CHAPTER I

GROUPS AND RINGS

1. Introduction. The usual textbook on college algebra begins with a *review of fundamental operations*. This review is really a rather incomplete formulation of the postulates for the mathematical system studied in elementary algebra and is really not even a good description of the system.

Modern algebra has many applications and requires a consideration of certain general, rigorously defined mathematical systems. We shall define these systems abstractly and most of the resulting properties will be the usual ones of elementary algebra. Any bizarre properties obtained will be due either to the generality of the systems studied, to the fact that *less* is assumed about our systems than is assumed in elementary algebra, or to the fact that we later specialize our general systems so as to give number systems different from those ordinarily used in algebra.

We shall usually replace the systems of real or complex numbers used as coefficients in elementary algebra by more general systems called "fields." There will generally be a fundamental or basic field whose elements will act as coefficients in our discussions, and we shall usually designate this field by the letter $\mathfrak{F}$. Whenever we talk about sets of elements we shall use Gothic letters to designate these sets.

The theorems and equations occurring in the text will be used in subsequent sections, and references will be made to them. We shall number the equations and theorems in each chapter separately and, after the first chapter, refer to them by a number consisting of the chapter number and the number of the theorem or equation. Thus, for example, we shall refer to Theorem 5 of Chapter X as Theorem 10.5 and to equation (22) of Chapter VII by (7.22).

2. Sets. Our first abstract notion is the elementary one of a *set* or aggregate $\mathfrak{G}$ of undefined entities $a, b, \ldots$ called the *elements* or *quantities* of $\mathfrak{G}$. We shall sometimes specify these elements, but they will usually be any abstract entities. For example, $\mathfrak{G}$ may consist of all even integers, or all real numbers, or all functions of x, or all rotations of a line in a plane about a point on the line. However, they will simply be unspecified. This is desirable as we thereby obtain mathematical systems of great generality and results applicable to many special theories.

When the elements of a set $\mathfrak{H}$ are all elements of a set $\mathfrak{G}$ we call $\mathfrak{H}$ a *subset* of $\mathfrak{G}$, say that $\mathfrak{H}$ *is contained in* $\mathfrak{G}$, and write

$$\mathfrak{H} \leqq \mathfrak{G}.$$

For example, $\mathfrak{G}$ may be the set of all rational numbers, $\mathfrak{H}$ the set of all integers. We also say that $\mathfrak{G}$ *contains* $\mathfrak{H}$, and indicate this by writing

$$\mathfrak{G} \geqq \mathfrak{H}.$$

If $\mathfrak{G}$ contains $\mathfrak{H}$ and $\mathfrak{H}$ contains $\mathfrak{G}$, then $\mathfrak{G}$ and $\mathfrak{H}$ are identical, that is, *equal* sets, and we write

$$\mathfrak{G} = \mathfrak{H}.$$

But when $\mathfrak{G}$ contains $\mathfrak{H}$ and also elements not in $\mathfrak{H}$, we say that $\mathfrak{G}$ contains $\mathfrak{H}$ *properly* and write

$$\mathfrak{G} > \mathfrak{H},$$

or that $\mathfrak{H}$ is a proper subset of $\mathfrak{G}$,

$$\mathfrak{H} < \mathfrak{G}.$$

Let $\mathfrak{G}$ and $\mathfrak{K}$ be two sets and $\mathfrak{H}$ consist of all elements which are in common to $\mathfrak{G}$ and $\mathfrak{K}$. Then the set $\mathfrak{H}$ is called the *intersection* (or cross-cut) of $\mathfrak{G}$ and $\mathfrak{K}$. This concept will occur frequently.

A set with no elements in it is called an *empty* set. When $\mathfrak{G}$ has at least one element we call $\mathfrak{G}$ a *non-empty* set. A set consisting of one element and the element are logically distinct concepts, but we may identify them. Then we indicate that g is an element of $\mathfrak{G}$ by writing

$$g \leqq \mathfrak{G}.$$

3. Correspondences. Let $\mathfrak{G}$ and $\mathfrak{G}'$ be any two sets and assume that to every element g of $\mathfrak{G}$ there corresponds a unique element g' of $\mathfrak{G}'$. We write

$$S: \qquad g \to g'$$

(read g goes to g') and call S a *correspondence from* $\mathfrak{G}$ *to* $\mathfrak{G}'$. It is clear that S need not be a correspondence from $\mathfrak{G}'$ to $\mathfrak{G}$.

