Preface

This book is designed to serve as a basic text of modern algebra at the undergraduate level. Modern mathematics facilitates unification of different areas of mathematics. It is characterized by its emphasis on the systematic study of a number of abstract mathematical structures. Modern algebra provides a language for almost all disciplines in contemporary mathematics.

This book introduces the basic language of modern algebra through a study of groups, group actions, rings, fields, vector spaces, modules, algebraic numbers, etc. The term Modern Algebra (or Abstract Algebra) is used to distinguish this area from classical algebra. Classical algebra grew over thousands of years. On the other hand, modern algebra began as late as 1770. Modern algebra is used in many areas of mathematics and other sciences. For example, it is widely used in algebraic topology of which the main objective is to solve topological and geometrical problems by using algebraic objects. Category theory plays an important role in this respect. Grigory Perelman solved the Poincaré conjecture by using the tools of modern algebra and other modern mathematical concepts (beyond the scope of the discussion in this book). A study of algebraic numbers includes studies of various number rings which generalize the set of integers. It also offers a natural inspiration to reinterpret the results of classical algebra and number theory and provides a scope of greater unity and generality. Algebraic number theory provides important tools to solve many problems in mathematics. For example, Andrew Wiles proved Fermat's last theorem by using algebraic number theory along with other theories (not discussed in this book). Moreover, an attempt has been made to integrate the classical materials of elementary number theory with modern algebra with an eye to apply them in different disciplines, specially in cryptography. Some applications unify computer science with mainstream mathematics. It dispels, at least, partly a general feeling that much of abstract algebra is of little practical value. The main purpose of this book is to give an accessible presentation to its readers. The materials discussed here have appeared elsewhere. Our contribution is the selection of the materials and their presentation. The title of the book suggests the scope of the book, which is expanded over 12 chapters and three appendices.

Chapter 1 studies basic concepts of set theory and properties of integers, which are used throughout the book and in many other disciplines. Set theory occupies a very prominent place in modern science. There are two general approaches to set theory. The first one is called "naive set theory" initiated by Georg Cantor around 1870; the second one is called "axiomatic set theory" originated by E. Zermelo in 1908 and modified by A. Fraenkel and T. Skolem. This chapter develops a naive set theory, which is a non-formalized theory by using a natural language to describe sets and their basic properties. For a precise description of many notions of modern algebra and also for mathematical reasoning, the concepts of relations, Zorn's lemma, mappings (functions), cardinality of sets are very important. They form the basics of set theory and are discussed in this chapter. The set of integers plays an important role in the development of science, engineering, technology and human civilization. In this chapter, some basic concepts and properties of integers, such as Peano's axioms leading to the principle of mathematical induction, well-ordering principle, division algorithm, greatest common divisors, prime numbers, fundamental theorem of arithmetic, congruences on integers, etc., are also discussed. Further studies on number theory are given in Chap. 10.

Chapter 2 gives an introduction to the group theory. This concept is used in subsequent chapters. Groups serve as one of the fundamental building blocks for the subject called today modern algebra. The theory of groups began with the work of J.L. Lagrange (1736–1813) and E. Galois (1811–1832). At that time, mathematicians worked with groups of transformations. These were sets of mappings, that, under composition, possessed certain properties. Mathematicians, such as Felix Klein (1849–1925), adopted the idea of groups to unify different areas of geometry. In 1870, L. Kronecker (1823–1891) gave a set of postulates for a group. Earlier definitions of groups were generalized to the present concept of an abstract group in the first decade of the twentieth century, which was defined by a set of axioms. In this chapter, we make an introductory study of groups with geometrical applications along with a discussion of free abelian groups and structure theorem for finitely generated abelian groups. Moreover, semigroups, homology groups, cohomology groups, topological groups, Lie groups, Hopf groups, and fundamental groups are also studied here.

