Sporadic Groups: Exceptions, or Part of a Pattern?

Last month news of the apparent discovery of yet another sporadic group filtered through the mathematical community. If confirmed, this mathematical entity would be one of only 21 known examples of the rare and still poorly understood class of finite groups known as sporadic. The discovery would also be the sixteenth such group found since 1965, reflecting a burst of activity in finite group theory that has turned up new sporadic groups almost every year and has resulted in several other important developments in the past decade. Among the most intriguing of these developments, although its importance is still uncertain, is the demonstration of an intimate connection between some sporadic groups and error-correcting codes of the type used to transmit binary information reliably in distortion-prone environments.

Sporadic groups play something of the role of the joker in finite group theory, which has as a basic goal determination of the structure of all finite groups. In classifying these groups mathematicians employ the concept of a simple group, one which, in some sense, cannot be decomposed into subgroups. Simple groups thus constitute the building blocks out of which all finite groups are constructed. There are two well-known classes of simple groups: alternating groups, consisting of all even permutations of n objects, and groups of the Lie type, which have strong geometrical analogies. Both classes have an infinite number of simple groups (each of which has a finite number of elements), but these groups occur in regular patterns and their properties have been extensively studied. Most simple groups belong to one of these two classes. The major exceptions are the sporadic groups.

Sporadic groups, as their name implies, do not seem to follow any regular pattern. If there should turn out to be an infinite number of such anomalous groups, then hopes of classifying all finite groups would have to be discarded. Hence, there is considerable interest in sporadic groups and in the possibility that they are either limited in number or ordered in some way not yet perceived.

Most of the known sporadic groups were found almost by accident in the course of trying to establish basic theorems about finite groups. Considering the uncertainties still surrounding sporadic groups, some remarkably general theorems have been proved. In 1963, for example, J. Thompson, then at the University of Chicago, and W. Feit of Yale showed that essentially every simple group has an even number of elements. Other investigators, trying to prove similar theorems, have on occasion run into difficulties that, on further examination, turned out to be evidence of a new sporadic group.

The most recently discovered sporadic group was found by M. O'Nan of Rutgers University. He was trying to classify a particular family of permutation groups. In the process, he encountered a configuration that could not be explained in terms of known simple groups or in terms of general theorems. O'Nan worked out the struc-

(Continued on page 148)

Mathematical Groups

One of the simplest and most useful algebraic structures is the group, study of which dates back to 1830. The concept is not only of mathematical interest, but has found application in fields ranging from quantum mechanics to crystallography. Despite their long history and many uses, groups remain a remote concept to many. Since the accompanying two articles concern advances in group theory and its applications, this short summary of the basic axioms and properties of groups is offered as a convenient primer.

A group is a set of elements together with an operation which satisfies the four axioms shown in Table 1. The elements (denoted **a**, **b**, . . .) may be any sort of object or transformation, including numbers, vectors, physical motions, and geometric spaces. The operation (denoted by *) may be algebraic or geometric, including addition, matrix multiplication, and rotation. In some instances what is of interest is a semigroup (a set of elements that obey all but one of the axioms; a semi-group may not have inverse elements, for example.

A familiar example of a group is the set of all integers (. . .−1, 0, 1, 2, . . .) combined with the operation of addition. Zero is the identity element and the inverse for an integer is its negative.

Table 1. Group axioms.

Closure: for any elements **a**,**b** **a*****b** is an element of the group
Associative: $(\mathbf{a}*\mathbf{b})*\mathbf{c} = \mathbf{a}*(\mathbf{b}*\mathbf{c})$
Identity: there is an element **I** such that $\mathbf{I}*\mathbf{a} = \mathbf{a}*\mathbf{I} = \mathbf{a}$
Inverse: for every element **a** there is an element $\mathbf{a}^{-1}$ such that $\mathbf{a}*\mathbf{a}^{-1} = \mathbf{a}^{-1}*\mathbf{a} = \mathbf{I}$

In this case, there is an infinite number of elements in the group.

Another common group is the set of all (nonsingular) n by n matrices with matrix multiplication as the group operation—the group known as the full linear group of dimension n. Not only is there an infinite number of elements in each group, but there are an infinite number of such groups.

An example of a finite group is given in Fig. 1. The elements of the group are the possible ways of rotating a square so as to change the relative orientation of its vertices from one of the eight possible positions to another; these eight motions, including the option of no motion at all (the identity element), comprise the group. Combination of two successive rotations, for example **a** followed by **d**, is the group operation (**a*****d** is equivalent to **g**, another element of the group, as required by the closure axiom). For this paricular group, the operation is not commutative and the order in which it is applied makes a difference ($\mathbf{a}*\mathbf{d} = \mathbf{g} \neq \mathbf{d}*\mathbf{a}$). Inverse elements exist for all members of the group—$\mathbf{d}*\mathbf{d} = \mathbf{I}$, for example.

The operations for a group may be summarized in a group multiplication

Table 1. Known sporadic groups.

