Algebra I: Chapter 6. Product Structure in Groups.

6.1 Direct products of groups.

We begin with a basic product construction for groups, similar to that for "direct sums" of vector spaces.

6.1.1 Definition (External Direct Product). *Given groups $A_1, \ldots, A_n$ their* **external direct product** *is the Cartesian product set $G = A_1 \times \ldots \times A_n$ equipped with component-by-component multiplication of n-tuples. If $\mathbf{a} = (a_1, \ldots, a_n)$, $\mathbf{b} = (b_1, \ldots, b_n)$ in the Cartesian product set G, their product is*

$$(1) \qquad \mathbf{a} \cdot \mathbf{b} = (a_1, \ldots, a_n) \cdot (b_1, \ldots, b_n) = (a_1 b_1, \ldots, a_n b_n) \qquad \text{for all } a_i, b_i \in A_i$$

The identity element is $\mathbf{e} = (e_1, \ldots, e_n)$ where e_i is the identity element in A_i; the inverse of an element $\mathbf{a}$ is $\mathbf{a}^{-1} = (a_1^{-1}, \ldots, a_n^{-1})$.

There is a natural isomorphism between A_i and the subgroup

$$\overline{A}_i = (e_1) \times \ldots \times A_i \times \ldots (e_n) \quad ,$$

the n-tuples whose entries are trivial except for a_i. From (1) it follows easily that

(a) Each $\overline{A}_i$ is a subgroup in G.

(b) The bijective map $J_i(a_i) = (e_1, \ldots, a_i, \ldots, e_n)$ defines an isomorphism from A_i to $\overline{A}_i$.

(c) The $\overline{A}_i$ commute with each other in the sense that $xy = yx$ if $x \in \overline{A}_i$, $y \in \overline{A}_j$ and $i \neq j$.

Note carefully what (c) *does not* say: the subgroup $\overline{A}_i$ need not commute *with itself* (the case when $i = j$) unless the group A_i happens to be abelian.

(d) Each $\overline{A}_i$ is a normal subgroup in G.

(e) The product set

$$\overline{A}_1 \cdot \ldots \cdot \overline{A}_n = \{x_1 \ldots x_n : x_i \in \overline{A}_i, 1 \leq i \leq n\}$$

is all of G.

(f) Every $x \in G$ has a *unique* factorization

$$x = \overline{x}_1 \cdot \ldots \cdot \overline{x}_n \qquad \text{with } \overline{x}_i \in \overline{A}_i$$

6.1.2 Exercise. Verify the claims (a) – (f) regarding the subgroups $\overline{A}_i$ in a direct product $G = A_1 \times \ldots \times A_n$. □

The order of entries in an n-tuple makes a difference; therefore the Cartesian product sets $A_1 \times A_2$ and $A_2 \times A_1$ are not the same thing (unless $A_1 = A_2$). For instance, are the direct product groups $\mathbb{Z}_3 \times \mathbb{Z}_5$ and $\mathbb{Z}_5 \times \mathbb{Z}_3$ *the same*? What do elements in these groups look like? However, in dealing with groups we only care whether they are isomorphic. It happens that $\mathbb{Z}_3 \times \mathbb{Z}_5 \cong \mathbb{Z}_5 \times \mathbb{Z}_3$ even though these groups are not "identical."

6.1.3 Exercise. Let $A_1, A_2, \ldots$ be groups. Prove that the following product groups are isomorphic.

(a) $A_1 \times A_2 \cong A_2 \times A_1$

(b) $A_1 \times (A_2 \times A_3) \cong (A_1 \times A_2) \times A_3 \cong A_1 \times A_2 \times A_3$ (as defined in (1))

(c) If one of the groups in the product $A_1 \times A_2$ is trivial we get

$$A_1 \times (e_2) \cong A_1 \qquad (e_1) \times A_2 \cong A_2 \quad \square$$

In essence, the operation of forming the direct product of two groups is commutative and associative, and the trivial group $E = (e)$ acts as an "identity element." The significance of (b) is that, up to isomorphism, we get the same group if we multiply groups together all at once, as in (1), or multiply them successively two at a time.

6.1.4 Exercise. In the product group $G = A \times A$ the *diagonal* is $\Delta = \{(a, a) : a \in A\}$

(a) Show that Δ is a subgroup of G

(b) Show that $\Delta \cong A$.

(c) Find a complete set of coset representatives for the coset space G/Δ.

In general Δ is not a *normal* subgroup of $G \times G$. Can you see why? In (c) you are looking for a set $X \subseteq G$ that meets each coset $g\Delta$ in a unique point. Such a set is a *transversal* for the space of cosets G/Δ. $\square$

6.1.5 Example. Euclidean space $\mathbb{R}^n$ equipped with vector addition $(+)$ as a binary operation is an abelian group. Its elements are *defined* as n-tuples $\mathbf{x} = (x_1, \ldots, x_n)$ of real numbers, elements of the Cartesian product set $\mathbb{R} \times \ldots \times \mathbb{R}$. Comparison of the sum

$$\mathbf{x} + \mathbf{y} = (x_1 + y_1, \ldots, x_n + y_n)$$

with (1) shows that $G = (\mathbb{R}^n, +)$ is precisely the direct product *group* $(\mathbb{R} \times \ldots \times \mathbb{R}, +)$ made up of n copies of the real line $(\mathbb{R}, +)$. $\square$

6.1.6 Example. The set of *integral vectors* in $\mathbb{R}^n$

$$\mathbb{Z}^n = \{\mathbf{x} \in \mathbb{R}^n : \mathbf{x} = (x_1, \ldots, x_n) \text{ with } x_i \in \mathbb{Z} \text{ for all } i\}$$

is a group under vector addition $(+)$. Explain why $(\mathbb{Z}^n, +) \cong \mathbb{Z} \times \ldots \times \mathbb{Z}$. If $\{u_i\}$ is an $\mathbb{R}$-basis for $\mathbb{R}^n$ and

$$\Lambda = \{a_1u_1 + \ldots + a_nu_n : a_i \in \mathbb{Z}\} = \mathbb{Z}u_1 + \ldots + \mathbb{Z}u_n$$

prove that $(\Lambda, +)$ is an abelian group isomorphic to $(\mathbb{Z}^n, +)$. What map $\psi : \mathbb{Z}^n \to \Lambda$ effects the isomorphism? $\square$

There is an important "internal" version of the direct product construction. Given a group G and subgroups $A_i \subseteq G$ we would like to know when G is isomorphic to the direct product $A_1 \times \ldots \times A_n$. From the conditions (a)-(f) we can read out some obvious necessary conditions,

(3)
- (i) Each A_i must be a normal subgroup in G.
- (ii) The A_i must generate G in the sense that G is equal to the product set $A_1 \cdots A_n = \{x_1 \cdots x_n : x_i \in A_i\}$
- (iii) Each $g \in G$ has a *unique* factorization $g = x_1 \cdots x_n$ such that $x_i \in A_i$.

Note that (ii) insures the *existence* of such a factorization while (iii) insures its uniqueness.

Conditions (i) – (iii) are also sufficient to insure $G \cong A_1 \times \ldots \times A_n$, but before we prove that we must work out a few simple consequences of these hypotheses.

6.1.7 Exercise. Let G be a group and A, B two subgroups. Then the product set

$$AB = \{ab : a \in A, b \in B\}$$

is a subgroup if either A or B is normal, and the product is a *normal* subgroup if both A and B are normal.
Note: Recall the discussion of Section 3.3, especially Exercise 3.3.14. $\square$

We are now ready to state the main result. It is framed in terms of the unique factorization condition (iii).

6.1.8 Theorem (Internal Direct Product). *Let G be a group and $A_1, \ldots, A_n$ subgroups such that*

(i) *Each A_i is a normal subgroup in G*

(ii) *The product set $A_1 \cdots A_n$ is equal to G.*

(iii) *Each $g \in G$ decomposes uniquely as $g = a_1 \cdots a_n$ with $a_i \in A_i$.*

Then G is isomorphic to the direct product group $A_1 \times \ldots \times A_n$. In particular, elements of A_i and A_j automatically commute if $i \neq j$.

PROOF: If $i \neq j$ we have pairwise disjointness $A_i \cap A_j = (e)$ because if $x \neq e$ is in $A_i \cap A_j$ it would have two different factorizations

$$x = e \ldots x \ldots e \ldots e = e \ldots e \ldots x \ldots e$$

one in A_i the other in A_j, contrary to (iii).

Using this we can show that A_i and A_j commute when $i \neq j$. To see why, suppose $x_i \in A_i, y_j \in A_j$ and consider the "commutator" $z = x_i y_j x_i^{-1} y_j^{-1}$. Since A_j is normal in G the element $z = (x_i y_j x_i^{-1}) y_j^{-1}$ must lie in A_j; the same argument applied to $x_i (y_j x_i^{-1} y_j^{-1})$ shows that z also lies in A_i. Since $A_i \cap A_j = (e)$ we get $x_i y_j x_i^{-1} y_j^{-1} = e$ which implies $x_i y_j = y_j x_i$, as required.

