# A Monstrous Piece of Research

Discovery of the 'monster group' helps complete mathematicians' program to classify the simple groups

BY LYNN ARTHUR STEEN

Mathematics is not an empirical science, but it shares with science one of the most powerful paradigms by which we come to understand the structure of things: identification of fundamental building blocks from which all objects of a certain type can be constructed. The premier example, of course, is the periodic table of elements, a classification of primitive components out of which all substances can be formed. The physicists' search for elementary particles is another example, as is the mathematicians' identification of prime numbers as the basic factors of all whole numbers.

Another lesser-known example has preoccupied mathematicians throughout the twentieth century — the classification of finite simple groups. Since groups are of profound importance in both mathematics and science, enormous effort has been devoted to completing this complex structural puzzle. In recent months the final pieces of the puzzle have been identified and put in their proper places. The classification program is now complete, except for final written reports on the recent work. When all details are down on paper, it will represent one of this century's major mathematical achievements — more than 5,000 journal pages of detailed proofs and classification arguments.

Groups are abstract representations of symmetry. They were introduced in the early nineteenth century by the radical young French mathematics student Evariste Galois as a device to solve one of the most vexing mathematics problems of his age: to discover a formula for solving polynomial equations of degree greater than four. The quadratic formula (now taught in high school algebra) solves equations of degree two, and similar but more complex formulas were developed in the late Renaissance to solve equations of degrees three and four. But by 1800, three centuries after these formulas had been discovered, no one had been able to find a formula for polynomial equations of degree five or greater.

Galois showed — in notes scribbled down the night before he died in a duel at the age of 20—that no such formula could exist: The possible symmetries (or permutations) of the roots of fifth degree polynomial equations exceed in complexity the symmetries that can be repre-

sented by algebraic formulas based on the four arithmetic operations and extraction of roots. The structure of these permutations forms what is called a permutation group. Since the two, three or four roots of polynomial equations of degree less than five can be permuted only in a small number of ways, the permutation groups of

these equations are rather simple and can be adequately represented by arithmetical formulas. But the number of permutations of the five roots of a fifth degree equation is 120. The complexities within such a large symmetry group are, as Galois showed, far beyond the expressive capacity of arithmetical formulas. Amazingly,

---

## The Cyclic Group of Order 5

Let five objects be represented by the numbers 1, 2, 3, 4, 5, in order. A cyclic permutation of these objects, denoted by p, yields the order 2, 3, 4, 5, 1. Repeating this yields 3, 4, 5, 1, 2. Since this permutation can be achieved by applying the cyclic permutation p *twice* to the original set, we call it by the name $p^2$.

Continuing in this manner yields p, $p^2$, $p^3$, $p^4$, and finally $p^5$, which is the identity permutation —since after five successive cyclic permutations the original order of the numbers 1, 2, 3, 4, 5 will be restored. Hence $p^5$ is denoted simply by 1, representing the identity.

These permutations form the cyclic group of order 5—one of the simple groups that are to finite groups what atoms are to molecules. The operation table of this group resembles a small multiplication table — which, in a way, is exactly what it is:

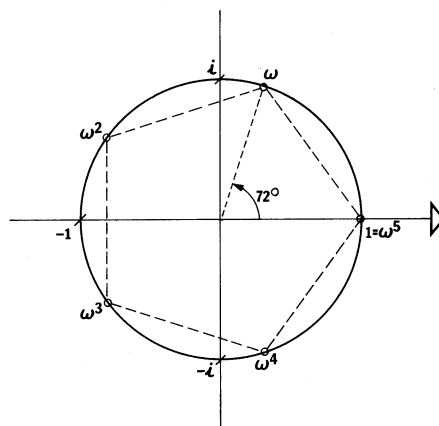|       | 1     | p     | $p^2$ | $p^3$ | $p^4$ |
|-------|-------|-------|-------|-------|-------|
| 1     | 1     | p     | $p^2$ | $p^3$ | $p^4$ |
| p     | p     | $p^2$ | $p^3$ | $p^4$ | 1     |
| $p^2$ | $p^2$ | $p^3$ | $p^4$ | 1     | p     |
| $p^3$ | $p^3$ | $p^4$ | 1     | p     | $p^2$ |
| $p^4$ | $p^4$ | 1     | p     | $p^2$ | $p^3$ |

This group also represents the rotational symmetries of a regular pentagon: let p signify rotation by 72°, which will cause the vertices of the pentagon to shift one step counterclockwise. Five successive rotations, yields 360° or $p^5$, the identity: all vertices are back where they started from. "Symmetry" here denotes that the pentagon did not change its shape under these rotations although the vertices changed position. Other kinds of "symmetric transformation" are possible, and they can operate on far more complicated figures than this.
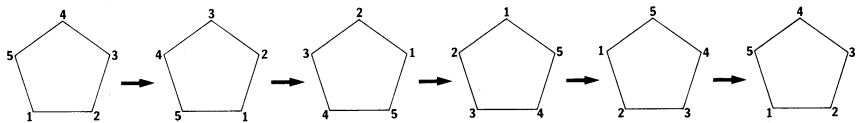


