FUNDAMENTAL CONCEPTS OF ALGEBRA

CHEVALLEY

FUNDAMENTAL CONCEPTS OF
ALGEBRA

By

CLAUDE CHEVALLEY

Columbia University, New York

1956

ACADEMIC PRESS INC • PUBLISHERS • NEW YORK

Preface

Algebra is not only a part of mathematics; it also plays within mathematics the role which mathematics itself played for a long time with respect to physics. What does the algebraist have to offer to other mathematicians? Occasionally, the solution of a specific problem; but mostly a language in which to express mathematical facts and a variety of patterns of reasoning, put in a standard form. Algebra is not an end in itself; it has to listen to outside demands issued from various parts of mathematics. This situation is of great benefit to algebra: for, a science, or a part of a science, which exists in view of its own problems only is always in danger of falling into a peaceful slumber and from there into a quiet death. But, in order to take full advantage of this state of affairs, the algebraist must have sensitive ears and the ability to derive profit from what he perceives is going on outside his own domain. Mathematics is changing constantly, and algebra must reflect these changes if it wants to stay alive. This explains the fact that algebra is one of the most rapidly changing parts of mathematics: it is sensitive not only to what happens inside its own boundaries, but also to the trends which originate in all other branches of mathematics.

This book represents an attempt to adapt the teaching of algebra to at least a part of what present day mathematics requires. The most important new demands on algebra come from topology, analysis, and algebraic geometry. These demands are of various kinds; but to all of them the general notion of a module seems to be absolutely essential. This is why the theory of modules occupies such an important place in this book. The concept of a module unites and generalizes those of an additive group and of a vector space; it differs from them by the generality which is allowed for the domain of operators, which may be an arbitrary ring instead of the ring of integers (in additive groups) or a field (in vector spaces). This generality is not there for its own merits, but because it is actually needed in many cases. The operations from the general theory of modules which are considered here are essentially the construction of the group of linear mappings of a module into another one and the construction of the tensor product of two modules. These concepts are not, by far, the only useful ones; but we believe that they contain "what everybody must know" from the theory of modules. The last part of the book is concerned with the theory of algebras and mostly of exterior algebras; the latter have become

essential to analysts because of the frequent use they make of the calculus of differential forms.

We are far from even hinting that this book represents a complete survey of those parts of algebra whose knowledge is essential to contemporary mathematicians; the most glaring lacuna is that of field theory, which is not touched on in this book. The principle which has presided over our choice of material is that it is better to acquire a complete familiarity with a few fundamental notions than to have a superficial knowledge of many. The contents of this book (with a few omissions) have been taught by the author in a one year first graduate course in algebra; we think that it would be impossible to cram any more matter into the program of such a course without destroying its usefulness. The presentation of the material will perhaps incur the reproach of being too dogmatic in its methods. To this possible objection, we would like to make two answers. Firstly that what the student may learn here is not designed to help him with problems he has already met but with those he will have to cope with in the future; it is therefore impossible to motivate the definitions and theorems by applications of which the reader does not know the existence as yet. Secondly, that one of the important pedagogical problems which a teacher of beginners in mathematics has to solve is to impart to his students the technique of rigorous mathematical reasoning; this is an exercise in rectitude of thought, of which it would be futile to disguise the austerity.

PARIS, JUNE 1956. CLAUDE CHEVALLEY.

LIBRARY OF CONGRESS CATALOG CARD NUMBER:
56-8682

PRINTED IN UNITED STATES OF AMERICA

Contents

Preface V

Prerequisite knowledge and terminological conventions 1

CHAPTER I. **Monoids** 3
1. Definition of a monoid 3
2. Submonoids. Generators 8
3. Homomorphisms 10
4. Quotient monoids 13
5. Products 15
6. Free monoids 18
Exercises 22

CHAPTER II. **Groups** 25
1. Definition of a group 25
2. Subgroups 27
3. Homomorphisms. Quotient groups 29
4. Groups operating on a set 35
5. Products of groups 39
6. Free groups 40
Exercises 43