The unique decomposition property (iii) means precisely that the map $p(a_1, \ldots, a_n) = a_1 \cdot \ldots \cdot a_n$ from the Cartesian product set $A_1 \times \ldots \times A_n$ to G is a bijection. It is also a homomorphism when $A_1 \times \ldots \times A_n$ is equipped with the multiplication law (1), because if $\mathbf{a} = (a_1, \ldots, a_n)$, $\mathbf{b} = (b_1, \ldots, b_n)$ we can make the following rearrangements of commuting group elements.

$$\begin{aligned} p(\mathbf{a})p(\mathbf{b}) &= a_1 \cdots a_n \cdot b_1 \cdots b_n \\ &= a_1 b_1 \cdot a_2 \cdots a_n \cdot b_2 \cdots b_n \\ &= a_1 b_1 \cdot a_2 b_2 \cdot a_3 \cdots a_n \cdot b_3 \cdots b_n \\ &\quad \vdots \\ &= a_1 b_1 \cdot a_2 b_2 \cdot \ldots \cdot a_n b_n \\ &= p(\mathbf{ab}) \qquad (\text{since } \mathbf{ab} = (a_1 b_1, \ldots, a_n b_n)) \end{aligned}$$

[Here b_1 commutes with $a_2, \ldots, a_n$; b_2 commutes with $a_3, \ldots, a_n$; etc.] Thus p is an isomorphism of groups. $\square$

In view of this result, a group satisfying the conditions of Theorem 6.1.8 is often called an **internal direct product** of the subgroups $A_1, \ldots, A_n$.

This decomposition theorem, and the notion of direct product, are most often applied when there are just two factors. Then the decomposability criteria are simpler, and direct product structure $G \cong A \times B$ much easier to recognize.

6.1.9 Corollary. *Let G be a group and A, B two subgroups such that*

(i) *A and B are normal subgroups in G.*

(ii) *The product set AB is equal to G.*

(iii) $A \cap B = (e)$.

Then G is isomorphic to the direct product $A \times B$ under the map $p(a,b) = a \cdot b$.

PROOF: Every $g \in G$ has a factorization $g = ab$ by (ii). Uniqueness follows from (iii) because

$$ab = a'b' \Rightarrow (a')^{-1}a = b(b')^{-1}$$

The expression on the left is in A while the one on the right is in B, so by (iii) both expressions are equal to e. That means $a' = a$ and $b' = b$, proving uniqueness. Unique factorization determines a bijection $f : G \to A \times B$ if we take $f(g) = f(ab) = (a,b)$, with inverse map $f^{-1}(a,b) = a \cdot b$.

To see that f is a group isomorphism when the Cartesian product set is given the direct product structure (1) we first note that elements of A commute with elements in B. This holds if all "commutators" $[a,b] = aba^{-1}b^{-1}$ are trivial. As in 6.1.8 the commutator can be written two ways. We see that $[a,b]$ is in B because

$$[a,b] = (aba^{-1}) \cdot b = b'b$$

and B is normal. But we also have $[a,b] = a(ba^{-1}b^{-1}) = aa'$ so we conclude that $[a,b]$ is also in A because A is normal. By (iii) the commutator must be trivial.

From commutativity $ab = ba$ in G and the definition of products in $A \times B$ we get

$$f(ab \cdot a'b') = f(aa' \cdot bb') = (aa', bb') = (a,b) \cdot (a',b') = f(ab) \cdot f(a'b')$$

so $f : G \to A \times B$ is an isomorphism. □

The following examples illustrate the use of these results to demonstrate the presence of direct product structure in a group.

6.1.10 Example (Groups of Order 4). Up to isomorphism, describe *all* groups of order $|G| = 4$.

DISCUSSION: We first consider *the largest possible order* $o(b)$ for an element of G, the only possibilities being $o(b) = 1, 2, 4$ by Lagrange. The maximal order obviously cannot be 1.

CASE 1: $o(b) = 4$. Then G is cyclic of order 4 and is abelian, isomorphic to $(\mathbb{Z}_4, +)$.

CASE 2: $o(b) = 2$. Now all elements $x \neq e$ have order $o(x) = 2$, so that $x^2 = e$ and $x^{-1} = x$ for each $x \in G$. Pick any $a \neq e$ and let $A = \langle a \rangle$; obviously $A \cong \mathbb{Z}_2$. Next pick any element $b \notin A$ and let $B = \langle b \rangle$; obviously $B \cong \mathbb{Z}_2$ too, but $B \neq A$. The subgroup $A \cap B$ lies within both A and B, and must be trivial; otherwise $|A \cap B| = 2$ and $A = B = A \cap B$, which has been excluded by our choice of b.

The product set $AB = \{e, a, b, ab\}$ is equal to G because it is easily seen that the element ab cannot equal e, a, or b. This also follows by invoking Theorem 3.4.7 which says that $|AB| = |A| \cdot |B| \,/\, |A \cap B| = (2 \cdot 2)/1 = 4 = |G|$, and hence that $AB = G$.

Finally, G must be abelian. In fact if $a, b \in G$ the element ab has $e = (ab)^2 = abab$; multiplying on the right by b^{-1} and on the left by a^{-1} we get $a^{-1}b^{-1} = ba$. But $a^{-1} = a$ and $b^{-1} = b$, so $ab = ba$ as required. It follows that A and B are normal subgroups in G, and hence by 6.1.9 that G is the internal direct product of these subgroups: $G \cong \mathbb{Z}_2 \times \mathbb{Z}_2$ in Case 2. □

Thus, up to isomorphism, the only possibilities for a group of order four are the groups $G \cong \mathbb{Z}_4$ and $G' \cong \mathbb{Z}_2 \times \mathbb{Z}_2$ of Example 6.1.10. When $|G| = 5$ we have $G \cong \mathbb{Z}_5$ because 5 is a prime; by Lagrange every element $x \neq e$ has $o(x) = 5$. We have now identified all groups of order $|G| \leq 5$.

6.1.11 Example (Groups of Order 6, Part I). Let G be an arbitrary group of order $|G| = 6$. The order of any element must divide $|G| = 6$, so the possible orders are $o(g) = 1, 2, 3, 6$. G is cyclic and isomorphic to $(\mathbb{Z}_6, +)$ if there is an element of order $o(a) = 6$. Otherwise, by Cauchy's Theorem 4.3.6 there must be elements with orders $o(a) = 3$ and $o(b) = 2$ which generate cyclic subgroups $H_3 = \langle a \rangle \cong \mathbb{Z}_3$ and $H_2 = \langle b \rangle \cong \mathbb{Z}_2$. The intersection $H = H_3 \cap H_2$ is a subgroup of both H_3 and H_2; by Lagrange $|H|$ must divide both 2 and 3, so $H_2 \cap H_3 = (e)$.

It follows from Theorem 3.4.7 that the product set H_3H_2 is all of G because

$$|H_3 \cdot H_2| = \frac{|H_3| \cdot |H_2|}{|H_3 \cap H_2|} = \frac{3 \cdot 2}{1} = |G|$$

Thus every $g \in G$ has at least one factorization $g = h_3h_2$ with $h_i \in H_i$. The factorization is also *unique* because if $g = h_3h_2 = h_3'h_2'$ we get $(h_3')^{-1}h_3 = h_2'h_2^{-1}$. On the left we have an element of H_3 while on the right an element of H_2, and since $H_3 \cap H_2 = (e)$ both elements equal e and $h_3' = h_3, h_2' = h_2$, as claimed. Thus $\phi(x, y) = x \cdot y$ is a bijection from the group G to the Cartesian product set $H_3 \times H_2$. *This is not yet an isomorphism* between G and $H_3 \times H_2$ equipped with the direct product group law; in fact there are two nonisomorphic groups of this type.

We next observe that the larger subgroup H_3 *must be normal in* G. Indeed if there were some conjugate $xH_3x^{-1} \neq H_3$ these two groups would have trivial intersection (by Lagrange again), and hence we would have

$$|H_3 \cdot xH_3x^{-1}| = \frac{|xH_3x^{-1}|\,|H_3|}{|H_3 \cap xH_3x^{-1}|} = \frac{3 \cdot 3}{1} = 9$$

which is impossible in a group having only 6 elements. Thus $H_3 \lhd G$. A similar argument cannot be made for the smaller group H_2 (why?), so there are two possibilities:

Case 1: $H_2 \lhd G$. The hypotheses of Corollary 6.1.13 are satisfied so G is isomorphic to the direct product $H_3 \times H_2 \cong \mathbb{Z}_3 \times \mathbb{Z}_2$, an abelian group.

Case 2: H_2 is not normal. We defer a complete analysis of this case, but we already know a noncommutative group of order 6, the permutation group S_3 on three objects. Every $\sigma \neq e$ in S_3 is either a 2-cycle or a 3-cycle, and these generate cyclic subgroups $H_2 \cong \mathbb{Z}_2$, $H_3 \cong \mathbb{Z}_3$. As in the preceding discussion $H_2 \cap H_3 = (e)$, $H_3 \lhd S_3$, and every element of S_3 has a unique factorization $\sigma = h_3 \cdot h_2$. Taking $\tau = (123)$ as the generator of H_3 and $H_2 = \langle (1, 2) \rangle$, the subgroup H_2 is *not* normal in S_3 because

$$\tau \cdot (12) \cdot \tau^{-1} = \text{ the 2-cycle } \big(\tau(1), \tau(2)\big) = (2, 3) \notin H_2$$

In the next section of the *Notes* we will show that $G \cong S_3$ is the only possibility in Case 2. Up to isomorphism $\mathbb{Z}_6, \mathbb{Z}_3 \times \mathbb{Z}_2$, and S_3 are the only groups of order 6. $\square$

This example also shows that normality of the factors A_i is an essential hypothesis in our definition (3) of an internal direct product. The product $S_3 = H_3H_2$ has the unique factorization property specified in (ii) and (iii), but one of the factors fails to be normal and S_3 is not a direct product of these abelian subgroups (if it were, S_3 would be abelian).

