Lectures in Abstract Algebra

N. JACOBSON

VOL. I

BASIC CONCEPTS

Lectures in Abstract Algebra

by

NATHAN JACOBSON

Professor of Mathematics
Yale University

VOLUME I—BASIC CONCEPTS

1951

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

CHAPTER I: SEMI-GROUPS AND GROUPS

CHAPTER II: RINGS, INTEGRAL DOMAINS AND FIELDS

CHAPTER III: EXTENSIONS OF RINGS AND FIELDS

CHAPTER IV: ELEMENTARY FACTORIZATION THEORY

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 $a \varepsilon S$ 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 $B \neq A$. 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 $c \varepsilon A$ and $c \varepsilon B$ 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 $c \varepsilon A$ for every A in $\{A\}$. If the collection $\{A\}$ is finite, so that its members can be denoted as $A_1, A_2, \cdots, A_n$, then the intersection can be written as $\bigcap_1^n A_i$ or as $A_1 \cap A_2 \cap \cdots \cap A_n$.

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 $u \varepsilon A$ for at least one A in $\{A\}$. We denote this set as $\cup A$ or, if the collection is finite, as $\bigcup_1^n A_i$ 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 members 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 $\varnothing$ for the vacuous set. The convenience of introducing this set is illustrated in the use of the equation $A \cap B = \varnothing$ 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 $\varnothing$, n sets containing single elements, $\cdots$, $\binom{n}{i} = \dfrac{n(n-1)\cdots(n-i+1)}{1\cdot 2\cdots i}$ sets containing i elements, and so on. Hence the total number of elements in $P(S)$ is

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

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 $s_1, s_2, \cdots, s_m$ and T consists of the n elements $t_1, t_2, \cdots, t_n$, then $S \times T$ consists of the mn elements (s_i,t_j). More generally, if $S_1, S_2, \cdots, S_r$ are any sets, then ΠS_i or $S_1 \times S_2 \times \cdots \times S_r$ is defined to be the collection of r-tuples $(s_1, s_2, \cdots, s_r)$ where the ith component s_i is in the set S_i.

A (single-valued) *mapping* α 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^α. With the mapping α we can associate the subset of $S \times T$ consisting of the points $(s,s\alpha)$. We shall call this set the *graph* of α. 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 α 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 α as $S\alpha$ or S^α. A mapping α 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 α 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* α^{-1} of α. It is immediate that α^{-1} is 1–1 of T onto S.

It is natural to regard two mappings α and β 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 α be a mapping of S into T and let β 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 α and β. 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 α is any transformation of S, it is clear that $\alpha 1 = \alpha = 1\alpha$.

If α is a 1–1 mapping of S onto T and α^{-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 α is a mapping of S into T, and β is a mapping of T into S such that $\alpha\beta = 1_S$ and $\beta\alpha = 1_T$, then α and β 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 $(a,b) \to$ 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 $a \varepsilon S$, 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 $a \varepsilon S$, let $\bar{a}$ denote the subset of S of elements b such that $b \sim a$. By 1, $a \varepsilon \bar{a}$ and by 2 and 3, if b_1 and $b_2 \varepsilon \bar{a}$, 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 $c \varepsilon \bar{a}$. We call $\bar{a}$ the *equivalence class* determined by (or containing) the element a. If $b \varepsilon \bar{a}$, then $\bar{b} \subseteq \bar{a}$; hence by the maximality of $\bar{b}$, $\bar{b} = \bar{a}$. 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 $\bar{S}$ 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 $\bar{S}$ 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 $\bar{S}$ is its quotient set relative to an equivalence relation, then we have a natural mapping ν of S onto $\bar{S}$. This is defined by the rule that the element a of S is sent into the equivalence class $\bar{a}$ determined by a. Evidently this mapping is a mapping onto $\bar{S}$.

On the other hand, suppose that we are given any mapping α of the set S onto a second set T. Then we can use α 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 α 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 $a'\alpha^{-1}$. 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 $\bar{a} \rightarrow a\alpha$ 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 α. The defining equation $\bar{a}\bar{\alpha} = a\alpha$ shows that the original mapping is the resultant of the natural mapping $a \rightarrow \bar{a}$ 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 $\bar{a}\bar{\alpha} = \bar{b}\bar{\alpha}$, 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 ν is the natural mapping.

As an illustration of our discussion we consider the perpendicular projection π_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 $\bar{\pi}_x$

sends a vertical line into its intersection with the x-axis. Clearly this mapping is 1–1, and $\pi_x = \nu\bar{\pi}_x$ where ν is the natural mapping of a point into the vertical line containing it.