CHAPTER III. **Rings and modules** 49
1. Rings 49
2. Field of quotients 52
3. Modules 54
4. Submodules 56
5. Linear mappings 63
6. Products 69
7. Uniqueness theorems for semi-simple modules 71
8. Tensor products of modules 74
9. Free modules. Bases 80
10. Multilinear mappings 83
11. Transfer of basic rings 97
12. Vector spaces 102
13. Vector spaces in duality 106
14. The rank of a linear mapping 111
15. Matrices 112
16. Systems of linear equations 123
17. Graded modules 124
Exercises 128

CHAPTER IV. **Algebras** 137
1. Definition 137
2. Subalgebras 138

3. Homomorphisms 139
4. Products 140
5. Free algebra 141
Exercises 143

CHAPTER V. **Associative algebras** 145
1. Definitions 145
2. Graded algebras 149
3. Tensor algebras 151
4. Tensor products of graded algebras 154
5. Anticommutative algebras 158
6. Derivations 162
7. Exterior algebras 165
8. Grassmann algebras 170
9. The determinant of a matrix 176
10. Some applications of determinants 182
11. Existence of certain derivations 187
12. The trace of a matrix 192
13. Alternating multilinear mappings 193
14. The Pfaffian of an alternating bilinear form 194
15. Exterior algebras on vector spaces 200
16. Transfer of the basic ring 204
17. Commutative tensor products 211
18. Symmetric algebras 213
19. Polynomial algebras 221
Exercises 228

Index 238

Prerequisite Knowledge and Terminological Conventions

The reader will be assumed to be familiar with the general principles of set theory, including Zorn's lemma, which will be used in the following form. Let E be a set and S a set of subsets of E. Assume that for any subset S' of S with the property that, for any two sets X and Y belonging to S', one is contained in the other, there exists a set in S which contains all sets in S'; then every set in S is contained in some maximal set X of S (i. e. in a set X such that the only set in S which contains X is X itself). From the theory of cardinals, we require the following results: to every set I there is associated an object card I, in such a way that a necessary and sufficient condition for I and I' to be equipotent is that card I = card I'; there is an order relation among the cardinals such that card I $\leqslant$ card I' if and only if I is equipotent to a subset of I'; if to every element i of an infinite set I there is associated a finite subset F_i of a set I', and if every element of I' belongs to at least one of the sets F_i, then card $I' \leqslant$ card I. A mapping f of a set A into a set B is called injective if the condition $a \neq a'$ (where a, a' are in A) implies $f(a) \neq f(a')$; f is called surjective if, for any b in B, there exists at least one a in A such that $f(a) = b$; a mapping which is both injective and surjective is called bijective. An injective (resp.: surjective, bijective) mapping is also called an injection (resp.: surjection, bijection). A mapping of a set I into a set A is also called a family of elements of A indexed by I; if this terminology is used, then the image under the mapping of an element i is generally denoted by f_i (instead of the usual notation $f(i)$); the mapping itself is often denoted by $(f_i)_{i \in I}$.

The set of all integers (positive, null or negative) will always be denoted by $\underline{Z}$. If m is an integer > 0, the factor group $\underline{Z}/m\underline{Z}$ (to be defined in chapter II) will be denoted by $\underline{Z}_m$. A family of elements of a set A which is indexed by the set of integers > 0 will be called a sequence of elements of A; a family of elements of A which is indexed by the set of all integers > 0 which are at most equal to an integer n will be called a finite sequence (of length n) of elements of A. Such a sequence will often be denoted by $(a_i)_{1 \leqslant i \leqslant n}$ or by $(a_1, \cdots, a_n)$. The elements a_i are called the terms of the sequence.

The formula $a \in A$ will mean that a is an element of the set A. The empty set will be denoted by $\emptyset$. If a is an object, then the set whose unique element

is a is denoted by $\{ a \}$. If $(a_1, \cdots, a_n)$ is a finite sequence, the set whose elements are $a_1, \cdots, a_n$ will be denoted by $\{ a_1, \cdots, a_n \}$; if a, b are objects, $\{ a, b \}$ denotes the set whose elements are a, b. The notation $A \subset B$ means that every element of A is an element of B; this does not exclude the possibility that $A = B$. If A and B are sets, $A \cup B$ represents the set whose elements are all objects which are elements either of A or of B (the union of A and B); $A \cap B$ represents the set of elements which belong to both A and B (the intersection of A and B). If a, b are objects, the finite sequence of length 2 which maps 1 upon a and 2 upon b is called the pair (a, b). If A and B are sets, the set of all pairs (a, b) such that $a \in A$ and $b \in B$ is called the (*Cartesian*) *product of A and B*, and is denoted by $A \times B$.