For example, $\mathfrak{G}$ may be the set of all football games in a season and $\mathfrak{G}'$ the set of all possible scores. Every game corresponds to a unique pair of integers called a score. But the set of scores so obtained will not exhaust $\mathfrak{G}'$. Also the same score may be obtained for more than one game. A more ab-

stract example is that given by the set $\mathfrak{G}$ of all ordinary integers and the set $\mathfrak{G}'$ of their squares. The correspondence $g \to g' = g^2$ from $\mathfrak{G}$ to $\mathfrak{G}'$ is evidently not a correspondence from $\mathfrak{G}'$ to $\mathfrak{G}$ since $-g \to g^2$. Another example is that in which both $\mathfrak{G}$ and $\mathfrak{G}'$ consist of all rational functions of x with real coefficients. We let S be the correspondence $g(x) \to g'(x)$ where $g'(x)$ is the derivative of $g(x)$ and is uniquely determined by $g(x)$. However, it is well known to the reader that not every rational function is the derivative of a rational function so that the correspondents $g'(x)$ do not exhaust the set $\mathfrak{G}'$. Finally, let $\mathfrak{G}$ be the set of all integers and $\mathfrak{G}'$ the set of all integral multiples of three. The correspondence $g \to 3g$ from $\mathfrak{G}$ to $\mathfrak{G}'$ is now also a correspondence $3g \to g$ from $\mathfrak{G}'$ to $\mathfrak{G}$.

Let S be a correspondence $g \to g'$ from $\mathfrak{G}$ to $\mathfrak{G}'$ and g range over all elements of $\mathfrak{G}$. Then g' ranges over all elements of a subset $\mathfrak{G}'_S$ of $\mathfrak{G}'$ and when S is simultaneously a correspondence from $\mathfrak{G}'$ to $\mathfrak{G}$ we must have $\mathfrak{G}'_S = \mathfrak{G}'$. If g and h in $\mathfrak{G}$ go to g' and h' respectively in $\mathfrak{G}'$ under a correspondence S from $\mathfrak{G}$ to $\mathfrak{G}'$ and $g' = h'$ then we must have $g = h$ if S is a correspondence from $\mathfrak{G}'$ to $\mathfrak{G}$. These necessary conditions are obviously sufficient and S from $\mathfrak{G}$ to $\mathfrak{G}'$ is a correspondence from $\mathfrak{G}'$ to $\mathfrak{G}$ if and only if $\mathfrak{G}'_S = \mathfrak{G}'$, and $g' = h'$ if and only if $g = h$. Correspondences of this type are quite important, and we call them one-to-one correspondences

$$S: \qquad g \longleftrightarrow g'$$

(read g corresponds to g') *between* $\mathfrak{G}$ and $\mathfrak{G}'$. We shall often write (1–1) instead of one-to-one.

A *transformation* S of a set $\mathfrak{G}$ is a (1–1) correspondence between $\mathfrak{G}$ and itself indicated by

$$S: \qquad g \longleftrightarrow g^S .$$

We say that g goes to g^S under the transformation S and notice that both g and g^S range over all elements of $\mathfrak{G}$. Every transformation S has what we will call an *inverse* defined by

$$S^{-1}: \qquad g^S \longleftrightarrow g ,$$

and the *identical transformation* is the particular transformation

$$I: \qquad g \longleftrightarrow g$$

carrying every g of $\mathfrak{G}$ into itself.

In some environments it is more natural to use the word *function* instead of correspondence. The concepts are identical but the notation and terminology are sometimes changed as follows.

A correspondence f from a set $\mathfrak{G}$ to a set $\mathfrak{R}$ may be called a *function*

$$f: \qquad g \to k = f(g) ,$$

on $\mathfrak{G}$ to $\mathfrak{R}$. As usual the elements of $\mathfrak{G}$ may be any entities whatever and in particular may be systems $(g_1, \ldots, g_r)$ where g_i is an element of a set $\mathfrak{G}_i$ $(i = 1, \ldots, r)$. The above correspondence may now be written

$$f: \qquad (g_1, \ldots, g_r) \to f(g_1, \ldots, g_r) ,$$

and we say that f is a *function on* $\mathfrak{G}_1\mathfrak{G}_2 \ldots \mathfrak{G}_r$ *to* $\mathfrak{R}$. The sets $\mathfrak{G}_i$ need not be distinct. If they are all equal to a set $\mathfrak{G}$, f is on $\mathfrak{G}\mathfrak{G} \ldots \mathfrak{G}$ to $\mathfrak{R}$.

