# Graduate Texts in Mathematics

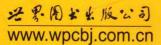
N. Jacobson

# Lectures in Abstract Algebra I

**Basic Concepts** 

抽象代数讲义 第1卷





# Nathan Jacobson

# Lectures in Abstract Algebra

I. Basic Concepts

### Nathan Jacobson

Department of Mathematics Yale University New Haven, Connecticut 06520

# Managing Editor

#### P. R. Halmos

Indiana University Department of Mathematics Swain Hall East Bloomington, Indiana 47401

#### **Editors**

### F. W. Gehring

University of Michigan Department of Mathematics Ann Arbor, Michigan 48104

#### C. C. Moore

University of California at Berkeley Department of Mathematics Berkeley, California 94720

# AMS Subject Classifications 06-01, 12-01, 13-01

Library of Congress Cataloging in Publication Data

Jacobson, Nathan, 1910-

Lectures in abstract algebra.

(Graduate texts in mathematics; 30-32)

Reprint of the 1951-1964 ed. published by Van Nostrand, New York in The University series in higher mathematics.

Bibliography: v. 3, p.

Includes indexes.

CONTENTS: 1. Basic concepts. 2. Linear algebra. 3. Theory of fields and Galois theory.

1. Algebra, Abstract. I. Title. II. Series.

QA162.J3 1975 512'.02 75-15564

#### All rights reserved

No part of this book may be translated or reproduced in any form without written permission from Springer-Verlag.

Reprint from English language edition:

Lectures in Abstract Algebra I

by N. Jacobson

Copyright © 1951, Springer New York

Springer New York is a part of Springer Science+Business Media

All Rights Reserved

This reprint has been authorized by Springer Science & Business Media for distribution in China Mainland only and not for export therefrom.

ISBN 0-387-90181-7 Springer-Verlag New York Heidelberg Berlin ISBN 3-540-90181-7 Springer-Verlag Berlin Heidelberg New York

# Graduate Texts in Mathematics 30

Editorial Board: F.W. Gehring

P. R. Halmos (Managing Editor)

C.C. Moore

# MY WIFE

此为试读,需要完整PDF请访问: www.ertongbook.com

## PREFACE

The present volume is the first of three that will be published under the general title Lectures in Abstract Algebra. These volumes are based on lectures which the author has given during the past ten years at the University of North Carolina, at The Johns Hopkins University, and at Yale University. The general plan of the work is as follows: The present first volume gives an introduction to abstract algebra and gives an account of most of the important algebraic concepts. In a treatment of this type it is impossible to give a comprehensive account of the topics which are introduced. Nevertheless we have tried to go beyond the foundations and elementary properties of the algebraic systems. This has necessitated a certain amount of selection and omission. We feel that even at the present stage a deeper understanding of a few topics is to be preferred to a superficial understanding of many.

The second and third volumes of this work will be more specialized in nature and will attempt to give comprehensive accounts of the topics which they treat. Volume II will bear the title Linear Algebra and will deal with the theory of vector spaces. Volume III, The Theory of Fields and Galois Theory, will be concerned with the algebraic structure of fields and with valuations of fields.

All three volumes have been planned as texts for courses. A great many exercises of varying degrees of difficulty have been included. Some of these perhaps rate stars, but we have felt that the disadvantages of the system of starring difficult exercises outweigh its advantages. A few sections have been starred (notation: \*1) to indicate that these can be omitted without jeopardizing the understanding of subsequent material.

We are indebted to a great many friends for helpful criticisms and encouragement during the course of preparation of this volume. Professors A. H. Clifford, G. Hochschild and R. E. Johnson, Drs. D. T. Finkbeiner and W. H. Mills have read parts of the manuscript and given us useful suggestions for improving it. Drs. Finkbeiner and Mills have assisted with the proofreading. I take this opportunity to offer my sincere thanks to all of these men.

