THE CYCLOTOMY OF FINITE COMMUTATIVE P.I.R.'s

BY

PHILIP C. KUTZKO[1]

Introduction

In recent years the term "cyclotomy" has been used to refer to various structures bearing only formal resemblance to the structure of nth division points on the circle whence the term derives [3], [7], [15]. Thus there is discussion of the cyclotomy of finite fields [9] or of "Galois Domains" [15] or even of Kloosterman or hyper-Kloosterman sums [11], [12]. It is the purpose of this paper to provide a unified theory of cyclotomy which will include the examples given above as special cases.

Following an approach used by Hall [9] we discuss in Sections 1–3 the conjugacy class structure and representations of finite split metabelian groups and under certain restrictions describe a certain duality between the classes and representations. In Section 4 we consider the group which is the split extension of the additive group of a finite commutative principal ideal ring by its group of units, the action being that of multiplication, and by applying the theory developed in Sections 1–3 are able to define generalized cyclotomic classes, periods, and numbers for the ring in question. In Section 5 we utilize the theory of finite dimensional Fourier transforms to generalize the classical Gauss and Jacobi sums and prove appropriate theorems concerning them. In Section 6.1 and Section 6.2 we compute the cyclotomy of a finite field and of a "Galois Domain" and show that our definitions coincide with those usually given. Finally, in Section 6.3, we show that by considering the cyclotomy of the ring which is a direct sum of n-copies of a given finite field we may determine the "cyclotomic" properties of Kloosterman and hyper-Kloosterman sums alluded to in [11] and [12].

We assume throughout a knowledge of the elementary properties of complex characters such as may be found in Chapter 1 of [5].

1. Preliminaries

All groups discussed will be finite and all characters will be complex. Unless otherwise noted, A will denote a multiplicatively written abelian group and G will denote a multiplicatively written abelian group of automorphisms of A.

Received October 16, 1973.

[1] The author was partially supported by a National Science Foundation grant. The author wishes to thank the University of Maine, Farmington, for providing him with an office for part of the summer of 1973.

The action of G (or more generally the integral group ring ZG) on A will be written exponentially as will group conjugation. If σ is an element of ZG we write A^σ and A_σ for the image and kernel of σ respectively. We denote the semi-direct product of A with G by $\mathscr{G}$ and we shall identify A and G with subgroups of $\mathscr{G}$ so that we may write $\mathscr{G} = AG$.

If C is a G-orbit in A then, since G is abelian, the stability subgroup in G of an element of C will be independent of the element chosen, depending only on C. We denote this stability subgroup by T_C and write $\mathscr{T}_C$ for the subgroup AT_C of $\mathscr{G}$.

Now let $\hat{A}$ be the complex dual of A. Then there is a natural action of G on $\hat{A}$ given by $\psi^\sigma(a) = \psi(a^\sigma)$ for ψ in $\hat{A}$, σ in G. As above, if $\hat{C}$ is a G-orbit in $\hat{A}$ we write $T_{\hat{C}}$ for the stability subgroup in G of any element of $\hat{C}$ and write $\mathscr{T}_{\hat{C}}$ for $AT_{\hat{C}}$.

For an arbitrary group K with subgroup H we shall denote by $(\ ,\ )_K$ and $(\ ,\ )_H$ the usual Hermitian inner product of complex valued functions on K and H respectively. For class functions μ on H and χ on K, μ^K and $\chi|_H$ denote respectively the class function induced by μ on K and the restriction of χ to H.

2. The characters of $\mathscr{G}$

We now describe the irreducible characters of $\mathscr{G}$. Since this description is, except for notation, identical to that given in Section 8.2 of [14], proofs are omitted and the reader is referred there for details.

To any G-orbit $\hat{C}$ in $\hat{A}$ we associate a set of characters $ch(\hat{C})$ of $\mathscr{G}$ as follows. Let ψ be any character in $\hat{C}$ and define the complex function η_ψ on $\mathscr{T}_{\hat{C}}$ by $\eta_\psi(at) = \psi(a)$ for a in A, t in $T_{\hat{C}}$. Then η_ψ is in fact a homomorphism. Let ω range through $\hat{T}_{\hat{C}}$ and view ω as a character on $\mathscr{T}_{\hat{C}}$. Then by $ch(\hat{C})$ we mean the set of characters $(\omega\eta_\psi)^{\mathscr{G}}$. It may be shown that if ϕ is any other character in $\hat{C}$ then $(\omega\eta_\psi)^{\mathscr{G}} = (\omega\eta_\phi)^{\mathscr{G}}$ for ω in $\hat{T}_{\hat{C}}$. Thus $ch(\hat{C})$ is well defined. In particular, the character $(\eta_\psi)^{\mathscr{G}}$ depends only on $\hat{C}$ and we denote this character by $\chi_{\hat{C}}$. Finally we have:

PROPOSITION 1. *The characters constructed above are all irreducible and in fact the set of irreducible characters of $\mathscr{G}$ is the disjoint union of the sets $ch(\hat{C})$ where $\hat{C}$ ranges over all G-orbits of $\hat{A}$.*

3. Conjugacy classes of $\mathscr{G}$

In this section we give a description of the conjugacy classes of $\mathscr{G}$ which is in some sense dual to the description given in Section 2 of the irreducible characters of $\mathscr{G}$. In order to do this we must first place a restriction on the pair (A, G).

DEFINITION 1. We say that the pair (A, G) is *admissible* if for each σ in G there exists f_σ in $\mathrm{Hom}_G(A, A)$ such that $\mathrm{Im}(1 - \sigma) = \ker f_\sigma$ and $\ker(1 - \sigma) = \mathrm{Im} f_\sigma$.

We assume from now on that (A, G) is admissible and that the maps f_σ have been fixed with f_1 = identity.

LEMMA 1. *Let C be a G-orbit of A and pick σ in G so that $C \subseteq A_{1-\sigma}$. Then the set $f_\sigma^{-1}(C)\sigma$ is a conjugacy class of $\mathscr{G}$. Conversely, each conjugacy class of G is in the form $f_\sigma^{-1}(C)\sigma$ with C and σ determined by the class.*

Proof. Let σ_1 and σ_2 be elements of G and let a_1 and a_2 be elements of A. Then $a_1\sigma_1$ and $a_2\sigma_2$ are in the same conjugacy class of $\mathscr{G}$ if and only if there exist elements τ in G and b in A such that

$$b\tau a_1\sigma_1 = a_2\sigma_2 b\tau$$

or equivalently such that

$$\sigma_1 = \sigma_2 \quad \text{and} \quad a_2 = a_1^\tau b^{1-\sigma_2}$$

Our result now follows easily.

DEFINITION 2. We denote the conjugacy class $f_\sigma^{-1}(C)\sigma$ described in Lemma 1 by (C, σ). We note that $C = (C, 1)$.

