# 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 $\mathcal{S}_n$, $n > 4$, there exists a third element y such that $\mathcal{S}_n = \langle x_1, y \rangle = \langle x_2, y \rangle$. 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 $\Gamma_r$ denote the collection of groups having spread r.

The content of Binder's cited work is that the symmetric group $\mathcal{S}_{2m}$ is in $\Gamma_2 \setminus \Gamma_3$, while $\mathcal{S}_{2m+1}$ 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 $\Gamma_1$ 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 $\Gamma_3$, 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 $\mathcal{A}_{2m}$ is in $\Gamma_4 \setminus \Gamma_5$ for $m = 2$ and $m \geq 4$, while $\mathcal{A}_6$ (ever the

Received May 24, 1974.

Michigan Math. J. 22 (1975).

exception!) is in $\Gamma_2 \setminus \Gamma_3$. The proof that $\mathcal{A}_{2m}$ is in $\Gamma_4$ for $m \geq 4$ is a relatively easy combinatorial argument based on a result of Williamson [14]. For alternating groups of odd degree, we are at a loss to make a sensible conjecture. The group $\mathcal{A}_5$ has spread 2 (and not 3). It is easy to see that $\mathcal{A}_n$ cannot have spread as great as $(n - 2)! + 3$, and that this bound can be improved in many cases. For example, let t denote the integer $17!/(3^4 6!)$. Then $\mathcal{A}_{19}$ has spread t - 1 (that is, 6, 098, 892, 799), but not spread t + 3, as we shall see in section 4. Moreover, if p is any prime such that the only unsolvable transitive groups of degree p are $\mathcal{A}_p$ and $\mathcal{S}_p$, then $\mathcal{A}_p$ also has vast spread. We shall treat $\mathcal{A}_{19}$ in detail in section 4; the result for any prime p with the property mentioned in the preceding sentence will be roughly similar.

The tracking-down of the primes with the property just mentioned (the "good" primes, we shall call them) is a difficult task indeed—see P. M. Neumann [10] and the literature cited there. Dr. M. D. Atkinson has informed us that he and Neumann are studying the primes up to 100 with the aid of Cardiff's ICL 4-70 computer. However, it ought to be possible to give an affirmative answer to our first problem without a detailed knowledge of the good primes.

1.03 PROBLEM. *Let* f(p) *denote the largest integer such that* $\mathcal{A}_p$ *has spread* f(p), *for primes* p. *Does* f(p) *tend to infinity with* p?

In section 4, we prove that if $q \equiv 1 \mod 4$, $q > 9$, the spread of PSL(2, q) is q - 1. If $q \equiv 3 \mod 4$, $q > 7$, the spread is q - 4; if q is even, the spread is q - 2. The methods are closely related to those used on $\mathcal{A}_p$. Thus there are simple groups, as well as solvable groups (see section 2) with arbitrarily large spread.

In section 6, we return to the groups PSL(2, q). Let $\Gamma_1^{(k)}$ stand for the collection of all finite nonabelian groups with the property that every nontrivial element is in a two-element basis in which one of the two generators has order k. We have here the extra information that the group PSL(2, q) lies in $\Gamma_1^{(2)}$ except when $q = 2, 3, 9$.

Also in section 6, we show that the groups PSL(n, q) with q odd and $n > 2$, or with q arbitrary and $n > 3$, are outside $\Gamma_1^{(2)}$. When n = 3, the group PSL(3, 2) is in $\Gamma_1^{(2)}$; for $s > 2$, the group $PSL(3, 2^s)$ is not in $\Gamma_1^{(2)}$. We also show that PSL(n, q) is not in $\Gamma_1^{(k)}$ if n is large, $n > N(k)$. These curious results arise from the geometry of the groups in question.

Finally, we pose some problems concerning spread.

1.04 PROBLEM. *What groups lie in* $\Gamma_1 \setminus \Gamma_2$? *In particular, is this set perhaps finite*?

As we said earlier, all groups in $\Gamma_1 \setminus \Gamma_2$ are unsolvable.

1.05 PROBLEM. *Are almost all finite simple groups in* $\Gamma_1^{(2)}$ *projective special linear groups*?

We are grateful to L. Carlitz for providing the results in section 7, on which the calculations in section 6 rest. We also thank the referee, Dr. P. M. Neumann, for pointing out a large mistake in an earlier version of the paper, for adding certain information concerning PSL(2, q) in section 4, for remedying our initial ignorance concerning $PSL(3, 2^m)$ in section 6, and for many useful suggestions.

## 2. $\Gamma_1$-GROUPS WITH ABELIAN MONOLITHS

We can sum up the main result of this section as follows:

2.01 THEOREM. (i) *Every group* G *in* $\Gamma_1$ *and having abelian monolith is just-metabelian (that is,* G *is solvable, non-nilpotent, and every proper homomorphic image is abelian).*

(ii) *Conversely, let* G *be a finite just-metabelian group and set* $|G'| = r$, $|G/G'| = k$. *Then* G *is in* $\Gamma_{r-1} \setminus \Gamma_r$ *if* k *is not prime, and* G *is in* $\Gamma_r \setminus \Gamma_{r+1}$ *if* k *is prime.*

*Proof.* Part (i) follows immediately from lemma 1.02, since the Frattini subgroup of every group in $\Gamma_1$ is trivial, and such groups are not nilpotent.

