Groups

1 Definition

The idea of a group has evolved from a concrete measure of symmetry of a mathematical object to an abstract algebraic structure in its own right. The work of Lagrange, Galois and others on groups was motivated by studying the symmetries of the roots of a polynomial equation.

The symmetry of an object is specified by its structure-preserving mappings and the manner in which they compose with one another. It is this notion of a set with a composition which is the basis of the definition.

A *binary operation* on a set G (typically denoted by a symbol like $\circ$) is a function from $G \times G$ to G. We write the value of the function on the pair $(g,h) \in G \times G$ (the result of 'composing' g and h) as $g \circ h$.

A *group* is a set G with a binary operation $\circ$ satisfying the following conditions:

(G1) For all $g,h,k \in G$, we have $g \circ (h \circ k) = (g \circ h) \circ k$ (the *associative law*).

(G2) There is an element $e \in G$ such that $g \circ e = e \circ g = g$ for all $g \in G$.

(G3) For any $g \in G$, there exists $g' \in G$ such that $g \circ g' = g' \circ g = e$.

If it satisfies the additional condition

(G4) For all $g,h \in G$, we have $g \circ h = h \circ g$ (the *commutative law*),

it is said to be an *Abelian group*.

The set of symmetries of a mathematical object (suitably defined) always has the structure of a group, where the operation is composition. For the composition of two symmetries is a symmetry; the identity map is a symmetry; a symmetry is a one-to-one and onto map, and so has an inverse, which is also a symmetry; and composition of maps is always associative.

Symmetry groups can be generalised as follows. A *permutation group* is a set G of permutations (one-to-one and onto maps) of a set Ω which is closed under composition, contains the identity map, and contains the inverse of each of its elements. (A permutation group is a group: the associative law is again automatic.) Thus, each symmetry group is a permutation group. A lot of work has gone into deciding which permutation groups are symmetry groups of objects

of particular types such as graphs or designs. (Every permutation group is the symmetry group of some suitably constructed object.)

Cayley's Theorem shows that, conversely, every group can be represented as a permutation group. The proof is as follows. (This argument is stated for finite groups but works more generally.) Let $G = \{g_1, g_2, \ldots, g_n\}$ be a group. The *Cayley table* of G is the $n \times n$ matrix with (i, j) entry k if $g_i \circ g_j = g_k$. It follows from the group axioms (G2) and (G3) that the Cayley table is a Latin square. Thus, each row is a permutation of $\{1, \ldots, n\}$. Now it can be checked that, if π_i is the permutation corresponding to the ith row, then $\pi_i \circ \pi_j = \pi_k$ if and only if $g_i \circ g_j = g_k$. (Here the operation on permutations is composition.) Thus the permutations form a group identical to G.

We say that a group G with operation $\circ$ and a group H with operation $*$ are *isomorphic* if there is a one-to-one correspondence from G to H so that, if g_1 corresponds to h_1 and g_2 to h_2, then $g_1 \circ g_2$ corresponds to $h_1 * h_2$. Isomorphic groups are 'the same' from an algebraic point of view, even though their elements may be quite different. Thus, Cayley's Theorem really states:

Theorem 1 *Every group is isomorphic to a permutation group.*

The *order* of a group is the number of elements in the group. It may be finite or infinite, but we will be mainly concerned with finite groups.

Two very different examples of groups, one infinite and abelian, the other finite and (almost always) non-abelian:

- the additive group $\mathbb{Z}$ of integers, with the operation of addition;
- the *symmetric group* S_n of degree n; its elements are all permutations of the set $\{1, \ldots, n\}$, and the operation is composition of permutations.

2 Subgroups: Lagrange and Sylow

From now on we suppress explicit mention of the group operation, and write $g_1 g_2$ instead of $g_1 \circ g_2$. This is especially appropriate when we think of the group operation as 'multiplication'. At the same time, we write the group identity as 1, and the inverse of g as g^{-1}.

[Sometimes instead we think of it as 'addition', and write $g_1 + g_2$. This is especially common when the group is abelian. In this case, we write the identity as 0, and the inverse of g as $-g$.]

Let G be a group. A *subgroup* of G is a non-empty subset which forms a group in its own right, with respect to the operation inherited from G. That is, H must satisfy the conditions

- for all $h_1, h_2 \in H$, we have $h_1 \circ h_2 \in H$ (the *closure law* – if this were not so, we would not have a well-defined operation on H);
- the identity of G is contained in H;
- the inverse of each element of H is in H.