Chapter 3 discusses actions of semigroups, groups, topological groups, and Lie groups. Each element of a group determines a permutation on a set under a group action. For a topological group action on a topological space, this permutation is a homeomorphism and for a Lie group action on a differentiable manifold it is a diffeomorphism. Group actions are used in the proofs of the counting principle, Cayley's Theorem, Cauchy's Theorem and Sylow Theorems for finite groups. Counting principle is used to determine the structure of a group of prime power order. These groups arise in the Sylow Theorems and in the description of finite abelian groups. Orbit spaces obtained by topological group actions, discussed in this chapter, are very important in topology and geometry. For example, n-dimensional real and complex projective spaces are obtained as orbit spaces. Finally, semigroup actions applied to theoretical computer science, yield state machines which unify computer science with mainstream mathematics.

Rings also serve as a fundamental building blocks for modern algebra. Chapter 4 introduces the concept of rings, another fundamental concept in the study of modern algebra. A "group" is endowed with only one binary operation while a "ring" is endowed with two binary operations connected by some interrelations. Fields form a very important class of rings. The concept of rings arose through the attempts to prove Fermat's last theorem and was initiated by Richard Dedekind (1831–1916) around 1880. David Hilbert (1862–1943) coined the term "ring". Emmy Noether (1882–1935) developed the theory of rings under his guidance. A very particular but important type of rings is known as commutative rings that play an important role in algebraic number theory and algebraic geometry. Further, non-commutative rings are used in non-commutative geometry and quantum groups. In this chapter, Wedderburn theorem on finite division rings, and some special rings, such as rings of power series, rings of polynomials, rings of continuous functions, rings of endomorphisms of abelian groups and Boolean rings are also studied.

Chapter 5 continues the study of theory of rings, and introduces the concept of ideals which generalize many important properties of integers. Ideals and homomorphisms of rings are closely related. Like normal subgroups in the theory of groups, ideals play an analogous role in the study of rings. The real significance of ideals in a ring is that they enable us to construct other rings which are associated with the first in a natural way. Commutative rings and their ideals are closely related. Their relations develop ring theory and are applied in many areas of mathematics, such as number theory, algebraic geometry, topology and functional analysis. In this chapter, basic properties of ideals are discussed and explained with interesting examples. Ideals of rings of continuous functions and Chinese remainder theorem for rings with their applications are also studied. Finally, applications of ideals to algebraic geometry with Hilbert's Nullstellensatz theorem, and the Zariski topology are discussed and certain connections among algebra, geometry and topology are given.

Chapter 6 extends the concepts of divisibility, greatest common divisor, least common multiple, division algorithm and fundamental theorem of arithmetic for integers with the help of theory of ideals to the corresponding concepts for rings. The main aim of this chapter is to study the problem of factoring the elements of an integral domain as products of irreducible elements. This chapter also caters to the study of the polynomial rings over a certain class of important rings and proves the Eisenstein irreducibility criterion, Gauss Lemma and related topics. Our study culminates in proving the Gauss Theorem which provides an extensive class of uniquely factorizable domains.

Chapter 7 continues to develop the theory of rings and studies chain conditions for ideals of a ring. The motivation came from an interesting property of the ring of integers $\mathbf{Z}$: that its every ascending chain of ideals terminates. This interesting property of $\mathbf{Z}$ was first recognized by the German mathematician Emmy Noether (1882–1935). This property leads to the concept of Noetherian rings, named after Noether. On the other hand, Emil Artin (1898–1962) showed that there are some rings in which every descending chain of ideals terminates. Such rings are called Artinian rings in honor of Emil Artin. This chapter studies special classes of rings, such as Noetherian rings and Artinian rings and obtains deeper results on ideal theory. This chapter further introduces a Noetherian domain and an Artinian domain

and establishes their interesting properties. Hilbert's Basis Theorem, which gives an extensive class of Noetherian rings, is also proved in this chapter. Its application to algebraic geometry is also discussed. This study culminates in rings with descending chain condition for ideals, which determines their ideal structure.

