# ON THE THEORY OF CLUSTERS

BY
R. A. GOOD

## INTRODUCTION

Modern algebra treats many varieties of algebraic systems, each subject to its own peculiar set of postulates. Abstracted from the familiar rational number system is the field, a system conveniently described in terms of two basic operations and satisfying a long list of axiomatic properties. As mathematicians during the past century have gradually relaxed the requirements in systems with two operations and have unveiled non-commutative fields, rings without unit elements, and non-associative rings, these new systems have, in many cases, found application in the sciences. More recently algebraists have ventured to speak of addition without the abelian property. In this paper, we investigate the generalization of a non-associative ring obtained by removing the restriction that the sum of two elements of the system is independent of the order of addition. For such a mathematical system we have adopted the name *cluster*.

The author is deeply indebted to Professor R. H. Bruck for his guidance in this study and to E. S. Sokolnikoff for suggesting the name *cluster*.

The opening chapter develops general results in the theory of clusters. The concept of homomorphism is applied and leads to consideration of ideals Important subsets studied are the derived ring and the annihilator ideal. Closing the chapter is a specific example demonstrating the existence of a cluster with not-abelian addition.

The viewpoint of extension of rings is adopted in Chapter II for the purpose of constructing clusters and describing various properties, special cases, and examples of clusters so obtained. The chief result is a solution for the problem of constructing all clusters. Specifically, Theorem 1 and the succeeding theory describe every cluster containing a given ring with the properties that the given ring contains the derived ring of the cluster and that the additive right cosets of the given ring are in one-to-one correspondence with a given set.

The corollary to Theorem 1 offers a theoretic solution to an analogous problem from the theory of groups: namely, to construct every group containing a given subgroup (which, in contrast to the classical extension problem, need not be a normal subgroup) with a given set of right cosets of the subgroup.

With a different approach, in the last chapter we obtain many clusters

Presented to the Society April 27, 1946; received by the editors July 19, 1946, and, in revised form, April 9, 1947.

by imposing upon a non-abelian group, with its operation written additively, a multiplication which will satisfy the closure and distributive laws. Clusters, the number of whose elements is prime or the product of two primes, are examined.

Several conventions concerning our terminology should be noted. The word *associative* will apply only to the operation of multiplication, unless the contrary is explicitly mentioned. The words *abelian* and *commutative* are often used interchangeably in the literature; we shall however distinguish between these words: *abelian* will apply only to an additive operation, *commutative* only to the operation of multiplication. Likewise we differentiate between the prefixes *not-* and *non-* in such phrases as *non-commutative*, *not-associative*; the prefix *non-* designates that the system does not necessarily possess the property: it may or it may not; the prefix *not-* indicates that the system possesses at least one example of the failure of the property. The word *ring* is used for a non-associative ring, that is, a system forming an abelian group under addition, closed under multiplication, and satisfying both distributive laws. (The unit element and commutative multiplication are not hypothesized.) If a subset of a cluster is a group under addition, we often speak of a *subgroup* without writing the complete phrase *subgroup of the additive group of the cluster*. A similar remark applies to normal (or invariant) subgroups. The *order* of a mathematical system is the number (finite or infinite) of distinct elements in the system. Every subset of a group generates a subgroup, the intersection of all subgroups containing the given subset, hence the minimal subgroup containing the given subset. According as the cyclic subgroup generated by a single element has finite order $N$ or infinite order, we say that the *order* of the generating element is $N$ or zero, respectively. Set inclusion is denoted by $\subseteq$, while $\subset$ will be reserved for proper inclusion.

## CHAPTER I

1. A not-empty mathematical system of elements, $A, B, C, \cdots$, in which an equals relation and two single-valued binary ordered operations are defined will be called a *cluster* $\mathfrak{L}$ if the system forms a group under the operation of addition $(+)$, is closed under the operation of multiplication $(\cdot)$, and satisfies both distributive laws. Symbolically, the last condition states that $A\cdot(B+C)=A\cdot B+A\cdot C$ and $(A+B)\cdot C=A\cdot C+B\cdot C$ for all $A, B, C$.

Thus a (non-associative) ring is a cluster whose additive group is abelian.

As usual, we designate the additive identity by 0, the additive inverse of each element $A$ by $-A$; we also abbreviate each sum of the form $A+(-B)$ by $A-B$. The method of proof customarily used in ring theory [van der Waerden, vol. I, p. 37][1] is also applicable here to demonstrate that the

[1] References in brackets refer to the bibliography at the end of the paper. References to sections of the present paper are enclosed in parentheses; the Roman numeral for the chapter is omitted whenever the indicated section belongs to the chapter in which the reference appears.

following relations are valid for all $A$, $B$, $C$: $A(B-C)=AB-AC$; $(A-B)C=AC-BC$; $A\cdot 0=0=0\cdot A$; $(-A)B=-(AB)=A(-B)$; $(-A)(-B)=AB$.

2. A not-void subset of a cluster $\mathfrak{L}$ is called a *subcluster* if its elements, under the operations defined in $\mathfrak{L}$, form a cluster. Necessary and sufficient is the condition that the subset contain both $A-B$ and $AB$ whenever it contains the elements $A$ and $B$.

Since the intersection of any number of subgroups of a group is also a subgroup, we conclude that the intersection of an arbitrary (finite or infinite) number of subclusters of a cluster is itself a subcluster: multiplicative closure is readily verified.

Given an arbitrary subset of a cluster, we may thus unambiguously speak of the minimal subcluster containing the given subset: namely, the intersection of all subclusters containing the given subset.

3. An element $E$ of a cluster will be called a *product-element* if it can be factored as the product of two elements of the cluster: $E=B\cdot C$. Two product-elements are always abelian [Taussky, p. 245; Baer, p. 638]: if $BC$ and $AD$ are product-elements, then $AC+AD+BC+BD=A(C+D)+B(C+D)=(A+B)(C+D)=(A+B)C+(A+B)D=AC+BC+AD+BD$ and subtraction of terms $AC$ and $BD$ yields $AD+BC=BC+AD$. The set of all product-elements generates additively a subgroup, indeed an abelian subgroup since the generators are pairwise abelian; this subset, certainly closed under multiplication, is therefore a ring. We call this ring the *derived ring* of the cluster and denote it by $\mathfrak{R}$. The derived ring may alternatively be defined as the minimal subcluster of $\mathfrak{L}$ which contains all product-elements.

The derived ring may consist of the zero element alone. In fact, such clusters are easily constructed by taking any group whatever, writing its operation additively, and defining the products $AB=0$ for all $A$, $B$; distributive laws are satisfied. Further, multiplication is associative and commutative. These clusters, which we call trivial, possess little interest and will frequently be rejected from our consideration. In a not-trivial not-abelian cluster, then, $(0)\subset\mathfrak{R}\subset\mathfrak{L}$; the converse is false.

A well known [MacDuffee, p. 150] sufficient condition that a cluster be a ring is that it contain a one-sided unit element. Suppose $U$ is a left unit; then every element $A$ is a product-element: $A=UA$. The derived ring and the cluster coincide. Occurrence of a right unit is treated similarly.

4. We introduce the summation notation $\sum^j A$ to designate the $j$th multiple of the element $A$, for each rational integer $j$; that is, $\sum^0 A=0$, $\sum^{j+1}A=A+\sum^j A$ when $j\geqq 0$, and $\sum^j A=\sum^{(-j)}(-A)$ when $j<0$.

If a cluster possesses elements $A$ and $B$ of positive (additive) orders $m$ and $n$, respectively, then the order $p$ of the product $AB$ divides the positive greatest common divisor of $m$ and $n$. For, by the distributive laws, the hypothesis $\sum^m A=0$ implies $\sum^m(AB)=(\sum^m A)B=0$, whence $p$ divides $m$; similarly, the hypothesis $\sum^n B=0$ implies $\sum^n(AB)=A(\sum^n B)=0$, whence

$p$ divides $n$. In particular, if $m$ and $n$ are relatively prime, $AB=0=BA$. By induction, if the elements $A_1, A_2, A_3, \cdots$ have positive orders $m_1, m_2, m_3, \cdots$, respectively, every product involving the factors $A_1, A_2, A_3, \cdots$ has order dividing the greatest common divisor of $m_1, m_2, m_3, \cdots$. If we consider zero as a divisor of itself but of no positive number and interpret the greatest common divisor of zero and zero to be zero, then the remarks of this paragraph remain valid even if some (or all) of the factors have zero order.

Suppose the element $A$ multiplicatively generates a semigroup (that is, a system closed and associative under multiplication). Then, for each natural number $j$, the product of $j$ factors each equal to $A$ is uniquely determined; designate the $j$th power, as usual, by $A^j$. Applying the results of the preceding paragraph, if $n_j$ is the (additive) order of $A^j$ for each $j \geqq 1$, then the sequence of numbers $n_1, n_2, n_3, \cdots$ has the property that every term is divisible by the succeeding term. In particular, if there exists a power $A^k$ with prime order $n_k$, then either every higher power $A^{k+j}$, where $j \geqq 0$, has the same order $n_{k+j}=n_k$ or else the element $A$ is multiplicatively *nilpotent* (that is, there exists a natural number $q$ such that $A^q=0$).

5. We extend to clusters the concepts of homomorphisms [van der Waerden, vol. I, p. 31]. A correspondence between the elements of a cluster $\mathfrak{L}$ and the elements of a cluster $\mathfrak{L}'$ is a mapping of $\mathfrak{L}$ *upon* $\mathfrak{L}'$ if each element $A \in \mathfrak{L}$ has a unique image $A' \in \mathfrak{L}'$ and each element $A' \in \mathfrak{L}'$ is the image of at least one element $A \in \mathfrak{L}$; the mapping is symbolized $A \to A'$. The cluster $\mathfrak{L}$ is *homomorphic* to the cluster $\mathfrak{L}'$ if there exists a mapping, $A \to A'$, of $\mathfrak{L}$ upon $\mathfrak{L}'$ which preserves both operations: that is, $A \to A'$ and $B \to B'$ imply both $A+B \to A'+B'$ and $AB \to A'B'$ for all $A$, $B$. A one-to-one homomorphic mapping is an *isomorphism*. Homomorphism is denoted by $\mathfrak{L} \sim \mathfrak{L}'$, and isomorphism by $\mathfrak{L} \cong \mathfrak{L}'$.

A cluster homomorphism involves, of course, a group homomorphism with respect to the additive groups of the clusters. Consequently, if $\mathfrak{L} \sim \mathfrak{L}'$, then the set $\mathfrak{J}$ of all elements in $\mathfrak{L}$ whose image is zero in $\mathfrak{L}'$ is an invariant subgroup. This set is called the *kernel* of the homomorphism. We shall also call such a set an *ideal* (specifically, two-sided ideal) by analogy with the terminology in ring theory. The set $\mathfrak{J}$ has the *ideal property* of being closed under multiplication on either the right or the left by every element of the cluster: thus, for all $I \in \mathfrak{J}$ and all $A \in \mathfrak{L}$, the correspondences $A \to A'$ and $I \to 0'$ imply $AI \to A'0'=0'$ and similarly $IA \to 0'$, whence $AI \in \mathfrak{J}$ and $IA \in \mathfrak{J}$. An ideal, then, is an invariant subgroup with the ideal property. The preceding statement may be interpreted as a definition for an ideal, equivalent to the original definition. To complete the verification of the equivalence, we let $\mathfrak{R} \subseteq \mathfrak{L}$ be an arbitrary normal subgroup possessing the ideal property and we construct a cluster upon which $\mathfrak{L}$ may be mapped homomorphically with $\mathfrak{R}$ as the kernel. Define in $\mathfrak{L}$ a congruence relationship: $A \equiv B \bmod \mathfrak{R}$ if and only if $(-B+A) \in \mathfrak{R}$. We denote the class of all elements congruent to an element

$A$ by $[A]$. Addition and multiplication of classes are then defined by $[A]+[B]=[A+B]$ and $[A]\cdot[B]=[AB]$, respectively. Applying the results of group theory and the techniques of ring theory, we readily verify that this system of well-defined classes, $[A]$, $[B]$, $[C]$, $\cdots$, forms a cluster; we call it the *difference cluster* $\mathfrak{L}-\mathfrak{K}$. Under the mapping $A\rightarrow[A]$, the difference cluster $\mathfrak{L}-\mathfrak{K}$ is a homomorphic image of $\mathfrak{L}$. The kernel of the homomorphism is the set of all elements in $\mathfrak{L}$ whose image is the class $[0]$, precisely the subset $\mathfrak{K}$.

We note that every ideal is a (possibly trivial) subcluster, but a subcluster need not be an ideal.

Granting the axiom of choice, we may choose, according to some prescribed law, one representative element from each residue class modulo an ideal $\mathfrak{I}$. Then if $D$ is the representative of the class to which $A$ belongs, we may write $A=D+I$, where $I\in\mathfrak{I}$. As $I$ varies over all elements of $\mathfrak{I}$, the sum $D+I$ varies over all elements of the class $[A]$. If $A_1$ is similarly decomposed, $A_1=D_1+I'$, then $A\equiv A_1 \bmod \mathfrak{I}$ if and only if $D=D_1$. Each decomposition is unique, for $A=A_1$ implies $D=D_1$ and hence $I=I'$. Every element $A\in\mathfrak{L}$ is representable uniquely as the non-abelian sum of a representative element and an element of $\mathfrak{I}$.

6. An important example of an ideal is the set $\mathfrak{A}$ of all annihilators. An element $F$ is called an *annihilator* if its products with every element are zero: that is, if $AF=0=FA$ for all $A$. We show that $\mathfrak{A}$ satisfies the second definition for an ideal. The difference of two annihilators is an annihilator: $A(F_1-F_2)=AF_1-AF_2=0=F_1A-F_2A=(F_1-F_2)A$ for all $A$; consequently, $\mathfrak{A}$ is a subgroup. Choose arbitrarily $F\in\mathfrak{A}$ and $B\in\mathfrak{L}$; then $(-B+F+B)A=-BA+FA+BA=-BA+BA=0$ and similarly $A(-B+F+B)=0$ for all $A$; hence the subgroup $\mathfrak{A}$ is invariant. The definition of an annihilator, together with the fact that $0\in\mathfrak{A}$, guarantees possession of the ideal property for $\mathfrak{A}$—indeed, for any subset of $\mathfrak{A}$ which contains 0. The *annihilator ideal* $\mathfrak{A}$, then, exemplifies a trivial subcluster—sometimes a ring, sometimes not (contrast Examples 1 and 3, below). In order that the cluster $\mathfrak{L}$ be not-trivial, it is necessary and sufficient that $\mathfrak{A}\subset\mathfrak{L}$.

Since every subset of $\mathfrak{A}$ which contains 0 possesses the ideal property, any subgroup of $\mathfrak{A}$ which is normal in $\mathfrak{L}$ will be an ideal in $\mathfrak{L}$.

The element $-B-C+B+C$ is the (additive) commutator of the ordered pair of elements $B$ and $C$. Since product-elements are abelian, $(-B-C+B+C)A=-BA-CA+BA+CA=-BA+BA-CA+CA=0$ and similarly $A(-B-C+B+C)=0$ for all $A$, $B$, $C$; thus every commutator is an annihilator [Taussky, p. 245]. According to group theory [Zassenhaus, p. 55], all the commutators may not themselves form a subgroup, but the subgroup generated by them is invariant. This subgroup $\mathfrak{C}$, by the preceding paragraph, is an ideal and will be called the *commutator ideal*; we have $\mathfrak{C}\subseteq\mathfrak{A}$.

Since a necessary and sufficient condition that addition be abelian is that $\mathfrak{C}=(0)$, a not-trivial cluster which is not a ring must possess not-zero com-

mutators, not-zero annihilators, and hence proper divisors of zero; thus, $(0)\subset\mathfrak{C}\subseteq\mathfrak{A}\subset\mathfrak{L}$.

