PACIFIC JOURNAL OF MATHEMATICS
Vol. 15, No. 2, 1965

A GENERALIZATION OF THE COSET DECOMPOSITION OF A FINITE GROUP

BASIL GORDON

Let G be a finite group, and suppose that G is partitioned into disjoint subsets: $G = \bigcup_{i=1}^{h} A_i$. If the A_i are the left (or right) cosets of a subgroup $H \subseteq G$, then the products xy, where $x \in A_i$ and $y \in A_j$, represent all elements of any A_k the same number of times. It turns out that certain other decompositions of G of interest in algebra enjoy this same property; we will call such a partition π an α-partition.

In this paper all α-partitions are determined in the case G is a cyclic group of prime order p; they arise by choosing a divisor d of $p-1$, and letting the A_i be the sets on which the d'th power residue symbol $(x/p)_d$ has a fixed value. It is shown that if an α-partition is invariant under the inner automorphisms of G (strongly normal) then it is also invariant under the antiautomorphism $x \rightarrow x^{-1}$. For such α-partitions (called weakly normal) it is shown that the set A_i containing the identity element is a group. An example shows that this need not hold for nonnormal partitions.

1. For any α-partition π, let N_{ijk} denote the number of times each element of A_k is represented among the products xy, $x \in A_i$, $y \in A_j$. Then if $\mathfrak{A}(G)$ is the group algebra of G over a field K, and if we put

$$a_i = \sum_{x \in A_i} x \,, \tag{1}$$

it is clear that $a_i a_j = \sum_{k=1}^{h} N_{ijk} a_k$. Therefore the vector space spanned over K by $a_1, \cdots, a_h$ is a subalgebra $\mathfrak{A}_\pi$ of $\mathfrak{A}(G)$, with structure constants N_{ijk}. Conversely, if $\pi : G = \bigcup_{i=1}^{h} A_i$ is any partition of G into disjoint subsets, and if the elements a_i defined by (1) span a subalgebra of $\mathfrak{A}(G)$, then π is an α-partition.

In the case where π is the decomposition of G into the cosets of a normal subgroup H whose order m is not divisible by the characteristic of K, the algebra $\mathfrak{A}_\pi$ is the group algebra $\mathfrak{A}(G/H)$ of the factor group G/H. For then the elements a_i/m form a group isomorphic to G/H, and are a basis of $\mathfrak{A}_\pi$.

In this paper some of the elementary properties of α-partitions are developed. I plan in a second paper to discuss in more detail the structure of the algebras $\mathfrak{A}_\pi$ and their application to the representation of G by matrices.

Received April 17, 1964. The author is an Alfred P. Sloan Fellow.

2. Normal partitions. Since the α-partitions are a generalization of the coset decomposition of G with respect to a subgroup H, it is natural to begin the study of them by asking which α-partitions should be called normal. Several different definitions of normality are possible, and two of them will be considered here. Note first that if π is an α-partition, and σ is an automorphism or anti-automorphism of G, then the partition π^σ obtained by applying σ to the sets of π, is again an α-partition. If $\pi = \pi^\sigma$, we will say that π is *invariant under* σ. This means that the sets of π are permuted among themselves by σ. If σ has the stronger property of mapping each set of π onto itself, π is called *setwise invariant under* σ.

An α-partition π is called *weakly normal* if it is invariant under the anti-automorphism $\sigma: x \to x^{-1}$. On the other hand π is called *strongly normal* if it is invariant under all inner automorphisms τ: $x \to t^{-1}xt$. It is easily seen that in the case where π is the left coset decomposition of G with respect to a subgroup H, either type of normality of π is equivalent to normality of H. The following theorem explains the choice of terminology.

