WHAT IS GROUP THEORY AND WHAT DO GROUP THEORISTS DO?*

Derek J. S. Robinson

First of all I would like to express my pleasure at this opportunity of addressing the Singapore Mathematical Society. It is also very pleasing to see so many promising young mathematicians here today. Clearly I cannot hope in the time available to give you complete answers to the questions posed in the title, but I hope by means of illustration to convey some idea of what group theory is about and what kind of problems group theorists are concerned with.

Most of the audience will, I suppose, know what a group is, but I shall not assume this. Following the principle that a few good examples are worth a thousand definitions, I shall review some familiar sources of groups and postpone the formal definition until later.

(i) Consider a regular tetrahedron T with 4 vertices, 6 edges and 4 faces. There are certain rotations that can be applied to T and which will leave it occupying the same region of space. Such rotations must of course be about an axis of symmetry; the latter are easily found. The possible rotations are about a line joining a vertex to the centroid of the opposite face through angle $2\pi/3$ or $4\pi/3$, and about a line joining the midpoints of opposite edges through angle π. This gives a total of $4 \times 2 + 3 \times 1 = 11$ rotations. To this list must be added the *identity rotation* which leaves every point of T fixed. Thus there are in all 12 possible rotations of T. The set of rotations of T is closed in the sense that if one forms the product of two rotations by performing first one and then the other (in the prescribed order) the result is equivalent to a single rotation of T. In addition each rotation of T has an *inverse rotation;* composition of a rotation with its inverse always produces the identity rotation. The set of 12 rotations of T is a group of order 12.

(ii) As a second example consider the set X_n consisting of the first n positive integers. Let $\alpha : X_n \rightarrow X_n$ be an invertible mapping. Thus α assigns to each i in X_n an integer $\alpha(i)$ in X_n, and $\alpha(1), \alpha(2), \ldots, \alpha(n)$ is just a rearrangement of the natural order $1, 2, \ldots, n$. In other words α is a *permutation* of X_n. The permutation fixing every element of X_n is the identity permutation. Now the product of two permutations is formed by applying them successively. Each permutation has a

*Text of an invited lecture at the prize-giving ceremony for the Interschool Mathematical Competition 1983 on 27 September 1983.

Biographical Note. Professor Derek J. S. Robinson received his degrees from the Universities of Edinburgh and Cambridge. Subsequently he was a Lecturer at the University of London and he is currently Professor of Mathematics at the University of Illinois. Professor Robinson has held visiting positions at several institutions including the Swiss Federal Institute of Technology, Zurich; University of Freiburg, West Germany and the University of Padua, Italy. He visited the National University of Singapore during 1 – 28 September 1983. Professor Robinson is a specialist in the theory of groups and its connections with other branches of algebra. He is the author of two books and numerous research articles. In 1979 he was awarded an Alexander von Humboldt Prize for his work in group theory.

natural inverse. Hence the set of all permutations of X_n is another closed system; this is the well-known *symmetric group* S_n *of degree n.* Its order is $n! = n(n-1)(n-2)\ldots 2.1$.

At this point I should like to draw attention to a connection between examples (i) and (ii) which illustrates two fundamental concepts of group theory, subgroup and isomorphism.

Let the vertices of the regular tetrahedron T be labelled by the integers 1, 2, 3, 4. Then each of the 12 rotations of T may be represented by a permutation of the set $\{1, 2, 3, 4\}$. Now S_4 has $4! = 24$ elements, so not every permutation of the vertices arises from a rotation: some permutations would require a twisting of the figure. A simple check reveals that the permutations that arise from rotations of T are exactly the *even permutations;* i.e. those which involve an even number of inversions of the natural order 1, 2, 3, 4. In general for $n > 1$ the even permutations of X_n form a subset A_n of S_n with $\frac{1}{2}(n!)$ elements; A_n is closed with respect to forming products and inverses of its members and contains the identity. Thus A_n is also a group, the well-known *alternating group of degree n.*

One says that A_n is a *subgroup* of S_n.

