Corollary 14. If K is any subgroup of the group G and $g \in G$, then $K \cong gKg^{-1}$. Conjugate elements and conjugate subgroups have the same order.

Proof: Letting $G = H$ in the proposition shows that conjugation by $g \in G$ is an automorphism of G, from which the corollary follows.

Corollary 15. For any subgroup H of a group G, the quotient group $N_G(H)/C_G(H)$ is isomorphic to a subgroup of $\text{Aut}(H)$. In particular, $G/Z(G)$ is isomorphic to a subgroup of $\text{Aut}(G)$.

Proof: Since H is a normal subgroup of the group $N_G(H)$, Proposition 13 (applied with $N_G(H)$ playing the role of G) implies the first assertion. The second assertion is the special case when $H = G$, in which case $N_G(G) = G$ and $C_G(G) = Z(G)$.

Definition. Let G be a group and let $g \in G$. Conjugation by g is called an *inner automorphism* of G and the subgroup of $\text{Aut}(G)$ consisting of all inner automorphisms is denoted by $\text{Inn}(G)$.

Note that the collection of inner automorphisms of G is in fact a subgroup of $\text{Aut}(G)$ and that by Corollary 15, $\text{Inn}(G) \cong G/Z(G)$. Note also that if H is a normal subgroup of G, conjugation by an element of G when restricted to H is an automorphism of H but need not be an inner automorphism of H (as we shall see).

Examples

(1) A group G is abelian if and only if every inner automorphism is trivial. If H is an abelian normal subgroup of G and H is not contained in $Z(G)$, then there is some $g \in G$ such that conjugation by g restricted to H is not an inner automorphism of H. An explicit example of this is $G = A_4$, H is the Klein 4-group in G and g is any 3-cycle.
(2) Since $Z(Q_8) = \langle -1 \rangle$ we have $\text{Inn}(Q_8) \cong V_4$.
(3) Since $Z(D_8) = \langle r^2 \rangle$ we have $\text{Inn}(D_8) \cong V_4$.
(4) Since for all $n \geq 3$, $Z(S_n) = 1$ we have $\text{Inn}(S_n) \cong S_n$.

Corollary 15 shows that any information we have about the automorphism group of a subgroup H of a group G translates into information about $N_G(H)/C_G(H)$. For example, if $H \cong Z_2$, then since H has unique elements of orders 1 and 2, Corollary 14 forces $\text{Aut}(H) = 1$. Thus if $H \cong Z_2$, $N_G(H) = C_G(H)$; if in addition H is a normal subgroup of G, then $H \leq Z(G)$ (cf. Exercise 10, Section 2.2).

Although the preceding example was fairly trivial, it illustrates that the action of G by conjugation on a *normal* subgroup H can be restricted by knowledge of the automorphism group of H. This in turn can be used to investigate the structure of G and will lead to some classification theorems when we consider semidirect products in Section 5.5.

A notion which will be used in later sections most naturally warrants introduction here:

Definition. A subgroup H of a group G is called *characteristic* in G, denoted H char G if every automorphism of G maps H to itself, i.e., $\sigma(H) = H$ for all $\sigma \in \mathrm{Aut}(G)$.

Results concerning characteristic subgroups which we shall use later (and whose proofs are relegated to the exercises) are

(1) characteristic subgroups are normal,
(2) if H is the unique subgroup of G of a given order, then H is characteristic in G, and
(3) if K char H and $H \trianglelefteq G$, then $K \trianglelefteq G$ (so although "normality" is not a transitive property (i.e., a normal subgroup of a normal subgroup need not be normal), a characteristic subgroup of a normal subgroup is normal).

Thus we may think of characteristic subgroups as "strongly normal" subgroups. For example, property (2) and Theorem 2.7 imply that every subgroup of a cyclic group is characteristic.

We close this section with some results on automorphism groups of specific groups.

Proposition 16. The automorphism group of the cyclic group of order n is isomorphic to $(\mathbb{Z}/n\mathbb{Z})^\times$, an abelian group of order $\varphi(n)$ (where φ is Euler's function).