For part (ii), let G be just-metabelian. Then by [11], G is monolithic; the monolith is G'; it is abelian and complemented in G; the complements are maximal, cyclic, pairwise disjoint, and conjugate, and they are centralizers of the elements outside G'; moreover, there are precisely r such complements. Let $x_1, \cdots, x_s$, $y_1, \cdots, y_t$ be any nontrivial elements of G, where the $x_i$ are in G' and the $y_j$ outside G'. If $s + t < r$, then there must exist a complement $\langle a \rangle$ of G' such that $\langle a \rangle \neq C(y_j)$ for $j = 1, \cdots, t$. The properties just mentioned now imply that $G = \langle a, x_i \rangle = \langle a, y_j \rangle$ for each i, j. This shows that G is in $\Gamma_{r-1}$ in all cases.

Suppose now that k is not prime, let p be a prime divisor of k, and let a be a generator of an arbitrary complement of G'. The conjugates of a are precisely the elements $x^{-1}ax$, where x ranges over G', and by what was said above, every element outside G' centralizes one of these elements. To show that G is not in $\Gamma_r$, consider the r-element set $X = \{x^{-1}a^p x \mid x \in G'\}$. Firstly, $\langle a^p, x \rangle \neq G$ for every x in G', since of course a is not in $\langle a^p, x \rangle$. Thus no element of G' can be a "supplementary generator" for every element in X. But because every element outside G' centralizes one of the elements of X, no element outside G' works either.

On the other hand, suppose that k is prime. To prove that G is in $\Gamma_r$, observe that the argument two paragraphs back works with $s + t = r$ unless $s = 0$ and $y_1, \cdots, y_r$ lie in r different centralizers of elements outside G . In the case where k is prime, $y_1, \cdots, y_r$ must actually generate these centralizers in any troublesome situation; therefore, if x is a nontrivial element of G', then $G = \langle y_i, x \rangle$ for each i. Thus $G \in \Gamma_r$. But $G \notin \Gamma_{r+1}$, since no element of G works with each element of $\{g, y_1, \cdots, y_r\}$, where now g is a nontrivial element of G' and $y_1, \cdots, y_r$ generate the r centralizers of elements outside G'.

2.02 COROLLARY. *If* G *is any solvable group in* $\Gamma_1$, *then* G *is in* $\Gamma_3$.

*Proof.* This is because G is just-metabelian and part (ii) works. G is in $\Gamma_3$ unless $|G'| \leq 3$; but $|G'| \leq 3$ only if G is the symmetric group on three letters, and in this case, $|G/G'|$ is prime.

## 3. ALTERNATING GROUPS OF EVEN DEGREE

The negative result here is relatively easy:

3.01 LEMMA. *For* $n \geq 2$, $\mathcal{A}_{2n}$ *is outside* $\Gamma_5$.

*Proof.* For $n = 2$, it is easy to verify that there is no common "mate" in $\mathcal{A}_4$ for the five elements

$$(1\,2\,3),\ (1\,2\,4),\ (1\,3\,4),\ (2\,3\,4),\ (1\,2)(3\,4).$$

Now suppose that $n > 2$ and consider the five elements $x_i$:

$$(2\,3)(4\,5),\ (1\,4)(3\,5),\ (1\,5)(2\,4),\ (1\,3)(2\,5),\ (1\,2)(3\,4).$$

We shall show that there is no common mate y in $\mathcal{A}_{2n}$ for each of these five elements. Firstly, y would have to move all the permuted symbols 1, 2, $\cdots$, 2n. Thus, since the canonical decomposition of every element of $\mathcal{A}_{2n}$ has an even number of cycles, it follows by transitivity that y is a product of exactly two cycles. It is a routine task, which we leave to the reader, to verify that every two-cycle element y must generate an intransitive subgroup with at least one of the five elements $x_i$.

As so often happens, $\mathcal{A}_6$ requires special arguments. It has been known for some time [9] that $\mathcal{A}_6$ cannot be generated by an element of order 2 and one of order 3; thus any element of $\mathcal{A}_6$ which is a common mate for each of the three elements

$$(1\,3)(2\,4),\ (1\,5)(2\,6),\ (3\,6)(4\,5)$$

must be a product of a 4-cycle and a transposition. A tedious verification shows that every such element generates either an intransitive subgroup, or else a transitive but imprimitive subgroup of $\mathcal{A}_6$, with at least one of the displayed permutations. Thus $\mathcal{A}_6 \notin \Gamma_3$. An equally tedious verification shows that every pair of nontrivial elements in $\mathcal{A}_6$ can be simultaneously mated by an element of order 4. The case of $\mathcal{A}_4$ is trivial, and we may make the following assertion.

3.02 PROPOSITION. *The relations* $\mathcal{A}_4 \in \Gamma_4 \setminus \Gamma_5$, $\mathcal{A}_6 \in \Gamma_2 \setminus \Gamma_3$ *hold.*

In the remainder of this section, $n \geq 4$. The basis of the argument is the following elegant theorem of Williamson [14].

