Abstract Algebra:

Supplementary

Lecture Notes

JOHN A. BEACHY

Northern Illinois University

1995

Revised, 1999, 2006

To accompany

Abstract Algebra, *Third Edition*
by John A. Beachy and William D. Blair

ISBN 1–57766–434–4, Copyright 2006

Waveland Press, Inc.
4180 IL Route 83, Suite 101
Long Grove, Illinois 60047
847 / 634-0081

Formatted January 12, 2007, at which time the original was available at:

http://www.math.niu.edu/~beachy/abstract_algebra/

Contents

PREFACE

These notes are provided as a supplement to the book **Abstract Algebra**, *Third Edition*, by John A. Beachy and William D. Blair, Waveland Press, 2006.

The notes are intended for the use of graduate students who are studying from our text and need to cover additional topics.

John A. Beachy
October, 2006

Chapter 7

STRUCTURE OF GROUPS (cont'd)

7.8 Nilpotent Groups

We now define and study a class of solvable groups that includes all finite abelian groups and all finite p-groups. This class has some rather interesting properties.

7.8.1 Definition. *For a group G we define the* ***ascending central series*** $Z_1(G) \subseteq Z_2(G) \subseteq \cdots$ *of G as follows:*

$Z_1(G)$ is the center $Z(G)$ of G;

$Z_2(G)$ is the unique subgroup of G with $Z_1(G) \subseteq Z_2(G)$ and $Z_2(G)/Z_1(G) = Z(G/Z_1(G))$.

We define $Z_i(G)$ inductively, so that $Z_i(G)/Z_{i-1}(G) = Z(G/Z_{i-1}(G))$.

The group G is called ***nilpotent*** *if there exists a positive integer n with $Z_n(G) = G$.*

We first note that any abelian group is nilpotent. We next note that any nilpotent group is solvable, since the factor groups $Z_{i+1}(G)/Z_i(G)$ are abelian. We also note that these classes are distinct. The proof of Theorem 7.6.3 shows that any finite p-group is nilpotent, so the group of quaternion units provides an example of a group that is nilpotent but not abelian. The symmetric group S_3 is solvable, but it is not nilpotent since its center is trivial.

We will show that the converse of Lagrange's theorem holds for nilpotent groups. Recall that the standard counterexample to the converse of Lagrange's theorem is the alternating group A_4, which has 12 elements but no subgroup of order 6. We note that A_4 is another example of a solvable group that is not nilpotent. It follows from Theorem 7.4.1, the first Sylow theorem, that any finite p-group has subgroups of all possible orders. This result can be easily extended to any group that is a direct product of p-groups. Thus the converse of Lagrange's theorem holds for any finite abelian group, and this argument will also show (see Corollary 7.8.5) that it holds for any finite nilpotent group.

We first prove that any finite direct product of nilpotent groups is nilpotent.

7.8.2 Proposition. *If $G_1, G_2, \ldots, G_n$ are nilpotent groups, then so is*

$$G = G_1 \times G_2 \times \cdots \times G_n \ .$$

Proof. It is immediate that an element $(a_1, a_2, \ldots, a_n)$ belongs to the center $Z(G)$ of G if and only if each component a_i belongs to $Z(G_i)$. Thus factoring out $Z(G)$ yields

$$G/Z(G) = (G_1/Z(G_1)) \times \cdots \times (G_n/Z(G_n)) \ .$$

Using the description of the center of a direct product of groups, we see that

$$Z_2(G) = Z_2(G_1) \times \cdots \times Z_2(G_n) \ ,$$

and this argument can be continued inductively. If m is the maximum of the lengths of the ascending central series for the factors G_i, then it is clear that the ascending central series for G will terminate at G after at most m terms. □

The following theorem gives our primary characterization of nilpotent groups. We first need a lemma about the normalizer of a Sylow subgroup.

7.8.3 Lemma. *If P is a Sylow p-subgroup of a finite group G, then the normalizer $N(P)$ is equal to its own normalizer in G.*

Proof. Since P is normal in $N(P)$, it is the unique Sylow p-subgroup of $N(P)$. If g belongs to the normalizer of $N(P)$, then $gN(P)g^{-1} \subseteq N(P)$, so $gPg^{-1} \subseteq N(P)$, which implies that $gPg^{-1} = P$. Thus $g \in N(P)$. □

7.8.4 Theorem. *The following conditions are equivalent for any finite group G.*

(1) *G is nilpotent;*

(2) *no proper subgroup H of G is equal to its normalizer $N(H)$;*

(3) *every Sylow subgroup of G is normal;*

(4) *G is a direct product of its Sylow subgroups.*

Proof. (1) implies (2): Assume that G is nilpotent and H is a proper subgroup of G. With the notation $Z_0(G) = \{e\}$, let n be the largest index such that $Z_n(G) \subseteq H$. Then there exists $a \in Z_{n+1}(G)$ with $a \notin H$. For any $h \in H$, the cosets $aZ_n(G)$ and $hZ_n(G)$ commute in $G/Z_n(G)$, so $aha^{-1}h^{-1} \in Z_n(G) \subseteq H$, which shows that $aha^{-1} \in H$. Thus $a \in N(H) - H$, as required.

(2) implies (3): Let P be a Sylow p-subgroup of G. By Lemma 7.8.3, the normalizer $N(P)$ is equal to its own normalizer in G, so by assumption we must have $N(P) = G$. This implies the P is normal in G.

(3) implies (4): Let $P_1, P_2, \ldots, P_n$ be the Sylow subgroups of G, corresponding to prime divisors $p_1, p_2, \ldots, p_n$ of $|G|$. We can show inductively that $P_1 \cdots P_i \cong P_1 \times \cdots \times P_i$ for $i = 2, \ldots, n$. This follows immediately from the observation that $(P_1 \cdots P_i) \cap P_{i+1} = \{e\}$ because any element in P_{i+1} has an order which is a power of p_{i+1}, whereas the order of an element in $P_1 \times \cdots \times P_i$ is $p_1^{k_1} \cdots p_i^{k_i}$, for some integers $k_1, \ldots, k_n$.

