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: $G = \bigcup_{i=1}^{k} A_i$. 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 $\pi$ an $\alpha$-partition.

In this paper all $\alpha$-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 $\alpha$-partition is invariant under the inner automorphisms of $G$ (strongly normal) then it is also invariant under the antiautomorphism $x \to x^{-1}$. For such $\alpha$-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 $\alpha$-partition $\pi$, let $N_{i,j,k}$ 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 $\mathfrak{U}(G)$ is the group algebra of $G$ over a field $K$, and if we put

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

it is clear that $a_i a_j = \sum_{k=1}^{h} N_{i,j,k} a_k$. Therefore the vector space spanned over $K$ by $a_i, \ldots, a_h$ is a subalgebra $\mathfrak{U}_x$ of $\mathfrak{U}(G)$, with structure constants $N_{i,j,k}$. 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 $\mathfrak{U}(G)$, then $\pi$ is an $\alpha$-partition.

In the case where $\pi$ 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 $\mathfrak{U}_x$ is the group algebra $\mathfrak{U}(G/H)$ 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 $\mathfrak{U}_x$.

In this paper some of the elementary properties of $\alpha$-partitions are developed. I plan in a second paper to discuss in more detail the structure of the algebras $\mathfrak{U}_x$ 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 \( \alpha \)-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 \( \alpha \)-partitions should be called normal. Several different definitions of normality are possible, and two of them will be considered here. Note first that if \( \pi \) is an \( \alpha \)-partition, and \( \sigma \) is an automorphism or anti-automorphism of \( G \), then the partition \( \pi^\sigma \) obtained by applying \( \sigma \) to the sets of \( \pi \), is again an \( \alpha \)-partition. If \( \pi = \pi^\sigma \), we will say that \( \pi \) is invariant under \( \sigma \). This means that the sets of \( \pi \) are permuted among themselves by \( \sigma \). If \( \sigma \) has the stronger property of mapping each set of \( \pi \) onto itself, \( \pi \) is called setwise invariant under \( \sigma \).

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

**Theorem 1.** If \( \pi \) is strongly normal, then it is also weakly normal.

**Proof.** Let \( \pi \) be strongly normal, let \( A_i \) be any set of \( \pi \), 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 \( p > n, p \equiv -1 \pmod{n} \), 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 \( x_i \in A_i \), and such that \( t^{-1}x^t = x_1x_2 \cdots x_p \). The mapping \( \theta : (t, x_1, \cdots, x_p) \rightarrow (tx_1, x_2, \cdots, x_p, x_1) \) maps \( S \) onto itself, and so \( S \) is decomposed into orbits by the cyclic group of mappings generated by \( \theta \). 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 \( t^{-1}x^t = x_i^p = x_i^{-1} \), or equivalently \( t^{-1}xt = x_i \). Therefore the number of such \((p + 1)\)-tuples is equal to the number of elements \( t \in H_i \) such that \( t^{-1}A_i t = A_i \). 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 \( \pi \) implies \( t^{-1}A_i t = A_i \); 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 \( N \equiv m_i \pmod{p} \). On the other hand it is immediately seen from the definition of a strongly normal \( \alpha \)-partition that if \( y \) is any element of \( A_i \), then the number of ordered \((p + 1)\)-tuples \((t, x_1, \cdots, x_p)\), \( t \in H_i \), \( x \in A_i \) 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 \( t^{-1}yt = x_i^p = x_i^{-1} \), where \( t \in H_i \), \( x_i \in A_i \) (here we use the fact that \( m_i \leq n < p \)). Hence all \( t \in H_i \) give rise to solutions of this equation. Taking \( t = e \) we get \( y = x_i^{-1} \), so that the inverse of any element of \( A_i \) 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 \( A_i \) is a nonnormal subgroup of \( G \) and \( A_3 = G - A_i \).

3. Weakly normal partitions. In this section we obtain a characteristic property of weakly normal \( \alpha \)-partitions which is useful in the further development of the theory. Let \( \pi : G = \bigcup_{i=1}^{k} A_i \) be any decomposition of \( G \) into disjoint sets (not necessarily an \( \alpha \)-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 \( A_i y \cap A_k \) depends only on \( i, j, k \). We will use the tentative term \( \beta \)-partition to describe such \( \pi \)'s, and will prove that they are precisely the weakly normal \( \alpha \)-partitions. Half of this can be proved at once.

**Theorem 2.** Every weakly normal \( \alpha \)-partition is a \( \beta \)-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 \( N_{k,j',i} \), which depends only on \( i, j, k \). In the same way we see that the cardinality of \( A_i y \cap A_k \), where \( y \in A_j \), depends only on \( i, j, k \), and the proof is complete.

The proof that every \( \beta \)-partition is a weakly normal \( \alpha \)-partition is somewhat more complicated, and we need two lemmas. For any \( \beta \)-partition, let \( Q_{i,j,k} \) denote the cardinality of \( A_i y \cap A_k \), where \( y \in A_j \).