3.03 THEOREM. *Let* G *be a primitive permutation group of degree* m *containing a nontrivial cyclic permutation of degree* t. *If* G *is neither alternating nor symmetric, then* $t > (m - t)!$.

3.04 COROLLARY. *Let* n *be an integer greater than* 3 *and let* x *denote the element* $(1, 2, \cdots, n+1)(n+2, \cdots, 2n)$ *of* $\mathcal{A}_{2n}$ *if* n *is even, and* $(1, 2, \cdots, n+2)(n+3, \cdots, 2n)$ *if* n *is odd. Then the only transilive subgroup of* $\mathcal{A}_{2n}$ *containing* x *is* $\mathcal{A}_{2n}$ *itself.*

*Proof.* First consider the case of even n. Here $n + 1$ and $n - 1$ are relatively prime, so that any transitive subgroup H of $\mathcal{A}_{2n}$ containing x contains an $(n + 1)$-cycle and an $(n - 1)$-cycle. But on the one hand, $n + 1$ is prime to 2n, since n is even. On the other hand, $n + 1$ is more than half of 2n, so that H is in fact *primitive*. Williamson's theorem 3.03 now applies, with $m = 2n$ and $t = n + 1$. It shows that H is $\mathcal{A}_{2n}$. The case of odd n is similar.

As an aside, we observe that corollary 3.04 is true for $n = 2$ as well, but not for $n = 3$: this because $\mathcal{A}_5$ has a primitive representation of degree 6.

We call an element of $\mathcal{A}_{2n}$ having the same shape as those figuring in corollary 3.04 a *standard element.* Thus a standard element is a product of an $(n+1)$-cycle and an $(n-1)$-cycle if $n$ is even, and is the product of an $(n+2)$-cycle and an $(n-2)$-cycle if $n$ is odd. The standard elements have the virtue that they are extremely numerous, and they have a strong tendency to belong to two-element bases for $\mathcal{A}_{2n}$. Given a standard element $x$, all one has to do is find an element $y$ such that $\langle x, y \rangle$ is transitive.

3.05 THEOREM. *For any four nontrivial elements* $x_1, x_2, x_3, x_4$ *of* $\mathcal{A}_{2n}$, $n \geq 4$, *there exists a standard element* $y$ *such that* $\langle x_i, y \rangle = \mathcal{A}_{2n}$ *for each* $i$.

To substantiate 3.05, we restate the problem in a combinatorial way as follows. We are working inside $\mathcal{A}_{2n}$, and we assume that the set of permuted symbols is $\Omega = \{1, 2, \cdots, 2n\}$; the data consist of four elements $x_1, x_2, x_3, x_4$ of $\mathcal{A}_{2n}$.

We call two elements $\alpha, \beta$ $(\alpha \neq \beta)$ of $\Omega$ $x_i$-*partners* if $\alpha x_i^{\nu} = \beta$ for some $\nu$. If we can complete the following construction, theorem 3.05 will be established.

3.06 *Construction.* Given $x_1, x_2, x_3, x_4$, we must partition $\Omega$ into the union of two disjoint subsets $T_1, T_2$ in such a way that

(i) $|T_1| = n - 1$ if $n$ is even, and $|T_1| = n - 2$ if $n$ is odd, so that $(|T_1|, |T_2|)$ is the type of a standard element;

(ii) for each $i = 1, 2, 3, 4$, there exist two $x_i$-partners $\alpha_i, \beta_i$ such that $\alpha_i \in T_i$, $\beta_i \in T_2$.

Once this is done, set $y = uv$, where $u$ is a cycle on the elements of $T_1$, in any order; and $v$ is a cycle on the element of $T_2$. Then $\langle x_i, y \rangle$ is transitive for each $i$, and so is the whole of $\mathcal{A}_{2n}$ by corollary 3.04.

The construction proceeds in several steps. We shall build up $T_1, T_2$, piece-by-piece until we are satisfied that the construction has gone far enough.

We begin by choosing, in the canonical decomposition of each $x_i$, a cycle $x_i'$ of more than two letters if such a cycle exists. If $x_i$ contains no such cycle, we choose for $x_i'$ the product of a pair of transpositions in $x_i$. It is not required that $x_i'$ even lie in $\mathcal{A}_{2n}$. We note that if $\alpha_i, \beta_i$ are $x_i'$-partners, they certainly are $x_i$-partners. Thus construction 3.06 will be completed if from now on, we simply replace each $x_i$ by the piece $x_i'$. There are three cases: (3.07), (3.08), (3.09). Suppose first that the relation

$$\text{Supp}(x_i') \cap \text{Supp}(x_j') = \emptyset \text{ for } i \neq j \tag{3.07}$$

holds. This case is straightforward. Clearly $2n \geq 12$, so that $n \geq 6$.

If $\alpha_i$ is some element of $\text{Supp}(x_i')$ $(i = 1, 2, 3, 4)$, we include $\alpha_1, \cdots, \alpha_4$ in $T_1$ (this is allowable, because $|T_1| \geq n - 2 > 4$) and we include $\alpha_1 x_1', \cdots, \alpha_4 x_4'$ in $T_2$; then we fill up $T_1, T_2$ in any arbitrary way.

