Part I

GROUP THEORY

The modern treatment of abstract algebra begins with the disarmingly simple abstract definition of a *group*. This simple definition quickly leads to difficult questions involving the structure of such objects. There are many specific examples of groups and the power of the abstract point of view becomes apparent when results for *all* of these examples are obtained by proving a *single* result for the abstract group.

The notion of a group did not simply spring into existence, however, but is rather the culmination of a long period of mathematical investigation, the first formal definition of an abstract group in the form in which we use it appearing in 1882.[1] The definition of an abstract group has its origins in extremely old problems in algebraic equations, number theory, and geometry, and arose because very similar techniques were found to be applicable in a variety of situations. As Otto Hölder (1859–1937) observed, one of the essential characteristics of mathematics is that after applying a certain algorithm or method of proof one then considers the scope and limits of the method. As a result, properties possessed by a number of interesting objects are frequently abstracted and the question raised: can one determine *all* the objects possessing these properties? Attempting to answer such a question also frequently adds considerable understanding of the original objects under consideration. It is in this fashion that the definition of an abstract group evolved into what is, for us, the starting point of abstract algebra.

We illustrate with a few of the disparate situations in which the ideas later formalized into the notion of an abstract group were used.

(1) In number theory the very object of study, the set of integers, is an example of a group. Consider for example what we refer to as "Euler's Theorem" (cf. Exercise 22 of Section 3.2), one extremely simple example of which is that a^{40} has last two digits 01 if a is any integer not divisible by 2 nor by 5. This was proved in 1761 by Leonhard Euler (1707–1783) using "group-theoretic" ideas of Joseph Louis Lagrange (1736–1813), long before the first formal definition of a group. From our perspective, one now proves "Lagrange's Theorem" (cf. Theorem 8 of Section 3.2), applying these techniques abstracted to an arbitrary group, and then *recovers* Euler's Theorem (and many others) as a *special case*.

[1] For most of the historical comments below, see the excellent book *A History of Algebra*, by B. L. van der Waerden, Springer-Verlag, 1980 and the references there, particularly *The Genesis of the Abstract Group Concept: A Contribution to the History of the Origin of Abstract Group Theory* (translated from the German by Abe Shenitzer), by H. Wussing, MIT Press, 1984. See also *Number Theory, An Approach Through History from Hammurapai to Legendre*, by A. Weil, Birkhäuser, 1984.

(2) Investigations into the question of rational solutions to algebraic equations of the form $y^2 = x^3 - 2x$ (there are infinitely many, for example $(0, 0)$, $(-1, 1)$, $(2, 2)$, $(9/4, -21/8)$, $(-1/169, 239/2197)$) showed that connecting any two solutions by a straight line and computing the intersection of this line with the curve $y^2 = x^3 - 2x$ produces another solution. Such "Diophantine equations," among others, were considered by Pierre de Fermat (1601–1655) (this one was solved by him in 1644), by Euler, by Lagrange around 1777, and others. In 1730 Euler raised the question of determining the indefinite integral $\int dx/\sqrt{1-x^4}$ of the "lemniscatic differential" $dx/\sqrt{1-x^4}$, used in determining the arc length along an ellipse (the question had also been considered by Gottfried Wilhelm Leibniz (1646–1716) and Johannes Bernoulli (1667–1748)). In 1752 Euler proved a "multiplication formula" for such elliptic integrals (using ideas of G.C. di Fagnano (1682–1766), received by Euler in 1751), which shows how two elliptic integrals give rise to a third, bringing into existence the theory of elliptic functions in analysis. In 1834 Carl Gustav Jacob Jacobi (1804–1851) observed that the work of Euler on solving certain Diophantine equations amounted to writing the multiplication formula for certain elliptic integrals. Today the curve above is referred to as an "elliptic curve" and these questions are viewed as two different aspects of the same thing — the fact that this geometric operation on points can be used to give the set of points on an elliptic curve the structure of a group. The study of the "arithmetic" of these groups is an active area of current research.[2]

