ACTA ARITHMETICA
XV (1969)

On the arithmetic structure of Galois Domains*

by

T. STORER (Ann Arbor, Mich.)

1. Introduction. The purpose of this paper is to show that the distributive law for classes in certain Galois Domains is completely contained in the distributive laws for the classes in the summand fields of these domains; in particular, we show that once the problem has been solved for the field, it has also been solved for the corresponding domains. We further show that the Jacobi and Lagrange functions can be extended in a natural way to these domains, and that these functions are decomposable into the corresponding functions for fields. Finally, we prove an analogue of Jacobi's Lemma for a subcollection of the above domains.

The setting for the results in this paper is $\boldsymbol{Z}_p$, $\boldsymbol{Z}_{pq}$, etc.; the extension to $\mathrm{GF}(p^a)$, $\mathrm{GD}(p^a q^\beta)$, etc. follows from the methods developed in [2], and is straightforward. The principal tool is the theory of cyclotomy, and we shall assume the results of this theory for finite fields and derive the corresponding results for domains. At present, the theory of cyclotomy for domains is almost completely independent of the corresponding theory for fields (although the two are formally very similar in appearance), each depending on a careful analysis of the individual structure involved. The novelty of the present approach is that no reference is made to the structure of the domain, the analysis being carried out entirely in the summand fields.

The paper is divided into five sections: Section 2 recalls those results from the theory of cyclotomy for the finite field necessary for the subsequent proofs. Sections 3 and 4 develop the (known) theory of cyclotomy for the domain $\boldsymbol{Z}_{pq}$ from the corresponding theories for the summand fields, $\boldsymbol{Z}_p$ and $\boldsymbol{Z}_q$. The main theorem (Theorem 1) of Section 3 gives an explicit formula for the cyclotomic numbers for $\boldsymbol{Z}_{pq}$ in terms of the corresponding cyclotomic numbers for $\boldsymbol{Z}_p$ and $\boldsymbol{Z}_q$; the principal step in the proof of Theorem 1 is Lemma 4, which gives a direct decomposition of the cyclotomic classes for $\boldsymbol{Z}_{pq}$ in terms of the corresponding classes for $\boldsymbol{Z}_p$

* Supported in part by an NSF research grant.

and Z_q. In Section 4 the functions of Jacobi and Lagrange for Z_{pq} are shown to decompose into the corresponding functions for Z_p and Z_q, and an analogue of Jacobi's Lemma for fields is proved. The latter result is of importance in discussing the existence of finite difference sets in Z_{pq}. Section 5 devotes itself to the general situation Z_n, where an extension of Theorem 1 is proved and the class structure discussed. The paper concludes with a new derivation of the only class-structure result known for domains whose order is a product of more than two distinct odd primes.

All results referenced in this paper (with the single exception of Lemma 12) will be found, with proofs, in [2], where the original sources are indicated.

2. Notation and preliminaries. Let $p_0 = ef_0+1$ be an odd prime, and let g_0 be a fixed primitive root of p_0 (i.e. g_0 is a fixed generator of the finite field Z_{p_0}). Define the *cyclotomic classes*

$$C_{p_0,i} = \{g_0^{es+i} (\mathrm{mod}\, p_0):\ s = 0, 1, \ldots, f_0-1\}; \qquad i = 0, 1, \ldots, e-1$$

so that $C_{p_0,0}$ is the (multiplicative) subgroup of eth powers modulo p_0, and the $C_{p_0,i}$, $i \neq 0$, are the cosets of $C_{p_0,0}$, *ordered on* g_0. Further, define the matrix $\mathbf{C}_{p_0,e} = [a_{i,j}]$, where $a_{i,j}$ is the number of solutions in Z_{p_0} of the equation

$$Z_i+1 \equiv Z_j\ (\mathrm{mod}\, p_0); \qquad Z_i \epsilon C_{p_0,i},\ Z_j \epsilon C_{p_0,j};$$

i.e., $a_{i,j}$ is the number of ordered pairs (s, t), with $0 \leqslant s, t \leqslant f_0-1$, such that

$$g_0^{es+i}+1 \equiv g_0^{et+j}\ (\mathrm{mod}\, p_0).$$

Then $\mathbf{C}_{p_0,e}$ is called the *cyclotomic matrix* of Z_{p_0} with respect to e for the fixed generator g_0, and the entries $a_{i,j} = (i, j)_{p_0}$, $0 \leqslant i, j \leqslant e-1$, of $\mathbf{C}_{p_0,e}$ are called the *cyclotomic numbers* for Z_{p_0} and e, with respect to g_0. Note that, since Z_{p_0} is unique up to isomorphism, replacement of g_0 by a new generator g_0^* of Z_{p_0} leaves $C_{p_0,0}$ fixed, and at most permutes the $C_{p_0,i}$, $i \neq 0$.

The cyclotomic numbers for Z_{p_0}, e, and g_0 satisfy the following relations (see [2], p. 25):

LEMMA 1.

(a) $(i, j)_{p_0} = (i+me, j+ne)_{p_0}$ *for all* $m, n \epsilon Z$,

(b) $(i, j)_{p_0} = (e-i, j-i)_{p_0}$,

(c) $$(i, j)_{p_0} = \begin{cases} (j, i)_{p_0} & \text{if } f_0 \text{ is even,} \\ (j+e/2, i+e/2)_{p_0} & \text{if } f_0 \text{ is odd,} \end{cases}$$

(d) $$\sum_{j=0}^{e-1} (i, j)_{p_0} = f_0 - \theta_{p_0,i},$$

where

$$\theta_{p_0,i} = \begin{cases} 1 & \text{if } f_0 \text{ is even and } i = 0, \\ 1 & \text{if } f_0 \text{ is odd and } i = e/2, \\ 0 & \text{otherwise.} \end{cases}$$

Note that

$$\theta_{p_0,i} = \begin{cases} 1 & \text{if } -1 \epsilon C_{p_0,i}, \\ 0 & \text{otherwise.} \end{cases}$$

Now let N be an arbitrary natural number, and define

$$\lambda_N = \exp(2\pi i/N).$$

We then define the *periods*

$$\eta_{p_0,k} = \sum_{a \epsilon C_{p_0,k}} \lambda_{p_0}^a = \sum_{s=0}^{f_0-1} \lambda_{p_0}^{g_0^{es+k}}; \qquad k = 0, 1, \ldots, e-1,$$

and note that

$$\sum_{k=0}^{e-1} \eta_{p_0,k} = -1.$$

Further, we have the following lemma (see [2], p. 38) relating the products of the periods to the cyclotomic numbers.

LEMMA 2.

$$\eta_{p_0,0}\eta_{p_0,k} = \sum_{j=0}^{e-1} (k, j)_{p_0} \eta_{p_0,j} + f_0 \theta_{p_0,k} \quad \textit{for} \quad k = 0, 1, \ldots, e-1.$$

Finally, we define the *Jacobi function*

$$F_{p_0}(\lambda_e^m) = \sum_{k=0}^{p_0-2} \lambda_e^{mk} \lambda_{p_0}^{g_0^k} = \sum_{k=0}^{e-1} \lambda_e^{mk} \eta_{p_0,k},$$

and, for natural numbers m and n such that e divides none of m, n, nor $m+n$, the *Lagrange function*

$$R_{p_0}(m, n) = \sum_{k=0}^{e-1} \lambda_e^{nk} \sum_{h=0}^{e-1} \lambda_e^{-(m+n)h} (k, h)_{p_0}.$$

The properties of these functions are well known (see [2], pp. 41-47 and 62-64); we list below those properties of interest to us.

LEMMA 3.

(a) $$R_{p_0}(m,n) = \frac{F_{p_0}(\lambda_e^m)F_{p_0}(\lambda_e^n)}{F_{p_0}(\lambda_e^{m+n})};$$

(b) *If l_0 is the natural number defined by*

$$g_0^{l_0} \equiv 2 \ (\mathrm{mod}\ p_0),$$

then

$$F_{p_0}(-1)F_{p_0}(\lambda_e^{2k}) = \lambda_e^{2kl_0}F_{p_0}(\lambda_e^k)F_{p_0}(-\lambda_e^k).$$

Part (b) of Lemma 3 is *Jacobi's Lemma* for finite fields.

