1(a', a, b) = E(a'A^*B^{-1}b)\, h_0(a', a, b).$$

Hence we have a linear transformation L such that

$$h_1 = Lg,$$

where $L = DF_1$, where D is a diagonal matrix and F_1 is built from a direct sum of $F(A^t)$ and a permutation matrix. Thus after some elementary operations, we may write

$$\hat{g}(c', b', a') = \sum_a E((c'BA^t + b'A^t + a')\, A^*B^{-1}A^{-1}a)$$

$$\times \sum_b E(b'B^{-1}b)\, h_1(a', a, b).$$

From this it is easy to see that

$$F(ABA^t) = L_2 \mathscr{J}_2 L,$$

where $\mathscr{J}_1$ is built from the Fourier transform $F(B)$ and L_2 is built from a direct sum of $F(A)$'s up to a diagonal and a permutation matrix. Unfortunately, $L_2 \neq L^{-1}$. We need to work harder to obtain $\mathscr{J}$ such that $F(ABA^t) = L^{-1}\mathscr{J}L$.

It will be clearer if we build $\mathscr{J}$ in stages. Begin by defining

$$h_2(a', a, b') = \sum_b E(b'B^{-1}b)\, h_1(a', a, b)$$

so that h_2 is obtained from h_1 by a direct sum of $F(B)$. Next define

$$h_3(\alpha, a', b') = h_2(a', a, b'),$$

where $\alpha = -a$. At this point in our computation

$$\hat{g}(c', b', a') = \sum_a E(c'A^{-1}a)\, E(b'B^{-1}A^{-1}a)\, E(a'A^*B^{-1}A^{-1}a)\, h_3(a, a', b').$$

Now multiply by $1 = E(a'A^*B^{-1}b')\, E(-a'A^*B^{-1}b')$ and let

$$\mathscr{J}(h_1(a', a, b)) = h_4(a, a', b'),$$

where

$$h_4(a, a', b') = E(a'A^*B^{-1}A^{-1}a)\, E(b'B^{-1}A^{-1}a)\, E(a', A^*B^{-1}b')\, h_3(a, a', b').$$

Then

$$\hat{g}(c', b', a') = \sum_a E(c'A^{-1}a)\, E(-a'A^*B^{-1}b')\, h_4(a, a', b').$$

Let $\hat{g}(c', b', a') = L_1 h_4(a, a', b')$. Then L_1 is built from the permutation matrix that takes $(a, a', b') \to (a, b', a')$ (notice this matrix is its own inverse), the diagonal matrix of multiplication by $E(-a'A^*B^{-1}b')$ which is the inverse of $E(a'A^*B^{-1}b)$ and finally from $\sum_a E(c'A^{-1}a)\, h_4(a, a', b')$. But because $\alpha = -a$ we have this as a sum

$$\sum_a E(-c'A^{-1}a)\, h_4(a, a', b)$$

or the matrix $F(A)^{-1}$. This proves that $L_1 = L^{-1}$ and we have that $F(ABA^t) = L^{-1}\mathscr{T}L$ as we wished to prove.

After sorting out indices we have that the trace $\mathscr{T}$ is describable as follows: Let $C = \{c \in S_A \mid -c = c\}$. Then

$$\operatorname{tr}(\mathscr{T}) = \sum_{c \in C} \sum_{b \in S_B} E((A^{-1}c + b)^t B^{-1}(A^{-1}c + b)).$$

Let $D = A^{-1}C$. Then $d \in D$ implies that $d = 1/2u$, where the coordinates of u are 0 or 1. Hence

$$\operatorname{tr}(\mathscr{T}) = \sum_{d \in D} \sum_{b \in S_B} E((d + b)^t B^{-1}(d + b)).$$

Let e_j be the jth coordinate vector. Assume the jth column of B is even or, equivalently, $\tau_j = e_j/2 \in S_B$. Let X be a coset of the subgroup generated by τ_j: then $S_B = X \cup (\tau_j + X)$, for fixed d,

$$\begin{aligned}
&\sum_{b \in S_B} E((d + b)^t B^{-1}(d + b)) \\
&\quad = \sum_{b \in X} E((d + b)^t B^{-1}(d + b)) + E((d + \tau_j + b)^t B^{-1}(d + \tau_j + b)) \\
&\quad = \sum_{b \in X} E((d + b)^t B^{-1}(d + b)) \left[1 + E(e_j^t(d + b))\, E\left(e_j^t \frac{B}{4} e_j\right)\right].
\end{aligned}$$