(4) implies (3): This follows immediately from Proposition 7.8.2 and the fact that any p-group is nilpotent (see Theorem 7.6.3). □

7.8.5 Corollary. *Let G be a finite nilpotent group of order n. If m is any divisor of n, then G has a subgroup of order m.*

Proof. Let $m = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ be the prime factorization of m. For each prime power $p_i^{\alpha_i}$, the corresponding Sylow p_i-subgroup of G has a subgroup of order $p_i^{\alpha_i}$. The product of these subgroups has order m, since G is a direct product of its Sylow subgroups. □

7.8.6 Lemma (Frattini's Argument). *Let G be a finite group, and let H be a normal subgroup of G. If P is any Sylow subgroup of H, then $G = H \cdot N(P)$, and $[G : H]$ is a divisor of $|N(P)|$.*

Proof. Since H is normal in G, it follows that the product $HN(P)$ is a subgroup of G. If $g \in G$, then $gPg^{-1} \subseteq H$ since H is normal, and thus gPg^{-1} is also a Sylow subgroup of H. The second Sylow theorem (Theorem 7.7.4) implies that P and gPg^{-1} are conjugate in H, so there exists $h \in H$ with $h(gPg^{-1})h^{-1} = P$. Thus $hg \in N(P)$, and so $g \in HN(P)$, which shows that $G = HN(P)$.

It follows from the first isomorphism theorem (Theorem 7.1.1) that $G/H \cong N(P)/(N(P) \cap H)$, and so $|G/H|$ is a divisor of $|N(P)|$. □

7.8.7 Proposition. *A finite group is nilpotent if and only if every maximal subgroup is normal.*

Proof. Assume that G is nilpotent, and H is a maximal subgroup of G. Then H is a proper subset of $N(H)$ by Theorem 7.8.4 and so $N(H)$ must equal G, showing that H is normal.

Conversely, suppose that every maximal subgroup of G is normal, let P be any Sylow subgroup of G, and assume that P is not normal. Then $N(P)$ is a proper subgroup of G, so it is contained in a maximal subgroup H, which is normal by assumption. Since P is a Sylow subgroup of G, it is a Sylow subgroup of H, so the conditions of Lemma 7.8.6 hold, and $G = HN(P)$. This is a contradiction, since $N(P) \subseteq H$. □

EXERCISES: SECTION 7.8

1. Show that the group G is nilpotent if $G/Z(G)$ is nilpotent.
2. Show that each term $Z_i(G)$ in the ascending central series of a group G is a characteristic subgroup of G.
3. Show that any subgroup of a finite nilpotent group is nilpotent.
4. (a) Prove that D_n is solvable for all n.

   (b) Find necessary and sufficient conditions on n such that D_n is nilpotent.
5. Use Theorem 7.8.7 to prove that any factor group of a finite nilpotent group is again nilpotent.

7.9 Semidirect Products

The direct product of two groups does not allow for much complexity in the way in which the groups are put together. For example, the direct product of two abelian groups is again abelian. We now give a more general construction that includes some very useful and interesting examples. We recall that a group G is isomorphic to $N \times K$, for subgroups N, K, provided (i) N and K are normal in G; (ii) $N \cap K = \{e\}$; and (iii) $NK = G$. (See Theorem 7.1.3.)

7.9.1 Definition. *Let G be a group with subgroups N and K such that*

(i) *N is normal in G;*

(ii) *$N \cap K = \{e\}$; and*

(iii) *$NK = G$.*

Then G is called the ***semidirect product*** *of N and K.*

Example 7.9.1 (S_3 is a semidirect product).

Let $S_3 = \{e, a, a^2, b, ab, a^2b\}$ be the symmetric group on three elements, and let $N = \{e, a, a^2\}$ and $K = \{e, b\}$. Then the subgroup N is normal, and it is clear that $N \cap K = \{e\}$ and $NK = G$. Thus S_3 is the semidirect product of N and K. $\square$

The difference in complexity of direct products and semidirect products can be illustrated by the following examples.

Example 7.9.2.

Let F be a field, let G_1 be a subgroup of $\mathrm{GL}_n(F)$, and let G_2 be a subgroup of $\mathrm{GL}_m(F)$. The subset of $\mathrm{GL}_{n+m}(F)$ given by

$$\left\{ \left[\begin{array}{cc} A_1 & 0 \\ 0 & A_2 \end{array} \right] \middle| A_1 \in G_1, \quad A_2 \in G_2 \right\}$$

is easily seen to be isomorphic to $G_1 \times G_2$. $\square$

The above example suggests that since a matrix construction can be given for certain direct products, we might be able to construct semidirect products by considering other sets of matrices.

Example 7.9.3.

Let F be a field, and let G be the subgroup of $\mathrm{GL}_2(F)$ defined by

$$G = \left\{ \left[\begin{array}{cc} 1 & 0 \\ x & a \end{array} \right] \middle| x, a \in F, \quad a \neq 0 \right\} .$$

For the product of two elements, with $x_1, a_1, x_2, a_2 \in F$, we have

$$\left[\begin{array}{cc} 1 & 0 \\ x_1 & a_1 \end{array} \right] \left[\begin{array}{cc} 1 & 0 \\ x_2 & a_2 \end{array} \right] = \left[\begin{array}{cc} 1 & 0 \\ x_1 + a_1 x_2 & a_1 a_2 \end{array} \right] .$$

The determinant defines a group homomorphism $\delta : G \to F^\times$, where $\ker(\delta)$ is the set of matrices in G of the form $\left[\begin{array}{cc} 1 & 0 \\ x & 1 \end{array} \right]$. Let N be the normal subgroup $\ker(\delta)$, and let K be the set of all matrices of the form $\left[\begin{array}{cc} 1 & 0 \\ 0 & a \end{array} \right]$. It is clear that $N \cap K$ is the identity matrix, and the computation

$$\left[\begin{array}{cc} 1 & 0 \\ x & 1 \end{array} \right] \left[\begin{array}{cc} 1 & 0 \\ 0 & a \end{array} \right] = \left[\begin{array}{cc} 1 & 0 \\ x & a \end{array} \right]$$

shows that $NK = G$ Thus G is the semidirect product of N and K.