We put a further condition on the pair (A, G) which will suffice to introduce a certain symmetry into the character table of $\mathscr{G}$.

DEFINITION 3. We say that A is a *symmetric* G-module if there exists a non-degenerate balanced symmetric G-map from $A \times A$ into the multiplicative group of the numbers, $\mathbf{C}^\times$.

We now assume that A is a symmetric G-module and denote the balanced symmetric G-map by $[\ ,\ ]$. We note that by definition $[\ ,\ ]$ has the following properties:

(1) $[a, b] = [b, a]$ for a, b in A.
(2) $[a_1a_2, b] = [a_1, b][a_2, b]$ for a_1, a_2, b in A.
(3) $[a^\sigma, b] = [a, b^\sigma]$ for a, b in A, σ in G.
(4) $[a, b] = 1$ for all b in A if and only if $a = 1$.

We note that we may identify A with $\hat{A}$ as G-modules by $a \mapsto [\ , a]$. We make this identification for the remainder of this paper and henceforth write $ch(C)$ for $ch(\hat{C})$, χ_C for $\chi_{\hat{C}}$, etc.

LEMMA 2. *Let C_1 and C_2 be G-orbits of A. Then*

$$\chi_{C_1}(C_2) = \frac{|C_1|}{|C_2|}\,\chi_{C_2}(C_1)$$

where by $\chi_{C_1}(C_2)$ we mean the value which χ_{C_1} takes on any element of C_2.

Proof. Let a_i be an element of C_i, $i = 1, 2$. Then by definition,

$$\chi_{C_1}(C_2) = \frac{1}{|\mathscr{T}_{C_1}|} \sum_{\gamma \text{ in } \mathscr{G}} [a_2^\gamma, a_1]$$

$$= \frac{1}{|T_{C_1}|} \sum_{g \text{ in } G} [a_2^g, a_1]$$

$$= \frac{|C_1|}{|G|} \sum_{g \text{ in } G} [a_2^g, a_1]$$

Similarly,

$$\chi_{C_2}(C_1) = \frac{|C_2|}{|G|} \sum_{g \text{ in } G} [a_1^g, a_2]$$

The result now follows from the properties of [,].

DEFINITION 4. Let C_1, C_2, and C_3 be G-orbits in A. Then by $c(C_1, C_2, C_3)$ we mean the number of pairs (x_1, x_2) in $C_1 \times C_2$ such that $x_1 x_2 = a_3$ for some fixed element a_3 in C_3. This number is clearly independent of the element a_3 chosen. By $\hat{c}(C_1, C_2, C_3)$ we mean the inner product $(\chi_{C_3}, \chi_{C_1}\chi_{C_2})_{\mathscr{G}}$.

PROPOSITION 2. *Let C_1, C_2, and C_3 be G-orbits in A and write T_i for T_{C_i}, $i = 1, 2, 3$. Then*

$$c(C_1, C_2, C_3) = \frac{|T_3|}{|T_1 \cap T_2 \cap T_3|} \hat{c}(C_1, C_2, C_3).$$

Proof. χ_{C_i} is 0 off $\mathscr{T}_{C_i}$. Also $\chi_{C_i}(at) = \chi_{C_i}(a)$ for t an element of T_i. Therefore

$$\hat{c}(C_1, C_2, C_3) = \frac{1}{|\mathscr{G}|} \sum_{\gamma \text{ in } \mathscr{G}} \chi_{C_1}(\gamma)\chi_{C_2}(\gamma)\overline{\chi_{C_3}(\gamma)}$$

$$= \frac{1}{|\mathscr{G}|} \sum_{\substack{t \text{ in} \\ T_1 \cap T_2 \cap T_3, \\ a \text{ in } A}} \chi_{C_1}(at)\chi_{C_2}(at)\overline{\chi_{C_3}(at)}$$

$$= \frac{|T_1 \cap T_2 \cap T_3|}{|\mathscr{G}|} \sum_{a \text{ in } A} \chi_{C_1}(a)\chi_{C_2}(a)\overline{\chi_{C_3}(a)}$$

$$= \frac{|T_1 \cap T_2 \cap T_3|}{|\mathscr{G}|} \sum_{C} |C|\chi_{C_1}(C)\chi_{C_2}(C)\overline{\chi_{C_3}(C)}$$

where this last sum is taken over all G-orbits C of A.

On the other hand,

$$c(C_1, C_2, C_3) = \frac{|C_1|\,|C_2|}{|\mathscr{G}|} \sum_{\chi} \frac{\chi(C_1)\chi(C_2)\overline{\chi(C_3)}}{\chi(1)}$$

where the sum is taken over all irreducible characters χ of G. We fix a G-orbit C of A and sum first over $ch(C)$. $\chi(C_i)$ does not depend on the character χ chosen in $ch(C)$; in particular $\chi(1) = |C|$ for all such characters. Since there are $|T_C| = |G|/|C|$ characters in $ch(C)$ we obtain

$$c(C_1, C_2, C_3) = \frac{|C_1|\,|C_2|}{|\mathcal{G}|} \sum_C \frac{|G|}{|C|^2} \chi_C(C_1)\chi_C(C_2)\overline{\chi_C(C_3)}.$$

By Lemma 2, this last sum is equal to

$$\frac{|T_3|}{|\mathcal{G}|} \sum_C |C|\chi_{C_1}(C)\chi_{C_2}(C)\overline{\chi_{C_3}(C)}$$

which establishes the result.

4. The cyclotomic group of a P.I.R.

DEFINITION 5. Let R be a finite commutative Principal Ideal Ring and let G and A be the group of units $R^{\times}$ and the additive group R^{+} of A respectively. (We now write A additively.) Let G act on A by ring multiplication. Then the group $\mathcal{G} = AG$ is called the *cyclotomic* group of R.

LEMMA 3. *If G and A are as above then*
(1) *(A, G) is admissible, and*
(2) *A is a symmetric G-module.*

Proof. (1) Let u be a unit in R and let $I = (a)$ be the annihilator in R of $1 - u$. Then viewing multiplication by a as an $R^{\times}$-homomorphism of R^{+}, we see that $\operatorname{im} a = \ker (1 - u)$. But $\operatorname{im} (1 - u)$ is contained in $\ker a$ so by a simple index computation, $\operatorname{im} (1 - u) = \ker a$.

(2) We may write R as a direct sum of primary P.I.R.'s [20]. Let R_0 be one such summand and let J be its unique minimal ideal. Then since $\mathbf{C}^{\times}$ is a divisible group we may take some non-trivial character of J^{+} and extend it to a character on R_0^{+}. Taking the product of one such character for each primary summand of R we obtain a character $\hat{a}$ of R^{+} which cannot contain any non-trivial ideal of R in its kernel. Define the pairing $[\ ,\ ]$ by $[a_1, a_2] = \hat{a}(a_1 a_2)$ for a_1 and a_2 in R. Then $[\ ,\ ]$ is clearly a symmetric balanced map on $R^{+} \times R^{+}$ and it is nondegenerate since $[R^{+}, a] = 1$ implies that $\hat{a}(aR) = 1$ so that $a = 0$.

