is an automorphism of $\mathfrak{G}$, since

$$a^{-1}(xy)a = (a^{-1}xa)(a^{-1}ya)$$

and, as is easy to verify, C_a is 1–1 of $\mathfrak{G}$ onto itself. As a matter of fact, the 1–1 ness is clear if we note that

$$C_a = a_r a_l^{-1} = a_l^{-1} a_r \tag{16}$$

where, as usual, a_r and a_l are respectively the right and the left multiplications determined by a. The automorphism C_a is called the *inner automorphism* determined by the element a.

We shall now show that the set $\mathfrak{I}$ of inner automorphisms forms an invariant subgroup of the group of automorphisms $\mathfrak{A}$. Let C_{a_1} and C_{a_2} be inner automorphisms. Then

$$xC_{a_1}C_{a_2} = a_2^{-1}a_1^{-1}xa_1a_2 = (a_1a_2)^{-1}x(a_1a_2) = xC_{a_1a_2}$$

so that

$$C_{a_1a_2} = C_{a_1}C_{a_2}. \tag{17}$$

This equation shows that the correspondence $a \to C_a$ is a homomorphism of $\mathfrak{G}$ into its group of automorphisms. It follows (Theorem 6) that the image set $\mathfrak{I}$ is a subgroup of $\mathfrak{A}$. Now let α be any automorphism and consider the product $\alpha^{-1}C_a\alpha$. Since

$$\begin{aligned} x\alpha^{-1}C_a\alpha &= (a^{-1}(x\alpha^{-1})a)\alpha = (a^{-1}\alpha)x(a\alpha) \\ &= (a\alpha)^{-1}x(a\alpha) \\ &= xC_{a\alpha}, \end{aligned}$$

$$\alpha^{-1}C_a\alpha = C_{a\alpha} \tag{18}$$

is inner. This proves the invariance of $\mathfrak{I}$. The factor group $\mathfrak{A}/\mathfrak{I}$ is called the *group of outer automorphisms* of the group $\mathfrak{G}$.

We return to the homomorphism $a \to C_a$ of $\mathfrak{G}$ onto $\mathfrak{I}$. The kernel $\mathfrak{C}$ of this mapping is the set of elements c such that $C_c = 1$. Thus $c \in \mathfrak{C}$ if and only if $c^{-1}xc = x$ for all x or equivalently,

$$cx = xc \tag{19}$$

for all x. We shall call $\mathfrak{C}$ the *center* of the group $\mathfrak{G}$. By Theorem 7 or directly we see that $\mathfrak{C}$ is an invariant subgroup. Also by the

fundamental theorem of homomorphism $\mathfrak{I} \cong \mathfrak{G}/\mathfrak{C}$. We summarize our results in the following

Theorem 9. *The set $\mathfrak{I}$ of inner automorphisms is an invariant subgroup of the group of automorphisms and $\mathfrak{I} \cong \mathfrak{G}/\mathfrak{C}$ where $\mathfrak{C}$ is the center of the group.*

EXERCISES

1. Prove that the mapping $a \to a^{-1}$ is an automorphism if and only if $\mathfrak{G}$ is commutative.
2. Show that, if k is an integer and $\mathfrak{G}$ is commutative, then $a \to a^k$ is an endomorphism.
3. Determine the group of automorphisms of any cyclic group.
4. Determine the group of automorphisms of the symmetric group $\mathfrak{S}_3$.
5. The transformation group generated by the group of automorphisms and the group of right multiplications is called the *holomorph* $\mathfrak{H}$ of the group $\mathfrak{G}$. Show that (1) $\mathfrak{H}$ contains all the left multiplications, (2) any element of $\mathfrak{H}$ can be written in one and only one way as a product αa_r of an automorphism α and a right multiplication a_r, (3) if $\mathfrak{G}$ is finite, then the order of $\mathfrak{H}$ is the product of the order of $\mathfrak{G}$ by the order of $\mathfrak{A}$.

18. Conjugate classes. The elements x and y of $\mathfrak{G}$ are said to be *conjugate* if they are equivalent relative to the congruence relation determined by the transformation group $\mathfrak{I}$. This means that there exists an a in $\mathfrak{G}$ such that $a^{-1}xa = y$. The transitivity sets determined by the group $\mathfrak{I}$ are called the *conjugate classes* of the group $\mathfrak{G}$. The conjugate class determined by the element c consists of a single element if and only if c is in the center of the group.