We may now assume, without loss of generality, that $\text{Supp}(x_1') \cap \text{Supp}(x_2')$ is not empty; let 1 denote a symbol in this intersection, renaming symbols if necessary. It may be that the condition

(3.08) *The symbol* 1 *has an* $x_1'$*-partner that is also an* $x_2'$*-partner*

holds. Let 2 be such a common partner. We put 1 in $T_1$ and 2 in $T_2$; this already accommodates $x_1'$ and $x_2'$. There are two possibilities under (3.08). The first is:

(3.081) *There exist* $x_3'$*-partners* $\alpha$, $\beta$, *both different from* 1, 2. Here we have some freedom of choice: we can take either

$$(3.0811)\quad T_1 = \{1, \alpha, \cdots,\}, \qquad T_2 = \{2, \beta, \cdots\},$$

or

$$(3.0812)\quad T_1 = \{1, \beta, \cdots\}, \qquad T_2 = \{2, \alpha, \cdots\},$$

and we have accommodated $x_1'$, $x_2'$, $x_3'$. If $x_4'$ is a 3-cycle, or if $x_4' = (1\,2)(\alpha\,\beta)$, or if $x_4' = (1\,\beta)(2\,\alpha)$, then (3.0811) is an allowable partitioning; if $x_4' = (1\,\alpha)(2\,\beta)$, we can use (3.0812). This finishes case (3.081).

If (3.08) holds but (3.081) does not, then it must be true that:

(3.082) *Every pair of* $x_3'$*-partners contains* 1 *or* 2.

Thus, $x_3'$ is of the form $(1\,2\,\alpha)^{\pm 1}$ or $(1\,\alpha)(2\,\beta)$; and clearly we may assume that the same is true of $x_4'$, else the problem is reducible to (3.081). Since 1 is in $T_1$ and 2 is in $T_2$, we have already accommodated elements like $(1\,2\,\alpha)^{\pm 1}$; thus we have only to think about the case where $x_3'$ and $x_4'$ are both of the general form $(1\,\alpha)\,(2\,\beta)$. But this case is trivial.

If neither (3.07) nor (3.08) holds, the following is clearly valid.

(3.09) *There is no element* v *of* $\Omega$ *with an* $x_i'$*-partner that is also an* $x_j'$*-partner for* $i \neq j$.

Let 1, 2 be $x_1'$-partners and let 1, 3 be $x_2'$-partners. We begin by including 1 in $T_1$ and 2, 3 in $T_2$. There are two subcases.

(3.091) $x_3'$ *has a pair of partners* $\alpha$, $\beta$ *both different from* 1, 2, 3.

This subcase proceeds just as case (3.081). The final possibility is

(3.092) *Every pair of* $x_3'$*-partners includes at least one of* 1, 2, 3.

And, of course, the same is true of $x_4'$. We tentatively put 1 in $T_1$ and 2, 3 in $T_2$. This accommodates all possibilities for $x_3'$ except those in which $x_3'$ is one of

$$(2\,3\,\alpha)^{\pm 1}, \quad (1\,\alpha)(2\,3), \quad (1\,\alpha)(2\,\beta), \quad (1\,\alpha)(3\,\beta), \quad (2\,\alpha)(3\,\beta),$$

where now $\alpha$, $\beta$ are different from 1, 2, 3. The reader will have no difficulty in completing the construction in these cases; we observe that the contingency $x_3' = (2\,3\,\alpha)^{\pm 1}$, $x_4' = (1\,\alpha)(2\,3)$ is excluded, since 2 has 3 as an $x_3'$-partner and also as an $x_4'$-partner.

We sum up our findings.

3.10 THEOREM. *For* $n = 2$ *or* $n \geq 4$, $\mathcal{A}_{2n}$ *is in* $\Gamma_4 \setminus \Gamma_5$; $\mathcal{A}_6$ *is in* $\Gamma_2 \setminus \Gamma_3$.

## 4. THE GROUPS $\mathcal{A}_p$ AND PSL(2, q)

As we mentioned in the introduction, certain primes p are good in the sense that the only unsolvable transitive groups of degree p are $\mathcal{A}_p$ and $\mathcal{S}_p$. To avoid certain complications and to illustrate the possibilities, let us consider the case of $\mathcal{A}_{19}$ in detail, 19 being a good prime.

Let the 19 symbols now be 0, 1, ⋯, 18, i.e., the residue classes modulo 19.

Let y be any cyclic permutation of order 19, and let x be any other element of $\mathcal{A}_{19}$. Then $\langle x, y\rangle = \mathcal{A}_{19}$ whenever $\langle x, y\rangle$ is unsolvable, since $\langle x, y\rangle$ is certainly transitive. But $\langle x, y\rangle$ is solvable only in the very rare circumstance that x lies in the normalizer M of $\langle y\rangle$. It is easy to see that M is of order $9 \cdot 19$; moreover, if $y = (0, 1, \cdots, 18)$, then a Sylow 3-subgroup of M is generated by the element $(1, 4, 4^2, \cdots)(2, 2 \cdot 4, 2 \cdot 4^2, \cdots)$, which transforms y to $y^4$ (everything here is taken mod 19). The crucial feature of the elements of M outside the 19-subgroup is that they all move precisely 18 symbols.