6.1.12 Example. The cyclic group $G = \mathbb{Z}_4$, with generator $a = [1]$, is an abelian group of order 4. So is the direct product $G' = \mathbb{Z}_2 \times \mathbb{Z}_2$, whose elements can be written as

$$e = (0, 0) \qquad a = (1, 0) \qquad b = (0, 1) \qquad c = (1, 1)$$

where by abuse of notation we write k for the class $[k]$. Can these groups be isomorphic – i.e. is the cyclic group a direct product of smaller subgroups? *Answer:* No. In G' every element $g \neq e$ has order order $o(g) = 2$; in fact, writing $(+)$ for the operation in $\mathbb{Z}_2 \times \mathbb{Z}_2$

we have $(a,b)+(a,b)=(2\cdot a, 2\cdot b)=(0,0)$. In contrast, $G=\mathbb{Z}_4$ has a cyclic generator a with additive order $o(a)=4$. That's impossible if $G\cong G'$. $\square$

There is more to be said about the groups $\mathbb{Z}_6$ and $\mathbb{Z}_3\times\mathbb{Z}_2$. The element $a=[3]_6$ in $\mathbb{Z}_6$ has additive order 2, since $[3]_6+[3]_6=[6]_6=[0]_6$, and the group A it generates is $\cong\mathbb{Z}_2$. Similarly the element $b=[2]_6$ has additive order $o(b)=3$ and generates a cyclic subgroup $B\cong\mathbb{Z}_3$ in $\mathbb{Z}_6$.

Since G is abelian both A and B are normal subgroups. Furthermore $A\cap B=(e)$ by Lagrange and the (additive) product set $A+B$ must be all of $\mathbb{Z}_6$ because $|A+B|=|A|\cdot|B|/|A\cap B|=6$. By 6.1.13 we conclude that $\mathbb{Z}_6\cong\mathbb{Z}_2\times\mathbb{Z}_3$. Thus the cyclic group $\mathbb{Z}_6$ and the direct product $\mathbb{Z}_3\times\mathbb{Z}_2$ are the same group up to isomorphism, even though they seem quite different at first sight. There are only two distinct groups of order $|G|=6$, $\mathbb{Z}_6$ and the permutation group S_3.

On the other hand we saw in Example 6.1.12 that $\mathbb{Z}_4$ cannot be isomorphic $\mathbb{Z}_2\times\mathbb{Z}_2$. What might account for the different outcomes these examples? A complete answer will emerge as we discuss the *Chinese Remainder Theorem* (below), but for the moment it suffices to point out that the subgroups A,B in the 6.1.11 are associated with *different* prime divisors of $|G|=6$. There are no distinct prime divisors when $|G|=4=2^2$.

***6.1.13 Exercise.** Show that the following map $\Phi:\mathbb{Z}_6\to\mathbb{Z}_3\times\mathbb{Z}_2$

$$\Phi\big([i]_6\big)=\big([i]_3,[i]_2\big)\qquad([i]_6\in\mathbb{Z}_6)$$

has the properties

(a) Φ is well defined (independent of choice of class representative i).

(b) Φ is a bijection.

(c) Φ is a homomorphism between $(\mathbb{Z}_6,+)$ and the direct product group $\mathbb{Z}_3\times\mathbb{Z}_2$.

so that Φ is an isomorphism. $\square$

6.1.14 Exercise. In 6.1.13 we showed $\mathbb{Z}_3\times\mathbb{Z}_2\cong\mathbb{Z}_6$. Is $\mathbb{Z}_m\times\mathbb{Z}_n$ *always* isomorphic to $\mathbb{Z}_{mn}$? Prove or give a counterexample. $\square$

6.1.15 Exercise. Do you think it possible to decompose the cyclic group $(Z_{15},+)$ as a direct product of smaller cyclic subgroups? How about the cyclic group $(\mathbb{Z}_9,+)$? Explain.
Hint: If G factors, what orders could the factors have? $\square$

***6.1.16 Exercise (Groups of order $\mathbf{p^2}$).** Assume G is a finite group of order $|G|=p^2$ for some prime $p>1$. Prove that $G\cong\mathbb{Z}_{p^2}$ or $G\cong\mathbb{Z}_p\times\mathbb{Z}_p$ and that the groups cannot be isomorphic.
Hint: Use the Cauchy Theorems of Chapter 4 and adapt the ideas of 6.1.11. $\square$

6.1.17 Exercise. Prove that $|A_1\times\ldots\times A_r|=|A_1|\cdot\ldots\cdot|A_r|$ for any direct product of groups. $\square$

***6.1.18 Exercise.** Prove that the order $o(x)$ of an element $x=(a,b)$ in the direct product group $A\times B$ is the least common multiple $\operatorname{lcm}(o(a),o(b))$. Is a similar result true for direct products of *several* groups?
Hint: Observe that in a direct product $A\rtimes B$ we have $x^m=e\Leftrightarrow a^m=e$ and $b^m=e$. In any group, $g^m=e\Leftrightarrow m$ is a multiple of $o(g)$. $\square$

6.1.19 Exercise. Is $\mathbb{Z}_{15}\times\mathbb{Z}_4$ a cyclic group – i.e. does it have an element of order 60? Does $\mathbb{Z}_{15}\times\mathbb{Z}_5$ have elements of order (i) 75? (ii) 25? (iii) 15? (iv) 3? (v) Any other order? $\square$

6.1.20 Exercise. Identify all elements $x=(a,b)$ of order $o(x)=5$ in $\mathbb{Z}_{15}\times\mathbb{Z}_5$. Same

for $\mathbb{Z}_{15} \times \mathbb{Z}_4$. $\square$

Ultimately we will have a lot to say about the structure of a finite group G in terms of the prime divisors of its order $n = |G|$. We have already noted that there is just one group of order $|G| = p$ when p is a prime.

6.1.21 Theorem. *If G is a nontrivial finite group of prime order $|G| = p > 1$ then G is isomorphic to the cyclic group $(\mathbb{Z}_p, +)$ and every $b \neq e$ is a cyclic generator.*

PROOF: Let $b \neq e$ and consider the cyclic subgroup $H = \{e, b, b^2, \ldots, b^{k-1}\}$, with $b^k = e$. By Lagrange, $|H| = k \geq 2$ must divide the order $|G| = p$ of the whole group. Hence $k = p$ and $H = G$. $\square$

Direct Products and the Chinese Remainder Theorem. The Chinese Remainder Theorem (CRT) has its roots in number theory but has many uses. One application completely resolves the issues regarding direct products $\mathbb{Z}_m \times \mathbb{Z}_n$ mentioned following 6.1.12. The original remainder theorem, part of Chinese folklore, arose in antiquity when attempts were made to solve systems of *congruences* involving several different moduli n_i

$$\begin{array}{ll} x \equiv a_1 & (\text{mod } n_1) \\ \vdots & \qquad\qquad\qquad\qquad x \in \mathbb{Z} \\ x \equiv a_r & (\text{mod } n_r) \end{array}$$

The notion of congruence is a modern one; the ancient Chinese would have viewed this problem as the search for an integer x with specified remainders a_i after division by n_i, $i = 1, 2, \ldots r$.

Such systems do not always have solutions. But solutions do exist if the moduli $n_1, \ldots, n_r$ are *pairwise relatively prime*, so that $\gcd(n_i, n_j) = 1$ if $i \neq j$, and then the solution x is unique up to added multiples of the least common multiple $m = \text{lcm}(n_1, \ldots, n_r)$ of the moduli.

6.1.22 Example. Here are two systems of congruences

$$\text{(a)} \quad \begin{cases} x \equiv 5 & (\text{mod } 3) \\ x \equiv 1 & (\text{mod } 12) \end{cases} \qquad\qquad \text{(b)} \quad \begin{cases} x \equiv 5 & (\text{mod } 3) \\ x \equiv 1 & (\text{mod } 5) \end{cases}$$

Taking a "bare hands" approach we shall verify that the system (a) has no solutions and that the solutions of (b) are of the form $x_0 + k \cdot 15$ where $x_0 = 11$ and $k \in \mathbb{Z}$.

DISCUSSION: If $x \in \mathbb{Z}$ solves (a) there must exist $k, \ell \in \mathbb{Z}$ such that

$$x = 5 + 3k = 1 + 12\,\ell$$

But then k and ℓ satisfy the equation $4 = 12\ell - 3k$, which would imply

$$4 = 12\ell - 3k \text{ is in } 12 \cdot \mathbb{Z} + 3 \cdot \mathbb{Z} = \gcd(12, 3) \cdot \mathbb{Z} = 3\mathbb{Z}$$

That's impossible because 4 is not a multiple of 3.

If x is a solution of (b) there must be integers $k, \ell \in \mathbb{Z}$ such that $x = 5 + 3k$ and $x = 1 + 5\ell$. Taking the difference of these identities we get

$$4 = -3k + 5\ell$$

Conversely, given two integers k, ℓ satisfying this identity it is clear that $5 + 3k = 1 + 5\ell$, so

$$x = 5 + 3k \qquad \text{and} \qquad x = 1 + 5\ell$$

describe the same number, and that x is a solution of the system (b). Therefore to solve (b) we need only find $k, \ell \in \mathbb{Z}$ such that $4 = -3k + 5\ell$.

