

On the algebraic structure of Gaussian periods

N.J. Wildberger

School of Mathematics
University of New South Wales
Kensington N.S.W. 2033
Australia.

§0. Introduction and Statement of the Main Result

Let p be a prime, \mathbb{Z}_p the field of residue classes mod p and U_p the (cyclic) group of automorphisms of the additive group \mathbb{Z}_p . We will identify U_p with the non-zero elements of \mathbb{Z}_p . For any positive integer n dividing $p - 1$ there is exactly one subgroup C of U_p of index n given by $C = \{x^n \mid x \in \mathbb{Z}_p, x \neq 0\}$; if $|C| = k$ then $p = kn + 1$. The orbits of C on \mathbb{Z}_p are $\{0\} = C_0$ together with the cosets of C in U_p . If y is a primitive root in U_p then we may order the cosets $C = C_1, C_2, \dots, C_n$ so that $yC_i = C_{i+1}$ for $i = 1, \dots, n - 1$ and $yC_n = C_1$. In terms of y ,

$$C_i = \{y^{n\ell+i-1} \mid \ell = 0, \dots, k - 1\} \quad \forall i = 1, \dots, n. \quad (0.1)$$

Let $\mathcal{C} = \{C_0, C_1, \dots, C_n\}$. For $C_i, C_j \in \mathcal{C}$ we may consider all possible sums $x_i + x_j$ with $x_i \in C_i$ and $x_j \in C_j$. Let N_{ij}^k denote the number of times a fixed $x_k \in C_k$ occurs in this list; this number is independent of the choice of x_k in C_k . The determination of the constants N_{ij}^k is one of the main problems in the theory of cyclotomy. In the literature one usually defines $(j, k)_n$ to be N_{1j+1}^{k+1} for $0 \leq j, k \leq n - 1$ and attempts to provide formulae for these ‘cyclotomic constants’ (the others are easily derivable from them) in terms of the solutions of certain Diophantine systems involving quadratic forms. Gauss himself studied and solved the cases $n = 2, 3$ and 4 . L.E. Dickson ([1]) studied the cases

$n = 5, 6, 8, 9, 10, 12, 14, 15, 16, 18$ and 20 with more complete and further work having been done by E. Lehmer [1] ($n = 8$), Whiteman [1], [2], ($n = 10, 12, 16$), Muskat ($n = 14, 24, 30$), Baument and Fredrickson ($n = 9, 18$), and Leonard and Williams [1], [2] ($n = 7, 11$). Further information and references may be found in Storer [1]. The connection with the theory of difference sets is discussed in Hall [1].

A related problem is the determination of the complex numbers $Q_j = \sum_{m \in C_j} e^{2\pi im/p}$ which are known as Gaussian periods. The Q_i are algebraic integers which satisfy the same multiplicative relations as the C_i . By determination one means finding the polynomial whose roots are the Q_i - the actual specification of which root corresponds to which Q_i is a more subtle problem analogous to the famous problem of the sign of the Gauss sum (see e.g. Myerson [1].)

Our aim in this paper is to study the algebraic structure of \mathcal{C} abstractly and prove a rigidity theorem which states roughly that the abstract algebra in the situation controls the number theory. To be more specific, we first write

$$C_i C_j = \sum_k N_{ij}^k C_k \tag{0.2}$$

where here and throughout this paper we adopt the convention that unspecified quantifiers or sums always range over the set $\{0, 1, \dots, n\}$. This gives $\mathbb{Z}\mathcal{C}$ the structure of an associative, abelian ring with identity C_0 . For $C_i \in \mathcal{C}$, let C_i^* denote the element of \mathcal{C} which consists of the additive inverses of the elements of C_i . Then clearly

$$C_i^* C_j^* = \sum_k N_{ij}^k C_k^* \tag{0.3}$$

and $N_{ij}^0 > 0$ if and only if $C_j = C_i^*$.

We abstract the above as follows. Let $\mathcal{C} = \{C_0, C_1, \dots, C_n\}$ be any set of $(n + 1)$ elements and suppose $\mathbb{Z}\mathcal{C}$ is given a ring structure with equations

$$C_i C_j = \sum_k N_{ij}^k C_k, \quad N_{ij}^k \in \mathbb{Z} \quad (0.4)$$

together with a distinguished map $*$: $\mathcal{C} \rightarrow \mathcal{C}$. We will say that \mathcal{C} is an **assembly** if the following axioms are satisfied.

A1. $\mathbb{Z}\mathcal{C}$ is associative, abelian and has identity C_0 .

A2. $N_{ij}^k \geq 0 \quad \forall i, j, k$

A3. $*$: $\mathcal{C} \rightarrow \mathcal{C}$ is an automorphism i.e. $C_i^* C_j^* = \sum_k N_{ij}^k C_k^* \quad \forall i, j$

A4. $N_{ij}^0 > 0$ if and only if $C_j = C_i^*$.