The cyclic group of order 5 also represents the symmetries of the solutions of the fifth degree equation $x^5 = 1$, since the five fifth-roots of 1 are complex numbers located at the corner of a regular pentagon centered at the origin of the complex plane. The first of these roots, traditionally called $\omega$, can be expressed as a complex number in the form

$\omega = \cos\left(\frac{2\pi}{5}\right) + i \sin\left(\frac{2\pi}{5}\right) = \cos 72° + i \sin 72°.$

The other four roots are just multiples of $\omega$: $\omega^2$, $\omega^3$, $\omega^4$ and $\omega^5$, which is, naturally, 1.
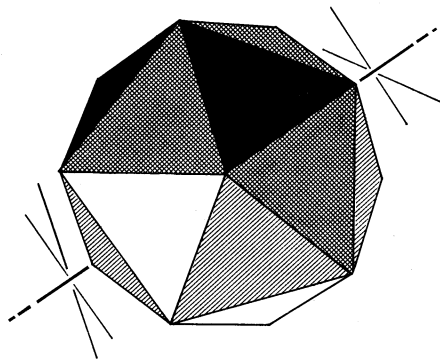
Illus.: John Ellis

Groups come in two types — finite and infinite. The symmetry group of the roots of a polynomial equation is a finite group, because there are only a finite number of permutations possible among the roots of a specific polynomial. In contrast, the Lie groups that represent symmetries of solutions of differential equations are infinite because they involve continuous transformations, and continuity carries the potential of an infinite number of changes. The classification of the infinite Lie groups was completed early in this century, but the full details of the classification of finite groups are still unfolding.

Finite groups can be built up from combinations of smaller groups by a process analogous to multiplication: As each whole number can be expressed as a product of prime numbers, so each finite group can be expressed as a combination of certain factors known as *simple* groups. Simple groups are the ones that cannot be factored; they are the irreducible constituents of all finite groups. The classification problem for finite group theory is this: find all finite simple groups.
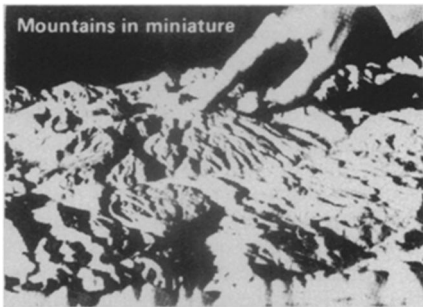
At the turn of the century the finite simple groups of order (or size) less than 2,000 were all known; by 1963 the classification had been completed up to order 20,000; by 1975 it had been completed through order 1,000,000. The results of this effort produced a tentative picture of simple groups, which has been confirmed by all subsequent research.

Most simple groups belong to one of three major families: the cyclic groups, the alternating groups or groups of Lie type. Cyclic groups consist of cyclic permutations of a prime number of objects. Alternating groups consist of even permutations — those permutations that are formed by interchanging the positions of two objects an even number of times. (The collection of all permutations also forms a group, but it is not a simple group since it contains the alternating group as a factor.) Sixteen subfamilies comprise the simple groups of Lie type, each associated with a family of infinite Lie groups. (The terminology gets rather confusing: A Lie group is not a group of Lie type, since the former is infinite and the latter is finite.) Altogether there are 18 specific families of finite simple groups.

Unfortunately some simple groups, 26 to be exact, do not belong to these families. The first five of these so-called *sporadic* groups were discovered in the last century by Emile Mathieu. Remarkably, from 1900, when the fifth Mathieu group was shown to be simple, until 1966 every other simple group that was discovered belonged to one of the three major families — cyclic, alternating or Lie type.

More than fifty years ago the British mathematician William Burnside conjectured that, apart from the cyclic groups, all finite simple groups have an even number of elements. This fundamental insight, so important for the general classification

the young Norwegian mathematician Niels Henrik Abel developed concurrently yet independently a similar solution to the problems of polynomial equations.

Galois and Abel's idea of a permutation group lay fallow for nearly half a century, until the Norwegian mathematician Sophus Lie used the same strategy to explain why certain elementary differential equations could be solved, whereas others could not be. These efforts led to a productive theory of what are now called Lie groups, which link the discrete structure of permutations with the continuous variation of differential equations.

The definition of a group incorporates the most basic behavioral features of mathematical functions and operations, so in some sense it is the most fundamental structure in algebra. It also provides an apt idiom for expressing geometric features such as rotation, reflection and symmetry. Since groups represent a confluence of fundamental patterns from

major branches of mathematics, it is not surprising that their structure contains the key to many diverse phenomena.