If we assume $e_j^t d = \frac{1}{2}$ and the (j, j) term of B, b_{jj}, is divisible by 4, then $1 + E(e_j^t(d + b))\, E(e_j^t(B/4)e_j) = 1 + E(\frac{1}{2}) = 0$. Hence, if for each $d \in D$, $d \neq 0$, there exists j such that $e_j/2 \in S_B$, $e_j^t d = \frac{1}{2}$, $b_{jj}/4 \in \mathbb{Z}$ (for example, if every element of B is even, and b_{jj} is divisible by 4 for every j), we obtain our desired result that

$$\operatorname{tr}(F(ABA^t)) = \operatorname{tr}(\mathscr{T}) = \sum_{b \in S_B} E(b^t B^{-1} b).$$

One verifies that the above conditions are satisfied when we want to apply this method to the Hecke results.

VI. From Induced Representations to Cooley–Tukey in a Hecke Setting

The results in Sections IV and V suggest that there must exist a deep relation between induced representations of finite Heisenberg groups and the generalize Cooley–Tukey algorithm. We will close this paper by establishing this relation in the setting of full modules of number fields. (The interested

reader should not have too much difficulty in carrying this out in a general setting.) Doing this will indicate how one could replace the discussion in Section IV with that of Section V.

In this section we will return to the notations of Sections I through IV. Let $\alpha \in \mathfrak{k}^x$ and let $M \subset M_1$ be α-integral modules in $\mathfrak{k}$. Set $A = (\alpha M)'/M$ and $A_1 = (\alpha M_1)'/M_1$. Let F and F_1 denote the Fourier transforms of A and A_1, respectively, where we have identified A and A_1 with their dual groups as usual. Put $r = o(M_1/M) = o((\alpha M)'/(\alpha M_1)'$ and $s = o(A_1)$. Then $rs = o((\alpha M_1)'/M)$ and $r^2 s = o(A)$. Let $0 = n_0, n_1, \ldots, n_{r-1} \in (\alpha M)'$ be a set of coset representations of $(\alpha M)'/(\alpha M_1)'$ and $0 = y_0, y_1, \ldots, y_{s-1} \in (\alpha M_1)'$ be a set of coset representatives of A_1.

Consider the representations ζ and π of $N(A)$ defined in Section IV. Recall that ζ is defined by the formula

$$(\zeta(a, b, c) f)(a') = c\langle b, a' \rangle f(a' + a),$$

where $(a, b, c) \in N(A)$, $a' \in A$, $f \in L^2(A)$. The representation π was given as an induced representation; namely, it was induced from the representation π_1 of

$$\mathscr{E} = (\alpha M_1)'/M \times (\alpha M_1)'/M \times C$$

on $L^2(A_1)$. The representation space W of π can be written as

$$W = \otimes \sum_{0 \leqslant i, j < r} W(i, j),$$

where each $W(i, j) \simeq L^2(A_1)$ is invariant and irreducible under the representation $\pi(\mathscr{E})$. In particular,

$$\pi(a, b, c) \mid W(i, j) = \langle n_i, b \rangle \langle n_j, a \rangle^{-1} \pi_1(a, b, c),$$

where $(a, b, c) \in \mathscr{E}$ and therefore $W(i, j)$ is the character space for $\pi(K)$, where $K = M_1/M \times M_1/M \times (1)$, corresponding to the character of K given by $(a, b, c) \to \langle n_i, b \rangle \langle n_j, a \rangle^{-1}$.

Let L: $L^2(A) \to W$ be an intertwining operator between ζ and π. Then we showed that there exists a unitary operator $\mathscr{T}$ of W such that $\mathscr{T}$ was an intertwining operator for π and $\pi_0 J$ and $F = L^{-1} \mathscr{T} L$. The importance of the operator $\mathscr{T}$ is that its structure is simplified by the property: $\mathscr{T}(W(i, j)) = W(j, -i)$. This is equivalent to $F(L^{-1}(W(i, j))) = L^{-1}(W(j, -i))$ and hence we shall study F on the subspaces $L^{-1}(W(i, j))$, $0 \leqslant i, j < r$.

Set $V(i, j) = L^{-1}(W(i, j))$, $0 \leqslant i, j < r$. We will begin by describing the subspaces $V(i, j)$ of $L^2(A)$.

LEMMA 6.1. *$V(i, j)$ consists of all functions $f \in L^2(A)$ which satisfy*

(i) *f vanishes outside of $(n_i + (\alpha M_1)')/M$;*

(ii) $f(a' + a) = \langle n_j, a\rangle^{-1} f(a')$, $a \in M_1/M$, $a' \in A$.