On the other hand since $\gcd(3,5) = 1$ there exist integers r, s such that $3r + 5s = 1$; multiplying through by 4 we get

$$4 = 4(3r) + 4(5s) = 3(4r) + 5(4s)$$

This tells us how to find k and ℓ such that $4 = -3k + 5\ell$: just take $k = -4r$ and $\ell = 4s$. Then $x = 5 + 3k$ (same as $x = 1 + 5\ell$) is a solution of the congruence (b).

As for uniqueness, if x' is any other solution then $y = x' - x \equiv 0 \pmod 3$ and also $\pmod 5$, so y is a multiple of 3 and 5, and of $\mathrm{lcm}(3,5) = 15$. On the other hand it is obvious that any $x' \in x + 15\mathbb{Z}$ is a solution, so solutions are unique (mod 15).

This solution of the congruence problem rests on our ability to compute $c = \gcd(a,b)$ efficiently via the GCD Algorithm, and to write c in the form $c = ra + sb$ by working that algorithm backwards. In this simple example we can work by hand to find that

$$1 = 3r + 5s = 3(-3) + 5(2) \quad \text{so that} \quad 4 = 3(-12) + 5(8) = -3(12) + 5(8) \ ,$$

which takes the form $-3k + 5\ell$ if we set $k = 12, \ell = 8$. Thus $x = 5 + 3k = 41$ is a solution to (b), as is $x = 1 + 5\ell = 41$. This solution is unique up to an added multiple of $\mathrm{lcm}(3,5) = 15$. Subtracting a multiple of the $lcm = 15$ we get a "normalized" solution $0 \leq 11 < 15$. □

***6.1.23 Exercise.** Adapt the preceding analysis to solve the following congruences by hand or determine that they have no solutions.

(a) $\begin{cases} x \equiv 2 \pmod{15} \\ x \equiv 5 \pmod 7 \end{cases}$ (b) $\begin{cases} x \equiv 3 \pmod 9 \\ x \equiv 5 \pmod{12} \end{cases}$ (c) $\begin{cases} x \equiv 2 \pmod{15} \\ x \equiv 5 \pmod{19} \end{cases}$ □

6.1.24 Exercise. Recall that the greatest common divisor $\gcd(a_1, \ldots, a_r)$ of $a_1, \ldots, a_r$ is the smallest positive element in the lattice $\Lambda = \mathbb{Z}a_1 + \ldots + \mathbb{Z}a_r$ of integer-linear combinations. (The proof is the same as when $r = 2$.) We say that the a_i are *jointly relatively prime* if this gcd = 1. Prove that

(a) (Pairwise relatively prime) ⇒ (Jointly relatively prime)

(b) Find three integers a_1, a_2, a_3 for which the converse *does not* hold. □

6.1.25 Exercise. Explain what "pairwise relatively prime" and "jointly relatively prime" mean in terms of the prime factorizations of $a_1, \ldots, a_r$. □

To keep things simple let's consider a system involving just two congruences

$$x \equiv a_1 \pmod m \qquad x \equiv a_2 \pmod n \tag{5}$$

This remainder problem is completely equivalent to a problem in group theory: the system is solvable for every choice of a_1, a_2 on the right if and only if the direct product group $\mathbb{Z}_m \times \mathbb{Z}_n$ is cyclic – i.e. if and only $\mathbb{Z}_m \times \mathbb{Z}_n \cong \mathbb{Z}_{mn}$ – and this happens ⇔ $\gcd(m,n) = 1$.

6.1.26 Theorem (Chinese Remainder Theorem). *If $m, n > 1$ are relatively prime, so that $\gcd(m,n) = 1$, then $\mathbb{Z}_m \times \mathbb{Z}_n \cong \mathbb{Z}_{mn}$ as additive groups. Furthermore, the system of congruences (5) has a solution for every choice of $a_1, a_2 \in \mathbb{Z}$, and if $x_0 \in \mathbb{Z}$ is one solution the full set of solutions in $\mathbb{Z}$ is the congruence class $[x_0]_{mn} = x_0 + \mathbb{Z}mn$.*

Proof: To keep track of the three different types of congruence classes we write $[k]_m =$

$k + \mathbb{Z}m, [k]_n = k + \mathbb{Z}n, [k]_{mn} = k + \mathbb{Z}mn$ to distinguish them. Observe that any element $[k]_{mn}$ in $\mathbb{Z}_{mn}$ determines well-defined classes $[k]_m, [k]_n$ in $\mathbb{Z}_m, \mathbb{Z}_n$ having the same representative k because the correspondences

$$[k]_{mn} \mapsto [k]_m \qquad \text{and} \qquad [k]_{mn} \mapsto [k]_n$$

are well defined maps from $\mathbb{Z}_{mn}$ into $\mathbb{Z}_m$ and $\mathbb{Z}_n$ respectively. In fact, if k' is any other representative of the class $[k]_{mn}$, that means $k' = k + s \cdot mn$ for some integer s. But $k' = k + (sn)m$ is congruent (mod m) to k and hence $[k']_m = [k]_m$; likewise $[k']_n = [k]_n$.

We now create a map ψ from $\mathbb{Z}_{mn}$ to the Cartesian product set $\mathbb{Z}_m \times \mathbb{Z}_n$ by setting

$$\psi([k]_{mn}) = ([k]_m, [k]_n) \in \mathbb{Z}_m \times \mathbb{Z}_n \qquad \text{for all } [k]_{mn} \text{ in } \mathbb{Z}_{mn} \tag{6}$$

This map is well-defined independent of how we choose representatives k of elements of $\mathbb{Z}_{mn}$. It is immediate from the definition that ψ intertwines the $(+)$ operations in the additive groups $\mathbb{Z}_{mn}$ and $\mathbb{Z}_m \times \mathbb{Z}_n$ because

$$\begin{aligned}
\psi([k]_{mn} + [\ell]_{mn}) &= \psi([k+\ell]_{mn}) \\
&= ([k+\ell]_m\,,\, [k+\ell]_n) \qquad \text{(definition of } (+) \text{ in } \mathbb{Z}_{mn}) \\
&= ([k]_m + [\ell]_m\,,\, [k]_n + [\ell]_n) \\
&= ([k]_m, [k]_n) + ([\ell]_m, [\ell]_n) \qquad \text{(defn. of } (+) \text{ in } \mathbb{Z}_m \times \mathbb{Z}_n) \\
&= \psi([k]_{mn}) + \psi([\ell]_{mn})
\end{aligned}$$

Thus $\psi : (\mathbb{Z}_{mn}, +) \to (\mathbb{Z}_m, +) \times (\mathbb{Z}_n, +)$ is a homomorphism of abelian groups.

So far we have not used the hypothesis $\gcd(m, n) = 1$, which we invoke to show that ψ is one-to-one. (It will then be surjective too, because the sets $\mathbb{Z}_{mn}$ and $\mathbb{Z}_m \times \mathbb{Z}_n$ have the same cardinality mn.) If two points in $\mathbb{Z}_{mn}$ have the same image, say with $\psi([k]_{mn}) = \psi([\ell]_{mn})$, the components in $\mathbb{Z}_m \times \mathbb{Z}_n$ must match up so that

$$\begin{cases} [k]_m = [\ell]_m \\ [k]_n = [\ell]_n \end{cases} \qquad \text{which means that} \qquad \begin{cases} k - \ell \text{ is divisible by } m \\ k - \ell \text{ is divisible by } n \end{cases}$$

We need to show that $k \equiv \ell \pmod{mn}$ or $k - \ell \equiv 0 \pmod{mn}$, so $[k]_{mn} = [\ell]_{mn}$. In general, divisibility of an integer r by m and n is not enough to insure that r is divisible by mn (try $m = 4, n = 4, r = 8$). But if m and n are relatively prime they have no prime factors in common. By comparing the prime factorizations of m, n and $k - \ell$ we see that

$$\text{If } \gcd(m, n) = 1 \text{ then } (m \text{ and } n \text{ both divide } k - \ell) \implies (mn \text{ divides } k - \ell)$$

Thus $[k]_{mn} = [\ell]_{mn}$, as required to show that ψ is one-to-one. The map ψ is the desired isomorphism between groups.

To connect all this with the remainder problem: If m, n are relatively prime the element $\mathbf{1} = ([1]_m, [1]_n)$ must be a cyclic generator for $\mathbb{Z}_m \times \mathbb{Z}_n$ because it is the ψ-image of the additive generator $[1]_{mn}$ in the cyclic group $(\mathbb{Z}_{mn}, +)$. Given $a_1, a_2 \in \mathbb{Z}$, consider the element $\mathbf{a} = ([a_1]_m, [a_2]_n)$ in the product group. Then some multiple of $\mathbf{1}$ is equal to $\mathbf{a}$, say $\mathbf{a} = k \cdot \mathbf{1}$:

$$([a_1]_m, [a_2]_n) = \mathbf{a} = k \cdot \mathbf{1} = (k \cdot [1]_m, k \cdot [1]_n) = ([k]_m, [k]_n) \qquad \text{in } \mathbb{Z}_m \times \mathbb{Z}_n$$

so that $k \equiv a_1 \pmod{m}$ and $k \equiv a_2 \pmod{n}$. That makes $x_0 = k$ a solution of the system (5), which has a solution because $\gcd(m, n) = 1$. If k' is another solution then $k' \cdot \mathbf{1} = \mathbf{a} = k \cdot \mathbf{1}$ so we get $(k' - k) \cdot \mathbf{1} = \mathbf{a} - \mathbf{a} = \mathbf{0} = ([0]_m, [0]_n)$. But $\mathbf{1}$ has order mn, being the generator of $\mathbb{Z}_{mn}$, so this happens $\Leftrightarrow (k' - k)$ is a multiple of mn. The full set of solutions is therefore $x_0 + \mathbb{Z} \cdot mn$ as claimed. $\square$

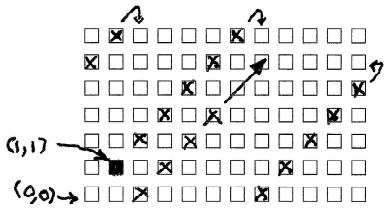

Figure 6.1 The product group $\mathbb{Z}_m \times \mathbb{Z}_n$ represented as an $m \times n$ array. The element $\mathbf{1} = (1,1)$ is shaded and its iterates are marked "x". In this portrayal the array is 7×12; since $gcd(7,12) = 1$ the iterates will cycle once through each point in the array before returning to position $\mathbf{1}$.

