HISTORICAL NOTE

There are three historical roots of the development of abstract group theory evident in the mathematical literature of the nineteenth century: the theory of algebraic equations, number theory, and geometry. All three of these areas used group-theoretic methods of reasoning, although the methods were considerably more explicit in the first area than in the other two.

One of the central themes of geometry in the nineteenth century was the search for invariants under various types of geometric transformations. Gradually attention became focused on the transformations themselves, which in many cases can be thought of as elements of groups.

In number theory, already in the eighteenth century Leonhard Euler had considered the remainders on division of powers a^n by a fixed prime p. These remainders have "group" properties. Similarly, Carl F. Gauss, in his *Disquisitiones Arithmeticae* (1800), dealt extensively with quadratic forms $ax^2 + 2bxy + cy^2$, and in particular showed that equivalence classes of these forms under composition possessed what amounted to group properties.

Finally, the theory of algebraic equations provided the most explicit prefiguring of the group concept. Joseph-Louis Lagrange (1736–1813) in fact initiated the study of permutations of the roots of an equation as a tool for solving it. These permutations, of course, were ultimately considered as elements of a group.

It was Walther von Dyck (1856–1934) and Heinrich Weber (1842–1913) who in 1882 were able independently to combine the three historical roots and give clear definitions of the notion of an abstract group.

2.6 Example The familiar additive properties of integers and of rational, real, and complex numbers show that $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ under addition are abelian groups. ▲

2.7 Example The set $\mathbb{Z}^+$ under multiplication is *not* a group. There is an identity 1, but no inverse of 3. ▲

HISTORICAL NOTE

Commutative groups are called *abelian* in honor of the Norwegian mathematician Niels Henrik Abel (1802–1829). Abel was interested in the question of solvability of polynomial equations. In a paper written in 1828, he proved that if all the roots of such an equation can be expressed as rational functions $f, g, \ldots, h$ of one of them, say x, and if for any two of these roots, $f(x)$ and $g(x)$, the relation $f(g(x)) = g(f(x))$ always holds, then the equation is solvable by radicals. Abel showed that each of these functions in fact permutes the roots of the equation; hence, these functions are elements of the group of permutations of the roots. It was this property of commutativity in these permutation groups associated with solvable equations that led Camille Jordan in his 1870 treatise on algebra to name such groups *abelian;* the name since then has been applied to commutative groups in general.

Abel was attracted to mathematics as a teenager and soon surpassed all his teachers in Norway. He finally received a government travel grant to study elsewhere in 1825 and proceeded to Berlin, where he befriended August Crelle, the founder of the most influential German mathematical journal. Abel contributed numerous papers to Crelle's *Journal* during the next several years, including many in the field of elliptic functions, whose theory he created virtually single-handedly. Abel returned to Norway in 1827 with no position and an abundance of debts. He nevertheless continued to write brilliant papers, but died of tuberculosis at the age of 26, two days before Crelle succeeded in finding a university position for him in Berlin.

2.8 Example The familiar multiplicative properties of rational, real, and complex numbers show that the sets $\mathbb{Q}^+$ and $\mathbb{R}^+$ of positive numbers and the sets $\mathbb{Q}^*$, $\mathbb{R}^*$, and $\mathbb{C}^*$ of nonzero numbers under multiplication are abelian groups. ▲

2.9 Example The set of all real-valued functions with domain $\mathbb{R}$ under function addition is a group. This group is abelian. ▲

2.10 Example **(Linear Algebra)** Those who have studied vector spaces should note that the axioms for a vector space V pertaining just to vector addition can be summarized by asserting that V under vector addition is an abelian group. ▲

2.11 Example The set $M_{m\times n}(\mathbb{R})$ of all $m \times n$ matrices under matrix addition is a group. The $m \times n$ matrix with all entries 0 is the identity matrix. This group is abelian. ▲

2.12 Example The set $M_n(\mathbb{R})$ of all $n \times n$ matrices under matrix multiplication is *not* a group. The $n \times n$ matrix with all entries 0 has no inverse. ▲

Each of the groups we have seen in the above examples is an abelian group. There are many examples of groups which are not abelian, two of which we now present.

2.13 Example Here we give an example of a group that is not abelian. We let T be the set of all isometries of the plane. An **isometry of the plane** is a function mapping the plane to the plane which preserves distance. So if ϕ is an isometry of the plane and P, Q are points in the plane, then the distance between P and Q is the same as the distance between $\phi(P)$ and $\phi(Q)$. Isometries of the plane map the plane one-to-one and onto itself. Examples of isometries include translations and rotations of the plane. The set T under the operation of composition forms a group. To verify this we first must check that function composition is an operation. Certainly, the composition of two isometries is an isometry since each preserves distance. So function composition gives an operation on T. Theorem 1.13 states that function composition is associative, so $\mathscr{G}_1$ is satisfied. The identity function ι that maps each point P in the plane to itself gives an identity element in T, which means that $\mathscr{G}_2$ is satisfied. Finally, for any isometry ϕ, the inverse function ϕ^{-1} is also an isometry and it serves as an inverse as defined in $\mathscr{G}_3$. Therefore T is a group under function composition.

