TWO-GENERATOR GROUPS, I

J. L. Brenner and James Wiegold

1. INTRODUCTION

The theory of generators for discrete groups has a long history: an authoritative text is Coxeter and Moser [5]. Miller [9] found two-element bases for alternating and symmetric groups. He showed that nearly all these groups can be generated by an element of order 2 and an element of order 3. Explicit generators of this type are given in [6]. Brahana [4] showed that every known finite nonabelian simple group G of order less than 10^6 has a two-element basis: $G = \langle a, b \rangle$, where a has order 2. The same result was established for the projective special linear groups PSL(n, q) ($(n, q) \neq (2, 2), (2, 3)$) by Albert and Thompson in [1]. Steinberg proved that every known finite simple group has a two-element basis [12], and as far as we know, the same is true for every simple group discovered since that time. In another direction, Binder [2], [3] showed that for any two nontrivial elements x_1, x_2 of the symmetric group $\mathscr{S}_n$, $n > 4$, there exists a third element y such that $\mathscr{S}_n = \langle x_1, y \rangle = \langle x_2, y \rangle$. Thus the element y acts simultaneously as a mate for either x_1 or x_2. In fact, he proved a little more, and his work inspires the following definition:

1.01 *Definition.* Let r be any positive integer. A finite nonabelian group G is said to have *spread* r if, for every set $\{x_1, x_2, \cdots, x_r\}$ of nontrivial elements of G, an element y of G can be found such that $\langle x_i, y \rangle = G$ for each i. Let Γ_r denote the collection of groups having spread r.

The content of Binder's cited work is that the symmetric group $\mathscr{S}_{2m}$ is in $\Gamma_2 \setminus \Gamma_3$, while $\mathscr{S}_{2m+1}$ is in $\Gamma_3 \setminus \Gamma_4$, apart from a few easy exceptions.

Clearly $\Gamma_r \supseteq \Gamma_{r+1}$ for each r. The structure of groups of this sort is very restricted. We recall that a group is *monolithic* if the intersection of all nontrivial normal subgroups is nontrivial; the *monolith* is this intersection.

1.02 LEMMA. *Let* G *be any group of spread* 1: $G \in \Gamma_1$. *Then* G *is monolithic, the derived group* G' *is the monolith, and* G/G' *is cyclic.*

Proof. Let A be a nontrivial normal subgroup of G; let x be any nontrivial element of A. Then $\langle x, y \rangle = G$ for some y in G, so that G/A is *cyclic*. From this it follows that $G' \subseteq A$. ||

In section 2 we give a characterization of those groups G that lie in Γ_1 and have abelian monolith. This category is precisely the set of JM-groups of M. F. Newman [11]; the structure of these groups is therefore completely determined. It will appear that every JM-group is in Γ_3, so that every *solvable* group of spread 1 is already of spread 3.

As we just saw, Binder dealt with the symmetric groups. The situation for alternating groups is radically different. In section 3, we shall prove that the alternating group $\mathscr{A}_{2m}$ is in $\Gamma_4 \setminus \Gamma_5$ for m = 2 and $m \geq 4$, while $\mathscr{A}_6$ (ever the

Received May 24, 1974.