7.15. Prove that $\text{Aut}(D_8) \cong D_8$, but that $\text{Aut}(D_{16}) \ncong D_{16}$.

7.16. Is $\text{Aut}(A_4) \cong S_4$? Is $\text{Aut}(A_6) \cong S_6$?

7.17. If $G = B \times K$ and $B \leq L \leq G$, then $L = B \times (L \cap K)$.

7.18. If $H \lhd G$, prove that

$$\{\varphi \in \text{Aut}(G): \varphi \text{ fixes } H \text{ pointwise and } \varphi(g)H = gH \text{ for all } g \in G\}$$

is an abelian subgroup of $\text{Aut}(G)$.

7.19. (i) Prove that the alternating groups A_n are never complete.
(ii) Show that if G is a complete group with $G \neq G'$, then G is not the commutator subgroup of any group containing it. Conclude that S_n, for $n \neq 2, 6$, is never a commutator subgroup.

7.20. If G is a complete group, then $\text{Hol}(G) = G^l \times G^r$. Conclude, for $n \neq 2$ and $n \neq 6$, that $\text{Hol}(S_n) \cong S_n \times S_n$.

7.21. Prove that every automorphism of a group G is the restriction of an inner automorphism of $\text{Hol}(G)$.

7.22. Let G be a group and let $f \in S_G$. Prove that $f \in \text{Hol}(G)$ if and only if $f(xy^{-1}z) = f(x)f(y)^{-1}f(z)$ for all $x, y, z \in G$.

Semidirect Products

Definition. Let K be a (not necessarily normal) subgroup of a group G. Then a subgroup $Q \leq G$ is a ***complement*** of K in G if $K \cap Q = 1$ and $KQ = G$.

A subgroup K of a group G need not have a complement and, even if it does, a complement need not be unique. In S_3, for example, every subgroup of order 2 serves as a complement to A_3. On the other hand, if they exist, complements are unique to isomorphism, for

$$G/K = KQ/K \cong Q/(K \cap Q) = Q/1 \cong Q.$$

A group G is the direct product of two normal subgroups K and Q if $K \cap Q = 1$ and $KQ = G$.

Definition. A group G is a ***semidirect product*** of K by Q, denoted by $G = K \rtimes Q$, if $K \lhd G$ and K has a complement $Q_1 \cong Q$. One also says that G ***splits*** over K.

We do not assume that a complement Q_1 is a normal subgroup; indeed, if Q_1 is a normal subgroup, then G is the direct product $K \times Q_1$.

In what follows, we denote elements of K by letters a, b, c in the first half of the alphabet, and we denote elements of Q by letters x, y, z at the end of the alphabet.

Before we give examples of semidirect products, let us give several different descriptions of them.

Lemma 7.20. *If K is a normal subgroup of a group G, then the following statements are equivalent:*

(i) *G is a semidirect product of K by G/K (i.e., K has a complement in G);*
(ii) *there is a subgroup $Q \leq G$ so that every element $g \in G$ has a unique expression $g = ax$, where $a \in K$ and $x \in Q$;*
(iii) *there exists a homomorphism $s: G/K \to G$ with $vs = 1_{G/K}$, where $v: G \to G/K$ is the natural map; and*
(iv) *there exists a homomorphism $\pi: G \to G$ with $\ker \pi = K$ and $\pi(x) = x$ for all $x \in \text{im}\, \pi$ (such a map π is called a **retraction** of G and $\text{im}\, \pi$ is called a **retract** of G).*

Proof. (i) ⇒ (ii) Let Q be a complement of K in G. Let $g \in G$. Since $G = KQ$, there exist $a \in K$ and $x \in Q$ with $g = ax$. If $g = by$ is a second such factorization, then $xy^{-1} = a^{-1}b \in K \cap Q = 1$. Hence $b = a$ and $y = x$.

(ii) ⇒ (iii) Each $g \in G$ has a unique expression $g = ax$, where $a \in K$ and $x \in Q$. If $Kg \in G/K$, then $Kg = Kax = Kx$; define $s: G/K \to G$ by $s(Kg) = x$. The routine verification that s is a well defined homomorphism with $vs = 1_{G/K}$ is left as an exercise for the reader.

(iii) ⇒ (iv) Define $\pi: G \to G$ by $\pi = sv$. If $x = \pi(g)$, then $\pi(x) = \pi(\pi(g)) = svsv(g) = sv(g) = \pi(g) = x$ (because $vs = 1_{G/K}$). If $a \in K$, then $\pi(a) = sv(a) = 1$, for $K = \ker v$. For the reverse inclusion, assume that $1 = \pi(g) = sv(g) = s(Kg)$. Now s is an injection, by set theory, so that $Kg = 1$ and so $g \in K$.

(iv) ⇒ (i) Define $Q = \text{im}\, \pi$. If $g \in Q$, then $\pi(g) = g$; if $g \in K$, then $\pi(g) = 1$; *a fortiori*, if $g \in K \cap Q$, then $g = 1$. If $g \in G$, then $g\pi(g^{-1}) \in K = \ker \pi$, for $\pi(g\pi(g^{-1})) = 1$. Since $\pi(g) \in Q$, we have $g = [g\pi(g^{-1})]\pi(g) \in KQ$. Therefore, Q is a complement of K in G and G is a semidirect product of K by Q. ∎

Example 7.7. S_n is a semidirect product of A_n by $\mathbb{Z}_2$.

