A Textbook of MODERN ALGEBRA

3rd Revised Edition

N Ramabhadran

A TEXTBOOK OF
MODERN ALGEBRA

R. BALAKRISHNAN
Post-graduate Professor and Head,
Department of Mathematics
National College,
Tiruchirapalli

N. RAMABHADRAN
Professor and Head,
Department of Mathematics
Madras University Centre,
Tiruchirapalli

Third Revised Edition
1979

VIKAS PUBLISHING HOUSE PVT LTD
New Delhi Bombay Bangalore Calcutta Kanpur

VIKAS PUBLISHING HOUSE PVT LTD
5 Ansari Road, New Delhi 110002
Savoy Chambers, 5 Wallace Street, Bombay 400001
10 First Main Road, Gandhi Nagar, Bangalore 560009
8/1-B Chowringhee Lane, Calcutta 700016
80 Canning Road, Kanpur 208004

Second edition : 1978
Third edition : 1979

1V2R4202

ISBN 0-7069-0909-7

Rs 15

(Paper used for the printing of this book was made available by the Government of India at concessional rates.)

Printed at Eskay Printers, 20/5, West Patel Nagar, New Delhi-110008.

PREFACE TO THE THIRD EDITION

This edition has been thoroughly revised by adding many new problems with their proofs at the appropriate places.

Modern Algebra—currently called Abstract Algebra, as it is no longer modern (!) deals with mathematical structures which are algebraic in character. Some of these structures are: Groups, Rings, Fields and Vector Spaces. These algebraic structures are built upon sets with certain algebraic operations. Our aim in this text is to make the students acquaint themselves with the basic concepts of some of these fundamental algebraic structures.

This book which is primarily written for the B.Sc. students of Mathematics in India is also designed to cater to the needs of students in allied fields such as Statistics, Physics, Chemistry and Engineering any may well be used as a reference book by them. We have presented what is normally expected to be covered in Modern Algebra for the B.Sc. degree course in as elementary and simple a manner as possible. While we fully realise the impossibility of our making an original imprint in an elementary text such as this, we can certainly make a claim in flooding the book with a volley of motivating examples and a wide variety of exercises and worked out problems. Further to aid the reader, we have given hints and solutions to all the exercises which need non-routine solutions. Also, the book is divided conveniently into two parts with Linear Algebra, as Part I and the more abstract concepts such as Groups and Rings forming Part II, as we believe that Linear Algebra is not only more accessible to student for an initial study but also provides a simple introduction to more abstract concepts of Groups and Rings through the Rings of Linear Transformations, Matrices and Matrix Groups which are introduced in Part I.

Also, in the semesterised pattern of B.Sc. courses in Indian universities, Part I may be had for an earlier semester while Part II can be done during a subsequent semester.

With many motivating and initiating examples through which abstract concepts are introduced, it is hoped that this book will be a readily acceptable companion to both the teacher and the taught.

As quite a few standard and well known examples and exercises are given at appropriate places, this would be found to be very helpful by the student from his examination preparation point.

We are thankful to R. Ganapathy, S. Ramanujam and N. Sridharan for their help in the preparation of this book.

AUTHORS

LIST OF SYMBOLS

$\in$	Is an element of
$\notin$	Is not an element of
$\subset$	Contained in
$\supset$	Contains
$=$	Equals
A' in X	Complement of A in X, where $A \subset X$
$\cup$	Union
$\cap$	Intersection
$\times$	Cartesian product
$(a_1, \ldots, a_n)$	Ordered n-tuple of elements $a_1, \ldots, a_n$
$\{\}$	Set with elements in the bracket
$\{/\}$	Set of elements such that
ϕ	Empty set or Null set
$f: A \to B$	Map, f, from A to B
f^{-1}	Inverse map of f
$f^{-1}(F)$	Inverse image of $F \subset B$, for the map $f: A \to B$ which is the subset of A of all elements $x \in A$ such that $f(x) \in F$.
dim T	Dimension of vector space V
$\simeq$	Is isomorphic to
$Sp<S>$	Span of the subset S
$<S>$	Subgroup generated by S
L_s	Linear span of S, consisting of all finite linear combinations of elements of S.
$L + M$	The set of all sums $l+m$ for $l \in L$ and $m \in M$.
$L \oplus M$	Direct sum of L and M
iff, also $\Leftrightarrow$	If and only if
$\Rightarrow$	Implies
Im f	Image of the map f
Ker f	Kernel of the homomorphism f
Z, N, Q, R, C	The set of all integers, all positive integers, all rational numbers, all real numbers, all complex numbers respectively.
$\mathbf{N}^n$, $\mathbf{R}^n$, $\mathbf{C}^n$	Cartesian product of **N**, **R**, **C** respectively taken n-times.