Let $(A_i)_{i \in I}$ be a family of sets. The union of these sets (i. e. the set of elements a such that there exists an $i \in I$ for which $a \in A_i$) is denoted by $\bigcup_{i \in I} A_i$. The intersection of the sets A_i (i. e. the set of elements a such that $a \in A_i$ for every $i \in I$) is denoted by $\bigcap_{i \in I} A_i$. The product of the sets A_i (i. e. the set of families $(a_i)_{i \in I}$, indexed by I, such that $a_i \in A_i$ for every $i \in I$) is denoted by $\prod_{i \in I} A_i$. If $(A_1, \cdots, A_n)$ is a finite sequence of sets, the union of the sets A_i is also denoted by $A_1 \cup \cdots \cup A_n$, their intersection by $A_1 \cap \cdots \cap A_n$ and their product by $A_1 \times \cdots \times A_n$.

Let f be a mapping of a set A into a set B. If $X \subset A$, then the set of elements b such that there exists an x such that $x \in X$ and $f(x) = b$ is denoted by $f(X)$. If $(X_i)_{i \in I}$ is a family of subsets of A, then

$$f(\bigcup_{i \in I} X_i) = \bigcup_{i \in I} f(X_i).$$

If Y is a subset of B, the set of elements a such that $a \in A$ and $f(a) \in Y$ is denoted by $f^{-1}(Y)$. If $(Y_i)_{i \in I}$ is a family of subsets of B, then we have

$$f^{-1}(\bigcup_{i \in I} Y_i) = \bigcup_{i \in I} f^{-1}(Y_i) \text{ and } f^{-1}(\bigcap_{i \in I} Y_i) = \bigcap_{i \in I} f^{-1}(Y_i).$$

If g is a mapping of B into a set C, then the mapping of A into C which assigns $g(f(a))$ to every $a \in A$ is denoted by $g \circ f$. If f is a bijection, then the mapping of B into A which maps any element b of B upon the unique element a of A such that $f(a) = b$ is denoted by f^{-1}. If $E(a)$ is an expression involving a letter a and which has a meaning whenever a stands for an element of a set A, then $a \to E(a)$ represents the mapping which assigns to every element a of A the value of the expression $E(a)$. If $(A_i)_{i \in I}$ is a family of sets and j an element of I, then the mapping of $\prod_{i \in I} A_i$ into A_j which assigns a_j to any element $(a_i)_{i \in I}$ of $\prod_{i \in I} A_i$ is called the j-th projection, or, if there is no danger of confusion, the projection on A_j.

CHAPTER I

Monoids

1. Definition of a monoid

An *internal law of composition*, or *law of composition*, on a set A is a mapping of $A \times A$ into A, i. e. a mapping which assigns to every ordered pair (a, b) of elements of A an element c of A, called their *composite*.

We shall have to consider a great variety of laws of composition. However we shall have only three notations for the composite of a and b: either $a + b$, ab, or $a \circ b$. If the composite is denoted by $a + b$, then it is called the sum of a and b, and we say that we have an additive law of composition. If the composite is denoted by ab or $a \circ b$, then it is called the product of a and b, and we say that we have a multiplicative law of composition. However, in the beginning of this discussion, we shall not make any distinction between additive and multiplicative laws of composition; therefore, we shall use the notation $a \tau b$ for a composite, which may be either a sum or a product.

A law of composition τ on the set A is called *associative* if it is true that

$$(a \tau b) \tau c = a \tau (b \tau c)$$

for all a, b, c in A.

EXAMPLES: *a*) A is the set $\underline{Z}$ of integers, and τ stands either for addition or multiplication: τ is then associative.

b) Let S be any set and A the set of all mappings of S into itself, with the law of composition $(f, g) \to f \circ g$ (where $(f \circ g)(x) = f(g(x))$ for any $x \in S$). This law of composition is associative, for if f, g, h are in A, then

$$((f \circ g) \circ h)(x) = (f \circ g)(h(x)) = f(g(h(x)))$$
$$(f \circ (g \circ h))(x) = f((g \circ h)(x)) = f(g(h(x)))$$

for any $x \in S$, which proves our assertion.

c) In the set of integers, subtraction, i. e. the law of composition $(a, b) \to a - b$, is not associative.