Applying the well known group-theoretic result [Pontrjagin, p. 14] that a quotient group modulo a normal subgroup is commutative if and only if the normal subgroup contains the commutator subgroup, we conclude that the difference cluster $\mathfrak{L}-\mathfrak{J}$ modulo an ideal $\mathfrak{J}$ is a ring if and only if $\mathfrak{C}\subseteq\mathfrak{J}$. In particular, $\mathfrak{L}-\mathfrak{A}$ is always a ring.

Congruences modulo any ideal $\mathfrak{B}$ contained in the annihilator ideal (special cases are $\mathfrak{B}=\mathfrak{A}$ and $\mathfrak{B}=\mathfrak{C}$) possess the following unusual property. If $A\equiv A_1$ and $B\equiv B_1$ mod $\mathfrak{B}$, then $AB=A_1B_1$; for, $AB=(A_1+F)(B_1+F')=A_1B_1+0$, where $F\in\mathfrak{A}$ and $F'\in\mathfrak{A}$.

7. The derived ring $\mathfrak{R}$ of a cluster $\mathfrak{L}$ is an additive subgroup possessing the ideal property. A necessary and sufficient condition, then, that $\mathfrak{R}$ be an ideal is that it be a normal subgroup. That $\mathfrak{R}$ sometimes is, and other times is not, an ideal is illustrated in later examples of clusters (§§I.10, III.3).

If $\mathfrak{J}$ is any ideal in $\mathfrak{L}$, a necessary and sufficient condition that the difference cluster $\mathfrak{L}-\mathfrak{J}$ be trivial is that $\mathfrak{J}$ contain the derived ring $\mathfrak{R}$. The sufficiency is immediate, because $AB\in\mathfrak{R}\subseteq\mathfrak{J}$ for all $A$, $B$. Conversely, if $AB\equiv 0$ mod $\mathfrak{J}$ for all $A$, $B$, then the ideal $\mathfrak{J}$ is a subcluster containing all product-elements; hence (§3) $\mathfrak{J}\supseteq\mathfrak{R}$. In particular, if $\mathfrak{R}$ is an ideal, then $\mathfrak{L}-\mathfrak{R}$ is a trivial cluster.

A sufficient condition that the cluster $\mathfrak{L}$ be associative is that the difference cluster $\mathfrak{L}-\mathfrak{A}$ be trivial. For the preceding paragraph guarantees that every product $AB\in\mathfrak{A}$; consequently every product of three (or more) factors is zero.

8. The intersection of an arbitrary (finite or infinite) number of ideals in a cluster is itself an ideal. We have already (§2) observed that the intersection is a subcluster; possession of the ideal property follows as in the theory of rings.

We are therefore entitled to speak of the minimal ideal containing a given subset of a cluster or to speak of the ideal generated by the elements of a subset of a cluster: namely, the intersection of all ideals containing the given subset.

The sum—or union—of any finite number of ideals in a cluster, designated by $\mathfrak{J}_1+\mathfrak{J}_2+\cdots+\mathfrak{J}_n$, is the set of all elements $I_1+I_2+\cdots+I_n$, where $I_j\in\mathfrak{J}_j$ for each $j=1, 2, \cdots, n$. This set is an invariant subgroup [Pontrjagin, p. 16]; by distributivity, it possesses the ideal property: $(I_1+I_2+\cdots+I_n)A=I_1A+I_2A+\cdots+I_nA$ and similarly $A\sum_{j=1}^{n}I_j=\sum_{j=1}^{n}(AI_j)$. Thus the sum of ideals is an ideal. Since each ideal is a normal subgroup, addition of ideals is an associative and abelian operation.

9. An element $E$ of a cluster is called an *idempotent* provided it is not zero and is equal to its own square, that is, $EE=E\neq 0$. Certainly, $E\in\mathfrak{R}$. Multiplicatively the element $E$ constitutes a group.

10. *Example* 1. We now cite an example to verify the existence of not-trivial not-abelian clusters. Our illustration is a cluster of order 8; that is, it has 8 elements. The additive group is the octic group: elements $xP+yQ$; $x=0, 1, 2, 3$; $y=0, 1$; relations between generators $4P=0=2Q$, $Q+P=3P+Q$. Hence the general law of addition is $(xP+yQ)+(x'P+y'Q)=[x+(-1)^{y}x']P+[y+y']Q$. The law of multiplication may be written $(xP+yQ)(x'P+y'Q)=xx'(2P)+xy'(P+Q)+x'y(Q+P)$. This law is equivalent to the requirements that the product of each pair of generators, distinct or alike, is the same as their sum in the same order and that distributivity holds. The product as we have defined it does not display the coefficients of the generators; use of the addition law enables us to write the product in either of the forms $[2xx'+(xy')^2+(-1)^{xy'+x'y}(x'y)^2]P+[xy'+x'y]Q$ or $[2xx'-(x'y)^2+(-1)^{x'y}(xy')^2]P+[xy'+x'y]Q$. In verifying the first of these, we make use of the fact that the elements $P+Q$ and $Q+P$ each have order two; hence, if $w\equiv 0$ or 1 mod 4, then $w(P+Q)=wP+wQ$ and $w(Q+P)=wQ+wP$. Thus,

$$
\begin{aligned}
&xx'(2P) + xy'(P + Q) + x'y(Q + P)\\
&\quad = 2xx'P + (xy')^2(P + Q) + (x'y)^2(Q + P)\\
&\quad = 2xx'P + (xy')^2P + (xy')^2Q + (x'y)^2Q + (x'y)^2P\\
&\quad = [2xx' + (xy')^2]P + [xy' + x'y]Q + (x'y)^2P \qquad \text{(since } Q \text{ has order two)}\\
&\quad = [2xx' + (xy')^2 + (-1)^{xy'+x'y}(x'y)^2]P + [xy' + x'y]Q \text{ (by addition law).}
\end{aligned}
$$

The second expression above for the product is verified similarly, after permuting the product-elements $xy'(P+Q)$ and $x'y(Q+P)$. The distributive laws must now be verified.

$$
\begin{aligned}
&(xP + yQ)\{(x'P + y'Q) + (x''P + y''Q)\}\\
&\qquad = [xx' + (-1)^{y'}xx''](2P) + [xy' + xy''](P + Q)\\
&\qquad\quad + [x'y + (-1)^{y'}x''y](Q + P),
\end{aligned}
\tag{1}
$$

while

$$
\begin{aligned}
&(xP + yQ)(x'P + y'Q) + (xP + yQ)(x''P + y''Q)\\
&\qquad = [xx' + xx''](2P) + [xy' + xy''](P + Q) + [x'y + x''y](Q + P).
\end{aligned}
\tag{2}
$$

When we recall that $2P$ and $Q+P$ have order two, we realize that the factor $(-1)^{y'}$ occurring in the right member of (1) is immaterial; thus the right members of (1) and (2) are identical. The right-hand law is checked similarly, by making use of the fact that $2P$ and $P+Q$ have order two. Our system is therefore a cluster. Its addition and multiplication tables are displayed in the accompanying tables, in which the left-hand summand or factor, respectively, appears in the left column and the right-hand summand or factor, respectively, appears in the top row.

| + | 0 | $P$ | $2P$ | $3P$ | $Q$ | $P+Q$ | $2P+Q$ | $3P+Q$ |
|---|---|---|---|---|---|---|---|---|
| 0 | 0 | $P$ | $2P$ | $3P$ | $Q$ | $P+Q$ | $2P+Q$ | $3P+Q$ |
| $P$ | $P$ | $2P$ | $3P$ | 0 | $P+Q$ | $2P+Q$ | $3P+Q$ | $Q$ |
| $2P$ | $2P$ | $3P$ | 0 | $P$ | $2P+Q$ | $3P+Q$ | $Q$ | $P+Q$ |
| $3P$ | $3P$ | 0 | $P$ | $2P$ | $3P+Q$ | $Q$ | $P+Q$ | $2P+Q$ |
| $Q$ | $Q$ | $3P+Q$ | $2P+Q$ | $P+Q$ | 0 | $3P$ | $2P$ | $P$ |
| $P+Q$ | $P+Q$ | $Q$ | $3P+Q$ | $2P+Q$ | $P$ | 0 | $3P$ | $2P$ |
| $2P+Q$ | $2P+Q$ | $P+Q$ | $Q$ | $3P+Q$ | $2P$ | $P$ | 0 | $3P$ |
| $3P+Q$ | $3P+Q$ | $2P+Q$ | $P+Q$ | $Q$ | $3P$ | $2P$ | $P$ | 0 |

| · | 0 | $P$ | $2P$ | $3P$ | $Q$ | $P+Q$ | $2P+Q$ | $3P+Q$ |
|---|---|---|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| $P$ | 0 | $2P$ | 0 | $2P$ | $P+Q$ | $3P+Q$ | $P+Q$ | $3P+Q$ |
| $2P$ | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| $3P$ | 0 | $2P$ | 0 | $2P$ | $P+Q$ | $3P+Q$ | $P+Q$ | $3P+Q$ |
| $Q$ | 0 | $3P+Q$ | 0 | $3P+Q$ | 0 | $3P+Q$ | 0 | $3P+Q$ |
| $P+Q$ | 0 | $P+Q$ | 0 | $P+Q$ | $P+Q$ | 0 | $P+Q$ | 0 |
| $2P+Q$ | 0 | $3P+Q$ | 0 | $3P+Q$ | 0 | $3P+Q$ | 0 | $3P+Q$ |
| $3P+Q$ | 0 | $P+Q$ | 0 | $P+Q$ | $P+Q$ | 0 | $P+Q$ | 0 |

Multiplication is not-associative and not-commutative. The derived ring $\mathfrak{R}$ consists of four elements: 0, $2P$, $P+Q$, $3P+Q$; it is a trivial subcluster and an ideal; its difference cluster $\mathfrak{L}-\mathfrak{R}$ is the trivial ring with two elements. The annihilator ideal $\mathfrak{A}$ and the commutator ideal $\mathfrak{C}$ coincide, each containing the two elements 0, $2P$; thus $(0)\subset\mathfrak{C}=\mathfrak{A}\subset\mathfrak{R}\subset\mathfrak{L}$. The difference cluster $\mathfrak{L}-\mathfrak{A}$, consisting of four elements, is a not-trivial ring; thus $\mathfrak{R}$ and $\mathfrak{L}-\mathfrak{A}$, although both of order four, are not isomorphic rings. As an illustration of the theory in §4, the ascending powers of the element $P$ have additive orders 4, 2, 1, 1, 1, $\cdots$, respectively; every term in this sequence of natural numbers is divisible by every succeeding term. To be noted, also, are the facts that every element satisfies the equation $A\cdot A=A+A$, and that several pairs of elements—including the generators, as mentioned above—satisfy the relation $A\cdot B=A+B$.

11. *Example* 2. By way of contrast, we may construct three other not-trivial not-abelian clusters, all of which have the very same additive group as that of the not-associative, not-commutative cluster in Example 1, namely

the octic group. One of these, in which multiplication is defined by $(xP+yQ)\cdot(x'P+y'Q)=x(x'+y')(2P)$, is associative but not commutative. Another, where the rule of multiplication is $(xP+yQ)(x'P+y'Q)=(xy'+x'y)(P+Q)$, is commutative but not associative. The third, in which products are defined by $(xP+yQ)(x'P+y'Q)=yy'Q$, possesses both associativity and commutativity.

## CHAPTER II

1. In this chapter we discuss an extension problem for clusters. Roughly, the problem is to find a cluster which contains a prescribed ring; but formally: given a ring $\mathfrak{S}$ and a set $\Gamma$ of elements, can there be constructed a cluster $\mathfrak{L}$ possessing a subring $\mathfrak{M}$ such that (i) $\mathfrak{M}$ is isomorphic to the given ring $\mathfrak{S}$, (ii) $\mathfrak{M}$ contains the derived ring $\mathfrak{N}$ of $\mathfrak{L}$, (iii) the set $\Gamma$ is equivalent to a subset $\mathfrak{G}$ of $\mathfrak{L}$, consisting of representative elements of the additive right cosets of $\mathfrak{M}$, (iv) $\mathfrak{M}\cap\mathfrak{G}=(0)$? A solution of the problem is given by the following theorem.

THEOREM 1. *The set of conditions in* §3 *is both necessary and sufficient that the desired cluster be constructible.*

The necessity will be proved in §2, by supposing that $\mathfrak{L}$ is known and then deriving the set of conditions from an examination of the structure and interrelation of the subsets $\mathfrak{M}$ and $\mathfrak{G}$. The sufficiency will be demonstrated by exhibiting the cluster (§4) and later (§7) showing that it has the desired properties.

In the other sections of the chapter, we desire to study further the structure and properties of clusters expressed in such form. As may be surmised, however, the construction outlined above is both powerful and unwieldy. Although reluctant to sacrifice full generality, we were soon obliged to realize that a reasonable amount of specialization would greatly facilitate the study. Consequently one additional restriction is imposed in §12. In spite of this specialization, the resulting theory which will be developed thereafter is applicable in many cases of significance. The chapter concludes with several specific cases and examples of a contrasting nature.

2. Let $\mathfrak{L}$ be an arbitrary cluster. Let $\mathfrak{M}$ be any subring which contains the derived ring $\mathfrak{N}$. Since $\mathfrak{M}$ forms an additive subgroup of $\mathfrak{L}$, we may consider the totality of right cosets of $\mathfrak{M}$. From each coset, we select exactly one representative element and we denote the set of these representatives by $\mathfrak{G}$; convenience dictates that the zero element of $\mathfrak{L}$ should be chosen as the representative of $\mathfrak{M}$ itself. In pursuit of our goal announced in §1, we adopt a notation which may be transferred easily to the problem of extending $\mathfrak{S}$ (the analog of $\mathfrak{M}$) by $\Gamma$ (the analog of $\mathfrak{G}$). Lower case Latin letters will denote elements of $\mathfrak{M}$; Greek letters, elements of $\mathfrak{G}$. Hence every element $R$ of $\mathfrak{L}$ is uniquely expressible as the non-abelian sum $r+\rho$, where $r\in\mathfrak{M}$ and $\rho\in\mathfrak{G}$. In particular, the zero element in $\mathfrak{L}$ may be decomposed: $0=z+\epsilon$,

where (although it is true that $0=z=\epsilon$ in the given cluster $\mathfrak{L}$) we wish to interpret $z$ as the zero in $\mathfrak{M}$ and $\epsilon$ as the representative of the coset $\mathfrak{M}$. Instead of writing $R=r+\rho$, we sometimes desire a coupling notation given by $[r, \rho]=r+\rho$.

Let $\mathfrak{L}$ contain also the element $S=s+\sigma=[s, \sigma]$. Then $T=R+S\in\mathfrak{L}$; or $t+\tau=T=[r, \rho]+[s, \sigma]=r+\rho+s+\sigma=r+(\rho+s+\sigma)$. Since $r\in\mathfrak{M}$, the element $\tau$, representing the coset in which $R+S$ lies, is determined by the elements $\rho$, $s$, $\sigma$, but is independent of $r$. To express this functional dependence we write $\tau=\gamma(s|\rho, \sigma)$ and thereby suggest that, for each fixed $s\in\mathfrak{M}$, there is defined a single-valued function on $\mathfrak{G}\mathfrak{G}$ into $\mathfrak{G}$. Then there exists $u\in\mathfrak{M}$ such that $\rho+s+\sigma=u+\tau$; this relation shows that $u$ is determined uniquely by $\rho$, $s$, $\sigma$ and we introduce the function $g(\rho, \sigma|s)$, defined by $g(\rho, \sigma|s)=u=\rho+s+\sigma-\tau=\rho+s+\sigma-\gamma(s|\rho, \sigma)$. The notation $g(\rho, \sigma|s)$ suggests that, for each fixed ordered pair of elements $\rho\in\mathfrak{G}$ and $\sigma\in\mathfrak{G}$, there exists a single-valued function of $\mathfrak{M}$ into itself. Since $t+\tau=r+u+\tau$, we conclude that $t=r+u=r+g(\rho, \sigma|s)$. Thus we may write $[r, \rho]+[s, \sigma]=[r+g(\rho, \sigma|s), \gamma(s|\rho, \sigma)]$.