It is easy to check that $N \cong F$ and $K \cong F^\times$. Finally, we note that if $-1 \neq 1$ in F, then for the elements

$$A = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \qquad \text{and} \qquad B = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

we have $BA = A^{-1}B \neq AB$, showing that G is not abelian. □

Example 7.9.4 (Construction of $\mathcal{H}_p$)).

Let p be a prime number. We next consider the **holomorph** of $\mathbf{Z}_p$, which we will denote by $\mathcal{H}_p$. It is defined as follows. (Recall that $\mathbf{Z}_p^\times$ is group of invertible elements in $\mathbf{Z}_p$, and has order $p-1$.)

$$\mathcal{H}_p = \left\{ \begin{bmatrix} 1 & 0 \\ a_{21} & a_{22} \end{bmatrix} \middle| a_{21} \in \mathbf{Z}_p, \quad a_{22} \in \mathbf{Z}_p^\times \right\}$$

Thus $\mathcal{H}_p$ is a subgroup of $\mathrm{GL}_2(\mathbf{Z}_p)$, with subgroups

$$N = \left\{ \begin{bmatrix} 1 & 0 \\ a_{21} & a_{22} \end{bmatrix} \middle| a_{21} \in \mathbf{Z}_p, \quad a_{22} = 1 \right\}$$

and

$$K = \left\{ \begin{bmatrix} 1 & 0 \\ a_{21} & a_{22} \end{bmatrix} \middle| a_{21} = 0, \quad a_{22} \in \mathbf{Z}_p^\times \right\} .$$

It is clear that $N \cap K = \{e\}$, $NK = \mathcal{H}_p$, and it can easily be checked that N is a normal subgroup isomorphic to $\mathbf{Z}_p$, and K is isomorphic to $\mathbf{Z}_p^\times$. Thus $\mathcal{H}_p$ is a semidirect product of subgroups isomorphic to $\mathbf{Z}_p$ and $\mathbf{Z}_p^\times$, respectively. □

Example 7.9.5.

The matrix construction of semidirect products can be extended to larger matrices, in block form. Let F be a field, let G be a subgroup of $\mathrm{GL}_n(F)$. and let X be a subspace of the n-dimensional vector space F^n such that $Ax \in X$ for all vectors $x \in X$ and matrices $A \in G$. Then the set of all $(n+1) \times (n+1)$ matrices of the form $\begin{bmatrix} 1 & 0 \\ x & A \end{bmatrix}$ such that $x \in X$ and $A \in G$ defines a group.

For example, we could let G be the subgroup of $\mathrm{GL}_2(\mathbf{Z}_2)$ consisting of $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ and $\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$, and we could let X be the set of vectors

$$\left\{ \begin{bmatrix} 0 \\ 0 \end{bmatrix}, \quad \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \quad \begin{bmatrix} 0 \\ 1 \end{bmatrix}, \quad \begin{bmatrix} 1 \\ 1 \end{bmatrix} \right\} . \ □$$

Example 7.9.6 (D_n is a semidirect product).

> Consider the dihedral group D_n, described by generators a of order n and b of order 2, with the relation $ba = a^{-1}b$. Then $\langle a \rangle$ is a normal subgroup, $\langle a \rangle \cap \langle b \rangle = \{e\}$, and $\langle a \rangle \langle b \rangle = D_n$. Thus the dihedral group is a semidirect product of cyclic subgroups of order n and 2, respectively. $\square$

We have said that a group G is a semidirect product of its subgroups N and K if (i) N is normal; (ii) $N \cap K = \{e\}$; and (iii) $NK = G$. This describes an "internal" semidirect product. We now use the automorphism group to give a general definition of an "external" semidirect product.

7.9.2 Definition. *Let G be a multiplicative group, and let X be an abelian group, denoted additively. Let $\mu : G \to \mathrm{Aut}(X)$ be a group homomorphism. The* ***semidirect product of*** X ***and*** G ***relative to*** μ *is defined to be*

$$X \rtimes_\mu G = \{(x, a) \mid x \in X, \quad a \in G\}$$

with the operation $(x_1, a_1)(x_2, a_2) = (x_1 + \mu(a_1)[x_2],\ a_1a_2)$, for $x_1, x_2 \in X$ and $a_1, a_2 \in G$.

For any multiplicative group G and any additive group X there is always the trivial group homomorphism $\mu : G \to \mathrm{Aut}(X)$ which maps each element of G to the identity mapping in $\mathrm{Aut}(X)$. Using this homomorphism, the semidirect product $X \rtimes_\mu G$ reduces to the direct product $X \times G$.

7.9.3 Proposition. *Let G be a multiplicative group, let X be an additive group, and let $\mu : G \to \mathrm{Aut}(X)$ be a group homomorphism.*

(a) *The semidirect product $X \rtimes_\mu G$ is a group.*

(b) *The set $\{(x, a) \in X \rtimes_\mu G \mid x = 0\}$ is a subgroup of $X \rtimes_\mu G$ that is isomorphic to G.*

(c) *The set $N = \{(x, a) \in X \rtimes_\mu G \mid a = e\}$ is a normal subgroup of $X \rtimes_\mu G$ that is isomorphic to X, and $(X \rtimes_\mu G)/N$ is isomorphic to G.*

Proof. (a) The associative law holds since

$$\begin{aligned}
((x_1, a_1)(x_2, a_2))(x_3, a_3) &= (x_1 + \mu(a_1)[x_2],\ a_1a_2)(x_3, a_3) \\
&= ((x_1 + \mu(a_1)[x_2]) + \mu(a_1a_2)[x_3],\ (a_1a_2)a_3)
\end{aligned}$$

and

$$\begin{aligned}(x_1, a_1)((x_2, a_2)(x_3, a_3)) &= (x_1, a_1)(x_2 + \mu(a_2)[x_3],\ a_2a_3) \\ &= (x_1 + \mu(a_1)[x_2 + \mu(a_2)[x_3]],\ a_1(a_2a_3))\end{aligned}$$

and these elements are equal because

$$\mu(a_1)[x_2] + \mu(a_1a_2)[x_3] = \mu(a_1)[x_2] + \mu(a_1)\mu(a_2)[x_3] = \mu(a_1)[x_2 + \mu(a_2)[x_3]]\ .$$