THEOREM 1. *If π is strongly normal, then it is also weakly normal.*

Proof. Let π be strongly normal, let A_i be any set of π, and let x be any element of A_i. Suppose $x^{-1} \in A_j$. If n is the order of G, there exists a prime p such that $p > n$, $p \equiv -1 (\mathrm{mod}\ n)$, by Dirichlet's theorem on primes in an arithmetic progression. Let H_i be the group generated by the elements of A_i, and denote its order by m_i. Consider the set S of all ordered $(p+1)$-tuples $(t, x_1, x_2, \cdots, x_p)$ with $t \in H_i$, all $x_\nu \in A_i$, and such that $t^{-1}x^{-1}t = x_1x_2 \cdots x_p$. The mapping $\theta: (t, x_1, \cdots, x_p) \to (tx_1, x_2, \cdots, x_p, x_1)$ maps S onto itself, and so S is decomposed into orbits by the cyclic group of mappings generated by θ. Clearly the cardinality of the orbit of $(t, x_1, \cdots, x_p)$ is a multiple of p unless $x_1 = x_2 = \cdots = x_p$. In this case we have $t^{-1}x^{-1}t = x_1^p = x_1^{-1}$, or equivalently $t^{-1}xt = x_1$. Therefore the number of such $(p+1)$-tuples is equal to the number of elements $t \in H_i$ such that $t^{-1}A_it = A_i$. But every element $t \in H_i$ has this property. Indeed, if $t \in A_i$ then $t^{-1}tt = t$, so that the assumed strong normality of π implies $t^{-1}A_it = A_i$; the same is then of course true for all $t \in H_i$.

From this we see that if N is the cardinality of S, then $N \equiv m_i$ (mod p). On the other hand it is immediately seen from the definition of a strongly normal α-partition that if y is any element of A_j, then the number of ordered $(p+1)$-tuples $(t, x_1, \cdots, x_p)$, $t \in H_i$, $x_\nu \in A_i$ such that $t^{-1}yt = x_1x_2 \cdots x_p$ is also N. Since these $(p+1)$-tuples can be divided into orbits as above, we see that there are exactly m_i solutions of the equation $t^{-1}yt = x_1^p = x_1^{-1}$, where $t \in H_i$, $x_1 \in A_i$ (here we use the fact that $m_i \leqq n < p$). Hence all $t \in H_i$, give rise to solutions of this equation. Taking $t = e$ we get $y = x_1^{-1}$, so that the inverse of any element of A_j is in A_i. Since the roles of A_i and A_j can be interchanged, we have $A_j = \{z^{-1} \mid z \in A_i\}$, and the proof is complete.

In general weak normality does not imply strong normality. This can be seen by considering the example where A_1 is a nonnormal subgroup of G and $A_2 = G - A_1$.

3. Weakly normal partitions. In this section we obtain a characteristic property of weakly normal α-partitions which is useful in the further development of the theory. Let $\pi : G = \cup_{i=1}^{h} A_i$ be any decomposition of G into disjoint sets (not necessarily an α-partition). Suppose that for any $x \in A_i$, the cardinality of the $xA_j \cap A_k$ depends only on i, j, k(that is, does not depend on the particular x chosen from A_i) and for any $y \in A_j$, the cardinality of $A_iy \cap A_k$ depends only on i, j, k. We will use the tentative term *β-partition* to describe such π's, and will prove that they are precisely the weakly normal α-partitions. Half of this can be proved at once.

THEOREM 2. *Every weakly normal α-partition is a β-partition.*

Proof. Suppose $x \in A_i$, and form the set $xA_j \cap A_k$. The cardinality of this set is the number of solutions of the equation $xy = z$, where $y \in A_j$, $z \in A_k$. Since this equation is equivalent to $x = zy^{-1}$, and since $\{y^{-1} \mid y \in A_j\} = A'_j$ for some j', the number of solutions is $N_{kj'i}$, which depends only on i, j, k. In the same way we see that the cardinality of $A_iy \cap A_k$, where $y \in A_j$, depends only on i, j, k, and the proof is complete.

The proof that every β-partition is a weakly normal α-partition is somewhat more complicated, and we need two lemmas. For any β-partition, let Q_{ijk} denote the cardinality of $A_iy \cap A_k$, where $y \in A_j$.

LEMMA 1. *Suppose that the identity element e of G is in the set A_1 of a β-partition. Then A_1 is a group. Each A_i is a union of right cosets A_1t, $t \in G$, and also a union of left cosets tA_1, $t \in G$.*

Proof. Since $eA_1 = A_1$, we must have $xA_1 = A_1$ for any $x \in A_1$, which proves that A_1 is a subgroup of G. For any other set A_i we have $eA_i = A_i$, and therefore $xA_i = A_i$ for all $x \in A_1$. Hence whenever A_i contains an element t, it also contains the right coset A_1t. By the same reasoning A_i contains the left coset tA_1, which completes the proof.