3. Galois Domains, I. Now let $p_0 = ef_0+1$ and $p_1 = ef_1+1$ be distinct odd primes such that g.c.d. $(f_0, f_1) = 1$ [i.e., $e =$ g.c.d. (p_0-1, p_1-1)]; let $d =$ l.c.m. $(p_0-1, p_1-1) = ef_0f_1$, and suppose that g is a fixed common primitive root of both p_0 and p_1. If $x_0 \epsilon \boldsymbol{Z}_{p_0p_1}$ is defined by

$$x_0 \equiv g \ (\mathrm{mod}\ p_0) \quad \text{and} \quad x_0 \equiv 1 \ (\mathrm{mod}\ p_1),$$

we define, as in the case of the finite field, the cyclotomic classes

$$C_{p_0p_1,i} = \{g^s x_0^i \ (\mathrm{mod}\ p_0p_1);\ s = 0, 1, \ldots, d-1\}, \qquad i = 0, 1, \ldots, e-1;$$

it is easily verified that the $C_{p_0p_1,i}$ are pairwise disjoint and that their union is $\boldsymbol{M}_{p_0p_1}$, the (multiplicative) subgroup of units of $\boldsymbol{Z}_{p_0p_1}$. There are, of course, other choices for x_0 [e.g., $x_1 \equiv 1 \ (\mathrm{mod}\ p_0)$, $x_1 \equiv g \ (\mathrm{mod}\ p_1)$], but replacement of x_0 by an x^* leaves $C_{p_0p_1,0}$ fixed, and at most permutes the cosets $C_{p_0p_1,i}$, $i \neq 0$, of $C_{p_0p_1,0}$. With x_0 (alternatively, x_1) chosen as above, we say that the cosets of $C_{p_0p_1,0}$ are *ordered on* p_0 (alternatively, *ordered on* p_1).

We now define the cyclotomic matrix $\mathbf{C}_{p_0p_1,e} = [a_{i,j}]$ for the fixed *generator* g of $\boldsymbol{Z}_{p_0p_1}$ by requiring $a_{i,j}$ to be the number of solutions in $\boldsymbol{Z}_{p_0p_1}$ of the equation

$$Z_i + 1 \equiv Z_j \ (\mathrm{mod}\ p_0p_1), \qquad Z_i \epsilon C_{p_0p_1,i},\ Z_j \epsilon C_{p_0p_1,j};$$

i.e., the number of ordered pairs (s,t), with $0 \leqslant s, t \leqslant d-1$, such that

$$g^s x_0^i + 1 \equiv g^t x_0^j \ (\mathrm{mod}\ p_0p_1).$$

Again, the entries $a_{i,j} = (i,j)_{p_0p_1}$ of $\mathbf{C}_{p_0p_1,e}$ are called the cyclotomic numbers for $\boldsymbol{Z}_{p_0p_1}$ with respect to g [1]. Now, in this case, replacement of g by a new generator g^* of $\boldsymbol{Z}_{p_0p_1}$ may no longer leave $C_{p_0p_1,0}$, nor hence any $C_{p_0p_1,i}$, fixed, and so in general there exist several distinct cyclotomic matrices $\mathbf{C}_{p_0p_1,e}$ corresponding to p_0 and p_1 which cannot be obtained one from the other by permutations. Since $\varphi(p_0-1)\,\varphi(p_1-1) = \varphi(e)\varphi(d)$, it is easy to show that there are at most $\varphi(e)$ such matrices (where φ is the Euler function).

[1] We suppress the e now, since e is uniquely determined by p_0 and p_1.

We now state the main theorem relating $\mathbf{C}_{p_0p_1,e}$ to $\mathbf{C}_{p_0,e}$ and $\mathbf{C}_{p_1,e}$.

THEOREM 1. *Let $p_0 = ef_0+1$ and $p_1 = ef_1+1$ be distinct odd primes, and $e =$ g.c.d. (p_0-1, p_1-1). Further, let g_0 and g_1 be generators of $\boldsymbol{Z}_{p_0}$ and $\boldsymbol{Z}_{p_1}$, respectively, and g the common primitive root of p_0 and p_1 corresponding to g_0 and g_1. Let $C_{N,i}$ ($N = p_0, p_1$, or p_0p_1) be the cyclotomic classes, with $C_{p_0p_1,i}$ ordered on p_0, and $\mathbf{C}_{N,e}$ the corresponding cyclotomic matrices. Then, if P and Q are the permutation matrices*

$$P = \mathrm{Circ}(\overbrace{0, 1, 0, \ldots, 0}^{e}) = \left(\begin{array}{c|c} 0 & I_{e-1} \\ \hline 1 & 0 \end{array}\right), \qquad Q = \mathrm{Circ}(\overbrace{0, 0, \ldots, 0, 1}^{e}) = \left(\begin{array}{c|c} 0 & 1 \\ \hline I_{e-1} & 0 \end{array}\right),$$

we have

$$\mathbf{C}_{p_0p_1,e} = [(P^i\mathbf{C}_{p_0,e}Q^j)\cdot\mathbf{C}_{p_1,e}],$$

where $\cdot$ indicates the inner product of the two matrices.

COROLLARY.

$$(0,0)_{p_0p_1} = \mathbf{C}_{p_0,e}\cdot\mathbf{C}_{p_1,e}.$$

We remark that Theorem 1 extends the knowledge of the class structure of the domains $\boldsymbol{Z}_{p_0p_1}$ to those e for which the corresponding problem in $\boldsymbol{Z}_{p_0}$ has been solved; namely, $e \leqslant 20$ (e even). In particular, if one wished to determine, for a fixed even $e \leqslant 20$ those primes p_0 and p_1, with $p_1 = (e-1)p_0+2$ for which all the cyclotomic numbers $(i,0)_{p_0p_1}$; $i = 0, 1, \ldots, e-1$, had the same value (as in the construction of finite difference sets modulo p_0p_1 (cf. [2], p. 89)), he would have only to examine the set $(P^i\mathbf{C}_{p_0,e})\cdot\mathbf{C}_{p_1,e}$ under the above condition. The problem is thus reduced to a straightforward, albeit lengthy, computation.

The proof of Theorem 1 is accomplished with the aid of the definition of a new class product, and two facts concerning this product. We give the definition and develope the necessary material in two rather lengthy lemmas.

Let $A_0 \subset \boldsymbol{Z}_{p_0}$ and $A_1 \subset \boldsymbol{Z}_{p_1}$, and define the *class product*

$$A_0A_1 = \{p_1a_0 + p_0a_1 \ (\mathrm{mod}\ p_0p_1);\ a_0 \epsilon A_0,\ a_1 \epsilon A_1\}.$$

As an elementary remark, we note that

$$\boldsymbol{M}_{p_0p_i} = \sum_{i,j=0}^{e-1} C_{p_0,i}C_{p_1,j},$$

where A_0+A_1 and $\sum_i A_i$ denote *strong union*. Let m_0 and m_1 be integers such that $m_1p_0 + m_0p_1 = 1$, and define the natural numbers a_0 and a_1 by $m_0 \epsilon C_{p_0,a_0}$, $m_1 \epsilon C_{p_1,a_1}$, so that

$$1 \epsilon C_{p_0,a_0}C_{\ 1,a_1} \subset \boldsymbol{M}_{p_0p_1}.$$

Finally, define $C'_{p_0p_1,i}$, $i = 0, 1, \ldots, e-1$ in $\boldsymbol{Z}_{p_0p_1}$ to be the sets

$$C'_{p_0p_1,i} = \sum_{k=0}^{e-1} C_{p_0,(a_0+i)+k} C_{p_1,a_1+k}.$$

Lemma 4.

$$C'_{p_0p_1,k} = C_{p_0p_1,k}; \qquad k = 0, 1, \ldots, e-1.$$

Proof. We must show that

$$C'_{p_0p_1,k} = \{g^s x_0^k (\text{mod } p_0p_1)\colon s = 0, 1, \ldots, d-1\}$$

for $k = 0, 1, \ldots, e-1$. Clearly $C'_{p_0p_1,k}$ consists of d distinct elements modulo p_0p_1 and, since

$$C_{p_0,i} = \{g_0^{es+i} \ (\text{mod } p_0)\colon s = 0, 1, \ldots, f_0-1\},$$
$$C_{p_1,j} = \{g_1^{et+j} \ (\text{mod } p_1)\colon t = 0, 1, \ldots, f_1-1\}$$

the general term of $C_{p_0p_1,k}$ may be written in the form

$$C_{p_0,i} C_{p_1,j} = \{g_1^{et+j} p_0 + g_0^{es+i} p_1\} \ (\text{mod } p_0p_1).$$

In particular, in the case of $C'_{p_0p_1,0}$, we know that there exist natural numbers s and t such that

$$1 \equiv g_1^{et+a_1} p_0 + g_0^{es+a_0} p_1 \ (\text{mod } p_0p_1),$$

whence

$$g \equiv g_1^{et+(a_1+1)} p_0 + g_0^{es+(a_0+1)} p_1 \ (\text{mod } p_0p_1),$$

and so $g \in C_{p_0,a_0+1} C_{p_1,a_1+1} \subset C'_{p_0p_1,0}$, by definition. It therefore follows that every power of g modulo p_0p_1 is an element of $C'_{p_0p_1,0}$, and hence $C'_{p_0p_1,0}$ consists solely of the d distinct powers of g modulo p_0p_1.