An element e is called *a neutral element* for a law of composition τ in A if we have

$$a \tau e = e \tau a = a$$

for all $a \in A$.

EXAMPLES: *a*) In the set of integers, 0 is a neutral element for addition and 1 a neutral element for multiplication.

b) In the law of composition of example *b*) above, the identity mapping e (i. e. the mapping $x \to x$) is a neutral element.

c) We have, for any integer a, $a - 0 = a$ but, in general, $0 - a \neq a$; thus 0 is not a neutral element for subtraction. It is easy to see that there does not exist *any* neutral element for subtraction.

Theorem 1. *If there is a neutral element for a law of composition τ in A, there is only one.*

Assume that e and e' are neutral elements. Then we have $e\tau e' = e'$ but also $e\tau e' = e$, whence $e = e'$.

The neutral element for an additive law of composition is always denoted by 0; the neutral element for a multiplicative law of composition is most often denoted by 1.

A *monoid* is a set A which has a law of composition that is associative and has a neutral element.

In what follows, unless otherwise stated, A shall denote a monoid, in which the law of composition is denoted by τ.

Composite of finite sequences. Let $(a_1, \cdots, a_n)$ be a finite sequence of elements of A; we shall then define the composite, $a_1\tau \cdots \tau a_n$, of this sequence in the following inductive manner. If the sequence is the empty sequence ($n = 0$), then the composite is by definition the neutral element e. If $n > 0$ and if the composites of sequences of less than n terms are already defined, then we define $a_1\tau \cdots \tau a_n$ by

$$a_1\tau \cdots \tau a_n = (a_1\tau \cdots \tau a_{n-1})\tau a_n.$$

EXAMPLES: The composite of a sequence (a) of a single term is this term a. We have $a\tau b\tau c = (a\tau b)\tau c$, $a\tau b\tau c\tau d = (a\tau b\tau c)\tau d = ((a\tau b)\tau c)\tau d$.

For an additive law of composition, the composite of $(a_1, \cdots, a_n)$ is denoted by $\sum_{i=1}^{n} a_i$; for a multiplicative law of composition, by $\prod_{i=1}^{n} a_i$. There are many variations in the notational conventions, with which the reader will familiarize himself by usage. Examples:

$$\sum_{i=6}^{9} a_i = a_6 + a_7 + a_8 + a_9,$$

$$\sum_{i=-3,\, i \text{ odd}}^{5} a_i = a_{-3} + a_{-1} + a_1 + a_3 + a_5, \quad \sum_{i=2}^{0} a_i = 0, \text{ etc.}$$

Theorem 2. (General associativity theorem) *Let $(a_1, \cdots, a_n)$ be a sequence of elements of A. Let $k_1, \cdots, k_h$ be integers such that $1 = k_1 \leqslant \cdots \leqslant k_h \leqslant n$. Let $b_1 = a_1\tau \cdots \tau a_{k_2-1}$, $b_2 = a_{k_2}\tau \cdots \tau a_{k_3-1}$, $\cdots$, $b_h = a_{k_h}\tau \cdots \tau a_n$. Then we have $a_1\tau \cdots \tau a_n = b_1\tau \cdots \tau b_h$.*

EXAMPLES: (case $n = 4$). We have

$$a\tau b\tau c\tau d = a\tau(b\tau c)\tau d = a\tau(b\tau c\tau d) = a\tau b\tau(c\tau d) = (a\tau b)\tau c\tau d = (a\tau b)\tau(c\tau d) = \text{etc.}$$

Proof. We proceed by induction on n. If $n = 0$, then, necessarily, $h = 0$, and both sides are equal to the neutral element. Assume that $n > 0$ and that the theorem is true for sequences of at most $n - 1$ terms.

