Symmetry in mathematics and mathematics of symmetry

Peter J. Cameron

Queen Mary
University of London

p.j.cameron@qmul.ac.uk

International Symmetry Conference, EdinburghJanuary 2007

Symmetry in mathematics

> Whatever you have to do with a structure-endowed entity Σ try to determine its group of automorphisms . . . You can expect to gain a deep insight into the constitution of Σ in this way.
>
> Hermann Weyl, *Symmetry*.

I begin with three classical examples, one from geometry, one from model theory, and one from graph theory, to show the contribution of symmetry to mathematics.

Example 1: Projective planes

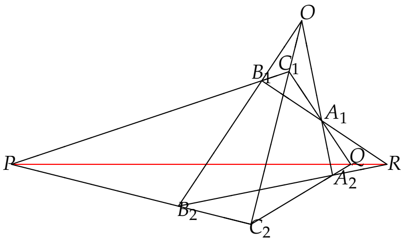
A *projective plane* is a geometry of points and lines in which

- two points lie on a unique line;
- two lines meet in a unique point;
- there exist four points, no three collinear.

Hilbert showed:

Theorem 1. *A projective plane can be coordinatised by a skew field if and only if it satisfies Desargues' Theorem.*

Desargues' Theorem



How not to prove Hilbert's Theorem

Set up coordinates in the projective plane, and define addition and multiplication by geometric constructions.

Then prove that, if Desargues' Theorem is valid, then the coordinatising system satisfies the axioms for a skew field.

This is rather laborious! Even the simplest axioms require multiple applications of Desargues' Theorem.

How to prove Hilbert's Theorem

A *central collineation* of a projective plane is one which fixes every point on a line L (the *axis*) and every line through a point O (the *centre*).

Desargues' Theorem is equivalent to the assertion:

> Let O be a point and L a line of a projective plane. Choose any line $M \neq L$ passing through O. Then the group of central collineations with centre O and axis L acts sharply transitively on $M \setminus \{O, L \cap M\}$.

Now the additive group of the coordinatising skew field is the group of central collineations with centre O and axis L where $O \in L$; the multiplicative group is the group of central collineations where $O \notin L$.

So all we have to do is prove the distributive laws (geometrically) and the commutative law of addition (which follows easily from the other axioms).

Example 2: Categorical structures

A *first-order language* has symbols for variables, constants, relations, functions, connectives and quantifiers. A *structure* M over such a language consists of a set with given constants, relations, and functions interpreting the symbols in the language. It is a *model* for a set Σ of sentences if every sentence in Σ is valid in M.

A set Σ is *categorical* in power α (an infinite cardinal) if any two models of Σ of cardinality α are isomorphic. Morley showed that a set of sentences over a countable language which is categorical in some uncountable power is categorical in all.

So there are only two types of categoricity: countable and uncountable.

Oligomorphic permutation groups

Let G be a permutation group on a set Ω. We say that G is *oligomorphic* if it has only a finite number of orbits on the set Ω^n for all natural numbers n.

Example 2. Let G be the group of order-preserving permutations of the set $\mathbb{Q}$ of rational numbers. Two n-tuples $\overline{a}$ and $\overline{b}$ of rationals lie in the same G-orbit if and only if they satisfy the same equality and order relations, that is,

$$a_i = a_j \Leftrightarrow b_i = b_j, \quad a_i < a_j \Leftrightarrow b_i < b_j.$$

So the number of orbits of G on $\mathbb{Q}^n$ is equal to the number of preorders on an n-set.

The theorem of Engeler, Ryll-Nardzewski and Svenonius

Axiomatisability is equivalent to symmetry!

Theorem 3. *Let M be a countable first-order structure. Then the theory of M is countably categorical if and only if the automorphism group* $\mathrm{Aut}(M)$ *is oligomorphic.*

Example 4. Cantor showed that $\mathbb{Q}$ is the unique countable dense linearly ordered set without endpoints. So $\mathbb{Q}$ (as ordered set) is countably categorical.

We saw that $\mathrm{Aut}(\mathbb{Q})$ is oligomorphic.

Oligomorphic groups and counting

The proof of the E–RN–S theorem shows that the number of orbits of $\mathrm{Aut}(M)$ on M^n is equal to the number of *n-types* in the theory of M.

The counting sequences associated with oligomorphic groups often coincide with important combinatorial sequences.

A number of general properties of such sequences are known. To state the next results, we let G be a permutation group on Ω; let $F_n(G)$ be the number of orbits of G on ordered n-tuples of distinct elements of Ω, and $f_n(G)$ the number of orbits on n-element subsets of Ω.