Group	Discovered	Number of elements
M_{11}	Mathieu (1860)	7,920
M_{12}	Mathieu (1860)	95,040
M_{22}	Mathieu (1861)	443,520
M_{23}	Mathieu (1861)	10,200,960
M_{24}	Mathieu (1861)	244,823,040
Ja	Janko (1965)	175,560
HaJ	Hall, Janko (1967)	604,800
HJM	Higman, McKay, Janko (1968)	50,232,960
HHM	Held, Higman, McKay (1967)	4,030,387,200
HiS	Higman, Sims (1967)	44,352,000
McL	McLaughlin (1968)	898,128,000
Suz	Suzuki (1967)	448,345,497,600
Co_1	Conway (1968)	4,157,776,806,543,360,000
Co_2	Conway (1968)	42,305,421,312,000
Co_3	Conway (1968)	495,766,656,000
Fi_{22}	Fischer (1969)	64,561,751,654,400
Fi_{23}	Fischer (1969)	4,089,470,473,293,004,800
Fi_{24}	Fischer (1969)	1,252,205,709,190,661,721,292,800
LyS	Lyons, Sims (1971)	51,765,179,004,000,000
R	Rudvalis (1972)	145,926,144,000
O'N(?)	O'Nan (1973)	460,815,505,920

tural properties of what he suspected was an unknown group, and computed that it would have about 460 billion elements. He was then able to construct what is known as a character table—a table of functions associated with the matrix representation of the group. These functions amount to the ultimate arithmetic objects associated with a finite group. In this instance, there turned out to be 30 functions or characters associated with the group.

Although most group theorists accept calculation of a character table as strong evidence that a group really exists, definite proof requires the explicit construction of the group itself—essentially, the construction of a multiplication table for the group (see box). For groups as large as the O'Nan group, doing the job by hand is out of the question. Sophisticated methods of constructing new groups by means of computers have been developed, however, and C. Sims of Rutgers is now working on the new group.

Sporadic groups have some surprising properties. For one thing, many of them are very large (Table 1). The Fischer group F_{24}, for example, has more than 10^{24} elements. According to A. Thaler of the mathematics section of the National Science Foundation, numbers of this magnitude play no significant role in any other part of mathematics.

Even more startling is the connection between sporadic groups and one type of error-correcting code. Because these codes allow data obscured by noise to be reconstructed, they have found practical applications ranging from storage of irreplaceable information on magnetic tape to transmission of data between the Mariner spacecraft and Earth. There are many types of error-correcting codes, of which one example is the Golay code used in certain military applications.

In the (23,12) Golay code, each segment of a coded message consists of 23 binary bits of which 12 contain information to be transmitted and 11 are redundant. Because of the pattern of original and redundant information within the coded message, as many as three separate transmission errors per segment can be detected and corrected during the decoding process. Mathematically, error-correcting codes can be described as a subspace of a vector space—in this instance a 12-dimensional subspace of a 23-dimensional vector space. (A vector space can be thought of as a set of elements that combine in the same manner as ordinary vector addition.) The code subspace has associated with it a finite group, known as the automorphism group, which is composed of all the (nonsingular) linear operations on the vector space which leave the code subspace unchanged. Remarkably, the automorphism group of the (23,12) Golay code is a sporadic group, the fourth Mathieu group M_{23}.

The connection between codes and sporadic groups became even more interesting when John Conway of Cambridge University in England investigated a generalized version of the Golay code in 24 dimensions. He found that the automorphism group of this code contained three new sporadic groups (Co_1, Co_2, and Co_3). Moreover, the first of these groups, Co_1, contained 12 of the 20 known sporadic groups as subgroups. This unexpected development raises the possibility that sporadic groups are not really sporadic, that there is some underlying order—although group theorists are still very uncertain on this point.

Unlike most of the sporadic groups found since 1965, the Conway groups were discovered as the result of research into the properties of error-correcting codes. These codes have strong geometric analogies, for example to the problem of packing unit spheres in n dimensions. In 24 dimensions, it is possible to pack extremely densely, so that in the configuration Conway studied any given sphere touches 196,560 others. Designing a good code (one which can correct as many errors as possible) is equivalent to picking a subset of these spheres in such a way that they are as far apart from each other as possible. The resulting configuration (the geometrical analog of the desired code) turns out to be very symmetrical, and hence to have a large symmetry group. According to this line of reasoning, therefore, a close connection between groups and codes is not too surprising. What is still unexplained, however, is why in a few cases the groups are of the sporadic type.

Mathematicians have long known that there is something special about 24-dimensional phenomena—what one group theorist calls "the miracle that happens in 24 dimensions"—and it may be that this accounts for the existence of the Conway groups and for the appearance of other sporadic groups as subgroups of Co_1. In any case, investigations of error-correcting codes in still higher dimensions (48 and 72) have so far failed to turn up any new sporadic groups or any further evidence of an ordered relationship among these exceptional groups. Nor has an understanding of the connection between codes and groups led to the construction of improved error-correcting codes of any commercial significance. But sporadic groups are closely tied to the central problem in finite group theory, and the issue of whether they are accidents or part of a pattern is likely to be of increasing interest to group theorists as more of these somewhat curious mathematical entities are discovered.—ALLEN L. HAMMOND