$\mathbf{Z}^*$, $\mathbf{Q}^*$, $\mathbf{R}^*$, $\mathbf{C}^*$	The set of all non-zero integers, non-zero rational numbers, non-zero real numbers, non-zero complex numbers respectively.
$\mathbf{Z}^+$, $\mathbf{Q}^+$, $\mathbf{R}^+$	The set of all positive integers, positive rational numbers, positive real numbers respectively.
$f : a \mapsto f(a)$	The map, f, mapping a to $f(a)$.
I_n	The identity matrix of order n.
A^t, $\overline{A}$, A^* for a complex matrix A	Transpose, complex conjugate, conjugate transpose of A respectively.
adj. A for a square matrix A over a field	Adjoint or Adjugate of A.
det A for a square matrix A over a field	Determinant of A
$p = \begin{pmatrix} 1 & 2 & \dots & n \\ p_1 & p_2 & \dots & p^n \end{pmatrix}$	Permutation p of degree n given by the map $p : i \mapsto p_i$ for $i = 1, 2, \dots, n$.
R_a for an equivalence relation R on A	The equivalence class $R_a \subset A$, consisting of all $b \in A$ such that $(a, b) \in R$.
$\mathbf{Z}+i\mathbf{Z}$	The set of all Gaussian integers, *i.e.*, all complex numbers $m + i\,n$ for $m, n \in \mathbf{Z}$.
$M_n(K)$	The set of all n by n matrices with entries from K.
$GL(n, \mathbf{R})$	The set of all n by n non-singular real matrices (called the General Linear Group of order n over $\mathbf{R}$).
$SL(n, \mathbf{R})$	The set of all n by n real matrices with determinant 1 (called the Special Linear Group of order n over $\mathbf{R}$).
$\mathbf{Z}[X]$, $\mathbf{R}[X]$, $\mathbf{C}[X]$	The set of all polynomials in X with integral, real, complex coefficients respectively.
$\mathbf{Z}_n$	The set of all integers modulo n.
■	End of proof.
*	Over an exercise indicates that it is comparatively more difficult.

CONTENTS

PART II

ALGEBRA

(Groups, Rings and Fields)

PART I

LINEAR ALGEBRA

0

ELEMENTS OF SET THEORY

0.1. PRELIMINARY CONCEPTS

We begin with some basic concepts of set theory. The term **set** is used in the sense of every day life. Thus a set A stands for a collection of elements which are such by some definite properties or description, it is possible to say whether or not an element a belongs to A. For example, let X denote *the set of all books in a book-shop* A. This means that by the defining property given in italics above, it is possible for us to assert whether an element a is in X or not.

Let X be a set. If an element a belongs to X, we denote this by $a \in X$. If an element a does not belong to X, this is denoted by $a \notin X$.

When a set is specified by its elements, its elements are enclosed in curly brackets. Thus, for example,

$\mathbf{N} = \{1, 2, 3, \ldots\}$ denotes the set $\mathbf{N}$ of natural numbers.

If Y is a set and if each element of Y is also an element of X, Y is called a **subset** of X, denoted by $Y \subset X$ or $X \supset Y$. We call Y a proper subset of X if Y is a subset of X and $Y \neq X$.

If a set has no element, it is called the **null set** or **empty set** and is denoted by ϕ. The empty set is a subset of every set.

Unless otherwise mentioned, all sets we consider in the succeeding chapters of this book are to be taken as nonempty.

If X and Y are sets and if $Y \subset X$, then $X - Y$ or Y' in X denotes the subset, called the **complement** of Y in X, $X - Y$ consisting of all those elements a of X such that $a \notin Y$.