Take $Q = \langle(1\ 2)\rangle$ to be a complement of A_n.

Example 7.8. D_{2n} is a semidirect product of $\mathbb{Z}_n$ by $\mathbb{Z}_2$.

If $D_{2n} = \langle a, x\rangle$, where $\langle a\rangle \cong \mathbb{Z}_n$ and $\langle x\rangle \cong \mathbb{Z}_2$, then $\langle a\rangle$ is normal and $\langle x\rangle$ is a complement of $\langle a\rangle$.

Example 7.9. For any group K, $\text{Hol}(K)$ is a semidirect product of K^l by $\text{Aut}(K)$.

This is contained in Lemma 7.16.

EXAMPLE 7.10. Let G be a solvable group of order mn, where $(m, n) = 1$. If G contains a normal subgroup of order m, then G is a semidirect product of K by a subgroup Q of order n.

This follows from P. Hall's theorem (Theorem 5.28).

EXAMPLE 7.11. $\mathrm{Aut}(S_6)$ is a semidirect product of S_6 by $\mathbb{Z}_2$.

This follows from P. Hall's theorem (Theorem 5.28).

EXAMPLE 7.12. If $G = \langle a \rangle$ is cyclic of order 4 and $K = \langle a^2 \rangle$, then G is not a semidirect product of K by G/K.

Since normality is automatic in an abelian group, an abelian group G is a semidirect product if and only if it is a direct product. But G is not a direct product. Indeed, it is easy to see that no primary cyclic group is a semidirect product.

EXAMPLE 7.13. Both S_3 and $\mathbb{Z}_6$ are semidirect products of $\mathbb{Z}_3$ by $\mathbb{Z}_2$.

Example 7.13 is a bit jarring at first, for it says, in contrast to direct product, that a semidirect product of K by Q is not determined to isomorphism by the two subgroups. When we reflect on this, however, we see that a semidirect product should depend on "how" K is normal in G.

Lemma 7.21. *If G is a semidirect product of K by Q, then there is a homomorphism $\theta: Q \to \mathrm{Aut}(K)$, defined by $\theta_x = \gamma_x | K$; that is, for all $x \in Q$ and $a \in K$,*

$$\theta_x(a) = xax^{-1}.$$

Moreover, for all $x, y, 1 \in Q$ and $a \in K$,

$$\theta_1(a) = a \quad \text{and} \quad \theta_x(\theta_y(a)) = \theta_{xy}(a).$$

Proof. Normality of K gives $\gamma_x(K) = K$ for all $x \in Q$. The rest is routine. ∎

Remark. It follows that K is a group with operators Q.

The object of our study is to recapture G from K and Q. It is now clear that G also involves a homomorphism $\theta: Q \to \mathrm{Aut}(K)$.

Definition. Let Q and K be groups, and let $\theta: Q \to \mathrm{Aut}(K)$ be a homomorphism. A semidirect product G of K by Q ***realizes*** θ if, for all $x \in Q$ and $a \in K$,

$$\theta_x(a) = xax^{-1}.$$

In this language, Lemma 7.21 says that every semidirect product G of K by Q determines some θ which it realizes. Intuitively, "realizing θ" is a way of

describing how K is normal in G. For example, if θ is the trivial map, that is, $\theta_x = 1_K$ for every $x \in G$, then $a = \theta_x(a) = xax^{-1}$ for every $a \in K$, and so $K \le C_G(Q)$.

Definition. Given groups Q and K and a homomorphism $\theta: Q \to \mathrm{Aut}(K)$, define $G = K \rtimes_\theta Q$ to be the set of all ordered pairs $(a, x) \in K \times Q$ equipped with the operation

$$(a, x)(b, y) = (a\theta_x(b), xy).$$

Theorem 7.22. *Given groups Q and K and a homomorphism $\theta: Q \to \mathrm{Aut}(K)$, then $G = K \rtimes_\theta Q$ is a semidirect product of K by Q that realizes θ.*

Proof. We first prove that G is a group. Multiplication is associative:

$$\begin{aligned} &[(a, x)(b, y)](c, z) && (a, x)[(b, y)(c, z)] \\ &= (a\theta_x(b), xy)(c, z) && = (a, x)(b\theta_y(c), yz) \\ &= (a\theta_x(b)\theta_{xy}(c), xyz), && = (a\theta_x(b\theta_y(c)), xyz). \end{aligned}$$

The formulas in Lemma 7.21 (K is a group with operators Q) show that the final entries in each column are equal.

The identity element of G is $(1, 1)$, for

$$(1, 1)(a, x) = (1\theta_1(a), 1x) = (a, x);$$

the inverse of (a, x) is $((\theta_{x^{-1}}(a))^{-1}, x^{-1})$, for

$$((\theta_{x^{-1}}(a))^{-1}, x^{-1})(a, x) = ((\theta_{x^{-1}}(a))^{-1}\theta_{x^{-1}}(a), x^{-1}x) = (1, 1).$$

We have shown that G is a group.