The element $(0, e)$ is an identity, and the inverse of (x, a) is $(\mu(a)^{-1}[-x], a^{-1})$, as shown by the following computation.

$$\begin{aligned}(x, a)(\mu(a)^{-1}[-x], a^{-1}) &= (x + \mu(a)\mu(a)^{-1}[-x], aa^{-1}) = (0, e) \\ (\mu(a)^{-1}[-x], a^{-1})(x, a) &= (\mu(a)^{-1}[-x] + \mu(a)^{-1}[x], a^{-1}a) = (0, e)\end{aligned}$$

(b) Define $\phi : G \to X \rtimes_\mu G$ by $\phi(a) = (0, a)$, for all $a \in G$. It is clear that ϕ is a one-to-one homomorphism and that the image $\phi(G)$ is the required subgroup.

(c) It is clear that X is isomorphic to N. Define $\pi : X \rtimes_\mu G \to G$ by $\pi(x, a) = a$, for all $(x, a) \in X \rtimes_\mu G$. The definition of multiplication in $X \rtimes_\mu G$ shows that π is a homomorphism. It is onto, and $\ker(\pi) = N$. The fundamental homomorphism theorem shows that $(X \rtimes_\mu G)/N \cong G$. □

Example 7.9.7 ($\mathcal{H}_n$).

Let X be the cyclic group $\mathbf{Z}_n$, with $n \geq 2$. Example 7.1.6 shows that $\mathrm{Aut}(X) \cong \mathbf{Z}_n^\times$, and if $\mu : \mathbf{Z}_n^\times \to \mathrm{Aut}(X)$ is the isomorphism defined in Example 7.1.6, we have $\mu(a)[m] = am$, for all $a \in \mathbf{Z}_n^\times$ and all $m \in \mathbf{Z}_n$. Thus $\mathbf{Z}_n \rtimes_\mu \mathbf{Z}_n^\times$ has the multiplication

$$(m_1, a_1)(m_2, a_2) = (m_1 + a_1m_2, a_1a_2)\ .$$

If n is prime, this gives us the holomorph $\mathcal{H}_p$ of $\mathbf{Z}_p$.

We can now give a more general definition. We say that $\mathbf{Z}_n \rtimes_\mu \mathbf{Z}_n^\times$ is the **holomorph** of $\mathbf{Z}_n$, denoted by $\mathcal{H}_n$. □

Example 7.9.8.

Let X be the cyclic group $\mathbf{Z}_n$, with $n \geq 2$. If $\theta : \mathbf{Z}_n^\times \to \mathrm{Aut}(X)$ maps each element of $\mathbf{Z}_n^\times$ to the identity automorphism, then $\mathbf{Z}_n \rtimes_\theta \mathbf{Z}_n^\times \cong \mathbf{Z}_n \times \mathbf{Z}_n^\times$. This illustrates the strong dependence of $X \rtimes_\theta G$ on the homomorphism θ, since $\mathcal{H}_n$ is not abelian and hence cannot be isomorphic to $\mathbf{Z}_n \times \mathbf{Z}_n^\times$. □

Example 7.9.9 (D_n is a semidirect product).

> We have already shown in Example 7.9.6 that D_n is an "internal" semidirect product, using the standard generators and relations. We can now give an alternate proof that the dihedral group is a semidirect product. Let
>
> $$G = \left\{ \left[\begin{array}{cc} 1 & 0 \\ a_{21} & a_{22} \end{array} \right] \middle| a_{21} \in \mathbf{Z}_n, \quad a_{22} = \pm 1 \in \mathbf{Z}_n^\times \right\} .$$
>
> The set we have defined is a subgroup of the holomorph $\mathcal{H}_n$ of $\mathbf{Z}_n$.
>
> If $n > 2$, then $|G| = 2n$, and for the elements
>
> $$A = \left[\begin{array}{cc} 1 & 0 \\ 1 & 1 \end{array} \right] \qquad \text{and} \qquad B = \left[\begin{array}{cc} 1 & 0 \\ 0 & -1 \end{array} \right]$$
>
> it can be checked that A has order n, B has order 2, and $BA = A^{-1}B$. Thus G is isomorphic to D_n, and we have given an alternate construction of D_n, as an "external" semidirect product. $\square$

Let V be a vector space over the field F. Among other properties that must hold for scalar multiplication, we have $(ab)v = a(bv)$, $1v = v$, and $a(v+w) = av+aw$, for all $a, b \in F$ and all $v, w \in V$. Thus if we let G be the multiplicative group $F^\times$ of nonzero elements of a field F, then scalar multiplication defines an action of G on V. The formula $a(v + w) = av + aw$ provides an additional condition that is very useful.

Let V be an n-dimensional vector space over the field F, and let G be any subgroup of the general linear group $\mathrm{GL}_n(F)$ of all invertible $n \times n$ matrices over F. The standard multiplication of (column) vectors by matrices defines a group action of G on V, since for any matrices $A, B \in G$ and any vector $v \in V$, we have $(AB)v = A(Bv)$ and $I_n v = v$. The distributive law $A(v + w) = Av + Aw$, for all $A \in G$ and all $v, w \in V$, gives us an additional property.

The previous example suggests a new definition.

7.9.4 Definition. *Let G be a group and let X be an abelian group. If G acts on X and $a(x + y) = ax + ay$, for all $a \in G$ and $x, y \in X$, then we say that G* ***acts linearly*** *on X.*

The point of view of the next proposition will be useful in giving some more interesting examples. It extends the result of Proposition 7.3.2, which states that any group homomorphism $G \to \mathrm{Sym}(S)$ defines an action of G on the set S, and conversely, that every action of G on S arises in this way.