Since the functions $g(\rho, \sigma|x)$ and $\gamma(s|\xi, \eta)$ characterize addition in $\mathfrak{L}$, we seek the essential properties of these functions. From the equation $0+S=S$, we deduce two necessary requirements: $g(\epsilon, \sigma|s)=s$ and $\gamma(s|\epsilon, \sigma)=\sigma$ for all $s\in\mathfrak{M}$ and all $\sigma\in\mathfrak{G}$. From the associativity relation $(R+S)+T=R+(S+T)$ comes another pair of necessary conditions: $g(\rho, \sigma|s)+g(\gamma(s|\rho, \sigma), \tau|t)=g(\rho, \gamma(t|\sigma, \tau)|s+g(\sigma, \tau|t))$ and $\gamma(t|\gamma(s|\rho, \sigma), \tau)=\gamma(s+g(\sigma, \tau|t)|\rho, \gamma(t|\sigma, \tau))$, each valid for all values of $s$, $t$, $\rho$, $\sigma$, $\tau$. Another requirement arises from the solvability of the equation $Y+S=0$ for $Y\in\mathfrak{L}$: we demand that, for all $s\in\mathfrak{M}$ and all $\sigma\in\mathfrak{G}$, there should exist at least one element $\eta\in\mathfrak{G}$ such that $\gamma(s|\eta, \sigma)=\epsilon$.

Having completed our work for addition, we turn now to multiplication and the distributive laws in $\mathfrak{L}$. Since $\mathfrak{M}$ contains the derived ring $\mathfrak{R}$, every product of elements in $\mathfrak{L}$ lies in $\mathfrak{M}$. Let $\rho$ be any element of $\mathfrak{G}$; then, for arbitrary elements $s$ and $t$ of $\mathfrak{M}$, we find that $\rho\cdot s\in\mathfrak{M}$ and further that $\rho\cdot(s+t)=\rho\cdot s+\rho\cdot t$ in $\mathfrak{L}$; thus $\rho$ acts as a left-operator for the additive subgroup $\mathfrak{M}$ and we introduce the notation $\rho\times s$ for this endomorphic mapping. A similar discussion shows that every element $\sigma\in\mathfrak{G}$ acts as a right-operator (notation: $r\times\sigma$) for the additive subgroup $\mathfrak{M}$. Finally, since $\rho\cdot\sigma\in\mathfrak{M}$ for all $\rho$ and all $\sigma$, we have a single-valued function on $\mathfrak{G}\mathfrak{G}$ into $\mathfrak{M}$; this function will be denoted by $\rho\square\sigma=v\in\mathfrak{M}$. In summary, for arbitrary $R$ and $S$ in $\mathfrak{L}$, their product lies in $\mathfrak{M}$ and we write $[r, \rho]\cdot[s, \sigma]=[rs+\rho\times s+r\times\sigma+\rho\square\sigma, \epsilon]$.

Four more conditions are necessary, as we find by examination of the distributive laws. In terms of our new notations, $R(S+T)$ and $RS+RT$ may be written $[u, \epsilon]$ and $[v, \epsilon]$, respectively, where $u=rs+rg(\sigma, \tau|t)+\rho\times s+\rho\times g(\sigma, \tau|t)+r\times\gamma(t|\sigma, \tau)+\rho\square\gamma(t|\sigma, \tau)$ and where $v=rs+\rho\times s+r\times\sigma+\rho\square\sigma+rt+\rho\times t+r\times\tau+\rho\square\tau$. Since $u=v$ for all values of $r$, $s$, $t$, $\rho$, $\sigma$, $\tau$, we may set $r=z$ and deduce the relation $\rho\times g(\sigma, \tau|t)+\rho\square\gamma(t|\sigma, \tau)=\rho\square\sigma+\rho\times t+\rho\square\tau$

satisfied by all $t, \rho, \sigma, \tau$. Using this special equation, the equation $u=v$ yields $rg(\sigma, \tau \mid t)+r\times\gamma(t \mid \sigma, \tau)=r\times\sigma+rt+r\times\tau$, valid for all $r, t, \sigma, \tau$. In a similar fashion we expand $(R+S)T$ and $RT+ST$, consider the special case $t=z$, and obtain the necessary conditions: $g(\rho, \sigma \mid s)\times\tau+\gamma(s \mid \rho, \sigma)\square\tau=\rho\square\tau+s\times\tau+\sigma\square\tau$ and $g(\rho, \sigma \mid s)t+\gamma(s \mid \rho, \sigma)\times t=\rho\times t+st+\sigma\times t$, each valid for all $s, t, \rho, \sigma, \tau$. This completes the catalog of our necessary set of conditions.

3. According to Theorem 1, the conditions enunciated in §2 suffice to construct a cluster when a ring $\mathfrak{S}$ and a set $\Gamma$ of representative elements are arbitrarily prescribed. We now restate the conditions formally and in §4 will exhibit the cluster. Henceforth our approach will be postulational, although many of the later results in the chapter may easily be obtained by the method of §2.

Let $\mathfrak{S}$ be a (non-associative) ring with elements $r, s, t, \cdots$; denote the zero element by $z$. Let $\Gamma$ be a not-void set of elements $\rho, \sigma, \tau, \cdots$, possessing a well-defined equivalence relation; let one of the elements of $\Gamma$ be selected arbitrarily and called $\epsilon$. Let these two sets be subjected to the following postulates, but otherwise be arbitrary.

(I) Every ordered pair of elements $\rho, \sigma$ in $\Gamma$ induces a mapping of $\mathfrak{S}$ *into* itself, symbolized by the function $g(\rho, \sigma \mid x)\in\mathfrak{S}$.

(II) Corresponding to each element $r\in\mathfrak{S}$, there exists a single-valued function on $\Gamma\Gamma$ *into* $\Gamma$, symbolized by $\gamma(r \mid \xi, \eta)\in\Gamma$.

(III) For all $s\in\mathfrak{S}$ and all $\sigma\in\Gamma$, there exists at least one element $\xi\in\Gamma$ such that $\gamma(s \mid \xi, \sigma)=\epsilon$.

(IV) Every element $\rho\in\Gamma$ is a left-operator for the additive group of $\mathfrak{S}$; the endomorphic mapping is denoted by $r\to\rho\times r$.

(V) Every element $\rho\in\Gamma$ is a right-operator for the additive group of $\mathfrak{S}$; the endomorphic mapping is denoted by $r\to r\times\rho$.

(VI) There exists a single-valued function on $\Gamma\Gamma$ *into* $\mathfrak{S}$; thus, given arbitrary elements $\rho$ and $\sigma$ of $\Gamma$, there corresponds a uniquely defined *combination-element* $\rho\square\sigma$ in $\mathfrak{S}$.

The remaining postulates are valid for every choice of the elements $r, s, t$ in $\mathfrak{S}$ and $\rho, \sigma, \tau$ in $\Gamma$.

(VII) $$g(\epsilon, \sigma \mid s) = s.$$

(VIII) $$\gamma(s \mid \epsilon, \sigma) = \sigma.$$

(IX) $$g(\rho, \sigma \mid s) + g(\gamma(s \mid \rho, \sigma), \tau \mid t) = g(\rho, \gamma(t \mid \sigma, \tau) \mid s + g(\sigma, \tau \mid t)).$$

(X) $$\gamma(t \mid \gamma(s \mid \rho, \sigma), \tau) = \gamma(s + g(\sigma, \tau \mid t) \mid \rho, \gamma(t \mid \sigma, \tau)).$$

(XI) $$rg(\sigma, \tau \mid t) + r \times \gamma(t \mid \sigma, \tau) = rt + r \times \sigma + r \times \tau.$$

(XII) $$\rho \times g(\sigma, \tau \mid t) + \rho \square \gamma(t \mid \sigma, \tau) = \rho \times t + \rho \square \sigma + \rho \square \tau.$$

(XIII) $$g(\rho, \sigma \mid s)t + \gamma(s \mid \rho, \sigma) \times t = st + \rho \times t + \sigma \times t.$$

(XIV) $$g(\rho, \sigma \mid s) \times \tau + \gamma(s \mid \rho, \sigma) \square \tau = s \times \tau + \rho \square \tau + \sigma \square \tau.$$

4. We proceed now to the definition of the cluster. Construct the system $\mathfrak{L}$ whose elements $R$, $S$, $T$, $\cdots$ are ordered couples $T=\{r, \rho\}$, where $r\in\mathfrak{S}$ and $\rho\in\Gamma$. We call $r$ and $\rho$ the *first* and *second components* of $R$, respectively. Elements $R$ and $S=\{s, \sigma\}$ are equal if and only if both $r=s$ and $\rho=\sigma$; this, according to our postulates, is a well-defined equals relation. Define in the system $\mathfrak{L}$ an operation of addition: $R+S=T=\{t, \tau\}$ if and only if both $r+g(\rho, \sigma\,|\,s)=t$ and $\gamma(s\,|\,\rho, \sigma)=\tau$. Define multiplication: $R\cdot S=T$ if and only if both $rs+\rho\times s+r\times\sigma+\rho\square\sigma=t$ and $\epsilon=\tau$. Under these two operations, both well-defined, the system $\mathfrak{L}$ forms, as we immediately check, a cluster.

First, addition is associative, for, with the aid of (IX) and (X):

$$\begin{aligned}(R+S)+T&=\{r+g(\rho, \sigma\,|\,s), \gamma(s\,|\,\rho, \sigma)\}+\{t, \tau\}\\&=\{r+g(\rho, \sigma\,|\,s)+g(\gamma(s\,|\,\rho, \sigma), \tau\,|\,t), \gamma(t\,|\,\gamma(s\,|\,\rho, \sigma), \tau)\}\\&=\{r+g(\rho, \gamma(t\,|\,\sigma, \tau)\,|\,s+g(\sigma, \tau\,|\,t)), \gamma(s+g(\sigma, \tau\,|\,t)\,|\,\rho, \gamma(t\,|\,\sigma, \tau))\}\\&=\{r, \rho\}+\{s+g(\sigma, \tau\,|\,t), \gamma(t\,|\,\sigma, \tau)\}=R+(S+T).\end{aligned}$$

Second, $\mathfrak{L}$ contains (at least) one additive left-identity, namely $0=\{z, \epsilon\}$; indeed, $0+S=\{z+g(\epsilon, \sigma\,|\,s), \gamma(s\,|\,\epsilon, \sigma)\}=\{s, \sigma\}$ for all $S\in\mathfrak{L}$, by (VII) and (VIII). Third, each element $R=\{r, \rho\}$ in $\mathfrak{L}$ has at least one additive left-inverse: by (III), there exists an element $\nu\in\Gamma$ such that

$$\gamma(r\,|\,\nu, \rho)=\epsilon; \tag{3}$$

using this element $\nu$, we write

$$n=-g(\nu, \rho\,|\,r); \tag{4}$$

then $N=\{n, \nu\}$ is an element satisfying $N+R=0$. Requirements for an additive group are now satisfied.

Verification of distributivity still remains. The following lemma will be convenient.

LEMMA. $\{m, \epsilon\}+\{m', \epsilon\}=\{m+m', \epsilon\}$ *for all* $m\in\mathfrak{S}$ *and all* $m'\in\mathfrak{S}$.

**Proof.** Use law of addition, (VII), and (VIII).

With the aid of (IV), (XI), (XII), and the lemma:

$$\begin{aligned}R(S+T)&=R\cdot\{s+g(\sigma, \tau\,|\,t), \gamma(t\,|\,\sigma, \tau)\}\\&=\{rs+rg(\sigma, \tau\,|\,t)+\rho\times s+\rho\times g(\sigma, \tau\,|\,t)\\&\quad+r\times\gamma(t\,|\,\sigma, \tau)+\rho\square\gamma(t\,|\,\sigma, \tau), \epsilon\}\\&=\{rs+\rho\times s+rt+r\times\sigma+r\times\tau+\rho\times t+\rho\square\sigma+\rho\square\tau, \epsilon\}\\&=\{rs+\rho\times s+r\times\sigma+\rho\square\sigma, \epsilon\}\\&\quad+\{rt+\rho\times t+r\times\tau+\rho\square\tau, \epsilon\}\\&=RS+RT\end{aligned}$$

for all $R$, $S$, $T$. A similar computation, with the aid of (V), (XIII), (XIV), and the lemma, verifies that $(R+S)T=RT+ST$ for all $R$, $S$, $T$.

Our system of couples has been shown to be a cluster. We proceed in the next few sections to discuss the properties and structure of this type of cluster.

5. Since the elements form an additive group, the left-negative $N$ of $R$, described in §4, is a two-sided negative, uniquely determined by $R$: we write $N=-R$. The components of $N$ are therefore uniquely determined by $r$ and $\rho$; consequently, the element $\xi$ described in (III) is unique when $s$ and $\sigma$ are prescribed. Since $R+N=0$, we deduce the results:

$$g(\rho, \nu \mid n) = -r, \tag{5}$$

$$\gamma(n \mid \rho, \nu) = \epsilon. \tag{6}$$

Since 0 is the unique two-sided additive identity, so that $S+0=S$ for all $S\in\mathfrak{R}$, we obtain the following relations, valid for all $\sigma\in\Gamma$:

$$g(\sigma, \epsilon \mid z) = z, \tag{7}$$

$$\gamma(z \mid \sigma, \epsilon) = \sigma. \tag{8}$$

When $R$ and $T$ are arbitrary elements of $\mathfrak{R}$, the equation $Y+R=T$ must possess a unique solution $Y\in\mathfrak{R}$. Again using $\{n, \nu\}=N=-R$, we find that $\{y, \eta\}=Y=T-R=T+N=\{t+g(\tau, \nu \mid n), \gamma(n \mid \tau, \nu)\}$. The reader may readily check the solution by computing $\{t+g(\tau, \nu \mid n), \gamma(n \mid \tau, \nu)\}+\{r, \rho\}$ and simplifying the sum with the aid of (IX), (X), (3), (4), (7), (8). We observe that $\eta$ is independent of $t$; thus the existence and uniqueness of $Y$ shows that (III) is a weak form of the derived result: namely, for all $s\in\mathfrak{S}$, all $\sigma\in\Gamma$, and all $\tau\in\Gamma$, there exists one and only one element $\eta\in\Gamma$ such that $\gamma(s \mid \eta, \sigma)=\tau$. In particular, the word *into* in the statement of (II) may be strengthened to read *upon*, since the functional values exhaust $\Gamma$.

For arbitrary elements $R$ and $T$ in $\mathfrak{R}$, a similar discussion displays the unique solution $X\in\mathfrak{R}$ for the equation $R+X=T$. The solution is $\{x, \xi\}=X=\{n+g(\nu, \tau \mid t), \gamma(t \mid \nu, \tau)\}$; verification utilizes (IX), (X), (5), (6), (VII), (VIII). In terms of components, the existence and uniqueness of $X$, when $r=z$, shows that, if $t$, $\rho$, $\tau$ are arbitrarily given, then the simultaneous equations

$$g(\rho, \xi \mid x) = t, \qquad \gamma(x \mid \rho, \xi) = \tau \tag{9}$$

possess one and only one solution for the elements $x\in\mathfrak{S}$ and $\xi\in\Gamma$. This statement, however, does not imply that the word *into* in the statement of (I) may be replaced by *upon*; indeed, when $\rho$ and $\sigma$ are prescribed, the functional values $g(\rho, \sigma \mid x)$ may not exhaust $\mathfrak{S}$. Likewise the solution of (9) does not imply the existence of $\xi\in\Gamma$ satisfying $\gamma(s \mid \rho, \xi)=t$ when $s$, $t$, $\rho$ are given arbitrarily.