Proof. For any $f \in V(i, j)$

$$\pi((a, b, 1))(L(f)) = \langle n_i, b\rangle\langle n_j, a\rangle^{-1} L(f), \qquad (a, b, 1) \in K.$$

Thus $\zeta((a, b, 1))f = \langle n_i, b\rangle\langle n_j, a\rangle^{-1} f$. By the definition of ζ this implies that

$$(*) \qquad \langle b, a'\rangle f(a' + a) = \langle n_i, b\rangle\langle n_j, a\rangle^{-1} f(a'),$$

where $a, b \in M_1/M$ and $a' \in A$. In particular,

$$\langle n_i, b\rangle f(a') = \langle b, a'\rangle f(a'), \qquad b \in M_1/M,\ a' \in A,$$

from which is follows that $f(a') = 0$, for $a' \in A$ unless $\langle a' - n_i, b\rangle = 1$ for all $b \in M_1/M$. Thus, f vanishes outside of $(n_i + (\alpha M_1)')/M$. The second assertion follows directly from (*) if we put $b = 0$.

Let $f \in L^2((\alpha M)'/M)$ and consider $F(f)$. Our method for evaluating $F(f)$ is as follows:

(1) Write $f = \sum_{0 \leqslant i, j < r} f_{ij}$, $\qquad f_{ij} \in V(i, j)$.

(2) Find $F(f_{ij})$, $0 \leqslant i, j < r$.

(3) From $F(f) = \sum_{0 \leqslant i, j < r} F(f_{ij})$.

Let $f \in L^2((\alpha M)'/M)$ and $a \in (\alpha M)'/M$. For $0 \leqslant j < r$, put

$$t_j(a) = \frac{1}{r} \sum_{x \in M_1/M} f(a + x)\langle x, n_j\rangle.$$

It is easy to see that

$$f_j(a + a') = \langle a', n_j\rangle^{-1} f_j(a), \qquad a' \in M_1/M,$$

and, since

$$\sum_{0 \leqslant j < r} \langle x, n_j\rangle = 0, \qquad x \neq 0,$$
$$= r, \qquad x = 0,$$

a simple computation shows that $f = \sum_{0 \leqslant j < r} f_j$. Take

$$f_{ij} = f_j \mid (n_i + (\alpha M_1)')/M.$$

The following result is now easily verified.

LEMMA 6.2. $L^2((\alpha M_1)'/M) = \oplus \sum_{0<j<r} V(0, j)$.

We will also require the following result.

LEMMA 6.3. $L^2((\alpha M)'/M_1) = \sum_{0<i<r} V(i, 0)$.

Proof. By Lemma 6.1, if $f \in \sum_{0<i<r} V(i, 0)$ then f is invariant under translation by M_1. The remainder of the proof is now obvious.

Recall that the symmetric isomorphism $D: A \to A^*$ was defined by

$$\langle a, b\rangle = \langle a, Db\rangle = e^{2\pi i T(\alpha a b)}, \qquad a, b \in A,$$

and consider its restriction to $(\alpha M_1)'/M$. Take $b \in (\alpha M_1)'/M$. Then,

$$Db(x) = \langle x, Db\rangle = \langle x, b\rangle = e^{2\pi i T(\alpha x b)} = 1$$

for all $x \in M_1/M$. Thus $Db \in ((\alpha M)'/M_1)^*$. It is easy to show that the mapping

$$b \to Db: (\alpha M_1)'/M \to ((\alpha M)'/M_1)^*$$

is an isomorphism. Also, D satisfies the short exact sequence

$$0 \to M_1 \to (\alpha M)' \xrightarrow{D} ((\alpha M_1)'/M)^* \to 0$$

and hence $(\alpha M)'/M_1 \simeq ((\alpha M_1)'/M)^*$. We will fix this identification in all that follows and let

$$F_0: L^2((\alpha M_1)'/M) \to L^2((\alpha M)'/M_1)$$

be the corresponding Fourier transform.

We will also need to consider the Fourier transform of the group $(\alpha M)'/(\alpha M_1)'$. The same argument as above shows that

$$M_1/M \simeq ((\alpha M)'/(\alpha M_1)')^*.$$

Let

$$F_2: L^2((\alpha M)'/(\alpha M_1)') \to L^2(M_1/M)$$

be the corresponding Fourier transform.

We will now consider the behavior of F restricted to each of the subspaces $V(i, j)$. By Lemma 4.8, F defines an isometry from $V(i, j)$ to $V(j, -i)$. Thus, it defines an isometry $\oplus \sum_{j=0}^{r-1} V(0, j) \to \oplus \sum_{i=0}^{r-1} V(i, 0)$. As above, we let F_0 be the Fourier transform of $(\alpha M_1)'/M$. Then the following result is now immediate.