As an illustration of these ideas we shall determine the conjugate classes of the symmetric group $\mathfrak{S}_n$. We remark first that if α is the permutation

$$\begin{pmatrix} 1 & 2 & \cdots & n \\ 1\alpha & 2\alpha & \cdots & n\alpha \end{pmatrix}$$

and β is arbitrary, then $\beta^{-1}\alpha\beta$ sends 1β into $1\alpha\beta$ so that $\beta^{-1}\alpha\beta$ can be represented by the symbol

$$\begin{pmatrix} 1\beta & 2\beta & \cdots & n\beta \\ 1\alpha\beta & 2\alpha\beta & \cdots & n\alpha\beta \end{pmatrix}.$$

It follows that if

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

then

(21) $\beta^{-1}\alpha\beta = (i_1\beta i_2\beta \cdots i_r\beta) \cdots (l_1\beta l_2\beta \cdots l_u\beta).$

We may suppose that $r \geq s \geq \cdots \geq u$ and that all the numbers are displayed in (20). Then $r + s + \cdots + u = n$. In this way we associate with α a set of positive integers $r, s, \cdots, u$ such that

(22) $r \geq s \geq \cdots \geq u, \quad r + s + \cdots + u = n.$

Equation (21) shows that α and α' are conjugates in S_n if and only if the associated sets $r, s, \cdots, u$ are the same for these two permutations. A system of integers satisfying (22) is called a *partition* of n. Hence we have a 1–1 correspondence between the conjugate classes in S_n and the partitions of n. The number of conjugate classes coincides with the number $p(n)$ of distinct partitions of n. The function $p(n)$ is an important arithmetic function. Its first few values are

$$p(2) = 2, \quad p(3) = 3, \quad p(4) = 5, \quad p(5) = 7, \quad p(6) = 11.$$

Also it is clear from (21) that, if $r > 1$ and $n > 2$, then β can be chosen so that $\beta^{-1}\alpha\beta \neq \alpha$. Hence, if $\alpha \neq 1$, then there exists a β such that $\beta\alpha \neq \alpha\beta$. This shows that the center of S_n, $n > 2$, is the identity.

EXERCISES

1. Prove that, if $\mathfrak{G}$ is a finite permutation group, then the number of elements in any transitivity set determined by $\mathfrak{G}$ is a factor of the order of the group. (Hint: If i is any number in the set $S = \{1, 2, \cdots, n\}$, the set of transformations $\alpha \in \mathfrak{G}$ that leave i fixed is a subgroup $\mathfrak{H}$. Show that the elements in the transitivity set containing i can be put into 1–1 correspondence with the left cosets of $\mathfrak{H}$. Hence prove that the number of elements in the transitivity set is the index of $\mathfrak{H}$ in $\mathfrak{G}$.)
2. Prove that the number of elements in any conjugate class of a finite group $\mathfrak{G}$ is a factor of the order of $\mathfrak{G}$.
3. Prove that the center of a group of prime power order contains more than one element.

Chapter II

RINGS, INTEGRAL DOMAINS AND FIELDS

In this chapter we begin the study of a second important type of algebraic system called a *ring*. As we shall see, rings are sets with two suitably restricted binary compositions. Unlike the theory of groups which had essentially one source, namely, the study of sets of 1–1 transformations relative to resultant composition, the theory of rings has been fused out of a number of special theories. For this reason it will appear to be somewhat less unified than the theory of groups. In the present chapter we introduce the basic concepts of integral domain, division ring, field, ideal, difference ring, isomorphism, homomorphism and anti-isomorphism. Also we introduce some important special instances of rings such as matrix rings and quaternions. Finally we prove the analogue for rings of Cayley's theorem on groups.

1. Definition and examples.

Definition 1. *A* ring *is a system consisting of a set* $\mathfrak{A}$ *and two binary compositions in* $\mathfrak{A}$ *called* addition *and* multiplication *such that*

1. $\mathfrak{A}$ *together with addition* $(+)$ *is a commutative group.*
2. $\mathfrak{A}$ *together with multiplication* $(\cdot)$ *is a semi-group.*
3. *The distributive laws*

D $$a(b + c) = ab + ac$$
$$(b + c)a = ba + ca$$

hold.