The question now becomes, What values of t are possible? Since T is an automorphism of G, it maps G onto itself, so that $a = gT$ for some $g \in G$. Thus $a = a^iT = (aT)^i$ for some integer i. Since $aT = a^t$, we must have that $a = a^{ti}$, so that $a^{ti-1} = e$. Hence $ti - 1 = 0$; that is, $ti = 1$. Clearly, since t and i are integers, this must force $t = \pm 1$, and each of these gives rise to an automorphism, $t = 1$ yielding the identity automorphism I, $t = -1$ giving rise to the automorphism $T: g \to g^{-1}$ for every g in the cyclic group G. Thus here, $\mathscr{A}(G) \approx$ cyclic group of order 2.

Problems

1. Are the following mappings automorphisms of their respective groups?
   (a) G group of integers under addition, $T: x \to -x$.
   (b) G group of positive reals under multiplication, $T: x \to x^2$.
   (c) G cyclic group of order 12, $T: x \to x^3$.
   (d) G is the group S_3, $T: x \to x^{-1}$.
2. Let G be a group, H a subgroup of G, T an automorphism of G. Let $(H)T = \{hT \mid h \in H\}$. Prove $(H)T$ is a subgroup of G.
3. Let G be a group, T an automorphism of G, N a normal subgroup of G. Prove that $(N)T$ is a normal subgroup of G.
4. For $G = S_3$ prove that $G \approx \mathscr{I}(G)$.
5. For any group G prove that $\mathscr{I}(G)$ is a normal subgroup of $\mathscr{A}(G)$ (the group $\mathscr{A}(G)/\mathscr{I}(G)$ is called the *group of outer automorphisms* of G).
6. Let G be a group of order 4, $G = \{e, a, b, ab\}$, $a^2 = b^2 = e, ab = ba$. Determine $\mathscr{A}(G)$.
7. (a) A subgroup C of G is said to be a *characteristic subgroup* of G if $(C)T \subset C$ for all automorphisms T of G. Prove a characteristic subgroup of G must be a normal subgroup of G.
   (b) Prove that the converse of (a) is false.
8. For any group G, prove that the commutator subgroup G' is a characteristic subgroup of G. (See Problem 5, Section 2.7).
9. If G is a group, N a normal subgroup of G, M a characteristic subgroup of N, prove that M is a normal subgroup of G.
10. Let G be a finite group, T an automorphism of G with the property that $xT = x$ for $x \in G$ if and only if $x = e$. Prove that every $g \in G$ can be represented as $g = x^{-1}(xT)$ for some $x \in G$.
11. Let G be a finite group, T an automorphism of G with the property that $xT = x$ if and only if $x = e$. Suppose further that $T^2 = I$. Prove that G must be abelian.

$4! = 24 < 36 = o(G)$ so that in H there must be a normal subgroup $N \neq (e)$, of G, of order a divisor of 9, that is, of order 3 or 9.

2. Let G be a group of order 99 and suppose that H is a subgroup of G of order 11 (we shall also see, later, that this must be true). Then $i(H) = 9$, and since $99 \nmid 9!$ there is a nontrivial normal subgroup $N \neq (e)$ of G in H. Since H is of order 11, which is a prime, its only subgroup other than (e) is itself, implying that $N = H$. That is, H itself is a normal subgroup of G.