LEMMA 2. *Let A_i be any set of a β-partition π. Then $\{x^{-1} \mid x \in A_i\}$ is also a set of π.*

Proof. Choose a fixed element $y \in A_i$, and let C be the set of π to which y^{-1} belongs (of course C may coincide with A_i). Then the complex yC contains at least one number of A_1, namely e. Hence if x is any other element of A_i, the complex xC must contain a member of A_1. Thus $xc = w$, where $c \in C$ and $w \in A_1$. Then $x^{-1} = cw^{-1}$ is in C by Lemma 1, which shows that $C \supseteqq \{x^{-1} \mid x \in A_i\}$. By the same reasoning $A_i \supseteqq \{z^{-1} \mid z \in C\}$, and hence $C = \{x^{-1} \mid x \in A_i\}$.

We define the mapping $i \rightarrow i'$ by putting $A_{i'} = \{x^{-1} \mid x \in A_i\}$.

THEOREM 3. *Every β-partition is a weakly normal α-partition.*

Proof. Let $\pi : G = \bigcup_{i=1}^{h} A_i$ be a β-partition. Fix $z \in A_k$ and consider the equation $xy = z$, where $x \in A_i$, $x \in A_j$. Since this equation is equivalent to $y = x^{-1}z$, it has $Q_{i'kj}$ solutions. Therefore every element of A_k is represented $Q_{i'kj}$ times among the products xy, $x \in A_i$, $y \in A_j$, and so π is an α-partition. It is weakly normal by Lemma 2.

In the next theorem we again let A_1 be the set of π containing e, and denote its cardinality by ν_1.

THEOREM 4. *If π is weakly normal, and if ν_1 is not a multiple of the characteristic of K, then $\mathfrak{A}_\pi$ has a two-sided identity element.*

Proof. By Lemma 1 each A_i is a union of right cosets of A_1. Hence $xA_i = A_i$ for any $x \in A_1$. Therefore, defining the elements a_i by (1), we have $a_1 a_i = \nu_1 a_i$. Similarly $a_i a_1 = \nu_1 a_i$, so that $\nu_1^{-1}\, a_1$ is a two-sided identity in $\mathfrak{A}_\pi$.

We conclude this section with some remarks and examples. Lemma 1 shows that if π is a weakly normal α-partition, then the set of π containing the identity element is a subgroup of G. If G is Abelian, then every α-partition is clearly strongly normal, and hence weakly normal by Theorem 1. Thus in this case the set containg e is always a subgroup. For non-Abelian groups this need not be so, as can be seen by considering the double coset decomposition $G = \bigcup_{i=1}^{h} Ha_iK$, where H and K are nonnormal subgroups of G. For example if $G = S_3$, the symmetric group on 3 letters, $H = \{e, (12)\}$, $K = \{e, (13)\}$, we obtain an α-partition into the two sets $A_1 = \{e, (12), (13), (123)\}$, $A_2 = \{(23), (132)\}$. Here A_1 is not a group.

An important class of weakly normal α-partitions can be constructed as follows. Let Γ be any group of automorphisms of G, and let the sets of π be the orbits of G under Γ, so that two elements x_1, $x_2 \in G$

are in the same set of π if and only if $x_1^\sigma = x_2$ for some $\sigma \in \Gamma$. Then if z and z^σ are two elements of A_k, to every representation $z = xy$ with $x \in A_i$, $y \in A_j$ corresponds the representation $z^\sigma = x^\sigma y^\sigma$ and conversely. Hence π is an α-partition. Also $x_1^\sigma = x_2$ implies $(x_1^{-1})^\sigma = x_2^\sigma$, so that if A_i is a set of π, so is $\{x^{-1} \mid x \in A_i\}$. Thus π is weakly normal. It is easily seen that π is strongly normal if and only if Γ is normalized by the group Γ_0 of inner automorphisms of G. This last situation includes the partition of G into its conjugacy classes, for then $\Gamma = \Gamma_0$.