In this century the role of group theory in both pure and applied mathematics has grown enormously. A major family known as the linear groups, introduced at the turn of the century by the U.S. mathematician Leonard Dickson, has turned out to be of crucial importance in the classification of elementary particles; indeed, these groups provided much of the theoretical basis for the work that led to the 1979 Nobel Prize in Physics. The ability of groups to capture the subtle essence of symmetry has made them no less useful to chemists working in crystallography and spectroscopy: Results from group theory, for example, enabled Rosalind Franklin, James Watson and Francis Crick to reduce from the infinite to the manageable the number of possible arrangements of molecules in their search for the structure of DNA.

program, remained unverified until 1963, when Walter Feit of Yale University and John G. Thompson of Cambridge University proved it in a massive, virtuoso display of group-theoretic technique. Their proof, more than 250 pages long, was full of new methods and tools; it launched an intensive effort to complete the classification program.

Thompson led the assault with a 400-page analysis — published over a seven-year period from 1968 to 1975 — showing how the structure of a major class of groups (called *solvable* groups, a term going back to Galois's use of groups to investigate solutions of polynomial equations) could be used to infer the structure of the finite simple groups. But during the same period various investigators discovered more sporadic groups, one after the other, in a rush that seemed destined to undermine the entire enterprise with more exceptions than rules.

Some of the most interesting of these new groups were discovered by John Horton Conway of Cambridge University using techniques based on geometric considerations dealing with efficient packing of objects (spheres) into boxes in 24-dimensional space. Inexplicably, Conway's largest group contains many of the other sporadic groups as subgroups, suggesting a family structure for sporadic groups that has not yet been discovered.

The symmetries reflected in the sporadic groups have found important application in the design of error-correcting codes. Special patterns in codes allow data obscured by noise to be reconstructed, so these "error-correcting" codes have been widely used in crucial military and space applications. Selecting a good code turns out to be equivalent to picking a collection of spheres that touch a given one but which are as widely spaced as possible. The symmetries of these patterns in 24-dimensional space yield one of Conway's sporadic groups, and also give a particularly efficient error-correcting code.

The most exotic of these new sporadic groups was one introduced by Bernd Fischer and Thompson in 1974, and was nicknamed the "monster." Fischer and Thompson did not actually discover the group; they merely found evidence suggesting that such a group might exist. Like cosmologists investigating black holes, Fischer and Thompson used properties of the known simple groups, together with the massive body of theory that had emerged in the classification effort, to identify a possible new sporadic group of enormous size. Its existence was consistent with all known information. Thus was launched the great "monster" search — to find the missing sporadic group.

The difficulty with this search was that the "monster" is unimaginably big. According to Fischer and Thompson's calculations, it should contain 808,017,424,794,- 512,875,886,459,904,961,710,757,005,754,-

368,000,000,000 elements! If they were right, if this group really did exist, then there would be good reason to believe that the theory leading to the prediction of this group is also right. And that theory, believed by most mathematicians who have worked on the classification problem, suggests that the "monster" is the last of the finite simple groups.

In mid-January of this year Robert Griess, of the University of Michigan, while working at the Institute for Advanced Study in Princeton, discovered the "monster," officially known as the sporadic group $F_1$ in honor of Fischer, who predicted it. Despite its size, or, more accurately, because of its size, Griess did not use any computer assistance in working out the proof that $F_1$ exists. It is unlikely that any computer could ever manage the calculations necessary to analyze a group of this size. Griess used existing theory to control carefully the calculations necessary to work out its properties and to confirm that such a group does indeed exist. Armed with knowledge of its properties and confirmation of its existence, he was able to locate it in a certain high dimensional Euclidean space. Specifically, he showed that it is a group of rotations in a space of dimension 196,560.

Griess's discovery of the monster confirmed the directions of current research and provided renewed momentum for the final sprint in this extraordinary endeavor. The final results were obtained this summer in an exchange of correspondence between Michael Aschbacher of the California Institute of Technology in Pasadena, Calif., and Daniel Gorenstein of Rutgers University in New Brunswick, N.J., and discussed avidly by group theorists attending the annual summer meeting of the American Mathematical Society in Ann Arbor, Mich. Although full details of the final steps have not yet been published, those in the inner circle of finite group theory research have checked each other's work and believe that the program is complete.

A single theorem with a proof exceeding 5,000 pages is without precedent in mathematical history. Gorenstein admits that the written proof, when completed, will inevitably contain certain local gaps — mistakes in reasoning, omitted steps — that break the logical chain of proof. But researchers in this field, like those who worked on the four-color problem — another problem with an extraordinarily long proof — know from experience that these short gaps can always be bridged by routine application of known methods. This assurance does not constitute the kind of absolute proof idealized by traditional Euclidean geometry. But it is typical of many parts of contemporary mathematics research — a conviction by a small group of experts, based on extensive experience, that whatever gaps may be discovered can always be closed. Proof, in this case, resides primarily in the mind of the expert.                    □