In fact the second condition follows from the others, and all follow from the single condition

- for all $h_1, h_2 \in H$, we have $h_1 \circ h_2^{-1} \in H$.

We write $H \leq G$ to denote that H is a subgroup of G.

Let H be a subgroup of G. The relation $\sim_r$ on G defined by

$$x \sim_r y \quad \text{if and only if} \quad xy^{-1} \in H$$

is an equivalence relation on H. Its equivalence classes are caller *right cosets* of H in G, and are sets of the form

$$Hx = \{hx : h \in H\}.$$

The element x is called a *right coset representative* for the right coset Hx.

Dually, the relation $\sim_l$ given by

$$x \sim_l y \quad \text{if and only if} \quad x^{-1}y \in H$$

is an equivalence relation, whose equivalence classes are called *left cosets* of H in G, and have the form

$$xH = \{xh : h \in H\}.$$

The left and right cosets of a given subgroup may give different partitions of the group. But the number of elements in a coset of either type is equal to the number of elements in the subgroup. (For right cosets, the correspondence $h \leftrightarrow hx$ is a bijection between H and Hx. So the number of cosets of either type (the *index* of H in G) is equal to $|G|/|H|$. We deduce *Lagrange's Theorem*:

Theorem 2 *The order of a subgroup H of a finite group G divides the order of G.*

The converse of Lagrange's Theorem is false; if $|G| = n$ and m divides n, there may be no subgroup of order m in G. One case where such a subgroup exists is given by *Sylow's Theorem*, one of the most important theorems in finite group theory.

Theorem 3 *Let G be a group of order $n = p^a \cdot b$, where p is prime and p does not divide b. Then*

(a) G contains a subgroup of order p^a;

(b) any two such subgroups P, Q are conjugate (that is, there exists $x \in G$ with $x^{-1}Px = Q$ – this implies that P and Q are isomorphic);

(c) the number of subgroups of order p^a is congruent to 1 mod *p and divides b.*

A subgroup whose order is the exact power of the prime p which divides G is called a *Sylow p-subgroup* of G.

3 Normal subgroups and homomorphisms

A subgroup H of G is said to be a *normal subgroup* if its left and right cosets coincide, that is, if $Hx = xH$ for all $x \in G$. This can be expressed in various equivalent ways, for example: H is a normal subgroup if and only if, for all $h \in H$ and $x \in G$, we have $x^{-1}hx \in H$. (The element $x^{-1}hx$ is called a *conjugate* of h.)

If H is a normal subgroup of G, then we can define an operation on the set G/H of (left or right) cosets of H in G by the rule

$$Hx \circ Hy = H(xy).$$

(Of course it is necessary to show that the definition doesn't depend on the choice of coset representatives x and y.) It can be shown that, with this operation, G/H is a group. This group is called the *factor group* or *quotient group* of G by H.

How do normal subgroups arise 'in nature'?

A *homomorphism* from a group G to a group H is a function $\theta : G \to H$ with the property that

$$\theta(g_1 g_2) = \theta(g_1)\theta(g_2)$$

for all $g_1, g_2 \in G$.

Perhaps the most familiar example of a homomorphism is the function from the additive group $\mathbb{Z}$ of integers to the group $\mathbb{Z}/n\mathbb{Z}$ of integers modulo n, for some positive integer n, which maps each integer k to the congruence class k mod n.

Another example is the *sign map* from the symmetric group S_n to the multiplicative group $\{+1,-1\}$, which maps each permutation to its sign. The sign of a permutation $g \in S_n$ is $(-1)^{n-c(g)}$, where $c(g)$ is the number of cycles of g.)

The *kernel* of a homomorphism θ is the set

$$\mathrm{Ker}(\theta) = \{g \in G : \theta(g) = 1_H\}$$

of elements of G mapped to the identity element of H. The *image* is, as usual, the set

$$\mathrm{Im}(\theta) = \{\theta(g) : g \in G\}$$

of elements of H to which some element of G is mapped. These are described by the *Isomorphism Theorem*:

Theorem 4 *Let θ be a homomorphism from G to H. Then*

- $\mathrm{Ker}(\theta)$ *is a normal subgroup of G;*
- $\mathrm{Im}(\theta)$ *is a subgroup of H;*
- *the factor group $G/\mathrm{Ker}(\theta)$ is isomorphic to* $\mathrm{Im}(\theta)$.