Now take G and A as above and let H be a subgroup of G. It is clear that the conclusions of Lemma 3 hold for the pair (A, H). The set of H orbits of A which are contained in the subset G of A are precisely the cosets of H in G.

DEFINITION 6. (a) With notation as above, we write C_σ for the coset of H in G corresponding to the element σ in G/H. Given elements σ and τ of G/H we write $(\sigma, \tau)_H$ for $c(C_1, C_\sigma, C_\tau)$ and call the numbers $(\sigma, \tau)_H$ *the cyclotomic numbers* of R with respect to H.

(b) We write χ_σ for the character χ_{C_σ}, σ an element of G/H. We write η_σ for $\chi_1(C_\sigma)$ and call the complex numbers η_σ the *cyclotomic periods* of R with respect to H.

We note that $c(C_\sigma, C_\tau, C_\mu) = \hat{c}(C_\sigma, C_\tau, C_\mu) = (\sigma\tau^{-1}, \mu\tau^{-1})_H$ and that $\chi_\sigma(C_\tau) = \eta_{\sigma\tau}$. It is immediate from this that $(\sigma, \tau)_H = (\sigma^{-1}, \tau\sigma^{-1})_H$ and that $(\sigma, \tau)_H = (\tau\tau_0, \sigma\tau_0)_H$ where τ_0 is the unique element of G/H such that -1 is an element of C_{τ_0}.

We conclude this section with a general result which will prove useful later.

LEMMA 4. *Let K be a group, let $\sqsubset_1, \sqsubset_2, \ldots, \sqsubset_h$ be the conjugacy classes of K and let $\chi_1, \chi_2, \ldots, \chi_h$ be the irreducible characters of K. Write $\chi_j(\sqsubset_i)$ for the value of χ_j on any element of $\sqsubset_i$ and write f_i for the value of X_i on the identity element of K. Let $\omega_{ij} = |\sqsubset_i|\chi_j(\sqsubset_i)/f_j$. Let c_{ijk} be the number of pairs (x_i, x_j) in $\sqsubset_i \times \sqsubset_j$ which are solutions to $x_i x_j = c_k$ for some fixed element c_k of $\sqsubset_K$. Let W be the matrix (ω_{ij}), V_i be the matrix (c_{ijk}), and write E_i for the diagonal matrix whose (j, j)th entry is ω_{ij}. Then $W^{-1}V_iW = E_i$ for $i = 1, 2, \ldots, h$.*

Proof. This result is well known and follows, for example from Section 33 of [2].

COROLLARY. *In the notation of Section 3 above, let $C_1, C_2, \ldots, C_s$ be an enumeration of the G-orbits of A. Let X be the matrix $(\chi_{C_i}(C_j))$, let U_i be the matrix $(c(C_i, C_j, C_k))$ and D_i be the diagonal matrix whose (j, j)th entry is $\chi_{C_i}(C_j)$. Then*

$$X^{-1}U_iX = D_i \quad \text{for } i = 1, 2, \ldots, s.$$

Proof. Let $\sqsubset_1, \ldots, \sqsubset_h$ be an enumeration of the conjugacy classes of $\mathscr{G}$ such that $\sqsubset_i = C_i$, $i = 1, 2, \ldots, s$. Then V_i has the form

$$\begin{pmatrix} U_i & 0 \\ 0 & * \end{pmatrix}.$$

In addition $\omega_{ij} = |C_i|\chi_{C_j}(C_i)/f_j = |C_i|\chi_{C_j}(C_i)/|C_j| = \chi_{Ci}(C_j)$ for $i, j = 1, 2, \ldots, s$ by Lemma 2. The lemma now follows.

5. Fourier transforms

In this section analogues to the classical Gauss and Jacobi sums (see [3] for definitions) will be developed for P.I.R.'s by means of Fourier transforms on finite groups (see [10] for a discussion of Gauss sums over finite rings). As in Section 4, we let R be a finite commutative P.I.R. and denote by $[\ ,\ ]$ some pairing of $R^+ \times R^+$ into $\mathbf{C}^\times$ constructed as in Lemma 3.

Identifying R^+ with its complex dual by means of $[\ ,\ ]$ we may define the Fourier transform $\hat{f}$ of a complex function f on R by

$$\hat{f}(a) = \sum_{b \text{ in } R} f(b)[b, a] \quad \text{for all } a \text{ in } A.$$

A knowledge of the elementary properties of the Fourier transform will be assumed in what follows. (See [19] for example.)

DEFINITION 7. Let π be a character on $R^{\times}$. Then π is said to be *primitive* if there is no nontrivial ideal I of R for which $(1 + I) \cap R^{\times} \subseteq \ker \pi$.

It may be remarked that primitive π exist and that their existence may be shown by an argument similar to that of Lemma 3, part 2.

Given any character of $R^{\times}$ we will view it as a complex function on A by defining it to be zero on nonunits.

LEMMA 5. *Let π be a primitive character on G. Then $\hat{\pi} = \pi^{-1}\hat{\pi}(1)$.*

Proof. First, let a be a unit of R. Then

$$\begin{aligned}\hat{\pi}(a) &= \sum_{b \text{ in } R} \pi(b)[b, a] = \sum_{b \text{ in } R^{\times}} \pi(b)[b, a] \\ &= \pi^{-1}(a) \sum_{b \text{ in } R^{\times}} \pi(ba)[ba, 1] = \pi^{-1}(a)\hat{\pi}(1).\end{aligned}$$

Now assume a is a nonunit, let I be the annihilator of a in R and let $H = (1 + I) \cap R^{\times}$. Then H is not trivial by the Chinese Remainder Theorem and

$$\begin{aligned}\hat{\pi}(a) &= \sum_{\substack{b_1 \text{ in } H, \\ b_2 \text{ in } R^{\times}/H}} \pi(b_1 b_2)[1, b_2 a] \\ &= \sum_{b_2 \text{ in } R^{\times}/H} \pi(b_2)[1, b_2 a] \sum_{b_1 \text{ in } H} \pi(b_1) \\ &= 0\end{aligned}$$

since π is primitive. Thus again we have $\hat{\pi} = \pi^{-1}\hat{\pi}(1)$.

DEFINITION 8. By analogy to the classical gamma function (see footnote on p. 144 of [8]) we define the function Γ on the primitive characters of $R^{\times}$ by $\Gamma(\pi) = \hat{\pi}(1)$.

We note that by Lemma 8, $\hat{\pi} = \pi^{-1}\Gamma(\pi)$.

LEMMA 6. $\Gamma(\pi)\Gamma(\pi^{-1}) = |R|\pi(-1)$.