Two sets X and Y are called equal, $X = Y$, if $X \subset Y$ and $Y \subset X$.

Let X and Y be sets. The **set union** of X and Y is the set $X \cup Y$ of all those elements a such that $a \in X$ or $a \in Y$. For instance, if X denotes the set of students of a class of height less than five feet and Y denotes the set of students of this class of height greater than or equal to five feet, $X \cup Y$ denotes the set of all students of this class.

The **set intersection** of two sets X and Y is the set $X \cap Y$ of all elements which belong to *both* the sets X and Y. For instance, let X denote the set of factories in an industrial city with at least 500

male workers, and at least 400 female workers, and let Y denote the set of factories in the same city with at least 400 male workers and at least 500 female workers. Then $X \cap Y$ is the set of factories that employ at least 500 male and 500 female workers.

When we have more than two sets, the definitions are made in the same way as above. For instance, if $\{X_i\}$ $i \in I$, with the index i varying over an indexing set I (which may be quite arbitrary) is a collection of sets (a more precise term for such an indexed collection of sets is a **family** of sets), the set union $\bigcup_{i \in I} X_i$ is the set of all those elements a such that $a \in X_i$ for *some* index $i \in I$. Similarly, the intersection $\bigcap_{i \in I} X_i$ is the set of all those a such that $a \in X_i$ for *each* $i \in I$.

Proposition 0.1.1. For sets A, B, C the following rules are valid:

$$(i)\ (A \cup B) \cup C = A \cup (B \cup C), \quad (A \cap B) \cap C = A \cap (B \cap C),$$
$$(ii)\ A \cup B = B \cup A; \quad A \cap B = B \cap A.$$
$$(iii)\ (A \cup B) \cap C = (A \cap C) \cup (B \cap C), \quad (A \cap B) \cup C = (A \cup C) \cap (B \cup C).$$

Proof. We prove (i). Others can be proved in a similar manner.

Let $a \in (A \cup B) \cup C$. Then $a \in A \cup B$ or $a \in C$. Hence $a \in A$ or B or C. This means that $a \in A \cup (B \cup C)$ as this also means as above that $a \in A$ or B or C i.e., $(A \cup B) \cup C \subset A \cup (B \cup C)$. In the same way, it follows that $A \cup (B \cup C) \subset (A \cup B) \cup C$. This proves the result (i). ∎

EXERCISE 0.1.2. Prove (ii) and (iii) above.

Proposition 0.1.3. (De Morgan's Laws). Let $\{A_i\}$ $i \in I$ be a family of subsets A_i of a set X. Then

$$(i)\ \left(\bigcup_{i \in I} A_i\right)' = \bigcap_{i \in I} A_i'$$

and $$(ii)\ \left(\bigcap_{i \in I} A_i\right)' = \bigcup_{i \in I} A_i',$$

where the complements are taken in the set X.

Proof. We prove (i). The proof of (ii) is similar.

Let $x \in \left(\bigcup_{i \in I} A_i\right)'$. This means that $x \notin \bigcup_{i \in I} A_i$ and hence $x \notin A_i$ for any $i \in I$. This of course implies that $x \in A_i'$ for each $i \in I$; a fortiori $x \in \bigcap_{i \in I} A_i'$. Thus $\left(\bigcup_{i \in I} A_i\right)' \subset \bigcap_{i \in I} A_i'$. Conversely, suppose that $x \in \bigcap_{i \in I} A_i'$. This means that $x \in A_i'$ for each $i \in I$ and hence $x \notin A_i$ for any i. Thus $x \notin \bigcup_{i \in I} A_i$; whence, $x \in \left(\bigcup_{i \in I} A_i\right)'$ and this proves that $\bigcap_{i \in I} A_i' \subset \left(\bigcup_{i \in I} A_i\right)'$. Consequently, $\left(\bigcup_{i \in I} A_i\right)' = \bigcap_{i \in I} A_i'$.

EXERCISE 0.1.4. Write down the De Morgan's Laws when the indexing set I is a set of (*i*) 2 elements (*ii*) 3 elements.

DEFINITION 0.1.5. A family $\{X_i\}$, $i \in I$ of sets is called disjoint if the intersection of any two distinct members of the family is empty i.e., for $i, j \in I$, $i \neq j$, $X_i \cap X_j = \phi$.