LEMMA 6.4. *$F_0 = \sqrt{r}\, F \mid L^2((\alpha M_1)'/M)$, where we identify $L^2((\alpha M_1)'/M)$ with $\oplus \sum_{j=0}^{r-1} V(0, j)$.*

Since $0 = y_0, y_1, \ldots, y_{s-1}$ is a complete set of coset representatives of $(\alpha M_1)'/M_1 = A$ and $0 = n_0, n_1, \ldots, n_{r-1}$ is a complete set of coset representatives of $(\alpha M)'/(\alpha M_1)'$, every $a \in (\alpha M_1)'/M$ can be written uniquely as $a' = n_j + y_k + x$, $0 \leqslant j < r$, $0 \leqslant k < s$, $x \in M_1/M$. This notation will be maintained for the rest of this section.

We will now study the action of F on $V(i, j)$. Take $f \in V(i, j)$ and consider the function

$$g(y) = \langle n_j, y \rangle f(n_i + y), \qquad y \in (\alpha M_1)'.$$

Property (ii) in the definition of $f \in V(i, j)$ implies that

$$g(y + x) = g(y), \qquad x \in M_1.$$

Thus, we may view $g \in L^2((\alpha M_1)'/M_1)$.

LEMMA 6.5. *Let $f \in V(i, j)$ and let $a = n_j + y_l + x \in (\alpha M)'/M$, $0 \leqslant j < r$, $0 \leqslant l < s$, $x \in M_1/M$. Then $F(f) \in V(j, -i)$ and*

$$F(f)(a) = \langle n_i, a \rangle \frac{1}{\sqrt{s}} \sum_{y \in A_1} g(y) \langle y, y_l \rangle = \langle n_i, a \rangle F_1(g)(y_l),$$

where $g \in L^2((\alpha M_1)'/M_1)$ is defined by

$$g(y) = \langle n_j, y \rangle f(n_i + y), \qquad y \in (\alpha M_1)'.$$

Remark. When we want to explicitly express the dependence of g on n_i we write $g = g_{ij}$.

Proof. Since f vanishes outside of $(n_i + (\alpha M_1)')/M$, it follows that

$$F(f)(a) = \frac{1}{\sqrt{r^2 s}} \sum_{x' \in M_1/M} \sum_{0 \leqslant k < s} f(n_i + y_k + x') \langle n_i + y_k + x', a \rangle.$$

Using

$$f(n_i + y_k + x') = \langle x', n_j \rangle^{-1} f(n_i + y_k)$$

we can write the above equation as

$$F(f) = \frac{1}{\sqrt{r^2 s}} \sum_{x' \in M_1/M} \langle x', a - n_j \rangle \sum_{0 \leqslant k < s} f(n_i + y_k) \langle n_i + y_k, a \rangle.$$

Because $\sum_{x' \in M_1/M} \langle x', a - n_j \rangle = r$, it follows that

$$F(f) = \frac{1}{\sqrt{s}} \sum_{0 \leqslant k < s} f(n_i + y_k)\langle n_i + y_k, a \rangle$$

$$= \frac{\langle n_i, a \rangle}{\sqrt{s}} \sum_{0 \leqslant k < s} f(n_i + y_k)\langle y_k, n_j \rangle \langle y_k, y_l \rangle.$$

The lemma now follows the definition of g.

Let $f \in L^2(\hat{M}/M)$. Write $f = \sum_{0 \leqslant i,j < r} f_{ij}$, $f_{ij} \in V(i, j)$. Then $F(f) = \sum_{0 \leqslant i,j < r} F(f_{ij})$ and if $a = n_j + y_l + x \in \hat{M}/M$,

$$F(f)(a) = \sum_{0 \leqslant i,j < r} F(f_{ij})(a).$$

We will now explicitly carry out the steps indicated by the above formula. Let $g_{ij} \in L^2((\alpha M_1)'/M_1)$ be defined by

$$g_{ij}(y) = \langle y, n_j \rangle f_{ij}(n_i + y), \qquad y \in (\alpha M_1)'.$$

Form $F_1(g_{ij})(y_l)$ and define $h \in L^2((\alpha M_1)'/(\alpha M_1)')$ by requiring

$$h(n_i) = \langle n_i, y_l + n_j \rangle F_1(g_{ij})(y_l), \qquad 0 \leqslant i < r.$$

Clearly, h depends upon y_l and n_j. By Lemma 7.3,

$$F(f)(a) = \sum_{0 \leqslant i < r} F(f_{ij})(a) = \sum_{0 \leqslant i < r} \langle n_i, x \rangle \langle n_i, n_j + y_l \rangle F_1(g_{ij})(y_l)$$

which by the definition of h becomes

$$F(f)(a) = \sqrt{r}\, F_2(h)(x).$$

We organize this discussion in the following lemma.

