19

Group Theory

19.1 The Group Concept

The notion of group is one of the most important unifying ideas in mathematics. It draws together a wide range of mathematical structures for which a notion of combination, or "product," exists. Such products include the ordinary arithmetical product of numbers, but a more typical example is the product, or composition, of functions. If f and g are functions, then gf is the function whose value for argument x is $f(g(x))$. [The reason for writing $f(g(x))$ as gf is that its meaning is "apply g, then f." We have to pay attention to order because in general $gf \neq fg$.]

A group G is defined formally to be a set with an operation, called *product* and denoted by juxtaposition, a specific element called the *identity* and written 1 and, for each $g \in G$, an element called the *inverse* of g and written g^{-1}, with the following properties:

(i) $g_1(g_2g_3) = (g_1g_2)g_3$ for all $g_1, g_2, g_3 \in G$. (associative property)

(ii) $g1 = 1g = g$ for all $g \in G$. (identity property)

(iii) $gg^{-1} = g^{-1}g = 1$ for all $g \in G$. (inverse property)

These axioms evolved over more than a century of work with particular groups, during which their essential features emerged only gradually. We look at some of the groups that played an important role in this process in the other sections of this chapter. In practice, properties (i) and (ii) are usually evident, and it is more important to ensure that the product operation

J. Stillwell, *Mathematics and Its History*

is in fact *defined* for all elements of G. Many mathematical concepts have been created in response to the desire, at first unconscious, for products to exist.

For example, we saw in Section 8.2 that a perspective view of a perspective view is not, in general, a perspective view. Thus if we take the "product" of a perspective transformation g and a perspective transformation f to be the result of performing g then f, then gf does not always belong to the set of perspective transformations. The set of *projective* transformations is the simplest possible extension of the set of perspective transformations to a set on which the product is always defined, namely, the set of finite products of perspective transformations.

In other instances, concepts have arisen from the desire to have inverses. Negative numbers, for example, can be regarded as the result of extending the set $\{0,1,2,3,\ldots\}$ to one in which each element has an inverse under the $+$ operation. Another example is the enlargement of the plane by points at infinity, which ensures that each projective transformation has an inverse, because it enables points that are projected to infinity to be projected back again.

Perhaps the earliest nontrivial use of an inverse occurs with the operation of "multiplication modulo p," which Euler (1758) (and possibly Fermat before him) used to give an essentially group-theoretic proof of Fermat's little theorem. Recall from Section 5.1 that integers m and n are called congruent modulo p if they differ by an integer multiple of p, and from Section 5.2 that b is an *inverse of* a with respect to multiplication mod p if ab is congruent to 1 modulo p, that is, if $ab+kp=1$ for some integer k. If p is prime and a is not a multiple of p, then such a b exists by application of the Euclidean algorithm to the relatively prime numbers a, p (Sections 3.3 and 5.2). Euler did not define a group in his proof, but it is easy for us to do so (and to rephrase his proof accordingly; see exercises). The group elements are the *nonzero residue classes* mod p:

$$\begin{aligned}
1 \bmod p &= \{\ldots,-p+1,1,p+1,2p+1,\ldots\},\\
2 \bmod p &= \{\ldots,-p+2,2,p+2,2p+2,\ldots\},\\
3 \bmod p &= \{\ldots,-p+3,3,p+3,2p+3,\ldots\},\\
&\vdots\\
(p-1) \bmod p &= \{\ldots,-1,p-1,2p-1,3p-1,\ldots\},
\end{aligned}$$

with product defined by

$$(a \bmod p)(b \bmod p) = (a \cdot b) \bmod p,$$

where $a \cdot b$ is the ordinary arithmetic product. Group properties (i) and (ii) follow from ordinary arithmetic; (iii), as we have seen, follows from the Euclidean algorithm.