Case 1. Assume first that $k_h = n$, whence $b_h = a_n$. We have, by definition, $a_1\tau \cdots \tau a_n = (a_1\tau \cdots \tau a_{n-1})\tau a_n$. By the inductive assumption, we have $a_1\tau \cdots \tau a_{n-1} = b_1\tau \cdots \tau b_{h-1}$, whence

$$a_1\tau \cdots \tau a_n = (b_1\tau \cdots \tau b_{h-1})\tau b_h = b_1\tau \cdots \tau b_h.$$

Case 2. Assume now that $k_h < n$. We have $b_1\tau \cdots \tau b_h = (b_1\tau \cdots \tau b_{h-1})\tau b_h$. Let $b'_h = a_{k_h}\tau \cdots \tau a_{n-1}$, whence $b_h = b'_h\tau a_n$. Then we have, using the assumed associativity of the law of composition τ,

$$\begin{aligned} b_1\tau \cdots \tau b_h &= (b_1\tau \cdots \tau b_{h-1})\tau(b'_h\tau a_n) \\ &= ((b_1\tau \cdots \tau b_{h-1})\tau b'_h)\tau a_n = (b_1\tau \cdots \tau b_{h-1}\tau b'_h)\tau a_n. \end{aligned}$$

But we have $a_1\tau \cdots \tau a_{n-1} = b_1\tau \cdots \tau b_{h-1}\tau b'_h$ by our inductive assumption, whence $b_1\tau \cdots \tau b_h = (a_1\tau \cdots \tau a_{n-1})\tau a_n = a_1\tau \cdots \tau a_n$. This concludes the proof.

Consider now the case where $a_1, \cdots, a_n$ are all equal to one and the same element a. Then the composite of the sequence $(a_1, \cdots, a_n)$ is denoted by na if the law of composition is additive, by a^n if the law of composition is multiplicative.

Let m and n be non-negative integers, and a an element of A. If the law of composition is additive, then we have

(1) $\qquad 0a = 0,\ 1a = a,\ (m + n)a = ma + na,\ (mn)a = m(na)$:

if the law of composition is multiplicative, we have

(2) $\qquad a^0 = 1,\ a^1 = a, \qquad a^{m+n} = a^m a^n, \qquad a^{mn} = (a^m)^n.$

These formulas follow easily from the definitions and from the general associativity theorem.

Commutative monoids. The monoid A is called *commutative* or *Abelian* if we have $a\tau b = b\tau a$ for any elements a and b of A.

EXAMPLES: *a*) The set Z of integers is a commutative monoid under both addition and multiplication.

b) Let R be the set of real numbers, and A the set of mappings of R into itself. Denote by f the mapping $x \to x + 1$ and by g the mapping $x \to x^2$. Then $(f \circ g)(x) = x^2 + 1$, $(g \circ f)(x) = x^2 + 2x + 1$; thus, the law of composition $\circ$ in A is not commutative.

Theorem 3. (general commutativity theorem). *Let A be a commutative monoid, $(a_1, \cdots, a_n)$ a finite sequence of elements of A and ϖ any permutation of the set $\{1, \cdots, n\}$. Then we have*

$$a_1 \tau \cdots \tau a_n = a_{\varpi(1)} \tau \cdots \tau a_{\varpi(n)}.$$

EXAMPLES: We have

$$a\tau b\tau c = a\tau c\tau b = b\tau a\tau c = b\tau c\tau a = c\tau a\tau b = c\tau b\tau a.$$

Proof. We proceed by induction on n. There is nothing to prove if $n = 0$. Assume that $n > 0$ and that the statement is true for sequences of $n - 1$ terms.

Case 1. Consider first the case where $\varpi(n) = n$. Then we have, by the inductive assumption, $a_1 \tau \cdots \tau a_{n-1} = a_{\varpi(1)} \tau \cdots \tau a_{\varpi(n-1)}$. Thus,

$$\begin{aligned} a_1 \tau \cdots \tau a_n &= (a_1 \tau \cdots \tau a_{n-1}) \tau a_n = (a_{\varpi(1)} \tau \cdots \tau a_{\varpi(n-1)}) \tau a_{\varpi(n)} \\ &= a_{\varpi(1)} \tau \cdots \tau a_{\varpi(n-1)} \tau a_{\varpi(n)}. \end{aligned}$$

