multiplication by $\frac{1}{2}$. In the group G, $\mathbb{Z} \leq \mathbb{Q}$ and the conjugate $x\mathbb{Z}x^{-1}$ of $\mathbb{Z}$ is a *proper* subgroup of $\mathbb{Z}$ (namely $2\mathbb{Z}$). Thus $x \notin N_G(\mathbb{Z})$ even though $x\mathbb{Z}x^{-1} \leq \mathbb{Z}$ (note that $x^{-1}\mathbb{Z}x$ is not contained in $\mathbb{Z}$). This shows that in order to prove an element g normalizes a subgroup A in an *infinite* group it is not sufficient in general to show that the conjugate of A by g is just *contained* in A (which is sufficient for finite groups).

(5) For H any group let $K = \text{Aut}(H)$ with φ the identity map from K to $\text{Aut}(H)$. The semidirect product $H \rtimes \text{Aut}(H)$ is called the *holomorph* of H and will be denoted by $\text{Hol}(H)$. Some holomorphs are described below; verifications of these isomorphisms are given as exercises at the end of this chapter.

(a) $\text{Hol}(Z_2 \times Z_2) \cong S_4$.

(b) If $|G| = n$ and $\pi : G \to S_n$ is the left regular representation (Section 4.2), then $N_{S_n}(\pi(G)) \cong \text{Hol}(G)$. In particular, since the left regular representation of a generator of Z_n is an n-cycle in S_n we obtain that for any n-cycle $(1\,2\,\ldots\,n)$:

$$N_{S_n}(\langle (1\,2\,\ldots\,n) \rangle) \cong \text{Hol}(Z_n) = Z_n \rtimes \text{Aut}(Z_n).$$

Note that the latter group has order $n\varphi(n)$.

(6) Let p and q be primes with $p < q$, let $H = Z_q$ and let $K = Z_p$. We have already seen that if p does not divide $q - 1$ then every group of order pq is cyclic (see the example following Proposition 4.16). This is consistent with the fact that if p does not divide $q - 1$, there is no nontrivial homomorphism from Z_p into $\text{Aut}(Z_q)$ (the latter group is cyclic of order $q - 1$ by Proposition 4.17). Assume now that $p \mid q - 1$. By Cauchy's Theorem, $\text{Aut}(Z_q)$ contains a subgroup of order p (which is unique because $\text{Aut}(Z_q)$ is cyclic). Thus there is a nontrivial homomorphism, φ, from K into $\text{Aut}(H)$. The associated group $G = H \rtimes K$ has order pq and K is not normal in G (Proposition 11). In particular, G is non-abelian. We shall prove shortly that G is (up to isomorphism) the unique non-abelian group of order pq. If $p = 2$, G must be isomorphic to D_{2q}.

(7) Let p be an odd prime. We construct two nonisomorphic non-abelian groups of order p^3 (we shall later prove that any non-abelian group of order p^3 is isomorphic to one of these two).

Let $H = Z_p \times Z_p$ and let $K = Z_p$. By Proposition 4.17, $\text{Aut}(H) \cong GL_2(\mathbb{F}_p)$ and $|GL_2(\mathbb{F}_p)| = (p^2 - 1)(p^2 - p)$. Since $p \mid |\text{Aut}(H)|$, by Cauchy's Theorem H has an automorphism of order p. Thus there is a nontrivial homomorphism, φ, from K into $\text{Aut}(H)$ and so the associated group $H \rtimes K$ is a non-abelian group of order p^3. More explicitly, if $H = \langle a \rangle \times \langle b \rangle$, and x is a generator for K then x acts on a and b by

$$x \cdot a = ab \quad \text{and} \quad x \cdot b = b$$

which defines the action of x on all of H. With respect to the $\mathbb{F}_p$-basis a, b of the 2-dimensional vector space H the action of x (which can be considered in additive notation as a nonsingular linear transformation) has matrix

$$\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \in GL_2(\mathbb{F}_p).$$

The resulting semidirect product has the presentation

$$\langle x, a, b \mid x^p = a^p = b^p = 1,\ ab = ba,\ xax^{-1} = ab,\ xbx^{-1} = b \rangle$$

(in fact, this group is generated by $\{x, a\}$, and is called the *Heisenberg group* over $\mathbb{Z}/p\mathbb{Z}$, cf. Exercise 25).

Next let $H = Z_{p^2}$ and $K = Z_p$. Again by Proposition 4.17, $\text{Aut}(H) \cong Z_{p(p-1)}$, so H admits an automorphism of order p. Thus there is a nontrivial homomorphism,

φ, from K into Aut(H) and so the group $H \rtimes K$ is non-abelian and of order p^3. More explicitly, if $H = \langle y \rangle$, and x is a generator for K then x acts on y by

$$x \cdot y = y^{1+p}.$$

The resulting semidirect product has the presentation

$$\langle x, y \mid x^p = y^{p^2} = 1,\ xyx^{-1} = y^{1+p} \rangle.$$

These two groups are not isomorphic (the former contains no element of order p^2, cf. Exercise 25, and the latter clearly does, namely y).