For $C_i \in \mathcal{C}$, define its **mass** $m(C_i)$ to be N_{ij}^0 where $C_j = C_i^*$. The final axiom we refer to as ‘**conservation of mass.**’

A5. $m(C_i)m(C_j) = \sum_k N_{ij}^k m(C_k) \quad \forall i, j$.

If $\mathcal{C} = \{C_0, C_1, \dots, C_n\}$ is any assembly then $C_0^* = C_0$ and $(C_i^*)^* = C_i \quad \forall i$. \mathcal{C} will be called **Hermitian** if $C_i^* = C_i \quad \forall i$. The number

$$m(\mathcal{C}) = \sum_{i=0}^n m(C_i) \quad (0.5)$$

will be called the **total mass** of \mathcal{C} . Define the **order** of an assembly $\mathcal{C} = \{C_0, C_1, \dots, C_n\}$ to be n . Two assemblies $\mathcal{C} = \{C_0, C_1, \dots, C_n\}$ and $\mathcal{D} = \{D_0, D_1, \dots, D_n\}$ are said to be **isomorphic** if there exists a bijection $\phi : \mathcal{C} \rightarrow \mathcal{D}$ whose linear extension to $\mathbb{Z}\mathcal{C}$ satisfies $\phi(C_i)\phi(C_j) = \phi(C_i C_j) \quad \forall i, j$ and $\phi(C_i^*) = \phi(C_i)^* \quad \forall i$.

It is straightforward to check that our original example forms an assembly of total mass p and order n which is Hermitian if and only if -1 is an n th residue mod p . A different choice of primitive root y leads to a reordering of the cosets C_i but an isomorphic assembly. If in the construction we (somewhat arbitrarily) let y be the least primitive root, then we refer to the assembly as $\mathcal{C}(p, n)$.

This assembly exhibits an important symmetry; cyclic permutation of the non-identity elements C_1, \dots, C_n preserves the structural equations. This is due to the fact that this permutation is implemented by multiplication by the primitive root y which is an automorphism of \mathbb{Z}_p .

Let σ be the permutation of $\{0, 1, \dots, n\}$ given by $\sigma(0) = 0$, $\sigma(j) = j+1$ for $j = 1, \dots, n-1$ and $\sigma(n) = 1$. Then an assembly $\mathcal{C} = \{C_0, C_1, \dots, C_n\}$ will be called **cyclotomic** if

$$N_{\sigma(i)\sigma(j)}^{\sigma(k)} = N_{ij}^k \quad \forall i, j, k. \quad (0.6)$$

The purpose of this paper is to prove the following result (which also justifies our terminology).

Main Theorem. *Let p be a prime and n a positive integer dividing $p - 1$. Then there is up to isomorphism exactly one cyclotomic assembly of total mass p and order n - namely $\mathcal{C}(p, n)$.*

This theorem shows that the problem of determining the algebraic structure of Gaussian periods can be viewed as a problem of abstract algebra. For $n = 2, 3$ and 4 this result has been established in Wildberger [2].

§1. Some harmonic analysis

Let $\mathcal{C} = \{C_0, C_1, \dots, C_n\}$ be an assembly of order n . We will need some harmonic analysis on \mathcal{C} . The facts that follow actually hold for all finite abelian hypergroups (see Wildberger [1].) Let $\mathbb{C}\mathcal{C}$ denote the complex vector space with basis \mathcal{C} ; it is an algebra. For $C_i \in \mathcal{C}$, let $\text{ad}C_i \in \text{End}(\mathbb{C}\mathcal{C})$ denote the operator of multiplication by C_i .

Lemma 1.1 *The set $\{\text{ad}C_i \mid i = 0, \dots, n\}$ is linearly independent in $\text{End}(\mathbb{C}\mathcal{C})$.*

Proof. If $\sum_i r_i \text{ad}C_i = 0$ for some constants $r_i \in \mathbb{C}$ then comparing the coefficients of C_0 on both sides of the equation $\sum_i r_i C_i C_j^* = 0$ gives $r_j = 0$. \square

For $a = \sum_i z_i C_i \in \mathbb{C}\mathcal{C}$, define

$$a^* = \sum_i \overline{z_i} C_i^*. \quad (1.1)$$

It follows from Axiom A3 that for all $a, b \in \mathbb{C}\mathcal{C}$, $(ab)^* = a^*b^*$.