7.9.5 Proposition. *Let G be a group and let X be an abelian group. Then any group homomorphism from G into the group $\mathrm{Aut}(X)$ of all automorphisms of X defines a linear action of G on X. Conversely, every linear action of G on X arises in this way.*

Proof. If X is an additive group, and $\phi : G \to \mathrm{Aut}(X)$, then for any $a \in G$ the function $\lambda_a = \phi(a)$ must be a group homomorphism, so $\lambda_a(x+y) = \lambda_a(x)+\lambda_a(y)$, for all $x, y \in X$. Thus $a(x + y) = ax + ay$.

Conversely, assume that G acts linearly on S, and $a \in G$. Then it is clear that λ_a defined by $\lambda_a(x) = ax$ for $x \in S$ must be a group homomorphism. Thus ϕ defined by $\phi(a) = \lambda_a$ actually maps G to $\mathrm{Aut}(S)$. □

Let G be any group, and let X be an abelian group. For any homomorphism $\mu : G \to \mathrm{Aut}(X)$ we defined the semidirect product $X \rtimes_\mu G$. We now know that such homomorphisms correspond to linear actions of G on X. If we have any such linear action, we can define the multiplication in $X \rtimes_\mu G$ as follows: $(x_1, a_1)(x_2, a_2) = (x_1 + a_1x_2, a_1a_2)$, for all $x_1, x_2 \in X$ and $a_1, a_2 \in G$. Thus the concept of a linear action can be used to simplify the definition of the semidirect product.

We now give another characterization of semidirect products.

7.9.6 Proposition. *Let G be a multiplicative group with a normal subgroup N, and assume that N is abelian. Let $\pi : G \to G/N$ be the natural projection. The following conditions are equivalent:*

(1) *There is a subgroup K of G such that $N \cap K = \{e\}$ and $NK = G$;*

(2) *There is a homomorphism $\epsilon : G/N \to G$ such that $\pi\epsilon = 1_{G/N}$;*

(3) *There is a homomorphism $\mu : G/N \to \mathrm{Aut}(N)$ such that $N \rtimes_\mu (G/N) \cong G$.*

Proof. (1) implies (2): Let $\mu : K \to G/N$ be the restriction of π to K. Then $\ker(\mu) = \ker(\pi) \cap K = N \cap K = \{e\}$, and μ is onto since if $g \in G$, then $G = NK$ implies $g = ab$ for some $a \in N$, $b \in K$, and so $g \in Nb$, showing that $Ng = \mu(b)$. If we let $\epsilon = \mu^{-1}$, then $\pi\epsilon = \mu\mu^{-1}$ is the identity function on G/N.

(2) implies (3): To simplify the notation, let $G/N = H$. Define $\mu : H \to \mathrm{Aut}(X)$ as follows. For $a \in H$, define $\mu(a)$ by letting $\mu(a)[x] = \epsilon(a)x\epsilon(a)^{-1}$, for all $x \in N$. We note that $\mu(a)[x] \in N$ since N is a normal subgroup. We first show

that $\mu(a)$ is a group homomorphism, for all $a \in H$. We have

$$\begin{aligned} \mu(a)[xy] &= \epsilon(a)xy\epsilon(a)^{-1} \\ &= \epsilon(a)x\epsilon(a)^{-1}\epsilon(a)y\epsilon(a)^{-1} \\ &= \mu(a)[x]\mu(a)[y] \ , \end{aligned}$$

for all $x, y \in N$. We next show that μ is a group homomorphism. For all $a, b \in H$ and all $x \in N$, we have

$$\begin{aligned} \mu(ab)[x] &= \epsilon(ab)x\epsilon(ab)^{-1} \\ &= \epsilon(a)\epsilon(b)x\epsilon(b)^{-1}\epsilon(a)^{-1} \\ &= \mu(a)[\mu(b)[x]] \ = \ \mu(a)\mu(b)[x] \ . \end{aligned}$$

Since $\mu(e)[x] = \epsilon(e)x\epsilon(e)^{-1} = x$ for all $x \in N$, the previous computation shows that $\mu(a^{-1})$ is the inverse of $\mu(a)$, verifying that $\mu(a)$ is an automorphism for all $a \in H$.

Using μ, we construct $N \rtimes_\mu H$, and then define $\phi : N \rtimes_\mu H \to G$ by $\phi(x, a) = x\epsilon(a)$, for all $(x, a) \in N \rtimes_\mu H$. Then ϕ is one-to-one since $\phi((x, a)) = e$ implies $\epsilon(a) \in N$, and so $\pi\epsilon(a) = e$, whence $a = e$ and therefore $x = e$.

Given $g \in G$, let $a = \pi(g)$ and $x = g\epsilon\pi(g^{-1})$. Then $\pi(x) = \pi(g)\pi\epsilon\pi(g^{-1}) = \pi(g)\pi(g^{-1}) = e$, and so $x \in N$. Thus ϕ is onto, since $\phi((x, a)) = x\epsilon(a) = g\epsilon\pi(g^{-1})\epsilon\pi(g) = g$.

Finally, we must show that ϕ is a homomorphism. For $(x_1, a_1),\ (x_2, a_2) \in N \rtimes_\mu H$ we have

$$\begin{aligned} \phi((x_1, a_1)(x_2, a_2)) &= \phi((x_1\epsilon(a_1)x_2\epsilon(a_1)^{-1},\ a_1a_2)) \\ &= (x_1\epsilon(a_1)x_2\epsilon(a_1)^{-1})\epsilon(a_1a_2) \\ &= x_1\epsilon(a_1)x_2\epsilon(a_2) \\ &= \phi((x_1, a_1))\phi((x_2, a_2)) \ . \end{aligned}$$

(3) implies (1): If $G \cong N \rtimes_\mu (G/N)$, then the subgroups $\{(x, e)\} \cong N$ and $\{(e, a)\} \cong G/N$ have the required properties. $\square$

EXERCISES: SECTION 7.9

1. Let C_2 be the subgroup $\{\pm 1\}$ of $\mathbf{Z}_n^\times$, and let C_2 act on $\mathbf{Z}_n$ via the ordinary multiplication μ of congruence classes. Prove that $\mathbf{Z}_n \rtimes_\mu C_2$ is isomorphic to D_n.