Case 2. Assume now that $\varpi(n) < n$. Let k be the integer such that $\varpi(k) = n$. Then we have

$$a_{\varpi(1)} \tau \cdots \tau a_{\varpi(n)} = (a_{\varpi(1)} \tau \cdots \tau a_{\varpi(k-1)}) \tau (a_{\varpi(k)} \tau (a_{\varpi(k+1)} \tau \cdots \tau a_{\varpi(n)})),$$

and this is equal to

$$(a_{\varpi(1)} \tau \cdots \tau a_{\varpi(k-1)}) \tau ((a_{\varpi(k+1)} \tau \cdots \tau a_{\varpi(n)}) \tau a_{\varpi(k)}) = a_{\varpi'(1)} \tau \cdots \tau a_{\varpi'(n)}$$

where we have set $\varpi'(i) = \varpi(i)$ if $i \leqslant k-1$, $\varpi'(i) = \varpi(i+1)$ if $k \leqslant i \leqslant n-1$, $\varpi'(n) = \varpi(k) = n$. But ϖ' is again a permutation of $\{1, \cdots, n\}$, and, this time, $\varpi'(n) = n$. Thus $a_{\varpi'(1)} \tau \cdots \tau a_{\varpi'(n)} = a_1 \tau \cdots \tau a_n$ by case 1. This complete the proof.

Assume that we have a commutative monoid where the law of composition is additive. Let I be any finite set, and $i \to a_i$ a mapping of I into A. If n is the number of elements of I, let us number these elements by the integers from 1 to n; denote by $i(k)$ the element of I to which we have assigned the number k. Then $(a_{i(1)}, \cdots, a_{i(n)})$ is a finite sequence, and has therefore a sum $\sum_{k=1}^{n} a_{i(k)}$. It follows from the general commutativity theorem that the value of this sum does not depend on the manner in which we have numbered the elements of I; this value is denoted by $\sum_{i \in I} a_i$.

Let I' be a subset of I and assume that $a_i = 0$ for all $i \in I$ not belonging to I'. Then we have $\sum_{i \in I} a_i = \sum_{i \in I'} a_i$ (i. e., in a sum, we may drop any number of terms all equal to 0). For, we may assume that we number I in such a way that the elements of I' come first; assume that $i(1), \cdots, i(m)$

are the elements of I' and $i(m+1), \cdots, i(n)$ the others. Then it is clear that $\sum_{i\in I} a_i = \sum_{i\in I'} a_i + (a_{i(m+1)} + \cdots + a_n)$, and we have only to prove that a sum of terms all equal to 0 has the value 0, which is easily done by induction on the number of terms.

This allows us to extend the notation $\sum_{i\in I} a_i$ to certain cases where the set I may be infinite. In fact, assume that there are only a finite number of elements i of I for which a_i is $\neq 0$. Then I admits at least one *finite* subset I' such that a_i is 0 for all i not in I'; the value of the sum $\sum_{i\in I'} a_i$ does not depend on the choice of the set I' satisfying these conditions. For, let I'' be another set satisfying the same conditions. Then $I' \cup I''$ is again a finite set, and we have $a_i = 0$ for all i in $I' \cup I''$ but not in I', whence $\sum_{i\in I'} a_i = \sum_{i\in I'\cup I''} a_i$, and we see in the same way that

$$\sum_{i\in I''} a_i = \sum_{i\in I'\cup I''} a_i,$$

which proves our assertion. The common value of the sums $\sum_{i\in I'} a_i$ for all sets I' satisfying the stated conditions is denoted by $\sum_{i\in I} a_i$.

Assume that we have subsets J_k of I, indexed by an index k which runs over a certain set K, and which satisfy the following conditions: they are pairwise disjoint, and the union of all of them is the whole of I (this is called a *partition* of I). Then, for each k, the sum $b_k = \sum_{i\in J_k} a_i$ is defined (i. e., it has only a finite number of terms $\neq 0$); moreover, the sum $\sum_{k\in K} b_k$ is defined, and we have the equality

$$\sum_{i\in I} a_i = \sum_{k\in K} b_k.$$

For, let I' be the set of indices $i \in I$ such that $a_i \neq 0$. Then I' is finite, and so, for each $k \in K$, $I' \cap J_k$ is finite, which shows that each sum $\sum_{i\in J_k} a_i$ is defined. Since the sets J_k are mutually disjoint, only a finite number of them can meet the set I' (this number is at most equal to the number of elements of I'). Now, if J_k does not meet I', we have $a_i = 0$ for *all* i in J_k, whence $b_k = 0$. This shows that the sum $\sum_{k\in K} b_k$ is defined. For each k, let $J'_k = J_k \cap I'$; then, by definition, $b_k = \sum_{i\in J'_k} a_i$. Let K' be the set of indices k for which $J'_k \neq \emptyset$; then we have

$$\sum_{k\in K} b_k = \sum_{k\in K'} b_k = \sum_{k\in K'} \left(\sum_{i\in J'_k} a_i\right),$$

and we have reduced the proof to establishing the formula

$$\sum_{i\in I'} a_i = \sum_{k\in K'} \left(\sum_{i\in J'_k} a_i\right)$$

where I' and K' are now finite sets. This is easily accomplished by means of the general associativity theorem.