Further,

$$x_0 \equiv g_1^{et+a_1} p_0 + g_0^{es+(a_0+1)} p_1 \ (\text{mod } p_0p_1)$$

is an element of $C_{p_0,a_0+1} C_{p_1,a_1} \subset C'_{p_0p_1,1}$. This completes the proof of the lemma.

We remark that $C'_{p_0p_1,i}$ may equivalently be written

$$C'_{p_0p_1,i} = \sum_{k=0}^{c-1} C_{p_0,a_0+k} C_{p_1,(a_1-i)+k}$$

since all subscripts are reduced modulo e. Further, had the cosets of $C_{p_0p_1,0}$ been ordered on p_1, we would have defined

$$C'_{p_0p_1,i} = \sum_{k=0}^{e-1} C_{p_0,a_0+k} C_{p_1,(a_1+i)+k}$$

or, alternatively

$$C'_{p_0p_1,k} = \sum_{k=0}^{e-1} C_{p_0,(a_0-i)+k} C_{p_1,a_1+k},$$

in which case Lemma 4 (with x_0 replaced by x_1) remains true. The corresponding form of Theorem 1 for an ordering on p_1 is

$$\mathbf{C}_{p_0p_1,e} = [\mathbf{C}_{p_0,c} \cdot (P^i \mathbf{C}_{p_1,c} Q^j)],$$

and the same proof obtains.

We now return to the case in which the cosets of $C_{p_0p_1,0}$ are ordered on p_0, and define the periods

$$\eta_{p_0p_1,k} = \sum_{b \in C_{p_0p_1,k}} \lambda_{p_0p_1}^b; \qquad k = 0, 1, \ldots, e-1.$$

Note that, in terms of the η's, Lemma 4 says no more than that

$$\eta_{p_0p_1,k} = \sum_{i=0}^{e-1} \eta_{p_0,(a_0+k)+i} \eta_{p_1,a_1+i} = \sum_{s=0}^{d-1} \lambda_{p_0p_1}^{g^s x_0^k}; \qquad k = 0, 1, \ldots, e-1.$$

Also, we clearly have

$$\sum_{k=0}^{c-1} \eta_{p_0p_1,k} = 1.$$

We now show that the products of the periods are related to the cyclotomic numbers for $\boldsymbol{Z}_{p_0p_1}$ in very much the same way as in the case $\boldsymbol{Z}_{p_0}$ (cf. Lemma 2). The proof below, which is done entirely in the summand fields, is new, but the result is not (see [2], p. 98). The present proof offers a combinatorial interpretation of

$$\delta_{p_0p_1,k} = \begin{cases} 1 & \text{if } -1 \in C_{p_0p_1,k}, \\ 0 & \text{otherwise.} \end{cases}$$

Lemma 5.

$$\eta_{p_0p_1,0} \eta_{p_0p_1,k} = \sum_{j=0}^{e-1} (k, j)_{p_0p_1} \eta_{p_0p_1,j} - 2f_0f_1 + \delta_{p_0p_1,k} \left(\frac{p_0p_1-1}{e}\right),$$

for $k = 0, 1, \ldots, e-1$.

Proof. By definition

$$\eta_{p_0p_1,0} \eta_{p_0p_1,k} = \Big(\sum_{a \in C_{p_0p_1,0}} \lambda_{p_0p_1}^a\Big)\Big(\sum_{b \in C_{p_0p_1,k}} \lambda_{p_0p_1}^b\Big) = \Big(\sum_{s=0}^{d-1} \lambda_{p_0p_1}^{g^s}\Big)\Big(\sum_{t=0}^{d-1} \lambda_{p_0p_1}^{g^t x_0^k}\Big)$$
$$= \sum_{s,t=0}^{d-1} \lambda_{p_0p_1}^{g^s(g^{t-s} x_0^k + 1)} = \sum_{s,t=0}^{d-1} \lambda_{p_0p_1}^{g^s(g^t x_0^k + 1)}.$$

Note that

$$g^t x_0^k \in \begin{cases} C_{p_0,t+k} \subset \boldsymbol{Z}_{p_0}, \\ C_{p_1,t} \subset \boldsymbol{Z}_{p_1}, \end{cases}$$

and that if $g^t x_0^k = a \epsilon C_{p_0,t+k}$, then for each u in the set

$$\{t+n(p_0-1):\ n=0,1,\ldots,f_1-1\},$$

we have that $g^u x_0^k = a \epsilon C_{p_0,t+k}$. A similar statement holds for p_1.

Now let $M = g^t x_0^k + 1 \epsilon \boldsymbol{Z}_{p_0p_1}$. Clearly, as a ranges over $C_{p_0,t+k}$, $a+1 = 0 \epsilon \boldsymbol{Z}_{p_0}$ exactly $\theta_{p_0,t+k}$ times; while as a ranges over $C_{p_1,t}$, $a+1 = 0 \epsilon \boldsymbol{Z}_{p_1}$ exactly $\theta_{p_1,t}$ times. Hence $M = g^t x_0 + 1 = 0 \epsilon \boldsymbol{Z}_{p_0p_1}$ exactly

$$\delta_{p_0p_1,k} = \sum_{t=0}^{e-1} \theta_{p_0,t+k}\,\theta_{p_1,t} = \begin{cases} 1 & \text{if } f_0f_1 \text{ is odd and } k=0, \\ 1 & \text{if } f_0f_1 \text{ is even and } k=e/2, \\ 0 & \text{otherwise} \end{cases}$$

times with t. For each such t,

$$\sum_{s=0}^{d-1} \lambda_{p_0p_1}^{g^s\cdot 0} = d,$$

whence the total contribution to the sum in question for $M = 0 \epsilon \boldsymbol{Z}_{p_0p_1}$ is $d\delta_{p_0p_1,k}$.

Suppose now that $p_0 | M \neq 0 \epsilon \boldsymbol{Z}_{p_0p_1}$, and that $M/p_0 \equiv g_1^h (\operatorname{mod} p_1)$. Then, if $p_0 \epsilon C_{p_1,\mu} \subset \boldsymbol{Z}_{p_1}$, there exists a natural number r such that

$$g^t x_0^k + 1 \equiv g_1^{er+\mu+h} \pmod{p_1},$$

i.e., such that some element of $C_{p_1,t}$ is immediately followed by an element of $C_{p_1,\mu+h}$. Conversely, each of the $(t,\mu+h)_{p_1}$ elements corresponding to a fixed h modulo e gives rise to f_0 distinct elements of $C_{p_0p_1,k}$ with the above property. In the present case

$$\lambda_{p_0p_1}^{g^sM} = \lambda_{p_1}^{g^s(g^tx_0^k+1)} = \lambda_{p_1}^{g_1^s(g_1^t+1)},$$

so the contribution for fixed t is

$$f_0 \sum_{s=0}^{p_1-2} \lambda_{p_1}^{g_1^s(g_1^t+1)} = f_0 \sum_{s=0}^{p_1-2} \lambda_{p_1}^{s+er+\mu+h} = f_0 \sum_{s=0}^{p_1-2} \lambda_{p_1}^{g_1^s} = -f_0.$$

Hence, the total contribution is

$$-f_0 \sum_{t=0}^{e-1} \theta_{p_0,t+k} \sum_{h=0}^{e-1} (t,\mu+h)_{p_1} = -f_0 \sum_{t=0}^{e-1} \theta_{p_0,t+k}(f_1 - \theta_{p_1,t}) = -f_0f_1 + f_1\,\delta_{p_0p_1,k}.$$

Similarly, if $p_1 | M \neq 0 \epsilon \boldsymbol{Z}_{p_0p_1}$, the contribution is $-f_0f_1 + f_0\,\delta_{p_0p_1,k}$.