***6.1.27 Exercise.** The CRT implies that $\gcd(m,n) = 1 \Rightarrow \mathbb{Z}_m \times \mathbb{Z}_n \cong \mathbb{Z}_{mn}$. Prove the converse implication ($\Leftarrow$).
Hint: Recall Exercise 6.1.18, and that $\operatorname{lcm}(a,b) = ab/\gcd(a,b)$. $\square$

Thus we have

$$\mathbb{Z}_m \times \mathbb{Z}_n \cong \mathbb{Z}_{mn} \Leftrightarrow \mathbb{Z}_m \times \mathbb{Z}_n \text{ is cyclic} \Leftrightarrow \gcd(m,n) = 1 \tag{7}$$

6.1.28 Exercise. Is $\mathbb{Z}_{45} \cong \mathbb{Z}_9 \times \mathbb{Z}_5$? Is $\mathbb{Z}_{45} \cong \mathbb{Z}_{15} \times \mathbb{Z}_3$? Is $\mathbb{Z}_3 \times \mathbb{Z}_4 \times \mathbb{Z}_5 \cong \mathbb{Z}_{60}$?
Hint: For the last part try writing $\mathbb{Z}_3 \times \mathbb{Z}_4 \times \mathbb{Z}_5 = (\mathbb{Z}_3 \times \mathbb{Z}_4) \times \mathbb{Z}_5$. $\square$

***6.1.29 Exercise.** For $\mathbb{Z}_7 \times \mathbb{Z}_{12}$ find an "additive exponent" k such that

$$k \cdot \mathbf{1} = k \cdot ([1]_7, [1]_{12}) \quad \text{is equal to} \quad ([3]_7, [-4]_{12})$$

Then find a "normalized" solution lying in the range $0 \le k < 7 \cdot 12 = \operatorname{lcm}(7,12) = 84$. $\square$

The underlying idea used to oprove 6.1.26 is illustrated in Figure 6.1 where we represent $\mathbb{Z}_m \times \mathbb{Z}_n$ as an $m \times n$ array of squares. Counting from the bottom left square $\mathbf{0} = (0,0)$, the element $\mathbf{1} = (1,1)$ is the dark shaded square and its additive "powers"

$$\mathbf{1},\ 2\cdot\mathbf{1} = \mathbf{1} + \mathbf{1} = (2,2), \ldots,\ k\cdot\mathbf{1} = (k,k), \ldots$$

move diagonally upward until they hit an edge, at which point they re-enter the array from the opposite edge. If $\gcd(m,n) = 1$ the CRT says that *all squares get hit exactly once* until we finally arrive back at $\mathbf{0} = mn \cdot \mathbf{1}$; the next step takes us to $\mathbf{1} = (1,1)$ and then the pattern repeats. This observation also tells us how to compute the inverse $\psi^{-1} : \mathbb{Z}_m \times \mathbb{Z}_n \to \mathbb{Z}_{mn}$ of the isomorphism ψ constructed in proving 6.1.26. A pair $\mathbf{a} = ([a_1]_m, [a_2]_n)$ is the ψ-image of some $[k]_{mn}$ back in $\mathbb{Z}_{mn} \Leftrightarrow k$ is the first integer $k = 0, 1, 2, \ldots$ such that $k \cdot \mathbf{1} = \mathbf{a}$. This k is of course the desired solution of the congruence system (5), so knowing how to compute ψ^{-1} is equivalent to being able to solve the remainder problem.

> Algorithm for Solving the Remainder Problem. If $\gcd(m,n) = 1$ we know that solutions exist and are unique up to an added multiple of mn; the problem is to lay hands on a particular solution x_0, say one normalized so that $0 \le x_0 < mn$.
>
> Let's work backward: if x_0 is a solution then
>
> $$\begin{cases} [x_0]_m = [a_1]_m \\ [x_0]_n = [a_2]_n \end{cases} \implies \text{there exist } K, L \in \mathbb{Z} \text{ such that } \begin{cases} x_0 = a_1 + Km \\ x_0 = a_2 + Ln \end{cases}$$

Thus $x_0 = a_1 + Km = a_2 + Sn$ which implies $a_2 - a_1 = Km - Ln$. Conversely if we can find integers K, L such that $a_2 - a_1 = Km - Ln$, than

$$x_0 = a_1 + Km = a_2 + Ln$$

is a solution of the congruence problem (5).

Since $\gcd(m, n) = 1$ we can find $r, s \in \mathbb{Z}$ such that $1 = rm + sn = rm - (-s)n$. Multiplying both sides by $(a_2 - a_1)$ yields

$$(a_2 - a_1) = \big[(a_2 - a_1)r\big]\, m - \big[(a_2 - a_1)(-s)\big]\, n$$

from which we can read off suitable values for K, L.

$$K = (a_2 - a_1)r \qquad L = -(a_2 - a_1)s$$

A particular solution is then $x_0 = a_1 + Km = a_2 + Ln$ (both values being equal). $\square$

6.1.30 Exercise. Use the method outlined above to find all solutions of the congruence problem

$$x \equiv 14 \pmod{18} \qquad x \equiv -2 \pmod{25}$$

Find a particular solution lying in the range $0 \leq x_0 < 480 = \text{lcm}(18, 25)$. $\square$

6.1.31 Exercise. If $\gcd(m, n) = c > 1$ can we *ever* have $\mathbb{Z}_m \times \mathbb{Z}_n \cong \mathbb{Z}_{mn}$? $\square$

The CRT can be generalized in many ways. It can be made to work, with essentially the same proof, for congruence systems of arbitrary size provided we require that the moduli $n_1, \ldots, n_r$ be *pairwise* relatively prime, so that $\gcd(n_i, n_j) = 1$ if $i \neq j$. This is a much stronger condition than saying $\gcd(n_1, \ldots, n_r) = 1$, which means that no single prime $p > 1$ divides every n_i.

6.1.32 Exercise. Using induction on r prove that $\mathbb{Z}_{n_1 n_2 \ldots n_r} \cong \mathbb{Z}_{n_1} \times \ldots \times \mathbb{Z}_{n_r}$ if the n_i are pairwise relatively prime (so $\gcd(n_i, n_j) = 1$ if $i \neq j$). $\square$

6.1.33 Exercise. Give an example of integers $n_1, n_2, n_3 > 1$ that are *jointly* relatively prime (so that $\gcd(n_1, n_2, n_3) = 1$: there is no single prime p such that $p | n_i$ for all i) but the n_i are not *pairwise* relatively prime (so $\gcd(n_i, n_j) = 1$ and n_i, n_j have no primes in common if $i \neq j$). $\square$

In another direction, recall that $\mathbb{Z}_n$ comes equipped with both a $(+)$ and a multiplication operation $(\cdot)$, making it a *commutative ring with identity* as in Chapter 2. One can define a direct product $R_1 \times R_2$ of commutative rings very much as we defined direct product of groups, by imposing the following sum and product operations on the Cartesian product set $R_1 \times R_2 = \{(a, b) : a \in R_1, b \in R_2\}$

$$\begin{aligned} (r_1, r_2) + (r_1', r_2') &= (r_1 + r_1', r_2 + r_2') \\ (r_1, r_2) \cdot (r_1', r_2') &= (r_1 r_1', r_2 r_2') \end{aligned}$$

It is easy to check that $(R_1 \times R_2, +, \cdot)$ is a new commutative ring, with identity element $\mathbf{1} = (1_1, 1_2)$ if each R_k has an identity element 1_k.

A review of the proof of the Chinese Remainder Theorem reveals that the bijective map $\psi : \mathbb{Z}_{mn} \to \mathbb{Z}_m \times \mathbb{Z}_n$ created there is actually an isomorphism of *commutative rings*

because it intertwines both the $(+)$ and $(\cdot)$ operations

$$\begin{aligned}
\psi([k]_{mn} + [\ell]_{mn}) &= \psi([k]_{mn}) + \psi([\ell]_{mn}) \qquad \text{(proved in 6.1.26)} \\
\psi([k]_{mn} \cdot [\ell]_{mn}) &= \psi([k\ell]_{mn}) = ([k\ell]_m, [k\ell]_n) \\
&= ([k]_m, [k]_n) \cdot ([\ell]_m, [\ell]_n) \qquad \text{(defn. of } (\cdot) \text{ in } \mathbb{Z}_m \times \mathbb{Z}_n) \\
&= \psi([k]_{mn}) \cdot \psi([\ell]_{mn})
\end{aligned}$$

Thus $\mathbb{Z}_{mn} \cong \mathbb{Z}_m \times \mathbb{Z}_n$ as *rings*, not just as groups. One consequence is a result about the group of units $\mathrm{U}_n \subseteq \mathbb{Z}_n$ that has important consequences in number theory, although we will just view it as a result about the direct product structure of certain groups of units.