Let $(a_i)_{i\in I}$ and $(b_i)_{i\in I}$ be families indexed by the same set I and for

which $\Sigma_{i\in I}a_i$ and $\Sigma_{i\in I}b_i$ are defined. Then $\Sigma_{i\in I}(a_i + b_i)$ is defined, and we have

$$\Sigma_{i\in I}(a_i + b_i) = \Sigma_{i\in I}a_i + \Sigma_{i\in I}b_i. \tag{3}$$

For, it is clear that there exists a finite set $I' \subset I$ such that $a_i = b_i = 0$ for all i not in I', whence

$$\Sigma_{i\in I}(a_i + b_i) = \Sigma_{i\in I'}(a_i + b_i),\ \Sigma_{i\in I}a_i = \Sigma_{i\in I'}a_i,\ \Sigma_{i\in I}b_i = \Sigma_{i\in I'}b_i.$$

Thus, we need only prove (3) in the case where I is finite. Let then $i(1), \cdots, i(n)$ be its elements. Let $c_{2j-1} = a_j$, $c_{2j} = b_j$ $(1 \leqslant j \leqslant n)$. Then $\Sigma_{i\in I}(a_i + b_i) = \Sigma_{j=1}^{n}(c_{2j-1} + c_{2j})$. This is equal by the general associativity theorem to $c_1 + \cdots + c_{2n}$, and, by the general commutativity and associativity theorems, to

$$(c_1 + c_3 + \cdots + c_{2n-1}) + (c_2 + c_4 + \cdots + c_{2n}) = \Sigma_{i\in I}a_i + \Sigma_{i\in I}b_i.$$

Similar considerations apply to the case of a commutative monoid A in which the law of composition is multiplicative, and lead to the definition of the symbol $\Pi_{i\in I}a_i$ in the case where there are only a finite number of indices $i \in I$ for which $a_i \neq 1$.

Let A be a commutative additive monoid, n an integer $\geqslant 0$ and a, b elements of A. Then we have

$$n(a + b) = na + nb;$$

this follows immediately from formula (1) above.

Similarly, if A is a commutative multiplicative monoid, then we have $(ab)^n = a^n b^n$.

If A is any monoid, two elements a and b of A are said to *commute with each other* if we have $a \tau b = b \tau a$. For instance, the neutral element commutes with every element of the monoid.

2. Submonoids. Generators

A subset B of a monoid A (in which the law of composition is denoted by τ) is called *stable* if we have $a \tau b \in B$ whenever a and b are in B.

EXAMPLES: In the additive monoid $\underline{Z}$ of integers, the set of integers $\geqslant k$ (where k is any integer) is stable under addition if $k \geqslant 0$ but not if $k < 0$. The set $\{-1, 1\}$ is stable under multiplication, but not under addition. In the set of all mappings of the set of real numbers into itself (with the law of composition $\circ$), the set of all mappings of the form $x \to x^n$ (n an integer $\geqslant 0$) is stable.

If B is stable, the restriction to $B \times B$ of the law of composition τ in A is a law of composition in B, called the *induced law of composition*. If τ is associative, then so is its induced law of composition. If τ admits a neutral element e and $e \in B$, then e is a neutral element for the induced law of composition.

Thus, if we assume that B contains e and is stable, then it constitutes a monoid when equipped with the induced law of composition. In that case, B is called a *submonoid* of A.

If B is a submonoid of A, then it is clear that the composite in A of a finite sequence of elements of B belongs to B and is also the composite of this sequence in B.

Theorem 4. *Let $(B_i)_{i \in I}$ be a family of submonoids of A, I being any (non empty) set of indices. Then the intersection B of all B_i's is a submonoid.*

Since $e \in B_i$ for all i, we have $e \in B$. Let a and b be in B; then, for each i, a and b are in B_i, whence $a \tau b \in B_i$; it follows that $a \tau b \in B$.

