tion group. The proof of this is the same as for $\mathfrak{G}_r$ with the modification that

$$a_l b_l = (ba)_l. \tag{8}$$

This follows from

$$xa_l b_l = b(ax) = (ba)x = x(ba)_l.$$

The mapping $a \to a_l$ is 1–1 of $\mathfrak{G}$ onto $\mathfrak{G}_l$ but in general this is not an isomorphism. In order to obtain an isomorphism we must replace this mapping by the mapping $a \to a_l{}^{-1} = (a^{-1})_l$; for then we have

$$(ab)_l{}^{-1} = (b_l a_l)^{-1} = a_l{}^{-1} b_l{}^{-1}.$$

We shall call the isomorphism $a \to a_l{}^{-1}$ the *left regular realization* of $\mathfrak{G}$.

The associative law in $\mathfrak{G}$ gives the rule $a_l b_r = b_r a_l$ for all $a,b$ in $\mathfrak{G}$ since $xa_l b_r = (ax)b$ and $xb_r a_l = a(xb)$. Hence any transformation belonging to the set $\mathfrak{G}_r$ commutes with any transformation belonging to $\mathfrak{G}_l$. The converse holds also, namely, if $\beta$ is any transformation in $\mathfrak{G}$ that commutes with all the $a_l$ ($a_r$), then $\beta$ is a right (left) multiplication; for we have

$$x\beta = (x1)\beta = (1x_l)\beta = (1\beta)x_l = x(1\beta) = xb$$

for $b = 1\beta$. Hence $\beta = b_r$.

EXERCISE

1. Obtain the regular realizations of $S_3$.

**11. Cyclic groups. Order of an element.** Let $M$ be any non-vacuous subset of a group $\mathfrak{G}$ and let $\{\mathfrak{H}\}$ be the collection of subgroups of $\mathfrak{G}$ that contain the set $M$. The collection $\{\mathfrak{H}\}$ contains $\mathfrak{G}$; hence it is not vacuous. Its intersection $\cap\mathfrak{H}$ is a subgroup of $\mathfrak{G}$ (ex. 4, p. 26). We denote this subgroup as $[M]$ and shall call it the *subgroup of* $\mathfrak{G}$ *generated by the set* $M$. The set $[M]$ has the following properties: (1) $[M]$ is a subgroup of $\mathfrak{G}$. (2) $[M] \supseteq M$. (3) If $\mathfrak{H}$ is any subgroup of $\mathfrak{G}$ containing $M$, then $\mathfrak{H} \supseteq [M]$. Also it is clear that these properties characterize $[M]$. Thus let $\mathfrak{K}$ be a subset of $\mathfrak{G}$ satisfying (1), (2) and (3) (for $M$).



Then since $\mathfrak{K}$ is a subgroup containing $M$, $\mathfrak{K} \supseteq [M]$. By symmetry $[M] \supseteq \mathfrak{K}$. Hence $\mathfrak{K} = [M]$.

We can use this characterization to obtain explicitly the elements of $[M]$. We assert that these are just the finite products $a_1 a_2 \cdots a_n$ ($n$ arbitrary) where $a_i \in M$ or $a_i$ is the inverse of an element of $M$. Let $\mathfrak{K}$ denote the collection of these products. Then it is immediate that $\mathfrak{K}$ is a subgroup of $\mathfrak{G}$ containing $M$. On the other hand, if $\mathfrak{H}$ is a subgroup of $\mathfrak{G}$ containing $M$, $\mathfrak{H}$ contains every $a \in M$ and every $a^{-1}$ with $a$ in $M$. Hence $\mathfrak{H}$ contains $\mathfrak{K}$. Thus $\mathfrak{K}$ satisfies (1), (2) and (3) and therefore $\mathfrak{K} = [M]$.

We consider now the special case in which $M = \{a\}$ is a set consisting of a single element $a$. Here we write $[a]$ for $[M]$, and we call this subgroup the (*cyclic*) *group generated by* $a$. A group $\mathfrak{Z}$ is called a *cyclic group* if there exists an $a \in \mathfrak{Z}$ such that $\mathfrak{Z} = [a]$. The element $a$ is then called a *generator* of $\mathfrak{Z}$. The remark above shows that $[a]$ consists of the elements $a^n$, $n > 0$, 1 and $(a^{-1})^n$, $n > 0$. We shall now define $a^0 = 1$ and $a^{-n} = (a^{-1})^n$ if $n > 0$. In this sense $[a]$ consists of the integral powers of the element $a$.

