SEQUENCES IN GROUPS WITH DISTINCT PARTIAL PRODUCTS

BASIL GORDON

1. In an investigation concerning a certain type of Latin square, the following problem arose:

Can the elements of a finite group G be arranged in a sequence $a_1, a_2, \cdots, a_n$ so that the partial products $a_1, a_1a_2, \cdots, a_1a_2 \cdots a_n$ are all distinct?

In the present paper a complete solution will be given for the case of Abelian groups, and the application to Latin squares will be indicated. Let us introduce the term *sequenceable group* to denote groups whose elements can be arranged in a sequence with the property described above. The main result is then contained in the following theorem.

THEOREM 1. *A finite Abelian group G is sequenceable if and only if G is the direct product of two groups A and B, where A is cyclic of order 2^k $(k > 0)$, and B is of odd order.*

Proof (i). To see the necessity of the condition, suppose that G is sequenceable, and let $a_1, a_2, \cdots, a_n$ be an ordering of the elements of G with $a_1, a_1a_2, \cdots, a_1a_2 \cdots a_n$ all distinct. The notation $b_i = a_1a_2 \cdots a_i$ will be used throughout the remainder of the paper. It is immediately seen that $a_1 = b_1 = e$, the identity element of G; for if $a_i = e$ for some $i > 1$, then $b_{i-1} = b_i$, contrary to assumption. Hence $b_n \neq e$, i.e., the product of all the elements of G is not the identity. It is well known (cf [2]) that this implies that G has the form $A \times B$ with A cyclic of order $2^k(k > 0)$ and B of odd order.

(ii) To prove sufficiency of the condition, suppose that $G = A \times B$, with A and B as above. We then show that G is sequenceable by constructing an ordering $a_1, a_2, \cdots, a_n$ of its elements with distinct partial products. From the general theory of Abelian groups, it is known that G has a basis of the form $c_0, c_1, \cdots, c_m$, where c_0 is of order 2^k, and where the orders $\delta_1, \delta_2, \cdots, \delta_m$ of $c_1, c_2, \cdots, c_m$ are odd positive integers each of which divides the next, i.e., $\delta_i \mid \delta_{i+1}$ for $0 < i < m$. If j is any positive integer, then there exist unique integers $j_0, j_1, \cdots, j_m$ such that

$$(1) \qquad \begin{aligned} &j \equiv j_0 (\mathrm{mod}\ \delta_1 \delta_2 \cdots \delta_m) \\ &j_0 = j_1 + j_2\delta_1 + j_3\delta_1\delta_2 + \cdots + j_m\delta_1 \cdots \delta_{m-1} \\ &\quad 0 \leqq j_1 < \delta_1 \end{aligned}$$

Received January 3, 1961.

$$\begin{aligned}&0 \leqq j_2 < \delta_2\\&\vdots\\&0 \leqq j_m < \delta_m\,.\end{aligned}$$

The proof of the existence and uniqueness of this expansion will be omitted here; it is entirely analogous to the expansion of an integer in powers of a number base.

We are now in a position to define the desired sequencing of G. It is convenient to define the products $b_1, b_2, \cdots, b_n$ directly, to prove they are all distinct, and then to verify that the corresponding a_i, as calculated from the formula $a_1 = e$, $a_i = b_{i-1}^{-1}b_i$, are all distinct. If i is of the form $2j + 1 (0 \leqq j < n/2)$, let

$$b_{2j+1} = c_0^{-j}c_1^{-j_1}c_2^{-j_2} \cdots c_m^{-j_m}\,,$$

where $j_1, j_2, \cdots, j_m$ are the integers defined in (1). On the other hand, if i is of the form $2j + 2 (0 \leqq j < n/2)$, let

$$b_{2j+2} = c_0^{j+1}c_1^{j_1+1}c_2^{j_2+1} \cdots c_m^{j_m+1}\,.$$

The elements $b_1, b_2, \cdots, b_n$ thus defined are all distinct. For if $b_s = b_t$ with $s = 2u + 1$, $t = 2v + 1$, then

$$\begin{aligned}u &\equiv v (\mathrm{mod}\ 2^k)\\u_1 &\equiv v_1 (\mathrm{mod}\ \delta_1)\\&\vdots\\u_m &\equiv v_m (\mathrm{mod}\ \delta_m)\,.\end{aligned}\tag{2}$$

From the inequalities in (1) we conclude that $u_1 = v_1, \cdots, u_m = v_m$. Hence $u_0 = v_0$, so that $u \equiv v (\mathrm{mod}\ \delta_1 \cdots \delta_m)$; coupled with the first of equations (2), this gives $u \equiv v\ (\mathrm{mod}\ n)$, which implies $u = v$. Similarly $b_{2u+2} = b_{2v+2}$ implies $u = v$, so that the "even" b's are distinct.