In estimating the spread of $\mathcal{A}_{19}$, we are going to use a 19-cycle as supplementary generator. Then the only troublesome cases are when the original elements lie in 19-normalizers: because if x does not lie in a 19-normalizer and y is a 19-cycle (and x, y are quite arbitrary otherwise), then $\langle x, y\rangle = \mathcal{A}_{19}$ for the reasons given above. In a given 19-normalizer, the nontrivial elements that fix the symbol 0 are eight in number: six of type $9^2 1$, and two of type $3^6 1$. First we discover how these elements are distributed among the 19-normalizers.

In $\mathcal{A}_{19}$, there are $19!/3^6 6!$ elements of type $3^6 1$; $2 \cdot 17!/3^4 6!$ of these fix the symbol 0. Every 19-normalizer contains precisely two of the latter, each being the square of the other. Therefore we can choose $t = 17!/3^4 6!$ elements $z_1, \cdots, z_t$ of type $3^6 1$, that all fix 0, such that every 19-normalizer will contain precisely one of these t elements (so that each $z_i$ lies in $3^4 6!$ different 19-normalizers). Every element of type $9^2 1$ lies in precisely fifty-four 19-normalizers.

We can now prove:

4.01 THEOREM. *Let* t *stand for the integer* $17!/3^4 6!$. *Then* $\mathcal{A}_{19}$ *has spread* $t - 1$, *but does not have spread* $t + 3$.

*Proof.* Let $x_1, \cdots, x_{t-1}$ be any nontrivial elements of $\mathcal{A}_{19}$. By what was said above, we may assume that each $x_i$ has one of the three types 19-cycle, $9^2 1$, $3^6 1$. Each of these lies in at most $3^4 6!$ 19-normalizers—indeed in exactly this number for the type $3^6 1$, in fifty-four for the type $9^2 1$, and one for a 19-cycle. But since $(t - 1) 3^4 6! < 17!$, the $x_i$ must all lie outside the normalizer of at least one cyclic subgroup $\langle y\rangle$ of order 19. Since each $\langle x_i, y\rangle$ is thus unsolvable, it is the whole of $\mathcal{A}_{19}$.

On the other hand, let

$$z_{t+1} = (1\,2)(3\,4), \qquad z_{t+2} = (1\,4)(2\,3), \qquad z_{t+3} = (1\,3)(2\,4).$$

If $\langle y, z_{t+i}\rangle = \mathcal{A}_{19}$ for $i = 1, 2, 3$, then y must be a 19-cycle. Thus the $t + 3$ elements $z_i$ do not have a common mate y.

There probably do exist t elements of $\mathcal{A}_{19}$ not possessing a common mate.

We repeat that $\mathcal{A}_5$ lies in $\Gamma_2$, but not in $\Gamma_3$.

We turn, now, to the group PSL(2, q).

We say that G has *exact spread* t if G has spread t but not t + 1.

4.02 THEOREM. *If* q *is a prime-power and is large enough, then* PSL(2, q) *has exact spread*

$$q - 1 \quad \textit{if } q \equiv 1 \pmod 4,$$

$$q - 4 \quad \textit{if } q \equiv 3 \pmod 4,$$

$$q - 2 \quad \textit{if } q \textit{ is a power of } 2.$$

The argument below works for $q \geq 11$ if q is odd, and for $q \geq 4$ if q is a power of 2. The group PSL(2, 9) is isomorphic to the alternating group $\mathcal{A}_6$. Also, PSL(2, 5) $\simeq$ PSL(2, 4) $\simeq \mathcal{A}_5$. This leaves the exact spread of PSL(2, 7) $\simeq$ PSL(3, 2) undecided; it is at least 3.

*Proof.* Here are details of the case $q \equiv 1 \pmod 4$.

The group PSL(2, q) contains $\frac{1}{2}q(q - 1)$ cyclic subgroups of order $\frac{1}{2}(q + 1)$. If $q \geq 11$ then there is one and only one maximal proper subgroup containing such a cyclic group, namely its normalizer, a dihedral group of order q + 1. (See [7, Chapter 12], [8, page 213].)

Let x be a nontrivial element of PSL(2, q). If the order $|x|$ of x divides $\frac{1}{2}q(q - 1)$, but is not 2, then x does not lie in any of the dihedral subgroups of order q + 1; if $|x|$ divides $\frac{1}{2}(q + 1)$, but is not 2 (automatic in this case, where $q \equiv 1 \pmod 4$), then x lies in exactly one dihedral group of order q + 1; and if $|x| = 2$ then there are precisely $\frac{1}{2}(q - 1)$ dihedral groups of order q + 1 which contain x. Consequently, if $x_1, \cdots, x_t$ are nontrivial elements of PSL(2, q), and if $t < q$, then there is a cyclic subgroup $\langle y \rangle$ of order $\frac{1}{2}(q + 1)$ which is not normalized by any of these elements. Then $\langle x_i, y \rangle$ = PSL(2, q) for all i. Thus PSL(2, q) has spread q - 1.