Define a function $\pi: G \to Q$ by $(a, x) \mapsto x$. Since the only "twist" occurs in the first coordinate, it is routine to check that π is a surjective homomorphism and that $\ker \pi = \{(a, 1): a \in K\}$; of course, $\ker \pi$ is a normal subgroup of G. We identify K with $\ker \pi$ via the isomorphism $a \mapsto (a, 1)$. It is also easy to check that $\{(1, x): x \in Q\}$ is a subgroup of G isomorphic to Q (via $x \mapsto (1, x)$), and we identify Q with this subgroup. Another easy calculation shows that $KQ = G$ and $K \cap Q = 1$, so that G is a semidirect product of K by Q.

Finally, G does realize θ:

$$(1, x)(a, 1)(1, x)^{-1} = (\theta_x(a), x)(1, x^{-1}) = (\theta_x(a), 1). \quad ∎$$

Since $K \rtimes_\theta Q$ realizes θ, that is, $\theta_x(b) = xbx^{-1}$, there can be no confusion if we write $b^x = xbx^{-1}$ instead of $\theta_x(b)$. The operation in $K \rtimes_\theta Q$ will henceforth be written

$$(a, x)(b, y) = (ab^x, xy).$$

Theorem 7.23. *If G is a semidirect product of K by Q, then there exists $\theta: Q \to \mathrm{Aut}(K)$ with $G \cong K \rtimes_\theta Q$.*

Proof. Define $\theta_x(a) = xax^{-1}$ (as in Lemma 7.21). By Lemma 7.20 (ii), each $g \in G$ has a unique expression $g = ax$ with $a \in K$ and $x \in Q$. Since multiplication in G satisfies

$$(ax)(by) = a(xbx^{-1})xy = ab^x xy,$$

it is easy to see that the map $K \rtimes_\theta Q \to G$, defined by $(a, x) \mapsto ax$, is an isomorphism. ∎

We now illustrate how this construction can be used.

EXAMPLE 7.14. The group T of order 12 (see Theorem 4.24) is a semidirect product of $\mathbb{Z}_3$ by $\mathbb{Z}_4$.

Let $\mathbb{Z}_3 = \langle a \rangle$, let $\mathbb{Z}_4 = \langle x \rangle$, and define $\theta: \mathbb{Z}_4 \to \mathrm{Aut}(\mathbb{Z}_3) \cong \mathbb{Z}_2$ by sending a into the generator. In more detail,

$$a^x = a^2 \qquad \text{and} \qquad (a^2)^x = a,$$

while x^2 acts on $\langle a \rangle$ as the identity automorphism: $a^{x^2} = a$.

The group $G = \mathbb{Z}_3 \rtimes_\theta \mathbb{Z}_4$ has order 12. If $s = (a^2, x^2)$ and $t = (1, x)$, then the reader may check that

$$s^6 = 1 \qquad \text{and} \qquad t^2 = s^3 = (st)^2,$$

which are the relations in T.

EXAMPLE 7.15. Let p be a prime, let $K = \langle a, b \rangle$ be an elementary abelian group of order p^2, and let $Q = \langle x \rangle$ be a cyclic group of order p. Define $\theta: Q \to \mathrm{Aut}(K) \cong \mathrm{GL}(2, p)$ by

$$x^i \mapsto \begin{bmatrix} 1 & 0 \\ i & 1 \end{bmatrix}.$$

Thus, $a^x = ab$ and $b^x = b$. The commutator $a^x a^{-1}$ is seen to be b. Therefore, $G = K \rtimes_\theta Q$ is a group of order p^3 with $G = \langle a, b, x \rangle$, and these generators satisfy relations

$$a^p = b^p = x^p = 1, \qquad b = [x, a], \qquad \text{and} \qquad [b, a] = 1 = [b, x].$$

If p is odd, then we have the nonabelian group of order p^3 and exponent p; if $p = 2$, then $G \cong D_8$ (as the reader may check). In Example 7.8, we saw that $D_8 \cong \mathbb{Z}_4 \rtimes_\theta \mathbb{Z}_2$; we have just seen here that $D_8 \cong \mathbf{V} \rtimes_\theta \mathbb{Z}_2$. A group may thus have distinct factorizations into a semidirect product.

EXAMPLE 7.16. Let p be an odd prime, let $K = \langle a \rangle$ be cyclic of order p^2, and let $Q = \langle x \rangle$ be cyclic of order p. By Theorem 7.3, $\mathrm{Aut}(K) \cong \mathbb{Z}_{p(p-1)} \cong \mathbb{Z}_{p-1} \times \mathbb{Z}_p$; indeed, by Theorem 6.9, the cyclic summand $\mathbb{Z}_p = \langle \alpha \rangle$, where $\alpha(a) = a^{1+p}$. If one defines $\theta: Q \to \mathrm{Aut}(K)$ by $\theta_x = \alpha$, then the group $G = K \rtimes_\theta Q$ has order p^3, generators x, a, and relations $x^p = 1$, $a^{p^2} = 1$, and $xax^{-1} = a^x = a^{1+p}$. We have constructed the second nonabelian group of order p^3 (see Exercise 4.32).

EXERCISES

7.23. Show that the group $\mathbf{Q}_n$ of generalized quaternions is not a semidirect product.

7.24. If $|G| = mn$, where $(m, n) = 1$, and if $K \leq G$ has order m, then a subgroup $Q \leq G$ is a complement of K if and only if $|Q| = n$.

