PARTITION RINGS OF CYCLIC GROUPS OF ODD PRIME POWER ORDER[1]

K. I. APPEL

A ring R over a commutative ring K, that has a basis of elements $g_1, g_2, \ldots, g_n$ forming a group G under multiplication, is called a *group ring* of G over K. Since all group rings of a given G over a given K are isomorphic, we may speak of the group ring KG of G over K.

Let π be any partition of G into non-empty sets $G_A, G_B, \ldots$. Any subring P of KG that has a basis of elements

$$A = \sum_{g \in G_A} m_g g, \ldots, m_g \neq 0 \text{ in } K,$$

is a *partition ring* of G over K.

If P is a partition ring of G over Z, the ring of integers, then the basis $A, B, \ldots$ for P clearly serves as a basis for a partition ring $P' = Q \otimes P$ of G over Q, the field of rationals. If, in addition, for each $A, B, \ldots$ the coefficients m_g, all $g \in G_A$, have no common factor, we shall call $A, B, \ldots$ a *reduced integral basis* for P'.

LEMMA. *Every partition ring P over the rationals has a reduced integral basis.*

By hypothesis, the ring P has a basis of elements

$$A = \sum_{g \in G_A} (u_g/v_g) g$$

where u_g, v_g are non-zero integers. We can write $A = (u_A/v_A) \Sigma m_g g$ where the $m_g \neq 0$ are integers without any common factor. Then the $A' = \Sigma m_g g$ forms a basis for P, and it remains to show that in the multiplication table,

$$A'_i A'_j = \sum b_{ij}{}^k A'_k,$$

the rationals $b_{ij}{}^k$ are in fact all integers. Fix i, j, and k, and consider $g \in G_{A_k}$. Since all coefficients on the left are clearly integers, the same is true on the right, and $b_{ij}{}^k m_g$ is an integer for each $g \in G_{A_k}$. Since the m_g have no common factor, this requires that $b_{ij}{}^k$ be an integer.

Henceforth, by partition ring we mean integral partition ring over the rationals, and by basis, we mean reduced integral basis, We will also adopt the convention that basis elements be chosen such that for each G_A at least one m_g is positive.

Received September 1, 1959; in revised form March 24, 1960.

[1]This paper is based on a portion of a dissertation submitted to the Graduate School of the University of Michigan in partial fulfilment of the requirements for the Ph.D. degree. The author wishes to thank Professor R. C. Lyndon for his advice and encouragement.

Let G be a finite abelian group. For each integer y prime to the order of G, define (y) to be the map $g \to g^y$ for each g in G. Then (y) is an automorphism of G, and we will call the automorphisms of this type the power automorphisms of G.

THEOREM 1. *Let G be a finite abelian group, and y an integer prime to the order n of G. Let A be a basis element of a partition ring P of G. Then there exists an element B, of the same basis, such that*

$$A^{(y)} = \sum_{g \in G_A} m_g g^y = \pm B.$$

Proof. First, we show that $G_A{}^{(y)} = \{g^y | g \in G_A\}$ is a union of partition classes under the partition induced by P. Assume not. Then there exists a basis element $D = ag_0{}^y + bg_1 + \ldots$ where $g_0 \in G_A$, $g_1 \neq g^y$ for any g in G_A. (Here we use $\ldots$ in a special sense meaning that a and b are the full coefficients of $g_0{}^y$ and g_1 respectively, that is, the elements occurring in the remaining terms of the sum are distinct from $g_0{}^y$ and g_1. In similar contexts the same convention is employed.)

Now we employ the theorem of Dirichlet that if j and k are relatively prime there exist infinitely many primes congruent to j modulo k. Since $(y, n) = 1$, by Dirichlet's theorem, we may choose $q \equiv y \pmod{n}$ such that $q > |m_g|$, all $g \in G_A$, $q > |b|$, q prime. But, modulo q,

$$A^q \equiv A^{(q)} = A^{(y)} = \sum_{g \in G_A} m_g g^y.$$

Since (y) is an automorphism of G, $g_1 \neq g_2$ implies $g_1{}^y \neq g_2{}^y$.

A^q must be a sum of basis elements of P. Therefore $A^q = ug_0{}^y + \ldots$, $A^q = kD + \ldots = kag_0{}^y + kbg_1 + \ldots$. However, $g_1 \neq g^y$ for any g in G_A so $q | kb$, and since $q > |b|$, $q | k$. But

$$ka \equiv m_{g_0} \pmod{q}$$

and

$$|m_{g_0}| < q, \; m_{g_0} \neq 0 \text{ so } q \nmid ka,$$

which is a contradiction.

Next, we show that $G_A{}^{(y)}$ is a partition set of the partition induced by P. Suppose not. Let $G_A{}^{(y)} = G_B \cup G_C \cup \ldots$. Let $yz \equiv 1 \pmod{n}$. Then $G_B{}^{(z)} \subset G_A{}^{(yz)} = G_A$. Since by the above, $g_B{}^{(z)}$ is a union of partition classes while G_A is a single partition class this implies that $G_B{}^{(z)} = G_A$ and $G_A{}^{(y)} = G_B$.

Write

$$B = \sum_{g \in G_A} n_g g^y$$

for the basis element corresponding to the partition class $G_A{}^{(y)}$. If q is a prime with $q \equiv y \pmod{n}$,

$$A^q = \Big(\sum_{g \in G_A} m_g g \Big)^q \equiv \sum_{g \in G_A} m_g g^y \pmod{q}.$$

https://doi.org/10.4153/CJM-1961-032-4 Published online by Cambridge University Press

It follows that B appears in the product A^q with non-zero coefficient, say

$$A^q = \lambda(q)B + \ldots = \sum_{g \in G_A} \lambda(q) n_g g^y + \ldots$$

for some integer $\lambda(q) \not\equiv 0 \pmod{q}$. If G_A has only a single element g_0, then $m_g = \pm 1$, $n_g = \pm 1$, and the conclusion follows. Otherwise, let $g, h \in G_A$, $g \neq h$. From the above we have $\lambda(q)n_g \equiv m_g \pmod{q}$, $\lambda(q)n_h \equiv m_h \pmod{q}$ whence $m_h n_g \equiv m_g n_h \pmod{q}$. This holds for infinitely many primes $q \equiv y \pmod{n}$, whence $m_h n_g = m_g n_h$, and there exists λ such that $m_g = \lambda n_g$ for all $g \in G_A$. Let $\lambda = r/s$, $(r, s) = 1$ and suppose $|s| \neq 1$. Then some prime t divides s, and therefore t divides each n_g, contrary to the fact that the greatest common divisor of the $n_g = 1$. Hence $|s| = 1$. Now each m_h is divisible by r, so $|r| = 1$, and hence $\lambda = \pm 1$.

If G is cyclic, every automorphism is a power automorphism. We assume henceforth that G is a cyclic group of odd prime power order p^e. Then its automorphism group is cyclic and contains an automorphism mapping g into g^2.