6.1.34 Theorem. *If $m, n > 1$ are relatively prime and $\mathrm{U}_m, \mathrm{U}_n, \mathrm{U}_{mn}$ are the abelian multiplicative groups of units in $\mathbb{Z}_m, \mathbb{Z}_m, \mathbb{Z}_{mn}$ then*

$$(\mathrm{U}_{mn}, \cdot\,) \cong (\mathrm{U}_m, \cdot\,) \times (\mathrm{U}_n, \cdot\,) \tag{8}$$

and in particular the sizes of these groups satisfy the following multiplicative condition

$$|\mathrm{U}_{mn}| = |\mathrm{U}_m| \cdot |\mathrm{U}_n| \qquad \textit{if } \gcd(m, n) = 1 \tag{9}$$

Before launching into the proof we remark that the set of units in any commutative ring R with identity $1_{_R} \in R$ is defined just as for $\mathbb{Z}_n$

$$\mathrm{U}_R = \{x \in R : \exists\, y \in R \text{ such that } x \cdot y = 1_{_R}\} \tag{10}$$

The element y in (10) is called the multiplicative inverse of x, written $y = x^{-1}$, and it is unique if it exists. As with $\mathbb{Z}_n$, the units U_R form a commutative group $(\mathrm{U}_R, \cdot\,)$ under multiplication. The proof of 6.1.34 rests on two easily verified properties of groups U_R.

***6.1.35 Exercise**. If $\psi : R \to R'$ is an isomorphism of commutative rings with identity show that

(a) ψ maps identity element to identity element: $\psi(1_R) = 1_{R'}$.

(b) ψ maps units to units, $\psi(\mathrm{U}_R) = \mathrm{U}_{R'}$, and is an isomorphism of these multiplicative groups. $\square$

***6.1.36 Exercise.** If R_1, R_2 are commutative rings with identities $1_1 \in R_1, 1_2 \in R_2$ show that the set of units $\mathrm{U}_{R_1 \times R_2}$ in the direct product ring is the Cartesian product of the separate groups of units

$$\mathrm{U}_{R_1 \times R_2} = \mathrm{U}_{R_1} \times \mathrm{U}_{R_2} = \{(x, y) : x \in \mathrm{U}_{R_1}, y \in \mathrm{U}_{R_2}\} \quad \square \tag{11}$$

Proof of (6.1.34): First observe that $\psi : \mathbb{Z}_{mn} \to \mathbb{Z}_m \times \mathbb{Z}_n$ maps U_{mn} one-to-one onto the group of units $\mathrm{U}_{\mathbb{Z}_m \times \mathbb{Z}_n}$, by 6.1.35. By 6.1.36, the group of units in $\mathbb{Z}_m \times \mathbb{Z}_n$ is equal to $\mathrm{U}_m \times \mathrm{U}_n$. Since ψ is a bijection that intertwines the $(\cdot)$ operations on each side it is a group isomorphism from $(\mathrm{U}_{mn}, \cdot\,)$ to the direct product group $(\mathrm{U}_m, \cdot\,) \times (\mathrm{U}_n, \cdot\,)$. $\square$

Remarks: Even if m and n are relatively prime, the orders $|\mathrm{U}_m|, |\mathrm{U}_n|$ of the groups of units need not have this property. For instance, if $p > 1$ is a prime then $|\mathrm{U}_p| = p - 1$ and there is no simple connection between p and the prime divisors of $p - 1$, or between the divisors of $|\mathrm{U}_p| = p - 1$ and $|\mathrm{U}_q| = q - 1$ if p, q are different primes. Furthermore the groups $\mathrm{U}_m, \mathrm{U}_n$ need not be cyclic, though they are abelian. Nevertheless we get a direct product decomposition (8). Theorem 6.1.34 operates in a very different environment from that of the Chinese Remainder Theorem 6.1.26. Its proof is also more subtle in that it rests on the interplay between the $(+)$ and $(\cdot)$ operations in $\mathbb{Z}$, while the CRT spoke only of $(+)$.

6.1.37 Exercise. If $n_1, \ldots, n_r$ are pairwise relatively prime, with $\gcd(n_i, n_j) = 1$ for $i \neq j$, use induction on r to prove that

$$\mathrm{U}_{n_1 n_2 \ldots n_r} \cong \mathrm{U}_{n_1} \times \ldots \times \mathrm{U}_{n_r} \qquad \text{and} \qquad |\mathrm{U}_{n_1 n_2 \ldots n_r}| = |\mathrm{U}_{n_1}| \cdot \ldots \cdot |\mathrm{U}_{n_r}| \quad \square$$

6.1.38 Exercise. Write $\mathbb{Z}_{630}$ as a direct product $\mathbb{Z}_{n_1} \times \ldots \times \mathbb{Z}_{n_r}$ of cyclic groups. Using 2.5.30 we could compute $|\mathrm{U}_{630}|$ by tediously comparing the prime divisors of $630 = 2 \cdot 3^2 \cdot 5 \cdot 7$ with those of each $1 \leq k < 630$. However, the formula of 6.1.35 might provide an easier way to calculate $|\mathrm{U}_{630}|$. Do it.
Hint: Is the group of units $(\mathrm{U}_9, \cdot)$ cyclic? (Check orders $o(x)$ of its elements.) $\square$

The **Euler Phi-Function** $\phi : \mathbb{N} \to \mathbb{N}$ is often mentioned in number theory. It has many equivalent definitions, but for us it is easiest to take

$$\phi(1) = 1 \qquad \phi(n) = |\mathrm{U}_n| = \#(\text{multiplicative units in } \mathbb{Z}_n)$$

Theorem 6.1.34 shows that ϕ is "multiplicative," with $\phi(mn) = \phi(m)\phi(n)$ if m and n are relatively prime, and it is this property that makes the ϕ-function so useful.

***6.1.39 Exercise**. The multiplicative property of Exercise 6.1.34 is no help in computing the size of the group of units U_{p^k} where p is a prime, since p^k does not split into relatively prime factors. (Think $p = 2, k = 7, p^k = 128$.) However, one can show directly that

$$\mathrm{U}_{p^k} = \#\{1 \leq j < p^k : \gcd(j, p^k) = 1\} = \#\{1 \leq j < p^k : j \text{ is not a multiple of } p\}$$

has cardinality $|\mathrm{U}_{p^k}| = p^{k-1}(p-1)$. Carry out this computation.
Hint: Every integer $0 \leq m < p^k$ has a unique "base p" expansion

$$m = a_0 + a_1 p + a_2 p^2 + \ldots + a_{k-1} p^{k-1}$$

where $0 \leq a_j < p$ for each j. Some divisiblity questions become easy using base p expansions. You may want to use the following exercise too. $\square$

6.1.40 Exercise. Explain why $\gcd(m, p^k) \neq 1 \Leftrightarrow m$ is a multiple of p. $\square$

6.1.41 Exercise. Compute the size $|\mathrm{U}_n|$ for

$$\text{(a) } n = 6561 \qquad \text{(b) } n = 3076 \qquad \text{(c) } n = 2 \cdot 3^2 \cdot 5^3 \cdot 49 = 110,250 \quad \square$$

By exploiting the multiplicative property of the ϕ-function we obtain a group-theoretic proof of the following important fact from number theory that reflects the subtle interplay between the operations $(+)$ and $(\cdot)$ in the ring $\mathbb{Z}_n$.

6.1.42 Theorem. *For any integer $n \geq 1$ we have*

$$n = \sum_{d|n\,,\,1 \leq d \leq n} \phi(d) = \sum_{d|n\,,\,1 \leq d \leq n} |\mathrm{U}_d|$$

Proof: In the cyclic group $(\mathbb{Z}_n, +)$ every element x has some additive order $o^+(x) =$ smallest integer $k \geq 1$ such that $k \cdot x = [0]$; by Lagrange, this must be a divisor of n. Letting $S_d = \{x \in \mathbb{Z}_n : o^+(x) = d\}$ we obviously have $\mathbb{Z}_n = \bigcup_{d|n} S_d$. These sets are disjoint, and they are all nonempty because, as in Theorem 3.4.7, there is a *unique* cyclic subgroup H_d of order d in $\mathbb{Z}_n$ for each divisor $d|n$. Its generator lies in S_d so S_d is nonempty, but by uniqueness of the group H_d we must have $\langle x \rangle = H_d$ for each $x \in S_d$, so that $S_d \subseteq H_d$. Under the isomorphism $H_d \cong (\mathbb{Z}_d, +)$ the set S_d corresponds to the cyclic

generators in $(\mathbb{Z}_d, +)$. But in Proposition 3.1.33 we identified these generators explicitly as the set of units $\mathrm{U}_d \subseteq \mathbb{Z}_d$. It follows that

$$n = \sum_{d|n} |S_d| = \sum_{d|n} |\mathrm{U}_d| = \sum_{d|n} \phi(d)$$

as claimed. □

6.2 Semidirect products.

We have determined all groups of order $1 \leq |G| \leq 5$ using the notion of direct product. But when $|G| = 6$ we encountered a case that cannot be understood in terms of cyclic groups and their direct products. In that example there were subgroups $H_2 \cong \mathbb{Z}_2$ and $H_3 \cong \mathbb{Z}_3$ such that

$$H_3 \cdot H_2 = G \qquad H_3 \cap H_2 = (e) \qquad H_3 \lhd G \qquad H_2 \textit{ not} \text{ normal in } G$$

If H_2 were normal we would have a direct product $H_3 \times H_2$, but since it is not we are confronted with something new. This leads us to a more general product construction, the **semidirect product** $N \rtimes H$ of two groups, motivated by the following considerations.