Finally, if neither p_0 nor p_1 divides M, then there exist natural numbers u and j such that $g^t x_0^k + 1 = g^u x_0^j \epsilon C_{p_0p_1,j}$, so that

$$\sum_{s=0}^{d-1} \lambda_{p_0p_1}^{g^s(g^ux_0^j)} = \sum_{s=0}^{d-1} \lambda_{p_0p_1}^{g^sx_0^j} = \eta_{p_0p_1,j},$$

and the total contribution is

$$\sum_{j=0}^{e-1} (k,j)_{p_0p_1}\,\eta_{p_0p_1,j}.$$

Upon noting that $d+f_0+f_1 = (p_0p_1-1)/e$ and combining the above results, the lemma is proved.

We now prove Theorem 1 by using Lemma 4 (and Lemma 2) to give an alternate evaluation of $\eta_{p_0p_1,0}\,\eta_{p_0p_1,k}$.

Proof of Theorem 1. By Lemma 4,

$$\begin{aligned}\eta_{p_0p_1,0}\,\eta_{p_0p_1,k} &= \Big(\sum_{i=0}^{e-1} \eta_{p_0,a_0+i}\,\eta_{p_1,a_1+i}\Big)\Big(\sum_{j=0}^{e-1} \eta_{p_0,a_0+k+j}\,\eta_{p_1,a_1+j}\Big) \\ &= \sum_{i,j=0}^{e-1} (\eta_{p_0,a_0+i}\,\eta_{p_0,a_0+k+j})(\eta_{p_1,a_1+i}\,\eta_{p_1,a_1+j}) \\ &= \sum_{i,j=0}^{e-1} (\eta_{p_0,a_0+i}\,\eta_{p_0,(a_0+i)+(k+j)})(\eta_{p_1,a_1+i}\,\eta_{p_1,(a_1+i)+j}).\end{aligned}$$

By Lemma 2 (with λ_{p_0} replaced by $\lambda_{p_0}^{a_0+i}$), this expression is equal to

$$\begin{aligned}&\sum_{i,j=0}^{e-1} \Big(\sum_{r=0}^{e-1} (k+j,r)_{p_0}\,\eta_{p_0,a_0+i+r} + f_0\,\theta_{p_0,k+j}\Big)\Big(\sum_{s=0}^{e-1} (j,s)_{p_1}\,\eta_{p_1,a_1+i+s} + f_1\theta_{p_1,j}\Big) \\ &= \sum_{i,j=0}^{e-1} \Big(\sum_{r,s=0}^{e-1} (k+j,r)_{p_0}(j,s)_{p_1}\,\eta_{p_0,a_0+i+r}\,\eta_{p_1,a_1+i+s} + \\ &\quad + f_1\,\theta_{p_1,j} \sum_{r=0}^{e-1} (k+j,r)_{p_0}\,\eta_{p_0,a_0+i+r} + f_0\,\theta_{p_0,k+j} \sum_{s=0}^{e-1} (j,s)_{p_1}\,\eta_{p_1,a_1+i+s} + \\ &\qquad\qquad + f_0f_1\,\theta_{p_0,k+j}\,\theta_{p_1,j}\Big).\end{aligned}$$

We evaluate this sum in four parts:

1) $$\sum_{i,j=0}^{e-1} f_0f_1\,\theta_{p_0,k+j}\,\theta_{p_1,j} = d\delta_{p_0p_1,k};$$

2) $$\begin{aligned}&\sum_{i,j=0}^{e-1} f_0\,\theta_{p_0,k+j} \sum_{s=0}^{e-1} (j,s)_{p_1}\,\eta_{p_1,a_1+i+s} \\ &= f_0 \sum_{j=0}^{e-1} \theta_{p_0,k+t} \sum_{s=0}^{e-1} (j,s)_{p_1} \sum_{i=0}^{e-1} \eta_{p_1,a_1+i+s} = -f_0 \sum_{j=0}^{e-1} \theta_{p_0,k+j}(f_1 - \theta_{p_1,j}) \\ &= -f_0f_1 + f_0\,\delta_{p_0p_1,k};\end{aligned}$$

3) $$\sum_{i,j=0}^{e-1} f_1\,\theta_{p_1,j} \sum_{r=0}^{e-1} (k+j,r)_{p_0}\,\eta_{p_0,a_0+i+r} = -f_0f_1 + f_1\,\delta_{p_0p_1,k};$$

$$4)\quad \sum_{i,j=0}^{e-1}\sum_{r,s=0}^{e-1}(k+j,r)_{p_0}(j,s)_{p_1}\eta_{p_0,a_0+i+r}\eta_{p_1,a_1+i+s}$$

$$=\sum_{j,r,s=0}^{e-1}(k+j,r)_{p_0}(j,s)_{p_1}\sum_{i=0}^{e-1}\eta_{p_0,a_0+(r-s)+i}\eta_{p_1,a_1+i}$$

$$=\sum_{r=0}^{e-1}\Big(\sum_{j,s=0}^{e-1}(k+j,r+s)_{p_0}(j,s)_{p_1}\Big)\eta_{p_0p_1,r}.$$

Hence we find that

$$\eta_{p_0p_1,0}\eta_{p_0p_1,k}=\sum_{r=0}^{e-1}\Big(\sum_{j,s=0}^{e-1}(k+j,r+s)_{p_0}(j,s)_{p_1}\Big)\eta_{p_0p_1,r}-2f_0f_1+\delta_{p_0p_1,k}\Big(\frac{p_0p_1-1}{e}\Big)$$

for $k=0,1,\ldots,e-1$. Equating this expression with that obtained in Lemma 5 we find, upon comparing coefficients, that

$$(k,r)_{p_0p_1}=\sum_{j,s=0}^{e-1}(k+j,r+s)_{p_0}(j,s)_{p_1},$$

the elementwise formulation of the product defined in the theorem.

Note that the entire statement of Lemma 5 and the complete alternative evaluation of the product $\eta_{p_0p_1,0}\eta_{p_0p_1,k}$ by Lemma 4 are not needed for the proof of Theorem 1; for if M is a nonunit in $\boldsymbol{Z}_{p_0p_1}$ its contribution to $\eta_{p_0p_1,0}\eta_{p_0p_1,k}$ is either a constant or a polynomial in λ_{p_0} or λ_{p_1}. Conversely, if M is a unit in $\boldsymbol{Z}_{p_0p_1}$ its contribution to $\eta_{p_0p_1,0}\eta_{p_0p_1,k}$ is a polynomial in $\lambda_{p_0p_1}$ with no terms in λ_{p_0} or λ_{p_1}. Similarly, the sum 4) in the evaluation of $\eta_{p_0p_1,0}\eta_{p_0p_1,k}$ by Lemma 4 is a polynomial in $\lambda_{p_0p_1}$ with no terms in λ_{p_0} or λ_{p_1}, and no other sum in that evaluation contributes a $\lambda_{p_0p_1}$. Hence the theorem is proved upon equating

$$\sum_{j=0}^{e-1}(k,j)_{p_0p_1}\eta_{p_0p_1,j}=\sum_{i,j=0}^{e-1}\sum_{r,s=0}^{e-1}(k+j,r)_{p_0}(j,s)_{p_1}\eta_{p_0,a_0+i+r}\eta_{p_1,a_1+i+s}$$

and comparing coefficients of $\eta_{p_0p_1,n}$, $n=0,1,\ldots,e-1$. The precise statement of Lemma 5, however, is of independent interest, and the proof is included for completeness.

Motivated by the conclusion of Theorem 1, we define a product $*$ for $(e\times e)$-matrices

$$A^{(n)}=\{[a_{i,j}^{(n)}]\colon\ i,j=0,1,\ldots,e-1\},\qquad n=0,1$$

as follows:

$$A^{(0)}*A^{(1)}=B$$

where $B=[b_{i,j}]$ is defined by

$$b_{i,j}=\sum_{r,s=0}^{e-1}a_{i+r,j+s}^{(0)}a_{r,s}^{(1)}.$$

The conclusion of Theorem 1 may then be more compactly written

$$\mathbf{C}_{p_0p_1,e}=\mathbf{C}_{p_0,e}*\mathbf{C}_{p_1,e}.$$

We now use Theorem 1 to derive the elementary cyclotomic relations for domains.

Lemma 6.