2. Let G be the subgroup of $\mathrm{GL}_2(\mathbf{Q})$ generated by the matrices

$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \quad \text{and} \quad \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}.$$

   Show that G is a group of order 8 that is isomorphic to D_4.

3. Let G be the subgroup of $\mathrm{GL}_3(\mathbf{Z}_2)$ generated by the matrices

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}, \quad \begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \quad \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix}.$$

   (a) Show that G is a group of order 8 that is isomorphic to D_4.

   (b) Define an action μ of $\mathbf{Z}_2$ on $\mathbf{Z}_2 \times \mathbf{Z}_2$ by $0(x, y) = (x, y)$ and $1(x, y) = (y, x)$. Show that G is isomorphic to $(\mathbf{Z}_2 \times \mathbf{Z}_2) \rtimes_\mu \mathbf{Z}_2$.

4. Show that the quaternion group cannot be written as a semidirect product of two proper subgroups.

5. Prove that S_n is isomorphic to a semidirect product $A_n \rtimes \mathbf{Z}_2$.

6. Show that if $n > 2$, then $\mathbf{Z}_n \rtimes \mathbf{Z}_n^\times$ is solvable but not nilpotent.

7. Let p be a prime, and let G be the subgroup of $\mathrm{GL}_3(\mathbf{Z}_p)$ consisting of all matrices of the form

$$\begin{bmatrix} 1 & 0 & 0 \\ a & 1 & 0 \\ b & c & 1 \end{bmatrix}.$$

   Show that G is isomorphic to a semidirect product of $\mathbf{Z}_p \times \mathbf{Z}_p$ and $\mathbf{Z}_p$.

7.10 Classification of Groups of Small Order

In this section we study finite groups of a manageable size. Our first goal is to classify all groups of order less than 16 (at which point the classification becomes more difficult). Of course, any group of prime order is cyclic, and simple abelian.

A group of order 4 is either cyclic, or else each nontrivial element has order 2, which characterizes the Klein four-group. There is only one possible pattern for this multiplication table, but there is no guarantee that the associative law holds, and so it is necessary to give a model such as $\mathbf{Z}_2 \times \mathbf{Z}_2$ or $\mathbf{Z}_8^\times$.

7.10.1 Proposition. *Any nonabelian group of order* 6 *is isomorphic to* S_3.

Proof. This follows immediately from Proposition 7.4.5. □

7.10.2 Proposition. *Any nonabelian group of order* 8 *is isomorphic either to* D_4 *or to the quaternion group* Q_8.

Proof. If G had an element of order 8, then G would be cyclic, and hence abelian. If each element of G had order 1 or 2, then we would have $x^2 = e$ for all $x \in G$, so $(ab)^2 = a^2b^2$ for all $a, b \in G$, and G would be abelian. Thus G must contain at least one element of order 4.

Let a be an element of order 4, and let $N = \langle a \rangle$. Since N has index 2, there are precisely 2 cosets, given by N and bN, for any element $b \notin N$. Thus there exists an element b such that $G = N \cup bN$.

For the elements given in the previous part, either $b^2 = e$ or $b^2 = a^2$. To show this, since N is normal, consider G/N. We have $(bN)^2 = N$, and so $b^2 \in N$. Since $b^4 = e$ (there are no elements of order 8) we have $(b^2)^2 = e$. In N the only elements that satisfy $x^2 = e$ are e and a^2, so either $b^2 = e$ or $b^2 = a^2$.

We next show that bab^{-1} has order 4 and must be equal to a^3. We have $(bab^{-1})^4 = ba^4b^{-1} = bb^{-1} = e$. If $(bab^{-1})^2 = e$, then $ba^2b^{-1} = e$ and so $a^2 = e$, a contradiction to the choice of a. Hence $o(bab^{-1}) = 4$. If $bab^{-1} = a$, then $ab = ba$ and we have $G = N \cdot \langle b \rangle$ and so G would be abelian. Thus $bab^{-1} = a^3$.

We have shown that G contains elements a, b such that $a^4 = e$, $bab^{-1} = a^3$, and $b^2 = e$ or $b^2 = a^2$. If $a^4 = e$, $b^2 = e$, and $bab^{-1} = a^3$, then G is isomorphic to the dihedral group D_4. If $a^4 = e$, $b^2 = a^2$, and $bab^{-1} = a^3$, then G is isomorphic to the quaternion group Q_8. □

We can now determine (up to isomorphism) almost all groups of order less than 16. A group of order 9 must be abelian by Corollary 7.2.9, and then its structure is determined by Theorem 7.5.6. Proposition 7.4.5 determines the possible groups of order 10 and 14. determines the possible groups of order 10 and 14. Proposition 7.4.6 implies that a group of order 15 is cyclic. The remaining problem is to classify the groups of order 12.

7.10.3 Proposition. *Let* G *be a finite group.*

(a) *Let* N *be a normal subgroup of* G. *If there exists a subgroup* H *such that* $H \cap N = \{e\}$ *and* $|H| = [G : N]$, *then* $G \cong N \rtimes H$.

(b) *Let* G *be a group with* $|G| = p^n q^m$, *for primes* p, q. *If* G *has a unique Sylow* p*-subgroup* P, *and* Q *is any Sylow* q*-subgroup of* G, *then* $G \cong P \rtimes Q$. *Furthermore, if* Q' *is any other Sylow* q*-subgroup, then* $P \rtimes Q'$ *is isomorphic to* $P \rtimes Q$.

(c) *Let* G *be a group with* $|G| = p^2 q$, *for primes* p, q. *Then* G *is isomorphic to a semidirect product of its Sylow subgroups.*

Proof. (a) The natural inclusion followed by projection defines a homomorphism $H \to G \to G/N$ with kernel $H \cap N$. Since $H \cap N = \{e\}$ and $|H| = [G : N]$, this mapping is an isomorphism, and thus each left coset of G/N has the form hN for some $h \in H$. For any $g \in G$ we have $g \in hN$ for some $h \in H$, and so $G = HN$.

(b) The first statement follows from the part (a), since $|Q| = |G|/|P|$.