If A and B are subgroups of a group G, the conditions

$$AB = G \qquad \text{and} \qquad A \cap B = (e) \tag{12}$$

imply that every $g \in G$ has a unique factorization $g = ab$. Existence is clear since $G = AB$, while uniqueness follows from the condition $A \cap B = (e)$ because

$$\begin{aligned} a_1 b_1 = a_2 b_2 \quad &\Rightarrow \quad (a_2)^{-1} a_1 = b_2 (b_1)^{-1} \text{ is in } A \cap B \\ &\Rightarrow \quad (a_2)^{-1} a_1 = e \text{ and } b_2 (b_1)^{-1} = e \\ &\Rightarrow \quad a_2 = a_1 \text{ and } b_2 = b_1 \end{aligned}$$

This means there is a natural "parametrization" of points in G by pairs (a, b) in the Cartesian product space $A \times B$, which at the moment is not equipped with a group structure. The correspondence $A \times B \approx G$ is effected by the bijection $p : A \times B \to G$ with $p(a, b) = a \cdot b$ (product of a and b in G). The labels a and b may be thought of as "coordinates" labeling all points in G, and it is natural to ask what the group operation looks like when described in terms of these parameters.

If *both* A and B are normal subgroups then by 6.1.9 the group G is their internal direct product and our question has a simple answer. When we identify G with the product set $A \times B$ the group operations take the familiar form

$$(a, b) * (a', b') = (aa', bb') \qquad (a, b)^{-1} = (a^{-1}, b^{-1})$$

and the identity element is $e = (e, e)$.

If *neither* subgroup is normal, the description of the group law in terms of these parameters can be formidable, and we will not attempt to analyze this situation here. There is, however, a fruitful middle ground: the case in which *just one* of the subgroups is normal, as in 6.1.11. This leads to the notion of *semidirect product*, which encompasses an enormous set of examples that arise in geometry and higher algebra

In this setting we relabel the subgroups as N and H with N the normal subgroup, so it will be readily apparent in calculations which group elements lie in the normal subgroup. Points in G are labeled by pairs (n, h) in the product set $N \times H$, and the product operation in G can be described explicitly in terms of these pairs. Given elements $g_1 = n_1 h_1$, $g_2 = n_2 h_2$ in G we must rewrite $g_1 g_2 = n_1 h_1 \cdot n_2 h_2$ as a product $n'' h''$ with $n'' \in N, h'' \in H$. The problem is, essentially, to move h_1 to the other side of n_2, keeping

track of the damage if they fail to commute. This is easy when $N \lhd G$ because we may multiply and divide by h_1 to get

$$n_1 h_1 n_2 h_2 = n_1(h_1 x h_1^{-1}) \cdot h_1 h_2 = n'' \cdot h''$$

in which $n'' \in N$ because $h_1 N h_1^{-1} \subseteq N$. Identifying each g_i with its corresponding pair (n_i, h_i) in $N \times H$, the group multiplication law takes the form

$$\begin{aligned} (n_1, h_1) \cdot (n_2, h_2) &= (n_1(h_1 n_2 h_1^{-1})\,,\, h_1 h_2) \\ &= (n_1 \phi_{h_1}(n_2)\,,\, h_1 h_2) \end{aligned} \tag{13}$$

where $\phi_h : N \to N$ is the conjugation operation $\phi_h(n) = hnh^{-1}$ for any $h \in H$. The normal subgroup N is invariant under the action of any conjugation $\alpha_g(n) = gng^{-1}$ by $g \in G$, and ϕ_h is just the restriction $\phi_h = \alpha_h | N$ of the inner automorphism α_h on G to the subset N. Obviously $\phi_h \in \mathrm{Aut}(N)$ for each $h \in H$, and we obtain a group action $H \times N \to N$ of H on N such that

$$\phi_e = \mathrm{id}_N \qquad \phi_{h_1 h_2} = \phi_{h_1} \circ \phi_{h_2} \qquad \phi_{h^{-1}} = (\phi_h)^{-1} \quad \text{(inverse of the operator } \phi_h)$$

which means that the correspondence $\Phi : H \to \mathrm{Aut}(N)$ given by $\Phi(h) = \phi_h$ is a group homomorphism. Conversely, as we noted in our previous discussion of group actions (Chapter 4), every such homomorphism Φ determines an action of H on N by automorphisms and there is a one-to-one correspondence between such actions $H \times N \to N$ and homomorphisms $\Phi : H \to \mathrm{Aut}(N)$. As we will see in Theorem 6.2.5 every such action determines a group law on the Cartesian product set $N \times H$:

$$(n_1, h_1) * (n_2, h_2) = (n_1 \cdot \phi_{h_1}(n_2)\,,\, h_1 h_2)$$

It is evident from (13) that the original group G can be reconstructed from its subgroups N, H if we know the action of H on N via conjugation operators ϕ_h. In this way G is realized as an "internal semidirect product" of N by H – i.e. as the Cartesian product set $N \times H$ equipped with the multiplication law (13) determined by ϕ_h. We summarize these remarks as follows.

6.2.1 Proposition (Internal Semidirect Product). *Let G be a group and N, H two subgroups such that*

$$\text{(i) } N \text{ is normal in } G \qquad \text{(ii) } NH = G \qquad \text{(iii) } N \cap H = (e)$$

Each $g \in G$ has a unique factorization as $g = nh$, so there is a natural bijection between G and the Cartesian product set $N \times H$. The group action $H \times N \to N$ via conjugation operators $\phi_h(n) = hnh^{-1}$ in $\mathrm{Aut}(N)$ determines the following "product operation" in the Cartesian product set $N \times H$.

$$(n, h) * (n', h') = (n \phi_h(n')\,,\, hh') \qquad \text{for } n, n' \in N \text{ and } h, h' \in H \tag{14}$$

This operation makes the Cartesian product set into a group, and the product map $p(n, h) = nh$ becomes an isomorphism from $(N \times H, *)$ to the original group G.

Proof: We have noted the unique factorization $g = nh$ in the remarks following (12); the bijection $N \times H \approx G$ is given by the product map $p(n, h) = nh$. Our other claims follow if we can just prove that the product map p intertwines group operations in $N \times H$ and G:

$$p\big((n, h) * (n', h')\big) = p(n, h) p(n', h')$$

From definition (14) we see that

$$\begin{aligned} p(n,h)p(n',h') &= nhn'h' = n(hn'h^{-1})hh' = n\phi_h(n')hh' \\ &= p\big(n\phi_h(n'), hh'\big) = p\big((n,h)*(n',h')\big) \end{aligned}$$

as desired (last step by definition (14)). □

All this is expressed by saying that G is the **internal semidirect product** of the subgroups N and H, which we indicate by writing $G = N \rtimes H$ or $N \rtimes_\phi H$ to distinguish it from the *direct* product $N \times H$ of Section 6.1. Of course if the action $H \times N \to N$ is trivial, as when the subgroups H and N commute (so that $\phi_h = \mathrm{id}_N$ for all $h \in H$), then the semidirect product reduces to the ordinary direct product.

6.2.2 Exercise. In a semidirect product $G = N \rtimes H$ with group law (14) the identity element is just the pair $e = (e, e)$. Use this observation to compute the inverse

$$(15) \qquad (n,h)^{-1} = (h^{-1}n^{-1}h, h^{-1}) = (\phi_{h^{-1}}(n^{-1}), h^{-1}) \qquad \text{for all } n \in N,\ h \in H$$

for any pair $(n, h) \in N \times H$. □

6.2.3 Exercise. In a semidirect product $G = N \rtimes_\phi H$ with group law (14) the pairs (n, e) and (e, h) in the product set $N \times H$ correspond under p to the group elements $n \in N$ and $h \in H$. Use (14) and (15) to verify that

(a) $(n,e)\cdot(e,h) = (n,h)$

(b) Conjugation of (n, e) by (e, h) under the group law (14) has the same effect in $N \rtimes H$ as conjugating n by h in the original group G – i.e. we have

$$(e,h)(n,e)(e,h)^{-1} = (hnh^{-1}, e) = (\phi_h(n), e)$$

What are the coordinates (n', h') of the group element $(e, h)\cdot(n, e)$ obtained by reversing the order of the factors in (a)? □

***6.2.3A Exercise.** In a semidirect product $N \rtimes_\phi H$ prove that conjugating an element $x = (n', h')$ by an element $g = (n, h)$ yields

$$\alpha_g(x) = (n,h)(n',h')(n,h)^{-1} = \big(n\cdot\phi_h(n')\cdot\phi_{hh'h^{-1}}(n^{-1})\,,\ hh'h^{-1}\big)$$

Write out the simpler formula describing the action of an arbitrary $g = (n, h)$ in G on an element $x = (n', e)$ of the normal subgroup N. □

The following observation often simplifies the job of deciding whether a group G is in fact a semidirect product of two of its subgroups.