7.25. If k is a field, then $\mathrm{GL}(n, k)$ is a semidirect product of $\mathrm{SL}(n, k)$ by $k^\times$, where $k^\times = k - \{0\}$.

7.26. If M is the group of all motions of $\mathbb{R}^n$, then M is a semidirect product of $\mathrm{Tr}(n, \mathbb{R})$ by $\mathrm{O}(n, \mathbb{R})$.

7.27. If K and Q are solvable, then $K \rtimes_\theta Q$ is also solvable.

7.28. Show that $K \rtimes_\theta Q$ is the direct product $K \times Q$ if and only if $\theta: Q \to \mathrm{Aut}(K)$ is ***trivial*** (that is, $\theta_x = 1$ for all $x \in Q$).

7.29. If p and q are distinct primes, construct all semidirect products of $\mathbb{Z}_p$ by $\mathbb{Z}_q$, and compare your results to Theorem 4.20. (The condition $q \nmid p - 1$ in that theorem should now be more understandable.)

Wreath Products

Let D and Q be groups, let Ω be a finite Q-set, and let $\{D_\omega: \omega \in \Omega\}$ be a family of isomorphic copies of D indexed by Ω.

Definition. Let D and Q be groups, let Ω be a finite Q-set, and let $K = \prod_{\omega \in \Omega} D_\omega$, where $D_\omega \cong D$ for all $\omega \in \Omega$. Then the ***wreath product*** of D by Q, denoted by $D \wr Q$ (or by D wr Q), is the semidirect product of K by Q, where Q acts on K by $q \cdot (d_\omega) = (d_{q\omega})$ for $q \in Q$ and $(d_\omega) \in \prod_{\omega \in \Omega} D_\omega$. The normal subgroup K of $D \wr Q$ is called the ***base*** of the wreath product.

The notation $D \wr Q$ is deficient, for it does not display the Q-set Ω; perhaps one should write $D \wr_\Omega Q$.

If D is finite, then $|K| = |D|^{|\Omega|}$; if Q is also finite, then $|D \wr Q| = |K \rtimes Q| = |K||Q| = |D|^{|\Omega|}|Q|$.

If Λ is a D-set, then $\Lambda \times \Omega$ can be made into a $(D \wr Q)$-set. Given $d \in D$ and $\omega \in \Omega$, define a permutation d_ω^* of $\Lambda \times \Omega$ as follows: for each $(\lambda, \omega') \in \Lambda \times \Omega$, set

$$d_\omega^*(\lambda, \omega') = \begin{cases} (d\lambda, \omega') & \text{if } \omega' = \omega, \\ (\lambda, \omega') & \text{if } \omega' \neq \omega. \end{cases}$$

It is easy to see that $d_\omega^* d_\omega'^* = (dd')_\omega^*$, and so D_ω^*, defined by

$$D_\omega^* = \{d_\omega^*: d \in D\},$$

is a subgroup of $S_{\Lambda \times \Omega}$; indeed, for each ω, the map $D \to D_\omega^*$, given by $d \mapsto d_\omega^*$, is an isomorphism.

For each $q \in Q$, define a permutation q^* of $\Lambda \times \Omega$ by

$$q^*(\lambda, \omega') = (\lambda, q\omega'),$$

and define

$$Q^* = \{q^*: q \in Q\}.$$

It is easy to see that Q^* is a subgroup of $S_{\Lambda\times\Omega}$ and that the map $Q \to Q^*$, given by $q \mapsto q^*$, is an isomorphism.

Theorem 7.24. *Given groups D and Q, a finite Q-set Ω, and a D-set Λ, then the wreath product $D \wr Q$ is isomorphic to the subgroup*

$$W = \langle Q^*, D^*_\omega: \omega \in \Omega \rangle \le S_{\Lambda\times\Omega},$$

and hence $\Lambda \times \Omega$ is a $(D \wr Q)$-set.

Proof. We show first that $K^* = \langle \bigcup_{\omega\in\Omega} D^*_\omega \rangle$ is the direct product $\prod_{\omega\in\Omega} D^*_\omega$. It is easy to see that D^*_ω centralizes $D^*_{\omega'}$ for all $\omega' \ne \omega$, and so $D^*_\omega \lhd K^*$ for every ω. Each $d^*_\omega \in D^*_\omega$ fixes all $(\lambda, \omega') \in \Lambda \times \Omega$ with $\omega' \ne \omega$, while each element of $\langle \bigcup_{\omega'\ne\omega} D^*_{\omega'} \rangle$ fixes all (λ, ω) for all $\lambda \in \Lambda$. It follows that if $d^*_\omega \in D^*_\omega \cap \langle \bigcup_{\omega'\ne\omega} D^*_{\omega'} \rangle$, then $d^*_\omega = 1$.