Typically, $F_n(G)$ counts labelled combinatorial structures and $f_n(G)$ counts unlabelled structures. Both sequences are non-decreasing.

Sequences from oligomorphic groups

Theorem 5. *There exists an absolute constant c such that, if G is an oligomorphic permutation group on Ω which is primitive (i.e. preserves no non-trivial partition of Ω), then either*

- *$f_n(G) = 1$ for all n; or*
- *$f_n(G) \geq c^n/p(n)$ and $F_n(G) \geq n!\,c^n/q(n)$, where p and q are polynomials.*

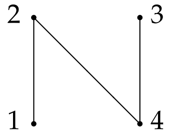
Merola gave $c = 1.324\ldots$. No examples are known with $c < 2$.

Theorem 6. *Let G be a group with $f_n(G) = 1$ for all n (in the above notation). Then either*

- *G preserves or reverses a linear or circular order on Ω; or*
- *$F_n(G) = 1$ for all n. (In this case we say that G is highly transitive on Ω.)*

Example 3: Random graphs

To choose a graph at random, the simplest model is to fix the set of vertices, then for each pair of vertices, toss a fair coin: if it shows heads, join the two vertices by an edge; if tails, do not join.



Finite random graphs

Let X be a random graph with n vertices. Then

- for every n-vertex graph G, the event $X \cong G$ has non-zero probability;
- The probability that $X \cong G$ is inversely proportional to the number of automorphisms of G;
- $\mathbb{P}(X \text{ has non-trivial automorphisms}) \to 0$ as $n \to \infty$ (very rapidly!)

So random finite graphs are almost surely asymmetric.

But . . .

The Erdős–Rényi Theorem

Theorem 7. *There is a countable graph R such that a random countable graph X satisfies*

$$\mathbb{P}(X \cong R) = 1.$$

Moreover, the automorphism group of R is infinite.

We will say more about R and its automorphism group later.

Symmetry and groups

The symmetries of any object form a group.

Is every group the symmetry group of something? This ill-defined question has led to a lot of interesting research. We have to specify

- whether we consider the group as a permutation group (so the action is given) or as an abstract group;
- what kinds of structures we are considering.

As a permutation group

Given a permutation group G on a set Ω, is there a structure M on Ω of some specified type such that $G = \mathrm{Aut}(M)$?

The most interesting case is where M is a relational structure over an arbitrary relational language.

- A permutation group on a finite set is the automorphism group of a relational structure.
- A permutation group on a countable set is the automorphism group of a relational structure if and only if it is closed in the symmetric group (in the topology of pointwise convergence).

Problem 8. *Which permutation groups of countable degree are automorphism groups of relational structures over finite relational languages?*

As an abstract group

Frucht showed that every abstract group is the automorphism group of some (simple undirected) graph. There are many variations on this theme.

Here are a couple of open questions.

- Every group is the collineation group of a projective plane. But is every *finite* group the automorphism group of a *finite* projective plane?
- Is every finite group the *outer automorphism group* (automorphisms modulo inner automorphisms) of some finite group?

Finite permutation groups

The study of finite permutation groups has been revolutionised by *CFSG* (the Classification of Finite Simple Groups):

Theorem 9. *A finite simple group is one of the following:*

- *a cyclic group of prime order;*
- *an alternating group A_n, for $n \geq 5$;*
- *a group of Lie type, roughly speaking a matrix group of specified type over a finite field modulo scalars;*

- *one of the* 26 *sporadic groups, whose orders range from* 7 920 *to* 808 017 424 794 512 875 886 459 904 961 710 757 005 754 368 000 000 000.

To apply this theorem, we need to understand these simple groups well!

Finite permutation groups

The current methodology uses the following reductions:

- Reduce arbitrary permutation groups to transitive ones (fixing no subset of the domain).
- Reduce transitive groups to primitive ones (fixing no partition of the domain).
- Reduce primitive groups to basic ones (preserving no product structure on the domain).
- Reduce basic groups to almost simple groups (the *O'Nan–Scott Theorem*).
- Apply CFSG.

Examples

Using all or part of the preceding methodology, many problems previously completely out of reach have been solved.

For example:

- All finite 2-transitive groups have been determined. In particular, there are no finite 6-transitive groups except the symmetric and alternating groups.
- More generally, the permutation groups having a bounded number of orbits on 5-tuples fall into well-understood infinite families together with some "small" exceptions.