(8) Let $H = Q_8 \times (Z_2 \times Z_2) = \langle i, j \rangle \times (\langle a \rangle \times \langle b \rangle)$ and let $K = \langle y \rangle \cong Z_3$. The map defined by

$$i \mapsto j \qquad j \mapsto k = ij \qquad a \mapsto b \qquad b \mapsto ab$$

is easily seen to give an automorphism of H of order 3. Let φ be the homomorphism from K to Aut(H) defined by mapping y to this automorphism, and let G be the associated semidirect product, so that $y \in G$ acts by

$$y \cdot i = j \qquad y \cdot j = k \qquad y \cdot a = b \qquad y \cdot b = ab.$$

The group $G = H \rtimes K$ is a non-abelian group of order 96 with the property that the element $i^2a \in G'$ but i^2a cannot be expressed as a single commutator $[x, y]$, for any $x, y \in G$ (checking the latter assertion is an elementary calculation).

As in the case of direct products we now prove a recognition theorem for semidirect products. This theorem will enable us to "break down" or "factor" all groups of certain orders and, as a result, classify groups of those orders. The strategy is discussed in greater detail following this theorem.

Theorem 12. Suppose G is a group with subgroups H and K such that

(1) $H \trianglelefteq G$, and

(2) $H \cap K = 1$.

Let $\varphi : K \to \text{Aut}(H)$ be the homomorphism defined by mapping $k \in K$ to the automorphism of left conjugation by k on H. Then $HK \cong H \rtimes K$. In particular, if $G = HK$ with H and K satisfying (1) and (2), then G is the semidirect product of H and K.

Proof: Note that since $H \trianglelefteq G$, HK is a subgroup of G. By Proposition 8 every element of HK can be written uniquely in the form hk, for some $h \in H$ and $k \in K$. Thus the map $hk \mapsto (h, k)$ is a *set* bijection from HK onto $H \rtimes K$. The fact that this map is a homomorphism is the computation at the beginning of this section which led us to the formulation of the definition of the semidirect product.

Definition. Let H be a subgroup of the group G. A subgroup K of G is called a *complement* for H in G if $G = HK$ and $H \cap K = 1$.

With this terminology, the criterion for recognizing a semidirect product is simply that there must exist a complement for some proper *normal* subgroup of G. Not every group is the semidirect product of two of its proper subgroups (for example, if the group is simple), but as we have seen, the notion of a semidirect product greatly increases our list of known groups.

Some Classifications

We now apply Theorem 12 to classify groups of order n for certain values of n. The basic idea in each of the following arguments is to

(a) show every group of order n has proper subgroups H and K satisfying the hypothesis of Theorem 12 with $G = HK$

(b) find all possible isomorphism types for H and K

(c) for each pair H, K found in (b) find all possible homomorphisms $\varphi : K \to \mathrm{Aut}(H)$

(d) for each triple H, K, φ found in (c) form the semidirect product $H \rtimes K$ (so any group G of order n is isomorphic to one of these explicitly constructed groups) and among all these semidirect products determine which pairs are isomorphic. This results in a list of the distinct isomorphism types of groups of order n.

In order to start this process we must first find subgroups H and K (of an arbitrary group G of order n) satisfying the above conditions. In the case of "small" values of n we can often do this by Sylow's Theorem. To show *normality* of H we use the conjugacy part of Sylow's Theorem or other normality criteria established in Chapter 4 (e.g., Corollary 4.5). Some of this work has already been done in the examples in Section 4.5. In many of the examples that follow, $|H|$ and $|K|$ are relatively prime, so $H \cap K = 1$ holds by Lagrange's Theorem.

Since H and K are proper subgroups of G one should think of the determination of H and K as being achieved inductively. In the examples we discuss, H and K will have sufficiently small order that we shall know all possible isomorphism types from previous results. For example, in most instances H and K will be of prime or prime squared order.

There will be relatively few possible homomorphisms $\varphi : K \to \mathrm{Aut}(H)$ in our examples, particularly after we take into account certain symmetries (such as replacing one generator of K by another when K is cyclic).

Finally, the semidirect products which emerge from this process will, in our examples, be small in number and we shall find that, for the most part, they are (pairwise) *not* isomorphic. In general, this can be a more delicate problem, as Exercise 4 indicates.

We emphasize that this approach to "factoring" every group of some given order n as a semidirect product does not work for arbitrary n. For example, Q_8 is not a semidirect product since no proper subgroup has a complement (although we saw that it is a *quotient* of a semidirect product). Empirically, this process generally works well when the group order n is not divisible by a large power of any prime. At the other extreme, only a small percentage of the groups of order p^α for large α (p a prime) are nontrivial semidirect products.

Example: (Groups of Order pq, p and q primes with $p < q$)

Let G be any group of order pq, let $P \in Syl_p(G)$ and let $Q \in Syl_q(G)$. In Example 1 of the applications of Sylow's Theorems we proved that $G \cong Q \rtimes P$, for some $\varphi : P \to \mathrm{Aut}(Q)$. Since P and Q are of prime order, they are cyclic. The group $\mathrm{Aut}(Q)$ is cyclic of order $q-1$. If p does not divide $q-1$, the only homomorphism from P to $\mathrm{Aut}(Q)$ is the trivial homomorphism, hence the only semidirect product in this case is the direct product, i.e., G is cyclic.

Consider now the case when $p \mid q-1$ and let $P = \langle y \rangle$. Since $\mathrm{Aut}(Q)$ is cyclic it contains a unique subgroup of order p, say $\langle \gamma \rangle$, and any homomorphism $\varphi : P \to \mathrm{Aut}(Q)$