Conversely, if H is a normal subgroup of G, then there is a 'canonical' homomorphism having H as its kernel and G/H as its image.

Thus we may say simply 'A normal subgroup is the kernel of a homomorphism.'

4 Simple groups: Jordan–Hölder

A group G always has two trivial normal subgroups, the whole group G and the identity $\{1\}$. It is called *simple* if it has no other normal subgroups, and *composite* otherwise.

An example of a simple group is the *cyclic group* C_p of prime order p, consisting of elements x^i for $i = 0,\ldots,p-1$, with composition $x^i x^j = x^{i+j \bmod p}$. By Lagrange's Theorem, this group has no non-trivial subgroups at all!

If G is composite, with a non-trivial normal subgroup H, then we can often reduce questions about G to questions about the smaller groups H and G/H. If

either of these is composite, we can continue the process. Eventually we reach a series

$$\{1\} = G_0 \leq G_1 \leq \cdots \leq G_r = G$$

which cannot be further refined. Thus, for $i = 1, \ldots, r$, we have that G_{i-1} is a normal subgroup of G_i, and G_i/G_{i-1} is simple. Such a series is called a *composition series* of G, and the simple groups G_i/G_{i-1} are the *composition factors*. We are only interested in the composition factors up to isomorphism; they form a multiset, since a given simple group may be isomorphic to G_i/G_{i-1} for several values of i.

The *Jordan–Hölder Theorem* states:

Theorem 5 *Any two composition series of a finite group G give rise to the same multiset of composition factors.*

In a sense, this reduces the study of finite groups to two parts:

- determine the finite simple groups;
- determine how a given multiset of finite simple groups can be 'glued together' as the composition factors of a finite group.

To indicate just how far we are from a solution of the second problem, here are some computational results obtained recently by Besche, Eick and O'Brien. The number of groups of order 2000 or less is $49,910,529,484$. Of these, more than 99% have order $1024 = 2^{10}$. However, for every group of order 2^{10}, the list of composition factors consists of a single group (the cyclic group of order 2) with multiplicity 10. There is a sense in which the most complicated groups are those of prime-power order; such a group has just one composition factor (cyclic of prime order) with the appropriate multiplicity.

However, the first part of the problem has been solved as a result of a major collaborative effort. We proceed to discuss this.

5 The Classification of Finite Simple Groups

The Classification of Finite Simple Groups, or CFSG for short, is probably the largest collaborative mathematical achievement ever. The first proof, covering an estimated 15000 pages in articles often not directly on CFSG at all, was announced

in 1980. It was subsequently found to contain a major gap. The 'revisionism' programme was then launched to produce a self-contained proof; this was completed in the early 2000s. Work on a 'third-generation' proof is currently underway.

Even the detailed statement of the theorem cannot be given here. Essentially the result is as follows.

Theorem 6 *A finite simple group is of one of the following types:*

(a) a cyclic group of prime order;

(b) an alternating group A_n, for $n \geq 5$;

(c) a simple group of Lie type;

(d) one of 26 *sporadic simple groups.*

We have already seen the cyclic groups of prime order. Here is a brief description of the remaining groups.

The *alternating group* A_n consists of all even permutations of the set $\{1,\ldots,n\}$. We saw earlier that it is the kernel of the sign homomorphism from the symmetric group S_n to C_2, so it is a normal subgroup of S_n. Galois showed that, for $n \geq 5$, the alternating group A_n is simple (so that the composition factors of S_n are A_n and C_2).

Groups of Lie type are harder to describe. They are closely related to certain matrix groups over finite fields. They fall into a number of families,of which the simplest consists of the projective special linear groups $\mathrm{PSL}(n,q) = \mathrm{SL}(n,q)/Z$, where $\mathrm{SL}(n,q)$ consists of all matrices of determinant 1, and Z is the normal subgroup consisting of scalar matrices. Further families correspond to other 'classical' groups (symplectic, orthogonal and unitary) over finite fields, and there are some 'exceptional' families constructed from exceptional Lie algebras or automorphisms of other groups. Carter's book [3] gives details.

The 26 sporadic groups have no uniform definition, but were constructed individually. See the $\mathbb{ATLAS}$ [4] for details.