Let

$$z(a) = G^{p^a} = \{g^{p^a} | g \in G\}.$$

The lattice of subgroups of G is a chain of characteristic subgroups:

$$G = Z(0) \supset Z(1) \supset \ldots \supset Z(e-1) \supset Z(e) = 1.$$

Define $C(a)$ to be the set difference $Z(a) - Z(a+1)$ for $e > a$, and $C(e) = Z(e) = 1$. We could alternatively define $C(a)$ as the set of g^t such that g is a generator of G and $t \equiv 0 \pmod{p^a}$, and $t \not\equiv 0 \pmod{p^{a+1}}$. We refer to the $C(a)$ as the *levels* of G.

Since the $Z(a)$ are characteristic subgroups of G, each $Z(a)$ and consequently each $C(a)$ is fixed under every automorphism of G.

If we define $G_A(a)$ as the intersection of G_A and $C(a)$, then by Theorem 1, if g_1 and g_2 are elements of $G_A(a)$ it follows that $m_{g_1} = \pm m_{g_2}$, for we can find an automorphism (y) which maps g_1 into g_2.

Let Y be the group of automorphisms of G. If A is a basis element of P, let Y_A be the subgroup of Y which leaves G_A fixed, that is

$$Y_A = \{(y) \in Y | A^{(y)} = \pm A\}.$$

We define the *spectrum of the set* G_A of the partition induced by P as $\mathrm{Sp}(G_A) = \{a | G_A(a) \neq 0\}$. Thus, the spectrum of a set is the collection of integers corresponding to levels intersected by the set. We define two basis elements B and D to be conjugate if $B = D^{(w)}$ for $(w) \in Y$.

If two basis elements are conjugate, their induced partition sets have the same spectra. Also, if two partition sets have intersecting spectra, there is an automorphism (y) of G mapping an element of one into an element of the other, and hence mapping the sets into each other. Thus, we can state:

LEMMA 1.1. *If the spectra of* G_A *and* G_B *intersect, then* $\mathrm{Sp}(G_A) = \mathrm{Sp}(G_B)$.

https://doi.org/10.4153/CJM-1961-032-4 Published online by Cambridge University Press

Now we will prove a corollary to Theorem 1.

COROLLARY. *Let G be a cyclic group of odd prime power order, and let P be a partition ring of G. There exists a basis for P such that if A is an element of this basis so is $A^{(y)}$ for any y prime to the order of G.*

Consider any basis for P. Choose $A_1, \ldots, A_k$ a maximal set of elements of this basis such that no A_i is conjugate to $\pm A_j$ for $i \neq j$. Let B be the set of all distinct $A_i{}^{(y)}$ for $(y) \in Y$. Clearly, if no $A_i{}^{(w)} = -A_i{}^{(z)}$ for (w), $(z) \in Y$, then B is a basis for P. Suppose that $A_i{}^{(w)} = -A_i{}^{(z)}$ for (w), $(z) \in Y$. Then

$$A_i{}^{(wz^{-1})} = -A_i.$$

We will now show that this is impossible.

First, we introduce the following notation. If W is any expression of the form

$$\sum_{g \in G_W} m_g g$$

where G_W is a subset of the elements of G and the m_g are integers, we define $|W|$ as

$$\sum_{g \in G_W} m_g.$$

If K is a set of elements, we let $|K|$ be the cardinal of the set. For $0 \leqslant z \leqslant e$, we define

$$W(a) = \sum_{g \in G_W \cap C(a)} (m_g g).$$

Let basis element

$$A = \sum_{g \in G_A} m_g g.$$

By Theorem 1, there exist integers m_a, and integers $\alpha_g = \pm 1$ such that

$$A = \sum_{a \in \mathrm{Sp}(G_A)} m_a \sum_{g \in G_A(a)} \alpha_g g.$$

Assume $A^{(u)} = -A$, $(u) \in Y_A$. First, we note that (u) and hence Y_A have even order, and second that for $g \in G_A$, precisely half of the α_g are -1.

Let b be the smallest integer in the spectrum of G_A. We may write $A = D + E$ where D is a linear combination of elements of $C(b)$ while E is a linear combination of elements of $Z(b+1)$. We note that $|D| = |E| = 0$.

Since $A^2(b)$ is a linear combination of conjugates of D, $|A^2(b)| = 0$. Thus

$$|(D+E)^2(b)| = |D^2(b)| + 2(|(DE)(b)|) + |E^2(b)| = 0.$$

Since $Z(b+1)$ is a group, $E^2(b) = 0$. Since no element of $C(b)$ is an element of $Z(b+1)$, every product gh for $g \in C(b)$, $h \in Z(b+1)$, is an element of $C(b)$ and $DE(b) = DE$, so $|(DE)(b)| = |DE| = 0$. Thus $|D^2(b)|$ must equal

https://doi.org/10.4153/CJM-1961-032-4 Published online by Cambridge University Press

zero. By computation, we will obtain a contradiction to this statement and hence show that $A^{(u)} = -A$ is impossible.

We have

$$D = A(b) = m_b \sum_{g \in G_A(b)} \alpha_g g.$$

Since Y_A acts transitively on $G_A(b)$, all the subgroups U_g leaving fixed an element $g \in G_A(b)$ have the same order u, and, for chosen g, each $g' \in G_A(b)$ appears as g^y for exactly u elements $(y) \in Y_A$. For each $(y) \in Y_A$, $A^{(y)} = \beta_y A$ where $\beta_y = \pm 1$. For $(y) \in U_g$, any g, comparison of the coefficients of g in A and $A^{(y)}$ shows that $\beta_y = +1$. Thus the β_y are equal for all those (y) carrying g into a given $g' = g^y$, and comparison of coefficients again shows that $\alpha_{g'} = \beta_y \alpha_g$. It follows that the term $\alpha_{g'} g'$ occurs exactly u times in the sum

$$\sum_{(y) \in Y_A} \beta_y \alpha_g g^y.$$

Hence, for any $g \in G_A(b)$, we have

$$D = \frac{m_b}{u} \sum_{(y) \in Y_A} \beta_y \alpha_g g^y.$$

Now we may write

$$\begin{aligned} D^2 &= \left(m_b \sum_{g \in G_A(b)} \alpha_g g \right) D \\ &= m_b \sum_{g \in G_A(b)} \left\{ \alpha_g g \frac{m_b}{u} \sum_{(y) \in Y_A} \beta_y \alpha_g g^y \right\} \\ &= \frac{m_b^2}{u} \sum_{g \in G_A(b)} \sum_{(y) \in Y_A} \beta_y \alpha^2 g^{y+1} \\ &= \frac{m_b^2}{u} \sum_{(y) \in Y_A} \beta_y \left(\sum_{g \in G_A(b)} g^{y+1} \right). \end{aligned}$$

For $g \in C(b)$, we have $g^{y+1} \in C(b)$ if and only if $y + 1 \not\equiv 0 \pmod{p}$, and thus

$$|D^2(b)| = \frac{m_b^2}{u} |G_A(b)| \sum{}' \beta_y,$$

with summation over all $(y) \in Y_A$ such that $y \not\equiv -1 \pmod{p}$. To obtain a contradiction it will suffice to show that this sum is not zero.