If $q \in Q$ and $\omega \in \Omega$, then a routine computation gives

$$q^* d^*_\omega q^{*-1} = d^*_{q\omega}$$

for each $\omega \in \Omega$. Hence $q^* K^* q^{*-1} \le K^*$ for each $q \in Q$, so that $K^* \lhd W$ (because $W = \langle K^*, Q^* \rangle$); it follows that $W = K^*Q^*$. To see that W is a semidirect product of K^* by Q^*, it suffices to show that $K^* \cap Q^* = 1$. Now $d^*_\omega(\lambda, \omega') = (d\lambda, \omega')$ or (λ, ω'); in either case, d^*_ω fixes the second coordinate. If $q^* \in Q^*$, then $q^*(\lambda, \omega') = (\lambda, q\omega')$ and q^* fixes the first coordinate. Therefore, any $g \in K^* \cap Q^*$ fixes every (λ, ω') and hence is the identity.

It is now a simple matter to check that the map $D \wr Q \to W$, given by $(d_\omega)q \mapsto (d^*_\omega)q^*$, is an isomorphism. ∎

Call the subgroup W of $S_{\Lambda\times\Omega}$ the ***permutation version*** of $D \wr Q$; when we wish to view $D \wr Q$ acting on $\Lambda \times \Omega$, then we will think of it as W.

Theorem 7.25. *Let D and Q be groups, let Ω be a finite Q-set, let Λ be a D-set, and let $W \le S_{\Lambda\times\Omega}$ be the permutation version of $D \wr Q$.*

(i) *If Ω is a transitive Q-set and Λ is a transitive D-set, then $\Lambda \times \Omega$ is a transitive $(D \wr Q)$-set.*

(ii) *If $\omega \in \Omega$, then its stabilizer Q_ω acts on $\Omega - \{\omega\}$. If $(\lambda, \omega) \in \Lambda \times \Omega$ and $D(\lambda) \le D$ is the stabilizer of λ, then the stabilizer $W_{(\lambda,\omega)}$ of (λ, ω) is isomorphic to $D(\lambda) \times (D \wr Q_\omega)$, and $[W : W_{(\lambda,\omega)}] = [D : D(\lambda)][Q : Q_\omega]$.*

Proof. (i) Let $(\lambda, \omega), (\lambda', \omega') \in \Lambda \times \Omega$. Since D acts transitively, there is $d \in D$ with $d\lambda = \lambda'$; since Q acts transitively, there is $q \in Q$ with $q\omega = \omega'$. The reader may now check that $q^* d^*_\omega(\lambda, \omega) = (\lambda', \omega')$.

(ii) Each element of W has the form $(d^*_\omega)q^*$, and $(d^*_\omega)q^*(\lambda, \omega) = (\prod_{\omega'\in\Omega} d^*_{\omega'})(\lambda, q\omega) = d^*_{q\omega}(\lambda, q\omega) = (d_{q\omega}\lambda, q\omega)$. It follows that $(d^*_\omega)q^*$ fixes (λ, ω) if and only if q fixes ω and d_ω fixes λ. Let $D^*_\omega(\lambda) = \{d^*_\omega: d \in D(\lambda)\}$. Now $D^*_\omega(\lambda)$ is disjoint from $\langle \prod_{\omega'\ne\omega} D^*_{\omega'}, Q^*_\omega \rangle$ and centralizes it: if $q^* \in Q^*_\omega$, then $q^* d^*_\omega q^{*-1} = d^*_{q\omega} = d^*_\omega$; hence

$$\begin{aligned} W_{(\lambda,\omega)} &= \left\langle D^*_\omega(\lambda), \prod_{\omega'\ne\omega} D^*_{\omega'}, Q^*_\omega \right\rangle \\ &= D^*_\omega(\lambda) \times \left\langle \prod_{\omega'\ne\omega} D^*_{\omega'}, Q^*_\omega \right\rangle \\ &\cong D(\lambda) \times (D \wr Q_\omega). \end{aligned}$$

It follows that $|W_{(\lambda,\omega)}| = |D(\lambda)||D|^{|\Omega|-1}|Q_\omega|$ and

$$[W : W_{(\lambda,\omega)}] = |D|^{|\Omega|}|Q|/|D(\lambda)||D|^{|\Omega|-1}|Q_\omega| = [D : D(\lambda)][Q : Q_\omega]. \quad ∎$$

Theorem 7.26. *Wreath product is associative: if both Ω and Λ are finite, if T is a group, and if Δ is a T-set, then $T \wr (D \wr Q) \cong (T \wr D) \wr Q$.*

Proof. The permutation versions of both $T \wr (D \wr Q)$ and $(T \wr D) \wr Q$ are subgroups of $S_{\Delta\times\Lambda\times\Omega}$; we claim that they coincide. The group $T \wr (D \wr Q)$ is generated by all $t^*_{(\lambda,\omega)}$ (for $t \in T$ and $(\lambda, \omega) \in \Lambda \times \Omega$) and all f^* (for $f \in D \wr Q$). Note that $t^*_{(\lambda,\omega)}: (\delta', \lambda', \omega') \mapsto (t\delta', \lambda', \omega')$ if $(\lambda', \omega') = (\lambda, \omega)$, and fixes it otherwise; also, $f^*: (\delta', \lambda', \omega') \mapsto (\delta', f(\lambda', \omega'))$. Specializing f^* to d^*_ω and to q^*, we see that $T \wr (D \wr Q)$ is generated by all $t^*_{(\lambda,\omega)}$, d^*_ω, and q^{**}, where $d^*_\omega: (\delta', \lambda', \omega') \mapsto (\delta', d\lambda', \omega')$ if $\omega' = \omega$, and fixes it otherwise, and $q^{**}: (\delta', \lambda', \omega') \mapsto (\delta', \lambda', q\omega')$.