4. The natural numbers. The system of natural numbers 1, 2, 3, $\cdots$ is fundamental in algebra in two respects. In the first place, it serves as a starting point for constructing examples of more elaborate systems. Thus we shall use this system to construct the system of integers, the system of rational numbers, of residue classes modulo an integer, etc. In the second place, in studying algebraic systems, functions or mappings of the set of natural numbers play an important role. For example, in a system in which an associative multiplication is defined, the powers a^n of a fixed a determine a function or mapping $n \to a^n$ of the set of natural numbers.

We shall begin with the following assumptions (essentially Peano's axioms) concerning the set P of natural numbers.

1. P is not vacuous.
2. There exists a 1–1 mapping $a \to a^+$ of P into itself. (a^+ is the immediate successor of a.)
3. The set of images under the successor mapping is a proper subset of P.
4. Any subset of P that contains an element that is not a successor and that contains the successor of every element in the set coincides with P. This is called the *axiom of induction.*

All the properties that we shall state concerning P are consequences of these axioms. By 3 and 4 any two elements of P that are not successors are equal. As usual, we denote the unique non-successor as 1. Also we set $1^+ = 2$, $2^+ = 3$, etc.

Property 4 is the basis of proofs by the *first principle of induction.* This can be stated as follows: Suppose that for each natural number n there is associated a statement $E(n)$. Suppose that $E(1)$ is true and that $E(r^+)$ is true whenever $E(r)$ is true. Then $E(n)$ is true for all n. This follows directly from 4. Thus let S be the set of natural numbers s for which $E(s)$ is true. This set contains 1 and it contains r^+ for every $r \varepsilon S$. Hence $S = P$ and this means that $E(n)$ is true for all n in P.

EXERCISE

1. Prove that $n^+ \neq n$ for every n.

Addition of natural numbers is defined to be a binary composition in P such that the value $x + y$ for the pair x,y satisfies

(a) $$1 + y = y^+$$

(b) $$x^+ + y = (x + y)^+.$$

It can be shown that such a function exists and is unique. Moreover, one has the following basic properties:

A1 $x + (y + z) = (x + y) + z$ (associative law)

A2 $x + y = y + x$ (commutative law)

A3 $x + z = y + z$ implies that $x = y$ (cancellation law).

The proofs of these results and the ones on multiplication and order that follow will be omitted. These can be found in the above-mentioned texts.

Multiplication in P is a binary composition satisfying

(a) $$1y = y$$

(b) $$x^+y = xy + y.$$

Such a composition exists, is unique, and has the usual properties:

M1 $x(yz) = (xy)z$

M2 $xy = yx$

M3 $xz = yz$ implies that $x = y$.

Also we have the following fundamental rule connecting addition and multiplication

D $x(y + z) = xy + xz$ (distributive law).

The third fundamental concept in the system P is that of *order*. This can be defined in terms of addition by stating that a is greater than b ($a > b$ or $b < a$) if the equation $a = b + x$

has a solution for x in P. The following are the basic properties of this relation:

O1 $x > y$ excludes $x \leq y$ (asymmetry)

O2 $x > y$ and $y > z$ imply $x > z$ (transitivity)

O3 For any ordered pair (x,y) one and only one of the following holds: $x > y$, $x = y$, $x < y$ (trichotomy). (Note that this implies O1. We include both of these since one is often interested in systems in which O1 and O2 hold but not O3.)

O4 In any non-vacuous set of natural numbers there is a least number, that is, a number l of the set such that $l \leq s$ for all s in the set.

Proof of O4. Let S be the given set and M the set of natural numbers m that satisfy $m \leq s$ for every $s \varepsilon S$. 1 is in M. If s is a particular element in S, then $s^+ > s$ and hence $s^+ \notin M$. Hence $M \neq P$. By the principle of induction there exists a natural number l such that $l \varepsilon M$ but $l^+ \notin M$. Then l is the required number; for $l \leq s$ for every s and $l \varepsilon M$ since otherwise $l < s$ for every s in S. Then $l^+ \leq s$ contradicting $l^+ \notin M$.

The property O4 is called the *well-ordering* property of P. It is the basis of the following *second principle of induction*. Suppose that for each $n \varepsilon P$ we have a statement $E(n)$. Suppose that it is known that $E(r)$ is true for a particular r if $E(s)$ is true for all $s < r$. (This implies that it is known that $E(1)$ is true.) Then $E(n)$ is true for all n. To prove this let F be the set of elements r such that $E(r)$ is not true. If F is not vacuous, let t be its least element. Then $E(t)$ is not true but $E(s)$ is true for all $s < t$. This contradicts our assumption. Hence F is vacuous and $E(n)$ is true for all n.

The main relations between order and addition, and order and multiplication are given in the following statements:

OA $a > b$ implies and is implied by $a + c > b + c$.

OM $a > b$ implies and is implied by $ac > bc$.