To show that T is not abelian, we only need to find two isometries ϕ and θ such that $\phi \circ \theta \neq \theta \circ \phi$. The functions $\phi(x, y) = (-x, y)$ (reflection across the y-axis) and $\theta(x, y) = (-y, x)$ (rotation by $\pi/2$ about the origin) foot the bill. Note that $\phi \circ \theta(1, 0) = \phi(\theta(1, 0)) = \phi(0, 1) = (0, 1)$ and $\theta \circ \phi(1, 0) = \theta(\phi(1, 0)) = \theta(-1, 0) = (0, -1)$, which implies that $\phi \circ \theta \neq \theta \circ \phi$ and T is not an abelian group under function composition. ▲

2.14 Example Show that the subset S of $M_n(\mathbb{R})$ consisting of all *invertible* $n \times n$ matrices under matrix multiplication is a group.

Solution We start by showing that S is closed under matrix multiplication. Let A and B be in S, so that both A^{-1} and B^{-1} exist and $AA^{-1} = BB^{-1} = I_n$. Then

$$(AB)(B^{-1}A^{-1}) = A(BB^{-1})A^{-1} = AI_nA^{-1} = I_n,$$

so that AB is invertible and consequently is also in S.

Since matrix multiplication is associative and I_n acts as the identity element, and since each element of S has an inverse by definition of S, we see that S is indeed a group. This group is *not* commutative. ▲

The group of invertible $n \times n$ matrices described in the preceding example is of fundamental importance in linear algebra. It is the **general linear group of degree** n,

and is usually denoted by $GL(n, \mathbb{R})$. Those of you who have studied linear algebra know that a matrix A in $GL(n, \mathbb{R})$ gives rise to an invertible linear transformation $T : \mathbb{R}^n \to \mathbb{R}^n$, defined by $T(\mathbf{x}) = A\mathbf{x}$, and that conversely, every invertible linear transformation of $\mathbb{R}^n$ into itself is defined in this fashion by some matrix in $GL(n, \mathbb{R})$. Also, matrix multiplication corresponds to composition of linear transformations. Thus all invertible linear transformations of $\mathbb{R}^n$ into itself form a group under function composition; this group is usually denoted by $GL(\mathbb{R}^n)$. Since the sets $\mathrm{GL}(\mathbb{R}^n)$ and $\mathrm{GL}(n, \mathbb{R})$ and their operations are essentially the same, we say that the two groups are *isomorphic*. We give a formal definition later in this section.

We conclude our list of examples of groups with one that may seem a bit contrived. We include it to show that there are many ways to define groups and to illustrate the steps needed to verify that a given set with an operation is a group.

2.15 Example Let $*$ be defined on $\mathbb{Q}^+$ by $a * b = ab/2$. Then

$$(a * b) * c = \frac{ab}{2} * c = \frac{abc}{4},$$

and likewise

$$a * (b * c) = a * \frac{bc}{2} = \frac{abc}{4}.$$

Thus $*$ is associative. Computation shows that

$$2 * a = a * 2 = a$$

for all $a \in \mathbb{Q}^+$, so 2 is an identity element for $*$. Finally,

$$a * \frac{4}{a} = \frac{4}{a} * a = 2,$$

so $a' = 4/a$ is an inverse for a. Hence $\mathbb{Q}^+$ with the operation $*$ is a group. ▲

Elementary Properties of Groups

As we proceed to prove our first theorem about groups, we must use Definition 2.1, which is the only thing we know about groups at the moment. The proof of a second theorem can employ both Definition 2.1 and the first theorem; the proof of a third theorem can use the definition and the first two theorems, and so on.

Our first theorem will establish cancellation laws. In real number arithmetic, we know that $2a = 2b$ implies that $a = b$. We need only divide both sides of the equation $2a = 2b$ by 2, or equivalently, multiply both sides by $\frac{1}{2}$, which is the multiplicative inverse of 2. We parrot this proof to establish cancellation laws for any group. Note that we will also use the associative law.

2.16 Theorem If G is a group with binary operation $*$, then the **left and right cancellation laws** hold in G, that is, $a * b = a * c$ implies $b = c$, and $b * a = c * a$ implies $b = c$ for all $a, b, c \in G$.

Proof Suppose $a * b = a * c$. Then by $\mathscr{G}_3$, there exists a', and

$$a' * (a * b) = a' * (a * c).$$

By the associative law,

$$(a' * a) * b = (a' * a) * c.$$

By the definition of a' in $\mathscr{G}_3$, $a' * a = e$, so

$$e * b = e * c.$$