If Q' is any other Sylow q-subgroup, then $Q' = gQg^{-1}$ for some $g \in G$, since Q' is conjugate to Q. Recall that the action of Q on P is given by $a * x = axa^{-1}$, for all $a \in Q$ and all $x \in P$. Define $\Phi : P \rtimes Q \to P \rtimes Q'$ by $\Phi(x, a) = (gxg^{-1}, gag^{-1})$, for all $x \in P$, $a \in Q$. The mapping is well-defined since P is normal and $Q' = gQg^{-1}$. For $x_1, x_2 \in P$ and $a_1, a_2 \in Q$ we have

$$\begin{aligned}
\Phi((x_1, a_1))\Phi((x_2, a_2)) &= (gx_1g^{-1}, ga_1g^{-1})(gx_2g^{-1}, ga_2g^{-1}) \\
&= (gx_1g^{-1}ga_1g^{-1}gx_2g^{-1}(ga_1g^{-1})^{-1}, ga_1g^{-1}ga_2g^{-1}) \\
&= (gx_1g^{-1}ga_1g^{-1}gx_2g^{-1}ga_1^{-1}g^{-1}, ga_1g^{-1}ga_2g^{-1}) \\
&= (gx_1a_1x_2a_1^{-1}g^{-1}, ga_1a_2g^{-1}) \\
&= \Phi((x_1a_1x_2a_1^{-1}, a_1a_2)) \;=\; \Phi((x_1, a_1)(x_2, a_2)) \ .
\end{aligned}$$

Thus Φ is a homomorphism.

(c) If $p > q$, then $q \not\equiv 1 \pmod p$, so there must be only one Sylow p-subgroup, which is therefore normal. If $p < q$, then $p \not\equiv 1 \pmod q$, and so the number of Sylow q-subgroups must be 1 or p^2. In the first case, the Sylow q-subgroup is normal. If there are p^2 Sylow q-subgroups, then there must be $p^2(q-1)$ distinct elements of order q, so there can be at most one Sylow p-subgroup. □

7.10.4 Lemma. *Let G, X be groups, let $\alpha, \beta : G \to \mathrm{Aut}(X)$, and let μ, η be the corresponding linear actions of G on X. Then $X \rtimes_\mu G \cong X \rtimes_\eta G$ if there exists $\phi \in \mathrm{Aut}(G)$ such that $\beta = \alpha\phi$.*

Proof. Assume that $\phi \in \mathrm{Aut}(G)$ with $\beta = \alpha\phi$. For any $a \in G$ we have $\beta(a) = \alpha(\phi(a))$, and so for any $x \in X$ we must have $\eta(a, x) = \mu(\phi(a), x)$. Define $\Phi : X \rtimes_\eta G \to X \rtimes_\mu G$ by $\Phi(x, a) = (x, \phi(a))$ for all $x \in X$ and $a \in G$. Since ϕ is an automorphism, it is clear that Φ is one-to-one and onto. For $x_1, x_2 \in X$ and $a_1, a_2 \in G$, we have

$$\begin{aligned}
\Phi((x_1, a_1))\Phi((x_2, a_2)) &= (x_1, \phi(a_1))(x_2, \phi(a_2)) \\
&= (x_1\mu(\phi(a_1), x_2), \phi(a_1)\phi(a_2)) \\
&= (x_1\eta(a_1, x_2), \phi(a_1a_2)) \;=\; \Phi((x_1\eta(a_1, x_2), a_1a_2)) \\
&= \Phi((x_1, a_1)(x_2, a_2)) \ .
\end{aligned}$$

Thus $X \rtimes_\eta G \cong X \rtimes_\mu G$. □

7.10.5 Proposition. *Any nonabelian group of order* 12 *is isomorphic to* A_4, D_6, *or* $\mathbf{Z}_3 \rtimes \mathbf{Z}_4$.

Proof. Let G be a group of order 12. The Sylow 2-subgroup must be isomorphic to $\mathbf{Z}_4$ or $\mathbf{Z}_2 \times \mathbf{Z}_2$, while the Sylow 3-subgroup must be isomorphic to $\mathbf{Z}_3$. Thus we must find all possible semidirect products of the four combinations.

Case (i): $\mathbf{Z}_4 \rtimes \mathbf{Z}_3$
Since $\mathrm{Aut}(\mathbf{Z}_4) = \mathbf{Z}_4^\times \cong \mathbf{Z}_2$, there are no nontrivial homomorphisms from $\mathbf{Z}_3$ into $\mathrm{Aut}(\mathbf{Z}_4)$. Therefore this case reduces to $\mathbf{Z}_4 \times \mathbf{Z}_3 \cong \mathbf{Z}_{12}$.

Case (ii): $(\mathbf{Z}_2 \times \mathbf{Z}_2) \rtimes \mathbf{Z}_3$
Since $\mathrm{Aut}(\mathbf{Z}_2 \times \mathbf{Z}_2) \cong S_3$ and S_3 has a unique subgroup of order 3, there two possible nontrivial homomorphisms from $\mathbf{Z}_3$ into S_3, but they define isomorphic groups by Proposition 7.10.4. The group A_4 has a unique Sylow 2-subgroup isomorphic to $\mathbf{Z}_2 \times \mathbf{Z}_2$, and so we must have $(\mathbf{Z}_2 \times \mathbf{Z}_2) \rtimes \mathbf{Z}_3 \cong A_4$.

Case (iii): $\mathbf{Z}_3 \rtimes (\mathbf{Z}_2 \times \mathbf{Z}_2)$
Since $\mathrm{Aut}(\mathbf{Z}_3) = \mathbf{Z}_3^\times \cong \mathbf{Z}_2$, there are 3 nontrivial homomorphisms from $\mathbf{Z}_2 \times \mathbf{Z}_2$ into $\mathrm{Aut}(\mathbf{Z}_3)$, but they define isomorphic semidirect products, by Proposition 7.10.4. It can be shown that $\mathbf{Z}_3 \rtimes (\mathbf{Z}_2 \times \mathbf{Z}_2) \cong D_6$.