Proof: Let x be a generator of the cyclic group Z_n. If $\psi \in \mathrm{Aut}(Z_n)$, then $\psi(x) = x^a$ for some $a \in \mathbb{Z}$ and the integer a uniquely determines ψ. Denote this automorphism by ψ_a. As usual, since $|x| = n$, the integer a is only defined mod n. Since ψ_a is an automorphism, x and x^a must have the same order, hence $(a, n) = 1$. Furthermore, for every a relatively prime to n, the map $x \mapsto x^a$ is an automorphism of Z_n. Hence we have a surjective map

$$\begin{aligned} \Psi : \mathrm{Aut}(Z_n) &\to (\mathbb{Z}/n\mathbb{Z})^\times \\ \psi_a &\mapsto a \pmod{n}. \end{aligned}$$

The map Ψ is a homomorphism because

$$\psi_a \circ \psi_b(x) = \psi_a(x^b) = (x^b)^a = x^{ab} = \psi_{ab}(x)$$

for all $\psi_a, \psi_b \in \mathrm{Aut}(Z_n)$, so that

$$\Psi(\psi_a \circ \psi_b) = \Psi(\psi_{ab}) = ab \pmod{n} = \Psi(\psi_a)\Psi(\psi_b).$$

Finally, Ψ is clearly injective, hence is an isomorphism.

A complete description of the isomorphism type of $\mathrm{Aut}(Z_n)$ is given at the end of Section 9.5.

Example

Assume G is a group of order pq, where p and q are primes (not necessarily distinct) with $p \leq q$. If $p \nmid q - 1$, we prove G is abelian.

If $Z(G) \neq 1$, Lagrange's Theorem forces $G/Z(G)$ to be cyclic, hence G is abelian by Exercise 36, Section 3.1. Hence we may assume $Z(G) = 1$.

If every nonidentity element of G has order p, then the centralizer of every nonidentity element has index q, so the class equation for G reads

$$pq = 1 + kq.$$

This is impossible since q divides pq and kq but not 1. Thus G contains an element, x, of order q.

Let $H = \langle x \rangle$. Since H has index p and p is the smallest prime dividing $|G|$, the subgroup H is normal in G by Corollary 5. Since $Z(G) = 1$, we must have $C_G(H) = H$. Thus $G/H = N_G(H)/C_G(H)$ is a group of order p isomorphic to a subgroup of $\mathrm{Aut}(H)$ by Corollary 15. But by Proposition 16, $\mathrm{Aut}(H)$ has order $\varphi(q) = q - 1$, which by Lagrange's Theorem would imply $p \mid q - 1$, contrary to assumption. This shows that G must be abelian.

One can check that every group of order pq, where p and q are distinct primes with $p < q$ and $p \nmid q - 1$ is *cyclic* (see the exercises). This is the first instance where there is a unique isomorphism type of group whose order is *composite*. For instance, every group of order 15 is cyclic.

The next proposition summarizes some results on automorphism groups of known groups and will be proved later. Part 3 of this proposition illustrates how the theory of vector spaces comes into play in group theory.

Proposition 17.

(1) If p is an odd prime and $n \in \mathbb{Z}^+$, then the automorphism group of the cyclic group of order p is cyclic of order $p - 1$. More generally, the automorphism group of the cyclic group of order p^n is cyclic of order $p^{n-1}(p-1)$ (cf. Corollary 20, Section 9.5).

(2) For all $n \geq 3$ the automorphism group of the cyclic group of order 2^n is isomorphic to $Z_2 \times Z_{2^{n-2}}$, and in particular is not cyclic but has a cyclic subgroup of index 2 (cf. Corollary 20, Section 9.5).

(3) Let p be a prime and let V be an abelian group (written additively) with the property that $pv = 0$ for all $v \in V$. If $|V| = p^n$, then V is an n-dimensional vector space over the field $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. The automorphisms of V are precisely the nonsingular linear transformations from V to itself, that is

$$\mathrm{Aut}(V) \cong GL(V) \cong GL_n(\mathbb{F}_p).$$

In particular, the order of $\mathrm{Aut}(V)$ is as given in Section 1.4 (cf. the examples in Sections 10.2 and 11.1).

(4) For all $n \neq 6$ we have $\mathrm{Aut}(S_n) = \mathrm{Inn}(S_n) \cong S_n$ (cf. Exercise 18). For $n = 6$ we have $|\mathrm{Aut}(S_6) : \mathrm{Inn}(S_6)| = 2$ (cf. the following Exercise 19 and also Exercise 10 in Section 6.3).