LEMMA 6.6. *For $f \in L^2((\alpha M)'/M)$ and $a = n_j + y_l + x \in (\alpha M)'/M$,*

$$F(f)(a) = \sqrt{r}\, F_2(h)(x),$$

where $h \in L^2((\alpha M)'/(\alpha M_1)')$ is defined by

$$h(n_i) = \langle n_i, n_j + y_l \rangle F_1(g_{ij})(y_l), \qquad 0 \leqslant i < r.$$

As a special case, consider $f \in L^2((\alpha M_1)'/M) \subset L^2((\alpha M)'/M)$. Recall that $F_0 = \sqrt{r}\, F \mid L^2(\alpha\alpha M_1)'/M)$.

COROLLARY 6.7. *Let* $f \in L^2((\alpha M_1)'/M)$ *and* $s = n_j + y \in (\alpha M)'/M_1$. *Then*

$$F_0(f)(a) = \frac{1}{\sqrt{s}} \sum_{y' \in A_1} \langle y', y\rangle \langle n_j, y'\rangle \frac{1}{\sqrt{r}} \sum_{x' \in M_1/M} f(y' + x')\langle x', n_j\rangle.$$

This corollary is the generalized Cooley–Tukey algorithm in a Hecke setting.

We will close this paper with an interesting special example—the classical Cooley–Tukey algorithm.

EXAMPLE. Let $a = 1/s$, $s \in \mathbb{Z}^x$ and $M = rs\mathbb{Z} \subset M_1 = s\mathbb{Z}$, $r \in \mathbb{Z}^x$. Then $(\alpha M_1)' = \mathbb{Z}$, $(\alpha M)' = (1/r)\mathbb{Z}$ and Corollary 6.7 becomes the following result. Let $f \in L^2(\mathbb{Z}/rs\mathbb{Z})$ and $a = n_j + y \in (1/r)\mathbb{Z}/s\mathbb{Z}$. Write $n_j = (1/r)n_j'$, $n_j' \in \mathbb{Z}/r\mathbb{Z}$. Then

$$F_0(f)(a) = \frac{1}{\sqrt{s}} \sum_{y' \in \mathbb{Z}/s\mathbb{Z}} E\left(\frac{y'y}{s}\right) E(n_j'y') \frac{1}{\sqrt{r}} \sum_{x' \in \mathbb{Z}/r\mathbb{Z}} f(y' + sr') E\left(\frac{x'n'}{r}\right),$$

where $E(\ ) = e^{2\pi i(\ )}$.

Note added in proof. R. M. Mersreau and T. C. Speake, in A unified treatment of Cooley–Tukey algorithms for evaluation of the multidimensional DFT, *IEEE Trans. Acoustics, Speech and Signal Processing* **29**, No. 5 (October 1981), 1011–1017, present a multidimensional Cooley–Tukey algorithm that is equivalent to that present in our paper.

REFERENCES

1. L. AUSLANDER AND R. TOLIMIERI, Is computing with the finite Fourier transform pure or applied mathematics, *Bull. Amer. Math. Soc. (New Series)*, (1979), 847–897.
2. L. AUSLANDER AND R. TOLIMIERI, "Abelian Harmonic Analysis, Theta Functions and Function Algebras on a Nilmanifold," Lecture Notes in Mathematics No. 436, Springer-Verlag, New York/Berlin, 1975.
3. H. BRAUN, Geschlechter quadratischer Formen, *J. Reine Angew. Math.* **182** (1940), 32–49.
4. J. W. COOLEY AND J. W. TUKEY, An algorithm for the machine calculation of complex Fourier series, *Math. Comp.* **19** (1965), 297–301.
5. E. HECKE, "Vorlesunger über die Theorie der Algebraischen Zahlen," Leitzig, 1923.
6. J. MILNOR AND D. HUSEMOLLER, "Symmetric Bilinear Forms," Springer-Verlag, New York/Berlin, 1973.
7. I. SCHUR, Ube die Gaussishaen summen, *Nachr. K. Ges. Wiss. Goettingen Math. Phys. Kl*, (1921), 147–153.
8. A. WEIL, Sur certaines groupes d'opérateurs unitaines, *Acta Math.* **11** (1964), 143–211.
9. D. J. ROSE, Matrix identities of the fast Fourier transform, *Linear Algebra and Appl.* **29** (1980), 423–443.