N. J.

New Haven, Conn. January 22, 1951

# **CONTENTS**

# INTRODUCTION: CONCEPTS FROM SET THEORY THE SYSTEM OF NATURAL NUMBERS

ION						PAGE
Operations on sets	٠	•		٠		2
Product sets, mappings	•					3
Equivalence relations			•			4
The natural numbers		•	9.00	٠.		7
The system of integers		٠	•	٠		10
The division process in $I$	• 9			•		12
CHAPTER I: SEMI-GROUPS AND GROUPS						
Definition and examples of semi-groups	•	•	٠	•	•	15
Non-associative binary compositions				•		18
Generalized associative law. Powers		×			•	20
Commutativity						21
Identities and inverses				٠	•	22
Definition and examples of groups				(*)		23
Subgroups	÷		•			24
Isomorphism					٠	26
Transformation groups	÷					27
						28
Cyclic groups. Order of an element						30
Elementary properties of permutations						34
						37
						40
						41
						43
		_				45
						47
	Operations on sets Product sets, mappings Equivalence relations The natural numbers The system of integers The division process in I  CHAPTER I: SEMI-GROUPS AND GROUPS Definition and examples of semi-groups Non-associative binary compositions Generalized associative law. Powers Commutativity Identities and inverses Definition and examples of groups Subgroups Isomorphism Transformation groups Realization of a group as a transformation group Cyclic groups. Order of an element Elementary properties of permutations Coset decompositions of a group Invariant subgroups and factor groups Homomorphism of groups The fundamental theorem of homomorphism for gr Endomorphisms, automorphisms, center of a group	Operations on sets Product sets, mappings Equivalence relations The natural numbers The system of integers The division process in I  CHAPTER 1: SEMI-GROUPS AND GROUPS  Definition and examples of semi-groups Non-associative binary compositions Generalized associative law. Powers Commutativity Identities and inverses Definition and examples of groups Subgroups Isomorphism Transformation groups Realization of a group as a transformation group Cyclic groups. Order of an element Elementary properties of permutations Coset decompositions of a group Invariant subgroups and factor groups Homomorphism of groups The fundamental theorem of homomorphism for group Endomorphisms, automorphisms, center of a group	Operations on sets Product sets, mappings Equivalence relations The natural numbers The system of integers The division process in I  CHAPTER 1: SEMI-GROUPS AND GROUPS  Definition and examples of semi-groups Non-associative binary compositions Generalized associative law. Powers Commutativity Identities and inverses Definition and examples of groups Subgroups Isomorphism Transformation groups Realization of a group as a transformation group Cyclic groups. Order of an element Elementary properties of permutations Coset decompositions of a group Invariant subgroups and factor groups Homomorphism of groups The fundamental theorem of homomorphism for groups Endomorphisms, automorphisms, center of a group	Operations on sets Product sets, mappings Equivalence relations The natural numbers The system of integers The division process in I  CHAPTER 1: SEMI-GROUPS AND GROUPS  Definition and examples of semi-groups Non-associative binary compositions Generalized associative law. Powers Commutativity Identities and inverses Definition and examples of groups Subgroups Isomorphism Transformation groups Realization of a group as a transformation group Cyclic groups. Order of an element Elementary properties of permutations Coset decompositions of a group Invariant subgroups and factor groups Homomorphism of groups The fundamental theorem of homomorphism for groups Endomorphisms, automorphisms, center of a group.	Operations on sets Product sets, mappings Equivalence relations The natural numbers The system of integers The division process in I  CHAPTER 1: SEMI-GROUPS AND GROUPS  Definition and examples of semi-groups Non-associative binary compositions Generalized associative law. Powers Commutativity Identities and inverses Definition and examples of groups Subgroups Isomorphism Transformation groups Realization of a group as a transformation group Cyclic groups. Order of an element Elementary properties of permutations Coset decompositions of a group Invariant subgroups and factor groups Homomorphism of groups The fundamental theorem of homomorphism for groups Endomorphisms, automorphisms, center of a group	Operations on sets Product sets, mappings Equivalence relations The natural numbers The system of integers The division process in I