A particularly important example of a function on sets is suggested by the operations of elementary algebra. For example, let $\mathfrak{G}$ be the set of all non-zero integers and $\mathfrak{R}$ the set of rational numbers. Then division is a function on $\mathfrak{G}\mathfrak{G}$ to $\mathfrak{R}$. Considering arbitrary sets $\mathfrak{G}$, $\mathfrak{H}$, $\mathfrak{R}$ any function

$$\mathrm{O} \text{ on } \mathfrak{G}\mathfrak{H} \text{ to } \mathfrak{R}$$

will be called an *operation*. For operations* every a of $\mathfrak{G}$ and b of $\mathfrak{H}$ define a unique element $\mathrm{O}(a, b)$, in $\mathfrak{R}$ and we shall prefer to write

$$a \,\mathrm{O}\, b$$

instead of $\mathrm{O}(a, b)$.

When $\mathfrak{H} = \mathfrak{R} = \mathfrak{G}$ and therefore every a and b of $\mathfrak{G}$ define a unique $a\mathrm{O}b$ in $\mathfrak{G}$ we have O on $\mathfrak{G}\mathfrak{G}$ to $\mathfrak{G}$. We then say that $\mathfrak{G}$ *is closed* with respect to the operation O. This will be our most important type of operation.

The equality, that is, actual identity of elements of $\mathfrak{G}$ is a relation among its elements. The reader has of course met many other relations in elementary mathematics and sees that they are all functions R on $\mathfrak{G}\mathfrak{G}$ to the set $\mathfrak{R}$ consisting of two elements, *true*, *false*. We are accustomed to writing either $a = b$ or $a \neq b$. Thus for relations we write

$$a \,R\, b$$

if $R(a, b) = \textit{true}$, and

$$a \,\not{R}\, b$$

if $R(a, b) = \textit{false}$. Our notation for relations is seen to be different from that used for operations.

* An example where $\mathfrak{G}$, $\mathfrak{H}$, $\mathfrak{R}$ are all distinct may be given as follows. Let $\mathfrak{G}$ be the set of all real numbers, $\mathfrak{H}$ consist of the numbers $1, i = \sqrt{-1}$. Then multiplication is an operation on $\mathfrak{G}\mathfrak{H}$ to the set $\mathfrak{R}$ of all real or pure imaginary numbers.

The example above of a set $\mathfrak{R}$ whose elements are the two concepts true, false indicates again that we are considering sets whose elements are absolutely arbitrary. Our notations are familiar to the reader who has written repeatedly $a = b$ and $a \neq b$, the latter of course being read a not equal to b. Similarly one writes $a > b$ and $a \not> b$, or $a \geqq b$ and $a \ngeqq b$. The first of these well-known relations, that of equality, is an example of a type of relation which will arise very frequently in our further work and which we shall wish to recognize when it arises. We write $\cong$ instead of R for this relation and make the

DEFINITION. *A relation* $\cong$ *among the elements of a set* $\mathfrak{G}$ *is called an equivalence relation if*

I. *For every* a *of* $\mathfrak{G}$ *it is true that* $a \cong a$;

II. *If* $a \cong b$ *then* $b \cong a$;

III. *If* $a \cong b$ *and* $b \cong c$ *then* $a \cong c$.

The reader should verify whether or not the relations $=$, $>$, $\geqq$ in the set $\mathfrak{G}$ of all real numbers satisfy these postulates. He should also do this for other elementary relations—for example, the inclusion relation in sets.

Every equivalence relation enables us to classify the elements of $\mathfrak{G}$ into subsets called *classes of equivalent elements*. We put into a class $\{a\}$ (read class a) all the elements of $\mathfrak{G}$ equivalent to a, and our above postulates show that a is always in $\{a\}$, and that $\{a\} = \{b\}$ if and only if $a \cong b$. We shall call the element a appearing in $\{a\}$ a *representative* of the class. Then any b equivalent to a will serve equally well as a representative of the same class.