(3) By 1824 it was known that there are formulas giving the roots of quadratic, cubic and quartic equations (extending the familiar quadratic formula for the roots of $ax^2 + bx + c = 0$). In 1824, however, Niels Henrik Abel (1802–1829) proved that such a formula for the roots of a quintic is impossible (cf. Corollary 40 of Section 14.7). The proof is based on the idea of examining what happens when the roots are permuted amongst themselves (for example, interchanging two of the roots). The collection of such permutations has the structure of a group (called, naturally enough, a "permutation group"). This idea culminated in the beautiful work of Evariste Galois (1811–1832) in 1830–32, working with explicit groups of "substitutions." Today this work is referred to as Galois Theory (and is the subject of the fourth part of this text). Similar explicit groups were being used in geometry as collections of geometric transformations (translations, reflections, etc.) by Arthur Cayley (1821–1895) around 1850, Camille Jordan (1838–1922) around 1867, Felix Klein (1849–1925) around 1870, etc., and the application of groups to geometry is still extremely active in current research into the structure of 3-space, 4-space, etc. The same group arising in the study of the solvability of the quintic arises in the study of the rigid motions of an icosahedron in geometry and in the study of elliptic functions in analysis.

The precursors of today's abstract group can be traced back many years, even before the groups of "substitutions" of Galois. The formal definition of an abstract group which is our starting point appeared in 1882 in the work of Walter Dyck (1856–1934), an assistant to Felix Klein, and also in the work of Heinrich Weber (1842–1913)

[2]See *The Arithmetic of Elliptic Curves* by J. Silverman, Springer-Verlag, 1986.

in the same year.

It is frequently the case in mathematics research to find specific application of an idea before having that idea extracted and presented as an item of interest in its own right (for example, Galois used the notion of a "quotient group" implicitly in his investigations in 1830 and the definition of an abstract quotient group is due to Hölder in 1889). It is important to realize, with or without the historical context, that the reason the abstract definitions are made is because it is useful to isolate specific characteristics and consider what structure is imposed on an object having these characteristics. The notion of the structure of an algebraic object (which is made more precise by the concept of an isomorphism — which considers when two apparently different objects are in some sense the same) is a major theme which will recur throughout the text.

CHAPTER 1

Introduction to Groups

1.1 BASIC AXIOMS AND EXAMPLES

In this section the basic algebraic structure to be studied in Part I is introduced and some examples are given.

Definition.

(1) A *binary operation* $\star$ on a set G is a function $\star : G \times G \to G$. For any $a, b \in G$ we shall write $a \star b$ for $\star(a, b)$.

(2) A binary operation $\star$ on a set G is *associative* if for all $a, b, c \in G$ we have $a \star (b \star c) = (a \star b) \star c$.

(3) If $\star$ is a binary operation on a set G we say elements a and b of G *commute* if $a \star b = b \star a$. We say $\star$ (or G) is *commutative* if for all $a, b \in G$, $a \star b = b \star a$.

Examples

(1) $+$ (usual addition) is a commutative binary operation on $\mathbb{Z}$ (or on $\mathbb{Q}$, $\mathbb{R}$, or $\mathbb{C}$ respectively).

(2) $\times$ (usual multiplication) is a commutative binary operation on $\mathbb{Z}$ (or on $\mathbb{Q}$, $\mathbb{R}$, or $\mathbb{C}$ respectively).

(3) $-$ (usual subtraction) is a noncommutative binary operation on $\mathbb{Z}$, where $-(a, b) = a - b$. The map $a \mapsto -a$ is not a binary operation (not binary).

(4) $-$ is not a binary operation on $\mathbb{Z}^+$ (nor $\mathbb{Q}^+, \mathbb{R}^+$) because for $a, b \in \mathbb{Z}^+$ with $a < b$, $a - b \notin \mathbb{Z}^+$, that is, $-$ does not map $\mathbb{Z}^+ \times \mathbb{Z}^+$ into $\mathbb{Z}^+$.

(5) Taking the vector cross-product of two vectors in 3-space $\mathbb{R}^3$ is a binary operation which is not associative and not commutative.

Suppose that $\star$ is a binary operation on a set G and H is a subset of G. If the restriction of $\star$ to H is a binary operation on H, i.e., for all $a, b \in H$, $a \star b \in H$, then H is said to be *closed* under $\star$. Observe that if $\star$ is an associative (respectively, commutative) binary operation on G and $\star$ restricted to some subset H of G is a binary operation on H, then $\star$ is automatically associative (respectively, commutative) on H as well.

Definition.

(1) A *group* is an ordered pair $(G, \star)$ where G is a set and $\star$ is a binary operation on G satisfying the following axioms: