SIMPLE GROUPS*

W. J. Wong
University of Notre Dame
Indiana, USA

If G is a group, not the identity group { 1 } , then G is said to be *simple* if G has no normal subgroups other than G and { 1 } . The significance of simple groups may be seen by considering a group G which is *not* simple. If N is a normal subgroup of G other than G or { 1 } , then G may be thought of as being broken up into two "smaller" groups N and G/N. If either of these groups is not simple, we can repeat this process. Ultimately, if G is finite, or "not too infinite", the process may come to an end with G having been broken up into a number of parts which are simple groups, the composition factors of G. In this way, the simple groups can be considered as the basic objects from which groups in general are built.

The first simple groups which are usually introduced in courses in algebra are the cyclic groups of prime order and the alternating groups. The object of the lecture is to acquaint the audience with some other simple groups, which actually are more typical in many ways. These are obtained from certain groups of matrices.

§1. Take the special linear group SL(n, K) of all n x n matrices of determinant 1 over a field K, where $n \geqslant 2$. This may be considered as a group of linear transformation on the n-dimensional vector space $V = K^n$ identified with the linear transformations $\nu \rightarrow \nu A$. In general the group SL(n, K) is not simple, but a simple group can be obtained from it.

Let S be the set of all 1-dimensional subspaces of V (lines through the origin). Each element A of SL(n, K) induces a permutation $\bar{A}$ of S, and we obtain a permutation group

$$PSL(n, K) = \{ \bar{A} \mid A \in SL(n, K) \},$$

called the *projective special linear group.* The map $A \rightarrow \bar{A}$ is a homomorphism of SL(n, K) onto PSL(n, K), so that

$$PSL(n, K) \cong SL(n, K)/Z,$$

where the kernel Z consists of all the scalar matrices λI, where $\lambda^n = 1$.

THEOREM. PSL(n, K) *is almost always a simple group.*

Since we obtain a group for each choice of the dimension n and each field K, we actually have a *family* of simple groups.

The same procedure can be used for other groups of matrices. If J is a nonsingular n x n matrix with coefficients in a field K, the matrices A over K such that

*Text of a lecture to Honours Year students of the National University of Singapore on 1 August 1983.

$A^T JA = J$ form a group. For different choices of J we obtain the orthogonal and symplectic groups. These then give permutation groups on S, the projective orthogonal and symplectic groups. In this way, further families of simple groups are obtained.

Some of the groups we have mentioned have "twisted" forms, giving additional families of simple groups. All these groups are known generally as *classical groups.*

There are also a few families of simple groups defined by linear transformations over a field K, which occur only in certain dimensions, ranging from 7 to 248. These are called *exceptional groups.*

The classical groups and the exceptional groups together may be called *linear groups,* and are in many ways the most typical of the simple groups.

§2. At this point we have mentioned the following finite simple groups:

Cyclic groups of prime order,

Alternating groups,

Linear groups over finite fields K.

The obvious *question* to ask now is:

Are there any other finite simple groups?

Culminating more than 30 years of research by hundreds of mathematicians, covering thousands of printed pages, the *answer* was announced in 1980:

There are exactly 26 other finite simple groups.

These "sporadic" groups range from a group of order 7,920 contained in the alternating group A_{11}, discovered by Mathieu in 1861, to a group of order

$$2^{46}\, 3^{20}\, 5^9\, 7^6\, 11^2\, 13^3\, 17\cdot 19\cdot 23\cdot 29\cdot 31\cdot 41\cdot 47\cdot 59\cdot 71$$

(approximately 8×10^{53}), discovered by Fischer and Griess, and constructed in 1980 by Griess as a group of $n \times n$ matrices with complex coefficients, where $n = 196, 883$. The latter group is sometimes called the Monster, although Griess prefers to call it the Friendly Giant. It contains 20 of the sporadic groups, called by Griess the Happy Family. Some of the remaining sporadic groups have so far been constructed only with the aid of a computer.

§3. We now give a proof of the theorem stated in §1 (and also explain the words "almost always"), using only elementary group theory and facts that can be verified without difficulty by means of matrix calculations.

Let G = PSL(n, K). We think of the elements of G as matrices of determinant 1 over K, where two matrices which differ by a scalar factor are considered the same. G is a group of permutations of the set S of lines $\langle v \rangle$ spanned by nonzero vectors v of $V = K^n$. We write the standard basis of V as

$$e_1 = (1, 0, 0, \dots, 0),\ e_2 = (0, 1, 0, \dots, 0), \dots .$$

In the proof we use two subgroups of G:

$$B = \left\{ \begin{pmatrix} * & 0 & 0 & \dots & 0 \\ * & * & * & \dots & * \\ * & * & * & \dots & * \\ \vdots & \vdots & \vdots & & \vdots \\ * & * & * & \dots & * \end{pmatrix} \right\}, \quad U = \left\{ \begin{pmatrix} 1 & 0 & 0 & \dots & 0 \\ * & 1 & 0 & \dots & 0 \\ * & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & & \vdots \\ * & 0 & 0 & \dots & 1 \end{pmatrix} \right\}$$

We have the following properties.

(1) B is the subgroup of G fixing $\langle e_1 \rangle$.

(2) $U \lhd B$.

(3) If T is any transvection (i.e. T-I has a single nonzero entry, not on the main diagonal), then T is conjugate in G to an element of U:

$$T \in A^{-1}UA,$$

for some A in G.

(4) U is abelian.

Now suppose $N \lhd G$, $N \neq \{1\}$. We wish to show that N = G.

Let $1 \neq Y \in N$. Then Y moves some element of S, which we may suppose to be $\langle e_1 \rangle$. This means that e_1, $e_1 Y$ are linearly independent, and we may suppose

$$e_1 Y = e_2 .$$

Now suppose $X \in G$, $X \notin B$. By (1), e_1, $e_1 X$ are linearly independent. We can take an element Z of B whose second row is $e_1 X$, so that

$$e_1 YZ = e_2 Z = e_1 X.$$

Now, $XZ^{-1}Y^{-1}$ fixes $\langle e_1 \rangle$, so that $XZ^{-1}Y^{-1} \in B$, by (1). Thus,

$$X \in BYZ = (BZ)(Z^{-1}YZ) \subseteq BN.$$

This proves that

$$G = BN.$$

From (2), we now have

$$UN \lhd BN = G.$$

If T is a transvection, then, by (3), there is an element A of G such that

$$T \in A^{-1}UA \subseteq A^{-1}(UN)A = UN,$$

so that UN contains all transvections. We now use a further property.

(5) G is generated by transvections.

It follows immediately that

$$G = UN.$$

(U is smaller than B so we are getting closer to our goal of proving that G = N.)

One of the basic isomorphism theorems now shows

$$G/N = UN/N \cong U/(U \cap N),$$

an abelian group, by (4). Hence

$$N \lhd G',$$

the commutator subgroup of G. The last fact we use is

(6) G′ = G, except when n = 2 and K has 2 or 3 elements. With these two exceptions, we now see that N = G as we wished to show, and so we have proved the

THEOREM. PSL(n, K) *is a simple group, except when* n = 2 *and* K *has* 2 *or* 3 *elements.*

In the exceptional cases, PSL(n, K) is isomorphic with the symmetric group S_3 and the alternating group A_4, which are not simple.