ix

	CHAFTER II. KINGS, INTEGRAL DOMAINS AND FIELDS	
	TION	PAGE
1.	Definition and examples	49
2.	Types of rings	53
	Quasi-regularity. The circle composition	55
4.	Matrix rings	56
	Quaternions	60
	Subrings generated by a set of elements. Center	63
7.	Ideals, difference rings	64
	Ideals and difference rings for the ring of integers	66
9.	Homomorphism of rings	68
10.	Anti-isomorphism	71
11.	Structure of the additive group of a ring. The charateristic	_
	of a ring	74
12.	Algebra of subgroups of the additive group of a ring. One-	
	sided ideals	75
	The ring of endomorphisms of a commutative group	78
14.	The multiplications of a ring	82
	CHAPTER III: EXTENSIONS OF RINGS AND FIELDS	
	T-1 10 - 7 1 - 1 - 1 - 1 - 21 - 5 -	0.4
	Imbedding of a ring in a ring with an identity	84 87
	Field of fractions of a commutative integral domain	87 91
	Uniqueness of the field of fractions	92
4.	Polynomial rings	96
٥.	Structure of polynomial rings	97
7	Properties of the ring $\mathfrak{A}[x]$	100
7.	Simple extensions of a field	100
	Structure of any field	103
	The number of roots of a polynomial in a field	104
	Polynomials in several elements	103
	Symmetric polynomials	
12.	Rings of functions	110
	CHAPTER IV: ELEMENTARY FACTORIZATION THEORY	
1.	Factors, associates, irreducible elements	114
	Gaussian semi-groups	
3.	Greatest common divisors	
	Principal ideal domains	

CONTENTS	xi

SECT		PAGE
	Euclidean domains	122
6.	Polynomial extensions of Gaussian domains	124
	CHAPTER V: GROUPS WITH OPERATORS	
	Definition and examples of groups with operators	128
	M-subgroups, M-factor groups and M-homomorphisms	130
	The fundamental theorem of homomorphism for M-groups .	132
4.	The correspondence between M-subgroups determined by a	
	homomorphism	133
	The isomorphism theorems for M-groups	135
	Schreier's theorem	137
	Simple groups and the Jordan-Hölder theorem	139
8.	The chain conditions	142
	Direct products	144
10.	Direct products of subgroups	145
	Projections	149
12.	Decomposition into indecomposable groups	152
13.	The Krull-Schmidt theorem	154
14.	Infinite direct products	159
	CHAPTER VI: MODULES AND IDEALS	
1	Definitions	162
	Fundamental concepts	164
	Generators. Unitary modules	166
J.	The chain conditions	168
	The Hilbert basis theorem	170
	Noetherian rings. Prime and primary ideals	
	Representation of an ideal as intersection of primary ideals	
	Uniqueness theorems	
	Integral dependence	
10.	Integers of quadratic fields	101
	CHAPTER VII: LATTICES	
		p 8000000
	Partially ordered sets	
	Lattices	
	Modular lattices	193
4.	Schreier's theorem. The chain conditions	197

ECT	DN PAGE
5.	Decomposition theory for lattices with ascending chain con-
	dition
6.	Independence
	Complemented modular lattices
	Boolean algebras
	Index

# Introduction

# CONCEPTS FROM SET THEORY THE SYSTEM OF NATURAL NUMBERS

The purpose of this volume is to give an introduction to the basic algebraic systems: groups, rings, fields, groups with operators, modules, and lattices. The study of these systems encompasses a major portion of classical algebra. Thus, in a sense our subject matter is old. However, the axiomatic development which we have adopted here is comparatively new. A beginner may find our account at times uncomfortably abstract since we do not tie ourselves down to the study of one particular system (e.g., the system of real numbers). Supplementary study of the exercises and examples should help to overcome this difficulty. At any rate, it will be obvious that much time is saved and a clearer insight is eventually achieved by the present method.

The basic ingredients of the systems that we shall study are sets and mappings of these sets. Notions from set theory will occur constantly in our discussion. Hence, it will be useful to consider briefly in the first part of this Introduction some of these ideas before embarking on the study of the algebraic systems. We shall not attempt to be completely rigorous in our sketchy account of the elements of set theory. The reader should consult the standard texts for systematic and detailed accounts of this subject. Of these we single out Bourbaki's *Théorie des Ensembles* as particularly appropriate for our purposes.

The second part of this Introduction sketches a treatment of the system P of natural numbers as an abstract mathematical system. The starting point here is a set and a mapping in the set (the successor mapping) that is assumed to satisfy Peano's axioms. By means of this, one can introduce addition, multiplication, and the relation of order in P. We shall also define the system I of integers as a certain extension of the system P of natural numbers. Finally, we shall derive one or two arithmetic facts concerning I that are indispensable in elementary group theory. Full accounts of the foundations of the system of natural numbers are available in Landau's Grundlagen der Analysis and in Graves' Theory of Functions of Real Variables.