Next suppose

$$b_{2u+1} = b_{2v+2}\,.$$

Then

$$\begin{aligned}-u &\equiv v + 1\ (\mathrm{mod}\ 2^k)\\-u_1 &\equiv v_1 + 1\ (\mathrm{mod}\ \delta_1)\\&\vdots\\-u_m &\equiv v_m + 1\ (\mathrm{mod}\ \delta_m)\end{aligned}$$

or equivalently,

$$u + v + 1 \equiv 0\ (\mathrm{mod}\ 2^k)\tag{3}$$

$$\begin{gathered} u_1 + v_1 + 1 \equiv 0 \pmod{\delta_1} \\ \vdots \\ u_m + v_m + 1 \equiv 0 \pmod{\delta_m} . \end{gathered}$$

Since $0 < u_1 + v_1 + 1 \leqq 2(\delta_1 - 1) + 1 < 2\delta_1$, we must have $u_1 + v_1 + 1 = \delta_1$. Reasoning similarly for $i = 2, \cdots, m$ we obtain

$$\begin{gathered} u_1 + v_1 + 1 = \delta_1 \\ u_2 + v_2 + 1 = \delta_2 \\ \vdots \\ u_m + v_m + 1 = \delta_m . \end{gathered}$$

Multiplying the $(i + 1)$'st equation of this system by $\delta_1\delta_2 \cdots \delta_i$ $(1 \leqq i < m)$ and adding, we get $u_0 + v_0 + 1 = \delta_1 \cdots \delta_m$, which implies $u + v + 1 \equiv o(\delta_1 \cdots \delta_m)$. Combining this with the first of equations (3), we find that $u + v + 1 \equiv 0 \pmod{n}$, which, on account of the inequality $0 < u + v + 1 < n$, is impossible. Hence $b_1, b_2, \cdots, b_n$ are all distinct.

Next we calculate $a_1, a_2, \cdots, a_n$. If $i = 2j + 2$ $(0 \leqq j < n/2)$, then

$$a_i = b_{i-1}^{-1} b_i = c_0^{2j+1} c_1^{2j_1+1} \cdots c_m^{2j_m+1} .$$

These are all different by the same argument as above. If $i = 2j + 1$, and $j_1 \neq 0$, then

$$a_i = c_0^{-2j} c_1^{-2j_1} c_2^{-2j_2-1} \cdots c_m^{-2j_m-1} .$$

If $i = 2j + 1$ and $j_1 = 0$, but $j_2 \neq 0$, then $a_i = c_0^{-2j} c_2^{-2j_2} c_3^{-2j_3-1} \cdots c_m^{-2j_m-1}$, while if $j_1 = j_2 = 0$ but $j_3 \neq 0$, then $a_i = c_0^{-2j} c_3^{-2j_3} c_4^{-2j_4-1} \cdots c_m^{-2j_m-1}$, etc. These a_i's are obviously distinct from each other by the same reasoning as before. Because of the exponent of c_0 they are also distinct from the a_i with i even. This completes the proof of the theorem.

As an example of the construction of Theorem 1, consider the group $G = C_2 \times C_3 \times C_3$. We use basis elements c_0, c_1, c_2 of orders 2, 3, 3 respectively. Using the notation (α, β, γ) for the element $c_0^\alpha c_1^\beta c_2^\gamma$, the sequences a_i and b_i are then the following:

a_i	b_i
(0 0 0)	(0 0 0)
(1 1 1)	(1 1 1)
(0 1 2)	(1 2 0)
(1 0 1)	(0 2 1)
(0 2 2)	(0 1 0)
(1 2 1)	(1 0 1)
(0 0 1)	(1 0 2)
(1 1 0)	(0 1 2)

a_i	b_i
(0 1 0)	(0 2 2)
(1 0 0)	(1 2 2)
(0 2 0)	(1 1 2)
(1 2 0)	(0 0 2)
(0 0 2)	(0 0 1)
(1 1 2)	(1 1 0)
(0 1 1)	(1 2 1)
(1 0 2)	(0 2 0)
(0 2 1)	(0 1 1)
(1 2 2)	(1 0 0)

2. Application to Latin squares. Consider the following Latin square:

$$\begin{matrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \\ 3 & 1 & 4 & 2 \\ 4 & 3 & 2 & 1 \end{matrix}$$