When $q \equiv 3 \pmod 4$ the calculation is similar, but one finds that each element of order 2 lies in $\frac{1}{2}(q + 3)$ dihedral subgroups of order q + 1; while if q is even, that is, if q is a power of 2, then the relevant dihedral groups have order 2(q + 1) and each element of order 2 lies in $\frac{1}{2}q$ of them.

To see that the spread of PSL(2, 7) (of order 168) is 3, we represent it as a permutation group of degree 8, and examine the Sylow subgroups and the transitive subgroups. Details are omitted.

## 5. THE GROUPS PSL(2, q) (CONTINUED)

In this section it turns out to be more advantageous to use the matrix definition of SL(2, q), rather than the permutational representation of PSL(2, q).

We begin with two simple lemmas. In what follows, the matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ will be written in the compact form (a, b; c, d).

5.01 LEMMA. *Let* q *be a prime power greater than* 2. *Then the* q - 1 *matrices* (1, 0; t, 1), (1, t; 0, 1), *with* t *running over the set of all nonzero squares* (*or of nonsquares*) *in* GF(q), *generate* SL(2, q).

*Proof.* Firstly, the set of matrices (1, 0; t, 1), (1, t; 0, 1), without restriction on t, forms a generating set. Thus, since every square is a sum of nonsquares, and every nonsquare is a sum of squares, the result follows from the simple equation

$$(1, 0; s, 1)(1, 0; t, 1) = (1, 0; s+t, 1).$$

5.02 LEMMA. *Let* $\alpha$ *be any nonzero element of* GF(q) *such that* $\alpha \neq \alpha^{-1}$, *and for each positive integer* u *let* $f(u) = (\alpha^u - \alpha^{-u})/(\alpha - \alpha^{-1})$. *Set*

$$A = (\alpha, \alpha^{-1}t; 0, \alpha^{-1}) \quad \textit{and} \quad B = (\alpha, 0; \alpha t, \alpha^{-1}).$$

*Then*

$$A^u = (\alpha, \alpha^{-1}tf(u); 0, \alpha^{-u}) \quad \textit{and} \quad B^u = (\alpha^u, 0; \alpha t f(u), \alpha^{-u}).$$

The proof is routine, and we omit it. Most of the groups PSL(2, q) are dealt with by the following theorem.

5.03 THEOREM. *Let* q *be a prime power greater than* 23, *and* M *any noncentral matrix in* SL(2, q). *Then there is a matrix* N *such that* $\langle M, N \rangle = SL(2, q)$ *and one of* M, N *has order* 4. *Consequently,* PSL(2, q) *is in* $\Gamma_1^{(2)}$ *for* $q > 23$.

*Proof.* Obviously, M has a conjugate $M_1$ of the form (0, 1; -1, t). We may assume that $t \neq 0$, the case $t = 0$ being clear. Suppose that $\alpha$ is a generator for GF(q), and write $N_1 = (0, -\alpha^{-1}; \alpha, 0)$; it will be enough to show that $\langle M_1, N_1 \rangle = SL(2, q)$, since $N_1$ is clearly of order 4. Straightforward calculation shows that $M_1^{-1}N_1^{-1} = A$, $M_1 N_1 = B$, where A, B are the matrices appearing in Lemma 5.2. For any integers s, u we can generate the matrix

$$A^s B^u N_1 = (\alpha^{-u}tf(s), -\alpha^{s+u-1} - \alpha^{-1}t^2 f(s)f(u); \alpha^{-s-u+1}, -\alpha^{-s}tf(u));$$

denote it by C. Lemma 7.4 is needed at this point: it promises that, for $q > 23$, we can find integers s, u so that the (1, 2)-element of C is zero, while C is not a power of B. With these values of s, u, it is easy to see that the commutator $F = CBC^{-1}B^{-1}$ has the form (1, 0; r, 1) with $r \neq 0$. The transforms of F and of $N_1 F N_1$ by powers of B fill out one of the generating sets of Lemma 5.1, and the theorem is thereby established.

What of PSL(2, q) with $q \leq 23$? If q is prime, the case is an easy one:

5.04 THEOREM (See Sunday [14].) *Let* p *be an odd prime, and let* X *be a noncentral element of* SL(2, p). *Then there is an element* Y *such that* $\langle X, Y \rangle = SL(2, p)$ *and one of* X, Y *has order* 4. *Consequently* PSL(2, p) *is in* $\Gamma_1^{(2)}$.

*Proof.* As in the preceding theorem, there is no loss in generality if we set X = (0, 1; -1, t). If $t \neq 0$, put Y = (0, 1; -1, 0), so that XY = (-1, 0; -t, -1) and $X^{-1}Y = (1, t; 0, 1)$. If t = 0 take Y = (0, 1; -1, 1); in both cases, Lemma 5.01 applies.

There remain the cases q = 4, 8, 9, 16. In fact, PSL(2, 9) is isomorphic with $\mathcal{A}_6$ and thus fails to be in $\Gamma_1^{(2)}$; there is no mate of order 2 for the permutation (1 2 3). *Ad hoc* arguments show that the groups PSL(2, q) are in $\Gamma_1^{(2)}$ when q = 4, 8, or 16; we do not go into details here.