4. The case $G = Z_p$. We next determine all α-partitions of Z_p, the cyclic group of prime order p. We use the additive notation for Z_p, so that its elements are $0, 1, \cdots, p-1$, and the group operation is addition (mod p). It is convenient in this case to call the sets of the partition $A_0, \cdots, A_h$ rather than $A_1, \cdots, A_h$, and to let A_0 be the set containing the identity element 0.

The only subgroups of Z_p are Z_p and $\{0\}$, and so by Lemma 1, $A_0 = Z_p$ or $A_0 = \{0\}$. The first case gives rise to a trivial α-partition, so only the second case need be considered. If ε is any primitive p'th root of unity, then the mapping $x \rightarrow \varepsilon^x$ maps Z_p isomorphically into the complex field, and by extension maps the group algebra $\mathfrak{A}(G)$ over the rational field Q homomorphically onto $Q(\varepsilon)$. Let η_i be the image of a_i under this mapping, so that $\eta_i = \sum_{x \in A_i} \varepsilon^x$.

LEMMA 3. *The η_i are algebraic integers of degree at most h.*

Proof. By (1), $\eta_i \eta_j = \sum_{k=0}^h N_{ijk} \eta_k$. Since $\eta_0 = 1 = -\eta_1 - \eta_2 - \cdots - \eta_h$, this can be written in the form $\eta_i \eta_j = \sum_{k=1}^h (N_{ijk} - N_{ij0}) \eta_k$; $(1 \leqq i, j \leqq h)$. Thus the vector $(\eta_1, \cdots, \eta_h)$ is an eigenvector of the matrix $(M_{jk}) = (N_{ijk} - N_{ij0})$ $(1 \leqq j, k \leqq h)$ with eigenvalue η_i. Since the M_{jk} are integers, it follows that η_i is an algebraic integer of degree $\leqq h$.

THEOREM 5. *Let $\bigcup_{i=0}^h A_i$ be an α-partition of Z_p with $A_0 = \{0\}$. Then*

(i) $p \equiv 1 \pmod{h}$

(ii) *If g is a primitive root of p, then the classes A_i can be numbered so that A_i consists of all residues x with $\mathrm{ind}_g x \equiv i \pmod{h}$; $(i > 0)$.*

(iii) *Conversely, for any h dividing $p-1$, the sets defined in* (ii) *form an α-partition of z_p.*

Proof. Let C_i be the number of elements in A_i, and suppose for the sake of the argument that $c_1 = \min\limits_{1 \leqq i \leqq h} c_i$. Theorem 2 implies that

$Q \subseteqq Q(\eta_1) \subseteqq Q(\varepsilon)$, where $S = [Q(\eta_1) : Q] \leqq h$. But $Q(\varepsilon)$ is a normal extension of Q whose Galois group $\mathfrak{G}$ is generated by the automorphism $\varepsilon \to \varepsilon^g$, and is cyclic of order $p-1$. By the fundamental theorem of Galois theory, the elements of $Q(\eta_1)$ are invariant under a subgroup $\mathfrak{H}$ of $\mathfrak{G}$ of order $t = (p-1)/s$. Since a cyclic group has only one subgroup of given order, $\mathfrak{H}$ is generated by the automorphism $\varepsilon \to \varepsilon^{g^s}$. From this it follows that if ε^x is a term of η_i, then $\varepsilon^{g^s x}$ is also a term of η_i. Hence η_i contains the t distinct terms $\varepsilon^x, \varepsilon^{g^s x}, \cdots, \varepsilon^{g^{(t-1)s}x}$, so that $c_1 \geqq t$. Hence $p - 1 = \sum_{i=1}^{h} c_i \geqq hc_1 \geqq ht \geqq st = p-1$. Equality must hold at each stage, and so $c_1 = c_2 = \cdots = c_h = t$, and $h = s$. Moreover each η_i is of the form $\eta_i = \varepsilon^{x_i} + \varepsilon^{g^s x_i} + \cdots + \varepsilon^{g^{(t-1)s}x_i}$, and accordingly each A_i is of the form $A_i = \{x_i, g^s x_i, \cdots, g^{(t-1)s}x_i\}$. Renumbering the A_i if necessary, this is equivalent to assertion (ii).

To prove (iii) it suffices to apply the remark made at the end of § 2, taking Γ to be the group of automorphisms of G generated by the mapping $x \to \mu x$, where μ is an element of order h in the multiplicative group of non-zero residues (mod p).