(a) $(i+ne,j+me)_{p_0p_1}=(i,j)_{p_0p_1}$ *for all* $m,n\in\boldsymbol{Z}$,

(b) $(i,j)_{p_0p_1}=(e-i,j-i)_{p_0p_1}$,

(c) $$(i,j)_{p_0p_1}=\begin{cases}(j,i)_{p_0p_1} & \textit{if } f_0f_1 \textit{ is odd},\\ (j+e/2,i+e/2)_{p_0p_1} & \textit{if } f_0f_1 \textit{ is even},\end{cases}$$

(d) $\sum_{j=0}^{e-1}(i,j)_{p_0p_1}=\dot{M}+\delta_{p_0p_1,i}$, *where* $e\dot{M}=(p_0-2)(p_1-2)-1$.

Proof. (a) Trivial.

(b) $$(e-i,j-i)_{p_0p_1}=\sum_{k,s=0}^{e-1}(e-i+k,j-i+s)_{p_0}(k,s)_{p_1}$$

$$=\sum_{k,s=0}^{e-1}(i-k,j+s-k)_{p_0}(e-k,s-k)_{p_1}$$

$$=\sum_{k,s=0}^{e-1}(i+k,j+s)_{p_0}(k,s)_{p_1}=(i,j)_{p_0p_1}.$$

(c) If f_0f_1 is odd, then

$$(j,i)_{p_0p_1}=\sum_{k,s=0}^{e-1}(j+k,i+s)_{p_0}(k,s)_{p_1}$$

$$=\sum_{k,s=0}^{e-1}(i+s,j+k)_{p_0}(s,k)_{p_1}=(i,j)_{p_0p_1},$$

while if f_0 is even, f_1 odd, we have

$$(j+e/2,i+e/2)_{p_0p_1}=\sum_{k,s=0}^{e-1}(j+e/2+k,i+e/2+s)_{p_0}(k,s)_{p_1}$$

$$=\sum_{k,s=0}^{e-1}(j+k,i+s)_{p_0}(k+e/2,s+e/2)_{p_1}$$

$$=\sum_{k,s=0}^{e-1}(i+s,j+k)_{p_0}(s,k)_{p_1}=(i,j)_{p_0p_1}.$$

The analysis for f_0 odd, f_1 even is identical.

$$\text{(d)}\quad \sum_{j=0}^{e-1}(i,j)_{p_0p_1} = \sum_{j=0}^{e-1}\sum_{k,s=0}^{e-1}(i+k,j+s)_{p_0}(k,s)_{p_1} = \sum_{k=0}^{e-1}(f_1-\theta_{p_1,k})(f_0-\theta_{p_0,i+k}) = \dot{M}+\delta_{p_0p_1,k}.$$

The next rather specialized result is of importance in the application of the theory of cyclotomy for domains to the existence of finite difference sets in these structures (see [2], p. 110).

LEMMA 7. *When $e = 4$ there are exactly two inequivalent cyclotomic matrices $\mathbf{C}_{p_0p_1,4}$ and $\mathbf{C}^*_{p_0p_1,4}$ for $\mathbf{Z}_{p_0p_1}$, and these differ in their first entry; i.e.,*

$$(0,0)_{p_0p_1} \neq (0,0)^*_{p_0p_1}.$$

Proof. Let $q = 4f+1$ be a prime; then the form of $\mathbf{C}_{q,4}$ is given by Lemma 1 to be

f odd

A	B	C	D
E	E	D	B
A	E	A	E
E	D	B	E

f even

A	B	C	D
B	D	E	E
C	E	C	E
D	E	E	B

and it is known (see [2], p. 48) that, for f odd

$$16B = a-8t, \quad 16D = a+8t,$$

while, for f even

$$16B = b+8t, \quad 16D = b-8t$$

where $a = q+1+2s$ and $b = q-3+2s$, and

$$q = s^2+4t^2, \quad s \equiv 1 \pmod 4,$$

the sign of t depending upon the choice of generator for $\mathbf{Z}_q$. Further if g is a generator of $\mathbf{Z}_q$ then so is g^3, and replacement of g by g^3 interchanges $C_{q,1}$ and $C_{q,3}$, and hence reverses the sign of t.

Now let $g \equiv g_0 \pmod{p_0}$ and $g \equiv g_1 \pmod{p_1}$ be a generator of $\mathbf{Z}_{p_0p_1}$. Then $g^* \equiv g_0^3 \pmod{p_0}$ and $g^* \equiv g_1 \pmod{p_1}$ is also a generator of $\mathbf{Z}_{p_0p_1}$. Suppose that g generates the cyclotomic numbers $(i,j)_{p_0p_1}$ and the cyclotomic matrix $\mathbf{C}_{p_0p_1,4}$, while g^* generates $(i,j)^*_{p_0p_1}$ and $\mathbf{C}^*_{p_0p_1,4}$. We now show that $(0,0)_{p_0p_1} \neq (0,0)^*_{p_0p_1}$, and hence that $\mathbf{C}_{p_0p_1,4}$ and $\mathbf{C}^*_{p_0p_1,4}$ are inequivalent; since there are at most $\varphi(4) = 2$ inequivalent cyclotomic matrices for $\mathbf{Z}_{p_0p_1}$, the lemma will be proved.

By the Corollary to Theorem 1 and the above discussion, we immediately find that

$$16^2[(0,0)_{p_0p_1}-(0,0)^*_{p_0p_1}] = \begin{cases} 3[(B_0B_1+D_0D_1)-(B_0^*B_1^*+D_0^*D_1^*)] & \text{if} \quad f_0f_1 \text{ is odd,} \\ [(B_0B_1+D_0D_1)-(B_0^*B_1^*+D_0^*D_1^*)] & \text{if} \quad f_0f_1 \text{ is even.} \end{cases}$$

Hence it remains to show that $(B_0B_1+D_0D_1)-(B_0^*B_1^*+D_0^*D_1^*) \neq 0$.

To that end, we let $p_0 = s_0^2+4t_0^2$, $s_0 \equiv 1 \pmod 4$ and $p_1 = s_1^2+4t_1^2$, $s_1 \equiv 1 \pmod 4$, so that, for f_0 odd

$$16B_0 = a_0-8t_0, \quad 16B_0^* = a_0+8t_0,$$
$$16D_0 = a_0+8t_0, \quad 16D_0^* = a_0-8t_0,$$

while, for f_0 even

$$16B_0 = b_0+8t_0, \quad 16B_0^* = b_0-8t_0,$$
$$16D_0 = b_0-8t_0, \quad 16D_0^* = b_0+8t_0,$$

where $a_0 = p_0+1+2s_0$ and $b_0 = p_0-3+2s_0$. Similarly, if f_1 is odd

$$16B_1 = 16B_1^* = a_1-8t_1, \quad 16D_1 = 16D_1^* = a_1+8t_1,$$

while, if f_1 is even

$$16B_1 = 16B_1^* = b_1+8t_1, \quad 16D_1 = 16D_1^* = b_1-8t_1,$$

where $a_1 = p_1+1+2s_1$ and $b_1 = p_1-3+2s_1$. Hence, if f_0f_1 is odd,

$$(B_0B_1+D_0D_1)-(B_0^*B_1^*+D_0^*D_1^*) = (B_0-B_0^*)B_1+(D_0-D_0^*)D_1 = -16t_0(B_1-D_1) = 16^2t_0t_1;$$

if f_0 is even,

$$(B_0-B_0^*)B_1+(D_0-D_0^*)D_1 = 16t_0(B_1-D_1) = -16^2t_0t_1;$$

and, if f_1 is even,

$$(B_0-B_0^*)B_1+(D_0-D_0^*)D_1 = -16t_0(B_1-D_1) = -16^2t_0t_1.$$

Hence

$$[(0,0)_{p_0p_1}-(0,0)^*_{p_0p_1}] = \begin{cases} 3t_0t_1 & \text{if} \quad f_0f_1 \text{ is odd,} \\ -t_0t_1 & \text{if} \quad f_0f_1 \text{ is even,} \end{cases}$$

and $t_0t_1 \neq 0$ since p_0 and p_1 have no improper representations as the sum of two squares.