Proof. $\pi = \pi^{-1}\Gamma(\pi)$. Hence by Fourier inversion

$$|R|\pi(-1)\pi = \hat{\pi}^{\wedge} = \pi\Gamma(\pi)\Gamma(\pi^{-1}).$$

The result now follows.

We recall that if the convolution of two complex functions f and g on R is defined by $f * g(a) = \sum_{b \text{ in } R} f(b)g(a - b)$ then $(f * g)^{\wedge} = \hat{f} \circ \hat{g}$.

LEMMA 7. *Let $\pi_1, \pi_2, \pi_1, \pi_2$ be primitive characters on $R^{\times}$. Then*

$$\pi_1 * \pi_2 = (\pi_1 * \pi_2(1))\pi_1\pi_2.$$

Proof. As in the proof of Lemma 5, we first let a be a unit of R. Then

$$\begin{aligned}\pi_1 * \pi_2(a) &= \pi_1\pi_2(a) \sum_{b \text{ in } R} \pi_1(ba^{-1})\pi_2(1 - ba^{-1}) \\ &= \pi_1\pi_2(a)\pi_1 * \pi_2(1).\end{aligned}$$

Now take a a nonunit and define H as in Lemma 8. Then

$$\begin{aligned}\pi_1 * \pi_2(a) &= \sum_{b \text{ in } R^\times} \pi_1(b)\pi_2(b(ab^{-1} - 1)) \\ &= \sum_{b \text{ in } R^\times} \pi_1\pi_2(b)\pi_2(ab^{-1} - 1) \\ &= \sum_{b_2 \text{ in } R^\times/H} \pi_1\pi_2(b_2)\pi_2(ab_2^{-1} - 1) \sum_{b_1 \text{ in } H} \pi_1\pi_2(b_1) \\ &= 0.\end{aligned}$$

DEFINITION 9. By analogy to the classical beta function, we define the complex function β on pairs of primitive characters by $\beta(\pi_1, \pi_2) = \pi_1 * \pi_2(1)$.

LEMMA 8. *Let $\pi_1, \pi_2, \pi_1\pi_2$ be primitive. Then*

$$\beta(\pi_1, \pi_2) = \frac{\Gamma(\pi_1)\Gamma(\pi_2)}{\Gamma(\pi_1\pi_2)}$$

Proof.

$$\begin{aligned}\Gamma(\pi_1)\Gamma(\pi_2)\pi_1^{-1}\pi_2^{-1} &= \hat{\pi}_1\hat{\pi}_2 = (\pi_1 * \pi_2)^\wedge = (\pi_1\pi_2)^\wedge\beta(\pi_1, \pi_2) \\ &= \Gamma(\pi_1\pi_2)(\pi_1\pi_2)^{-1}\beta(\pi_1, \pi_2)\end{aligned}$$

COROLLARY. $|\beta(\pi_1, \pi_2)|^2 = |R|$.

Now let us consider a subgroup H of $R^\times$. If there exists a nontrivial ideal I of R for which $(1 + I) \cap R^\times$ is a subset of H, then the cyclotomy of R with respect to H may be determined by considering the ring R/I as is easily seen. Thus we may assume that H contains no such subset and we shall call such subgroups primitive. Let $H^\perp$ be the subgroup of characters on $R^\times$ which are trivial on H. Then it is clear that there are primitive characters of G contained in $H^\perp$.

PROPOSITION 3. *Let $\pi_1, \pi_2, \pi_1\pi_2$ be primitive characters of $R^\times$ contained in $H^\perp$. Then*

$$\beta(\pi_1, \pi_2) = \sum_{\sigma, \tau \text{ in } R^\times/H} \pi_1(\sigma)\pi_2(\tau)(\sigma, \tau)_H.$$

Proof. We have that

$$\Gamma(\pi_1)\Gamma(\pi_2) = \sum_{\sigma, \tau \text{ in } R^\times/H} \pi_1(\sigma)\pi_2(\tau)\eta_\sigma\eta_\tau$$

since π_1, π_2 are in $H^{\perp}$. Now

$$\begin{aligned}\eta_\sigma\eta_\tau &= \chi_\sigma(C_1)\chi_\tau(C_1)\\ &= \sum_{\mu \text{ in } R^\times/H} (\sigma\mu^{-1}, \tau\mu^{-1})_H\chi_\mu(C_1) + \sum_{\chi} (\chi, \chi_\sigma\chi_\tau)_{\mathscr{H}}\chi(C_1)\\ &= \sum_{\mu \text{ in } R^\times/H} (\sigma\mu^{-1}, \tau\mu^{-1})_H\eta_\mu + S\end{aligned}$$

where χ in the sum S runs through all irreducible characters of $\mathscr{H}$ except for the characters χ_μ with μ in $R^\times/H$. Furthermore

$$\begin{aligned}S &= \sum_C \frac{|H|}{|C|} \hat{c}(C_\sigma, C_\tau, C)\chi_C(C_1)\\ &= \sum_C c(C_\sigma, C_\tau, C)\chi_C(C_1)\end{aligned}$$

where C runs through all H orbits of R^+ consisting of nonunits. Therefore

$$\begin{aligned}\Gamma(\pi_1)\Gamma(\pi_2) = &\sum_{\sigma,\tau \text{ in } R^\times/H} \pi_1(\sigma)\pi_2(\tau)(\sigma\mu^{-1}, \tau\mu^{-1})_H\eta_\mu\\ &+ \sum_{\sigma,\tau \text{ in } R^\times/H} \pi_1(\sigma)\pi_2(\tau)c(C_\sigma, C_\tau, C)\chi_C(C_1).\end{aligned}$$

Let $\nu = \sigma^{-1}\tau$ in the second sum so that that sum becomes

$$\sum_{\sigma,\nu \text{ in } R^\times/H} \pi_1\pi_2(\sigma)\pi_2(\nu)c(C_\sigma, C_{\sigma\nu}, C)\chi_C(C_1).$$

Fix C to be an H-orbit in R^+ composed of nonunits of R and fix a in C. For each H-orbit C_ρ of R^+, fix some element x_ρ in C_ρ. Then $c(C_\sigma, C_{\sigma\nu}, C)$ is the number of pairs (h_1, h_2) in $H \times H$ which are solutions to

$$h_1x_\sigma + h_2x_{\sigma\nu} = a.$$

This equation has the same number of solutions as $h_3 + h_4x_\nu = ax_{\sigma^{-1}}$. Let I be the annihilator of a. Then the image of $(1 + I) \cap R^\times$ under the natural map of $R^\times$ onto $R^\times/H$ is a nontrivial subgroup of $R^\times/H$ and we have shown that $c(C_\sigma, C_{\sigma\nu}C)$ viewed as a function of σ is constant on cosets of this subgroup. Thus since $\pi_1\pi_2$ is primitive, the second sum above is 0. Therefore,

$$\begin{aligned}\Gamma(\pi_1)\Gamma(\pi_2) &= \sum_{\sigma,\tau,\mu \text{ in } G/H} \pi_1(\sigma)\pi_2(\tau)(\sigma\mu^{-1}, \tau\mu^{-1})_H\eta_\mu\\ &= \sum_{\sigma,\tau} \pi_1(\sigma)\pi_2(\tau)(\sigma, \tau)_H \sum_{\mu} \pi_1\pi_2(\mu)\eta_\mu\\ &= \sum_{\sigma,\tau} \pi_1(\sigma)\pi_2(\tau)(\sigma, \tau)_H\Gamma(\pi_1\pi_2).\end{aligned}$$

Thus $\beta(\pi_1\pi_2) = \sum_{\sigma,\tau} \pi_1(\sigma)\pi_2(t)(\sigma,\tau)_H$.