ORAL EXERCISES

1. Show that addition is an operation on $\mathfrak{G}\mathfrak{G}$ to $\mathfrak{G}$ where $\mathfrak{G}$ is the set of all even integers.

2. Let $\mathfrak{G}$ be the set of all non-zero even integers and ordinary division be an operation on $\mathfrak{G}\mathfrak{G}$ to $\mathfrak{R}$. Find a $\mathfrak{R}$.

3. Let $\mathfrak{G}$ be the set of all integers, $\mathfrak{H}$ consist of the integer 2. Describe the operation of ordinary multiplication as a function on $\mathfrak{G}\mathfrak{H}$ to a set $\mathfrak{R}$ to be determined.

4. Call two integers equivalent if they are both odd or both even, and otherwise inequivalent. Show that the relation so defined in the set of all integers is an equivalence relation and find the corresponding two classes of integers and representatives thereof.

5. Let a and b be any integers and write $a \, R \, b$ or $a \not R \, b$ according as the relation $|a - b| = 3$ is or is not true. Is this relation an equivalence relation? Does it become an equivalence relation if we replace the above equality by the statement $a \, R \, b$ if and only if $a - b$ is divisible by 3?

4. Integers. The ordinary integers

$$0, \pm 1, \pm 2, \ldots$$

occur frequently in all mathematics. This is not only true when they are elements of selected number systems but also when they are not. For they are sometimes used as exponents and subscripts on elements of arbitrary number systems. We shall discuss some of their elementary properties.

One of the most important properties of the set $\mathfrak{P}_P$ of all positive integers is called the *principle of complete induction*. Consider a subset $\mathfrak{G}$ of $\mathfrak{P}_P$ such that $\mathfrak{G}$ contains 1, and $a + 1$ for every a of $\mathfrak{G}$. Then the principle states that $\mathfrak{G} = \mathfrak{P}_P$. Many of our proofs will be inductive proofs and will thus depend on this principle. An illustration is given by the proof of the theorem on the **Division Algorithm** in the set $\mathfrak{P}$ of all integers.

Theorem 1. *Let* f *and* g $\neq 0$ *be integers and define* $|g| = g$ *or* $-g$ *according as* $g > 0$, $g < 0$. *Then there exist unique integers* q, r *such that*

$$f = qg + r, \qquad 0 \leqq r < |g| . \tag{1}$$

We first take $f > 0$. If $f = 1$ then $q = 0$, $r = 1$ when $|g| > 1$ and $r = 0$, $q = \pm 1$ when $|g| = 1$ so this case is complete. We make an induction on f and assume that $f = qg + r$. Then if $r < |g| - 1$ we have $f + 1 = qg + (r + 1)$, while if $r = |g| - 1$ then $f + 1 = (q \pm 1)g$ according as $g > 0$ or $g < 0$. This completes our induction on f and proves the existence of q and r when $f > 0$. If $f = 0$ we have $q = r = 0$ while if $f < 0$ we let $f_0 = -f = q_0 g + r_0$ by proof. Then $f = -q_0 g - r_0 = qg + r$, where $r = |g| - r_0$ and $q = -(q_0 \pm 1)$ according as $|g| = \pm g$. It remains to prove q, r unique. If then $f = sg + t = qg + r$ we have $(s - q)g = r - t$ where $|r - t| < |g|$. But g cannot divide an integer $r - t$ with $|r - t| < |g|$ unless $r - t = 0$. Hence $r = t$, $(s - q)g = 0$, $s = q$.

The principle of complete induction was used in the above proof as we have said. We shall of course use it later in many other situations.

Two integers a and b with the same remainder $r = 0, 1, \ldots, |g| - 1$ on division by g are said to be *congruent modulo* g, and it is customary in the elementary theory of numbers to write

$$a \equiv b \pmod{g} ,$$

or the simpler form

$$a \equiv b \ (g) .$$

Evidently $a \equiv b \ (g)$ if and only if $a - b$ is divisible by g. We shall sometimes use this congruence notation.