The above discussion shows that the rotations of the tetrahedron T are in one-one correspondence with the elements of A_4. Moreover a check reveals that products in the rotation group correspond to products in A_4. From the group theoretical point of view these groups are identical; in technical language they are *isomorphic.*

The two examples of groups already discussed are merely special cases of a general situation.

(iii) Let $\mathcal{S}$ be a "structure" of some kind – here I am being deliberately vague. Let there be associated with $\mathcal{S}$ certain natural invertible mappings $\alpha : \mathcal{S} \rightarrow \mathcal{S}$ including the identity mapping. The set of such mappings is to be closed under composition and inversion. Then the set of all such mappings

$$\mathrm{Gp}\,(\mathcal{S})$$

is a group. Here $\mathcal{S}$ could be a geometrical figure, a physical object like a molecule, a set etc. The idea is that the more "symmetric" $\mathcal{S}$ is, the larger will the group $\mathrm{Gp}(\mathcal{S})$ be.

Thus one arrives at the idea of a group as a measure of the symmetry of a structure. This underlies many of the applications of group theory in mathematics, physics and chemistry.

There is no reason why the group $\mathrm{Gp}\,(\mathcal{S})$ needs to be finite. For example, let be the set of lattice points of the plane i.e. all points with integral coordinates, and let $Gp(\mathcal{S})$ be the set of all rotations, reflections and translations of $\mathcal{S}$; then $Gp(\mathcal{S})$ is clearly an infinite group.

Now I really ought to tell you what a group actually is. It is a non-empty set G with a *law of composition,* so that given $x, y \in G$, there is a unique element $xy \in G$. There is an *identity element* 1_G in G with the property $x1_G = x = 1_G x$ for all x in G. Each x in G has an *inverse* x^{-1} in G, and $xx^{-1} = 1_G = x^{-1}x$. Finally the *associative law* must hold: $(xy)z = x(yz)$.

Let me now say something aoout what group theorists do. Ideally the group theorist would like to classify all groups or possibly all groups with some specific properties. A word about the force of the term "classify". The object is to describe a group by associating with it a set of invariants which determine the group up to isomorphism. These invariants can be objects of any kind but obviously, if the classification is to be useful, they should be simpler objects than the original groups. It should be said that perfect schemes of classification of this type are quite rare in group theory; groups can be just too complicated.

At this point I would like to draw your attention to a fundamental procedure in mathematics. If the objects under study are too complicated to understand, try to break them up into simpler objects and study these. A good illustration of this principle is provided by the reduction of finite groups to finite simple groups.

To understand this it is necessary to recall some definitions. A subgroup H of a group G is said to be *normal* if $g^{-1}hg \in H$ whenever $g \in G$ and $h \in H$; for brevity one writes $H \lhd G$ to denote the fact that H is a normal subgroup of G. If $H \lhd G$, it is possible to construct a new group, the *quotient group* G/H; its elements are the *cosets* $xH = \{ xh \mid h \in H \}$ and its law of composition is the natural one $(xH)(yH) = (xy)H$. A group G is *simple* if $1_G = (\{1_G\})$ and G are the only normal subgroups of G and if $|G| > 1$.

For a *finite* group G considerations of order reveal the existence of a series of subgroups $1_G = G_0 \lhd G_1 \lhd \ldots \lhd G_n = G$ for which every factor G_{i+1}/G_i is simple; this is called a *composition series* of G. Thus a finite group is built up from finite simple groups by means of a composition series. To construct all finite groups it suffices to (i) classify all finite simple groups, and (ii) solve the *extension problem,* i.e. construct all groups G with prescribed normal subgroup N and quotient group $Q = G/N$. However this program is not easy to carry out. The classification of finite simple groups is an extremely hard problem; also, although in a formal sense the extension problem can be solved, the form of the solution tells one little about the structure of the constructed groups. In particular it is not easy to decide whether two of them are isomorphic.