A consideration of cases can be used to extend the basic laws of exponents (5) to all integral powers. For example, suppose $n > |m|$ and $m < 0$. Then $a^n a^m = a^n a^{-|m|} = a^n (a^{-1})^{|m|} = a^{n-|m|} = a^{n+m}$. We leave it to the reader to verify the other cases. We remark that by the laws of exponents, or directly, $[a]$ is a commutative group. The following are some familiar examples of cyclic groups.

*Examples.* (1) Let $I_+$ be the group of integers relative to addition. It is clear by the axiom of induction that a set of positive integers that contains 1 and that is closed under addition contains all the positive integers. From this it follows that $I_+ = [1]$. It is clear also that $I_+ = [-1]$ and that $1 \notin [k]$ if $k \neq 1, -1$. Hence 1 and $-1$ are the only generators of $I$.

(2) Let $U_n$ be the group of complex $n$th roots of 1. Then $U_n$ consists of the complex numbers $e^{\frac{2k\pi}{n}i}$, $k = 0, 1, 2, \cdots, n-1$. Using the standard geometric representation of complex numbers, we see that these numbers are represented as the vertices of the regular $n$-gon inscribed in the unit circle that has (1,0) as one of its vertices. If we set $e^{\frac{2\pi}{n}i} = \rho$, we see that the elements of $U_n$ are $1, \rho, \rho^2, \cdots, \rho^{n-1}$. Hence $U_n$ is a cyclic group of order $n$.

Let $\mathfrak{Z}$ be a cyclic group with generator $a$ and consider the mapping $n \to a^n$ of $I_+$ onto $\mathfrak{Z}$. This correspondence has the property

$$m + n \to a^{m+n} = a^m a^n.$$

Hence, if our mapping is 1–1, then it is an isomorphism of $I_+$ onto $\mathfrak{Z}$.

Suppose next that the mapping is not 1–1. Then $a^m = a^n$ for $m \neq n$. We may assume $n > m$. Then $a^{n-m} = a^n a^{-m} = a^m a^{-m} = 1$. Hence there exist positive integers $p$ such that $a^p = 1$. Let $r$ be the smallest positive integer having this property. Then we assert that the elements $1, a, \cdots, a^{r-1}$ are distinct and that every element of $\mathfrak{Z}$ is in this set; for if $a^k = a^l$ for $k \neq l$ and $k, l$ in the range $0, 1, \cdots, r-1$, then $a^p = 1$ for $0 < p < r$ contrary to the choice of $r$. Next let $a^n$ be any element of $\mathfrak{Z}$. Write $n = qr + s$, $0 \leq s < r$. Then $a^n = a^{qr+s} = a^{qr}a^s = (a^r)^q a^s = a^s$. This proves our assertion. Thus $\mathfrak{Z}$ is a finite group of order $r$.

We now see that if $\mathfrak{Z}$ is infinite the mapping $n \to a^n$ is necessarily 1–1. Hence any infinite cyclic group is isomorphic to $I_+$ and consequently any two infinite cyclic groups are isomorphic. We shall show next that any two cyclic groups of the same finite order are isomorphic. Let $\mathfrak{Z} = [a]$ and $\mathfrak{W} = [b]$ be of order $r$. We have seen that the order $r$ of $[a]$ (or of $[b]$) is the smallest positive integer such that $a^r = 1$ ($b^r = 1$). We shall now show that, if $h$ is any integer such that $a^h = 1$, then $r \mid h$. Thus suppose $h = rq + s$, $0 \leq s < r$. Then $a^h = 1$ gives $a^s = a^s 1^q = a^s(a^r)^q = a^{s+rq} = a^h = 1$. Hence $s = 0$ by the minimality of $r$. Now suppose that $a^n = a^m$. Then $a^{n-m} = 1$ and so $n - m = rq$. Hence $1 = b^{rq} = b^{n-m}$ and $b^n = b^m$. We can now map $a^n \to b^n$ and be sure that this correspondence is single-valued. By symmetry $b^n = b^m$ implies that $a^n = a^m$. Hence our mapping is 1–1. Clearly $a^n a^m = a^{n+m} \to b^{n+m} = b^n b^m$. Hence $a^n \to b^n$ is an isomorphism. This completes the proof of the following

**Theorem 2.** *Any two cyclic groups of the same order are isomorphic.*

The concept of a cyclic group gives us a first classification of the elements of an arbitrary group $\mathfrak{G}$. If $a$ is any element of $\mathfrak{G}$, then we say that $a$ is of *infinite order* or of *finite order* $r$, according as $[a]$ is infinite or is a finite group of order $r$. In the first case we know that $a^n \neq 1$ if $n$ is any integer $\neq 0$, and if the second alternative holds, then $a^r = 1$. Also we know that $r$ is the least positive integer such that $a^r = 1$.