A similar analysis of $(T \wr D) \wr Q$ shows that it is generated by all q^{**}, d^*_ω, and $(t_\lambda)^*_\omega$, where $(t_\lambda)^*_\omega: (\delta', \lambda', \omega') \mapsto (t\delta', \lambda', \omega')$ if $\omega' = \omega$ and $\lambda' = \lambda$, and fixes it otherwise. Since $(t_\lambda)^*_\omega = t^*_{(\lambda,\omega)}$, the two wreath products coincide. ∎

The best way to understand wreath products is by considering graphs.

Definition. A ***graph*** Γ is a nonempty set V, called ***vertices***, together with an ***adjacency*** relation on V, denoted by $v \sim u$, that is symmetric ($v \sim u$ implies $u \sim v$ for all $u, v \in V$) and irreflexive ($v \not\sim v$ for all $v \in V$).

One can draw pictures of finite graphs; regard the vertices as points and join each adjacent pair of vertices with a line segment or ***edge***. Notice that our graphs are *nondirected*; that is, one can traverse an edge in either direction; moreover, there are no "loops"; every edge has two distinct endpoints. An ***automorphism*** of a graph Γ with vertices V is a bijection $\varphi: V \to V$ such that $u, v \in V$ are adjacent if and only if $\varphi(u)$ and $\varphi(v)$ are adjacent. It is plain that the set of all automorphisms of a graph Γ, denoted by $\mathrm{Aut}(\Gamma)$, is a group under composition.

For example, consider the following graph Γ:

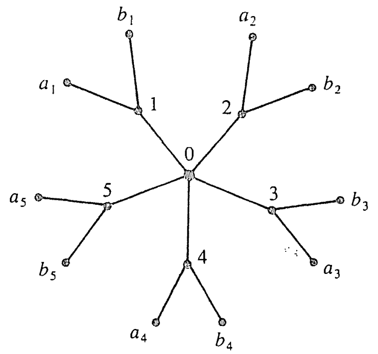

Figure 7.1

If $\varphi \in \text{Aut}(\Gamma)$, then φ fixes vertex 0 (it is the only vertex adjacent to 5 vertices), φ permutes the "inner ring" $\Omega = \{1, 2, 3, 4, 5\}$, and, for each i, either $\varphi(a_i) = a_{\varphi i}$ and $\varphi(b_i) = b_{\varphi i}$ or $\varphi(a_i) = b_{\varphi i}$ and $\varphi(b_i) = a_{\varphi i}$. It is now easy to see that $|\text{Aut}(\Gamma)| = 2^5 \times 5!$. Regard S_5 as acting on Ω and regard S_2 as acting on $\Lambda = \{a, b\}$. Identify the outer ring of all vertices $\{a_i, b_i: i \in \Omega\}$ with $\Lambda \times \Omega$ by writing a_i as (a, i) and b_i as (b, i). If $q \in S_5$, then q permutes the inner ring: $q^*(a_i) = a_{qi}$ and $q^*(b_i) = b_{qi}$; that is, $q^*(a, i) = (a, qi)$ and $q^*(b, i) = (b, qi)$. If $d \in S_2$ and $i \in \Omega$, then $d_i^*(a, i) = (da, i)$, $d_i^*(b, i) = (db, i)$, while d_i^* fixes (a, j) and (b, j) for $j \neq i$. For example, if d interchanges a and b, then $d_i^*(a_i) = b_i$ and $d_i^*(b_i) = a_i$, while d_i^* fixes a_j and b_j for all $j \neq i$. Thus, both q^* and d_i^* correspond to automorphisms of Γ. In Exercise 7.30 below, you will show that $\text{Aut}(\Gamma) \cong S_2 \wr S_5$.

A special case of the wreath product construction has $\Omega = Q$ regarded as a Q-set acting on itself by left multiplication. In this case, we write $W = D \wr_r Q$, and we call W the ***regular wreath product***. Thus, the base is the direct product of $|Q|$ copies of D, indexed by the elements of Q, and $q \in Q$ sends a $|Q|$-tuple $(d_x) \in \prod_{x \in Q} D_x$ into (d_{qx}). Note that $|D \wr_r Q| = |D|^{|Q|}|Q|$. It is easy to see that the formation of regular wreath products is *not* associative when all groups are finite, for $|T \wr_r (D \wr_r Q)| \neq |(T \wr_r D) \wr_r Q|$.

If Ω is an infinite set and $\{D_\omega: \omega \in \Omega\}$ is a family of groups, then there are two direct product constructions. The first, sometimes called the *complete direct product*, consists of all "vectors" (d_ω) in the cartesian product $\prod_{\omega \in \Omega} D_\omega$ with "coordinatewise" multiplication: $(d_\omega)(d'_\omega) = (d_\omega d'_\omega)$. The second, called the *restricted direct product*, is the subgroup of the first consisting of all those (d_ω) with only finitely many coordinates $d_\omega \neq 1$. Both versions coincide when the index set Ω is finite. The wreath product using the complete direct product is called the ***complete wreath product***; the wreath product using the restricted direct product is called the ***restricted wreath product***. We shall see a use for the complete wreath product at the end of the next section. The

first example of a (necessarily infinite) centerless p-group was given by D.H. McLain (1954); it is a restricted wreath product of a group of prime order p by $\mathbb{Z}(p^\infty)$ (the latter group is discussed in Chapter 10; it is the multiplicative group of all pth power roots of unity). McLain's example is thus a p-group that is not nilpotent.