(5) $\mathrm{Aut}(D_8) \cong D_8$ and $\mathrm{Aut}(Q_8) \cong S_4$ (cf. the following Exercises 4 and 5 and also Exercise 9 in Section 6.3).

The group V described in Part 3 of the proposition is called the *elementary abelian* group of order p^n (we shall see in Chapter 5 that it is uniquely determined up to isomorphism by p and n). The Klein 4-group, V_4, is the elementary abelian group of order 4. This proposition asserts that

$$\mathrm{Aut}(V_4) \cong GL_2(\mathbb{F}_2).$$

By the exercises in Section 1.4, the latter group has order 6. But $\mathrm{Aut}(V_4)$ permutes the 3 nonidentity elements of V_4, and this action of $\mathrm{Aut}(V_4)$ on $V_4 - \{1\}$ gives an injective permutation representation of $\mathrm{Aut}(V_4)$ into S_3. By order considerations, the homomorphism is onto, so

$$\mathrm{Aut}(V_4) \cong GL_2(\mathbb{F}_2) \cong S_3.$$

Note that V_4 is abelian, so $\mathrm{Inn}(V_4) = 1$.

For any prime p, the elementary abelian group of order p^2 is $Z_p \times Z_p$. Its automorphism group, $GL_2(\mathbb{F}_p)$, has order $p(p-1)^2(p+1)$. Thus Corollary 9 implies that for p a prime

$$\text{if } |P| = p^2, \quad |\mathrm{Aut}(P)| = p(p-1) \text{ or } p(p-1)^2(p+1)$$

according to whether P is cyclic or elementary abelian, respectively.

Example

Suppose G is a group of order $45 = 3^2 5$ with a normal subgroup P of order 3^2. We show that G is necessarily abelian.

The quotient $G/C_G(P)$ is isomorphic to a subgroup of $\mathrm{Aut}(P)$ by Corollary 15, and $\mathrm{Aut}(P)$ has order 6 or 48 (according to whether P is cyclic or elementary abelian, respectively) by the preceding paragraph. On the other hand, since the order of P is the square of a prime, P is an abelian group, hence $P \leq C_G(P)$. It follows that $|C_G(P)|$ is divisible by 9, which implies $|G/C_G(P)|$ is 1 or 5. Together these imply $|G/C_G(P)| = 1$, i.e., $C_G(P) = G$ and $P \leq Z(G)$. Since then $G/Z(G)$ is cyclic, G must be an abelian group.

EXERCISES

Let G be a group.

1. If $\sigma \in \mathrm{Aut}(G)$ and φ_g is conjugation by g prove $\sigma\varphi_g\sigma^{-1} = \varphi_{\sigma(g)}$. Deduce that $\mathrm{Inn}(G) \trianglelefteq \mathrm{Aut}(G)$. (The group $\mathrm{Aut}(G)/\mathrm{Inn}(G)$ is called the *outer automorphism group* of G.)
2. Prove that if G is an abelian group of order pq, where p and q are distinct primes, then G is cyclic. [Use Cauchy's Theorem to produce elements of order p and q and consider the order of their product.]
3. Prove that under any automorphism of D_8, r has at most 2 possible images and s has at most 4 possible images (r and s are the usual generators — cf. Section 1.2). Deduce that $|\mathrm{Aut}(D_8)| \leq 8$.
4. Use arguments similar to those in the preceding exercise to show $|\mathrm{Aut}(Q_8)| \leq 24$.
5. Use the fact that $D_8 \trianglelefteq D_{16}$ to prove that $\mathrm{Aut}(D_8) \cong D_8$.
6. Prove that characteristic subgroups are normal. Give an example of a normal subgroup that is not characteristic.
7. If H is the unique subgroup of a given order in a group G prove H is characteristic in G.
8. Let G be a group with subgroups H and K with $H \leq K$.
   (a) Prove that if H is characteristic in K and K is normal in G then H is normal in G.
   (b) Prove that if H is characteristic in K and K is characteristic in G then H is characteristic in G. Use this to prove that the Klein 4-group V_4 is characteristic in S_4.
   (c) Give an example to show that if H is normal in K and K is characteristic in G then H need not be normal in G.