6. Computations and examples

Let R_i, $i = 1, 2$ be finite commutative P.I.R.'s and let $R = R_1 \oplus R_2$. Then if $\mathscr{G}_i$, $i = 1, 2$ and $\mathscr{G}$ are the cyclotomic groups of R_i, $i = 1, 2$ and R, we see that $\mathscr{G}$ is canonically isomorphic to $\mathscr{G}_1 \times \mathscr{G}_2$. We use this isomorphism to identify $\mathscr{G}_i$, $i = 1, 2$ with subgroups of $\mathscr{G}$ and this identification identifies R_i^+, $i = 1, 2$ and $R_i^\times$, $i = 1, 2$ with subgroups of R^+ and $R^\times$ respectively in the usual way. If H_i is a subgroup of $R_i^\times$, $i = 1, 2$ and $H = H_1H_2$ is viewed as a subgroup of $R^\times$ then $R^\times/H$ is canonically isomorphic to $R_1^\times/H_1 \times R_2^\times/H_2$ and again we use this isomorphism to identify $R_i^\times/H_i$, $i = 1, 2$ with subgroups of $R^\times/H$.

LEMMA 9. *With notation as above let σ be an element of $R^\times/H$ and write $\sigma = \sigma_1\sigma_2$ with σ_i in $R_i^\times/H_i$, $i = 1, 2$. Let $\mathscr{H}$ be the subgroup $R^\times H$ of $\mathscr{G}$. Then if the characters χ_{σ_i} of H_i, $i = 1, 2$ are viewed as characters on $\mathscr{H}$, $\chi_\sigma = \chi_{\sigma_1}\chi_{\sigma_2}$.*

Proof. This lemma follows from the fact that induction of characters commutes with direct products [2, 43.2].

COROLLARY. *Let σ, τ be elements of $R^\times/H$ and write $\sigma = \sigma_1\sigma_2$, $\tau = \tau_1\tau_2$; σ_i, τ_i in $R_i^\times/H_i$, $i = 1, 2$. Then $(\sigma, \tau)_H = (\sigma_1, \tau_1)_{H_1}(\sigma_2, \tau_2)_{H_2}$.*

We now fix R to be an arbitrary finite commutative P.I.R., let H be a subgroup of $R^\times$ and let K be a subgroup of H. Pick coset representatives $\sigma_1, \sigma_2, \ldots, \sigma_s$ of H in $R^\times$ and $\tau_1, \tau_2, \ldots, \tau_t$ of K in H. Then as is well known the elements $\sigma_i\tau_j$ form a complete set of coset representatives of K in $R^\times$.

LEMMA 10. $(\sigma_i, \sigma_j)_H = \sum_{l=1}^t \sum_{k=1}^t (\sigma_i\tau_k, \sigma_j\tau_l)_K$.

Proof. Since for $i, j = 1, 2, \ldots, s$, the cosets $H\sigma_i$, $H\sigma_j$ are respectively the disjoint unions of the cosets $K\sigma_i\tau_k$, $k = 1, \ldots, t$ and $K\sigma_j\tau_l$, $l = 1, \ldots, t$, the result follows from Definition 6.

Now write R as a product of primary rings R_i, $i = 1, 2, \ldots, s$ and let H_i be the image in $R_i^\times$ of H under the natural map. Then letting $K = \prod_{i=1}^s H_i$ viewed as a subgroup of $R^\times$, it follows from Lemmas 9 and 10 that to determine the cyclotomic constants of R with respect to H it is sufficient to know the cyclotomic constants of R_i with respect to H_i for $i = 1, 2, \ldots, s$.

6.1. Primary rings

Let $q = p^n$ where p is an odd prime and let $\mathbf{F}_q$ be the finite field of q elements. Let Tr be the trace mapping from $\mathbf{F}_q$ to $\mathbf{F}_p$. Then we may define a nondegenerate symmetric balanced map $[\ \ ,\ \ ]_q$ from $\mathbf{F}_q \times \mathbf{F}_q$ to $\mathbf{C}^\times$ by

$$[a, b]_q = \exp\left(\frac{2\pi i \operatorname{Tr}(ab)}{p}\right).$$

For the remainder of this paper it will be implicit that $[\ ,\ ]_q$ is to be used whenever the cyclotomy of $\mathbf{F}_q$ or of some ring of which $\mathbf{F}_q$ is a direct summand is discussed. We note that $\mathbf{F}_q^\times$ is cyclic of order $q - 1$ so that we may pick a generator g of $\mathbf{F}_q^\times$.

If H is any subgroup of $\mathbf{F}_q^\times$ then there is a divisor e of $q - 1$ such that H consists precisely of the elements $1, g^e, g^{2e}, \ldots, g^{(f-1)e}$ where $f = (q - 1)/e$. Thus we may pick the elements $1, g, \ldots, g^{e-1}$ as coset representatives of H in $\mathbf{F}_q^\times$. If we now define $(i, j)_e$, η_i, and C_i by $(i, j)_e = (g^i, g^j)_H$, $\eta_i = \eta_{g^i}$, $C_i = C_{g^i}$ then it may be seen [9] that $(i, j)_e$, η_i, C_i are just the e-cyclotomic numbers, periods, and classes as they are usually defined. Furthermore, the Γ and β functions defined in Section 5 correspond exactly to the classical Gauss and Jacobi sums and the results of Section 5 provide an exposition of the properties of these sums. The techniques of Section 5 may also be applied to provide a proof of a result due to Jacobi which appears to be considerably simpler than the proof usually given.