Proposition 1.2 *The algebra $\mathbb{C}\mathcal{C}$ is semisimple.*

Proof. If $a \in \mathbb{C}\mathcal{C}$ is non-zero then Axiom A4 implies that the coefficient of C_0 in aa^* is non-zero, so that aa^* is non-zero. But then $(aa^*)(aa^*)^* = a^2(a^2)^*$ is also non-zero so that a^2 is non-zero. Therefore $\mathbb{C}\mathcal{C}$ has no nilpotent elements. \square

Let $A = \text{span}_{\mathbb{C}}\{\text{ad}C_i\}$. By the preceding Lemma and Proposition, the algebra A is isomorphic to $\mathbb{C}\mathcal{C}$, has dimension $n + 1$ and is semisimple. It is thus isomorphic to the algebra of diagonal matrices in $M(n+1, \mathbb{C})$. That means one can find a basis $\{e_0, e_1, \dots, e_n\}$ of $\mathbb{C}\mathcal{C}$ in which the operators $\text{ad}C_i$ are simultaneously diagonal, i.e.

$$C_i e_j = X_j(C_i) e_j \quad \forall i, j \quad (1.2)$$

for some functions $X_j : \mathcal{C} \rightarrow \mathbb{C}$. Furthermore the set of functions $\{X_0, X_1, \dots, X_n\}$ is linearly independent in the space $\mathcal{F}(\mathcal{C})$ of all complex valued functions on \mathcal{C} .

If the structure equations of \mathcal{C} are given by (0.4), define a **character** of \mathcal{C} to be a function $\chi \in \mathcal{F}(\mathcal{C})$ that satisfies

$$\chi(C_i)\chi(C_j) = \sum_k N_{ij}^k \chi(C_k) \quad \forall i, j. \quad (1.3)$$

If the linear extension of χ to $\mathbb{C}\mathcal{C}$ is also denoted by χ , then (1.3) has the equivalent formulation

$$\chi(C_i)\chi(C_j) = \chi(C_i C_j) \quad \forall i, j. \quad (1.4)$$

As an example, the map $C_i \rightarrow Q_i$ is a character of the assembly $\mathcal{C}(p, n)$.

Proposition 1.3 *The set of characters of \mathcal{C} is $\{X_0, X_1, \dots, X_n\}$.*

Proof. The fact that each X_j is a character is obvious from (1.2). Since $\mathbb{C}\mathcal{C}$ is abelian and semisimple, it is isomorphic to the algebra \mathbb{C}^{n+1} and hence has exactly $n + 1$ characters. \square

Axiom A5 implies that the function $C_i \rightarrow m(C_i)$ is a character of \mathcal{C} . We will henceforth label it as X_0 . The set of characters of \mathcal{C} will be denoted by $\hat{\mathcal{C}}$. The space $\mathbb{C}\hat{\mathcal{C}}$ is naturally identified with $\mathcal{F}(\mathcal{C})$.

The table of values $X_j(C_i)$ will be called the character table of \mathcal{C} . It has the form

	X_0	X_1	\cdots	X_n
C_0	1	1	\cdots	1
C_1	$m(C_1)$	$X_1(C_1)$	\cdots	$X_n(C_1)$
\vdots	\vdots	\vdots		\vdots
C_n	$m(C_n)$	$X_1(C_n)$	\cdots	$X_n(C_n)$

The character table allows us to give a concrete realization of \mathcal{C} -namely we may identify C_i with the corresponding row in the character table viewed as an element in the algebra \mathbb{C}^{n+1} .

For $f, g \in \mathcal{F}(\mathcal{C})$, define $\overline{f}(C_i) = \overline{f(C_i)}$ and $f^*(C_i) = f(C_i^*)$. Also introduce on $\mathcal{F}(\mathcal{C})$ the Hermitian inner product

$$\langle f, g \rangle = \frac{1}{m(\mathcal{C})} \sum_i \frac{f(C_i) \overline{g(C_i)}}{m(C_i)}. \quad (1.5)$$

Now $C_i e_j e_k = X_j(C_i) e_j e_k = X_k(C_i) e_j e_k \quad \forall i, j, k$. It follows from the independence of the functions X_j, X_k that if $j \neq k$ then $e_j e_k = 0$ and so we may normalize the e_j so that $e_j^2 = e_j$. Since both \mathcal{C} and $\{e_0, e_1, \dots, e_n\}$ are a basis of $\mathbb{C}\mathcal{C}$, we may then find constants $\alpha_j^k \in \mathbb{C}$ such that

$$e_j = \sum_k \alpha_j^k C_k \quad \forall j. \quad (1.6)$$

Multiplying this equation by C_i^* and comparing coefficients of C_0 , we get

$$X_j(C_i^*) \alpha_j^0 = \alpha_j^i m(C_i) \quad (1.7)$$

so that

$$e_j = \alpha_j^0 \sum_k \frac{X_j(C_k^*)}{m(C_k)} C_k. \quad (1.8)$$

Substituting (1.8) into $e_i e_j = \delta_{ij} e_i$ and again comparing coefficients of C_0 we obtain

$$\alpha_j^0 \sum_k \frac{X_i(C_k) X_j(C_k^*)}{m(C_k)} = \delta_{ij} \quad (1.9)$$

or

$$\alpha_j^0 m(\mathcal{C}) \langle X_i, \overline{X_j^*} \rangle = \delta_{ij} \quad (1.10)$$

When $i = j = 0$ we get $\alpha_0^0 = \frac{1}{m(\mathcal{C})}$ so that from (1.8),

$$e_0 = \frac{1}{m(\mathcal{C})} \sum_k C_k. \quad (1.11)$$

This element plays a special role in harmonic analysis on \mathcal{C} — it is the analog of Haar measure. Note that if $X_i \in \mathcal{C}^\wedge$, then $\overline{X_i}, X_i^* \in \mathcal{C}^\wedge$ as well, so that (1.10) allows us to conclude the following.