1. Operations on sets. We begin our discussion with a brief survey of the fundamental concepts of the theory of sets.

Let S be an arbitrary set (or collection) of elements  $a, b, c, \cdots$ . The nature of the elements is immaterial to us. We indicate the fact that an element a is in S by writing  $a \in S$  or  $S \ni a$ . If A and B are two subsets of S, then we say that A is contained in B or B contains A (notation:  $A \subseteq B$  or  $B \supseteq A$ ) if every a in A is also in B. The statement A = B thus means that  $A \supseteq B$  and  $B \supseteq A$ . Also we write  $A \supset B$  if  $A \supseteq B$  but  $B \ne A$ . In this case A is said to contain B properly, or B is a proper subset of A.

If A and B are any two subsets of S, the collection of elements c such that  $c \in A$  and  $c \in B$  is called the *intersection*  $A \cap B$  of A and B. More generally we can define the intersection of any finite number of sets, and still more generally, if  $\{A\}$  denotes any collection of subsets of S, then we define the intersection  $\cap A$  as the set of elements c such that  $c \in A$  for every A in  $\{A\}$ . If the collection  $\{A\}$  is finite, so that its members can be denoted as

 $A_1, A_2, \dots, A_n$ , then the intersection can be written as  $\bigcap_{i=1}^{n} A_i$  or as  $A_1 \cap A_2 \cap \dots \cap A_n$ .

Similar remarks apply to logical sums of subsets of S. The logical sum or union of the collection  $\{A\}$  of subsets A is the set of elements u such that  $u \in A$  for at least one A in  $\{A\}$ . We denote this set as  $\bigcup A$  or, if the collection is finite, as  $\bigcup A$  or

 $A_1 \cup A_2 \cup \cdots \cup A_n$ .

The collection of all subsets of the given set S will be denoted as P(S). In order to avoid considering exceptional cases it is necessary to count the whole set S and the vacuous set as mem-

bers of P(S). One may regard the latter as a zero element that is adjoined to the collection of "real" subsets. We use the notation  $\emptyset$  for the vacuous set. The convenience of introducing this set is illustrated in the use of the equation  $A \cap B = \emptyset$  to indicate that A and B are non-overlapping, that is, they have no elements in common. If S is a finite set of n elements, then P(S) consists of  $\emptyset$ , n sets containing single elements,  $\cdots$ ,  $\binom{n}{i} = \frac{n(n-1)\cdots(n-i+1)}{1\cdot 2\cdots i}$  sets containing i elements, and

so on. Hence the total number of elements in P(S) is

$$1 + \binom{n}{1} + \binom{n}{2} + \dots + \binom{n}{n} = (1+1)^n = 2^n.$$

2. Product sets, mappings. If S and T are arbitrary sets, we define the product set  $S \times T$  to be the collection of pairs (s,t), s in S, t in T. The two sets S and T need not be distinct. In the product  $S \times T$  the elements (s,t) and (s',t') are regarded as equal if and only if s = s' and t = t'. Thus if S consists of the m elements  $s_1, s_2, \dots, s_m$  and T consists of the n elements  $t_1, t_2, \dots, t_n$ , then  $S \times T$  consists of the mn elements  $(s_i,t_j)$ . More generally, if  $S_1, S_2, \dots, S_r$  are any sets, then  $\Pi S_i$  or  $S_1 \times S_2 \times \dots \times S_r$  is defined to be the collection of r-tuples  $(s_1, s_2, \dots, s_r)$  where the ith component  $s_i$  is in the set  $S_i$ .

A (single-valued) mapping  $\alpha$  of a set S into a set T is a correspondence that associates with each  $s \in S$  a single element  $t \in T$ . It is customary in elementary mathematics to write the image in T of s as  $\alpha(s)$ . We shall find it more convenient to denote this element as  $s\alpha$  or  $s^{\alpha}$ . With the mapping  $\alpha$  we can associate the subset of  $S \times T$  consisting of the points  $(s,s\alpha)$ . We shall call this set the graph of  $\alpha$ . Its characteristic properties are:

- 1. If s is any element of S, then there is an element of the form (s,t) in the graph.
  - 2. If  $(s,t_1)$  and  $(s,t_2)$  are in the graph, then  $t_1 = t_2$ .