6. Since every element $\rho \in \Gamma$ is both a left-operator and a right-operator for the additive group of $\mathfrak{S}$, we have $\rho \times z = z = z \times \rho$ for all $\rho$. We also note that $\epsilon$ is a zero operator on both the left and the right, that is, $\epsilon \times r = z = r \times \epsilon$ for all $r \in \mathfrak{S}$. The proof, for the left-sided case, is an application of (XIII) with $\rho = \epsilon$ and $t = r$: thus, $sr + \sigma \times r = g(\epsilon, \sigma \mid s)r + \gamma(s \mid \epsilon, \sigma) \times r = sr + \epsilon \times r + \sigma \times r$. In similar fashion, setting $\sigma = \epsilon$ in (XI) verifies the right-sided case. Analogously the two results $\epsilon \square \rho = z = \rho \square \epsilon$ for all $\rho \in \Gamma$ may be obtained from (XIV) with $\rho$ replaced by $\epsilon$ and $\tau$ replaced by $\rho$, and from (XII) with $\sigma = \epsilon$, respectively. Summarizing this section, every product in $\mathfrak{S}$, either of elements in $\mathfrak{S}$ or of the types in (IV), (V), or (VI), such that one factor is $z$ or $\epsilon$, is the element $z$.

7. We have constructed a cluster $\mathfrak{L}$ by a process which we called extension of a ring. In order to justify our terminology, we should show that the original ring $\mathfrak{S}$ is isomorphic to a subset of the constructed cluster $\mathfrak{L}$. Let $\mathfrak{M}$ denote the subset of $\mathfrak{L}$ consisting of all elements with second component $\epsilon$, that is, elements of the form $\{m, \epsilon\}$. Since $\{m, \epsilon\} + \{m', \epsilon\} = \{m + m', \epsilon\}$ by the lemma (§4) and $\{m, \epsilon\} \cdot \{m', \epsilon\} = \{mm' + \epsilon \times m' + m \times \epsilon + \epsilon \square \epsilon, \epsilon\} = \{mm', \epsilon\}$ by §6, the mapping $\{m, \epsilon\} \rightarrow m$ is an isomorphic mapping of $\mathfrak{M}$ upon $\mathfrak{S}$. Hence $\mathfrak{M}$ is an abelian subcluster of $\mathfrak{L}$.

Inasmuch as every product-element has second component $\epsilon$, the derived ring $\mathfrak{R}$ is contained in the ring $\mathfrak{M}$.

Let $\mathfrak{G}$ designate the set of all elements in $\mathfrak{L}$ whose first component is $z$, that is, elements of the form $\{z, \mu\}$. Except for logical precision, the sets $\mathfrak{G}$ and $\Gamma$ may be regarded as equivalent. We observe that the intersection $\mathfrak{M} \cap \mathfrak{G}$ contains only the element zero.

Every element $R \in \mathfrak{L}$ is expressible as the (non-abelian) sum of an element of $\mathfrak{M}$ and an element of $\mathfrak{G}$: namely,

$$R = \{r, \rho\} = \{r, \epsilon\} + \{z, \rho\}. \tag{10}$$

Furthermore, the decomposition is unique.

The elements $R$ and $S$ belong to the same additive right coset of $\mathfrak{M}$ if and only if there exists $M = \{m, \epsilon\} \in \mathfrak{M}$ such that $S = M + R$ or, equivalently, $\{s, \sigma\} = \{m, \epsilon\} + \{r, \rho\} = \{m + r, \rho\}$; hence, if and only if the second components of $R$ and $S$ are equal; hence, if and only if the second summands in their respective decompositions (10) coincide. Truly then $\mathfrak{G}$ is a set of uniquely determined representative elements, one and only one from each right coset of the subgroup $\mathfrak{M}$ in $\mathfrak{L}$. The proof of Theorem 1 is now complete.

Every product-element in $\mathfrak{L}$ is the sum of products of elements from one or both of the subsets $\mathfrak{M}$ and $\mathfrak{G}$; indeed, $RS = (\{r, \epsilon\} + \{z, \rho\}) \cdot (\{s, \epsilon\} + \{z, \sigma\}) = \{r, \epsilon\}\{s, \epsilon\} + \{z, \rho\}\{s, \epsilon\} + \{r, \epsilon\}\{z, \sigma\} + \{z, \rho\}\{z, \sigma\}$. Hence the derived ring is additively generated by all elements representable in one (or more) of the following types: $\{rs, \epsilon\}$ or $\{\rho \times s, \epsilon\}$ or $\{r \times \sigma, \epsilon\}$ or $\{\rho \square \sigma, \epsilon\}$. Elements of the first type alone may not generate $\mathfrak{R}$. Thus a sufficient, but

not necessary, condition that $\mathfrak{R}=\mathfrak{M}$ is that the ring $\mathfrak{S}$ be additively generated by its own product-elements.

As a consequence of §6 and the preceding paragraph, a necessary and sufficient set of conditions that the cluster $\mathfrak{L}$ be trivial (§I.3) is that the ring $\mathfrak{S}$ be trivial and every product described in (IV), (V), or (VI) vanish; thus, $rs=\rho\times s=r\times\sigma=\rho\square\sigma=z$ for all $r, s, \rho, \sigma$.

8. We temporarily digress in order to observe that the extension technique outlined thus far readily admits of generalization. Careful examination reveals that the property of abelian addition in $\mathfrak{S}$ is never used except when multiplication in $\mathfrak{L}$ is discussed. Consequently the construction can also be carried through if we allow $\mathfrak{S}$ itself to be a cluster, provided there exists in $\mathfrak{S}$ a subring $\mathfrak{U}$ such that (i) $\mathfrak{U}$ contains the derived ring of $\mathfrak{S}$, (ii) all the left-operators and right-operators described in (IV) and (V), respectively, map $\mathfrak{S}$ into $\mathfrak{U}$, (iii) the operation described in (VI) is a function on $\Gamma\Gamma$ into $\mathfrak{U}$. Furthermore, all the theory thus far enunciated remains valid, except for the result that $\mathfrak{M}$ is abelian.

9. A second digression leads us to the theory of groups. The classical problem in group extension [Schreier, p. 165] seeks the construction of a group such that it contains a normal subgroup isomorphic to a given group and such that the cosets of this invariant subgroup form a system isomorphic to another given group. We formulate a less restricted problem, the following: given a group $\Sigma$ and a not-empty set $\Gamma$ of elements, under what conditions may there be constructed a group $\Lambda$ such that $\Lambda$ contains a subgroup $\Sigma'$ isomorphic to $\Sigma$ and such that there exists a complete system of representative elements (including the identity of $\Lambda$) of the right cosets of $\Sigma'$ which will form a system equivalent to $\Gamma$? As the reader may readily check, a portion of the construction technique applied to clusters is completely independent of the operation of multiplication and yet fully describes the group properties under addition. Or, approached differently, we may extract the essentials of the additive operation of the cluster extension by making all products vanish. Either viewpoint demonstrates that our group theory problem admits the following solution, expressed in the notation of §3, with $\Sigma$ playing the role of the additive group of $\mathfrak{S}$.

COROLLARY (TO THEOREM 1). *A necessary and sufficient set of conditions that the desired group $\Lambda$ be constructible is that the given systems $\Sigma$ and $\Gamma$ satisfy Postulates* (I), (II), (III), (VII), (VIII), (IX), (X).

We remark that §8 allows us to dispense with the assumption of an abelian operation in the given group $\Sigma$. This completes our digressions.

10. A necessary and sufficient set of conditions that the cluster $\mathfrak{L}$ (§4) be a ring is that, for all $r, \rho, \sigma$, each of the following statements be valid: $g(\sigma, \epsilon|r)=r$; $\gamma(r|\sigma, \epsilon)=\sigma$; $g(\rho, \sigma|z)=g(\sigma, \rho|z)$; $\gamma(z|\rho, \sigma)=\gamma(z|\sigma, \rho)$. Indeed, since (§7) the cluster $\mathfrak{L}$ is additively generated by the elements of $\mathfrak{M}$ and $\mathfrak{G}$,

then $\mathfrak{L}$ will be abelian if and only if the elements of $\mathfrak{M}$ and $\mathfrak{G}$ are pairwise permutable. The first two conditions named are necessary and sufficient that every element of $\mathfrak{M}$ permute with every element of $\mathfrak{G}$; the last two conditions are likewise equivalent to the abelian addition for elements of $\mathfrak{G}$. We observe that we have tacitly assumed $\mathfrak{S}$ to be a ring; if, as suggested in §8, the cluster $\mathfrak{S}$ is not-abelian, then $\mathfrak{L}$ will never be abelian. All of the succeeding discussion in the present section remains valid for the generalized situation of §8.

A necessary and sufficient condition that our cluster $\mathfrak{L}$ be commutative is that, for all $r, s, \rho, \sigma$, the following three relations hold: $rs = sr$; $r \times \sigma = \sigma \times r$; $\rho \square \sigma = \sigma \square \rho$. Since $RS = \{rs + \rho \times s + r \times \sigma + \rho \square \sigma, \epsilon\}$ and $SR = \{sr + \sigma \times r + s \times \rho + \sigma \square \rho, \epsilon\}$, commutativity is equivalent to the relation $rs + \rho \times s + r \times \sigma + \rho \square \sigma = sr + \sigma \times r + s \times \rho + \sigma \square \rho$ for all $r, s, \rho, \sigma$. The three stated conditions are apparently sufficient. The necessity of each may be seen by successively taking $\rho = \sigma = \epsilon$, then $s = z$ and $\rho = \epsilon$, thirdly, $r = s = z$. Note that commutativity of $\mathfrak{S}$ is essential.

A necessary and sufficient condition that our cluster $\mathfrak{L}$ be associative is that, for all $r, s, t, \rho, \sigma, \tau$, the following eight relations hold: (i) $(rs)t = r(st)$, (ii) $(\rho \times s)t = \rho \times (st)$, (iii) $(r \times \sigma)t = r(\sigma \times t)$, (iv) $(\rho \square \sigma)t = \rho \times (\sigma \times t)$, (v) $(rs) \times \tau = r(s \times \tau)$, (vi) $(\rho \times s) \times \tau = \rho \times (s \times \tau)$, (vii) $(r \times \sigma) \times \tau = r(\sigma \square \tau)$, (viii) $(\rho \square \sigma) \times \tau = \rho \times (\sigma \square \tau)$. Indeed, by expanding $(RS)T$ and $R(ST)$, we observe that associativity is equivalent to the relation

$$
\begin{aligned}
&(rs)t + (\rho \times s)t + (r \times \sigma)t + (\rho \square \sigma)t + (rs) \times \tau \\
&\qquad + (\rho \times s) \times \tau + (r \times \sigma) \times \tau + (\rho \square \sigma) \times \tau \\
&= r(st) + \rho \times (st) + r(\sigma \times t) + \rho \times (\sigma \times t) + r(s \times \tau) \\
&\qquad + \rho \times (s \times \tau) + r(\sigma \square \tau) + \rho \times (\sigma \square \tau)
\end{aligned} \tag{11}
$$

for all $r, s, t, \rho, \sigma, \tau$. The eight given conditions are certainly sufficient. By considering successively each of the following special cases in (11), the correspondingly numbered condition is shown to be necessary: (i) $\rho = \sigma = \tau = \epsilon$, (ii) $r = z$, $\sigma = \tau = \epsilon$, (iii) $s = z$, $\rho = \tau = \epsilon$, (iv) $r = s = z$, $\tau = \epsilon$, (v) $t = z$, $\rho = \sigma = \epsilon$, (vi) $r = t = z$, $\sigma = \epsilon$, (vii) $s = t = z$, $\rho = \epsilon$, (viii) $r = s = t = z$. Note that associativity of the ring $\mathfrak{S}$ is essential for an associative cluster $\mathfrak{L}$.

A necessary and sufficient set of conditions that the element $F = \{f, \phi\} \in \mathfrak{L}$ should belong to the annihilator ideal $\mathfrak{A}$ is that $fr + \phi \times r = f \times \rho + \phi \square \rho = rf + r \times \phi = \rho \times f + \rho \square \phi = z$ for all $r, \rho$. The sufficiency is apparent from the definition of the product of two elements. The necessity follows from the demands that $F\{r, \epsilon\} = F\{z, \rho\} = \{r, \epsilon\}F = \{z, \rho\}F = 0$. The simpler set of conditions, namely $fr = rf = \phi \times r = r \times \phi = f \times \rho = \rho \times f = \phi \square \rho = \rho \square \phi = z$ for all $r, \rho$, is a sufficient set, but not necessary (cf. Example 5). Nor is it necessary that $f$ be an annihilator in $\mathfrak{S}$.

11. Our concern now is with multiplicative powers of an element of a

cluster. We confine our attention to the special case in which the cluster $\mathfrak{L}$ is associative and commutative. However we allow $\mathfrak{S}$ to satisfy the generalized hypothesis of §8. If $j \geqq 2$ and $0 \leqq i \leqq j$, then $i$ elements each equal to $\tau \in \Gamma$ and $j-i$ elements each equal to $t \in \mathfrak{S}$ may, in a variety of ways, be combined to form an element $v \in \mathfrak{S}$ by $j-1$ successive operations of one or more of the following types: multiplication in $\mathfrak{S}$ or any operation described in (IV), (V), or (VI). As a consequence of the associativity and commutativity, all such elements $v$ are equal to $v_0 = (\cdots((tt\cdots t \times \tau)\times\tau)\times\cdots)\times\tau$ if $i<j$ or to $v_0 = (\cdots((\tau \square \tau \times \tau)\times\tau)\times\cdots)\times\tau$ if $i=j$; in each case we abbreviate $v_0$ by $t^{j-i}\times^i\tau$. With such an abbreviated notation, we may express, in a form reminiscent of the binomial theorem expansion, the first component of a power of the element $T=\{t, \tau\}$; thus, $T^j = \{\sum_{i=0}^{j} C_{j,i} t^{j-i}\times^i\tau, \epsilon\}$ whenever $j \geqq 2$. Our assertion is easily established by an induction proof, which we omit since it is essentially a replica of the proof of the binomial theorem.