Let S be any subset of A. Then S is contained in at least one submonoid of A, viz. A itself. By theorem 4, the intersection B of all submonoids of A containing S is a submonoid; B is the smallest submonoid of A containing S (in the sense that it is contained in any submonoid which contains S). It is called the *submonoid generated by* S.

For instance, if $S = \emptyset$, then B is the submonoid $\{ e \}$ consisting of the neutral element e alone. If $\underline{Z}$ is the monoid of integers under addition, and k any integer, the submonoid generated by the set $\{ k \}$ consists of all elements nk, where n runs over the integers $\geqslant 0$.

Theorem 5. *Let U be any subset of a monoid A. Then the set C of those elements of A which commute with every element of U is a submonoid of A.*

It is clear that C contains the neutral element. Let a, b be elements of C, and u any element of U. Then we have

$$(a \tau b) \tau a = a \tau (b \tau u) = a \tau (u \tau b) = (a \tau u) \tau b = (u \tau a) \tau b = u \tau (a \tau b),$$

which shows that $a \tau b$ commutes with u; C is therefore stable.

Corollary 1. *If all elements of a subset S of A commute with all elements of U, then all elements of the submonoid A' generated by S commute with all elements of U.*

For, we have $S \subset C$ (in the notation of theorem 5), whence $A' \subset C$, since A' is the smallest submonoid containing S.

Corollary 2. *If the elements of a subset S of A commute with each other, then the submonoid A' generated by S is Abelian.*

For, any element of S commutes with any element of A', by corollary 1. Applying corollary 1 again, with A' taking the place of U, we see that any element of A' commutes with any element of A'.

3. Homomorphisms

Let A and B be monoids. A mapping f of A into B is called a *homomorphism* if the following conditions are satisfied:

a) f maps the neutral element e_A of A upon the neutral element e_B of B;

b) if a, b are any elements of A, we have

$$f(a\tau b) = f(a)\tau f(b).$$

(We use the same notation τ for the laws of composition in A and in B; but the reader should remember that it may happen that the law of composition in A is additive and that in B multiplicative.)

EXAMPLES: *a*) Let A be a commutative additive monoid, and let n be an integer $\geqslant 0$; then the mapping $x \to nx$ is a homomorphism of A into itself.

b) Let R be the set of real numbers. Then the mapping $x \to e^x$ is a homomorphism of the additive monoid $\underline{R}$ into the multiplicative monoid $\underline{R}$.

If f is a homomorphism of A into B and g a homomorphism of B into a third monoid C, then $g \circ f$ is a homomorphism of A into C. The proof is obvious.

Let f be a homomorphism of A into B. If $(a_1, \cdots, a_n)$ is a finite sequence of elements of A, then we have

$$f(a_1\tau \cdots \tau a_n) = f(a_1)\tau \cdots \tau f(a_n).$$

This is easily proved by induction on n. In particular, if A and B are both additive, we have $f(na) = nf(a)$; if they are both multiplicative, we have $f(a^n) = (f(a))^n$; if A is additive and B multiplicative, we have $f(na) = (f(a))^n$.

Theorem 6. *Let f be a homomorphism of A into B. Then the image under f of a submonoid of A is a submonoid of B. If S is a subset of A, the image of the submonoid of A generated by S is the submonoid of B generated by $f(S)$. If B' is a submonoid of B, then $f^{-1}(B')$ (the set of elements $x \in A$ such that $f(x) \in B'$) is a submonoid of A.*

The first assertion follows immediately from the definitions. Let B' be a submonoid of B; since $f(e_A) = e_B \in B'$, we have $e_A \in f^{-1}(B')$; if a, b are in $f^{-1}(B')$, then $f(a)$ and $f(b)$ are in B', whence $f(a\tau b) = f(a)\tau f(b) \in B'$ and $a\tau b \in f^{-1}(B')$; this proves that $f^{-1}(B')$ is a submonoid of A. Let S be a subset of A and A' the submonoid generated by S. Then $f(A')$ is a submonoid of B and contains $f(S)$. Let B' be any submonoid of B containing $f(S)$; then $f^{-1}(B')$ is a submonoid of A and obviously contains S. Since A' is the *smallest* submonoid of A containing S, we have $A' \subset f^{-1}(B')$, which means that