The Division Algorithm may be used to prove

Theorem 2. *Let* f *and* g *be integers not both zero. Then there exist a unique positive integer divisor* d *of* f *and* g *and integers* a *and* b *such that*

$$d = af + bg . \tag{2}$$

For let $\mathfrak{L}$ be the set of all positive integers $xf + yg$ for integers x, y. Since $\mathfrak{L}$ contains one of $f, g, -f, -g$, it is not an empty set. Thus there is a least positive integer $d = af + bg$ in $\mathfrak{L}$. We may write $f = qd + r$ with $0 \leqq r < d$ and obtain $(1 - aq)f + (-bq)g = r$ which is in $\mathfrak{L}$ or is zero. But the definition of d and $0 \leqq r < d$ imply that r is not in $\mathfrak{L}$, $r = 0$, d divides f. Similarly d divides g. If also d_1 divides f and g it must divide $d = af + bg$. When $d_1 = a_1 f + b_1 g$ we have d a divisor of d_1, $d = d_1$. This proves that d is unique.

We call d the *greatest common divisor* (abbreviated g.c.d.) of f and g. It is evidently the largest positive integral divisor of f and g.

Two integers f and g are called *relatively prime* if their g.c.d. is unity. We also say that f is *prime* to g or g is prime to f. When this occurs there always exist integers a, b such that $af + bg = 1$. This case of Theorem 2 is applied in

Theorem 3. *Let* f *divide* gh *and let* f *be prime to* g. *Then* f *divides* h.

For $af + bg = 1$, $gh = qf$, $afh + bgh = (ah + bq)f = h$ is divisible by f.

An integer $p \neq \pm 1, 0$ is called a *prime* if the only divisors of p are ± 1, $\pm p$. Theorem 3 then gives

Theorem 4. *Every integer* f *not zero or* ± 1 *is expressible uniquely apart from the order of the factors as a product*

$$\mathrm{f} = \pm \mathrm{p}_1^{e_1} \mathrm{p}_2^{e_2} \ldots \mathrm{p}_r^{e_r}$$

where the p_i *are positive primes.*

We leave the proof of Theorem 4 to the reader.

EXERCISES

1. Let m be a positive integer and call two integers *equivalent* (or *congruent*) if they have the same positive remainder r on division by m as in Theorem 1. Prove that the relation so defined is an equivalence relation.

2. The equivalence relation of Exercise 1 defines classes $\{a\}$ of elements a of $\mathfrak{B}$. Define $\{a_1\} + \{a_2\} = \{a_1 + a_2\}$, $\{a_1\}\{a_2\} = \{a_1 a_2\}$ and prove that the classes $\{a_1 + a_2\}$, $\{a_1 a_2\}$ are independent of the particular a_1, a_2 used.

5. Groups. The notion of a group is fundamental in our subject. We shall define groups and obtain some of their elementary properties.

DEFINITION. *A non-empty set* $\mathfrak{G}$ *of elements* a, b, . . . *is said to form a group with respect to an operation* O *if:*

I. $\mathfrak{G}$ *is closed with respect to* O;

II. *The associative law holds in* $\mathfrak{G}$, *that is,*

$$\mathrm{a\ O\ (b\ O\ c)} = \mathrm{(a\ O\ b)\ O\ c}$$

for every a, b, c *of* $\mathfrak{G}$;

III. *For every* a *and* b *of* $\mathfrak{G}$ *there exist solutions* x *and* y *in* $\mathfrak{G}$ *of the equations*

$$\text{a O x} = \text{b}, \qquad \text{y O a} = \text{b}. \tag{3}$$

A group is thus a *system* consisting of a set of elements $\mathfrak{G}$ and an operation O with respect to which $\mathfrak{G}$ forms a group. We shall generally designate the entire system by the set $\mathfrak{G}$ of its elements and shall call $\mathfrak{G}$ a group. The notation used for the operation is generally unimportant and may be taken in as convenient a way as possible. When $\mathfrak{G}$ is an abstract set of elements and multiplication is not already defined for these elements we may designate any given O as multiplication and write ab instead of $a\text{O}b$. We designate this by calling $\mathfrak{G}$ a *multiplicative* group. We may similarly write $a + b$ and call $\mathfrak{G}$ an *additive* group. However, we shall generally not use the addition symbol except when $a\ \text{O}\ b = b\ \text{O}\ a$.

DEFINITION. *A group* $\mathfrak{G}$ *is called commutative or abelian if*

$$\text{a O b} = \text{b O a}$$

for every a *and* b *of* $\mathfrak{G}$.