12. Further study of the construction technique based on §3 involves complications in generality so that the results seem more cumbersome than valuable. We find it therefore desirable to modify the necessary and sufficient set of conditions thus far discussed. By inserting an additional restriction into the set, we lose the necessity but acquire a set of conditions which are sufficient for constructing clusters and which may be diversely illustrated with examples. The extra restriction which we select is designed to make the first component $t$ in the sum $\{r, \rho\}+\{s, \sigma\} = \{t, \tau\}$ independent of the element $\sigma$. In other words, the mappings $g(\rho, \sigma \mid x)$ postulated in (I) should not depend upon $\sigma$. The notation may be simplified by defining $x_\rho = g(\rho, \epsilon \mid x)$ for all $x \in \mathfrak{S}$ and all $\rho \in \Gamma$. We now phrase our restriction formally as follows:

(XV) $$g(\rho, \sigma \mid x) = x_\rho \qquad \text{for all } x, \rho, \sigma.$$

The consequences of (XV) are quite extensive. First, (7) may be rewritten as follows:

(12) $$z_\sigma = z \qquad \text{for all } \sigma.$$

Second, we have observed that, given $t, \rho, \tau$, the simultaneous equations (9), or, in the new notation,

(13) $$x_\rho = t, \qquad \gamma(x \mid \rho, \xi) = \tau,$$

possess unique solution for $x$ and $\xi$. Now however the first equation is independent of $\xi$; thus, for each $\rho \in \Gamma$, the mapping $x \to x_\rho$ is a one-to-one mapping of $\mathfrak{S}$ *upon* itself. Next, if $r, \rho, \tau$ are arbitrarily given, then (13) with $t = r_\rho$ demonstrates that the equation $\gamma(r \mid \rho, \xi) = \tau$ is solvable uniquely for $\xi$. This statement, together with the third paragraph of §5, shows that for each $r \in \mathfrak{S}$, the functional relationship $\gamma(r \mid \xi, \eta) = \zeta$ describes a quasigroup in $\Gamma$. In particular, the quasigroup induced by the element $z$ is a group. Before verifying the associativity, we introduce an abbreviated notation suggestive of a

multiplicative operation in $\Gamma$, namely $\rho\sigma = \gamma(z|\rho, \sigma)$ for all $\rho, \sigma$. Then $(\rho\sigma)\tau = \gamma(z|\gamma(z|\rho, \sigma), \tau) = \gamma(z+z_\sigma|\rho, \gamma(z|\sigma, \tau)) = \gamma(z|\rho, \sigma\tau) = \rho(\sigma\tau)$ by use of (X) and (12). Henceforth, then, we shall consider the set $\Gamma$ to be a multiplicative group with the operation denoted by $\rho\sigma$. It should be noted that (VIII) and (8) show that $\epsilon$ is the two-sided identity of the group $\Gamma$. Another simplification in notation is defined by $s\rho = \gamma(s|\rho, \epsilon)$ for all $s, \rho$. Consequently, for each $s \in \mathfrak{S}$, the mapping $\rho \to s\rho$ is a one-to-one mapping of $\Gamma$ upon itself. In terms of the multiplication in the group $\Gamma$, we now have $\gamma(r|\rho, \sigma) = (r\rho)\sigma$ for all $r, \rho, \sigma$; indeed, (12), (VIII), (X) give $\gamma(r|\rho, \sigma) = \gamma(r+z_\epsilon|\rho, \gamma(z|\epsilon, \sigma)) = \gamma(z|\gamma(r|\rho, \epsilon), \sigma) = \gamma(z|r\rho, \sigma) = (r\rho)\sigma$. We customarily omit the parentheses and write $r\rho\sigma$ instead of $(r\rho)\sigma$. Equation (8) becomes

$$z\sigma = \sigma \qquad \text{for all } \sigma. \tag{14}$$

In (IX), we set $s = z$, simplify with the aid of (12), and obtain $t_{\rho\sigma} = (t_\sigma)_\rho$ for all $t, \rho, \sigma$. In (IX), we set $\sigma = \epsilon$, utilize (VII), and obtain $s_\rho + t_{s\rho} = (s+t)_\rho$ for all $s, t, \rho$. In (X), we set $s = z$ and $\tau = \epsilon$ to deduce that $t(\rho\sigma) = (t_\sigma\rho)(t\sigma)$ for all $t, \rho, \sigma$. In (X), we set $\sigma = \epsilon = \tau$ and use (VII) and (VIII) to deduce that $t(s\rho) = (s+t)\rho$ for all $s, t, \rho$.

For our later work, it will be convenient to collect together, with the simplified notation, a set of postulates equivalent to the set (I) through (XV) inclusive.

13. Let the (non-associative) ring $\mathfrak{S}$ with elements $r, s, t, \cdots$, be given; denote the zero element by $z$. Let the multiplicative group $\Gamma$ with elements $\rho, \sigma, \tau, \cdots$, be given; denote the identity element by $\epsilon$. Let the ring $\mathfrak{S}$ and the group $\Gamma$ be subject to the following postulates, but otherwise arbitrary.

(I′) Every element $\rho \in \Gamma$ induces a one-to-one mapping of $\mathfrak{S}$ upon itself, denoted by $r \to r_\rho$.

(II′) Every element $r \in \mathfrak{S}$ induces a one-to-one mapping of $\Gamma$ upon itself, denoted by $\rho \to r\rho$.

(IV′) Same as (IV).

(V′) Same as (V).

(VI′) Same as (VI).

The remaining postulates are valid for all $r, s, t, \rho, \sigma, \tau$.

$$(s+t)_\rho = s_\rho + t_{s\rho}. \tag{IX′}$$

$$(t_\sigma)_\rho = t_{\rho\sigma}. \tag{IX″}$$

$$s(\rho\sigma) = (s_\sigma\rho)(s\sigma). \tag{X′}$$

$$t(s\rho) = (s+t)\rho. \tag{X″}$$

$$rt_\sigma + r \times (t\sigma\tau) = rt + r \times \sigma + r \times \tau. \tag{XI′}$$

$$\rho \times t_\sigma + \rho \square (t\sigma\tau) = \rho \times t + \rho \square \sigma + \rho \square \tau. \tag{XII′}$$

$$s_\rho t + (s\rho\sigma) \times t = st + \rho \times t + \sigma \times t. \tag{XIII′}$$

(XIV′) $$s_\rho \times \tau + (s\rho\sigma) \square \tau = s \times \tau + \rho \square \tau + \sigma \square \tau.$$

THEOREM 2. *The set of postulates of* §3 *with* (XV) *adjoined is equivalent to the set just enunciated in* §13.

That the earlier set implies the latter has already been shown. For the most part, the converse will be left to the reader. We shall however indicate proofs of the analogs of (VII) and (VIII), namely:

(15) $$s_\epsilon = s \qquad \text{for all } s,$$

(16) $$s\epsilon = \epsilon \qquad \text{for all } s.$$

Postulates (I′) and (IX″) prove (15): the elements $t_\epsilon$ exhaust $\mathfrak{S}$, and $(t_\epsilon)_\epsilon = t_{\epsilon\epsilon} = t_\epsilon$. Equation (16) is a consequence of the group property in $\Gamma$, of (X′), and of (15): $s\epsilon = s(\epsilon\epsilon) = (s_\epsilon\epsilon)(s\epsilon) = (s\epsilon)(s\epsilon)$.

14. The set of primed postulates therefore suffices to permit the construction of a cluster $\mathfrak{L}$ whose elements are couples and in which addition is given by the rule $\{r, \rho\} + \{s, \sigma\} = \{r + s_\rho, s\rho\sigma\}$. We investigate further the set $\mathfrak{G}$ (§7) of elements having the form $\{z, \mu\}$. Since $\{z, \mu\} + \{z, \mu'\} = \{z + z\mu, z\mu\mu'\} = \{z, \mu\mu'\}$, the mapping $\{z, \mu\} \to \mu$ demonstrates that the set $\mathfrak{G}$ forms an additive group which is isomorphic to the multiplicative group $\Gamma$.

THEOREM 3. *Given a ring* $\mathfrak{S}$ *and a group* $\Gamma$, *the set of conditions in* §13 *is both necessary and sufficient for the construction of a cluster* $\mathfrak{L}$ *possessing a subcluster* $\mathfrak{M}$ *and an additive subgroup* $\mathfrak{G}$ *such that* (i) $\mathfrak{M}$ *is isomorphic to the given ring* $\mathfrak{S}$, (ii) $\mathfrak{M}$ *contains the derived ring* $\mathfrak{R}$ *of* $\mathfrak{L}$, (iii) *the elements of* $\mathfrak{G}$ *constitute a complete system of representative elements of the additive right cosets of* $\mathfrak{M}$, (iv) *the system* $\mathfrak{G}$ *under addition is isomorphic to the given group* $\Gamma$.

The sufficiency has already been shown; the necessity, analogous to the discussion of §2, is left to the reader.

Again the system $\mathfrak{S}$ in Theorem 3 may be generalized as described in §8.

COROLLARY. *Given two groups* $\Sigma$ *and* $\Gamma$, *then the additive portion of the postulates of* §13—*namely*, (I′), (II′), (IX′), (IX″), (X′), (X″)—*is a necessary and sufficient set of conditions for the construction of a group* $\Lambda$ *containing a subgroup* $\Sigma'$ *isomorphic to* $\Sigma$ *and a subgroup* $\Gamma'$ *isomorphic to* $\Gamma$ *such that the elements of* $\Gamma'$ *constitute a complete system of representative elements of the right cosets of* $\Sigma'$.

For the proof, compare Theorem 3 and §§8, 9.

In the cluster $\mathfrak{L}$, since $\mathfrak{M} \cong \mathfrak{S}$ and $\mathfrak{G}^+ \cong \Gamma$, we note that $-\{m, \epsilon\} = \{-m, \epsilon\}$ and $-\{z, \mu\} = \{z, \mu^{-1}\}$. Therefore, if $\omega = \rho^{-1}$, the solution (§5) of the equation $\{z, \rho\} + X = \{t, \epsilon\}$ shows that the (unique) solution $x \in \mathfrak{S}$ of the equation $x_\rho = t$ is $x = t_\omega$. Thus, for each $\rho \in \Gamma$, the inverse of the mapping $r \to r_\rho$ is the corresponding mapping induced by $\rho^{-1}$. Similarly the solution (§5) of the

equation $Y+\{r, \epsilon\}=\{z, \tau\}$ shows that the (unique) solution $\eta\in\Gamma$ of the equation $r\eta=\tau$ is $\eta=(-r)\tau$. Hence the inverse of the mapping $\rho\to r\rho$ is the corresponding mapping induced by $-r$.

For reference, we cite the following relations among the components of $R=\{r, \rho\}$ and its negative $N=\{n, \nu\}=-R$; each equation follows from the definition of $N$ or from the preceding paragraph.

(17) $$n = (-r)_\omega \quad \text{or} \quad r + n_\rho = z, \qquad \text{where } \omega = \rho^{-1};$$

(18) $$\nu = (n\rho)^{-1} \quad \text{or} \quad n\rho\nu = \epsilon;$$

$$n = -(r_\nu) \quad \text{or} \quad n + r_\nu = z;$$

(19) $$\nu = (-r)\rho^{-1} \quad \text{or} \quad r\nu = \rho^{-1}.$$

Immediate application of (XI'), (XIII') (XII'), (XIV') yields the following results for all $t, \rho, \sigma, \tau$:

(20) $$t\times\rho + t\times\sigma = t\times(\rho\sigma);$$

(21) $$\rho\times t + \sigma\times t = (\rho\sigma)\times t;$$

(22) $$\rho\square\sigma + \rho\square\tau = \rho\square(\sigma\tau);$$

(23) $$\rho\square\tau + \sigma\square\tau = (\rho\sigma)\square\tau.$$

A derivation of (20) will indicate the method of verifying the others. By (12), (14), (XI'), we have $t\times(\rho\sigma)=tz_\rho+t\times(z\rho\sigma)=tz+t\times\rho+t\times\sigma=t\times\rho+t\times\sigma$. An induction proof based on (22) and (23) reveals that $(\rho_1\rho_2\cdots\rho_h)\square(\sigma_1\sigma_2\cdots\sigma_k)=\sum_{i=1}^{h}\sum_{j=1}^{k}(\rho_i\square\sigma_j)$ for all $\rho_i\in\Gamma$, all $\sigma_j\in\Gamma$, all $h\geqq 1$, all $k\geqq 1$.

Corollaries of the preceding paragraph are the following relations, valid for all $t, \rho, \sigma, \tau$: (i) $t\times(\rho\sigma)=t\times(\sigma\rho)$, (ii) $(\rho\sigma)\times t=(\sigma\rho)\times t$, (iii) $\rho\square(\sigma\tau)=\rho\square(\tau\sigma)$, (iv) $(\rho\sigma)\square\tau=(\sigma\rho)\square\tau$. The proofs are immediate, since abelian addition in $\mathfrak{S}$ allows the terms in the left member of each of (20), (21), (22), (23) to be permuted.

The decomposition (10), which we may here, on the basis of Theorem 3, symbolize by $\mathfrak{L}=\mathfrak{M}+\mathfrak{G}$, possesses some of the properties belonging to a direct-sum decomposition, but neither $\mathfrak{M}$ nor $\mathfrak{G}$ need be an ideal. In the next two paragraphs, we inquire about the possibility that $\mathfrak{G}$ may be an ideal; in §15, a similar inquiry is made concerning $\mathfrak{M}$.

A necessary and sufficient set of conditions that any subset $\mathfrak{J}$ of $\mathfrak{G}$ be an ideal in $\mathfrak{L}$ is that $\mathfrak{J}$ should be a normal subgroup in $\mathfrak{L}$ and be contained in $\mathfrak{A}$. The sufficiency follows from §I.6, and the first part of the necessity from §I.5. To complete the proof, let $J$ and $R$ be any elements in $\mathfrak{J}$ and $\mathfrak{L}$, respectively. Both products, $JR$ and $RJ$, are in $\mathfrak{R}$ and also, by the ideal property, in $\mathfrak{J}$. But $\mathfrak{R}\cap\mathfrak{J}\subseteq\mathfrak{M}\cap\mathfrak{G}=(0)$, whence $J$ is an annihilator.

In particular, in order that $\mathfrak{G}$ be an ideal, not only must the subgroup $\mathfrak{G}$ be normal but also it is necessary that $\{z, \mu\}\in\mathfrak{A}$ for all $\mu\in\Gamma$.

15. We consider in $\mathfrak{S}$ the subset $\mathfrak{E}$ of all elements $q$ such that $q\rho=\rho$ for all $\rho\in\Gamma$. Let $q_1$ and $q_2$ be any two elements of $\mathfrak{E}$; then $q_1\rho=q_2\rho$ for all $\rho$; hence (§14) $\rho=(-q_1)(q_2\rho)=(q_2-q_1)\rho$ for all $\rho$; the set $\mathfrak{E}$ is a (normal) subgroup in $\mathfrak{S}$. In the additive group of $\mathfrak{S}$, therefore, $x\equiv y \bmod \mathfrak{E}$ if and only if $x\rho=y\rho$ for every $\rho\in\Gamma$. If $q$ is any element of $\mathfrak{E}$ and $\mu$ any element of $\Gamma$, then $q_\mu\in\mathfrak{E}$; for, (X′) and the hypothesis that $q\in\mathfrak{E}$ yield $\rho\mu=q(\rho\mu)=(q_\mu\rho)(q\mu)=(q_\mu\rho)\mu$, hence $q_\mu\rho=\rho$ for all $\rho$. The (normal) subgroup $\mathfrak{E}$ is therefore admissible under every mapping of the type $q\to q_\mu$.

The following result is significant: $(q+r)_\sigma=q_\sigma+r_\sigma$ for all $q\in\mathfrak{E}$, all $r\in\mathfrak{S}$, all $\sigma\in\Gamma$. Proof: $(q+r)_\sigma=q_\sigma+r_{q\sigma}=q_\sigma+r_\sigma$. This statement is of course stronger than the fact that $x\equiv y \bmod \mathfrak{E}$ implies $x_\sigma\equiv y_\sigma \bmod \mathfrak{E}$. Since $\mathfrak{S}$ is a ring, we deduce immediately that $q_\sigma=q_{r\sigma}$ for all $q\in\mathfrak{E}$, all $r\in\mathfrak{S}$, all $\sigma\in\Gamma$. Proof: $q_\sigma+r_\sigma=(q+r)_\sigma=(r+q)_\sigma=r_\sigma+q_{r\sigma}=q_{r\sigma}+r_\sigma$. Consequently, every mapping $s\to s_\tau$, where $\tau$ has the form $(r\sigma)^{-1}\sigma$ or the form $\sigma^{-1}(r\sigma)$, is an identity mapping for the subgroup $\mathfrak{E}$. Finally, for every $\rho$, the mapping $q\to q_\rho$, considered as a transformation defined in $\mathfrak{E}$, is an automorphism of $\mathfrak{E}$. Since the inverse of each mapping $r\to r_\rho$ defined in $\mathfrak{S}$ is a mapping of the same type (§14) and since each of these mappings transforms $\mathfrak{E}$ into itself, the assertion follows from the first sentence of this paragraph.