**Lemma 1.** Suppose that the identity element \( e \) of \( G \) is in the set \( A_i \) of a \( \beta \)-partition. Then \( A_i \) is a group. Each \( A_i \) is a union of right cosets \( A_i t \), \( t \in G \), and also a union of left cosets \( tA_i \), \( t \in G \).

**Proof.** Since \( eA_i = A_i \), we must have \( xA_i = A_i \) for any \( x \in A_i \), which proves that \( A_i \) 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 \( x \in A_i \). Hence whenever \( A_i \) contains an element \( t \), it also contains the right coset \( A_i t \). By the same reasoning \( A_i \) contains the left coset \( tA_i \), which completes the proof.
Lemma 2. Let \( A_i \) be any set of a \( \beta \)-partition \( \pi \). Then \( \{x^{-1} \mid x \in A_i\} \) is also a set of \( \pi \).

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

We define the mapping \( i \mapsto i' \) by putting \( A_i = \{x^{-1} \mid x \in A_i\} \).

Theorem 3. Every \( \beta \)-partition is a weakly normal \( \alpha \)-partition.

Proof. Let \( \pi : G = \bigcup_{i=1}^{k} A_i \) be a \( \beta \)-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 \( Q_i \times j \) solutions. Therefore every element of \( A_k \) is represented \( Q_i \times j \) times among the products \( xy, x \in A_i, y \in A_j \), and so \( \pi \) is an \( \alpha \)-partition. It is weakly normal by Lemma 2.

In the next theorem we again let \( A_i \) be the set of \( \pi \) containing \( e \), and denote its cardinality by \( \nu_i \).

Theorem 4. If \( \pi \) is weakly normal, and if \( \nu_i \) is not a multiple of the characteristic of \( K \), then \( A_i \) has a two-sided identity element.

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

We conclude this section with some remarks and examples. Lemma 1 shows that if \( \pi \) is a weakly normal \( \alpha \)-partition, then the set of \( \pi \) containing the identity element is a subgroup of \( G \). If \( G \) is Abelian, then every \( \alpha \)-partition is clearly strongly normal, and hence weakly normal by Theorem 1. Thus in this case the set containing \( e \) is always a subgroup. For non-Abelian groups this need not be so, as can be seen by considering the double coset decomposition \( G = \bigcup_{i=1}^{k} Ha_i K \), 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 \( \alpha \)-partition into the two sets \( A_1 = \{e, (12), (13), (123)\}, A_2 = \{(23), (132)\} \). Here \( A_i \) is not a group.

An important class of weakly normal \( \alpha \)-partitions can be constructed as follows. Let \( \Gamma \) be any group of automorphisms of \( G \), and let the sets of \( \pi \) be the orbits of \( G \) under \( \Gamma \), so that two elements \( x_i, x_2 \in G \)
are in the same set of \( \pi \) if and only if \( x_1^\sigma = x_2 \) for some \( \sigma \in \Gamma \). Then if \( z \) and \( z^\sigma \) 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 \( \pi \) is an \( \alpha \)-partition. Also \( x_1^\sigma = x_2 \) implies \( (x_1^{-1})^\sigma = x_2^{-1} \), so that if \( A_i \) is a set of \( \pi \), so is \( \{x^{-1} \mid x \in A_i\} \). Thus \( \pi \) is weakly normal. It is easily seen that \( \pi \) is strongly normal if and only if \( \Gamma \) is normalized by the group \( I_\sigma \) of inner automorphisms of \( G \). This last situation includes the partition of \( G \) into its conjugacy classes, for then \( I' = I_\sigma \).

4. The case \( G = Z_p \). We next determine all \( \alpha \)-partitions of \( Z_p \), the cyclic group of prime order \( p \). We use the additive notation for \( Z_p \), so that its elements are \( 0, 1, \ldots, p - 1 \), and the group operation is addition \( \pmod{p} \). It is convenient in this case to call the sets of the partition \( A_0, \ldots, A_h \) rather than \( A_1, \ldots, A_h \), 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 \( \alpha \)-partition, so only the second case need be considered. If \( \varepsilon \) 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 \( \mathbb{F}(G) \) over the rational field \( \mathbb{Q} \) homomorphically onto \( \mathbb{Q}(\varepsilon) \). Let \( \eta_i \) be the image of \( a_i \) under this mapping, so that \( \eta_i = \sum_{x \in A_i} \varepsilon^x \).

**Lemma 3.** The \( \eta_i \) 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 \( \leq i, j \leq h \)). Thus the vector \( (\eta_1, \ldots, \eta_h) \) is an eigenvector of the matrix \( (M_{jk}) = (N_{ijk} - N_{ij0}) \) (1 \( \leq j, k \leq h \)) with eigenvalue \( \eta_i \). Since the \( M_{jk} \) are integers, it follows that \( \eta_i \) is an algebraic integer of degree \( \leq h \).