Proposition 1.4 $X_i^* = \overline{X_i} \quad \forall X_i \in \mathcal{C}^\wedge$ □

Proposition 1.5 $\{X_0, X_1, \dots, X_n\}$ is an orthogonal basis of $\mathcal{F}(\mathcal{C})$ with respect to the inner product $\langle \cdot, \cdot \rangle$ of (1.5). □

§2. Cyclic Symmetry

We now begin the proof of the Main Theorem. Consider a cyclotomic assembly $\mathcal{C} = \{C_0, C_1, \dots, C_n\}$ of order n with total mass $p = nk + 1$ for some prime p . Let $\mathcal{C}^\wedge = \{X_0, X_1, \dots, X_n\}$ and let the character table of \mathcal{C} be

$$\begin{array}{c|cccc}
 & X_0 & X_1 & \cdots & X_n \\
 \hline
 C_0 & 1 & 1 & \cdots & 1 \\
 C_1 & k & S_{11} & \cdots & S_{1n} \\
 \vdots & \vdots & \vdots & & \vdots \\
 C_n & k & S_{n1} & \cdots & S_{nn}
 \end{array} \quad (2.1)$$

for some complex numbers $S_{ij}, 1 \leq i, j \leq n$.

For $C_i \in \mathcal{C}$, set $\sigma(C_i) = C_{\sigma(i)}$ and for $X_j \in \mathcal{C}^\wedge$, set $\sigma(X_j)(C_i) = X_j(C_{\sigma^{-1}(i)})$. Then since \mathcal{C} is cyclic, $\sigma(X_j) \in \mathcal{C}^\wedge$ and so the map $X_j \rightarrow \sigma(X_j)$ generates an action of \mathbb{Z}_n on \mathcal{C}^\wedge .

Proposition 2.1 The action of \mathbb{Z}_n is transitive on $\{X_1, \dots, X_n\}$.

Proof. We will employ the orthogonality of the columns of (2.1) as given by Proposition 1.5. The sum of the columns of (2.1) corresponding to elements of a \mathbb{Z}_n orbit on $\{X_1, \dots, X_n\}$ must necessarily have the form $(\ell x \cdots x)^t$ for some positive integer ℓ and some $x \in \mathbb{C}$. This vector, when viewed as a function on \mathcal{C} , must be orthogonal to X_0 and this forces x to be $-\ell/n$, a negative real number. Two such sums corresponding to two distinct \mathbb{Z}_n orbits will both have this form so their inner product will be strictly positive, which is impossible. \square

Setting $S_{i1} = S_i$ for $i = 1, \dots, n$ it follows that the character table of \mathcal{C} has the form

$$\begin{array}{c|cccc}
 & X_0 & X_1 & \cdots & X_n \\
 \hline
 C_0 & 1 & 1 & \cdots & 1 \\
 C_1 & k & S_1 & \cdots & S_2 \\
 \vdots & \vdots & \vdots & \ddots & \vdots \\
 C_n & k & S_n & \cdots & S_1
 \end{array} \tag{2.2}$$

Corollary 2.2 $S_1 + \cdots + S_n = -1$.

Proof. This follows from the orthogonality of the first two columns of (2.2). \square

The action of \mathbb{Z}_n on \mathcal{C} generated by $C_i \rightarrow \sigma(C_i)$ extends to an action on $\mathbb{Z}\mathcal{C}$. Note that the subset of $\mathbb{Z}\mathcal{C}$ invariant under this action is the \mathbb{Z} submodule of $\mathbb{Z}\mathcal{C}$ spanned by C_0 and the element $C_1 + \cdots + C_n$. Let $\overline{C} = C_1 + \cdots + C_n$.

Now introduce the polynomial

$$f(t) = \prod_{i=1}^n (t - S_i). \tag{2.3}$$

Proposition 2.3 $f(t) \in \mathbb{Z}[t]$.