Cyclic groups are the simplest kinds of groups. It is therefore not surprising that most questions concerning groups are readily answered for this type. Thus, for example, it is generally a very difficult task to determine all the subgroups of a given group. We shall now see that this can be done very simply for cyclic groups.

Let $\mathfrak{W}$ be a subgroup of the cyclic group $\mathfrak{Z} = [a]$. Assume first that $\mathfrak{W} \neq 1$. Then there exist positive integers $m$ such that $a^m \in \mathfrak{W}$; for there exist integers $m \neq 0$ such that $a^m \in \mathfrak{W}$, and if $a^m \in \mathfrak{W}$, then so does $(a^m)^{-1} = a^{-m}$. Now let $s$ be the smallest positive integer such that $a^s \in \mathfrak{W}$. We propose to show that $\mathfrak{W} = [a^s]$ and that the correspondence $\mathfrak{W} \to s$ is 1–1. To prove these results let $c = a^m$ be any element in $\mathfrak{W}$ and write $m = sq + u$ where $0 \leq u < s$. Then $a^u = a^m(a^s)^{-q} \in \mathfrak{W}$. Hence, by the minimality of $s$, $u = 0$. Thus $c = a^m = (a^s)^q$ and $\mathfrak{W} = [a^s]$. Also the 1–1 ness is clear since, if $\mathfrak{W} \to s$ and $\mathfrak{W}' \to s$, then $\mathfrak{W} = [a^s] = \mathfrak{W}'$.

If $\mathfrak{Z}$ is an infinite cyclic group, then our mapping $\mathfrak{W} \to s$ is a mapping onto the set of positive integers; for if we take any positive integer $s$, then $[a^s] \to s$ since the smallest positive integer $p$ such that $a^p \in [a^s]$ is $s$ itself.

Suppose next that $\mathfrak{Z}$ is finite of order $r$. Then we shall show that the mapping $\mathfrak{W} \to s$ is a mapping onto the set of positive integers $< r$ which are divisors of $r$. Since $1 = a^r \in \mathfrak{W}$, the argument used before shows that $r$ is a multiple of $s$, that is, $s \mid r$. On the other hand, let $s$ be any divisor of $r$ and write $r = st$. Then $(a^s)^t = 1$, but $(a^s)^{t'} \neq 1$ if $0 < t' < t$. Hence, $t$ is the order of $[a^s]$. Now if $s'$ is the smallest positive integer such that $a^{s'} \in [a^s]$, then also $r = s't$ since $[a^{s'}] = [a^s]$. It follows that $s = s'$. Hence $[a^s] \to s$.

We have therefore proved the following

**Theorem 3.** *Let $\mathfrak{Z}$ be a cyclic group with generator $a$ and let $\mathfrak{W}$ be any subgroup $\neq 1$ of $\mathfrak{Z}$. Then if $s$ is the smallest positive integer such that $a^s \in \mathfrak{W}$, $\mathfrak{W} = [a^s]$. If $\mathfrak{Z}$ is infinite, then the correspondence $\mathfrak{W} \to s$ is a 1–1 mapping of the set of subgroups $\neq 1$ onto the set of*

*positive integers. If $\mathfrak{Z}$ is finite of order $r$, then our mapping is* 1–1 *of the set of subgroups $\neq 1$ onto the set of positive divisors of $r$ that are less than $r$.*

If $\mathfrak{Z}$ is infinite we can extend our correspondence to include the subgroup 1 consisting of 1 alone by mapping $1 \to 0$. In the finite case we map $1 \to r$, so that in all cases we have $\mathfrak{W} = [a^s]$. We note also that in the finite case if $\mathfrak{W} \to s$, then the order of $\mathfrak{W}$ is $r/s = t$. Hence, we obtain another 1–1 correspondence here by associating with $\mathfrak{W}$ the order of this subgroup. We state this result as

**Theorem 4.** *Let $\mathfrak{Z}$ be cyclic of order $r$ ($<\infty$). Then the order of any subgroup of $\mathfrak{Z}$ is a divisor of $r$ and, if $t$ is any positive divisor of $r$, $\mathfrak{Z}$ possesses one and only one subgroup of order $t$.*

It is customary to denote the number of positive divisors of an integer $r$ by $d(r)$. Thus $\mathfrak{Z}$ possesses $d(r)$ subgroups.