## 6. GENERATING SETS IN PSL(n, q), $n > 2$

Let $\mathscr{F}_q^n$ be projective (n - 1)-space over the Galois field $\mathscr{F}_q$ of q elements. We recall that a subspace of $\mathscr{F}_q^n$ has *codimension* d if its dimension is n - 1 - d. We use the natural action of PSL(n, q) on $\mathscr{F}_q^n$.

6.01 LEMMA. *Let* M *be an element of* PSL(n, q) *that fixes pointwise a subspace of* $\mathscr{F}_q^n$ *that has codimension* d. *Let* N *be an element of* PSL(n, q) *such that* $N^k = 1$. *If* $kd < n$, *then* $\langle M, N \rangle$ *is a proper subgroup of* PSL(n, q).

Before proceeding to the proof, we point out that the hypothesis on M means, in matrix terms, that M is similar to a matrix that has at least n - d Jordan boxes, all of which have the same proper value.

*Proof.* Let $W = \bigcap_{i=1}^{k} SN^i$. Then certainly W is N-invariant and, as it is a subspace of S, it is also M-invariant. Furthermore,

$$\operatorname{codim}(W) \leq \sum_{i=0}^{k-1} \operatorname{codim}(SN^i) = kd < n,$$

so that W is nonempty. Either $W = \mathscr{F}_q^n$ or $W \neq \mathscr{F}_q^n$. If (first) $W = \mathscr{F}_q^n$, then M = 1; and as $n > 1$, the lemma is true. If $W \neq \mathscr{F}_q^n$, W is a nonempty proper subspace and W is $\langle M, N \rangle$-invariant; thus $\langle M, N \rangle$ is a proper subgroup of PSL(n, q), as the lemma claims. ‖

6.02 COROLLARY. *If* n *is large enough, then* $PSL(n, q) \not\subseteq \Gamma_1^{(k)}$.

*Proof.* Choose a natural number d (depending on k but not on q) so that SL(d, q) contains a matrix K whose order does not divide k. If M is represented by the matrix $K \oplus I_{n-d}$, and if $n > kd$, lemma 6.01 shows that no element N of order k can be found such that $PSL(n, q) = \langle M, N \rangle$.

6.03 *Remark.* The bound $n > kd$ is independent of q; but for certain values of q—including those coprime with k —it can be improved to $n > k$.

6.04 THEOREM. *If* q *is a prime power, if* n *is a natural number, and if* $n \geq 3$, *then* $PSL(n, q) \not\subseteq \Gamma_1^{(2)}$ *unless* n *is* 3 *and* q *is* 2 *or* 4.

6.05 *Remark.* The group PSL(3, 2) does lie in $\Gamma_1^{(2)}$; we have not been able to decide whether PSL(3, 4) lies in $\Gamma_1^{(2)}$.

*Proof of* 6.04. If $n > 4$ then, whatever q may be, we take M to be represented by $(0, 1; -1, -1) \oplus I_{n-2}$. This is an element in PSL(n, q) whose order exceeds 2 and, since there are n - 2 Jordan boxes corresponding to the proper value 1, lemma 6.01 shows that if N has order 2, then $\langle M, N \rangle \neq PSL(n, q)$.

If q is odd and $n > 2$ we take M to be $(1, 1; 0, 1) \oplus I_{n-2}$ and apply the lemma in the same way.

If q - 1 does not divide n ($q - 1 \nmid n$) we take M to be represented by the matrix $\operatorname{diag}[\theta^{1-n}, \theta, \theta, \cdots, \theta]$, where $\theta$ is a primitive element of $\mathscr{F}_q$. Since $\theta^{1-n} \neq \theta$, this is a nontrivial element of PSL(n, q) and the lemma applies with $\alpha = 1$.

The only possibilities not covered by these three examples are those in which n is 3 or 4, q is even (hence a power of 2), and q - 1 divides n. That is, the only

groups not covered are PSL(4, 2), PSL(3, 2), and PSL(3, 4). Now PSL(4, 2) is isomorphic to $\mathcal{A}_8$ and is not in $\Gamma_1^{(2)}$, since the 3-cycle M = (1 2 3) has no involutary mate N such that $\langle M, N \rangle = \mathcal{A}_8$. An easy calculation shows that PSL(3, 2) does not lie in $\Gamma_1^{(2)}$.

Finally, we feel sure that there is an analogue to Theorems 5.03 and 5.04. Let us state this as a problem:

6.06 PROBLEM. *Is it true that for every nontrivial element* a *of* PSL(3, q) *there is an element* b *such that* $\langle a, b \rangle$ = PSL(3, q) *and the order of at least one of* a, b *divides* 6?

## 7. THE LEMMA FROM NUMBER THEORY

The main argument of this section has been kindly communicated to us by L. Carlitz. Throughout, it is assumed that q is a prime-power greater than 23. Thus, $\phi(q - 1) > 4$; there are at least five primitive elements in GF(q).