LEMMA 11. *Let $p \neq 2$, let π_0 be the character of $\mathbf{F}_q^\times$ defined by $\pi_0(g) = -1$ and let π be any character of $\mathbf{F}_q^\times$ except for π_0 and the identity character. Then*

$$\Gamma(\pi_0)\Gamma(\pi^2) = \pi(4)\Gamma(\pi)\Gamma(\pi\pi_0).$$

Proof. By definition

$$\beta(\pi, \pi_0) = \sum_{x \text{ in } \mathbf{F}_q} \pi_0(x)\pi(1 - x).$$

Since

$$\sum_{x \text{ in } \mathbf{F}_q} \pi(1 - x) = 0,$$

we see that

$$\beta(\pi, \pi_0) = \sum_{x \text{ in } \mathbf{F}_q} \pi(1 - x^2).$$

Let $y = \frac{1}{2}(1 + x)$. Then

$$\begin{aligned}\beta(\pi, \pi_0) &= \sum_{y \text{ in } \mathbf{F}_q} \pi(2y(2 - 2y)) \\ &= \pi(4) \sum_{y \text{ in } \mathbf{F}_q} \pi(y)\pi(1 - y) = \pi(4)\beta(\pi, \pi).\end{aligned}$$

Therefore, by Lemma 8,

$$\frac{\Gamma(\pi)\Gamma(\pi_0)}{\Gamma(\pi\pi_0)} = \pi(4)\frac{\Gamma(\pi)\Gamma(\pi)}{\Gamma(\pi^2)} \quad \text{or} \quad \Gamma(\pi_0)\Gamma(\pi^2) = \pi(4)\Gamma(\pi)\Gamma(\pi\pi_0).$$

We note that this proof is a step by step imitation of the proof of an analogous result for the Γ-function of a locally compact field as given in [8, p. 155].

The corollary to Lemma 4 may be applied to yield a form for the cyclotomic "period equation."

LEMMA 12. *The polynomial $\prod_{i=0}^{e-1}(x - \eta_i)$ is the characteristic polynomial of the matrix $A = (a_{ij})$ where $a_{ij} = (i,j)_e - f\delta_{i_0,j}$, $i,j = 0, 1, \ldots, e-1$. Here, $i_0 = 0$ if e is odd, $i_0 = e/2$ if e is even, and $\delta_{i,j}$ is the Kronecker delta.*

Proof. Since $-1 = g^{(q-1)/2}$, it is clear that $c(C_0, C_i, \{0\}) = f\delta_{i,i_0}$ and that $c(C_0, \{0\}, C_j) = \delta_{0,j}$. Let B be the $(e+1) \times (e+1)$ matrix where $b_{ij} = (i,j)_e$, $i,j = 0, 1, \ldots, e-1$; $b_{ie} = f\delta_{i,i_0}$, $i = 0, 1, \ldots, e$; $b_{e,j} = \delta_{0,j}$, $j = 0, \ldots, e$. Then by Lemma 4, B has eigenvalues $\eta_0, \eta_1, \ldots, \eta_{e-1}, f$.

Now let I_t be the $t \times t$ identity matrix, let x be an unknown, let R be the $1 \times e$ matrix all of whose entries are $f - x$, and let S be the $e \times 1$ matrix whose ith row is $f\delta_{i,i_0}$. Then since

$$c(C_0, \{0\}, C_j) + \sum_{i=0}^{e-1} c(C_0, C_i, C_j) = f \quad \text{for } j = 0, 1, \ldots, e-1,$$

we have

$$|B - xI_{e+1}| = \begin{vmatrix} ((i,j) - xI_e) & S \\ R & f - x \end{vmatrix} = \begin{vmatrix} (A - xI_e) & S \\ 0 & f - x \end{vmatrix}$$
$$= (f - x)|A - xI_e|$$

so that A has precisely $\eta_0, \eta_1, \ldots, \eta_{e-1}$ for its characteristic roots.

We note that Lemma 4 states that the $e \times e$ matrices $B_k = (b_{ij}^{(k)})$ with $b_{ij}^{(k)} = (i-k, j-k)_e$, $i,j = 0, 1, \ldots, e-1$; $b_{ie} = f\delta_{i,k+i_0}$, $i = 0, 1, \ldots, e$; $b_{ej} = \delta_{k,j}$, $j = 0, 1, \ldots, e$ may be simultaneously diagonalized for $k = 0, 1, \ldots, e-1$. By taking products of matrices $B_k B_l$, diagonalizing, and taking traces on both sides, one obtains quadratic equations in the cyclotomic constants which provide an alternate means of deriving explicit formulae for these constants at least for $e = 3, 4$. Since it is known [18] that such quadratic equations cannot suffice to determine the constants $(i,j)_7$ for example, it may be conjectured that the cubic relations determined by diagonalizing products of the form $B_k B_l B_m$ may provide the missing data.

Next, let R be a primary finite commutative P.I.R. and let P be its prime ideal. Then R/P is a finite field and hence the cyclotomy of R with respect to a given subgroup H may be determined as in the discussion above if H contains $1 + P$ as a subgroup. On the other extreme, if H is primitive, it appears to be a difficult matter to obtain any explicit formulae.

Even the simplest case, $R = Z/p^2Z$, $H = G^p$ involves solving the congruence $x^p + 1 \equiv y^p \pmod{p^2}$ which plays an important role in the history of Fermat's theorem[2] [13].

6.2. Galois Domains

In [15], the phrase Galois Domain is used to describe those finite commutative P.I.R.'s all of whose primary summands are fields. In this and later papers

[2] The author wishes to thank Morris Newman for his correspondence on this matter.

[16], [17], the cyclotomy of a Galois Domain is determined with respect to a cyclic subgroup of the units whose generator is a product of generators of the groups of units of the primary summands. The major result in these papers is seen to follow immediately from Lemmas 9 and 10.

PROPOSITION 4 (Storer). *Let $R_i = \mathbf{F}_{q_i}$, $i = 1, 2, \ldots, n$ where the numbers q_i are powers of distinct primes and are of the form $q_i = ef_i + 1$ for fixed e with the numbers f_i relatively prime in pairs. Let g_i generate the group of units of R_i. Let $R = R_1 \oplus R_2 \oplus \cdots \oplus R_n$ and let $g = \prod g_i$ in $R^\times$. Let $H = (g)$. Then:*

(1) *The elements $\prod_{i=2}^n g_i^{s_i}$, $s_i = 0, 1, \ldots, e-1$ form a complete set of representatives of the cosets of H in $R^\times$.*

(2) *If given $(n-1)$-tuples (s), (t) we write $((s), (t))$ for*

$$\left(\prod_{i=2}^n g_i^{s_i}, \prod_{i=2}^n g_i^{t_i}\right)_H$$

then

$$((s), (t)) = \sum_{k=0}^{e-1} \sum_{j=0}^{e-1} (j, k)_e^{(1)} \prod_{i=2}^n (s_i + j, t_i + k)_e^{(i)}$$

where $(\ , \ )_e^{(i)}$ is an e-cyclotomic number for R_i.

Proof. The proof of (1) consists of a straightforward calculation as does verification of the fact that the elements $g^j, j = 0, 1, \ldots, e-1$ form a complete set of representatives for the cosets of G^e in H. Since G^e is precisely the subgroup $\prod H_i$ described in the discussion following Lemma 13, the result now follows from Lemmas 9 and 10.