0.2. MAPS

DEFINITION 0.2.1. A **map (mapping** or **function** or **single-valued mapping)** $f : A \to B$ from a set A to a set B is a rule by which to each $a \in A$ there is assigned a unique element $f(a) \in B$.

Set A is then called the domain of f.

For example, if A is the set of students of a class X and B is the set of positive integers, a map $f : A \to B$ is defined if we set $f(a)$ to be the age of the student $a \in A$.

As another example, let A be the set of all factories in a country and B, the set of positive integers. A map $f : A \to B$ is defined if we set $f(a)$ as the value in rupees of goods produced in the factory a during a particular year.

Two maps $f : A \to B$ and $g : A \to B$ are called equal if $f(a) = g(a)$ for each $a \in A$.

Let $f : A \to B$ be a map from set A to set B.

DEFINITION 0.2.2. The **image of an element** $a \in A$, denoted by $f(a)$, is that element $f(a)$ which is assigned to a under the rule f.

The **image of a subset** E of A under $f : A \to B$, denoted by $f(E)$, is the subset $f(E) \subseteq B$ consisting of $f(a)$ for all $a \in A$. In symbols: $f(E) = \{f(a) \in B \mid a \in A\}$.

DEFINITION 0.2.3. A map $f : A \to B$ is called **one-to-one** (1-1 or one-one or **injective**) if $a \neq a'$ in A implies that $f(a') \neq f(a')$ in B (or equivalently, $f(a) = f(a')$ implies that $a = a'$).

Thus, if $f : A \to B$ is a one-to-one map, no two distinct elements of A can have the same image in B under the map f.

For example, let A denote the set of cars registered during last year in a district X and let B stand for the set of registration numbers of these cars. Let $f : A \to B$ be the map defined by setting $f(a)$ as the registration number of the car a during last year. Then f is a one-to-one map (as no two different cars are given the same registration number).

On the other hand, if A denotes the set of people in India and B, the set of positive integers and if $f : A \to B$ is the map defined by setting $f(a)$ as the age of the person a, then f is clearly not one-to-one (Correct !).

DEFINITION 0.2.4. A map $f : A \to B$ is called **onto** or **(surjective)** if for each $b \in B$, there exists at least one $a \in A$ such that $f(a) = b$ (i.e., the image $f(A) = B$ and not merely $f(A) \subset B$.

REMARK. There may be more than one such $a \in A$ with $f(a) = b$.

For example, let A denote the set of students in a college X and B denote the set of all classes in this college. Let $f : A \to B$ be the map where $f(a)$ is the class to which the student $a \in A$ belongs. Then f is an onto map. (A class in any college exists if only there is at least one student in it !).

DEFINITION 0.2.5. Let $f : A \to B$ and $g : B \to C$ be maps. The composition of g with f, denoted by gof, is the map $gof : A \to C$ defined by $(gof)(a) = g(f(a))$ for $a \in A$.

Example 0.2.6. Let $\mathbf{R}$ denote the set of real numbers, $\mathbf{R}^+$ the set of positive real numbers and let $S = R^+ \cup \{0\}$. If $f : \mathbf{R} \to S$ and $g : \mathbf{S} \to \mathbf{R}^+$ are maps defined by $f(r) = r^2$, $r \in \mathbf{R}$ and $g(s) = s + 1$, $s \in S$, then gof is defined by $(gof)(r) = g(f(r)) = g(r^2) = r^2 + 1$, $r \in \mathbf{R}$.

Proposition 0.2.7. Composition of maps (when defined) is associative i.e., If $f : A \to B$, $g : B \to C$ and $h : C \to D$ are maps then the two maps $ho(gof)$ and (hog) of from A to D are equal.

The proof is immediate from the fact that for $a \in A$, $(ho(gof))(a) = ((hog)of)(a) = h(g(f(a)))$.

EXERCISE 0.2.8. Give an example of each of the following:

(*a*) a one-to-one map which is not onto.

(*b*) an onto map which is not one-to-one.

(*c*) a one-to-one and onto map.

(*d*) a map which is neither one-to-one nor onto.