Proof. Let $\tau_\ell(x_1, \dots, x_n) = \sum_{i_1 < \dots < i_\ell} x_{i_1} \cdots x_{i_\ell}$ be the ℓ^{th} symmetric function of x_1, \dots, x_n . Then the element $\alpha = \tau_\ell(C_1, \dots, C_n) \in \mathbb{Z}\mathcal{C}$ is clearly \mathbb{Z}_n -invariant so there

are integers a and b such that $\alpha = aC_0 + b\overline{C}$. Applying the character X_1 to both sides gives us

$$\tau_\ell(S_1, \dots, S_n) = a + b(S_1 + \dots + S_n) = a - b \quad (2.4)$$

by Corollary 2.2. This is clearly an integer. \square

Corollary 2.4 S_i is an algebraic integer for all $i = 1, \dots, n$. \square

We remark that we could also prove this fact directly by constructing a monic polynomial satisfied by S_i from the structure equations of \mathcal{C} . Suppose for example that we wish to obtain an equation satisfied by S_1 . Use the equation for $S_1 S_n$ to express S_n as a rational function of S_1, \dots, S_{n-1} . Then use the equation for $S_1 S_{n-1}$ and the previous formula to express S_{n-1} , and then S_n , as a rational function of S_1, \dots, S_{n-2} . Continuing in this way one eventually obtains a rational (and thus polynomial) equation for S_1 . If one examines this procedure carefully one sees that this final polynomial is in fact monic. We leave the details to the reader.

Theorem 2.4 *The polynomial $f(t)$ is irreducible over \mathbb{Q} .*

Proof. Suppose not, so that $f(t) = f_1(t) \cdots f_r(t)$ with $f_j(t) \in \mathbb{Z}[t]$ non-constant and irreducible and $r \geq 2$. Let $\mathcal{S} = \{S_1, \dots, S_n\}$ and let \mathcal{S}_j denote the subset of \mathcal{S} such that $f_j(t) = \prod_{S_i \in \mathcal{S}_j} (t - S_i)$ for $j = 1, \dots, r$. Let $|\mathcal{S}_j| = \ell_j$.

Let $y_j = \sum_{S_i \in \mathcal{S}_j} S_i$; this is necessarily an integer and by Corollary 2.2,

$$y_1 + \dots + y_r = -1. \quad (2.5)$$

Since $r \geq 2$, at least one of the y_i must be non-negative; so suppose without loss of generality that $y_1 \geq 0$.

Now let

$$\alpha = \sum_{S_i \in \mathcal{S}_1} C_i - y_1 C_0. \quad (2.6)$$

Then $\alpha \in \mathbb{Z}\mathcal{C}$, $X_0(\alpha) = \ell_1 k - y_1$ and $X_1(\alpha) = 0$. Then for each $j = 1, \dots, n-1$, $\sigma^j(\alpha) \in \mathbb{Z}\mathcal{C}$, $X_0(\sigma^j(\alpha)) = \ell_1 k - y_1$ and $X_{j+1}(\sigma^j(\alpha)) = 0$.

Set

$$\beta = \prod_{j=0}^{n-1} \sigma^j(\alpha). \quad (2.7)$$

Then $\beta \in \mathbb{Z}\mathcal{C}$, $X_0(\beta) = (\ell_1 k - y_1)^n$ and $X_j(\beta) = 0 \forall j = 1, \dots, n$. But β is also \mathbb{Z}_n -invariant, so we can find integers e_1, e_2 such that $\beta = e_1 C_0 + e_2 \overline{C}$. We obtain the equations

$$\begin{aligned} (\ell_1 k - y_1)^n &= e_1 X_0(C_0) + e_2 X_0(\overline{C}) \\ &= e_1 + e_2 n k \end{aligned} \quad (2.8)$$

and for $j = 1, \dots, n$,

$$\begin{aligned} 0 &= e_1 X_j(C_0) + e_2 X_j(\overline{C}) \\ &= e_1 - e_2. \end{aligned} \quad (2.9)$$

Thus $e_1 = e_2$ and

$$(\ell_1 k - y_1)^n = e_1(1 + nk) = e_1 p. \quad (2.10)$$

Since p is a prime, we deduce that $p \mid (\ell_1 k - y_1)$. But $\ell_1 k < nk < p$ and y_1 is non-negative, so that

$$\ell_1 k \leq y_1. \quad (2.11).$$

We now wish to show that $|S_i| \leq k \forall i = 1, \dots, n$. To see this, change basis in $\mathbb{C}\mathcal{C}$ by setting $c_i = C_i/m(C_i)$.

Then

$$c_i c_j = \sum_k n_{ij}^k c_k \quad (2.12)$$

where

$$n_{ij}^k = N_{ij}^k m(C_k) / m(C_i) m(C_j). \quad (2.13)$$

The n_{ij}^k are non-negative rational numbers that satisfy $\sum_k n_{ij}^k = 1 \forall i, j$, so that the set $\{c_0, c_1, \dots, c_n\}$ forms a finite abelian hypergroup with character table

	X_0	X_1	\cdots	X_n	
C_0	1	1	\cdots	1	
C_1	1	S_1/k	\cdots	S_2/k	
\vdots	\vdots	\vdots	\ddots	\vdots	
C_n	1	S_n/k	\cdots	S_1/k	(2.13)

The powers of any element c_i must always be a convex linear combination of the c_j ; when we identify c_i with the corresponding row in the above character table we deduce immediately that each entry must be a complex number of modulus at most one. This proves that

$$|S_i| \leq k \quad \forall i. \quad (2.15)$$

Combining this with (2.11) we deduce that $S_j = k$ for all $S_j \in \mathcal{S}_1$.

Now let $\mathcal{D} = \{C_0\} \cup \{C_j \mid X_1(C_j) = k\}$. We claim that this set is a proper subassembly of \mathcal{C} in the obvious sense. This is seen by considering $\mathcal{D}' = \{c_0\} \cup \{c_j \mid X_i(c_j) = 1\}$ and noting that since 1 can be expressed as a convex combination of numbers of modulus at most one in essentially only one way, the product of two elements of \mathcal{D}' is contained in $\mathbb{C}\mathcal{D}'$. If $\mathcal{D} = \mathcal{C}$ then X_1 would be identical to X_0 which is impossible by orthogonality, and since \mathcal{S}_1 is non empty, $\mathcal{D} \neq \{C_0\}$, so this proves our claim. Let n' be the order of \mathcal{D} (that is $n' = |\mathcal{D}| - 1$.)

Now let $f_0 = \sum_{C_i \in \mathcal{D}} C_i$. Then from (1.2) and (1.11) applied to the assembly \mathcal{D} , $C_j f_0 = m(C_j) f_0 \forall C_j \in \mathcal{D}$. Thus for any $C_i \in \mathcal{C}$, $C_i \sigma^j(f_0) = m(C_i) \sigma^j(f_0)$ for some $j \in 0, \dots, n-1$. Let

$$f = \prod_{j=0}^{n-1} \sigma^j(f_0). \quad (2.16)$$

Then $f \in \mathbb{Z}\mathcal{C}$ and

$$C_i f = m(C_i) f \quad \forall i. \quad (2.17)$$

But recall that $e = m(\mathcal{C})e_0 = C_0 + C_1 + \dots + C_n$ satisfies $C_i e = m(C_i) e \forall i$ and that e is up to a scalar the unique element of $\mathbb{Z}\mathcal{C}$ with this property. Thus we must have $f = ue$ for some integer u . Applying conservation of mass, we get

$$(1 + n'k)^n = up \quad (2.18)$$

where $0 < n' < n$. But since $p = 1 + nk$ is a prime, this is impossible. \square

§3 Some algebraic number theory

Let A be the \mathbb{Z} span of $\{S_1, \dots, S_n\}$; by Corollary 2.2, $\mathbb{Z} \subseteq A$ and by Corollary 2.4, A is a ring of algebraic integers. Let K be the \mathbb{Q} span of $\{S_1, \dots, S_n\}$. Then $\mathbb{Q} \subseteq K$ and K is a ring of algebraic numbers, so that K is actually a field. From Theorem 2.4, we deduce that $[K : \mathbb{Q}] = n$ and that $\{S_1, \dots, S_n\}$ is linearly independent over \mathbb{Q} . The map $\sigma : K \rightarrow K$ defined by $\sigma(S_i) = S_{\sigma(i)}$ is thus a well-defined automorphism of K and the powers $\{\sigma^j \mid j = 0, 1, \dots, n-1\}$ are all distinct. Thus $\text{Gal}(K : \mathbb{Q}) \simeq \mathbb{Z}_n$ and K is a cyclic extension of \mathbb{Q} of degree n .

Let D denote the discriminant of K over \mathbb{Q} .

Proposition 3.1 $D = \pm(p^r)$ for some integer r .

Proof. Let B denote the ring of algebraic integers of K . Then $A \subseteq B$, and since $\{S_1, \dots, S_n\}$ is a \mathbb{Z} base for A , the result will follow from showing that $\text{discr } \{S_1, \dots, S_n\}$ is up to a sign a power of p . We use the formula $\text{discr } \{S_1, \dots, S_n\} = \det[\text{tr}(S_i S_j)]$.

We need therefore to evaluate some traces. Consider first the case when \mathcal{C} is Hermitian. Then by cyclic symmetry and conservation of mass, we have in $\mathbb{Z}\mathcal{C}$ the equations

$$\begin{aligned} C_1^2 + \dots + C_n^2 &= nkC_0 + (k-1)\overline{C} \\ C_1 C_2 + \dots + C_n C_1 &= k\overline{C} \\ &\vdots \\ C_1 C_n + \dots + C_n C_{n-1} &= k\overline{C}. \end{aligned} \tag{3.1}$$

It follows that we obtain the following quadratic equations for the S_i .

$$\begin{aligned} S_1^2 + \dots + S_n^2 &= nk - (k-1) = p - k \\ S_1 S_2 + \dots + S_n S_1 &= -k \\ &\vdots \\ S_1 S_n + \dots + S_n S_{n-1} &= -k. \end{aligned} \tag{3.2}$$