EXERCISES

1. List the subgroups of the cyclic group of order 12.
2. Let $\mathfrak{Z} = [a]$ be of order $r < \infty$. Show that the order of $a^m$ is $[m,r]/m = r/(m,r)$.
3. Show that a cyclic group of order $r$ possesses exactly $\phi(r)$ generators where $\phi(r)$ (the Euler $\phi$-*function*) denotes the number of positive numbers $<r$ that are *prime* to $r$ in the sense $(r,h) = 1$.
4. Show that the subgroup $\mathfrak{H}$ of order $t$ ($r = st$) of a cyclic group of order $r$ can be characterized in either of the following ways: (1) $\mathfrak{H}$ is the set of $s$th powers of the elements of $\mathfrak{G}$ or (2) $\mathfrak{H}$ is the set of elements $h$ such that $h^t = 1$.

**12. Elementary properties of permutations.** A permutation $\gamma$ which permutes cyclically a set of elements $i_1, i_2, \cdots, i_r$ in the sense that

$$(9) \qquad i_1\gamma = i_2, \quad i_2\gamma = i_3, \quad \cdots, \quad i_{r-1}\gamma = i_r, \quad i_r\gamma = i_1$$

and leaves fixed the other numbers in $\{1, 2, \cdots, n\}$ is called a *cycle*. If $\gamma$ is of this form, we denote it as $(i_1 i_2 \cdots i_r)$. It is clear that we can just as well write

$$\gamma = (i_2 i_3 \cdots i_r i_1) = (i_3 i_4 \cdots i_r i_1 i_2) = \cdots.$$

Two cycles $\gamma$ and $\gamma'$ are said to be *disjoint* if their symbols contain no common letters. In this case it is clear that the numbers



which are moved by one of these transformations are left fixed by the other. Hence if $i$ is any number and $i\gamma \neq i$, then $i\gamma'\gamma = i\gamma$ and since $i\gamma^2 \neq i\gamma$ also, $i\gamma\gamma' = i\gamma$. Similarly if $i\gamma' \neq i$ then $i\gamma\gamma' = i\gamma'\gamma$ and if $i\gamma = i$ and $i\gamma' = i$ then $i\gamma\gamma' = i\gamma'\gamma$. Thus $\gamma\gamma' = \gamma'\gamma$, that is, any two disjoint cycles commute.

Any permutation $\alpha$ can be written as a product of disjoint cycles. For example, if

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 6 & 5 & 4 & 8 & 2 & 7 & 1 \end{pmatrix},$$

then

$$1\alpha = 3, \quad 3\alpha = 5, \quad 5\alpha = 8, \quad 8\alpha = 1; \quad 2\alpha = 6, \quad 6\alpha = 2;$$
$$4\alpha = 4; \quad 7\alpha = 7;$$

from which it follows that

$$\alpha = (1\ 3\ 5\ 8)(2\ 6)(4)(7).$$

In general, for any $\alpha$ we can begin with any number in $1, 2, \cdots, n$, say $i_1$, and form $i_1\alpha = i_2$, $i_2\alpha = i_3$, $\cdots$, until we reach a number that occurs previously in this list. The first such repetition occurs when $i_{r+1} = i_r\alpha = i_1$; for $i_k = i_1\alpha^{k-1}$ and if $i_k = i_l$, $l > k$, then $i_1\alpha^{k-1} = i_1\alpha^{l-1}$ and $i_1\alpha^{l-k} = i_1$. Thus the numbers $i_1, i_2, \cdots, i_r$ are permuted cyclically by $\alpha$. If $r < n$ we can find a $j_1$ not in this set. If $j_1\alpha^k = i_1\alpha^q$, then $j_1 = i_1\alpha^{q-k}$ is in the original set contrary to assumption. Hence we obtain a new set $\{j_1, j_2, \cdots, j_s\}$ that is cyclically permuted by $\alpha$ and that has no element in common with the original set. If we continue in this way we finally exhaust the set $\{1, 2, \cdots, n\}$. Also it is clear by comparing effects on any number that

$$(10) \qquad \alpha = (i_1 i_2 \cdots i_r)(j_1 j_2 \cdots j_s) \cdots (l_1 l_2 \cdots l_u)$$

where these cycles are disjoint.

A cycle $(i)$ is the identity mapping. Such cycles can be dropped in (10) and we may therefore suppose that $r, s, \cdots, u > 1$ in (10). The factorization thus obtained is unique since we can deduce from it the fact that

$$i_1\alpha = i_2, \quad \cdots, \quad i_{r-1}\alpha = i_r, \quad i_r\alpha = i_1; \quad \cdots; \quad l_1\alpha = l_2, \quad \cdots,$$
$$l_{u-1}\alpha = l_u, \quad l_u\alpha = l_1$$