Refer to Theorem 5.03. Write $x = \alpha^{-u}$, $y = \alpha^{-s}$, $v = 1 + t^{-2}(\alpha - \alpha^{-1})^2$. The condition that the (1, 2)-element of C be zero is

$$y^{-2} + x^{-2} - 1 = vx^{-2}y^{-2}; \tag{7.1}$$

the condition that C not be a power of B is

$$x^{-2} + y^{-2} \neq 1 + v. \tag{7.2}$$

If $q \equiv 3 \pmod 4$, there is no danger that v be zero. But if $q \equiv 1 \pmod 4$ or if $q = 2^z$, v could well be zero, and (7.1), (7.2) would then be incompatible. For fixed t, this can be avoided by not permitting the primitive element $\alpha$ to assume any one of four forbidden values if $q \equiv 1 \pmod 4$, or either of two forbidden values if $q = 2^z$.

Next, consider the pair (7.1) together with

$$x^{-2} + y^{-2} = 1 + v \tag{7.3}$$

as a simultaneous set. If $v \neq 0$, then (7.3) is certainly not tantamount to (7.1), but (7.3) may be compatible with (7.1). But if (7.3), (7.1) are compatible, and if $v \neq 0$, $xy \neq 0$, then $x^2 = y^{-2}$, so that there are no more than 4 simultaneous solutions (u, s) for each fixed t, $\alpha$.

7.4 LEMMA. *For fixed* t, *and for* $q > 23$, $\alpha$ *can be chosen so that* $v \neq 0, 1$. *For this value of* $\alpha$, (7.1) *and* (7.2) *have a simultaneous solution with* $xy \neq 0$.

*Proof.* The condition $v \neq 1$ is always met. It is a question of showing that (7.1) has at least five solutions with $x, y \neq 0$ for every value of $v \neq 0, 1$. Now (7.1) may be written

$$y^2 = (u - x^2)/(1 - x^2). \tag{7.5}$$

Let $\chi(c)$ denote the quadratic character of c in GF(q), that is,

$$\chi(c) = 1 \quad \text{if c is a square, } c \neq 0,$$
$$\chi(c) = -1 \quad \text{if c is a nonsquare,}$$
$$\chi(0) = 0.$$

The number of solutions of $y^2 = c$ is always $1 + \chi(c)$. Thus, the number of solutions of (7.5), or of (7.1) with $x, y \neq 0$, is

$$(7.6)\qquad \begin{aligned} m &= \sum_{x^2 \neq 1} \left\{ 1 + \chi\left( \frac{u - x^2}{1 - x^2} \right) \right\} = q - 2 + \sum_{x^2 \neq 1} \chi((u - x^2)(1 - x^2)) \\ &= q - 2 + \sum_{x} \chi((u - x^2)(1 - x^2)) . \end{aligned}$$

By a result of Weil, the sum is known to have absolute value less that $3q^{1/2}$. This means that

$$(7.7)\qquad |m - q + 2| < 3q^{1/2},$$

so that $m > 8$ if $q > 23$. But there are at most four solutions with $xy = 0$. The assertion is established.

## REFERENCES


1. A. A. Albert and John Thompson, *Two-element generation of the projective unimodular group*. Illinois J. Math. 3 (1959), 421-439.
2. G. Ja. Binder, *The bases of the symmetric group*. Izv. Vyss. Učebn. Zaved. Matematika 1968, no. 11 (78), 19-25.
3. ———, *The two-element bases of the symmetric group*. Izv. Vyss. Učebn. Zaved. Matematika 1970, no. 1 (92), 9-11.
4. H. R. Brahana, *Pairs of generators of the known simple groups whose orders are less than one million*. Ann. of Math. (2) 31 (1930), 529-549.
5. H. S. M. Coxeter and W. O. J. Moser, *Generators and relations for discrete groups*. Springer-Verlag, Berlin, Göttingen, and Heidelberg, 1957.
6. I. M. S. Dey and James Wiegold, *Generators for alternating and symmetric groups*. J. Austral. Math. Soc. 12 (1971), 63-68.
7. L. E. Dickson, *Linear groups, with an exposition of the Galois field theory*. Teubner, 1901; Dover, 1958.
8. B. Huppert, *Endliche Gruppen. I*. Springer-Verlag, Berlin, Heidelberg, New York, 1967.
9. G. A. Miller, *On the groups generated by two operators*. Bull. Amer. Math. Soc. 7 (1901), 424-426.
10. Peter M. Neumann, *Transitive permutation groups of prime degree*. Proc. 2nd International Conference on the Theory of Groups. Edited by M. F. Newman, Springer Lecture Notes in Mathematics, no. 372 (1974).
11. M. F. Newman, *On a class of metabelian groups*. Proc. London Math. Soc. (3) 10 (1960), 354-364.
12. R. Steinberg, *Generators for simple groups*. Canad. J. Math. 14 (1962), 277-283.
13. J. G. Sunday, *Presentations of the groups* SL(2, m) *and* PSL(2, m). Canad. J. Math. 24 (1972), 1129-1131.
14. A. Williamson, *On primitive permutation groups containing a cycle*. Math. Z. 130 (1973), 159-162.


J. L. Brenner: 10 Phillips Road, Palo Alto, California 94303
James Wiegold: University College, Cardiff, U. K. CF1 1XL