4. Arithmetic functions on domains. When e divides none of m, n, nor $m+n$, we define the functions of Jacobi and Lagrange for the domains $\mathbf{Z}_{p_0p_1}$ as follows:

$$F_{p_0p_1}(\lambda_e^m) = \sum_{k=0}^{e-1}\lambda_e^{mk}\eta_{p_0p_1,k}$$

and

$$R_{p_0p_1}(m, n) = \sum_{k=0}^{e-1} \lambda_e^{nk} \sum_{h=0}^{e-1} \lambda_e^{-(m+n)h} (k, h)_{p_0p_1}.$$

The following theorem relates the functions $R_{p_0p_1}$ to the oridinary Lagrange functions R_{p_0} and R_{p_1}.

THEOREM 2.

$$R_{p_0p_1}(m, n) = R_{p_0}(m, n) R_{p_1}(-m, -n).$$

Proof.

$$\begin{aligned} R_{p_0p_1}(m, n) &= \sum_{k=0}^{e-1} \lambda_e^{nk} \sum_{h=0}^{e-1} \lambda_e^{-(m+n)h} (k, h)_{p_0p_1} \\ &= \sum_{k=0}^{e-1} \lambda_e^{nk} \sum_{h=0}^{e-1} \lambda_e^{-(m+n)h} \sum_{j,s=0}^{e-1} (k+j, h+s)_{p_0} (j, s)_{p_1} \\ &= \Big(\sum_{k=0}^{e-1} \lambda_e^{nk} \sum_{h=0}^{e-1} \lambda_e^{-(m+n)h} (k, h)_{p_0}\Big) \Big(\sum_{j=0}^{e-1} \lambda_e^{-nj} \sum_{s=0}^{e-1} \lambda_e^{(m+n)s} (j, s)_{p_1}\Big) \\ &= R_{p_0}(m, n) R_{p_1}(-m, -n). \end{aligned}$$

The well known properties of the functions $R_{p_0p_1}(m, n)$ (see [2], p. 100) are immediate corollaries of Theorem 2 and the corresponding properties of the functions $R_{p_0}(m, n)$ and $R_{p_1}(m, n)$.

We now prove a corresponding result for the functions $F_{p_0p_1}(\lambda_e^m)$.

THEOREM 3.

$$F_{p_0p_1}(\lambda_e^m) = \lambda_e^{m(a_1-a_0)} F_{p_0}(\lambda_e^m) F_{p_1}(\lambda_e^{-m}).$$

Proof.

$$\begin{aligned} F_{p_0p_1}(\lambda_e^m) &= \sum_{j=0}^{e-1} \lambda_e^{mj} \eta_{p_0p_1,j} = \sum_{j=0}^{e-1} \lambda_e^{mj} \sum_{i=0}^{e-1} \eta_{p_0,a_0+j+i} \eta_{p_1,a_1+i} \\ &= \lambda_e^{m(a_1-a_0)} \Big(\sum_{j=0}^{e-1} \lambda_e^{mj} \eta_{p_0,j}\Big) \Big(\sum_{i=0}^{e-1} \lambda_e^{-mi} \eta_{p_1,i}\Big) \\ &= \lambda_e^{m(a_1-a_0)} F_{p_0}(\lambda_e^m) F_{p_1}(\lambda_e^{-m}). \end{aligned}$$

COROLLARY 1.

$$F_{p_0p_1}(-1) = (-1)^{2e+a_1-a_0} F_{p_0}(-1) F_{p_1}(-1).$$

COROLLARY 2.

$$F_{p_0p_1}(-\lambda_e^k) = (-1)^{2e+a_1-a_0} \lambda_e^{k(a_1-a_0)} F_{p_0}(-\lambda_e^k) F_{p_1}(-\lambda_e^{-k}).$$

Other immediate corollaries to Theorem 3 are the usual properties of the functions $F_{p_0p_1}(\lambda_e^m)$ (see [2], pp. 99-100); in particular, the F's and R's are related as in $\boldsymbol{Z}_{p_0}$ (see Lemma 3(a)) as we now show.

COROLLARY 3.

$$R_{p_0p_1}(m, n) = \frac{F_{p_0p_1}(\lambda_e^m) F_{p_0p_1}(\lambda_e^n)}{F_{p_0p_1}(\lambda_e^{m+n})}.$$

Proof.

$$\begin{aligned} R_{p_0p_1}(m, n) &= R_{p_0}(m, n) R_{p_1}(-m, -n) \\ &= \left(\frac{F_{p_0}(\lambda_e^m) F_{p_0}(\lambda_e^n)}{F_{p_0}(\lambda_e^{m+n})}\right) \left(\frac{F_{p_1}(\lambda_e^{-m}) F_{p_1}(\lambda_e^{-n})}{F_{p_1}(\lambda_e^{-(m+n)})}\right) \\ &= \frac{\lambda_e^{-m(a_1-a_0)} F_{p_0p_1}(\lambda_e^m) \lambda_e^{-n(a_1-a_0)} F_{p_0p_1}(\lambda_e^n)}{\lambda_e^{-(m+n)(a_1-a_0)} F_{p_0p_1}(\lambda_e^{m+n})} \\ &= \frac{F_{p_0p_1}(\lambda_e^m) F_{p_0p_1}(\lambda_e^n)}{F_{p_0p_1}(\lambda_e^{m+n})}. \end{aligned}$$

We now use Theorem 3 and its Corollaries 1 and 2 to prove an analogue of Jacobi's Lemma 3 (b) for the domains $\boldsymbol{Z}_{p_0p_1}$.

LEMMA 8. *Define the natural numbers l_0 and l_1 by*

$$g^{l_0} \equiv 2 \pmod{p_0} \quad \textit{and} \quad g^{l_1} \equiv 2 \pmod{p_1}.$$

Then

$$F_{p_0p_1}(-1) F_{p_0p_1}(\lambda_e^{2k}) = \lambda_e^{2(l_0-l_1)k} F_{p_0p_1}(\lambda_e^k) F_{p_0p_1}(-\lambda_e^k).$$

Proof. From Theorem 3 and its first corollary, we have

$$\begin{aligned} &F_{p_0p_1}(-1) F_{p_0p_1}(\lambda_e^{2k}) \\ &\qquad = (-1)^{2e+a_1-a_0} \lambda_e^{2k(a_1-a_0)} F_{p_0}(-1) F_{p_0}(\lambda_e^{2k}) F_{p_1}(-1) F_{p_1}(\lambda_e^{-2k}). \end{aligned}$$

But, by Lemma 3 (b) this expression is equal to

$$\lambda_e^{2(l_0-l_1)k} \big(\lambda_e^{k(a_1-a_0)} F_{p_0}(\lambda_e^k) F_{p_1}(\lambda_e^{-k})\big) \big((-1)^{2e+a_1-a_0} \lambda_e^{k(a_1-a_0)} F_{p_0}(-\lambda_e^k) F_{p_1}(-\lambda_e^{-k})\big)$$

which, by Theorem 3 and its second corollary is equal to

$$\lambda_e^{2(l_0-l_1)k} F_{p_0p_1}(\lambda_e^k) F_{p_0p_1}(-\lambda_e^k).$$

The conclusion of Lemma 8, for an ordering on p_1, becomes

$$F_{p_0p_1}(-1) F_{p_0p_1}(\lambda_e^{2k}) = \lambda_e^{2(l_1-l_0)k} F_{p_0p_1}(\lambda_e^k) F_{p_0p_1}(-\lambda_e^k),$$

and the corresponding statement of Theorem 2 is

$$R_{p_0p_1}(m, n) = R_{p_0}(-m, -n) R_{p_1}(m, n).$$

5. Galois Domains, II. We conclude with an indication of the results for the general case. Let $N = \prod_{i=0}^{n} p_i$, where the $p_i = ef_i+1$ are $(n+1)$ distinct primes such that the f_i are pairwise relatively prime; let g be a common primitive root of the p_i, and define

$$x_i \equiv \begin{cases} g\,(\mathrm{mod} p_i), \\ 1\,\big(\mathrm{mod} \prod_{j\neq i} p_j\big). \end{cases}$$

Further, if $m_0, m_1, \ldots, m_n$ are integers such that

$$\sum_{i=0}^{n}\Big(\prod_{j\neq i} p_j\Big)\, m_i = 1,$$

define the natural numbers $a_0, a_1, \ldots, a_n$ by

$$m_i \epsilon C_{p_i,a_i}, \qquad i = 0, 1, \ldots, n.$$

Lemma 9. *If $d = e\prod_{i=0}^{n} f_i$ and $\bar{k} = (k_0, k_1, \ldots, k_{n-1}, k_n)$, where $k_n = 0$, we define*

$$C_{N,\bar{k}} = \sum_{j=0}^{e-1}\prod_{i=0}^{n} C_{p_i,a_1+k_i+j};$$

then

$$C_{N,\bar{k}} = \Big\{g^s \prod_{i=0}^{n-1} x_j^{k_i}\,(\mathrm{mod}\ N)\colon\ s = 0, 1, \ldots, d-1\Big\}$$

for all $k_i = 0, 1, \ldots, e-1$.

Proof. We have,

$$1 \epsilon C_{N,a_0,a_1,\ldots,a_{n-1}}$$

by definition,

$$g \epsilon C_{N,a_0+1,a_1+1,\ldots,a_{n-1}+1}, \qquad \text{and} \qquad x_i \epsilon C_{N,a_0,a_1,\ldots,a_{i-1},a_i+1,\ldots,a_{n-1}},$$

whence the proof follows from the method of the proof of Lemma 4.

The cyclotomic number $(\bar{k}^{(0)}, \bar{k}^{(1)})_N$ is defined to be the number of solutions of the equation

$$Z_{\bar{k}^{(0)}}+1 \equiv Z_{\bar{k}^{(1)}}\ (\mathrm{mod}\ N); \qquad Z_{\bar{k}^{(0)}} \epsilon C_{N,\bar{k}^{(0)}}, \qquad Z_{\bar{k}^{(1)}} \epsilon C_{N,\bar{k}^{(1)}};$$

i.e., the number of ordered pairs (s, t), with $0 \leqslant s, t < d-1$, such that

$$g^s \prod_{i=0}^{n-1} x_i^{k_i^{(0)}} + 1 \equiv g^t \prod_{j=0}^{n-1} x_j^{k_j^{(1)}}\ (\mathrm{mod}\ N).$$

We then have the following generalization of Theorem 1.

Theorem 4. *If P and Q are the permutation matrices*

$$P = \mathrm{Circ}\overbrace{(0, 1, 0, \ldots, 0)}^{e} = \left(\begin{array}{c|c} 0 & I_{e-1} \\ \hline 1 & 0 \end{array}\right),\ Q = \mathrm{Circ}\overbrace{(0, 0, \ldots, 0, 1)}^{e} = \left(\begin{array}{c|c} 0 & 1 \\ \hline I_{e-1} & 0 \end{array}\right),$$

then

$$(\bar{k}^{(0)}, \bar{k}^{(1)})_N = \mathop{\bullet}\limits_{i=0}^{n} (P_i^{k_i^{(0)}} \mathbf{C}_{p_i,e} Q^{k_i^{(1)}}),$$

where $k_n^{(0)} = k_n^{(1)} = 0$, $P^0 = Q^0 = I_e$, and ● denotes the inner product of the $(n+1)$ matrices.

Proof. We define the periods for $\boldsymbol{Z}_N$ by

$$\eta_{N,\bar{k}} = \sum_{b \epsilon C_{N,\bar{k}}} \lambda_N^b,$$

and then use the direct method of Lemma 5 and the implicit method in the proof of Theorem 1 to give two expressions for the coefficients of the primitive Nth roots of unity in the evaluation of the product $\eta_{N,\bar{0}}\eta_{N,\bar{k}^{(0)}}$. Equating coefficients of like terms yields

$$(\bar{k}^{(0)}, \bar{k}^{(1)})_N = \sum_{t,r=0}^{e-1}\Big(\prod_{i=0}^{n} (k_i^{(0)}+t, k_i^{(1)}+r)_{p_i}\Big)$$

for all ordered n-tuples $\bar{k}^{(0)}, \bar{k}^{(1)}$ with $0 \leqslant k_i^{(0)}, k_i^{(1)} \leqslant e-1$, and $i = 0, 1, \ldots$ $\ldots, n-1$; always, $k_n^{(0)} = k_n^{(1)} = 0$. This is the elementwise formulation of the matrix product defined in the theorem.

Corollary.

$$(\bar{0}, \bar{0})_N = \mathop{\bullet}\limits_{i=0}^{n} \mathbf{C}_{p_i,e}.$$

For the ordered $(n+1)$-tuples $\bar{k}^{(0)}$ and $\bar{k}^{(1)}$, we define $\bar{k}^{(0)}+\bar{k}^{(1)}$ and $a\bar{k}^{(0)}$ coordinatewise, and we let $\bar{e}^{(i)}/2$ be the $(n+1)$-tuple whose ith coordinate is $e/2$ and whose remaining n coordinates are all 0. The cyclotomic structure of $\boldsymbol{Z}_N$ will be given in Lemma 10, below. First note that, since

$$\prod_{i=0}^{n} \varphi(p_i-1) = [\varphi(e)]^n \varphi(d),$$

there are at most $[\varphi(e)]^n$ distinct cyclotomic matrices definable for $\boldsymbol{Z}_N$.

LEMMA 10.

(a) $(\bar{k}^{(0)}+a\bar{e},\ \bar{k}^{(1)}+b\bar{e})_N = (\bar{k}^{(0)},\ \bar{k}^{(1)})_N$ *for all* $a, b \in \boldsymbol{Z}$,

(b) $(\bar{k}^{(0)},\ \bar{k}^{(1)})_N = (\bar{e}-\bar{k}^{(0)},\ \bar{k}^{(1)}-\bar{k}^{(0)})_N$,

(c) $$(\bar{k}^{(0)},\ \bar{k}^{(1)})_N = \begin{cases} (\bar{k}^{(1)},\ \bar{k}^{(0)})_N & \textit{if} \ \prod\limits_{i=0}^{n} f_i \ \textit{is odd}, \\ (\bar{k}^{(1)}+\bar{e}^{(i)}/2,\ \bar{k}^{(0)}+\bar{e}^{(i)}/2)_N & \textit{if} \ f_i \ \textit{is even}, \ i<n, \\ (\bar{k}^{(1)}+\bar{e}/2,\ \bar{k}^{(0)}+\bar{e}/2)_N & \textit{if} \ f_n \ \textit{is even}, \end{cases}$$

(d) $\sum\limits_{\bar{k}^{(1)}=0}^{e-1}(\bar{k}^{(0)},\ \bar{k}^{(1)})_N = \sum\limits_{t=0}^{e-1}\Big(\prod\limits_{i=0}^{n}(f_i-\theta_{p_i,k_i^{(0)}+t})\Big)$, *where the sum over* $\bar{k}^{(1)}$ *means "as* $\bar{k}^{(1)}$ *runs over all* $(n+1)$*-tuples whose entries lie between* 0 *and* $e-1$*, inclusive".*

Proof. (a) Obvious.

(b) $$(\bar{e}-\bar{k}^{(0)},\ \bar{k}^{(1)}-\bar{k}^{(0)})_N = \sum_{t,r=0}^{e-1}\Big(\prod_{i=0}^{n}(e-k_i^{(0)}+t,\ k_i^{(1)}-k_i^{(0)}+r)_{p_i}\Big)$$
$$= \sum_{t,r=0}^{e-1}\Big(\prod_{i=0}^{n}(k_i^{(0)}-t,\ k_i^{(1)}+r-t)_{p_i}\Big)$$
$$= (\bar{k}^{(0)},\ \bar{k}^{(1)})_N.$$

(c) If f_i is even, then

$$(\bar{k}^{(1)}+\bar{e}^{(i)}/2,\ \bar{k}^{(0)}+\bar{e}^{(i)}/2)_N$$
$$= \sum_{t,r=0}^{e-1}\Big(\prod_{\substack{j=0\\ j\neq i}}^{n}(k_j^{(1)}+t,\ k_j^{(0)}+r)_{p_j}\Big)(k_i^{(1)}+e/2+t,\ k_i^{(0)}+e/2+r)_{p_i}$$
$$= \sum_{r,t=0}^{e-1}\Big(\prod_{j=0}^{n}(k_j^{(0)}+r,\ k_j^{(1)}+t)_{p_j}\Big) = (\bar{k}^{(0)},\ \bar{k}^{(1)})_N.$$

The remaining cases are entirely similar.