Postulates (XI′), (XIII′), (XII′), (XIV′), paired respectively with (20), (21), (22), (23), show that, if $q$ and $\mu$ are any elements of $\mathfrak{E}$ and $\Gamma$ respectively, then for all $r\in\mathfrak{S}$ and all $\rho\in\Gamma$, we have

$$(24)\qquad r(q-q_\mu)=z;\quad (q-q_\mu)r=z;\quad \rho\times(q-q_\mu)=z;\quad (q-q_\mu)\times\rho=z.$$

The first two of these relations state that every element of the form $q-q_\mu$ is an annihilator in the ring $\mathfrak{S}$.

Although both $\mathfrak{M}$ and $\mathfrak{N}$ have the ideal property in $\mathfrak{L}$, we must not expect either of them to be an ideal, since an ideal is an invariant subgroup. We examine the question, what subgroups of $\mathfrak{M}$ may be normal in $\mathfrak{L}$? If we denote by $\mathfrak{Q}$ the subset of $\mathfrak{M}$ consisting of all elements $Q=\{q,\ \epsilon\}$ with $q\in\mathfrak{E}$, an answer to our question is given in Theorem 4.

THEOREM 4. *The subgroup $\mathfrak{Q}$ is normal in $\mathfrak{L}$, and every subset of $\mathfrak{M}$ which is an invariant subgroup of $\mathfrak{L}$ is a subgroup of $\mathfrak{Q}$.*

**Proof.** We first suppose that $\mathfrak{Q}'$ is any subgroup of $\mathfrak{M}$ invariant in $\mathfrak{L}$ and show that necessarily $\mathfrak{Q}'\subseteq\mathfrak{Q}$. Computation reveals that the conjugate of the element $M=\{m,\ \epsilon\}\in\mathfrak{M}$ by the element $G=\{z,\ \rho\}$ is $G+M-G=\{m_\rho,\ (m\rho)\rho^{-1}\}$. If $M\in\mathfrak{Q}'$, then $(G+M-G)\in\mathfrak{Q}'$ for all $G$, whence $(m\rho)\rho^{-1}=\epsilon$ for all $\rho$. Thus $m\in\mathfrak{E}$ and $M\in\mathfrak{Q}$.

On the other hand, the properties possessed by the set $\mathfrak{E}$ show that $\mathfrak{Q}$ itself is normal in $\mathfrak{L}$. Recalling (§§4, 14) the notation $-R=-\{r,\rho\}=\{n,\nu\}$ and utilizing the previous results of the present section together with (17) and (18), we find, for all $Q\in\mathfrak{Q}$ and all $R\in\mathfrak{L}$, that $R+Q-R=\{r+(q+n)_\rho,$

$(q+n)\rho\cdot\nu\} = \{r+q_\rho+n_\rho,\ n\rho\nu\} = \{q_\rho,\ \epsilon\} \in \mathfrak{Q}$.

The subgroup $\mathfrak{Q}'$ of $\mathfrak{Q}$, invariant in $\mathfrak{L}$, will be an ideal if and only if, for all $Q = \{q,\ \epsilon\} \in \mathfrak{Q}'$, the elements $\{qr,\ \epsilon\}$, $\{sq,\ \epsilon\}$, $\{q\times\rho,\ \epsilon\}$, $\{\sigma\times q,\ \epsilon\}$ belong to $\mathfrak{Q}'$ for all $r, s, \rho, \sigma$.

As a corollary, each of the following is a necessary and sufficient condition that the ring $\mathfrak{M}$ be an ideal: (i) $\mathfrak{M} = \mathfrak{Q}$, (ii) $\mathfrak{E} = \mathfrak{S}$, (iii) every mapping $\rho \to r\rho$ is the identity transformation.

§§10 and 6 and equations (24) tell us that, for all $\mu \in \Gamma$, if $q \in \mathfrak{E}$, then $\{q,\ \epsilon\} \equiv \{q_\mu,\ \epsilon\}$ mod $\mathfrak{A}$ or $\{q-q_\mu,\ \epsilon\} \in (\mathfrak{A}\cap\mathfrak{Q})$. Thus a necessary condition that $\mathfrak{M}$ be an ideal is that $\{r-r_\rho,\ \epsilon\} \in (\mathfrak{M}\cap\mathfrak{A})$ for all $r \in \mathfrak{S}$, all $\rho \in \Gamma$. In particular, if $\mathfrak{M}$ were an ideal and if $\mathfrak{M}\cap\mathfrak{A} = (0)$, then each mapping described in (I′) and (II′) could be only an identity mapping.

16. This section will discuss the multiples of an arbitrary element $R \in \mathfrak{L}$. Again we use the summation notation $\sum^j R$ to designate the $j$th multiple of $R$, for any rational integer $j$. Explicitly writing the first few multiples of $R = \{r, \rho\}$, we obtain

$$
\begin{aligned}
&\textstyle\sum^0 R = \{z, \epsilon\}, && \textstyle\sum^1 R = \{r, \rho\},\\
&\textstyle\sum^2 R = \{r + r_\rho, r\rho\rho\}, && \textstyle\sum^3 R = \{r + r_\rho + r_{r\rho\rho}, r(r\rho\rho)\rho\},\\
&\textstyle\sum^4 R = \{r + r_\rho + r_{r\rho\rho} + r_{r(r\rho\rho)\rho},\ r(r(r\rho\rho)\rho)\rho\}.
\end{aligned} \tag{25}
$$

In order to shorten the notation, we introduce the following two functions of the three independent variables $r \in \mathfrak{S}$, $\rho \in \Gamma$, and the rational integer $j$. The function $w[r, \rho, j]$, with values in $\mathfrak{S}$, is defined recursively:

$$
\begin{aligned}
w[r, \rho, 0] &= z,\\
w[r, \rho, j+1] &= r + (w[r, \rho, j])_\rho \qquad \text{for all } r, \rho, j.
\end{aligned} \tag{26}
$$

The function $\psi[r, \rho, j]$ is defined in $\Gamma$ recursively:

$$
\begin{aligned}
\psi[r, \rho, 0] &= \epsilon,\\
\psi[r, \rho, j+1] &= r\psi[r, \rho, j]\cdot\rho \qquad \text{for all } r, \rho, j.
\end{aligned} \tag{27}
$$

Observe that both functions are defined recursively, not only for $j \geqq 0$, but also for negative values of $j$, since $x$ and $\xi$ are uniquely determined when $x_\rho$ and $r\xi$, respectively, are given. Indeed, letting $-R = -\{r, \rho\} = \{n, \nu\}$, we obtain from the fourth and third paragraphs of §5 the two following results, valid for all $r, \rho, j$:

$$n + (w[r, \rho, j+1])_\nu = w[r, \rho, j], \tag{28}$$

$$n\psi[r, \rho, j+1]\cdot\nu = \psi[r, \rho, j]. \tag{29}$$

We desire to show, by induction on $j$, that the functions $w[r, \rho, j]$ and $\psi[r, \rho, j]$ are the first and second components of $\sum^j\{r, \rho\}$, respectively; that is,

$$\sum^{j}\{r, \rho\} = \{w[r, \rho, j], \psi[r, \rho, j]\} \qquad \text{for all } r, \rho, j. \tag{30}$$

We remark that in our proofs we shall frequently write merely $w[j]$ and $\psi[j]$ instead of $w[r, \rho, j]$ and $\psi[r, \rho, j]$, respectively, if there is no possibility of ambiguity.

To prove (30), let $r \in \mathfrak{S}$ and $\rho \in \Gamma$ be chosen arbitrarily. Then $\sum^{0} R = 0 = \{z, \epsilon\} = \{w[0], \psi[0]\}$. Suppose the result true for $j$; then $\sum^{j+1} R = \sum^{j} R + R = \{w[j], \psi[j]\} + \{r, \rho\} = \{w[j] + r_{\psi[j]}, r\psi[j] \cdot \rho\} = \{w[j] + r_{\psi[j]}, \psi[j+1]\}$. Also, $\sum^{j+1} R = R + \sum^{j} R = \{r, \rho\} + \{w[j], \psi[j]\} = \{r + (w[j])_{\rho}, w[j]\rho \cdot \psi[j]\} = \{w[j+1], w[j]\rho \cdot \psi[j]\}$. Hence (30) holds for all $j \geqq 0$. The case $j < 0$ remains to be considered. Suppose the result true for $j+1$; then, using (29), $\sum^{j} R = \sum^{j+1} R - R = \{w[j+1], \psi[j+1]\} + \{n, \nu\} = \{w[j+1] + n_{\psi[j+1]}, n\psi[j+1] \cdot \nu\} = \{w[j+1] + n_{\psi[j+1]}, \psi[j]\}$. Also, using (28), $\sum^{j} R = -R + \sum^{j+1} R = \{n, \nu\} + \{w[j+1], \psi[j+1]\} = \{n + (w[j+1])_{\nu}, w[j+1]\nu \cdot \psi[j+1]\} = \{w[j], w[j+1]\nu \cdot \psi[j+1]\}$. Therefore the assertion is true for all $j < 0$ and hence for every integer $j$ and for all $r$, $\rho$. The recursive definitions in (26) and (27) completely characterize the components of $\sum^{j}\{r, \rho\}$.

Our induction steps were written in detail because they prove, as by-products, the following relations, valid for all $r$, $\rho$, $j$:

$$w[r, \rho, j+1] = w[r, \rho, j] + r_{\psi[r, \rho, j]}; \tag{31}$$

$$\psi[r, \rho, j+1] = w[r, \rho, j]\rho \cdot \psi[r, \rho, j]; \tag{32}$$

$$w[r, \rho, j] = w[r, \rho, j+1] + n_{\psi[r, \rho, j+1]};$$

$$\psi[r, \rho, j] = w[r, \rho, j+1]\nu \cdot \psi[r, \rho, j+1]. \tag{33}$$

Examination of the explicitly written multiples in (25) makes plausible the following identity:

$$w[r, \rho, j] = \sum_{i=0}^{j-1} r_{\psi[r, \rho, i]} \qquad \text{for all } r, \rho, \text{ all } j \geqq 1. \tag{34}$$

Our conjecture is easily established by induction on $j$. Let $r \in \mathfrak{S}$ and $\rho \in \Gamma$. be selected arbitrarily. When $j = 1$, both members of (34) are equal to $r$. Suppose the assertion true for the value $j$; then, by (31),

$$w[r, \rho, j+1] = w[j] + r_{\psi[j]} = \sum_{i=0}^{j-1} r_{\psi[i]} + r_{\psi[j]} = \sum_{i=0}^{j} r_{\psi[i]}.$$

The assertion is true for $j+1$; the induction is complete.

COROLLARY. *For all $r$, $\rho$, all $j \geqq 1$,*

$$\left( \sum_{i=0}^{j-1} r_{\psi[r, \rho, i]} \right)_{\rho} = \sum_{i=1}^{j} r_{\psi[r, \rho, i]}.$$

*For, by successive applications of* (34), (26), (34), (27), (15),

$$r + \left( \sum_{i=0}^{j-1} r_{\psi[i]} \right)_\rho = r + (w[j])_\rho = w[j+1] = \sum_{i=0}^{j} r_{\psi[i]}$$

$$= r_\epsilon + \sum_{i=1}^{j} r_{\psi[i]} = r + \sum_{i=1}^{j} r_{\psi[i]}.$$

17. *Special Case* A. We shall illustrate the theory of this chapter by considering two special cases and a few simple examples. Let the ring $\mathfrak{S}$ be an arbitrary not-trivial ring and let the group $\Gamma$ be an arbitrary not-commutative group. We specialize all the mappings described in (I′) and (II′) to be identity mappings, that is, $r_\rho = r$ and $r\rho = \rho$ for all $r$, $\rho$; all left-operator-products, all right-operator-products, all combination-elements described in (IV′), (V′), or (VI′) to be zero, that is, $\rho \times r = r \times \rho = \rho \square \sigma = z$ for all $r$, $\rho$, $\sigma$. The remaining postulates of §13 are trivially satisfied. The construction of §14 yields a not-trivial, not-abelian (§10) cluster $\mathfrak{L}$ whose rules of addition and multiplication are, respectively, $\{r, \rho\} + \{s, \sigma\} = \{r+s, \rho\sigma\}$ and $\{r, \rho\} \cdot \{s, \sigma\} = \{rs, \epsilon\}$.

The cluster $\mathfrak{L}$ is associative if and only if $\mathfrak{S}$ is associative; $\mathfrak{L}$ is commutative if and only if $\mathfrak{S}$ is commutative. The set $\mathfrak{M}$ (§7), coinciding with the set $\mathfrak{Q}$ (§15), is the kernel of the homomorphic mapping $\{r, \rho\} \to \{z, \rho\}$ of $\mathfrak{L}$ upon the set $\mathfrak{G}$ (§14). On the other hand, $\mathfrak{G}$ is the kernel of the homomorphic mapping $\{r, \rho\} \to \{r, \epsilon\}$ of $\mathfrak{L}$ upon $\mathfrak{M}$. Since both $\mathfrak{M}$ and $\mathfrak{G}$ are ideals, we may write a direct-sum decomposition: $\mathfrak{L} = \mathfrak{M} \oplus \mathfrak{G}$. Regardless of the element $\rho \in \Gamma$, the element $F = \{f, \rho\}$ belongs to $\mathfrak{A}$ (§10) if and only if $f$ is an annihilator in $\mathfrak{S}$. Hence $\mathfrak{G} \subseteq \mathfrak{A}$; the equality holds if and only if $\mathfrak{S}$ has no not-zero annihilators. Since the commutator of any pair of elements $R$ and $S$ is $\{z, \rho^{-1}\sigma^{-1}\rho\sigma\}$, an element $C$ belongs to the commutator ideal $\mathfrak{C}$ if and only if both $C \in \mathfrak{G}$ and the second component of $C$ belongs to the commutator subgroup of $\Gamma$. For every rational integer $j$, we have $\sum^j \{r, \rho\} = \{\sum^j r, \rho^j\}$; in particular, $-\{r, \rho\} = \{-r, \rho^{-1}\}$. If the element $t \in \mathfrak{S}$ generates multiplicatively a semigroup, then $\{t, \tau\}^j = \{t^j, \epsilon\}$ for all $\tau \in \Gamma$ and all $j \geqq 2$.

18. *Example* 3. As a specific example of Special Case A, let $\mathfrak{S}$ be the field of complex numbers and let $\Gamma$ be the group of nonsingular second order (square) matrices with complex number elements under the group operation of matrix multiplication. Typical operations in this cluster are:

$$\left\{2i, \begin{pmatrix} 1 & i \\ -i & -1 \end{pmatrix}\right\} + \left\{7^{1/2}, \begin{pmatrix} 6i & 4 \\ 1/2 & 0 \end{pmatrix}\right\} = \left\{2i + 7^{1/2}, \begin{pmatrix} 13i/2 & 4 \\ 11/2 & -4i \end{pmatrix}\right\}$$

while

$$\left\{7^{1/2}, \begin{pmatrix} 6i & 4 \\ 1/2 & 0 \end{pmatrix}\right\} + \left\{2i, \begin{pmatrix} 1 & i \\ -i & -1 \end{pmatrix}\right\} = \left\{7^{1/2} + 2i, \begin{pmatrix} 2i & -10 \\ 1/2 & i/2 \end{pmatrix}\right\},$$

and

$$\left\{2i, \begin{pmatrix} 1 & i \\ -i & -1 \end{pmatrix}\right\} \left\{7^{1/2}, \begin{pmatrix} 6i & 4 \\ 1/2 & 0 \end{pmatrix}\right\} = \left\{2\left(7^{1/2}\right)i, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\right\}$$

This cluster is associative and commutative. Its derived ring $\mathfrak{R}$ coincides with $\mathfrak{M} = \mathfrak{Q}$ and hence is isomorphic to the field $\mathfrak{S}$. Since $\mathfrak{S}$ has no proper divisors of zero, $\mathfrak{G} = \mathfrak{A}$. The cluster $\mathfrak{k}$ is the direct sum of its derived ring and its annihilator ideal: $\mathfrak{k} = \mathfrak{R} \oplus \mathfrak{A}$. The zero element is

$$\left\{0, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\right\},$$

while the element

$$\left\{1, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\right\}$$

is a multiplicative unit for the derived ring $\mathfrak{R}$.