DEFINITION 0.2.9. Let $f : A \to B$ be a map. For $F \subset B$, the inverse image $f^{-1}(F)$ of the subset F is defined as the subset of A consisting of all elements $a \in A$ such that $f(a) \in F$. In symbols, $f^{-1}(F) = \{a \in A / f(a) \in F\}$.

Proposition 0.2.10. Let $f : A \to B$. Let $E_1, E_2 \subset A$ and $F_1, F_2 \subset B$. Then the following statements hold:

(*i*) $f(E_1 \cup E_2) = f(E_1) \cup f(E_2)$

(*ii*) $f(E_1 \cap E_2) \subset f(E_1) \cap f(E_2)$

(*iii*) $f^{-1}(F_1 \cup F_2) = f^{-1}(F_1) \cup f^{-1}(F_2)$

(*iv*) $f^{-1}(F_1 \cap F_2) = f^{-1}(F_1) \cap f^{-1}(F_2)$.

Proof. We prove (*i*). The proofs of the others follow in a similar way.

Let $b \in f(E_1 \cup E_2)$. Then there exists an element $a \in E_1 \cup E_2$ such that $f(a) = b$. As $a \in E_1 \cup E_2$, $a \in E_1$ or E_2. In either case, $f(a) \in F(E_1) \cup f(E_2)$. As $b = f(a)$ is arbitrarily chosen in $f(E_1 \cup E_2)$, it follows that $f(E_1 \cup E_2) \subset f(E_1) \cup f(E_2)$.

To prove the reverse inclusion, let $b' \in F(E_1) \cup F(E_2)$. Hence $b' \in f(E_1)$ or $f(E_2)$. If $b' \in f(E_1)$, there exists an element $a' \in E_1 \subset E_1 \cup E_2$

such that $f(a')=b'$ and $f(a') \in f(E_1 \cup E_2)$. If $b' \notin f(E_1)$, then $b' \in f(E_2)$ and it follows in a similar manner that $b' \in f(E_1 \cup E_2)$. Thus $f(E_1) \cup f(E_2) \subset f(E_1 \cup E_2)$ and this proves (*i*).■

EXERCISE 0.2.11. Prove (*ii*), (*iii*) and (*iv*) in proposition 0.2.10 above.

REMARK. Note that there is equality in (*iv*) above while there is, in general, only inequality in (*ii*).

Example 0.2.12. An example to show that $\subset$ in (*ii*) of proposition 0.2.10 above need not always be equality.

Let $A=\{1, 2, 3, 4, 5\}$ and $B=\{6, 7\}$. Define $f: A \to B$ by $f(1)=f(2)=f(4)=6$ and $f(3)=f(5)=7$. Let $E_1=\{1, 2, 3\}$ and $E_2=\{3, 4, 5\}$. Then E_1 and E_2 are subsets of A such that $f(E_1)=f(E_2)=\{6, 7\}=B$ while $f(E_1 \cap E_2)=f(\{3\})=\{7\}$. Thus $f(E_1) \cap f(E_2)=B \neq F \subset E_1 \cap E_2)=\{7\}$.

DEFINITION. 0.2.13. A **family** $\{x_i\}$ $i \in I$, of elements x_i in a set E is a map $x: I \to E$ (I is called the indexing set of this family) where $x_i =$ image $x(i)$, $i \in I$.

A sequence $\{x_n\}$, $n \in \mathbf{N}$ of elements x_n of a set E is a map $x: \mathbf{N} \to E$ i.e., sequence is a family where the indexing set I is the set $\mathbf{N}$ of all natural numbers.

0.3. EQUIVALENCE RELATIONS

DEFINITION 0.3.1. A relation R on a set A is a set of ordered pairs (a_1, a_2) of elements a_1, a_2 of A.

REMARK. The word 'ordered pair' refers to the order in which we write a_1 and a_2 i.e., $(a_1, a_2)=(b_1, b_2)$ if, and only if, $a_1=b_1$ and $a_2=b_2$. For instance, if $a \neq b$ in A, $(a, b) \neq (b, a)$. As the set of all ordered pairs (a, a') of elements a, a' of A is the cartesian product $A \times A$ (by definition), a relation on A is nothing but a subset of $A \times A$. Hence a relation may as well be empty.