**Theorem 5.** Let \( \bigcup_{i=0}^{h} A_i \) be an \( \alpha \)-partition of \( Z_p \) with \( A_0 = \{0\} \). Then

(i) \( p = 1 \pmod{h} \)

(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 \( \text{ind}_g x = i \pmod{h} \); (i > 0).

(iii) Conversely, for any \( h \) dividing \( p - 1 \), the sets defined in (ii) form an \( \alpha \)-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 \( c_i = \min_{1 \leq i \leq h} c_i \). Theorem 2 implies that
Let $Q \subseteq Q(\eta_i) \subseteq Q(\delta)$, where $S = [Q(\eta_i) : Q] \leq h$. But $Q(\delta)$ is a normal extension of $Q$ whose Galois group $\mathfrak{G}$ is generated by the automorphism $\varepsilon \rightarrow \varepsilon^s$, and is cyclic of order $p - 1$. By the fundamental theorem of Galois theory, the elements of $Q(\eta_i)$ are invariant under a subgroup $\mathfrak{G}$ of $\mathfrak{G}$ of order $t = (p - 1)/h$. Since a cyclic group has only one subgroup of given order, $\mathfrak{G}$ is generated by the automorphism $\varepsilon \rightarrow \varepsilon^s$. From this it follows that if $\varepsilon^s$ is a term of $\eta_i$, then $\varepsilon^s^t$ is also a term of $\eta_i$. Hence $\eta_i$ contains the $t$ distinct terms $\varepsilon^s, \varepsilon^{2s}, \ldots, \varepsilon^{(t-1)s}$, so that $c_i \cong t$. Hence $p - 1 = \sum_{i=1}^{c_i} \cong hc_i \cong ht \cong st = p - 1$. Equality must hold at each stage, and so $c_1 = c_2 = \cdots = c_h = t$, and $h = s$. Moreover each $\eta_i$ is of the form $\eta_i = \varepsilon^s + \varepsilon^s^2 + \cdots + \varepsilon^{(t-1)s}$, and accordingly each $A_i$ is of the form $A_i = \{x_i, g'x_i, \ldots, g'(t-1)x_i\}$. Re-numbering 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 $\Gamma$ to be the group of automorphisms of $G$ generated by the mapping $x \rightarrow \mu x$, where $\mu$ 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 $\mathfrak{A}_s$ of $\mathbb{Z}_p$ is an interesting and difficult problem. For a survey of the known results, see [1].

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

**Theorem 6.** Let $\pi_0$ be a given partition of $G$. Then the set of $\alpha$-partitions $\pi$ satisfying $\pi \leq \pi_0$ has a greatest element.

**Proof.** If $\pi_0$ is itself an $\alpha$-partition the theorem is clearly true. So we can suppose that there are three sets $A_i$, $A_j$, $A_k$ of $\pi_0$ 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 $A_{k1}, A_{k2}, \ldots, A_{k\gamma} (\gamma \cong 2)$, by putting two elements $u, v \in A_k$ in the same $A_{kv}$ if and only if $u$ and $v$ are represented the same number of times in the form $xy$. Call $\pi_i$ the resulting partition of $G$. If $\pi$ is an $\alpha$-partition with $\pi \leq \pi_0$, then $A_i$ and $A_j$ are both unions of sets of $\pi$. Therefore each $A_{kv}$ is a union of sets of $\pi$, so that $\pi \leq \pi_0 < \pi_0$. If $\pi_i$ is an $\alpha$-partition we are through; otherwise we can treat $\pi_i$ in the same way as $\pi_0$, thus obtaining a partition $\pi_2 < \pi_i$ with the property that any $\alpha$-partition $\pi \leq \pi_0$ is $\leq \pi_2$. 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 \( \alpha \)-partitions of \( G \) form a lattice \( L \). The weakly and strongly normal \( \alpha \)-partitions form sublattices \( L_w \) and \( L_s \) with \( L_s \subseteq L_w \subseteq L \).

**Proof.** If \( \pi_1 : G = \bigcup_{i=1}^{a} A_i \) and \( \pi_2 : G = \bigcup_{j=1}^{b} B_j \) are any two \( \alpha \)-partitions of \( G \), let \( \pi_0 \) be the partition \( G = \bigcup_{i} A_i \cap B_j \). Clearly any \( \alpha \)-partition \( \pi \) satisfying \( \pi \leq \pi_1 \) and \( \pi \leq \pi_2 \) satisfies \( \pi \leq \pi_0 \) and conversely. Hence by Theorem 6 there is a greatest such \( \alpha \)-partition, which we denote by \( \pi_1 \cap \pi_2 \). It follows at once that any finite set \( \pi_1, \cdots, \pi_m \) of \( \alpha \)-partitions have a meet \( \pi_1 \cap \cdots \cap \pi_m \). Therefore any two \( \alpha \)-partitions \( \pi_1, \pi_2 \) have a join \( \pi_1 \cup \pi_2 \), namely the meet of all \( \alpha \)-partitions \( \pi \) such that \( \pi_1 \leq \pi, \pi_2 \leq \pi \).

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

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

**Reference**