3. Let G be a non-abelian group of order 6. By Problem 11, Section 2.3, there is an $a \neq e \in G$ satisfying $a^2 = e$. Thus the subgroup $H = \{e, a\}$ is of order 2, and $i(H) = 3$. Suppose, for the moment, that we know that H is not normal in G. Since H has only itself and (e) as subgroups, H has no nontrivial normal subgroups of G in it. Thus G is isomorphic to a subgroup T of order 6 in $A(S)$, where S is the set of right cosets of H in G. Since $o(A(S)) = i(H)! = 3! = 6$, $T = S$. In other words, $G \approx A(S) = S_3$. We would have proved that any non-abelian group of order 6 is isomorphic to S_3. All that remains is to show that H is not normal in G. Since it might be of some interest we go through a detailed proof of this. If $H = \{e, a\}$ were normal in G, then for every $g \in G$, since $gag^{-1} \in H$ and $gag^{-1} \neq e$, we would have that $gag^{-1} = a$, or, equivalently, that $ga = ag$ for every $g \in G$. Let $b \in G$, $b \notin H$, and consider $N(b) = \{x \in G \mid xb = bx\}$. By an earlier problem, $N(b)$ is a subgroup of G, and $N(b) \supset H$; $N(b) \neq H$ since $b \in N(b)$, $b \notin H$. Since H is a subgroup of $N(b)$, $o(H) \mid o(N(b)) \mid 6$. The only even number n, $2 < n \leq 6$ which divides 6 is 6. So $o(N(b)) = 6$; whence b commutes with all elements of G. Thus every element of G commutes with every other element of G, making G into an abelian group, contrary to assumption. Thus H could not have been normal in G. This proof is somewhat long-winded, but it illustrates some of the ideas already developed.

Problems

● 1. Let G be a group; consider the mappings of G into itself, λ_g, defined for $g \in G$ by $x\lambda_g = gx$ for all $x \in G$. Prove that λ_g is one-to-one and onto, and that $\lambda_{gh} = \lambda_h\lambda_g$.

● 2. Let λ_g be defined as in Problem 1, τ_g as in the proof of Theorem 2.9.1. Prove that for any $g, h \in G$, the mappings λ_g, τ_h satisfy $\lambda_g\tau_h = \tau_h\lambda_g$. (*Hint:* For $x \in G$ consider $x(\lambda_g\tau_h)$ and $x(\tau_h\lambda_g)$.)

● 3. If θ is a one-to-one mapping of G onto itself such that $\lambda_g\theta = \theta\lambda_g$ for all $g \in G$, prove that $\theta = \tau_h$ for some $h \in G$.

● 4. (a) If H is a subgroup of G show that for every $g \in G$, gHg^{-1} is a subgroup of G.

(b) Prove that W = intersection of all gHg^{-1} is a normal subgroup of G.

● 5. Using Lemma 2.9.1 prove that a group of order p^2, where p is a prime number, must have a normal subgroup of order p.

6. Show that in a group G of order p^2 any normal subgroup of order p must lie in the center of G.

7. Using the result of Problem 6, prove that any group of order p^2 is abelian.

8. If p is a prime number, prove that any group G of order $2p$ must have a subgroup of order p, and that this subgroup is normal in G.

9. If $o(G)$ is pq where p and q are distinct prime numbers and if G has a normal subgroup of order p and a normal subgroup of order q, prove that G is cyclic.

*10. Let $o(G)$ be pq, $p > q$ are primes, prove
(a) G has a subgroup of order p and a subgroup of order q.
(b) If $q \nmid p - 1$, then G is cyclic.
(c) Given two primes p, q, $q \mid p - 1$, there exists a non-abelian group of order pq.
(d) Any two non-abelian groups of order pq are isomorphic.

2.10 Permutation Groups

We have seen that every group can be represented isomorphically as a subgroup of $A(S)$ for some set S, and, in particular, a finite group G can be represented as a subgroup of S_n, for some n, where S_n is the symmetric group of degree n. This clearly shows that the groups S_n themselves merit closer examination.

Suppose that S is a finite set having n elements $x_1, x_2, \ldots, x_n$. If $\phi \in A(S) = S_n$, then ϕ is a one-to-one mapping of S onto itself, and we could write ϕ out by showing what it does to every element, e.g., $\phi: x_1 \to x_2$, $x_2 \to x_4$, $x_4 \to x_3$, $x_3 \to x_1$. But this is very cumbersome. One short cut might be to write ϕ out as

$$\begin{pmatrix} x_1 & x_2 & x_3 & \cdots & x_n \\ x_{i_1} & x_{i_2} & x_{i_3} & \cdots & x_{i_n} \end{pmatrix},$$

where x_{i_j} is the image of x_j under ϕ. Returning to our example just above, ϕ might be represented by

$$\begin{pmatrix} x_1 & x_2 & x_3 & x_4 \\ x_2 & x_4 & x_1 & x_3 \end{pmatrix}.$$