6.3. Kloosterman and hyper-Kloosterman sums

Let q be a prime power and let $R = \mathbf{F}_q \oplus \mathbf{F}_q$. We write elements of R as pairs of elements in $\mathbf{F}_q$. Let H be the subgroup of $R^\times$ consisting of pairs (a, b) with $ab = 1$. Then the elements $(1, u)$ u in $\mathbf{F}_q^\times$ form a complete set of representatives of H in $R^\times$ and we write $\langle u, v\rangle$ for $((1, u), (1, v))_{\mathscr{H}}$.

DEFINITION 10. For u in $\mathbf{F}_q^\times$, let $K(u)$ be the *Kloosterman sum*

$$\sum_{x \text{ in } \mathbf{F}_q{}^\times} \exp\left(\frac{2\pi i \operatorname{Tr}(x + u/x)}{p}\right).$$

PROPOSITION 5. (1) $\langle u, v\rangle = 1 + \pi_0((u-v)^2 - 2(u+v) + 1)$ where π_0 *is defined as in Lemma* 11 *and is extended to* $\mathbf{F}_q$ *by letting* $\pi_0(0) = 0$.

(2) $\eta_{(1,u)} = K(u)$.

Proof. $\langle u, v\rangle$ is equal to the number of solutions to $(x, x^{-1}) + (y, uy^{-1}) = (1, v)$ for x, y in $\mathbf{F}_q^\times$. Thus we have $x + y = 1$ and $x^{-1} + uy^{-1} = v$ so that $\langle u, v\rangle$ is seen to be the number of solutions to

$$vx^2 + (u - v - 1)x + 1 = 0;$$

that is $\langle u, v\rangle = 2, 1, 0$ according to whether $(u - v - 1)^2 - 4v = (u - v)^2 - 2(u + v) + 1$ is a square, is equal to 0, or is a nonsquare.

Let $\psi_{(1,1)}$ be the character on R^+ identified with (1, 1) (see Section 3). Then

$$\begin{aligned}\eta_{(1,u)} &= \psi^{\mathscr{H}}_{(1,1)}(1, u) = \sum_{x \text{ in } \mathbf{F}_q^\times} \psi^{(x, x^{-1})}_{(1,1)}(1, u)\\ &= \sum_{x \text{ in } \mathbf{F}_q^\times} \exp\left(\frac{2\pi i \operatorname{Tr}(x + ux^{-1})}{p}\right)\\ &= K(u).\end{aligned}$$

Proposition 5 may be used to give character-theoretical proofs for the "cyclotomic" properties of Kloosterman sums described in [11]. As an example we prove:

Proposition 6 (*Lehmer*).

(1) $\sum_{u \text{ in } \mathbf{F}_q^\times} K(u)K(cu) = q^2\delta_{1,c} - q - 1.$

(2) $\sum_{u \text{ in } \mathbf{F}_q^\times} K(u)K(cu)K(du) = q^2\langle c, d\rangle - q^2 + 2q + 1.$

(3) $\sum_{u \text{ in } \mathbf{F}_q^\times} K^2(u)K^2(cu) = q^3(1 + \delta_{1,c}) - q^2(2 + \pi_0(c)) - 3q - 1.$

Proof. (1) Let $C_{(1,0)}$ (respectively $C_{(0,1)}$ be the H-orbit of R^+ consisting of the elements $(u, 0)$ (respectively $(0, u)$) with u in $\mathbf{F}_q^\times$. Then since $\chi_{(1,u)}$ is real,

$$\begin{aligned}\delta_{1,c} &= (\chi_{(1,1)}, \chi_{(1,c)})_{\mathscr{H}}\\ &= \frac{1}{|\mathscr{H}|}\Bigg[\sum_{u \text{ in } \mathbf{F}_q^\times} |C_{(1,u)}|\eta_{(1,u)}\eta_{(1,cu)} + |C_{(1,0)}|(\chi_{(1,1)}(1, 0))(\chi_{(1,c)}(1, 0))\\ &\qquad + |C_{(0,1)}|(\chi_{(1,1)}(0, 1))(\chi_{(1,c)}(0, 1)) + (\chi_{(1,1)}(0, 0))(\chi_{(1,c)}(0, 0))\Bigg].\end{aligned}$$

Now $\chi_{(1,u)}((1, 0)) = \chi_{(1,u)}((0, 1)) = -1$ for u in $\mathbf{F}_q^\times$ as is easily seen. Thus

$$q^2(q - 1)\delta_{1,c} = (q - 1) \sum_{u \text{ in } \mathbf{F}_q^\times} K(u)K(cu) + 2(q - 1) + (q - 1)^2$$

so that

$$\sum_{u \text{ in } \mathbf{F}_q^\times} K(u)K(cu) = q^2\delta_{1,c} - q - 1.$$

(2)
$$\begin{aligned}\langle c, d\rangle &= (\chi_{(1,d)}, \chi_{(1,1)}\chi_{(1,c)})\\ &= \frac{1}{q^2(q - 1)}\Bigg[(q - 1) \sum_{u \text{ in } \mathbf{F}_q^\times} K(u)K(cu)K(du)\\ &\qquad - 2(q - 1) + (q - 1)^3\Bigg]\end{aligned}$$

so

$$\sum_{u \text{ in } \mathbf{F}_q^\times} K(u)K(cu)K(du) = q^2\langle c, d\rangle - q^2 + 2q + 1.$$

(3) Using the results of Sections 3–4 it is seen that

$$\chi^2_{(1,c)} = \sum_{u \text{ in } \mathbf{F}_q^\times} \langle 1, uc^{-1}\rangle \chi_{(1,u)} + \psi^{\mathscr{H}}_{(0,0)}$$

where $\psi_{(0,0)}$ is the identity character on R^+. Therefore

$$\begin{aligned}(\chi_{(1,1)}, \chi_{(1,1)}\chi^2_{(1,c)})_{\mathscr{H}} &= \sum_{u \text{ in } \mathbf{F}_q^\times} \langle 1, uc^{-1}\rangle (\chi_{(1,1)}, \chi_{(1,1)}\chi_{(1,u)}) \\ &\quad + (q-1)(\chi_{(1,1)}, \chi_{(1,1)})_{\mathscr{H}} \\ &= \sum_{u \text{ in } \mathbf{F}_q^\times} \langle 1, uc^{-1}\rangle\langle 1, u\rangle + q - 1.\end{aligned}$$

Now $\langle 1, uc^{-1}\rangle = 1 + \pi_0(u(u - uc))$ so

$$\begin{aligned}\sum_{u \text{ in } \mathbf{F}_q^\times} \langle 1, uc^{-1}\rangle\langle 1, u\rangle &= p - 1 + \sum_{u \text{ in } \mathbf{F}_q^\times} \pi_0(u(u-4c)) + \sum_{u \text{ in } \mathbf{F}_q^\times} \pi_0(u(u-4)) \\ &\quad + \sum_{u \text{ in } \mathbf{F}_q^\times} \pi_0((u-4)(u-4c)) \\ &= q - 1 - 1 - 1 + q\delta_{1,c} - 1 - \pi_0(c)\end{aligned}$$

(see [15, p. 58] for such computations.)