The determination of the structure constants N_{ijk} of the algebras $\mathfrak{A}_\pi$ of Z_p is an interesting and difficult problem. For a survey of the known results, see [1].

5. The lattice of α-partitions. If π_1 and π_2 are any two partitions of G into disjoint sets, we will say that $\pi_1 \leqq \pi_2$ if every set of π_1 is contained in some set of π_2. This clearly defines a partial ordering, and the purpose of this section is to show that the set of all α-partitions of G is a lattice under this ordering. The following theorem is the key to the proof of this fact.

THEOREM 6. *Let π_0 be a given partition of G. Then the set of α-partitions π satisfying $\pi \leqq \pi_0$ has a greatest element.*

Proof. If π_0 is itself an α-partition the theorem is clearly true. So we can suppose that there are three sets A_i, A_j, A_k of π_0 such that not all elements of A_k are represented the same numbers of times among the products xy, $x \in A_i$ $y \in A_j$. Thus A_k can be decomposed into sets $A_{k1}, A_{k2}, \cdots, A_{k\gamma} (\gamma \geqq 2)$, by putting two elements $u, v \in A_k$ in the same $A_{k\nu}$ if and only if u and v are represented the same number of times in the form xy. Call π_1 the resulting partition of G. If π is an α-partition with $\pi \leqq \pi_0$, then A_i and A_j are both unions of sets of π. Therefore each $A_{k\nu}$ is a union of sets of π, so that $\pi \leqq \pi_1 < \pi_0$. If π_1 is an α-partition we are through; otherwise we can treat π_1 in the same way as π_0, thus obtaining a partition $\pi_2 < \pi_1$ with the property that any α-partition $\pi \leqq \pi_0$ is $\leqq \pi_2$. Proceeding in this manner we obtain a chain $\pi_0 > \pi_1 > \pi_2 \cdots$, which must terminate after a finite number of steps since G is finite.

THEOREM 7. *The α-partitions of G form a lattice L. The weakly and strongly normal α-partitions form sublattices L_w and L_s with $L_s \subseteqq L_w \subseteqq L$.*

Proof. If $\pi_1 : G = \bigcup_{i=1}^{h} A_i$ and $\pi_2 : G = \bigcup_{j=1}^{k} B_j$ are any two α-partitions of G, let π_0 be the partition $G = \cup_{i,j} A_i \cap B_j$. Clearly any α-partition π satisfying $\pi \leqq \pi_1$ and $\pi \leqq \pi_2$ satisfyes $\pi \leqq \pi_0$ and conversely. Hence by Theorem 6 there is a greatest such α-partition, which we denote by $\pi_1 \cap \pi_2$. It follows at once that any finite set $\pi_1, \cdots, \pi_m$ of α-partitions have a meet $\pi_1 \cap \cdots \cap \pi_m$. Therefore any two α-partitions π_1, π_2 have a join $\pi_1 \cup \pi_2$, namely the meet of all α-partitions π such that $\pi_1 \leqq \pi$, $\pi_2 \leqq \pi$.

To prove the second part of the theorem, suppose that π_1 and π_2 are both invariant under a group Σ of automorphisms and antiautomorphisms of G. Then for any $\sigma \in \Sigma$ we have $(\pi_1 \cap \pi_2)^\sigma \leqq \pi_1^\sigma = \pi_1$ and similarly $(\pi_1 \cap \pi_2)^\sigma \leqq \pi_2$. Therefore $(\pi_1 \cap \pi_2)^\sigma \leqq \pi_1 \cap \pi_2$, and reasoning in the same way with σ^{-1}, we see that $(\pi_1 \cap \pi_2)^\sigma = \pi_1 \cap \pi_2$. This shows that $\pi_1 \cap \pi_2$ is invariant under Σ, and the same is of course true of $\pi_1 \cup \pi_2$.

The lattice of α-partitions of G conveys more information about G than its lattice of subgroups. A fuller account of this will be given elsewhere.

REFERENCE

1. R. H. Bruck, *Computational aspects of certain combinatorial problems*, Proceedings of Symposia in Applied Mathematics, **6** (1956), 31-43.