A mapping  $\alpha$  is said to be a mapping of S onto T if every  $t \in T$  occurs as an image of some  $s \in S$ . In any case we shall denote the image set (= set of image elements) of S under  $\alpha$  as  $S\alpha$  or  $S^{\alpha}$ . A mapping  $\alpha$  of S into T is said to be 1-1 if  $s_1\alpha = s_2\alpha$  holds only

if  $s_1 = s_2$ , that is, distinct points of S have distinct images. Suppose now that  $\alpha$  is a 1-1 mapping of S onto T. Then if t is any element in T, there exists a unique element s in S such that  $s\alpha = t$ . Hence if we associate with t this element s we obtain a mapping of T into S. We shall call this mapping the inverse mapping  $\alpha^{-1}$  of  $\alpha$ . It is immediate that  $\alpha^{-1}$  is 1-1 of T onto S.

It is natural to regard two mappings  $\alpha$  and  $\beta$  of S into T as equal if and only if  $s\alpha = s\beta$  for all s in S. This means that  $\alpha = \beta$  if and only if these mappings have the same graph.

Let  $\alpha$  be a mapping of S into T and let  $\beta$  be a mapping of T into a third set U. The mapping that sends the element s of S into the element  $(s\alpha)\beta$  of U is called the *resultant* or *product* of  $\alpha$  and  $\beta$ . We denote this mapping as  $\alpha\beta$ , so that by definition  $s(\alpha\beta) = (s\alpha)\beta$ .

Mappings of a set into itself will be called *transformations* of the set. Among these are included the *identity mapping* or *transformation* that leaves every element of S fixed. We denote this mapping as 1 (or  $1_S$  if this is necessary). If  $\alpha$  is any transformation of S, it is clear that  $\alpha 1 = \alpha = 1\alpha$ .

If  $\alpha$  is a 1-1 mapping of S onto T and  $\alpha^{-1}$  is its inverse, then  $\alpha\alpha^{-1}=1_S$  and  $\alpha^{-1}\alpha=1_T$ . The following useful converse of this remark is also easy to verify: If  $\alpha$  is a mapping of S into T, and  $\beta$  is a mapping of T into S such that  $\alpha\beta=1_S$  and  $\beta\alpha=1_T$ , then  $\alpha$  and  $\beta$  are 1-1, onto mappings and  $\beta=\alpha^{-1}$ .

The concept of a product set permits us to define the notion of a function of two or more variables. Thus a function of two variables in S with values in T is a mapping of  $S \times S$  into T. More generally we can consider mappings of  $S_1 \times S_2$  into T. Of particular interest for us will be the mappings of  $S \times S$  into S. We shall call such mappings binary compositions in the set S.

3. Equivalence relations. We say that a relation R is defined in a set S if, for any ordered pair of elements (a,b), a,b in S, we can determine whether or not a is in the given relation to b. More precisely, a relation can be defined as a mapping of the set  $S \times S$  into a set consisting of two elements. We can take these to be the words "yes" and "no." Then if  $(a,b) \rightarrow yes$  (that is, is mapped into "yes"), we say that a is in the given relation to b.

In this case we write a R b. If  $(a,b) \rightarrow no$ , then we say that a is not in the given relation to b and we write  $a \not R b$ .

A relation  $\sim$  (in place of R) is called an equivalence relation if it satisfies the following conditions:

- 1.  $a \sim a$  (reflexive property).
- 2.  $a \sim b$  implies  $b \sim a$  (symmetric property).
- 3.  $a \sim b$  and  $b \sim c$  imply that  $a \sim c$  (transitive property).

An example of an equivalence relation is obtained by letting S be the collection of points in the plane and by defining  $a \sim b$  if a and b lie on the same horizontal line. If  $a \in S$ , it is clear that the collection  $\bar{a}$  of elements  $b \sim a$  is the horizontal line through the point a. The collection of these lines gives a decomposition of the set S into non-overlapping subsets. We shall now show that this phenomenon is typical of equivalence relations.