Chapter 8 introduces another algebraic system, called vector spaces (linear spaces) interlinking both internal and external operations. In this chapter, vector spaces and their closely related fundamental concepts, such as linear independence, basis, dimension, linear transformation and its matrix representation, eigenvalue, inner product space, etc., are presented. Such concepts form an integral part of linear algebra. Vector spaces have multi-faceted applications. Such spaces over finite fields play an important role in computer science, coding theory, design of experiments and combinatorics. Vector spaces over the infinite field $\mathbf{Q}$ of rationals are important in number theory and design of experiments while vector spaces over $\mathbf{C}$ are essential for the study of eigenvalues. As the concept of a vector provides a geometric motivation, vector spaces facilitate the study of many areas of mathematics and integrate the abstract algebraic concepts with the geometric ideas.

Chapter 9 initiates module theory, which is one of the most important topics in modern algebra. It is a generalization of an abelian group (which is a module over the ring of integers $\mathbf{Z}$) and also a natural generalization of a vector space (which is a module over a division ring or over a field). Many results of vector spaces are generalized in some special classes of modules, such as free modules and finitely generated modules over principal ideal domains. Modules are closely related to the representation theory of groups. One of the basic concepts which accelerates the study of commutative algebra is module theory, as modules play the central role in commutative algebra. Modules are also widely used in structure theory of finitely generated abelian groups, finite abelian groups and rings, homological algebra, and algebraic topology. In this chapter, we study the basic properties of modules. We also consider modules of special classes, such as free modules, modules over principal ideal domains along with structure theorems, exact sequences of modules and their homomorphisms, Noetherian and Artinian modules, homology and cohomology modules. Our study culminates in a discussion on the topology of the spectrum of modules and rings with special reference to the Zariski topology.

Chapter 10 discusses some more interesting properties of integers, in particular, properties of prime numbers and primality testing by using the tools of modern algebra, which are not studied in Chap. 1. In addition, we study the applications of number theory, particularly those directed towards theoretical computer science. Number theory has been used in many ways to devise algorithms for efficient computer and for computer operations with large integers. Both algebra and number theory play an increasingly significant role in computing and communication, as evidenced by the striking applications of these subjects to the fields of coding theory and cryptography. The motivation of this chapter is to provide an introduction to the algebraic aspects of number theory, mainly the study of development of the theory of prime numbers with an emphasis on algorithms and applications, necessary for studying cryptography to be discussed in Chap. 12. In this chapter, we start with the introduction to prime numbers with a brief history. We provide several different proofs of

the celebrated Theorem of Euclid, stating that there exist infinitely many primes. We further discuss Fermat number, Mersenne numbers, Carmichael numbers, quadratic reciprocity, multiplicative functions, such as Euler ϕ-function, number of divisor functions, sum of divisor functions, etc. This chapter ends with a discussion of primality testing both deterministic and probabilistic, such as Solovay–Strassen and Miller–Rabin probabilistic primality tests.

Chapter 11 introduces algebraic number theory which developed through the attempts of mathematicians to prove Fermat's last theorem. An algebraic number is a complex number, which is algebraic over the field $\mathbf{Q}$ of rational numbers. An algebraic number field is a subfield of the field $\mathbf{C}$ of complex numbers, which is a finite field extension of the field $\mathbf{Q}$, and is obtained from $\mathbf{Q}$ by adjoining a finite number of algebraic elements. The concepts of algebraic numbers, algebraic integers, Gaussian integers, algebraic number fields and quadratic fields are introduced in this chapter after a short discussion on general properties of field extension and finite fields. There are several proofs of fundamental theorem of algebra. It is proved in this chapter by using homotopy (discussed in Chap. 2). Moreover, countability of algebraic numbers, existence of transcendental numbers, impossibility of duplication of a general cube and that of trisection of a general angle are shown in this chapter.