The kernel of the natural map from the group Y, of order $p^{e-1}(p-1)$, onto the multiplicative group, of order $p-1$, of residues modulo p, has odd order p^{e-1}. Hence the intersection of this kernel with Y_A has odd order $p^{e'}$ dividing p^{e-1}. Since Y_A has even order, it contains elements mapping into -1, and hence exactly $p^{e'}$ of them. But $\Sigma' \beta_y$, as a sum of an odd number $|Y_A| - p^{e'}$ of terms $\beta_y = \pm 1$, cannot vanish.

https://doi.org/10.4153/CJM-1961-032-4 Published online by Cambridge University Press

We define the spectrum $S(B)$ of an element B of P as the sum of its distinct conjugates. We let $\bar{C}(a)$ be the sum of the elements of $C(a)$ and let $\bar{Z}(a)$ be the sum of the elements of $Z(a)$. We note that, since each $Z(a)$ is a group, for $b \geqslant a$, $\bar{Z}(a)\bar{Z}(b) = (|\bar{Z}(b)|)\bar{Z}(a)$, and since $\bar{C}(a) = \bar{Z}(a) - \bar{Z}(a+1)$ (where we define $Z(y)$ empty for $y > e$),

$$\bar{C}(a)\bar{C}(b) = (\bar{Z}(a) - \bar{Z}(a+1))(\bar{Z}(b) - \bar{Z}(b+1)).$$

If $b > a$, this is $(|\bar{C}(b)|)\bar{C}(a)$, while

$$\bar{C}(a)^2 = (|\bar{Z}(a)| - |(\bar{Z}(a+1)|)\bar{Z}(\mathrm{a}) - (\bar{Z}(a) - \bar{Z}(a+1))(|\bar{Z}(\mathrm{a}+1)|)$$
$$= (|\bar{C}(a)|)\bar{Z}(a) - (|\bar{Z}(a+1)|)\bar{C}(a).$$

Thus, if S is an element of the form

$$\sum_{x=0}^{e} m_x \bar{C}(x)$$

then

$$S^2 = \sum_{x=0}^{e} \left(m_x^2 \bar{C}(x)^2 + 2 \sum_{y=x+1}^{e} m_x m_y \bar{C}(x)\bar{C}(y) \right)$$
$$= \sum_{x=0}^{e} m_x^2(|\bar{C}(x)|)\bar{Z}(x) - m_x^2(|\bar{Z}(x+1)|)\bar{C}(x) + 2 \sum_{y=x+1}^{e} m_x m_y(|\bar{C}(y)|)\bar{C}(x)$$
$$= \sum_{x=0}^{e} h_x \bar{C}(x)$$

where

$$(1) \qquad h_x = \sum_{y=0}^{x} m_y^2(|\bar{C}(y)|) - m_x^2 \sum_{y=x+1}^{e} |\bar{C}(y)| + 2 \sum_{y=x+1}^{e} m_x m_y(|\bar{C}(y)|).$$

An immediate result of this computation is the following lemma.

LEMMA 1.2. *If*

$$S = \sum_{x=0}^{e} m_x \bar{C}(x)$$

then

$$S^2 = \sum_{x=0}^{e} h_x \bar{C}(x)$$

where, if $m_x = 0$, *then*

$$h_x = \sum_{y=0}^{x-1} m_y^2(|\bar{C}(y)|).$$

LEMMA 1.3. *If* A *is a basis element of* P, *then* $S_p(G_A) = \{x | a \leqslant x \leqslant d\}$ *for some* $d \geqslant a$.

Suppose not. Then there exists a smallest a such that there exists G_A with $a \in \mathrm{Sp}(G_A)$ and such that there exist d and c such that $d > c > a$ with

$d \in \mathrm{Sp}(G_A)$ and $c \notin \mathrm{Sp}(G_A)$. Then $c \in \mathrm{Sp}(G_B)$ for some basis element B, and by minimality of a, the minimal element of $\mathrm{Sp}(G_B)$ is greater than a. But, by previous calculations, if

$$S(B) = \sum_{x=0}^{e} m_x \bar{C}_x,$$

$$(S(B))^2 = \sum_{x=0}^{e} h_x \bar{C}(x)$$

where h_x is given by (1). Thus, since a is less than the minimal integer of $\mathrm{Sp}(G_B)$, $h_a = 0$. However, by Lemma 1.2,

$$h_d = \sum_{y=0}^{d-1} m_y^2 |\bar{C}(y)| > 0$$

since $m_c^2 > 0$. Hence the partition set of $(S(B))^2$ contains part but not all of the partition set of A, which contradicts the assumption that A is a basis element.

We have shown that the spectrum of a basis element is a set of consecutive integers. Now we will examine coefficients of the levels of the basis elements.

First, we note that if $S = S(A)$, S^2 and S have intersecting partition sets. For if b is the maximal integer in $\mathrm{Sp}(G_A)$,

$$S^2 = \sum_{x=0}^{e} h_x \bar{C}(x),$$

h_x given by (1), and $m_a = 0$ unless $a \in \mathrm{Sp}(G_A)$. Thus

$$h_b = \sum_{\substack{a \in \mathrm{Sp}\, G_A \\ a<b}} m_a^2 |\bar{C}(a)| + m_b^2 [\bar{C}(b)| - |\bar{Z}(b+1)|].$$

If $e = b$, $h_b > 0$ since $\bar{Z}(b+1) = 0$, otherwise $|\bar{Z}(b)| = p|\bar{Z}(b+1)|$ and $\bar{C}(b) = \bar{Z}(b) - \bar{Z}(b+1)$, and hence

$$h_b = \sum_{\substack{a<b \\ a \in \mathrm{Sp}\, G_A}} m_a^2 |\bar{C}(a)| + m_b^2 (p-2)|\bar{Z}(b+1)| > 0.$$

If $\mathrm{Sp}(G_A) = a, a+1, \ldots d, d > a$ we may write

$$S(A) = S = \sum_{x=a}^{d+1} n_x \bar{Z}(x)$$

where $n_x = m_x - m_{x-1}$, $m_x = 0$ for $x < a$ or $x > d$, but since for $x < y$,

$$\bar{Z}(x)\bar{Z}(y) = (|\bar{Z}(y)|)\bar{Z}(x) = p^{e-y}\bar{Z}(x),$$

$$S^2 = \sum_{x=a}^{d} \left(n_x p^{e-x} + 2 \sum_{w=x+1}^{d+1} n_w p^{e-w} \right) n_x \bar{Z}(x) + n_{d+1}^2 p^{e-d-1} \bar{Z}(d+1).$$

Since the spectra of S and S^2 intersect, $S^2 = kS + \ldots$, where k is a non-zero integer. So for $x = a, a+1, \ldots, d$,

$$kn_x = \left(n_x p^{e-x} + 2 \sum_{w=x+1}^{d+1} n_w p^{e-w} \right) n_x.$$

https://doi.org/10.4153/CJM-1961-032-4 Published online by Cambridge University Press

But we know that $n_a = m_a$ is not equal to 0. If all the n_x, $a < x \leqslant d$ are zero, then the m_x are all equal and thus all $m_x = 1$. Suppose that not all m_x are equal. Let $H = \{h | a \leqslant h \leqslant d, n_h \neq 0\}$.

Let u and v, $u < v$ be two consecutive members of H. Then

$$kn_u = \left(n_u p^{e-u} + 2\sum_{w=u+1}^{d+1} n_w p^{e-w}\right) n_u,$$

$$kn_v = \left(n_v p^{e-v} + 2\sum_{w=v+1}^{d+1} n_w p^{e-w}\right) n_v.$$

Since u and v are consecutive in H, $n_u \neq 0$, $n_v \neq 0$ but $n_k = 0$ for $u < k < v$, and hence solving the above equations, we obtain $n_v = -p^{v-u} n_u$. Now $n_v = m_v - m_u$ since $m_{v-1} = m_u$. But $m_a \neq 0$ since $a \in \mathrm{Sp}(G_A)$, so that if there exists an integer larger than a in H we set $u = a$ and let v be the next smallest integer in H. Then $m_v = m_a(1 - p^{v-a})$.

Therefore, the sign of m_v is the negative of that of m_a and we can state:

LEMMA 1.4. *If*

$$S(A) = \sum_{x \in \mathrm{Sp}(G_A)} m_x \bar{C}(x)$$

and each m_x is positive, then all $m_x = 1$.

A basis element such that each m_g is positive will be called a *positive* basis element. If A is not a positive basis element, the above equations show that

$$H = \{a, h_1, h_2, \ldots, h_k\}$$

where $a < h_1 < \ldots < h_k$, $k > 0$, and

$$S = n_a \bar{Z}(a) + n_{h_1} \bar{Z}(h_1) + n_{h_2} \bar{Z}(h_2) + \ldots + n_{h_k} \bar{Z}(h_k) \tag{2}$$

where

$$n_{h_j} = (-1)^j (p^{h_j - a}) n_a$$

for $j = 1, 2, \ldots, k$.

A basis element with spectrum S as defined by (2) is called an *alternating* basis element.

LEMMA 1.5. *If A is an alternating basis element then*

$$S(A) = \sum_{x=0}^{d+1} n_x \bar{Z}(x), \quad n_0 = \pm 1,$$

and if $0 < h_1, < \ldots < h_k$ are the elements of $\mathrm{Sp}(G_A)$ with $n_h \neq 0$, then

$$n_{h_j} = (-1)^j (p^{h_j}) n_0.$$

We must show that $n_0 \neq 0$. Suppose $n_0 = 0$. There exists a basis element $B \neq A$, such that G_B intersects $C(0)$, and therefore

$$S(B)^2 = \sum_{t \in \mathrm{Sp}(G_A)} m_t \bar{C}(t) + \ldots$$

https://doi.org/10.4153/CJM-1961-032-4 Published online by Cambridge University Press

where each $m_t > 0$ by Lemma 1.2. Then $S(B)^2 = kA + \ldots$, and the coefficients in A must have the same sign as k, so A must be a positive element. This shows that $n_0 \neq 0$ and thus $a = 0$ in (2) and n_0 divides all the n_h. Thus since the greatest common divisor of the m_g is 1 for g in the partition set corresponding to basis element A, n_0 must be $+1$ or -1. We will always choose $n_0 = 1$ for an alternating element of the canonical basis of its partition ring.

We now show that if A is a basis element then $A \neq S(A)$ implies $G_A \subseteq C(a)$ for some a.

LEMMA 2.1. *Let A be a basis element of a partition ring P of a group G of odd prime power order p^e. Let Y be the automorphism group of G, and Y_A the subgroup of Y leaving A fixed. If $[Y: Y_A]$ is not a power of p, there exists $(z) \in Y$ such that $G_A(a) \cdot G_A{}^{(z)}(a) \subseteq C(a)$ for all a.*

Let (y) be a generator of Y, g a generator of G, and let a be an integer. $[Y: Y_A] = p^s b$ where $b | p-1$ since Y has order $p^{e-1}(p-1)$ and $b \neq 1$ by hypothesis. Both Y and Y_A are cyclic so Y_A is generated by $y_A = y^{p^s b}$.

If $G_A(a)$ is empty, the result is trivial for any $(z) \in Y$.

If $G_A(a)$ is non-empty, $G_A(a)$ contains g^{vp^a} for some $(v) \in Y$. Then, for all $(z) \in Y$,

$$g^{vzp^a} \in G_A^{(z)}(a),$$

and $G_A(a)$ and $G_A{}^{(z)}(a)$ are closed under Y_A. Therefore the existence of a $z \not\equiv 0 \pmod p$ such that $G_A(a) \cdot G_A{}^{(z)}(a) \subseteq C(a)$ is equivalent to the existence of a z such that for all m, n, $p \nmid (vy_A{}^m + vzy_A{}^n)$, hence is equivalent to the existence of a z such that for all r, $p \nmid (y_A{}^r + z)$ or $y_A{}^r \not\equiv -z \pmod p$. This condition is clearly independent of a.

But

$$y_A = y^{p^s b} \equiv y^b \pmod p$$

and y is primitive of order $p-1 \pmod p$ while y_A is of order $(p-1)/b \pmod p$ and hence has order less than $p-1$. Thus we may choose $-z$ from the residues which do not appear as powers of y_A.

Next, we mention a well-known lemma.

LEMMA 2.2.

$$\text{If} \quad a^{p^i} \equiv b^{p^i} \pmod p$$

for some $i \geqslant 0$, p a prime, then

$$a^{p^n} \equiv b^{p^n} \pmod{p^{n+1}}$$

for all non-negative integers n. (*See* **2**, Theorem 4.5, vol. 1.)

LEMMA 2.3. *Under the hypotheses of Lemma* 2.1, if

$$[Y: Y_A] = p_s,\ s > 0, \text{ then } G_A(a)^2 \cap C(a+1) = 0$$

for all a.

https://doi.org/10.4153/CJM-1961-032-4 Published online by Cambridge University Press

Let $g^{p^a u}$ be an element of $G_A(a)$. Then an element of $G_A(a)^2$ would be of the form

$$g^{p^a}(u)\ (y_A^{n_1} + y_A^{n_2}).$$

If this element is contained in $C(a+1)$, $p||(y_A{}^{n_1} + y_A{}^{n_2})$ (where we use $p^k||u$ to mean that p^k is the highest power of p dividing u).

Let $p|y_A{}^{n_1} + y_A{}^{n_2}$. Then $y_A{}^{n_1} \equiv -\ y_A{}^{n_2} \pmod p$. But

$$y_A = y^{p^s}$$

(where y generates Y) so

$$y^{p^s n_1} \equiv -y^{p^s n_2} \pmod p.$$

Now Lemma 2.2 shows that

$$y^{p^s n_1} \equiv -y^{p^s n_2} \pmod{p^{s+1}}$$

and since $s > 0$, $p^2|(y_A{}^{n_1} + y_A{}^{n_2})$, which means that the element does not lie in $C(a+1)$.