Thus we have

$$\begin{aligned}(2 + \delta_{1,c})q - 5 - \pi_0(c) &= (\chi_{(1,1)}, \chi_{(1,1)}\chi^2_{(1,c)})_{\mathscr{H}} \\ &= \frac{1}{q^2(q-1)}\Bigg[(q-1)\sum_{u \text{ in } \mathbf{F}_q^\times} K^2(u)K^2(cu) \\ &\qquad + 2(q-1) + (q-1)^4\Bigg]\end{aligned}$$

or

$$\sum_{u \text{ in } \mathbf{F}_q^\times} K^2(u)K^2(cu) = q^3(1 + \delta_{1,c}) - q^2(2 + \pi_0(c) - 3q - 1).$$

In addition we obtain the following formula which may be of interest.

LEMMA 13.

$$\sum_{s,t=0}^{e-1} (s,t)_e(i-s, j-t)_e = \sum_{u,v=0}^{f-1} \langle g^{i+eu}, g^{j+ev}\rangle \quad \textit{for } i,j = 0, 1, \ldots, e-1.$$

for $i, j = 0, 1, \ldots, e - 1$.

Proof. Let G_e be the subgroup of $R^\times$ consisting of all pairs (a, b) such that ab is an eth power in $\mathbf{F}_q$. Then $(R^\times G_e) = e$ and we may take elements $(1, g^i)$, $i = 0, 1, \ldots, e - 1$ as representatives of G_e in $R^\times$. By Lemmas 9 and 10 we have

$$((1, g^i), (1, g^j))_{\mathscr{G}_e} = \sum_{s,t=0}^{e-1} (s,t)_e(i-s, j-t)_e.$$

On the other hand we also clearly have

$$((1, g^i), (1, g^j))_{\mathscr{G}_e} = \sum_{u, v=0}^{f-1} \langle g^{i+eu}, g^{j+ev} \rangle.$$

As in Section 6.1, Lemma 4 may be utilized to obtain a "period equation" for Kloosterman sums. As the matrix manipulations are similar to those in the proof of Lemma 12 we merely state the result.

LEMMA 14. *The equation* $(x + 1) \prod_{u=1}^{p-1} (x - K(u))$ *is the characteristic equation for the* $p \times p$ *matrix* $A = (a_{ij})$ *where* $a_{ij} = \langle i, j \rangle - (p - 1)\delta_{1,i}$ *for* $i, j = 1, 2, \ldots, p - 1$; *where* $a_{1p} = -p - 1$, $a_{ip} = 1$, $i = 2, 3, \ldots, p$ *and where* $a_{pj} = 2(1 - \delta_{1j})$, $j = 1, 2, \ldots, p - 1$.

We now comment briefly on hyper-Kloosterman sums.

DEFINITION 11. For u in $\mathbf{F}_q^\times$ let $K_n(u)$ be the n-dimensional hyper-Kloosterman sum

$$\sum \exp \left(\frac{2\pi i \operatorname{Tr} (\sum_{i=1}^n x_i + u \prod_{i=1}^n x_i^{-1})}{p} \right)$$

where the sum is over all points (x_i) with x_i in $\mathbf{F}_q^\times$, $i = 1, 2, \ldots, n$. We note that $K(u) = K_1(u)$.

If we define R_n to be the ring which is a direct sum of $n + 1$ copies of $\mathbf{F}_q$ and if we let H_n be the subgroup of $R_n^\times$ consisting of all $(n + 1)$-tuples (x) such that $\prod_{i=1}^{n+1} x_i = 1$ then exactly as in Proposition 5 we obtain:

PROPOSITION 7. $\eta_{(1, 1, \ldots, u)} = K_n(u)$.

We remark that an application of the general theory to the ring R_n will suffice to determine those properties of the hyper-Kloosterman sum that have been called "cyclotomic." For specific properties see [12].

REFERENCES

1. B. G. BASMAJI, *Monomial representations and metabelian groups*, Nagoya Math. J., vol. 35 (1969), pp. 99–107.
2. C. W. CURTIS AND I. REINER, *Representation theory of finite groups and associative algebras*, Interscience, New York, 1962.
3. L. E. DICKSON, *Cyclotomy, higher congruences, and Waring's problems*, Amer. J. Math., vol. 57 (1935), pp. 391–424.
4. ———, *Cyclotomy and trinomial congruences*, Trans. Amer. Math. Soc., vol. 37 (1935), pp. 363–380.
5. W. FEIT, *Characters of finite groups*, Benjamin, New York, 1967.
6. P. X. GALLAGHER, *Group characters and normal Hall subgroups*, Nagoya Math. J., vol. 21 (1962), pp. 223–230.
7. C. F. GAUSS, *Disquisitiones arithmeticae* (translated by A. S. Clarke), Yale Univ. Press, New Haven, 1966.
8. I. M. GEL'FAND, ET AL, *Representation theory and automorphic forms* (translated by K. A. Hirsch), Saunders, Philadelphia, 1969.

9. M. Hall, Jr., *Characters and Cyclotomy*, Proc. Sympos. Pure Math., vol. 8, Amer. Math. Soc., Providence, R.I., 1965, pp. 31–43.
10. E. Lamprecht, *Allgemeine Theorie der Gausschen Summen in endlichen kommutativen Ringen*, Math. Nachr., vol. 9 (1953), pp. 149–196.
11. D. H. and Emma Lehmer, *The cyclotomy of Kloosterman sums*, Acta Arithmetica, vol. 12 (1967), pp. 385–407.
12. ———, *The cyclotomy of hyper-Kloosterman sums*, Acta Arithmetica, vol. 14 (1968), pp. 89–111.
13. L. J. Mordell, *Three lectures on Fermat's last theorem*, Cambridge University Press, Cambridge, 1921.
14. J. P. Serre, *Représentations Linéaires des Groupes Finis*, Hermann, Paris, 1967.
15. T. Storer, *Cyclotomy and difference sets*, Markham, Chicago, 1967.
16. ———, *On the arithmetic structure of Galois Domains*, Acta Arithmetica, vol. 15 (1969), pp. 139–159.
17. ———, *Extensions of cyclotomic theory*, Proc. Sympos. Pure Math., Amer. Math. Soc., Providence, R.I., vol. 20 (1969), pp. 123–134.
18. A. L. Whiteman, *Theorems on quadratic partitions*, Proc. Nat. Acad. Sci., vol. 36 (1950), pp. 60–65.
19. ———, *Finite Fourier series and cyclotomy*, Proc. Nat. Acad. Sci., vol. 37 (1951), pp. 373–378.
20. O. Zariski and P. Samuel, *Commutative algebra*, Van Nostrand, Princeton, 1958.

Princeton University
Princeton, New Jersey