Then

$$\begin{aligned} \det[\text{tr}(S_i S_j)] &= \det \begin{vmatrix} p-k & -k & \dots & -k \\ -k & p-k & -k \dots & \\ & -k & & \\ & \vdots & & \\ -k & & & p-k \end{vmatrix} \\ &= g(-p) \end{aligned} \tag{3.3}$$

where g is the characteristic polynomial of the $n \times n$ matrix all of whose entries are $-k$. Such a matrix has an eigenvalue 0 of multiplicity $n-1$ and an eigenvalue $-nk$ of multiplicity 1. Thus $g(t) = t^{n-1}(t+nk)$ and $g(-p) = (-1)^n p^{n-1}$. The result follows.

If \mathcal{C} is not Hermitian, then cyclic symmetry forces n to be even and $C_i^* = C_{i+\frac{n}{2}} \forall i = 1, \dots, n$ where the index is taken modulo n in the range $1, \dots, n$. The corresponding quadratic relations are then

$$\begin{aligned} S_1 S_{1+\frac{n}{2}} + \dots + S_n S_{n+\frac{n}{2}} &= p - k \\ S_1 S_{1+i} + \dots + S_n S_{n+i} &= -k \quad \text{for } i \neq \frac{n}{2}. \end{aligned} \tag{3.4}$$

The matrix $[\text{tr}(S_i S_j)]$ is thus a permutation of (3.3) so the result follows in this case as well. \square

Corollary 3.2 *p is the only prime in \mathbb{Z} which ramifies in K .*

Proof. This is a standard consequence from algebraic number theory (see e.g. Samuel [1]). \square

We now utilize the following result proved in Greenberg [1], [2]. Let $\mathbb{Q}(p) = \mathbb{Q}(e^{\frac{2\pi i}{p}})$ be the cyclotomic field of p^{th} roots of unity.

Result. (Greenberg [1]) Let K be an abelian extension of \mathbb{Q} of prime-power degree λ^m and suppose that $p \neq \lambda$ is the only prime ramified in K . Then p is totally ramified in K , $p \equiv 1 \pmod{\lambda^m}$ and K is the unique subfield of $\mathbb{Q}(p)$ of degree λ^m . \square

Proposition 3.3 *K is the unique subfield of $\mathbb{Q}(p)$ of degree n over \mathbb{Q} .*

Proof: Let $n = p_1^{\alpha_1} \dots p_t^{\alpha_t}$ be the prime power decomposition of n and let K_i be the unique subfield of K of degree $p_i^{\alpha_i}$ over \mathbb{Q} . (This exists since K is cyclic over \mathbb{Q}) Then K is the compositum of the fields K_i , $i = 1, \dots, t$. The preceding result implies that $K_i \subseteq \mathbb{Q}(p)$ for all $i = 1, \dots, t$, so that $K \subseteq \mathbb{Q}(p)$. Uniqueness is clear. \square

Recall the numbers Q_1, \dots, Q_n associated to the assembly $\mathcal{C}(p, n)$ in §0.

Proposition 3.4 $\{S_1, \dots, S_n\} = \{Q_1, \dots, Q_n\}$.

Proof. It is a standard fact that $\{Q_1, \dots, Q_n\}$ forms a \mathbb{Z} base for the ring of algebraic integers of the unique subfield of $\mathbb{Q}(p)$ of degree n over \mathbb{Q} , which we now know to be K . Since our labelling is such that $\sigma(Q_i) = Q_{\sigma(i)} \forall i$ (where we identify σ with the automorphism of K which it induces), we may find integers a_1, \dots, a_n such that

$$\begin{aligned}
S_1 &= a_1 Q_1 + \dots + a_n Q_n \\
S_2 &= a_n Q_1 + a_1 Q_2 + \dots + a_{n-1} Q_n \\
&\vdots \\
S_n &= a_2 Q_1 + \dots + a_n Q_{n-1} + a_1 Q_n.
\end{aligned} \tag{3.5}$$

Now the Q_i are the character values of the cyclotomic assembly $\mathcal{C}(p, n)$, so any relations which we have derived for the S_i must also hold for the Q_i . In particular, $Q_1 + \dots + Q_n = -1$ (this is obvious anyway) so that summing all the equations in (3.5) gives us

$$a_1 + \dots + a_n = 1. \tag{3.6}$$

Let us note also that (3.5) implies that \mathcal{C} is Hermitian if and only if $\mathcal{C}(p, n)$ is Hermitian.