Given any ordered pair $(\alpha\beta)$ with $\alpha \neq \beta$, it occurs as a pair of consecutive entries in some row of this square. In general, an $n \times n$ Latin square (c_{st}) whose elements are the integers $1, \cdots, n$ will be called *horizontally complete* if for every ordered pair (α, β) with $1 \leqq \alpha,\ \beta \leqq n$ and $\alpha \neq \beta$, the equations

$$\begin{aligned} c_{st} &= \alpha \\ c_{s,t+1} &= \beta \end{aligned} \tag{4}$$

are solvable. Similarly a vertically complete square is one for which

$$\begin{aligned} c_{st} &= \alpha \\ c_{s+1,t} &= \beta \end{aligned}$$

can be solved for any such choice of α, β. A square which is both horizontally and vertically complete is called complete.

Note that in a horizontally complete square, the solution of equations (4) is unique, since the total number of consecutive pairs a_{st}, $a_{s,t+1}$ is equal to the total number of order pairs (α, β) with $\alpha \neq \beta$. Conversely, uniqueness implies existence for the same reason.

Complete Latin squares are useful in the design of experiments in which it is desired to investigate the interaction of nearest neighbors.

THEOREM 2. *Suppose that G is a sequenceable group, and let a_1, $a_2 \cdots, a_n$ be an ordering of its elements such that $b_1, b_2, \cdots, b_n$ are distinct. Then the matrix $(c_{st}) = (b_s^{-1}b_t)$ is a complete Latin square.*

Proof. It is immediately seen that (c_{st}) is a Latin square, since either $b_s^{-1}b_t = b_s^{-1}b_u$ or $b_t^{-1}b_s = b_u^{-1}b_s$ imply $t = u$ by elementary properties of groups. To show that (c_{st}) is horizontally complete, suppose

$$c_{st} = c_{uv}$$
$$c_{s,t+1} = c_{u,v+1} .$$

We must show that $s = u$ and $t = v$. From the definition of c_{st},

$$b_s^{-1}b_t = b_u^{-1}b_v \tag{5}$$

$$b_s^{-1}b_{t+1} = b_u^{-1}b_{v+1} . \tag{6}$$

Inverting both sides of (5) yields $b_t^{-1}b_s = b_v^{-1}b_u$. Combining this with (6) we get $(b_t^{-1}b_s)(b_s^{-1}b_{t+1}) = (b_v^{-1}b_u)(b_u^{-1}b_{v+1})$, or $b_t^{-1}b_{t+1} = b_v^{-1}b_{v+1}$, i.e., $a_{t+1} = a_{v+1}$. This implies $t = v$. Substituting in (5) we obtain $b_s^{-1}b_t = b_u^{-1}b_t$, from which $s = u$ follows immediately. The proof that (c_{st}) is vertically complete is entirely similar and will be omitted.

This method enables one to construct a complete Latin square of order n for any even n (note that B may be trivial in Theorem 1). Whether or not complete, or even horizontally complete, squares exist for odd n is an open question.

3. Extension to non-Abelian groups. The problem of determining which non-Abelian groups G are sequencable is unsolved at the present time. Considerable information about the nature of a sequence $a_1, \cdots, a_n$ with distinct partial products, if one exists, can be obtained by mapping G onto the Abelian group G/C, where C is the commutator subgroup. Using this technique, for example, it can be shown that the non-Abelian group of order 6 and the two non-Abelian groups of order 8 are not sequencable. On the other hand the non-Abelian group of order 10 is sequencable. To see this, denote its elements by $e, a, b, ab, ba, aba, bab, abab, baba, ababa$, where $a^2 = b^2 = (ab)^5 = e$. A suitable ordering is then given by $e, ab, abab, ababa, bab, aba, b, a, baba, ba$, the partial products being $e, ab, baba, a, abab, bab, ba, b, aba, ababa$. In view of Theorem 1 and the results of [2], one might conjecture that G is sequencable if and only if it does not possess a complete mapping. However, the symmetric group S_3 does not possess a complete mapping (cf [1]) and is also not sequenceable. Whether or not the two properties are at least mutually exclusive is still an open question.

REFERENCES

1. L. J. Paige, *Complete mappings of finite groups*, Pacific J. Math. **1** (1951), 111-116.
2. M. Hall and L. J. Paige, *Complete mappings of finite groups*, Pacific J. Math. **5** (1955), 541-549.

UNIVERSITY OF CALIFORNIA, LOS ANGELES