An elementary physical example of an abelian group is a certain rotation group. We let $\mathfrak{G}$ consist of the rotations of the spoke of a wheel through multiples of 90° and $a\text{O}b$ be the result of the rotation a followed by the rotation b. The reader will easily verify that $\mathfrak{G}$ forms a group with respect to O and that $a\text{O}b = b\text{O}a$. Slightly more complicated examples will be found in the exercises at the end of this section.

There is no loss of generality when we restrict our attention to multiplicative groups, that is, write ab instead of $a\text{O}b$. *We shall do this in our proofs* and shall obtain some elementary properties of groups. Let a be in $\mathfrak{G}$ so that Postulate III implies the existence of elements e, f in $\mathfrak{G}$ such that

$$ea = af = a.$$

By the same postulate every b of $\mathfrak{G}$ has the form

$$b = ac = da,$$

and thus $eb = e(ac) = (ea)c = ac = b$ by the associative law. Similarly $bf = b$. But then, taking $b = f$, $b = e$ in turn, we get $ef = f = e$ and have proved that there exists an element e in $\mathfrak{G}$ such that

$$eb = be = b \tag{4}$$

for every b of $\mathfrak{G}$. If also either $e_0a_0 = a_0$ or $a_0e_0 = a_0$ for some a_0 our proof shows that $e_0b = be_0 = b$ for every b of $\mathfrak{G}$. Then $e_0e = ee_0 = e = e_0$ so that

e is a unique element of $\mathfrak{G}$. We call e the *identity element* of $\mathfrak{G}$. This is a very important concept.

Let e satisfy (4) so that Postulate III implies that for every a of $\mathfrak{G}$ there exists an element a^{-1} of $\mathfrak{G}$ such that $aa^{-1} = e$. Then $a^{-1}(aa^{-1}) = a^{-1}e = a^{-1} = (a^{-1}a)a^{-1}$ and $a^{-1}(a^{-1})^{-1} = e = [(a^{-1}a)a^{-1}](a^{-1})^{-1} = (a^{-1}a)[a^{-1}(a^{-1})^{-1}] = (a^{-1}a)e = a^{-1}a$. We have proved that $aa^{-1} = a^{-1}a = e$. If also $ab = e$ then $a^{-1}(ab) = a^{-1}e = a^{-1} = (a^{-1}a)b = eb = b$ so that a^{-1} is unique. Moreover, $ax = b$ implies that $x = a^{-1}b$, $ya = b$ implies that $y = ba^{-1}$. We state the properties above in

Theorem 5. *There exists a unique identity element* $\mathfrak{e}$ *of any group* $\mathfrak{G}$ *such that*

$$\mathfrak{a} \circ \mathfrak{e} = \mathfrak{e} \circ \mathfrak{a} = \mathfrak{a}$$

for every $\mathfrak{a}$ *of* $\mathfrak{G}$. *Every* $\mathfrak{a}$ *of* $\mathfrak{G}$ *has a unique* ***inverse*** $\mathfrak{a}^{-1}$ *for which*

$$\mathfrak{a} \circ \mathfrak{a}^{-1} = \mathfrak{a}^{-1} \circ \mathfrak{a} = \mathfrak{e}\,. \tag{5}$$

Moreover (3) *have the unique solutions*

$$\mathfrak{x} = \mathfrak{a}^{-1} \circ \mathfrak{b}, \qquad \mathfrak{y} = \mathfrak{b} \circ \mathfrak{a}^{-1}\,. \tag{6}$$

The uniqueness in (6) gives immediately

COROLLARY. *Let* $\mathfrak{G}$ *be a group and let* $\mathfrak{a}$, $\mathfrak{f}$ *be in* $\mathfrak{G}$ *such that either* $\mathfrak{a}\circ\mathfrak{f} = \mathfrak{a}$ *or* $\mathfrak{f}\circ\mathfrak{a} = \mathfrak{a}$. *Then* $\mathfrak{f} = \mathfrak{e}$ *is the identity element of* $\mathfrak{G}$.

If $\mathfrak{G}$ is an additive group we call e the *zero element* of $\mathfrak{G}$ and write 0 for e. We also write $-a$ for the inverse of a with respect to addition and write $x = -a + b$, $y = b - a$ in (6). An additive abelian group is frequently called a *modul*.