Now suppose \mathcal{C} is Hermitian. Then

$$\begin{aligned}
S_1^2 + \dots + S_n^2 &= (a_1^2 + \dots + a_n^2)(Q_1^2 + \dots + Q_n^2) \\
&+ (a_1 a_2 + \dots + a_n a_1)(Q_1 Q_2 + \dots + Q_n Q_1) + \dots \\
&+ (a_1 a_n + \dots + a_n a_{n-1})(Q_1 Q_n + \dots + Q_n Q_{n-1})
\end{aligned} \tag{3.7}$$

and applying (3.2) to both $\{S_i\}$ and $\{Q_i\}$ we get

$$\begin{aligned}
p - k &= (a_1^2 + \dots + a_n^2) (p - k) \\
&+ (a_1 a_n + \dots + a_n a_1)(-k) + \dots \\
&+ (a_1 a_n + \dots + a_n a_{n-1})(-k)
\end{aligned} \tag{3.8}$$

But

$$\begin{aligned}
1 &= (a_1 + \cdots + a_n)^2 \\
&= (a_1^2 + \cdots + a_n^2) + (a_1a_2 + \cdots + a_na_1) + \cdots + (a_1a_n + \cdots + a_na_{n-1})
\end{aligned} \tag{3.9}$$

so that setting $a_1^2 + \cdots + a_n^2 = L$, we have from (3.8)

$$p - k = L(p - k) - (1 - L)k \tag{3.10}$$

or

$$p(1 - L) = 0. \tag{3.11}$$

Thus $L = 1$ which implies that exactly one of the a_i is 1 and the others are 0, i.e. that $\{S_1, \dots, S_n\} = \{Q_1, \dots, Q_n\}$.

The case when \mathcal{C} is not Hermitian is similar; we leave it to the reader. \square

We are free to relabel the characters X_i of \mathcal{C} so that $S_1 = Q_1$. If we do this then by cyclic symmetry $S_i = Q_i \forall i$. Since an assembly is determined by its character table, we conclude that $\mathcal{C} \simeq \mathcal{C}(p, n)$. This proves our main result.

Theorem 3.5 Let p be a prime and n a positive integer dividing $p - 1$. Then there is up to isomorphism exactly one cyclotomic assembly of total mass p and order n – namely $\mathcal{C}(p, n)$. \square

Let us note that we may now deduce that $\mathbb{Z}\mathcal{C}$ is a Dedekind domain (since it is isomorphic to a ring of algebraic integers) – a result which is not obvious from the axiomatic definition of $\mathbb{Z}\mathcal{C}$. This suggests some questions. If \mathcal{C} is an arbitrary assembly, how close is $\mathbb{Z}\mathcal{C}$ to being a Dedekind domain? Which Dedekind domains are of this form?

To conclude, we give an example to show that our result does not necessarily hold if the condition p is a prime is removed. The following equations describe two non-isomorphic

cyclotomic assemblies of total mass 49 and order 3, found by Elizabeth Lee using the results in Wildberger [2].

i)
$$C_1^2 = 16C_0 + 3C_1 + 6C_2 + 6C_3$$
$$C_1C_2 = 6C_1 + 6C_2 + 4C_3 \tag{3.12}$$

ii)
$$C_1^2 = 16C_0 + 6C_1 + 4C_2 + 5C_3$$
$$C_1C_2 = 4C_1 + 5C_2 + 7C_3 \tag{3.13}$$

Bibliography

- Dickson, L.E. [1] Cyclotomy, higher congruences, and Waring's problem, Amer. J. Math. 57 (1935) 391–424.
- Greenberg M.J. [1] An elementary proof of the Kronecker-Weber Theorem, Amer. Math. Monthly 8 June–July 81 (1974), 601–607
- Greenberg, M.J. [2] Erratum, Ibid 82 (1975), 803.
- Hall, M., Jr. [1] *Combinatorial Theory*, Blaisdell Publishing Co., Waltham, Mass., 1967.
- Leonard P.A., Williams, K.S. [1] The cyclotomic numbers of order seven. Proc. Amer. Math. Soc. 51 (1975), 295–300.
- Leonard P.A., Williams, K.S. [2] The cyclotomic numbers of order eleven, Acta Arith. 26 (1974/75), No. 4, 365–383.
- Myerson, G. [1] Period polynomials and Gauss sums for finite fields. Acta Arithmetica 39 (1981) 251–264.
- Samuel, P. [1] *Algebraic Theory of Numbers*, Hermann, Paris, 1970.
- Storer, T. [1] *Cyclotomy and difference sets*. Lectures in Advanced Mathematics, No. 2, Markham Publishing Co., Chicago, Ill. 1967.
- Whiteman, A.L. [1] The cyclotomic numbers of order ten. Proc. Sympos. Appl. Math., Vol. 10, pp.95–111. AMS, Providence, R.I., 1960.
- Whiteman, A.L. [2] The cyclotomic numbers of order twelve, Acta Arith. 6 (1960) 53–76.

Wildberger N.J. [1] Duality and entropy for finite abelian hypergroups, Preprint (1990)

University of New South Wales.

Wildberger N.J. [2] Hypergroups and cyclotomy, Preprint (1990), University of New South

Wales.