Case (iv): $\mathbf{Z}_3 \rtimes \mathbf{Z}_4$
There is only one nontrivial homomorphism from $\mathbf{Z}_4$ into $\mathrm{Aut}(\mathbf{Z}_3)$, in which $\mu(1)$ corresponds to multiplication by 2. It is left as an exercise to show that this group is isomorphic to the one called "T" by Hungerford. □

The following table summarizes the information that we have gathered.

Order	Groups	Order	Groups
2	$\mathbf{Z}_2$	9	$\mathbf{Z}_9$, $\mathbf{Z}_3 \times \mathbf{Z}_3$
3	$\mathbf{Z}_3$	10	$\mathbf{Z}_{10}$, D_5
4	$\mathbf{Z}_4$, $\mathbf{Z}_2 \times \mathbf{Z}_2$	11	$\mathbf{Z}_{11}$
5	$\mathbf{Z}_5$	12	$\mathbf{Z}_{12}$, $\mathbf{Z}_6 \times \mathbf{Z}_2$
6	$\mathbf{Z}_6$, S_3		A_4, D_6, $\mathbf{Z}_3 \rtimes \mathbf{Z}_4$
7	$\mathbf{Z}_7$	13	$\mathbf{Z}_{13}$
8	$\mathbf{Z}_8$, $\mathbf{Z}_4 \times \mathbf{Z}_2$, $\mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_2$	14	$\mathbf{Z}_{14}$, D_7
	D_4, Q_8	15	$\mathbf{Z}_{15}$

We now turn our attention to another question. The list of simple nonabelian groups that we know contains A_n, for $n > 4$, (by Theorem 7.7.4), and $\mathrm{PSL}_2(F)$, where F is a finite field with $|F| > 3$ (by Theorem 7.7.9). The smallest of these groups are A_5 and $PSL_2(\mathbf{Z}_5)$, each having 60 elements. Exercise 7.7.9 shows that in fact they are isomorphic.

It is not difficult to show that A_5 is the smallest nonabelian simple group. If G is a group of order n, then G is abelian if n is prime, and has a nontrivial center (which is normal) if n is a prime power. If $n = p^2q$, where p, q are distinct primes, then we have shown that G is a semidirect product of its Sylow subgroups, and so G is not simple. These results cover all numbers less than 60, with the exception of 30, 36, 40, 42, 48, 54, and 56.

Example 7.4.2 shows that a group of order 30 cannot be simple. It is easy to check the following: in a group of order 40, the Sylow 5-subgroup is normal; in a group of order 42, the Sylow 7-subgroup is normal; in a group of order 54, the Sylow 3-subgroup is normal. The case $n = 56$ is left as an easy exercise.

We will use the following proposition to show that no group of order 36 or 48 can be simple, which finishes the argument.

7.10.6 Proposition. *Let G be a finite simple group of order n, and let H be any proper, nontrivial subgroup of G.*

(a) *If $k = [G : H]$, then n is a divisor of $k!$.*

(b) *If H has m conjugates, then n is a divisor of $m!$.*

Proof. (a) Let S be the set of left cosets of H, and let G act on S by defining $a * xH = (ax)H$, for all $a, x \in G$. For any left coset xH and any $a, b \in G$, we have $a(bxH) = (ab)xH$. Since $e(xH) = (ex)H = xH$, this does define a group action. The corresponding homomorphism $\phi : G \to \mathrm{Sym}(S)$ is nontrivial, so ϕ must be one-to-one since G is simple. Therefore $\mathrm{Sym}(S)$ contains a subgroup isomorphic to G, and so n is a divisor of $k! = |\,\mathrm{Sym}(S)|$.

(b) Let S be the set of subgroups conjugate to H, and define an action of G on S as in Example 7.3.7, by letting $a * K = aKa^{-1}$, for all $a \in G$ and all $K \in S$. In this case, $|\,\mathrm{Sym}(S)| = m!$, and the proof follows as in part (a). □

7.10.7 Proposition. *The alternating group A_5 is the smallest nonabelian simple group.*

Proof. Assuming the result in Exercise 1 the proof can now be completed by disposing of the cases $n = 36$ and $n = 48$. For a group of order 36, there must be either 1 or 4 Sylow 3-subgroups. Since 36 is not a divisor of 4!, the group cannot be simple. For a group of order 48, there must be either 1 or 3 Sylow 2-subgroups. Since 48 is not a divisor of 3!, the group cannot be simple. □

EXERCISES: SECTION 7.10

1. Complete the proof that A_5 is the smallest nonabelian simple group by showing that there is no simple group of order 56.
2. Prove that the automorphism group of $\mathbf{Z}_2 \times \mathbf{Z}_2$ is isomorphic to S_3.
3. Show that the nonabelian group $\mathbf{Z}_3 \rtimes (\mathbf{Z}_2 \times \mathbf{Z}_2)$ is isomorphic to the dihedral group D_6.
4. Show that the nonabelian group $\mathbf{Z}_3 \rtimes \mathbf{Z}_4$ is generated by elements a of order 6, and b of order 4, subject to the relations $b^2 = a^3$ and $ba = a^{-1}b$.

BIBLIOGRAPHY

Dummit, D., and R. Foote, *Abstract Algebra* (3^{rd} ed.). John Wiley & Sons, 2003.
Herstein, I. N., *Topics in Algebra* (2^{nd} ed.). John Wiley & Sons, 1973.
Hungerford, T., *Algebra*. Springer-Verlag New York, 1974.
Isaacs, I. M., *Algebra, a graduate course*. Brooks/Cole, 1993
Jacobson, N., *Basic Algebra I* (2^{nd} ed.). W. H. Freeman, 1985.
——————-, *Basic Algebra II* (2^{nd} ed.). W. H. Freeman, 1989.
Lang, S., *Algebra* (3^{rd} ed.). Springer-Verlag New York, 2002.
Rotman, J. J., *Advanced Algebra*. (2^{nd} ed.). Springer-Verlag New York, 2002.
——————-, *An Introduction to the Theory of Groups*. (4^{th} ed.). Springer-Verlag New York, 1995.
Van der Waerden, B. L., *Algebra* vol. 1. Springer-Verlag New York, 2003.

Index