19. *Special Case* B. We examine another special case of the theory of this chapter by allowing $\mathfrak{S}$ to be an arbitrary not-trivial ring and $\Gamma$ to be an arbitrary (commutative or not-commutative) group subject only to the requirement that the automorphism group of the group $\Gamma$ should contain a subgroup $\Delta$ (not the identity) which is a homomorphic image of the additive group of the ring $\mathfrak{S}$. Certainly $\Delta$ must be commutative. For each mapping (Postulate (II′)) of $\Gamma$ upon itself induced by an element $r \in \mathfrak{S}$, we select the automorphism of $\Gamma$ which is the image in $\Delta$ of $r$ under the homomorphic mapping of the additive group of $\mathfrak{S}$ upon $\Delta$. We choose each mapping described in (I′) to be the identity mapping, $r_\rho = r$ for all $r$, $\rho$; as in Special Case A, we select $\rho \times r = r \times \rho = \rho \square \sigma = z$ for all $r$, $\rho$, $\sigma$. Verification of the remaining postulates of §13 is immediate, since $r\rho$ is an automorphism of $\Gamma$ induced by $r$. The not-trivial cluster $\mathfrak{k}$ constructed by this method possesses the following rules of addition and multiplication: $\{r, \rho\} + \{s, \sigma\} = \{r+s, s\rho\sigma\}$ and $\{r, \rho\} \cdot \{s, \sigma\} = \{rs, \epsilon\}$. That the cluster $\mathfrak{k}$ is not-abelian (§10) has been guaranteed by the requirement that $\Delta$ contain at least one element other than the identity automorphism, for then there exist elements $r \in \mathfrak{S}$ and $\sigma \in \Gamma$ such that $r\sigma \neq \sigma$.

The cluster $\mathfrak{k}$ is associative if and only if $\mathfrak{S}$ is associative; $\mathfrak{k}$ is commutative if and only if $\mathfrak{S}$ is commutative. The set $\mathfrak{Q}$ (§15) is a proper subset of the set $\mathfrak{M}$ (§7), and hence $\mathfrak{M}$ is not an ideal. The set $\mathfrak{E}$ (§15), consisting of first components of elements of $\mathfrak{Q}$, forms the kernel of the homomorphic mapping of the additive group of $\mathfrak{S}$ upon $\Delta$. The ring $\mathfrak{M}$ is a homomorphic image of $\mathfrak{k}$ under the mapping $\{r, \rho\} \to \{r, \epsilon\}$; the kernel of the homomorphism is the ideal $\mathfrak{G}$ (§14). As in Special Case A, $\mathfrak{G} \subseteq \mathfrak{A}$, the equality holding if and only if $\mathfrak{S}$ has no not-zero annihilators; indeed, $\mathfrak{A}$ contains an element $F = \{f, \rho\}$ if and only if $f$ belongs to the annihilator ideal of $\mathfrak{S}$, regardless of the element $\rho \in \Gamma$. For each rational integer $j$, the function $w[r, \rho, j] = \sum^{j} r$

(§16). Equations (32) and (33), with the aid of (X″) and (19), enable us to write relations for the corresponding function $\psi[r, \rho, j]$: namely, $\psi[r, \rho, j+1] = (\sum i r)\rho \cdot \psi[r, \rho, j]$ and $\psi[r, \rho, j] = (\sum i r)\rho^{-1} \cdot \psi[r, \rho, j+1]$. The former is useful for $j \geqq 0$; the latter, for $j \leqq -1$. Respective examples are $\psi[r, \rho, 4] = (r+r+r)\rho \cdot (r+r)\rho \cdot r\rho \cdot \rho$ and $\psi[r, \rho, -3] = (-r-r-r)\rho^{-1} \cdot (-r-r)\rho^{-1} \cdot (-r)\rho^{-1}$. If the element $t \in \mathfrak{S}$ generates multiplicatively a semigroup, then $\{t, \tau\}^j = \{t^j, \epsilon\}$ for all $\tau \in \Gamma$ and all $j \geqq 2$.

20. *Example* 4. As a specific example of Special Case B, let $\mathfrak{S}$ be the ring of even rational integers and let $\Gamma$ be the cyclic group of order four, which we may conveniently express as the multiplicative group of fourth roots of unity. According as $s \in \mathfrak{S}$ is congruent 0 or 2 modulo 4, let the corresponding automorphism of $\Gamma$ be the identity or the mapping $i \to -i$. To illustrate the operations in the resulting cluster $\mathfrak{L}$, we offer

$$\{-2, i\} + \{6, 1\} = \{(-2) + 6, (-i)1\} = \{4, -i\},$$
$$\{6, 1\} + \{-2, i\} = \{6 + (-2), 1 \cdot i\} = \{4, i\},$$
$$\{-2, i\} \cdot \{6, 1\} = \{-12, 1\}.$$

Our illustrations demonstrate that $\mathfrak{L}$ is not-abelian; nevertheless, it is associative and commutative. We note that here $\Delta$ is the (whole) group of automorphisms of $\Gamma$. Modulo the annihilator ideal, which consists of the four elements $\{0, i^k\}$ with $k = 0, 1, 2, 3$, the difference cluster $\mathfrak{L} - \mathfrak{A}$ is isomorphic to the ring $\mathfrak{M}$ and to the ring $\mathfrak{S}$. Zero, that is, $\{0, 1\}$, and the element $\{0, -1\}$ form an ideal, the kernel of the homomorphism which maps each element $\{r, i^k\}$ upon the element $\{r, (-1)^k\}$; since the difference cluster modulo this ideal is abelian, the ideal contains (§I.6), and hence—consisting of only two elements—must coincide with, the commutator ideal $\mathfrak{C}$; thus $\mathfrak{C}$ is a proper subset of $\mathfrak{A}$. The derived ring $\mathfrak{R}$, coinciding with the set $\mathfrak{Q}$, consists of all elements $\{q, 1\}$ with $q \equiv 0 \bmod 4$; since $\mathfrak{Q}$ is an invariant subgroup, $\mathfrak{R}$ is an ideal (§I.7). Of note are the facts that $\mathfrak{R}$ is a proper subset of $\mathfrak{M}$ and that $\mathfrak{R}$ is not isomorphic to $\mathfrak{S}$. For no not-zero element $R \in \mathfrak{L}$ is the equation $RX = R$ solvable for $X$.

21. *Example* 5. We conclude the chapter by examination of another example, not an illustration of either special case, but rather an illustration of an extension of an integral domain by the infinite cyclic group. Let the ring $\mathfrak{S}$ be the integral domain of rational integers; let the group $\Gamma$ be the group of rational integers under the operation of addition. (Thus $\mathfrak{S}$ and $\Gamma$ have the same elements!) Let the mapping $r \to r_\rho$ be defined by $r_\rho = (-1)^\rho r$ for each $\rho$; for each $r \in \mathfrak{S}$, let the mapping (Postulate (II′)) of $\Gamma$ upon itself induced by $r$ transform each element $\rho \in \Gamma$ into the element $\rho + r - (-1)^\rho r$ of $\Gamma$; let each of the products $\rho \times r$, $r \times \rho$, and $\rho \square \sigma$ (Postulates (IV′), (V′), (VI′)) be ordinary products of rational integers, for all $r$, $\rho$, $\sigma$. Verification of the various postulates in §13 is a problem in computation, which we omit. The de-

mand of one-to-one mappings in (II′) requires the solution of the equation $\xi+s-(-1)^{\xi}s=\sigma$ for $\xi$ when $s$ and $\sigma$ are known; the solution, perhaps not apparent, as indicated in §14, is $\xi=\sigma-s+(-1)^{\sigma}s$. The rules of operation in $\mathfrak{L}$, then, are:

$$\{r,\rho\}+\{s,\sigma\}=\{r+(-1)^{\rho}s,\ \rho+\sigma+s-(-1)^{\rho}s\};$$

$$\{r,\rho\}\cdot\{s,\sigma\}=\{rs+\rho\cdot s+r\cdot\sigma+\rho\cdot\sigma,\ 0\}\quad\text{or}\quad\{(r+\rho)(s+\sigma),\ 0\}. \tag{35}$$

The cluster is associative and commutative.

Since $\{m,0\}=\{m,0\}\cdot\{1,0\}$, the derived ring $\mathfrak{R}$ coincides with the ring $\mathfrak{M}$ and is isomorphic to the integral domain $\mathfrak{S}$. But $\mathfrak{R}$ is not an ideal; indeed, since the image of $1\in\Gamma$, namely $1+r-(-1)r=1+2r$, under the mapping described in (II′), is never 1 unless $r=0$, we see that $\mathfrak{Q}$ contains only zero; hence no subgroup of $\mathfrak{M}$, except $\mathfrak{Q}$, is invariant in $\mathfrak{L}$.

Consider the mapping $\Phi$ of the cluster $\mathfrak{L}$ upon the rational integral domain $\mathfrak{S}$ defined by the equation $\Phi(R)=\Phi(\{r,\rho\})=r+\rho$. The rules of operation in $\mathfrak{L}$ immediately show that $\Phi$ is a homomorphism. The kernel of this homomorphism is the set of all elements $T$ for which $\Phi(T)=0$, thus elements of the form $\{t,\tau\}$ where $\tau=-t$. But this set, as shown by (35), is precisely the annihilator ideal. Consequently the difference cluster $\mathfrak{L}-\mathfrak{A}\cong\mathfrak{S}\cong\mathfrak{R}$. The intersection of $\mathfrak{R}$ and $\mathfrak{A}$ consists of the zero element alone. Every element $R=\{r,\rho\}\in\mathfrak{L}$ possesses a unique decomposition into the ordered sum of an element of $\mathfrak{R}$ and an element of $\mathfrak{A}$: $\{r,\rho\}=\{r+\rho,0\}+\{-\rho,\rho\}$. We symbolize this almost-direct-sum decomposition by writing $\mathfrak{L}=\mathfrak{R}+\mathfrak{A}$. This decomposition has more of the properties of a direct sum than the decomposition (§14) $\mathfrak{L}=\mathfrak{R}+\mathfrak{G}$, for $\mathfrak{G}$ is not an ideal while $\mathfrak{A}$ is. In contrast to Special Cases A and B, where we observed $\mathfrak{G}\subseteq\mathfrak{A}$, here $\mathfrak{A}\cap\mathfrak{G}=(0)$. The annihilator ideal is not abelian; for example, $\{1,-1\}+\{-2,2\}=\{3,-3\}$ while $\{-2,2\}+\{1,-1\}=\{-1,1\}$

Corresponding to each positive rational integer $d$, there exists an ideal in $\mathfrak{L}$, namely the set of all elements $T$ for which $\Phi(T)\equiv 0 \bmod d$. This ideal is the kernel of a homomorphism which maps $\mathfrak{L}$ upon the ring of rational integers reduced modulo $d$; each element $R\in\mathfrak{L}$ is mapped upon the residue class modulo $d$ which contains $\Phi(R)$.

Besides the infinitely many ideals cited in the preceding paragraph, we mention the ideal $\mathfrak{J}_2$ consisting of all elements $\{s,\sigma\}$ such that $\sigma\equiv 0 \bmod 2$. Addition in $\mathfrak{J}_2$ is componentwise: $\{s,\sigma\}+\{s',\sigma'\}=\{s+s',\sigma+\sigma'\}$. Since $\mathfrak{J}_2$ has additive group index two and since $\mathfrak{J}_2$ contains $\mathfrak{R}$ (§1.7), the difference cluster $\mathfrak{L}-\mathfrak{J}_2$ is the trivial ring with two elements.

Since $\mathfrak{L}-\mathfrak{J}_2$ is abelian, $\mathfrak{J}_2\supseteq\mathfrak{C}$; and thus the commutator ideal $\mathfrak{C}$ is contained in the intersection $\mathfrak{A}\cap\mathfrak{J}_2$, a set consisting of all elements $\{f,\phi\}$ for which $\phi=-f\equiv 0 \bmod 2$. On the other hand, $\mathfrak{A}\cap\mathfrak{J}_2\subseteq\mathfrak{C}$; for the commutator of $\{0,1\}$ and $\{1,0\}$, namely $\{2,-2\}$, additively generates the subgroup

$\mathfrak{A} \cap \mathfrak{J}_2$, as demonstrated by the componentwise addition in $\mathfrak{J}_2$. Thus $\mathfrak{C} = \mathfrak{A} \cap \mathfrak{J}_2$, and $\mathfrak{C}$ is a cyclic infinite subgroup.

The functions $w[r, \rho, j]$ and $\psi[r, \rho, j]$ (§16) in the present example may be written as follows:

$$w[r, \rho, j] = \begin{cases} jr, & \text{if } \rho \equiv 0 \bmod 2, \\ 0, & \text{if } j \not\equiv \rho \equiv 1 \bmod 2, \\ r, & \text{if } j \equiv \rho \equiv 1 \bmod 2; \end{cases}$$

$$\psi[r, \rho, j] = \begin{cases} j\rho, & \text{if } \rho \equiv 0 \bmod 2, \\ j(r+\rho), & \text{if } j \not\equiv \rho \equiv 1 \bmod 2, \\ j(r+\rho) - r, & \text{if } j \equiv \rho \equiv 1 \bmod 2. \end{cases}$$

Examination of these functions reveals a necessary and sufficient set of conditions that a not-zero element $R$ have positive order: namely, that both $\Phi(R) = 0$ and $\rho \equiv 1 \bmod 2$. Thus the set of not-zero elements with positive order is the set of all elements $\{f, \phi\}$ such that $\phi = -f \equiv 1 \bmod 2$, hence the set of all annihilators which do not belong to $\mathfrak{C}$. Each element in this set, moreover, has order two.

From (35), if $j \geqq 2$, then $T^j = \{t, \tau\}^j = \{(t+\tau)^j, 0\}$ for all $t, \tau$. Hence an element $T \in \mathfrak{L}$ is (multiplicatively) nilpotent if and only if $T \in \mathfrak{A}$. Thus every not-zero nilpotent element is nilpotent of order two.

The equation $RU = R$ can be satisfied only if $R \in \mathfrak{R}$. This condition is also sufficient. Every element $U$ of the form $\{u, 1-u\}$—in other words, for which $\Phi(U) = 1$—is a two-sided unit for the ring $\mathfrak{R}$. Of course, only one of these elements, namely $\{1, 0\}$, itself belongs to the integral domain $\mathfrak{R}$.

## Chapter III

1. A very fruitful means of constructing clusters is the method of taking a group with its operation written additively and defining a second operation, multiplication, in the system so that the closure and both distributive laws are satisfied. Certainly not every conceivable rule for multiplication is admissible, but many cases may be discussed. The purpose of Chapter III is to obtain some useful results concerning this construction technique.

In this chapter we shall use lower case Greek letters to represent rational integers and replace the summation notation (§I.4) $\sum^{\alpha} A$ by $\alpha A$.