What is the order of a Sylow p-subgroup of the symmetric group S_m? If $k \leq m$ are positive integers, define $t = [m/k]$, the greatest integer in m/k. Thus, $k, 2k, \ldots, tk \leq m$, while $(t + 1)k > m$, so that t is the number of integers $i \leq m$ which are divisible by k. If p is a prime, what is the largest power μ of p dividing $m!$? Think of $m!$ as factored: $m! = 2 \times 3 \times 4 \times \cdots \times m$. By our initial remark, $[m/p]$ factors of $m!$ are divisible by p, $[m/p^2]$ factors are divisible by p^2, etc. Hence, if $m! = p^\mu m'$, where $(m', p) = 1$, then

$$\mu = [m/p] + [m/p^2] + [m/p^3] + \cdots.$$

For example, if $p = 2$, then $[m/2]$ is the number of even integers $\leq m$, $[m/4]$ is the number of multiples of $4 \leq m$, and so forth. (Notice, for example, that $8 = 2^3$ is counted three times by the formula for μ.) In particular, if $m = p^n$, then the largest power of p dividing $p^n!$ is

$$\mu = \mu(n) = p^{n-1} + p^{n-2} + \cdots + p + 1,$$

and so the order of a Sylow p-subgroup of the symmetric group S_{p^n} is $p^{\mu(n)}$.

Theorem 7.27 (Kaloujnine, 1948). *If p is a prime, then a Sylow p-subgroup of S_{p^n} is an iterated regular wreath product $W_n = \mathbb{Z}_p \wr_r \mathbb{Z}_p \wr_r \cdots \wr_r \mathbb{Z}_p$ of n copies of $\mathbb{Z}_p$, where $W_{n+1} = W_n \wr_r \mathbb{Z}_p$.*

Proof. The proof is by induction on n, the case $n = 1$ holding because a Sylow p-subgroup of S_p has order p. Assume that $n > 1$. Let Λ be a set with p^n elements and let D be a Sylow p-subgroup of S_Λ; thus, Λ is a D-set. Let $\Omega = \{0, 1, \ldots, p - 1\}$, and let $Q = \langle q \rangle$ be a cyclic group of order p acting on Ω by $qi = i + 1 \bmod p$. The permutation version of the wreath product $P = D \wr_r \mathbb{Z}_p$ is a subgroup of $S_{\Lambda \times \Omega}$; of course, $|\Lambda \times \Omega| = p^{n+1}$. By induction, D is a wreath product of n copies of $\mathbb{Z}_p$, and so P is a wreath product of $n + 1$ copies of $\mathbb{Z}_p$. To see that P is a Sylow p-subgroup, it suffices to see that its order is $p^{\mu(n+1)}$, where $\mu(n + 1) = p^n + p^{n-1} + \cdots + p + 1$. Now $|D| = p^{\mu(n)}$, so that $|P| = |D \wr_r \mathbb{Z}_p| = (p^{\mu(n)})^p p = p^{p\mu(n)+1} = p^{\mu(n+1)}$. ∎

Theorem 7.27 may be used to compute the Sylow p-subgroup of S_m for any m (not necessarily a power of p). First write m in base p:

$$m = a_0 + a_1 p + a_2 p^2 + \cdots a_t p^t, \qquad \text{where} \quad 0 \leq a_i \leq p - 1.$$

Partition $X = \{1, 2, \ldots, m\}$ into a_0 singletons, a_1 p-subsets, a_2 p^2-subsets, $\ldots$, and a_t p^t-subsets. On each of these p^i-subsets Y, construct a Sylow p-subgroup of S_Y. Since disjoint permutations commute, the direct product of all these Sylow subgroups is a subgroup of S_X of order p^N, where $N = a_1 + a_2\mu(2) + \cdots + a_t\mu(t)$ (recall that $\mu(i) = p^{i-1} + p^{i-2} + \cdots + p + 1$). But p^N is the highest power of p dividing $m!$, for

$$m = a_0 + a_1 p + a_2 p^2 + \cdots + a_t p^t,$$

and so

$$\begin{aligned}[m/p] + [m/p^2] + [m/p^3] + \cdots &= (a_1 + a_2 p + a_3 p^2 + \cdots + a_t p^{t-1}) \\ &\quad + (a_2 + a_3 p + a_4 p^2 + \cdots + a_t p^{t-2}) \\ &\quad + (a_3 + a_4 p + \cdots + a_t p^{t-3}) + \cdots \\ &= a_1 + a_2(p+1) + a_3(p^2 + p + 1) + \cdots \\ &= a_1 + a_2 \mu(2) + \cdots + a_t \mu(t) = N.\end{aligned}$$

Thus, the direct product has the right order, and so it must be a Sylow p-subgroup of $S_X \cong S_m$.