6 Permutation groups

Another essay in this series describes aspects of permutation groups of relevance to design theory. Here we give some corollaries of CFSG for permutation groups.

First, a brief reminder about terminology. A *permutation group* on the set $\{1,\ldots,n\}$ is a subgroup of the symmetric group S_n (that is, a group whose elements are permutations and whose operation is composition). The number n is its *degree*. A permutation group G is

- *transitive* if, for any two points of $\{1,\ldots,n\}$, there is an element of G which maps the first to the second;
- *primitive* if, for any subset Y of $\{1,\ldots,n\}$ satisfying $1 < |Y| < n$, there is an element $g \in G$ with $Y \neq g(Y)$ and $Y \cap g(Y) \neq \emptyset$;
- *t-transitive* (for $1 \leq t \leq n$) if, given any two t-tuples of distinct points, there is an element of G which maps the first to the second.

Among the consequences of CFSG are the following:

- all finite t-transitive groups, for $t \geq 2$, are known (see the lists in [2]);
- for almost all positive integers n, the only primitive groups of degree n are the symmetric and alternating groups;
- primitive groups have small order (with known exceptions);
- there are only finitely many distance-transitive graphs of given valency (greater than 2).

Further details about many of these results appear in [2].

7 Computation

Most familiar programming languages and systems allow the user to handle integers, real numbers, and strings. Modern systems often extend this to vectors, complex numbers, etc. To deal with groups as easily, there are two systems available: GAP [5] and MAGMA [1].

A permutation group often arises in practice as the automorphism group of some structure (graph, design, etc.) The program of choice for testing isomorphism of graphs and other combinatorial objects, and for calculating their automorphism groups, is `nauty` [6]. The GAPshare package GRAPE includes an interface with `nauty`; the automorphism groups of graphs returned by the latter

can be handled directly in GAP. The forthcoming package DESIGN will extend this functionality to designs.

In the remainder of this essay we sketch briefly how permutation groups are handled in a computer.

A group is usually input to the computer by giving a set of permutations which generate it. Now given a set of generators, the *orbit* of a point x (the set of all images of x under elements of G) can be computed by an algorithm similar to that for finding a connected component of a graph: starting with x, add in any point which is the image of an existing point under a generator until the resulting set is closed under all generators. The procedure implicitly finds coset representatives for the stabiliser of x: such a set consists of one element mapping x to each possible image.

Now *Schreier's Lemma* provides an algorithm which, given generators for a group and coset representatives for a subgroup, finds generators for the subgroup. So we can compute generators for the subgroup G_1 fixing x.

Continuing this process, we find a sequence

$$G = G_0 > G_1 > \cdots > G_d = \{1\}$$

of subgroups of G, where G_i is the stabiliser of points $x_1, \ldots, x_i$, for $1 \leq i \leq d$. At this point we can calculate the order of G and can test any permutation for membership in G. Moreover, an element of G is uniquely determined by the images of $x_1, \ldots, x_d$, so arbitrary elements of G can be represented in more compact form.

Using this representation, the packages enable the user to compute any group-theoretical properties of interest, including (but far from limited to) Sylow subgroups, composition factors, images of homomorphisms, etc.

It should be mentioned that groups can be handled in other ways too. Instead of permutation generators, we may give matrix generators, or abstract generators and defining relations.

References

[1] W. Bosma and J. Cannon, *The MAGMA Handbook*, available from the Computational Algebra Group, University of Sydney, 1999.

[2] P. J. Cameron, *Permutation Groups*, London Math. Soc. Student Textx **45**, Cambridge University Press, Cambridge, 1999.

[3] R. W. Carter, *Simple Groups of Lie Type*, Wiley, New York, 1972.

[4] J. H. Conway, R. T. Curtis, S. P. Norton, R. A, Parker and R. A. Wilson, *An* ATLAS *of Finite Groups*, Oxford University Press, Oxford, 1985.

[5] The GAP Group, GAP — Groups, Algorithms, and Programming, Version 4.3; Aachen, St Andrews, 2002.
(`http://www-gap.dcs.st-and.ac.uk/~gap`)

[6] B. D. McKay, `nauty` user's guide (version 1.5), Technical report TR-CS-90-02, Computer Science Department, Australian National University, 1990.

Peter J. Cameron
May 30, 2003