LEMMA 2.4. *If A is a basis element of a partition ring of a cyclic group G of odd prime power order and G_A meets more than one level of G, then G_A is a union of levels.*

To show this, we need only show that $Y_A = Y$. Suppose $Y_A \neq Y$; since by Lemma 3.1 the spectrum of A is consecutive and G_A meets more than one level, there exists a such that $G_A(a) \neq 0$, $G_A(a+1) \neq 0$. Let $[Y\colon Y_A] = p^s b$, $(b, p) = 1$. First, assume $b \neq 1$. Choose z by Lemma 2.1 such that $G_A(h)G_A{}^{(z)}(h) \subseteq C(h)$ for all h. Let $B = A^{(z)}$.

$$(AB)(a) = A(a)B(a) + A(a)[B(a+1) + \ldots + B(d)] + B(a)[A(a+1) + \ldots + A(d)].$$

But since $|A(h)| = |B(h)|$, by Theorem 1,

$$\frac{|AB(a)|}{|A(a)|} = |A(a)| + 2[|A(a+1)| + \ldots + |A(d)|]$$

while similarly

$$\frac{|AB(a+1)|}{|A(a+1)|} = |A(a+1)| + 2[|A(a+2)| + \ldots + |A(d)|].$$

We chose z so that $G_A(a)\, G_B(a) \subseteq C(a)$, thus the spectra of AB and A intersect, and hence

$$AB = \sum_w k_w A^{(w)}$$

with distinct values of k_W, and the sum of the coefficients in AB of the elements in a given level is in a fixed proportion to those in A. Thus the left sides of the two equations above must be equal and, by subtracting, we obtain $|A(a)| + |A(a+1)| = 0$. But, by Theorem 1,

$$\frac{|G_A(a)|}{|G_A(a+1)|} = \frac{|C(a)|}{|C(a+1)|} = p$$

(where for any set S we shall write $|S| = |\bar{S}|$) and since $|A(a)| \neq 0$, we have $m_{a+1} = -pm_a$.

We have shown, however, that if A is a positive element $m_{a+1} = m_a$, and if A is an alternating element $m_{a+1} = -(p-1)m_a$, so we have obtained a contradiction.

By the above reasoning $b = 1$, whence the hypothesis that $Y_A \neq Y$ implies that $s > 0$. Now, by Lemma 2.3, for all h, $G_A(h)^2 \cap C(h+1) = 0$.

Let $g \in G_A(h)$. Then, an element of $G_A(h)^2$ is of the form $g^{(1+y_A{}^k)}$ and this is an element of $C(h)$ unless $p|1 + y_A{}^k$, that is, unless $y_A{}^k \equiv -1$ modulo p.

Let W be the set of elements of Y_A which are congruent to -1 modulo p. W is non-empty since Y_A is of even order (divisible by $p-1$) and hence is equal in order to the subgroup of Y_A of elements congruent to 1 modulo p. But this is a subgroup of index $p-1$ in Y_A, and hence

$$|W| = \frac{1}{p-1}(|Y_A|).$$

Thus

$$|G_A^2(h) \cap C(h)| = \frac{p-2}{p-1}|G_A(h)^2|.$$

So

$$\frac{|A^2(a)|}{|A(a)|} = \frac{p-2}{p-1}[|A(a)|] + 2[|A(a+1)| + \ldots + |A(d)|]$$

while

$$\frac{|A^2(a+1)|}{|A(a+1)|} = \frac{p-2}{p-1}[|A(a+1)|] + 2[|A(a+2)| + \ldots + |A(d)|]$$

and

$$\frac{p-2}{p-1}|A(a)| + \frac{p}{p-1}|A(a+1)| = 0 \quad \text{or} \quad m_{a+1} = -(p-2)m_a,$$

which also contradicts previous lemmas. Thus the lemma is proved.

Thus we have proved:

THEOREM 2. *Let A be a basis element of a partition ring of a cyclic group of odd prime power order. If $Y_A \neq Y$, then $G_A \subset C(a)$ for some a, and all m_g are 1. If $Y_A = Y$ then G_A is a union of consecutive levels. If all m_g are positive, then all m_g are 1. If not all m_g are positive, then $C(0) \subset G_A$ and A is an alternating basis element.*

Next, we examine some relations between sets which intersect consecutive levels.

https://doi.org/10.4153/CJM-1961-032-4 Published online by Cambridge University Press

Let G be a cyclic group of odd prime power order p^e and let Y be the automorphism group of G. A non-empty subset J of G is called a basic set if it is the set of all images of an element g of G under a subgroup of Y. The largest subgroup Z of Y such that $J = \{g^y | y \in Z\}$ is called the automorphism group of J.

We will now state three lemmas concerning basic sets and the sums of their elements. Let G_A be a basic set contained in $C(a)$, $0 \leqslant a < e - 1$ and let Y_A be the automorphism group of G_A. Let $[Y: Y_A] = p^s b$ where $s > 0$ and $b | p - 1$.

LEMMA 3.1. *G_A is a union of $d = (p-1)/b$ cosets of G^{p^a} modulo $G^{p^{a+s+1}}$.*

Let H be a coset contained in G_A. We define $H^{[p]}$ to be the coset containing the pth powers of the elements of H. Let A be the sum of all elements of G_A and $A^{[p]}$ the sum of all elements of the cosets $H^{[p]}$ for cosets $H \subseteq G_A$.

LEMMA 3.2.

$$A^p \equiv |G^{p^{a+s+1}}|^{p-1} A^{[p]} \pmod{p|G^{p^{a+s+1}}|^{p-1}}.$$

Let G_B be a basic subset contained in

$$\bigcup_{H \subseteq G_A} H^{[p]}$$

and Y_B be the automorphism group of G_B. Let B be the sum of all elements of G_B.

LEMMA 3.3. *AB is a sum of conjugates, under Y, of A if and only if $G_B \cap H^{[p]} \neq 0$ for each coset $H \subseteq G_A$.*

Proof of Lemma 3.1. If (y) is a generator of Y, then $(Y_A) = (y^{p^s b})$ is a generator for Y_A. As a generator of Y, (y) is transitive on all levels of G and hence on $C(a)$. The order of $C(a)$ is $p^{e-a-1}(p-1)$, and thus this is the order of (y) on $C(a)$. Let

$$(z) = (y_A)^d = (y^{p^s(p-1)}).$$

Then (z) has order

$$p^{e-a-s-1} = p^{e-a-1}(p-1)/p^s(p-1)$$

on $C(a)$. By Lemma 2.2, $z \equiv 1 \pmod{p^{s+1}}$, and hence, for any $h = g^{p^a}$ in G^{p^a}, $h^{(z)} \equiv h \pmod{G^{p^{a+s+1}}}$. Since the order of (z) on $C(a)$ is equal to the number of elements in a coset modulo $G^{p^{a+s+1}}$ and (z) maps each coset into itself, (z) is transitive on each coset contained in $C(a)$. It follows that G_A is a union of cosets.