For example, let us compute a Sylow 2-subgroup of S_6 (this has been done by hand in Exercise 4.15 (ii)). In base 2, we have $6 = 0 \times 1 + 1 \times 2 + 1 \times 4$. A Sylow 2-subgroup of S_2 is $\mathbb{Z}_2$; a Sylow 2-subgroup of S_4 is $\mathbb{Z}_2 \wr \mathbb{Z}_2$. We conclude that a Sylow 2-subgroup P of S_6 is $\mathbb{Z}_2 \times (\mathbb{Z}_2 \wr \mathbb{Z}_2)$. By Exercise 7.31 below, $\mathbb{Z}_2 \wr \mathbb{Z}_2 \cong D_8$, so that $P \cong \mathbb{Z}_2 \times D_8$.

EXERCISES

7.30. Prove that $\mathrm{Aut}(\Gamma) \cong S_2 \wr S_5$, where Γ is the graph in Figure 7.1. (*Hint.* Every $\varphi \in \mathrm{Aut}(\Gamma)$ is completely determined by its behavior on the outer ring consisting of all vertices of the form a_i or b_i.)

7.31. Prove that $\mathbb{Z}_2 \wr \mathbb{Z}_2 \cong D_8$. (*Hint.* $\mathbb{Z}_2 \wr \mathbb{Z}_2$ has several involutions.)

7.32. If both D and Q are solvable, then $D \wr Q$ is solvable.

7.33. **Definition.** Let D be a (multiplicative) group. A ***monomial matrix μ over D*** is a permutation matrix P whose nonzero entries have been replaced by elements of D; we say that P is the ***support*** of μ. If Q is a group of $n \times n$ permutation matrices, then

$$M(D, Q) = \{\text{all monomial matrices } \mu \text{ over } D \text{ with support in } Q\}.$$

(i) Prove that $M(D, Q)$ is a group under matrix multiplication.
(ii) Prove that the subgroup $Q \cong M(1, Q) \leq M(D, Q)$.
(iii) Prove that the diagonal $M(D, 1)$ is isomorphic to the direct product $D \times \cdots \times D$ (n times).
(iv) Prove that $M(D, 1) \lhd M(D, Q)$ and that $M(D, Q)$ is a semidirect product of $M(D, 1)$ by $M(1, Q)$.
(v) Prove that $M(D, Q) \cong D \wr Q$.

7.34. (i) Fix a group Q and a finite Q-set Ω. For all groups D and A and all homomorphisms $f: D \to A$, there is a homomorphism $M(f): M(D, Q) \to M(A, Q)$ such that $M(1_D) = 1_{M(D,Q)}$ and, whenever $g: A \to B$, then $M(gf) = M(g)M(f)$. (*Hint.* Just replace every nonzero entry x of a monomial matrix over D by $f(x)$.) (In categorical language, this exercise shows that wreath product is a functor.)

(ii) If D is abelian, show that determinant $d: M(D, Q) \to D$ is a (well defined) homomorphism.

7.35. If $(a, x) \in D \wr Q$ (so that $a \in K = \prod D_\omega$), then

$$(a, x)^n = (aa^x a^{x^2} \ldots a^{x^{n-1}}, x^n).$$

7.36. Let $X = B_1 \cup \cdots \cup B_m$ be a partition of a set X in which each B_i has k elements. If

$$G = \{g \in S_X: \text{for each } i, \text{ there is } j \text{ with } g(B_i) = B_j\},$$

then $G \cong S_k \wr S_m$.

Factor Sets

Since there are nonsimple groups that are not semidirect products, our survey of extensions is still incomplete. Notice the kind of survey we already have: if we know Q, K, and θ, then we know the semidirect product $K \rtimes_\theta Q$ in the sense that we can write a multiplication table for it (its elements are ordered pairs and we know how to multiply any two of them).

In discussing general extensions G of K by Q, it is convenient to use the additive notation for G and its subgroup K (this is one of the rare instances in which one uses additive notation for a nonabelian group). For example, if $k \in K$ and $g \in G$, we shall write the conjugate of k by g as $g + k - g$.

Definition. If $K \leq G$, then a ***(right) transversal*** of K in G (or a *complete set of right coset representatives*) is a subset T of G consisting of one element from each right coset of K in G.

If T is a right transversal, then G is the disjoint union $G = \bigcup_{t \in T} K + t$. Thus, every element $g \in G$ has a unique factorization $g = k + t$ for $k \in K$ and $t \in T$. There is a similar definition of left transversal; of course, these two notions coincide when K is normal.

If G is a semidirect product and Q is a complement of K, then Q is a transversal of K in G.

Definition. If $\pi: G \to Q$ is surjective, then a ***lifting*** of $x \in Q$ is an element $l(x) \in G$ with $\pi(l(x)) = x$.

If one chooses a lifting $l(x)$ for each $x \in Q$, then the set of all such is a transversal of $\ker \pi$. In this case, the function $l: Q \to G$ is also called a ***right transversal*** (thus, both l and its image $l(Q)$ are called right transversals).

Theorem 7.28. *Let G be an extension of K by Q, and let $l: Q \to G$ be a transversal.*

If K is abelian, then there is a homomorphism $\theta: Q \to \mathrm{Aut}(K)$ with

$$\theta_x(a) = l(x) + a - l(x)$$