Hence we can choose the number in the first position in n different ways. Since no repetitions are allowed in the second row of our symbol, we have $n-1$ choices for the second position, $n-2$ for the third, etc. Hence in all we have $n!$ symbols and consequently $n!$ elements in S_n.

EXERCISES

1. Calculate $\alpha\beta$, $\beta\alpha$ and α^{-1} if

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix}, \quad \beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 4 & 5 & 2 \end{pmatrix}.$$

2. Write down the elements of S_3 and work out a multiplication table for this group.

3. Verify that the transformations

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

form a transformation group.

4. Which of the examples given in § 6 are transformation groups?

5. Verify that the set of transformations of the line given by the rule $x \to ax + b$, $a \neq 0$ form a transformation group. Show that this group is isomorphic to the one given in ex. 1, p. 23.

6. Verify that the totality of transformations of the plane defined by $(x,y) \to (x + a, 0)$ constitute a group relative to resultant composition. Is this a transformation group?

10. Realization of a group as a transformation group. Historically the theory of groups dealt at first only with transformation groups. The concept of an abstract group was introduced later for the purpose of deriving in the simplest and most direct manner those properties of transformation groups that concern the resultant composition only and do not refer to the set S in which the transformations act. It is natural to ask whether or not the abstract concept is completely appropriate in the sense that the class of systems covered by it is just the class of transformation groups. This question is answered affirmatively in the following fundamental theorem due to Cayley:

Theorem 1. *Any group is isomorphic to a transformation group.*

Proof. The transformation group that we shall define will act in the set $\mathfrak{G}$ of the given group. With each element a of the group $\mathfrak{G}$ we associate the mapping

$$x \to xa$$

of the set $\mathfrak{G}$ into itself. We denote this mapping as a_r and call it the *right multiplication* determined by a. Since the right cancellation law holds, a_r is 1–1. Since any b can be written in the form $(ba^{-1})a = (ba^{-1})a_r$, a_r is a mapping onto $\mathfrak{G}$. Hence a_r is in the group of 1–1 transformations of the set $\mathfrak{G}$. We wish to show now that the totality $\mathfrak{G}_r = \{a_r\}$ is a transformation group in $\mathfrak{G}$. Consider first the product a_rb_r. This sends x into $(xa)b$. By the associative law $(xa)b = x(ab)$. Thus a_rb_r has the same effect as $(ab)_r$. Hence

$$a_rb_r = (ab)_r \tag{7}$$

is in $\mathfrak{G}_r$. We note next that $1 = 1_r$ is in $\mathfrak{G}_r$. Finally by (7) $a_r(a^{-1})_r = 1_r = (a^{-1})_ra_r$. Hence $a_r{}^{-1} = (a^{-1})_r$ is in $\mathfrak{G}_r$. Thus $\mathfrak{G}_r$ is a transformation group. We consider now the correspondence $a \to a_r$ of the group $\mathfrak{G}$ onto the group $\mathfrak{G}_r$. If $a \neq b$, then $1a_r = a \neq b = 1b_r$. Hence $a_r \neq b_r$. Thus $a \to a_r$ is 1–1. Since (7) holds, the mapping $a \to a_r$ is an isomorphism. This completes the proof.

We shall refer to the isomorphism $a \to a_r$ as the (right) *regular realization* of $\mathfrak{G}$ as a transformation group. It should be observed that if $\mathfrak{G}$ is a finite group of order n, then $\mathfrak{G}_r$ is a subgroup of the symmetric group S_n. Hence we have the

Corollary. *Any finite group of order n is isomorphic to a subgroup of* S_n.

Examples. (1) R_+, the group of real numbers and addition. If $a \in R_+$, a_r is the translation $x \to x' = x + a$. (2) R^*, the group of real numbers $\neq 0$ under multiplication. Here a_r is the dilation $x \to x' = ax$. (3) The group of pairs of real numbers (a,b), $a \neq 0$, where $(a,b)(c,d) = (ac, bc + d)$. Here $(c,d)_r$ maps (x,y) into (x',y') where

$$x' = cx, \quad y' = cy + d.$$

There is a second realization of $\mathfrak{G}$ as a transformation group that one obtains by using left multiplications. We define the *left multiplication* a_l as the mapping $x \to ax$ of $\mathfrak{G}$ into itself. As in the case of right multiplication it is easy to see that a_l is 1–1 of $\mathfrak{G}$ onto itself. Also the set $\mathfrak{G}_l$ of the a_l is a transforma-

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 β is any transformation in $\mathfrak{G}$ that commutes with all the a_l (a_r), then β 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 nth roots of 1. Then U_n consists of the complex numbers $e^{\frac{2k\pi i}{n}}$, $k = 0, 1, 2, \cdots, n-1$. 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 $e^{\frac{2\pi i}{n}} = \rho$, 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