Chapter 12 presents applications and initiates a study of cryptography. In the modern busy digital world, the word "cryptography" is well known to many of us. Everyday, knowingly or unknowingly, in many places we use different techniques of cryptography. Starting from the logging on a PC, sending e-mails, withdrawing money from ATM by using a PIN code, operating the locker at a bank with the help of a designated person from the bank, sending message by using a mobile phone, buying things through the internet by using a credit card, transferring money digitally from one account to another over internet, we are applying cryptography everywhere. If we observe carefully, we see that in every case we are required to hide some information to transfer information secretly. So, intuitively, we can guess that cryptography has something to do with security. So, intuitively, we can guess that cryptography and secrecy have a close connection. Naturally, the questions that come to our mind are: What is cryptography? How is it that it is important to our daily life? In this chapter, we introduce cryptography and provide a brief overview of the subject and discuss the basic goals of cryptography and present the subject, both intuitively and mathematically. More precisely, various cryptographic notions starting from the historical ciphers to modern cryptographic notions like public key encryption schemes, signature schemes, secret sharing schemes, oblivious transfer, etc., by using mathematical tools mainly based on modern algebra are explained. Finally, the implementation issues of three public key cryptographic schemes, namely RSA, ElGamal, and Rabin by using the open source software SAGE are discussed.

Appendix A studies some interesting properties of semirings. Semiring theory is a common generalization of the theory of associative rings and theory of distributive lattices. Because of wide applications of results of semiring theory to different branches of computer science, it has now become necessary to study structural results on semirings. This chapter gives some such structural results.

Appendix B discusses category theory initiated by S. Eilenberg and S. Mac Lane during 1942–1945, to provide a technique for unifying certain concepts. In general, the pedagogical methods compartmentalize mathematics into its different branches without emphasizing their interconnections. But the category theory provides a convenient language to tie together several notions and existing results of different areas of mathematics. This language is conveyed through the concepts of categories, functors, natural transformations, which form the basics of category theory and provide tools to shift problems of one branch of mathematics to another branch to have a better chance for solution. For example, the Brouwer fixed-point theorem is proved here with the help of algebraic objects. Moreover, extension problems and classification of topological spaces are discussed in this chapter.

Appendix C gives a brief historical note highlighting contributions of some mathematicians to modern algebra and its closely related topics. The list includes a few names only, such as the names of Leonhard Euler (1707–1783), Joseph Louis Lagrange (1736–1813), Carl Friedrich Gauss (1777–1855), Augustin Louis Cauchy (1789–1857), Niels Henrik Abel (1802–1829), C.G.J. Jacobi (1804–1851), H. Grassmann (1809–1877), Evariste Galois (1811–1832), Arthur Cayley (1821–1895), Leopold Kronecker (1823–1891), Bernhard Riemann (1826–1866), Richard Dedekind (1831–1926), Peter Ludvig Mejdell Sylow (1832–1918), Camille Jordan (1838–1922), Sophus Lie (1842–1899), Georg Cantor (1845–1918), C. Felix Klein (1849–1925), Henri Poincaré (1854–1912), David Hilbert (1862–1943), Amalie Emmy Noether (1882–1935), MecLagan Wedderburn (1882–1948), Emil Artin (1898–1962) and Oscar Zariski (1899–1986).

The authors express their sincere thanks to Springer for publishing this book. The authors are very thankful to many individuals, our postgraduate and Ph.D. students, who have helped in proof reading the book. Our thanks are due to the institute IMBIC, Kolkata, for kind support towards the manuscript development work of this book. Finally, we acknowledge, with heartfelt thanks, the patience and sacrifice of our long-suffering family, specially Minati, Sahibopriya, and little Avipriyo.

Kolkata, India

Mahima Ranjan Adhikari
Avishek Adhikari

http://www.springer.com/978-81-322-1598-1

Basic Modern Algebra with Applications

Adhikari, M.R.; Adhikari, A.

2014, XIX, 637 p. 48 illus., Hardcover
ISBN: 978-81-322-1598-1