If $h = g^{p^a} \in G_A$, then

$$h^{py_A^i} \equiv h^p \pmod{G^{p^{a+s+1}}}$$

$$py_A^i \equiv p \pmod{p^{s+1}}$$

and since $s > 0$, ${y_A}^i \equiv 1 \pmod{p}$. But

$$y_A = y^{p^s b} \equiv y^b \pmod{p},$$

whence $d|i$. Thus, for $h \in G_A$ the elements

$$h, h^{y_A}, \ldots, h^{y_A^{d-1}}$$

lie in distinct cosets, say $H_0, H_1, \ldots, H_{d-1}$, and further, the cosets

$$H_0^{[p]}, \ldots, H_{d-1}^{[p]}$$

are distinct. This proves that $G_A = H_0 \cup H_1 \cup \ldots \cup H_{d-1}$, a union of d cosets.

Proof of Lemma 3.2. Let

$$S_i = \sum_{g \in H_i} g, \quad S_i^{[p]} = \sum_{g \in H_i{}^{[p]}} g$$

whence

$$A = \sum_{i=0}^{d-1} S_i, \quad A^{[p]} = \sum_{i=0}^{d-1} S_i^{[p]}.$$

Now

$$A^p = \left(\sum S_i\right)^p = \sum \binom{p}{k_0, \ldots k_{d-1}} {S_0}^{k_0} {S_1}^{k_1} \ldots {S_{d-1}}^{k_{d-1}},$$

and

$${S_0}^{k_0} \ldots {S_{d-1}}^{k_{d-1}} = |G^{p^{a+s+1}}|^{p-1} S$$

for S the sum of the elements of some coset H. Hence,

$$\text{modulo } p|G^{p^{a+s+1}}|^{p-1},$$

$$A^p \equiv \sum_{i=0}^{d-1} {S_i}^p \equiv \sum_{i=0}^{d-1} |G^{p^{a+s+1}}|^{p-1} S_i^{[p]} = |G^{p^{a+s+1}}|^{p-1} A^{[p]}.$$

Proof of Lemma 3.3. For $i = 0, 1, \ldots, d-1$, let $|G_B \cap H_i{}^{[p]}| = m_i$. If $m_i, m_j \neq 0$, there is an automorphism in Y_B mapping $G_B \cap H_i{}^{[p]}$ onto $G_B \cap H_j{}^{[p]}$, whence $m_i = m_j$. Thus, if some non-zero $m_i = m$, each $m_j = 0$ or m, for $j = 0, 1, \ldots, d-1$.

For $h \in H_0$, $H_i H_j{}^{[p]}$ contains

$$h^{y_A^i + p y_A^j} = h^{y_A^i (1 + p y_A^{j-1})},$$

hence

$$H_i H_j^{[p]} = H_i^{(1 + p y_A^{j-1})},$$

a conjugate of H_i. Moreover, the

$$H_i^{(1 + p y_A^k)}$$

https://doi.org/10.4153/CJM-1961-032-4 Published online by Cambridge University Press

for $0 \leqslant i, k \leqslant d-1$ are distinct, for

$$h^{y_A^i(1+py_A^k)} \equiv h^{y_A^{i'}(1+py_A^{k'})} \pmod{G^{p^{a+s+1}}}$$

implies

$$y_A^i(1+py_A^k) \equiv y_A^{i'}(1+py_A^{k'}) \pmod{p^{s+1}},$$

hence, since

$$s+1 \geqslant 2, y_A^i \equiv y_A^{i'} \text{ and } y_A^k \equiv y_A^{k'}$$

modulo p, and thus $i = i'$, $k = k'$.

Thus

$$AB = \sum_{i=0}^{d-1} S_i \sum_{j=0}^{d-1} \left(\sum_{g \in H_j^{[p]} \cap G_B} g \right) = \sum_{i=0}^{d-1} \sum_{j=0}^{d-1} m_j S_i^{(1+py_A^{j-1})},$$

where $m_i = |H_i^{[p]} \cap G_B|$. Since

$$A^{(1+py_A^k)} = \sum_i S_i^{(1+py_A^k)},$$

AB is a sum of such conjugates if and only if all $m_j = m \neq 0$, that is, since $G_B \neq 0$, if G_B meets each $H_i^{[p]}$.

A result of these lemmas is the following theorem.

THEOREM 3. *Let G be a cyclic group of odd prime power order p^e. Let A be a basis element of a partition ring P of G such that the number of distinct conjugates of A is greater than or equal to p. Then G_A is entirely contained in some level $C(a)$ of G, and, if G_B is a partition set intersecting $C(a+1)$, G_B is contained in $C(a+1)$ and $|G_A| = p^t|G_B|$ for t an integer greater than or equal to zero.*

Proof of Theorem 3. That A has more than $p-1$ conjugates implies that the index $[Y: Y_A]$ of the automorphism group of A is greater than p, hence $[Y: Y_A] = p^s b$ for some $s > 0$ and $b|p-1$. By Theorem 2, $G_A \subseteq C(a)$ for some a, and since $C(e-1)$ has only $p-1$ elements, $0 \leqslant a < e-1$. Writing $G_A = H_0 \cup \ldots \cup H_{d-1}$ in accordance with Lemma 3.1 we note that, using Lemma 3.2, we can show that $A^{[p]}$ is a linear combination of basis elements by an argument identical with that used in the first part of the proof of Theorem 1. But the partition set of $A^{[p]}$ is contained in $C(a+1)$, and hence $C(a+1)$ is a sum of partition sets of basis elements. Since all basis elements contained in a level are conjugate, and

$$H_0^{[p]} \cup \ldots \cup H_{d-1}^{[p]}$$

is a union of partition sets of basis elements, we may assume G_B is a set of this union. By Lemma 3.3, since G_B is a basic subset of G, $|G_B| = md$ where $m|(|H_i^{[p]}|)$. Since $|H_i^{[p]}| = p^{e-a-s-1}$ and $|G_A| = p^{e-a-s-1}d$, $|G_A| = p^t|G_B|$ for some $t \geqslant 0$.

https://doi.org/10.4153/CJM-1961-032-4 Published online by Cambridge University Press

We now show that the necessary conditions for a set Σ of elements

$$A = \sum_{g \in G_A} m_g g$$

of the group ring of a cyclic group G of odd prime power order p^e, where the G_A constitute a partition π of G to be a canonical basis for a reduced integral partition ring of the group, as stated in Theorems 1, 2, and 3, are also sufficient. These conditions are as follows.

The partition π consists of sets of two sorts:

(*i*) $G_A = C(a) \cup C(a+1) \cup \ldots \cup C(d) = G^{p^a} - G^{p^{d+1}}$, $d > a$;

(*ii*) $G_A \subseteq C(a) = G^{p^a} - G^{p^{a+1}}$.

The sets of type (ii) are subject to the two conditions:

(iii) $G_A \subseteq C(a)$ implies that $G_A{}^{(y)} \in \pi$ for all $(y) \in Y$;

(iv) If $C(a)$ is a union of k sets G_A of π and $k \geqslant p$;

then $C(a+1)$ is a union of sets G_B of π, and $|G_A| = p^t|G_B|$ for t a non-negative integer.

(v) The elements of Σ are of two sorts:

$$A = \sum_{g \in G_A} g,$$

(we will call such an element positive);

(b) Possibly, for a single

$$G_A = C(0) \cup C(1) \cup \ldots \cup C(d),\ d > 0,$$

A is an alternating element as defined earlier. The sufficiency of these conditions is asserted by the following theorem.

THEOREM 4. *Let G be a cyclic group of odd prime power order p^e. If π is a partition of G and Σ a set of elements of G such that π and Σ satisfy conditions* (i)–(v) *above, then Σ is a canonical basis for a partition ring of G.*

We need only show that if A and B are elements of the given set, Σ, then AB is a sum of elements of Σ. We may assume that the least element of the spectrum of G_A is less than or equal to the least element of the spectrum of G_B. Let Y_A be the automorphism group of G_A.

Case I. Let $Y = Y_A$ and let $\mathrm{Sp}(G_A) = \{a, \ldots, d\}$, $d \geqslant a$. Suppose $B = A$. Then $A^2 = kA + n\bar{Z}(d+1)$ for some k and n, and $\bar{Z}(d+1)$ is clearly a sum of elements of Σ such that all $m_g = 1$. If $B \neq A$ then $G_B \subseteq Z(d+1)$ and $BA = |B|A$.

We have considered the case in which $Y_A = Y$. Now we may assume that Y_A is a proper subgroup of Y, and thus $G_A \subset C(a)$ for some a.

Case II. Let $1 < [Y: Y_A] < p$. We consider two subcases:

Subcase II.1. Let G_B not intersect $C(a)$. Then since, by the construction employed in the proof of Lemma 3.1. G_A is a union of cosets of

https://doi.org/10.4153/CJM-1961-032-4 Published online by Cambridge University Press

$$G^{p^a} \text{ modulo } G^{p^{a+1}},$$

$G_B \subseteq G^{p^{a+1}}$ and hence $AB = |B|A$.

Subcase II.2. Let G_B intersect $C(a)$. By (iii) $B = A^{(v)}$ for some $(v) \in Y$. G_A must be a union of cosets modulo $G^{p^{a+1}}$ since $[Y: Y_A] < p$. If $G_A = H_0 \cup H_1 \cup \ldots \cup H_{d-1}$ then

$$G_B = H_0^{(v)} \cup H_1^{(v)} \cup \ldots \cup H_{d-1}^{(v)}.$$

Let

$$S_i = \sum_{g \in H_i} g.$$

Then

$$AB = A\,A^{(v)} = \sum_{i=0}^{d-1} S_i \sum_{j=0}^{d-1} S_j^{(v)} = |S_j| \sum_{i=0}^{d-1} \sum_{j=0}^{d-1} S_i^{(1+vy_A^{j-i})}$$

$$= |S_j| \sum_{k=0}^{d-1} \sum_{i=0}^{d-1} S_i^{(1+vy_A^k)}.$$

If $vy_A{}^k \equiv -1 \pmod p$ then $S^{(1+vy_A^k)}$ is the sum of the elements of the unit coset $G^{p^{a+1}}$ and hence a sum of elements of Σ. If $vy_A{}^k \not\equiv -1 \pmod p$ then

$$\sum_{i=0}^{d-1} S_i^{(1+vy_A^k)}$$

is a conjugate of A. Thus AB is a sum of elements of Σ.

Case III. The index $[Y: Y_A] \geqslant p$. Then $[Y: Y_A] = p^s b$ where $s > 0$ and $b | p-1$. Let $d = (p-1)/b$. By Lemma 3.1, G_A is a sum of cosets of

$$G^{p^a} \text{ modulo } G^{p^{a+s+1}}.$$

We will retain the convention that $G_A = H_0 \cup H_1 \cup \ldots \cup H_{d-1}$, where

$$H_0^{(y_A^i)} = H_i.$$

We define $H^{\{t\}}$ to be the coset containing the t^{th} powers of the elements of H and $S^{\{t\}}$ to be the sum of the elements of $H^{\{t\}}$. Let $h \in H_0$ and let H_i and H_j be distinct cosets contained in G_A. If $H_i{}^{\{t\}}$ and $H_j{}^{\{t\}}$ are not distinct then

$$h^{ty_A^i} \text{ and } h^{ty_A^j}$$

are elements of the same coset and $ty_A{}^i \equiv ty_A{}^j \pmod{p^{s+1}}$. This implies that $p^{s+1} | t$, for otherwise we obtain $y_A{}^i \equiv y_A{}^j \pmod p$ contradicting the assumption of distinctness of cosets. We can now define $A^{\{t\}}$ as

$$\sum_{i=0}^{d-1} S_i{}^{\{t\}},$$

https://doi.org/10.4153/CJM-1961-032-4 Published online by Cambridge University Press

and note that if $t \equiv 0\ (p^{s+1})$,

$$A^{\{t\}} = d\Big(\sum_{g \in G^{p^{a+s+1}}} g\Big),$$

while otherwise $A^{\{t\}}$ is a sum of distinct coset sums.

We will now prove two lemmas, under the assumptions of Case III.

LEMMA 4.1. *For $0 \leqslant k \leqslant s$, $C(a + k)$ is a union of at least p sets of π, each of which meets precisely d cosets of G^{p^a} modulo $G^{p^{a+s+1}}$ and these cosets are conjugate under Y_A.*

LEMMA 4.2. *The sum of $A^{\{t\}}$ is a sum of elements of Σ.*

Proof. of Lemma 4.1. We know that $|C(a)| = p^{e-a-1}(p-1)$ and

$$|G_A| = \frac{|C(a)|}{[Y:Y_A]} = p^{e-a-s-1}\,d.$$

By (iv), if G_{A_k} is a set of π contained in $C(a + k)$ and

$$\frac{|C(a+k)|}{|G_{A_k}|} \geqslant p,$$

then $C(a + k + 1)$ is a union of sets of π and $|G_{A_{k+1}}| \leqslant |G_{A_k}|$, and since $|C(a + k)| = p|C(a + k + 1)|$ we obtain

$$\frac{|C(a+k+1)|}{|G_{A_{k+1}}|} \geqslant \frac{|C(a+k+1)|}{|G_{A_k}|} = \frac{|C(a+k)|}{p|G_{A_k}|} \geqslant p^{s-k-1} \text{ for } 0 \leqslant k \leqslant s.$$

But since $|G_{A_k}| = p^t|G_{A_{k+1}}|$ for $t \geqslant 0$, and

$$[Y: Y_{A_k}] = \frac{|C(a+k)|}{|G_{A_k}|},$$

we may write $[Y: Y_{A_k}] = p^{s-k+\epsilon}b$ for $\epsilon \geqslant 0$.

If (y) is a generator for Y then $(y_A) = (y^{p^s b})$ is a generator for Y_A and $(y_{A_k}) = (y^{p^{s-k+\epsilon}b})$ is a generator for Y_{A_k}. Let H be a coset contained in G_A and $h \in H$. Now $h^{p^k} \in H^{\{p^k\}}$, and we examine the effect of (y_A) and (y_{A_k}) on this coset.

If $\epsilon \geqslant k$, from $y^{p^{\epsilon-k}} \equiv y \pmod p$, by Lemma 2.2, we obtain

$$y^{p^{s-k+\epsilon}} \equiv y^{p^s} \pmod{p^{s+1}}.$$

If $k \geqslant \epsilon$, from $y^{p^{k-\epsilon}} \equiv y \pmod p$ we obtain

$$y^{p^s} \equiv y^{p^{s-k+\epsilon}} \pmod{p^{s-k+e+1}}.$$

In either case

$$y^{p^s} \equiv y^{p^{s-k+\epsilon}} \pmod{p^{s-k+1}},$$

and thus

$$p^k y^{p^s b} \equiv p^k y^{p^{s-k+\epsilon}b} \pmod{p^{s-1}}.$$

Hence (y_A) and (y_{A_k}) map an element of $H^{\{p^k\}}$ into the same coset and thus they permute the cosets contained in $C(a + k)$ in the same way. It follows

https://doi.org/10.4153/CJM-1961-032-4 Published online by Cambridge University Press

that G_{A^k} meets precisely those cosets that belong to some family of d cosets conjugate under Y_A. This completes the proof of Lemma 4.1.

Proof of Lemma 4.2. By (v), since $\bar{C}(a)$ is not contained in an alternating element, each element of Σ with partition set contained in G^{p^a} is the sum of the elements of its partition set. Since, by Lemma 4.1, $C(a+s)$ is a union of elements of π, by (i) and (ii), $G^{p^{a+s+1}}$ is a union of elements of π, and hence for $t \equiv 0 \pmod{p^{s+1}}$, $A^{\{t\}}$ is a sum of elements of Σ.

If $p^{s+1} \nmid t$, $H_0^{\{t\}}$ is contained in some $C(a+k)$, $0 \leqslant k \leqslant s$, and by Lemma 4.1,

$$H_0^{\{t\}} \cup \ldots \cup H_{d-1}^{\{t\}}$$

is a union of sets of π. Hence $A^{\{t\}}$ is a sum of elements of Σ. This completes the proof of Lemma 4.2.

Let $G_B \in \pi$ be the partition set of some $B \in \Sigma$ where b, the smallest element of the spectrum of G_B, satisfies $b \geqslant a$. Then

$$B = \sum_{g \in G_B} g.$$

Subcase III.1. $b = a$. Then by (iii), $G_B = G_A{}^{(z)}$ for some $(z) \in Y$, whence

$$B = \sum_{j=0}^{d-1} S_j{}^{\{z\}}.$$

Now $|G_B \cap H_i{}^{\{z\}}| = |G^{p^{a+s+1}}|$ where $0 \leqslant i < d$ and

$$AB = \sum_{i=0}^{d-1} \sum_{j=0}^{d-1} S_i S_j{}^{\{z\}} = |G^{p^{a+s+1}}| \sum_{j=0}^{d-1} \sum_{i=0}^{d-1} S_i^{\{1+zy_A^{j-1}\}}$$

$$= |G^{p^{a+s+1}}| \sum_{j=0}^{d-1} A^{\{1+zy_A^j\}}$$

which, by Lemma 4.2, is a sum of elements of Σ.

Subcase III.2. $a < b \leqslant a+s$. Then $C(b)$ is a union of conjugates of G_B, and writing $b = a+k$, we know that G_B meets $H_0{}^{\{t\}}$ for some t where $p^k \| t$, whence, by Lemma 4.1, G_B meets precisely the d cosets

$$H_0{}^{\{t\}}, H_1{}^{\{t\}}, \ldots, H_{d-1}^{\{t\}}.$$

By an earlier argument, see proof of Lemma 3.3, all $|H_i{}^{\{t\}} \cup G_B| = m$ for a fixed $m > 0$. Thus

$$AB = \sum_{i=0}^{d-1} S_i \left(\sum_{j=0}^{d-1} \sum_{g \in H_j{}^{\{t\}}} g \right) = m \sum_{j=0}^{d-1} A^{\{1+ty_A^j\}},$$

which again is a sum of elements of Σ.

Subcase III.3. If $b > a+s$, then B is an element of Σ with partition set contained in $G^{p^{a+s+1}}$. Then $BA = |B|A$ and the theorem is proved.

In view of Theorem 4, in order to list all reduced integral partition rings of a cyclic group G of odd prime power order p^e, it suffices to list all proper

https://doi.org/10.4153/CJM-1961-032-4 Published online by Cambridge University Press

partitions of G, that is, partitions satisfying (i)–(iv), and, in the case of partitions in which $C(0)$ is properly contained in a partition set, to list the possible ways in which an alternating element may occur.

If π is a proper partition of G, the restriction π' of π to G^p is a proper partition of the subgroup G^p. Thus, a proper partition π of G can be obtained from a proper partition π' of G^p in at most two ways:

1. $C(0)$ may be partitioned and the sets of this partition, together with those of π' will form π.

2. If $C(1)$, the lowest level of G^p, is contained in a set of π', $C(0)$ may be adjoined to this set to extend π' to π.

A partition formed by the first procedure must be made in such a manner that conditions (i)–(iv) are satisfied. This can be done as follows.

Let G_A be a set of the partition of $C(a)$. By condition (iii) G_A must be a basic set and from condition (iv) it follows that any such G_A for which

$$\frac{|C(0)|}{|G_A|} < p$$

yields a proper partition, while such a partition with

$$\frac{|C(0)|}{|G_A|} \geqslant p$$

is permissible just in case $C(1)$ contains some G_B and $|G_A| = p^s|G_B|$ for some $s \geqslant 0$. Any partition ring formed in this manner must contain only positive elements by (v) and hence is fully determined.

If the partition π is formed in the second manner, π contains a set $G_A = C(0) \cup C(1) \cup \ldots \cup C(d)$ for some $d > 0$. Then by (v), the element A of the partition ring with partition set G_A can be taken as a positive element or an alternating element. By the definition of an alternating element, the coefficient $m(0)$ of the elements of $C(0)$ must equal one, while the coefficients $m(a)$ of levels $C(a)$, $0 < a \leqslant d$ may each be chosen positive or negative, and by Lemma 1.5 the signs of these coefficients determine their values.

Since the group containing one element has only one partition ring, we have established an inductive procedure for finding all partition rings of cyclic groups of odd prime power order p^e.

References

1. B. Jónsson, and A. Tarski, *Representation problems for relation algebras*, Bull. Amer. Math. Soc. *54*, (1948), 80.
2. W. J. Leveque, *Topics in number theory*, 2 vols. (Reading, Mass.: Addison Wesley, 1956).
3. R. C. Lyndon, *The representation of relation algebras*, Ann. of Math. (2), *51* (1950), 707–729.
4. H. B. Mann, *On products of sets of group elements*, Can. J. Math., *4* (1952), 64–66.
5. A. Tarski, *On the calculus of relations*, J. Symb. Logic, *6* (1941), 73–89.
6. H. Zassenhaus, *The theory of groups* (New York: Chelsea, 1958).

University of Michigan and
Institute forDefence Analyses, Princeton