I should like to make some comments about the classification of finite simple groups; this has been the most famous or even notorious problem in group theory in the last few years. The known finite simple groups fall into four classes:

(a) the groups of prime order,

(b) the alternating groups A_n, $n \geqslant 5$,

(c) the groups of Lie type,

(d) the 26 "sporadic" groups.

There is little mystery about (a) since the groups of prime order are exactly the groups G with only two subgroups 1_G and G; such groups are cyclic. The simplicity of A_n, $n \geqslant 5$, was known to Galois and underlies the impossibility of solving the general equation of degree n by radicals if $n \geqslant 5$. The groups of Lie type arise as groups of automorphisms of simple Lie algebras; they fall into several infinite families, the best known being the projective special linear groups PSL(n, p). The sporadic groups are still a mystery and are apparently the result of number theoretic accidents; the smallest one has order 7,920 and was discovered by Mathieu over a century ago, while the existence of the largest (of order roughly 8×10^{53}) was only established within the last few years by R. L. Griess.

It is now generally believed that the above is a complete list of the finite simple groups. However no complete proof of this has yet been published and it is estimated that if a proof were written down, it would occupy at least 5000 pages! This will give you some idea of the difficulty of the classification problem; without doubt its solution constitutes one of the major mathematical achievements of this century.

Finally I would like to discuss another classification problem, one that has occupied my attention for several years. This is concerned with automorphism groups. If G is a group, recall that an *automorphism* of G is an invertible mapping $\alpha : G \rightarrow G$ such that $\alpha(xy) = \alpha(x)\alpha(y)$. The set of all automorphisms of G is a group, the *automorphism group* AutG, of G. (This can be thought of in the spirit of the example (iii), as the group Gp(G) of mappings of the "structure" G.)

The question is, given a group G, does there exist a group X such that AutX is isomorphic with G, and if so, can one find all such X? If at least one X exists, the group G is said *to be an automorphism group.* The problem is: which groups are automorphism groups?

In full generality this problem is too hard to handle. There are just too many examples of automorphism groups and it seems to be difficult to recognize them by any internal property. The only general fact known is that given a finite group G there are only finitely many *finite* groups X such that AutX is isomorphic with G (due to V.T. Nagrebeckii).

One natural source of automorphism groups is the class of *complete groups*; here a group G is called complete if every automorphism of G is inner, i.e. induced by conjugation by some element of G, and if the centre of G is 1_G. Since AutG is isomorphic with G if G is complete, all complete groups are automorphism groups. Another fact worth mentioning is the result of J.T. Hallett and K.A. Hirsch that a cyclic group of order n is an automorphism group if and only if $n = \phi(p^m)$ where ϕ is Euler's function and p is an odd prime.

In conclusion I would like to discuss the position of finite simple groups vis-a-vis automorphism groups. Here it has turned out to be possible to give a complete answer using the classification of finite simple groups. The finite simple groups which are automorphism groups are precisely the following:

(a) groups of order 2,

(b) GL(n, 2) where $n > 2$,

(c) the finite simple groups which are complete,

(d) the Suzuki group Sz(8) of order 29,120.

A few comments on this list. There are no surprises in (a), (b), (c); obviously Aut($\mathbb{Z}$) has order 2 and if G is an elementary abelian 2-group of order 2^r, then AutG is well-known to be $GL(n, 2) \equiv PSL(n, 2)$ which is simple if $n > 2$. Also the finite simple groups which are complete are known. However the occurrence of the Suzuki group $S \equiv Sz(8)$ is quite unexpected. One could say that this is the only finite simple group which is an automorphism group in a non-natural way.

For the expert I shall draw attention to the unique features of the group S which lead to its special behaviour. The Schur multiplicator M(S) is a Klein 4-group while the outer automorphism group OutS has order 3 and acts on M(S) by permuting the three elements of order 2. Thus if K is any subgroup of M(S) with order 2, then $N_{\mathrm{OutS}}(K) = 1$; this is the crucial property of S. In fact it turns out that S is the automorphism group of a proper covering group of order 58,240 and of no other group.