2. Let $\Gamma$ be a non-abelian group with operation written additively. Suppose $\Gamma$ contains a not-zero element $P$ such that $\Gamma$ is homomorphic to the cyclic subgroup generated by $P$. If $W$ is any element of $\Gamma$ and if $\nu$ is the (positive or zero) order of $P$, the mapping may be symbolized by $W \to \omega P$, where $\omega$ is unique modulo $\nu$. In particular, let $\omega = \pi$ when $W = P$; thus $\pi P$ is the image of $P$ itself under the homomorphic mapping. When $W' \to \omega' P$, then, of course, $W + W' \to (\omega + \omega')P$. Upon the system $\Gamma$ we impose a multiplication operation

by defining $W \cdot W' = (\omega\omega')P$ for all $W$, $W'$. The distributive laws follow readily since $W(W'+W'') = (\omega[\omega'+\omega''])P = (\omega\omega')P + (\omega\omega'')P = WW' + WW''$; the right distributive law is treated similarly or may be considered a consequence of multiplicative commutativity.

The not-trivial cluster $\mathfrak{L}$ thus constructed is not only commutative but also associative; for, $(WW')W'' = (\omega\omega'P)W'' = ([\omega\omega'\pi]\omega'')P = (\omega[\omega'\omega''\pi])P = W(W'W'')$. Our cluster is a ring if and only if $\Gamma$ is abelian. The derived ring $\mathfrak{R}$ of the cluster consists of the multiples of the element $P$; in $\mathfrak{R}$, the rules of operation are: $\alpha P + \beta P = (\alpha+\beta)P$ and $(\alpha P)(\beta P) = (\alpha\beta\pi^2)P$. The annihilator ideal $\mathfrak{A}$ consists of all elements $W$ such that $\omega \equiv 0 \bmod \nu$; hence $W \equiv W' \bmod \mathfrak{A}$ if and only if $\omega \equiv \omega' \bmod \nu$.

Since many well known (for example, [Burnside, chap. VIII; Hilton, chap. XIV]) types of groups satisfy the requirements for $\Gamma$, the current construction method easily yields many illustrations of associative commutative clusters.

Of particular significance is the case of a homomorphic mapping $W \to \omega P$ in which $\pi = 1$; that is, when $P$ is its own image. Then the aforementioned rules of operation in the derived ring show that $\mathfrak{R}$ is isomorphic to the system $\mathfrak{N}$ of rational integers reduced modulo $\nu$—in particular, to the rational integral domain itself if $\nu = 0$, or to the prime finite field $GF(\nu)$ if $\nu$ is prime. Further, the difference cluster $\mathfrak{L} - \mathfrak{A}$, under the one-to-one mapping $[W] \to \omega P$, is isomorphic to $\mathfrak{R}$ and hence also to $\mathfrak{N}$; thus $\mathfrak{L} - \mathfrak{A} \cong \mathfrak{R} \cong \mathfrak{N}$. From the viewpoint of the preceding chapter, the cluster $\mathfrak{L}$ may be considered as an extension of $\mathfrak{N}$ by the group which serves as the kernel of the homomorphic mapping $W \to \omega P$.

3. *Example* 6. As an illustration of the case where $\pi = 1$, consider the alternating group of order 12, whose elements may be expressed $\xi P + \eta Q + \zeta R$ subject to the rules $3P = 2Q = 2R = 0$, $Q+P = P+Q+R$, $R+P = P+Q$, $R+Q = Q+R$. We define a multiplication by $(\xi P + \eta Q + \zeta R) \cdot (\xi' P + \eta' Q + \zeta' R) = (\xi\xi')P$. The system is a not-abelian, associative, commutative cluster. The elements 0, $Q$, $R$, $Q+R$ form the annihilator ideal; the elements 0, $P$, $2P$ constitute the derived ring; $\mathfrak{L} - \mathfrak{A} \cong \mathfrak{R} \cong GF(3)$. Every element of the cluster is uniquely expressible as the not-abelian sum of a product-element and an annihilator; this almost-direct-sum-decomposition—$\mathfrak{R}$ fails to be an ideal—we express by writing $\mathfrak{L} = \mathfrak{R} + \mathfrak{A}$.

4. To exemplify the restrictiveness of the distributive laws and the use of the theory of §I.4 in attempts to construct a cluster by imposing arbitrary rules of multiplication upon an additive group, we prove that every cluster whose additive group is the alternating group of order 12 must be commutative. Indeed, the cluster may be additively generated by the two elements $P$ and $V$, where $V = 2P + R$ (§3). The multiplication rules in the distributive system are then determined by the products $PP$, $PV$, $VP$, $VV$. The first and fourth of these products are certainly commutative. Since $P$ has

additive order three and $P+V=R$ has order two, then $PP+PV=P(P+V)=0=(P+V)P=PP+VP$; hence $PV=VP$.

5. The remainder of this chapter deals with topics related to finite clusters whose orders are prime or the product of two primes. If the order is the square of a prime, the additive group is abelian [Burnside, p. 47], and the cluster is a ring. A much stronger conclusion, contained in the following theorem, may be asserted when the order is a prime.

THEOREM 5. *Every cluster, the number of whose elements is prime, is either trivial or a prime finite field.*

**Proof.** Let the number of elements be $\pi$ and let $A$ be any not-zero element of the cluster $\mathfrak{L}$. Since $A$ additively generates the whole cluster, an integer $\lambda$ in the interval $0\leqq\lambda<\pi$ is defined by the equation $AA=\lambda A$; and $\lambda$ characterizes all products in $\mathfrak{L}$, by virtue of distributivity: $(\alpha A)(\beta A)=(\alpha\beta\lambda)A$. If $\lambda=0$, the cluster is trivial. Otherwise, the element $B=\lambda^{-1}A$, where $\lambda^{-1}\lambda\equiv 1 \bmod \pi$, also generates $\mathfrak{L}$ additively, and $B$ is idempotent. The rules of operation are now $\alpha B+\beta B=(\alpha+\beta)B$ and $(\alpha B)(\beta B)=(\alpha\beta)B$. The mapping $\alpha B\rightarrow\alpha$ demonstrates the isomorphism $\mathfrak{L}\cong GF(\pi)$.

COROLLARY. *For any prime number $\pi$, there exists one and (isomorphically) only one not-trivial cluster of order $\pi$.*

6. THEOREM 6. *Every (finite or infinite) cluster $\mathfrak{L}$ whose difference cluster $\mathfrak{L}-\mathfrak{A}$ modulo the annihilator ideal $\mathfrak{A}$ is of prime order possesses associative and commutative multiplication; further, if $\mathfrak{L}-\mathfrak{A}$ is not-trivial, then $\mathfrak{L}$ possesses one and only one idempotent.*

**Proof.** By hypothesis, the difference cluster $\mathfrak{L}-\mathfrak{A}$ has only a prime number $\pi$ of elements. These elements, which are residue classes $[A]$, may (Theorem 5) be designated $[0]$, $[B]$, $2[B]$, $\cdots$, $(\pi-1)[B]$, with $[B][B]=\mu[B]$, where $\mu$ is 0 or 1 according as $\mathfrak{L}-\mathfrak{A}$ is trivial or is isomorphic to $GF(\pi)$. Let $B$ represent any fixed element whatsoever from the class $[B]$. For each $\kappa$ in $0\leqq\kappa<\pi$, the multiple $\kappa B$ belongs to the class $\kappa[B]$. Every element $A\in\mathfrak{L}$ is congruent modulo $\mathfrak{A}$ to exactly one of these multiples: $A\equiv\alpha B \bmod \mathfrak{A}$, where $0\leqq\alpha<\pi$. For all $A\in\mathfrak{L}$, $A_1\in\mathfrak{L}$, we have (§I.6) $AA_1=(\alpha B)(\alpha_1 B)=\alpha\alpha_1 BB=(\alpha_1 B)(\alpha B)=A_1A$. The cluster is commutative. The associativity of $\mathfrak{L}$ has already (§I.7) been shown in the case $\mu=0$. Suppose, then, $\mu=1$. We choose any element $B'$ from the unit class $[B]$. Let its square be $B=B'B'$; since $B'$ belongs to the unit residue class, so does its square; consequently $B\equiv B' \bmod \mathfrak{A}$. Therefore $B$ is an idempotent, for (§I.6) $BB=B'B'=B$. If, now, $A$, $A_1$, $A_2$ are any three elements of $\mathfrak{L}$, then $(AA_1)A_2=((\alpha B)(\alpha_1 B))(\alpha_2 B)=(\alpha\alpha_1 B)(\alpha_2 B)=\alpha\alpha_1\alpha_2 B=(\alpha B)(\alpha_1\alpha_2 B)=A(A_1A_2)$. In this case, also, $\mathfrak{L}$ is associative. We must still prove the uniqueness of the idempotent $B$. Suppose $C$ is an idempotent; since $CC=C$, we have $[C][C]=[C]$. Now $[C]=[0]$ implies

$C \in \mathfrak{A}$ and therefore $C = CC = 0$, contrary to hypothesis. Consequently $[C]$ must be the unit residue class in $\mathfrak{L} - \mathfrak{A}$, namely $[C] = [B]$. Hence $C \equiv B \bmod \mathfrak{A}$, which congruence implies $CC = BB$ and therefore $C = B$.

We apply the theorem in a second proof of the assertion in §4. In fact, every not-trivial cluster $\mathfrak{L}$ whose additive group is the alternating group of order 12 must not only be commutative, but also be associative and possess a unique idempotent. For, the commutator ideal $\mathfrak{C}$ has four elements, whence $\mathfrak{C} \subseteq \mathfrak{A} \subset \mathfrak{L}$ implies $\mathfrak{C} = \mathfrak{A}$, and $\mathfrak{L} - \mathfrak{A}$ has prime order three. To show also that $\mathfrak{L} - \mathfrak{A}$ is not trivial, it suffices (§I.7) to reach a contradiction by assuming $\mathfrak{N} \subseteq \mathfrak{A}$. Since each element in $\mathfrak{A}$ has additive order two while $P$ and $V$ (§4) each have additive order three, the products $PP$, $PV = VP$, $VV$ would all vanish, $\mathfrak{N}$ would consist of zero alone, and $\mathfrak{L}$ itself would be trivial.

To illustrate Theorem 6 in a different manner, we recall Example 1 (§I.10). There the difference cluster $\mathfrak{L} - \mathfrak{A}$ has order four, the least composite natural number, and the cluster $\mathfrak{L}$ lacks associativity, commutativity, and an idempotent.

7. We investigate the existence of not-trivial not-abelian clusters of order $\pi\rho$, where $\pi$ and $\rho$ are distinct (positive) primes with $\rho > \pi$ and $\rho \equiv 1 \bmod \pi$. Assume there is such a cluster. There exists one and (isomorphically) only one group [Burnside, p. 48] which may serve as the additive group of our cluster $\mathfrak{L}$. The only normal subgroup (other than (0) and $\mathfrak{L}$) is $\mathfrak{C}$ and hence also $\mathfrak{A}$ (§I.6); its order is $\rho$. Since each element not in $\mathfrak{A}$ has order $\pi$ and since only these elements may be factors in not-vanishing products, every not-zero product has order $\pi$ and consequently is not in $\mathfrak{A}$; therefore $\mathfrak{L} - \mathfrak{A}$, of prime order $\pi$, is not-trivial. If $P$ represents the unique idempotent (Theorem 6) in $\mathfrak{L}$ and $Q$ is any not-zero element in $\mathfrak{A}$, then the elements of $\mathfrak{L}$ may be written $\xi P + \eta Q$. The rules of addition are $\pi P = 0 = \rho Q$ and $Q + P = P + \lambda^{\epsilon} Q$, where $\lambda = \beta^{(\rho-1)/\pi}$ with $\beta$ the least positive primitive root modulo $\rho$, and where $\epsilon$ satisfies $0 < \epsilon < \pi$. We note that the additive group of the cluster alone determines $\epsilon$, independently of the choice of element $Q \in \mathfrak{A}$. The rule of multiplication is $(\xi P + \eta Q)(\xi' P + \eta' Q) = \xi\xi' P$. We observe that multiplication is both associative and commutative. We are now in a position to complete the proof of the following theorem.

THEOREM 7. *Let $\pi$ and $\rho > \pi$ be any two distinct primes. If $\rho \not\equiv 1 \bmod \pi$, every cluster of order $\pi\rho$ is a ring. If $\rho \equiv 1 \bmod \pi$, there exist exactly $\pi - 1$ isomorphically distinct clusters of order $\pi\rho$ which are neither trivial clusters nor rings; every such cluster is associative, is commutative, contains one and only one idempotent, and satisfies the relations $\mathfrak{N} \cong \mathfrak{L} - \mathfrak{A} \cong GF(\pi)$.*

**Proof.** Our first assertion is true, since $\rho \not\equiv 1 \bmod \pi$ guarantees that the additive group of the cluster is abelian.

Suppose, then, $\rho \equiv 1 \bmod \pi$. Since there exists a not-abelian group of order $\pi\rho$ with elements $\xi P + \eta Q$ such that the cyclic subgroup generated by $P$

of order $\pi$ is a homomorphic image of the whole group, we may construct (§2) a not-trivial not-abelian cluster of order $\pi\rho$ by defining $(\xi P+\eta Q)(\xi' P+\eta' Q) = \xi\xi' P$. If two such clusters $\mathfrak{L}$ and $\mathfrak{L}'$ are isomorphic, then their idempotents $P$ and $P'$ must correspond; let any $Q'$ of order $\rho$ correspond to $Q$; then $Q+P=P+\lambda^{\epsilon} Q$ corresponds to $Q'+P'=P'+\lambda^{\epsilon'} Q'$. This is impossible unless $\epsilon=\epsilon'$. Consequently, with $\pi-1$ choices for $\epsilon$, there are at least $\pi-1$ isomorphically distinct clusters $\mathfrak{L}$. That each of these has the properties asserted in the theorem and that no others exist are consequences of the discussion in §2 and the first paragraph of this section.

COROLLARY. *There exists one and (isomorphically) only one not-trivial not-abelian cluster of order* $2\rho$, *where* $\rho$ *is any odd prime.*

8. Combining results of this chapter, we remark that the smallest order possible for a not-abelian cluster is 6. There exists one such not-trivial cluster; its construction is an application of the foregoing theory. The next smallest order is 8; Example 1 illustrates this possibility and furthermore verifies the assertion that 8 is the smallest order for a not-trivial not-abelian cluster which fails to possess either associativity or commutativity—Example 1 possesses neither. Clusters of order 15 are abelian; one not-trivial not-abelian cluster each of orders 10 and 14 occurs; order 12 has been exemplified; all other integers from 2 to 15 are prime or squares of primes.

## BIBLIOGRAPHY

A. A. Albert, *Modern higher algebra*, Chicago, 1937.

R. Baer, *Inverses and zero-divisors*, Bull. Amer. Math. Soc. vol. 48 (1942) pp. 630–638.

W. Burnside, *Theory of groups of finite order*, 2d ed., Cambridge, 1911.

H. Hilton, *Theory of groups of finite order*, Oxford, 1908.

N. Jacobson, *The theory of rings*, Mathematical Surveys, vol. 2, New York, 1943.

C. C. MacDuffee, *An introduction to abstract algebra*, New York, 1940.

L. Pontrjagin, *Topological groups*, Princeton, 1939.

O. Schreier, *Ueber die Erweiterung von Gruppen* I, Monatshefte für Mathematik und Physik vol. 34 (1926) pp. 165–180.

Olga Taussky, *Rings with non-commutative addition*, Bull. Calcutta Math. Soc. vol. 28 (1936) pp. 245–246.

B. L. van der Waerden, *Moderne Algebra*, 2d ed., Berlin, vol. I, 1937; vol. II, 1940.

H. Zassenhaus, *Lehrbuch der Gruppentheorie*, Leipzig, 1937.

UNIVERSITY OF MARYLAND,
COLLEGE PARK, MD.