Much is known about primitive groups. For example,

- They are rare: for almost all n, the only primitive groups of degree n are symmetric and alternating groups.
- They are small: order at most $n^{c \log\log n}$ with "known" exceptions.
- They have small base size: almost simple primitive groups have base size bounded by an absolute constant with known exceptions.

A test question

Sometimes there are problems ...

- A finite transitive permutation group of degree $n > 1$ contains a fixed-point-free element. (Jordan 1871)
- A finite transitive permutation group of degree $n > 1$ contains a fixed-point-free element *of prime-power order* (Fein–Kantor–Schacher 1982; uses CFSG)

The remarkable thing about the second result, apart from requiring CFSG, is that it is equivalent to a result in number theory (concerning the infiniteness of relative Brauer groups of finite extensions of global fields).

Problem 10. *Find an "elementary" proof!*

Related questions

- The FKS theorem doesn't tell us which prime! Does there exist a function $f(p,b)$ such that, if $n = p^a \cdot b$ with $a \geq f(p,b)$, then a transitive permutation group of degree n contains a fixed-point-free element of p-power order?
- More generally, is there a function $g(p,b)$ such that, if a p-group acts with b orbits, each of size at least $p^{g(p,b)}$, then it contains a fixed-point-free element?
- There do exist transitive groups containing no fixed-point-free elements of prime order. (Such groups are called *elusive*.) Can they be classified?

The problem in these cases is that there is no simple reduction to primitive groups.

Local or global?

Among other (mostly more vague) definitions of symmetry, the dictionary will typically list two something like this:

- exact correspondence of parts;
- remaining unchanged by transformation.

Photo ©Lucy Pringle

Local or global?

Mathematicians typically consider the second, global, notion, but what about the first, local, notion, and what is the relationship between them?

A structure M is *homogeneous* if every isomorphism between finite substructures of M can be extended to an automorphism of M; in other words, "any local symmetry is global".

Example 11. The pentagon is homogeneous.

Homogeneous structures

In a remarkable paper published posthumously in 1927, the Russian mathematician P. S. Urysohn constructed, and proved unique, a *Polish space* (a complete separable metric space) U with the properties:

- U is universal (every Polish space has an isometric embedding into U);
- U is homogeneous (every isometry between finite subsets extends to an isometry of U).

This paper was ignored for a time, and universal homogeneous relational structures were considered in about 1950 by R. Fraïssé.

This is now a very active field bordering logic, group theory, combinatorics, dynamics, etc.

The countable random graph revisited

Let R be the (unique!) countable random graph, and G its automorphism group.

- R is homogeneous.
- G is oligomorphic; indeed, the numbers $F_n(G)$, resp. $f_n(G)$, of orbits of G on n-tuples of distinct elements, resp. n-subsets, is equal to the number of labelled, resp. unlabelled, graphs on n vertices.
- G is a simple group of cardinality $2^{\aleph_0}$.

The group G has many other striking properties:

- The *small index property* (every subgroup of index less than $2^{\aleph}_0$ contains the stabiliser of a finite tuple).
- If $g, h \in G$ with $g \neq 1$ then h is the product of three conjugates of g.
- Every countable group is embeddable as a semiregular subgroup of G.

Other applications of Fraïssé's method

The amalgamation method can be used to produce various interesting permutation groups. A couple of simple examples:

- A permutation group which is k-transitive and the stabiliser of any $k+1$ points is the identity, for any $k \geq 1$.
- A permutation group which has any given degree of transitivity, where any element fixes finitely many points but the fixed point numbers are unbounded.

By contrast, Jacques Tits and Marshall Hall showed that a 4-transitive group in which the stabiliser of any 4 points is the identity must be one of four finite groups: S_4, S_5, A_6 or M_{11}. (Finiteness is not assumed!)

Using a variant of Fraïssé's method, Hrushovski and others have constructed various generalised polygons, distance-transitive graphs, etc., with lots of symmetry.

More generally ...

The condition of homogeneity can be weakened in various ways, using the notion of *homomorphism* or *monomorphism* in place of *isomorphism*. Investigation of these ideas is quite recent. If H='homo', M='mono', and I='iso', we can say that a structure X has the *IH-property* if any isomorphism between finite substructures of X extends to a homomorphism of X, with similar definitions for MH, HH, IM, and MM (and, indeed, II, which is "classical" homogeneity).

Here is a sample result due to Debbie Lockett.

Theorem 12. *For countable partially ordered sets with strict order, the classes IH, MH, HH, IM, and MM all coincide, and are strictly weaker than II.*