The preceding examples illustrate the influence of geometry and number theory on the group concept. An even more decisive influence was the theory of equations, which we look at briefly in the next section. A more detailed account of the development of the group concept may be found in Wussing (1984).

EXERCISES

Here is the proof of Fermat's little theorem using inverses mod p. Start with the nonzero residue classes

$$1 \bmod p, \quad 2 \bmod p, \quad \ldots, \quad (p-1) \bmod p$$

and multiply them all by a nonzero class $(a \bmod p)$.

19.1.1 Notice that if we multiply again by the *inverse* of $(a \bmod p)$ we get back the classes

$$1 \bmod p, \quad 2 \bmod p, \quad \ldots, \quad (p-1) \bmod p.$$

Why does this show that the classes

$$(a \bmod p)(1 \bmod p), (a \bmod p)(2 \bmod p), \ldots, (a \bmod p)((p-1) \bmod p)$$

are distinct and nonzero?

19.1.2 Deduce from Exercise 19.1.1 that if $(a \bmod p)$ is a nonzero residue class, then

$$\{(a \bmod p)(1 \bmod p), (a \bmod p)(2 \bmod p), \ldots, (a \bmod p)((p-1) \bmod p)\}$$

is the same set as

$$\{1 \bmod p, 2 \bmod p, \ldots, (p-1) \bmod p\}.$$

19.1.3 Deduce from Exercise 19.1.2 that

$$a^{p-1} \cdot 1 \cdot 2 \cdot \cdots \cdot (p-1) \bmod p = 1 \cdot 2 \cdot \cdots \cdot (p-1) \bmod p.$$

19.1.4 Finally, deduce that

$$a^{p-1} \bmod p = 1 \bmod p,$$

that is,

$$a^{p-1} \equiv 1 \pmod p$$

(Fermat's little theorem).

19.2 Permutations and Theory of Equations

We saw in Section 11.1 that, as early as 1321, Levi ben Gershon found that there are $n!$ permutations of n things. These permutations are invertible functions that form a group S_n under composition, though their behavior under composition was not considered until the eighteenth century. It was when the idea of permutation was applied to the roots of polynomial equations, by Vandermonde (1771) and Lagrange (1771), that the first truly group-theoretic properties of permutations were discovered. At the same time, Vandermonde and Lagrange discovered the key to understanding the solution of equations by radicals.

They began with the observation that if an equation

$$x^n + a_1 x^{n-1} + \cdots + a_{n-1}x + a_n = 0 \tag{1}$$

has roots $x_1, x_2, \ldots, x_n$, then

$$x^n + a_1 x^{n-1} + \cdots + a_{n-1}x + a_n = (x - x_1)(x - x_2)\ldots(x - x_n), \tag{2}$$

and by multiplying out the right-hand side and comparing coefficients one finds that the a_i are certain functions of $x_1, x_2, \ldots, x_n$. For example,

$$a_n = (-1)^n x_1 x_2 \ldots x_n,$$
$$a_1 = -(x_1 + x_2 + \cdots + x_n).$$

These functions are *symmetric*, that is, unaltered by any permutation of $x_1, x_2, \ldots, x_n$, since the right-hand side of (2) is unaltered by such permutations. Consequently, any rational function of $a_1, a_2, \ldots, a_n$ is symmetric as a function of $x_1, x_2, \ldots, x_n$. Now the object of solution by radicals is to apply rational operations *and radicals* to $a_1, a_2, \ldots, a_n$ so as to obtain the roots, that is, the completely *asymmetrical* functions x_i.

Radicals must therefore reduce symmetry in some way, and one can see that they do in the quadratic case. The roots of

$$x^2 + a_1 x + a_2 = (x - x_1)(x - x_2) = 0$$

are

$$x_1, x_2 = \frac{-a_1 \pm \sqrt{a_1^2 - 4a_2}}{2} = \frac{(x_1 + x_2) \pm \sqrt{x_1^2 - 2x_1x_2 + x_2^2}}{2},$$