(d) $$\sum_{\bar{k}^{(1)}=0}^{e-1}(\bar{k}^{(0)},\ \bar{k}^{(1)})_N = \sum_{\bar{k}^{(1)}=0}^{e-1}\Big\{\sum_{t,r=0}^{e-1}\Big(\prod_{i=0}^{n}(k_i^{(0)}+t,\ k_i^{(1)}+r)_{p_i}\Big)\Big\}$$
$$= \sum_{t,r=0}^{e-1}\Big(\prod_{i=0}^{n-1}(f_i-\theta_{p_i,k_i^{(0)}+t})\Big)(t,\ r)_{p_n}$$
$$= \sum_{t=0}^{e-1}\Big(\prod_{i=0}^{n}(f_i-\theta_{p_i,k_i^{(0)}+t})\Big).$$

We conclude with a few brief remarks concerning arithmetic functions on $\boldsymbol{Z}_N$. If

$$\bar{k} = (k_0, k_1, \ldots, k_{n-1}, k_n = 0),$$

then we define

$$|\bar{k}| = \sum_{i=0}^{n} k_i.$$

Further, if $n \not\equiv 1 \pmod{e}$, and if none of the natural numbers m_0, m_1, nor m_0+m_1 is divisible by e, we define the functions

$$F_N(\lambda_e^{m_0}) = \sum_{\bar{k}=0}^{e-1}\lambda_e^{m_0|\bar{k}|}\,\eta_{N,\bar{k}}$$

and

$$R_N(m_0, m_1) = \sum_{\bar{k}^{(0)}=0}^{e-1}\lambda_e^{m_1|\bar{k}^{(0)}|}\sum_{\bar{k}^{(1)}=0}^{e-1}\lambda_e^{-(m_0+m_1)|\bar{k}^{(1)}|}(\bar{k}^{(0)},\ \bar{k}^{(1)})_N,$$

and prove, as in Theorems 2 and 3, that

$$F_N(\lambda_e^{m_0}) = \lambda_e^{-m_0[\sum\limits_{i=0}^{n-1}a_i-(n-1)a_n]}\prod_{i=0}^{n-1}F_{p_i}(\lambda_e^{m_0})F_{p_n}(\lambda_e^{-(n-1)m_0})$$

and

$$R_N(m_0, m_1) = \frac{F_N(\lambda_e^{m_0})F_N(\lambda_e^{m_1})}{F_N(\lambda_e^{m_0+m_1})}$$
$$= \prod_{i=0}^{n-1}R_{p_i}(m_0, n_0)R_{p_n}[-(n-1)m_0,\ -(n-1)m_1].$$

Analogues of the usual properties for the F's and the R's in $\boldsymbol{Z}_{p_0}$ and $\boldsymbol{Z}_{p_0p_1}$ may easily be developed for the structure $\boldsymbol{Z}_N$ from the above. In particular, if $n \equiv 0 \pmod{2}$, the method of Lemma 8 can be used to prove a direct analogue of Jacobi's Lemma for $\boldsymbol{Z}_N$.

LEMMA 11. *Let* $g^{l_i} \equiv 2 \pmod{p_i}$ *for* $i = 0, 1, \ldots, n$. *Then*

$$F_N(-1)F_N(\lambda_e^{2s}) = \lambda_e^{2s[\sum\limits_{i=0}^{n-1}l_i-(n-1)l_n]}F_N(\lambda_e^{s})F_N(-\lambda_e^{s}).$$

Finally, as an application of the general theory, we derive the sole class structure theorem known for Galois domains whose order is a product of more than two distinct primes (see [1]).

For $e=2$, the cyclotomic matrices $\mathbf{C}_{p,2}$ for f even or odd are given directly by Lemma 1:

$$\mathbf{C}_{p,2}:\quad \underset{f \text{ even}}{\begin{array}{|c|c|}\hline \frac{p-5}{4} & \frac{p-1}{4} \\ \hline \frac{p-1}{4} & \frac{p-1}{4} \\ \hline \end{array}} \qquad \underset{f \text{ odd}}{\begin{array}{|c|c|}\hline \frac{p-3}{4} & \frac{p+1}{4} \\ \hline \frac{p-3}{4} & \frac{p-3}{4} \\ \hline \end{array}}$$

and, if p_0, p_1, and p_2 are distinct odd primes with

$$e = \text{l.c.m.}\langle \text{g.c.d.}(p_0-1, p_1-1), \text{g.c.d.}(p_0-1, p_2-1), \text{g.c.d.}(p_1-1, p_2-1)\rangle = 2,$$

then, by the Corollary to Theorem 7,

$$(0,0;0,0)_{p_0p_1p_2} = \mathbf{C}_{p_0,2}\cdot\mathbf{C}_{p_1,2}\cdot\mathbf{C}_{p_2,2}.$$

We proceed to an explicit evaluation.

LEMMA 12. *Let*

$$e = 2 \quad \textit{and} \quad \dot{M} = (p_0-2)(p_1-2)(p_2-2)+p_0+p_1+p_2-8;$$

then

$$16(0,0;0,0)_{p_0p_1p_2} = \begin{cases} \dot{M}+2(p_0+p_1+p_2)-4 & \textit{if} \quad f_0f_1f_2 \textit{ is odd}, \\ \dot{M}+2p_0 & \textit{if} \quad f_0 \textit{ is even}, \\ \dot{M}+2p_1 & \textit{if} \quad f_1 \textit{ is even}, \\ \dot{M}+2p_2 & \textit{if} \quad f_2 \textit{ is even}. \end{cases}$$

Proof. Here there is exactly $[\varphi(2)]^2 = 1$ distinct cyclotomic matrix for $\mathbf{Z}_{p_0p_1p_2}$, and the entry $(0,0;0,0)_{p_0p_1p_2}$ of this matrix is given by the Corollary to Theorem 7.

Hence we find that

$$(0,0;0,0)_{p_0p_1p_2} = \mathbf{C}_{p_0,2}\cdot\mathbf{C}_{p_1,2}\cdot\mathbf{C}_{p_2,2}$$

takes the following values.

Case I. $f_0f_1f_2$ odd. Then

$$\begin{aligned}\mathbf{C}_{p_0,2}\cdot\mathbf{C}_{p_1,2}\cdot\mathbf{C}_{p_2,2} &= 3\left(\frac{p_0-3}{4}\right)\left(\frac{p_1-3}{4}\right)\left(\frac{p_2-3}{4}\right)+\left(\frac{p_0+1}{4}\right)\left(\frac{p_1+1}{4}\right)\left(\frac{p_2+1}{4}\right) \\ &= \tfrac{1}{16}[(p_0-2)(p_1-2)(p_2-2)+3(p_0+p_1+p_2)-12] \\ &= \tfrac{1}{16}[\dot{M}+2(p_0+p_1+p_2)-4].\end{aligned}$$

Case II. One of $f_0f_1f_2$ even. Suppose f_0 is even; then

$$\begin{aligned}\mathbf{C}_{p_0,2}\cdot\mathbf{C}_{p_1,2}\cdot\mathbf{C}_{p_2,2} &= \left(\frac{p_0-5}{4}\right)\left(\frac{p_1-3}{4}\right)\left(\frac{p_2-3}{4}\right)+\left(\frac{p_0-1}{4}\right)\left(\frac{p_1+1}{4}\right)\left(\frac{p_2+1}{4}\right)+ \\ &\quad +2\left(\frac{p_0-1}{4}\right)\left(\frac{p_1-3}{4}\right)\left(\frac{p_2-3}{4}\right) \\ &= \tfrac{1}{16}[(p_0-2)(p_1-2)(p_2-2)+3p_0+p_1+p_2-8] \\ &= \tfrac{1}{16}(\dot{M}+2p_0).\end{aligned}$$

If f_1 is even, $\mathbf{C}_{p_0,2}\cdot\mathbf{C}_{p_1,2}\cdot\mathbf{C}_{p_2,2}$ is the first sum of products on the right above with the subscripts 0 and 1 interchanged. Since $\dot{M}$ is invariant under permutations of its subscripts, we have

$$\mathbf{C}_{p_0,2}\cdot\mathbf{C}_{p_1,2}\cdot\mathbf{C}_{p_2,2} = \begin{cases} \frac{1}{16}(\dot{M}+2p_1) & \text{if } f_1 \text{ is even}, \\ \frac{1}{16}(\dot{M}+2p_2) & \text{if } f_2 \text{ is even}, \end{cases}$$

and combination of the above results gives the lemma.

References

[1] L. Carlitz and A. L. Whiteman, *The number of solutions of some congruences modulo a product of primes*, Trans. Amer. Math. Soc. 112 (1964), pp. 536-552.

[2] T. Storer, *Cyclotomy and Difference Sets*, Markham 1967.

UNIVERSITY OF MICHIGAN

Reçu par la Rédaction le 23. 2. 1968