Let S be any set and let  $\sim$  be any equivalence relation in S. If  $a \in S$ , let  $\bar{a}$  denote the subset of S of elements b such that  $b \sim a$ . By 1,  $a \in \bar{a}$  and by 2 and 3, if  $b_1$  and  $b_2 \in \bar{a}$ , then  $b_1 \sim b_2$ . Hence  $\bar{a}$  is a collection of equivalent elements. Moreover,  $\bar{a}$  is a maximal collection of this type; for, if c is any element equivalent to some b in  $\bar{a}$ , then  $c \in \bar{a}$ . We call  $\bar{a}$  the equivalence class determined by (or containing) the element a. If  $b \in \bar{a}$ , then  $\bar{b} \subseteq \bar{a}$ ; hence by the maximality of b,  $\bar{b} = \bar{a}$ . This implies the important conclusion that any two equivalence classes are either identical or they have a vacuous intersection. Hence, the collection of distinct equivalence classes gives a decomposition of the set S into non-intersecting sets.

Conversely, suppose that a given set S is decomposed in any way into sets A, B,  $\cdots$  no two of which overlap. Then we can define an equivalence relation in S by specifying that  $a \sim b$  if the sets A, B containing a and b respectively are identical. It is clear that this relation has the required properties. Also, obviously, the equivalence classes determined by this relation are just the given sets A, B,  $\cdots$ .

The collection  $\overline{S}$  of equivalence classes defined by an equivalence relation in S is called the *quotient set* of S relative to the given relation. It should be emphasized that  $\overline{S}$  is not a subset of S but rather a subset of the collection P(S) of subsets of S.

There is an intimate connection between equivalence relations and mappings. In the first place, if S is a set and  $\overline{S}$  is its quotient set relative to an equivalence relation, then we have a natural mapping  $\nu$  of S onto  $\overline{S}$ . This is defined by the rule that the element a of S is sent into the equivalence class  $\overline{a}$  determined by a. Evidently this mapping is a mapping onto  $\overline{S}$ .

On the other hand, suppose that we are given any mapping  $\alpha$  of the set S onto a second set T. Then we can use  $\alpha$  to define an equivalence relation. Our rule here is that  $a \sim b$  if  $a\alpha = b\alpha$ . Clearly this satisfies the axioms 1, 2 and 3. If a' is an element of T and a is an element of S such that  $a\alpha = a'$ , then the equivalence class  $\bar{a}$  is just the set of elements of S that are mapped into a'. We call this set the inverse image of a' and we denote it as  $\alpha^{-1}(a')$ .

Suppose now that  $\sim$  is any equivalence relation in S with quotient set  $\bar{S}$ . Let  $\alpha$  be a mapping of S onto T which has the property that the inverse images  $\alpha^{-1}(a')$  are logical sums of sets belonging to  $\bar{S}$ . This is equivalent to saying that any set belonging to  $\bar{S}$  is contained in some inverse image  $\alpha^{-1}(a')$ . Hence it means simply that, if a and b are any two elements of S such that  $a \sim b$ , then  $a\alpha = b\alpha$ . It is therefore clear that the rule  $\bar{a} \to a\alpha$  defines a mapping of  $\bar{S}$  onto T. We denote this mapping as  $\bar{\alpha}$  and call it the mapping of  $\bar{S}$  induced by the given mapping  $\alpha$ . The defining equation  $\bar{a}\bar{\alpha} = a\alpha$  shows that the original mapping is the resultant of the natural mapping  $a \to \bar{a}$  and the mapping  $\bar{\alpha}$ , that is,  $\alpha = \nu \bar{\alpha}$ .

This type of factorization of mappings will play an important role in the sequel. It is particularly useful when the set of inverse images  $\alpha^{-1}(a')$  coincides with  $\bar{S}$ ; for, in this case, the mapping  $\bar{\alpha}$  is 1-1. Thus if  $\bar{a}\bar{\alpha} = b\bar{\alpha}$ , then  $a\alpha = b\alpha$  and  $a \sim b$ . Hence  $\bar{a} = \bar{b}$ . Thus we obtain here a factorization  $\alpha = \nu\bar{\alpha}$  where  $\bar{\alpha}$  is 1-1 onto T and  $\nu$  is the natural mapping.

As an illustration of our discussion we consider the perpendicular projection  $\pi_x$  of the plane S onto the x-axis T. Here a point a is sent into the foot of the perpendicular joining it to the x-axis. If a' is a point on the x-axis,  $\pi_x^{-1}(a')$  is the set of points on the vertical line through a'. The set of inverse images is the collection of these vertical lines, and the induced mapping  $\bar{\pi}_x$