DEFINITION 0.3.2. An **equivalence relation** R on a set A is a relation R such that

(*i*) R is reflexive i.e., for each $a \in A$, $(a, a) \in R$,

(*ii*) R is symmetric i.e., whatever be elements a, b in A such that $(a, b) \in R$, then $(b, a) \in R$, and

(*iii*) R is transitive i.e., whatever be a, b, c in A such that $(a, b) \in R$ and $(b, c) \in R$, then $(a, c) \in R$.

For example, let A denote the set of all triangles in a plane P. Let R denote the set of ordered pairs (t_1, t_2) of triangles t_1, t_2 in the plane P such that triangle t_1 is congruent to t_2 (in the geometrical sense). From elementary geometry, it follows that R is an equivalence relation on A.

DEFINITION 0.3.3. By a **partition of a set** A is meant a division of the set A into mutually disjoint non-empty subsets $A_i \subset A$, $i \in I$, for some indexing set I. In symbols: For each $i \in I$, $A_i \subset A$, $A_i \neq \phi$,

$A_i \cap A_j = \phi$ for $i \neq j$ and $A = \bigcup_{i \in I} A_i$. (The sets A_i are called the sets of the partition).

DEFINITION 0.3.4. Let R be an equivalence relation defined on a set A. For $a \in A$, **the equivalence class of** a is the subset $R_a \subset A$ of all elements $b \in A$ such that $(a, b) \in R$. In symbols:

$$R_a = \{b \in A / (a, b) \in R\}.$$

THEOREM 0.3.5. *An equivalence relation on a set A induces a partition of A. Conversely, every partition of A defines in a natural way an equivalence relation on A.*

Proof. Let R be an equivalence relation on A. For any $a \in A$, $(a, a) \in R$ and hence $a \in R_a$ (condition (i) of definition 0.3.2). In particular R_a is non-empty and $A = \bigcup_{a \in A} R_a$. We claim that if $b \notin R_a$, $R_a \cap R_b = \phi$. For, if $c \in R_a \cap R_b$, $c \in R_a$ and $c \in R_b$; and therefore, $(a, c) \in R$, and (b, c) and hence by symmetry $(c, b) \in R$. Thus by transitivity, $(a, b) \in R$ i.e., $b \in R_a$, a contradiction. In other words, distinct equivalence classes are disjoint and their union is A. This of course means that the distinct equivalence classes of R form a partition of A where for the indexing set I we take the set I of equivalence classes of R.

Conversely, given a partition $\{A_i\}$, $i \in I$ of A, we define a relation R on A by setting $(a, b) \in R$ iff a and b lie in the set A_i of the partition for the same $i \in I$. It is then easy to check that R is an equivalence relation on A whose equivalence classes are the sets A_i of the given partition $\{A_i\}$, $i \in I$. For instance, to verify symmetry, consider $(a, b) \in R$. Then for some $i \in I$, $a, b \in A_i$, hence $b, a \in A_i$ so that $(b, a) \in R$■

EXERCISE 0.3.6. Verify that the relation R above is reflexive and transitive.

Example 0.3.7. On the set **Z** of integers define a relation R by setting $(a, b) \in R$ iff a is congruent to b modulo 5 (in symbols : $a \equiv b \pmod 5$; by this is meant that 5 divides $(a-b)$). It is then an easy matter to check that R is an equivalence relation on **Z**. The 5 distinct equivalence classes of R are:

$$R_0 = \{\ldots, -10, -5, 0, 5, 10, \ldots\},$$
$$R_1 = \{\ldots, -9, -4, 1, 6, 11, \ldots\},$$
$$R_2 = \{\ldots, -8, -3, 2, 7, 12, \ldots\},$$
$$R_3 = \{\ldots, -7, -2, 3, 8, 13, \ldots\}, \text{ and}$$
$$R_4 = \{\ldots, -6, -1, 4, 9, 14, \ldots\}.$$

These are called congruence classes modulo 5. Clearly they form a partition of **Z**. It is further obvious that if we replace 5 by any fixed non-zero integer n, we still have an equivalence relation on **Z**, defined as above (namely, $(a, b) \in R$ iff $n/(a-b)$).