Let $\mathfrak{G}$ be a set of elements, O be an operation on $\mathfrak{G}\mathfrak{G}$ to $\mathfrak{G}$ such that the associative law, Postulate II, holds. Suppose that $\mathfrak{G}$ contains an element e such that $a\mathrm{O}e = e\mathrm{O}a = a$ for every a of $\mathfrak{G}$, and that for this e and every a there exists an element a^{-1} such that $a\mathrm{O}a^{-1} = a^{-1}\mathrm{O}a = e$. Then $\mathfrak{G}$ is a group. For clearly Postulate III is satisfied by (6). The criterion that $\mathfrak{G}$ be a group thus obtained is in a sense a converse of Theorem 5, and is often simpler to apply than our definition of a group.

EXERCISES

1. Verify that the set $\mathfrak{B}$ of all integers is an additive abelian group. Prove the same result for the set $\mathfrak{E}$ of all even integers.

2. Prove that no subset of $\mathfrak{B}$ with more than two elements is a multiplicative group.

3. Determine whether the elements of $\mathfrak{E}$, $\mathfrak{B}$ form a group with respect to the operations defined by $\mathrm{O}(a, b) = 2(a + b)$, $2a + b$, $a - b$.

4. Show that the set $\mathfrak{A}$ of all classes $\{a\}$ defined by division by m as in Ex. 1 of Section 4 is an additive abelian group with $0 = \{0\}$.

5. Prove that if m is a prime p in Exercise 4 then the set $\mathfrak{A}$ with $\{0\}$ omitted is a multiplicative abelian group.

6. Let $m = pq$ with $p > 1$, $q > 1$ in Exercise 4. Prove that then the set $\mathfrak{A}$ with $\{0\}$ omitted does not form a multiplicative group.

7. Show that if a and b are elements of a multiplicative group $\mathfrak{G}$, then there exist elements x and y in $\mathfrak{G}$ such that $abx = ba$, $yab = ba$. We call x and y the *right* and *left commutators*, respectively, of the pair a, b. How are the commutators of a, b related to those of b, a? Of a^{-1}, b^{-1} and of b^{-1}, a^{-1}?

6. Equivalence, subgroups. In any study of mathematical systems the concept of equivalence of systems of the same kind always arises. Equivalent systems are logically distinct but we usually can replace any one by any other in a mathematical discussion with no loss of generality. For groups this notion is given by the

DEFINITION. *Let $\mathfrak{G}$ and $\mathfrak{G}'$ be groups with respective operations* O, O′ *and let there be a* (1–1) *correspondence*

$$\text{S:} \qquad \mathrm{a} \longleftrightarrow \mathrm{a}' \qquad (\mathrm{a} \text{ in } \mathfrak{G},\ \mathrm{a}' \text{ in } \mathfrak{G}')$$

between $\mathfrak{G}$ and $\mathfrak{G}'$ such that

$$(\mathrm{a\ O\ b})' = \mathrm{a}'\ \mathrm{O}'\ \mathrm{b}'$$

for all a, b *of $\mathfrak{G}$. Then we call $\mathfrak{G}$ and $\mathfrak{G}'$ equivalent* (*or simply-isomorphic*) *groups.*

The relation of equivalence is an equivalence relation in the technical sense in the set of all groups. We again emphasize that while equivalent groups may be logically distinct they have identical properties.

The groups $\mathfrak{G}$, $\mathfrak{G}'$ of the above definition need not be distinct of course, and O′ may be O. When this is the case the *self-equivalence* S of $\mathfrak{G}$ is called an *automorphism* of $\mathfrak{G}$. A particular automorphism is the identity automorphism

$$I: \qquad a \longleftrightarrow a\,,$$

of $\mathfrak{G}$, but other automorphisms may also exist. We notice though that in every automorphism the identity element is self-corresponding, $e \longleftrightarrow e$. In fact, if $\mathfrak{G}$ and $\mathfrak{G}'$ are equivalent groups with respective identity elements e, e', then $e \longleftrightarrow e'$ under any correspondence S defining the equivalence of $\mathfrak{G}$, $\mathfrak{G}'$. For $(a\mathrm{O}e) = a$, $(a\mathrm{O}e)' = a'\ \mathrm{O}'\ e'$ where $e \longleftrightarrow e'$ in $\mathfrak{G}'$. Thus e' is a solution of $a'\ \mathrm{O}'\ e' = a'$. But $\mathfrak{G}'$ is a group and e' is the identity element of $\mathfrak{G}'$ by Theorem 5.