***6.2.4 Exercise.** Let G be a group and N, H subgroups such that (i) $NH = G$, (ii) $N \cap H = (e)$, and assume that

(iii) H *normalizes* N in the sense that $hNh^{-1} \subseteq N$ for every $h \in H$.

Prove that N is in fact normal in G, so G is the internal semidirect product $N \rtimes H$. □

External Semidirect Product. We now reverse this bottom-up analysis, in which N and H lie within a pre-existing group G. Instead we shall construct a new group $N \rtimes H$, the **external semidirect product** of N by H, given the following ingredients

(16)
(i) Two unrelated abstract groups N and H

(ii) A group action $H \times N \to N$ implemented by automorphisms $\phi_h \in \mathrm{Aut}(N)$ for each h.

Of course, specifying the action in (ii) is completely equivalent to specifying some homomorphism $\Phi : H \to \mathrm{Aut}(N)$; just take $\phi_h = \Phi(h)$.

6.2.5 Theorem. *Given abstract groups N, H and a homomorphism $\Phi : H \to \mathrm{Aut}(N)$, define a binary operation on the Cartesian product set $G = N \times H$ as in* (14) *and* (15).

$$(17) \qquad (n,h) * (n',h') = (n\phi_h(n')\,,\, hh') \qquad \text{for all } n,n' \in N \text{ and } h,h' \in H$$

where $\phi_h = \Phi(h) \in \mathrm{Aut}(N)$. Then $(G,*)$ is a group, the **external semidirect product**, *which we denote by $N \rtimes_\phi H$. The inversion operation $g \mapsto g^{-1}$ has the form* (15).

The subsets $\overline{N} = \{(n,e) : n \in N\}$ and $\overline{H} = \{(e,h) : h \in H\}$ are subgroups in G that are isomorphic to N and H. They satisfy the conditions $\overline{N} \cdot \overline{H} = G$, $\overline{N} \cap \overline{H} = (e)$, and $\overline{N}$ is normal in G. Thus G is the internal semidirect product of these subgroups.

Proof: There is some bother involved in checking that the operation (17) is associative, with $(x * y) * z = x * (y * z)$ for all $x, y, z \in N \times H$, because the action does not arise via multiplications in some pre-existing group as it did in 6.2.1. We leave this routine but tedious calculation to the reader.

The identity element is obviously $e = (e,e) = (e_{_N}, e_{_H})$. The inverse operation is

$$(n,h)^{-1} = (\phi_{h^{-1}}(n^{-1}), h^{-1})$$

In fact, recalling that $\phi_e = \mathrm{id}_{_N}$ and that $\phi_{h^{-1}} = (\phi_h)^{-1}$ because $\Phi : H \to \mathrm{Aut}(N)$ is a homomorphism, (17) gives

$$\begin{aligned} (n,h) * \big(\phi_{h^{-1}}(n^{-1}), h^{-1}\big) &= \big(n\phi_h(\phi_h^{-1}(n^{-1}))\,,\, hh^{-1}\big) = (nn^{-1}, e) = (e,e) \\ (\phi_{h^{-1}}(n^{-1}), h^{-1}) * (n,h) &= \big(\phi_{h^{-1}}(n^{-1})\phi_h^{-1}(n)\,,\, h^{-1}h\big) \\ &= \big(\,(\phi_h^{-1}(n))^{-1}\phi_h^{-1}(n)\,,\, e\big) = (e,e) \end{aligned}$$

In G the maps $n \mapsto (n,e) \in \overline{N}$ and $h \mapsto (e,h) \in \overline{H}$ are isomorphic embeddings of N and H in G because they are bijections such that

$$(n,e) * (n',e) = (nn',e) \qquad \text{and} \qquad (e,h) * (e,h') = (e,hh')$$

We get $G = \overline{N} * \overline{H}$ because $(n,e) * (e,h) = (n\phi_e(e), eh) = (n,h)$ and it is obvious that $\overline{N} \cap \overline{H} = \{(e,e)\}$. Normality of $\overline{N}$ follows because

$$\begin{aligned} (n,h) * (n',e) * (n,h)^{-1} &= \big(n\phi_h(n'),h\big) * \big(\phi_{h^{-1}}(n^{-1}), h^{-1}\big) \\ &= \big(n\phi_h(n') \cdot \phi_h\big(\phi_{h^{-1}}(n^{-1})\big)\,,\, hh^{-1}\big) \\ &= \big(n\phi_h(n')n^{-1}\,,\, e\big) \end{aligned}$$

for all $n' \in \overline{N}$; the result is back in $\overline{N}$ so that $g\overline{N}g^{-1} \subseteq \overline{N}$ for any g, as required.

When we identify $\overline{N} \cong N$ and $\overline{H} \cong H$, the action of $\overline{h} \in \overline{H}$ by conjugation on $\overline{n} \in \overline{N}$ matches up with the original action of $H \times N \to N$ determined by Φ, so the group G we have constructed is the internal semidirect product $\overline{N} \rtimes \overline{H}$. $\square$

6.2.5A Exercise. Let $G = N \rtimes_\phi H$ be an external semidirect product. When we identify $N \cong \overline{N}, H \cong \overline{H}$ show that the action of $\overline{h} = (e,h)$ by conjugation on $\overline{n} = (n,e)$ becomes the action of the automorphism $\phi_h : N \to N$ appearing in (17). $\square$

The next example is important in geometry.

6.2.6 Example The Dihedral Groups $\mathbf{D_n}$). These groups of order $|D_n| = 2n$, defined for $n \geq 2$, are the full symmetry groups of regular n-gons. To describe D_n consider a regular n-gon in the xy-plane, centered at the origin and with one vertex on the positive

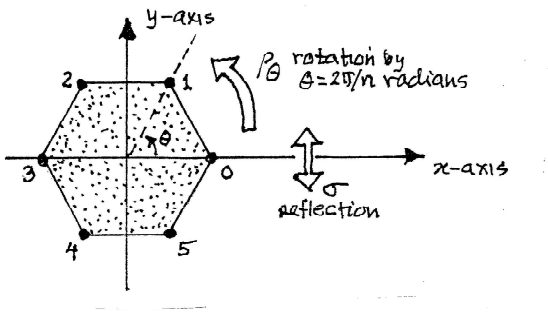

Figure 6.2. The basic symmetry operations on a regular n-gon, shown here for the regular hexagon ($n = 6$). The same idea works for all n. In our discussions vertices are labeled $0, 1, 2, \ldots, n-1$ as indicated. The symmetry groups D_n have different properties for even and odd n, and $n = 2$ is exceptional.

x-axis, as shown in Figure 6.2 (where $n = 6$). Let $\theta = 2\pi/n$ radians, and define the basic symmetry operations

$$\begin{aligned} \rho_\theta &= \text{(counterclockwise rotation about the origin by } \theta \text{ radians)} \\ \sigma &= \text{(reflection across the } x\text{-axis)} \end{aligned}$$

Obviously these elements have orders

$$\begin{aligned} &o(\sigma) = 2 \ \text{ so } \sigma^2 = e \text{ and } \sigma^{-1} = \sigma \\ &o(\rho_\theta) = n \ \text{ with distinct powers } \rho_\theta^j \text{ for } 0 \le j < n \text{ and } \rho_\theta^n = I. \end{aligned} \tag{18A}$$

The **dihedral group** D_n is the subgroup $D_n = \langle \rho_\theta, \sigma \rangle$ generated by ρ_θ and σ in the group $\mathrm{O}(2)$ of linear *isometries* (distance-preserving transformations) of the plane. Obviously $N = \langle \rho_\theta \rangle$ is a cyclic subgroup isomorphic to $\mathbb{Z}_n$ and $H = \langle \sigma \rangle$ is a copy of $\mathbb{Z}_2$ embedded in D_n. We will show that N is normal and D_n is the semidirect product $N \rtimes H$.

We begin by verifying another relation, which together with the obvious relations (18A) completely determines D_n.

$$\sigma\rho_\theta\sigma = \sigma\rho_\theta\sigma^{-1} = \rho_\theta^{-1} \qquad \text{(Note that } \rho_\theta^{-1} = \rho_{-\theta} \text{ and } \sigma^{-1} = \sigma\text{)} \tag{18B}$$

This relation tells us how to pass a rotation across a reflection when forming products, since $\sigma\rho_\theta = \rho_\theta^{-1}\sigma$; furthermore, since conjugation by σ is an automorphism we also get

$$\sigma\rho_\theta^k\sigma = \sigma\rho_\theta^k\sigma^{-1} = (\sigma\rho_\theta\sigma^{-1})^k = \rho_\theta^{-k} = \rho_{-k\theta} \qquad \text{for all } \ k \in \mathbb{Z}$$

One could check (18B) by tedious matrix computations, but it is easier simply to track the action of each factor on the standard unit vectors $\mathbf{e}_1 = (1, 0), \mathbf{e}_2 = (0, 1)$ in $\mathbb{R}^2$, as shown in Figure 6.3 below. Once we know what the product does to basis vectors we know what it does to all vectors, and it is not hard to recognize the outcome as a familiar linear operator. (In (18B) the end result is *clockwise* rotation by θ radians.)

Note also what happens if we repeatedly conjugate an element $\rho_\theta^k \in N$ by the reflection operation σ.

$$\sigma^i\rho_\theta^k\sigma^{-i} = \sigma^i\rho_\theta^k\sigma^i = \rho_\theta^{(-1)^i k} \tag{18C}$$

The reason is simple: conjugation by σ yields ρ_θ^{-k}, doing it again reverses the sign on

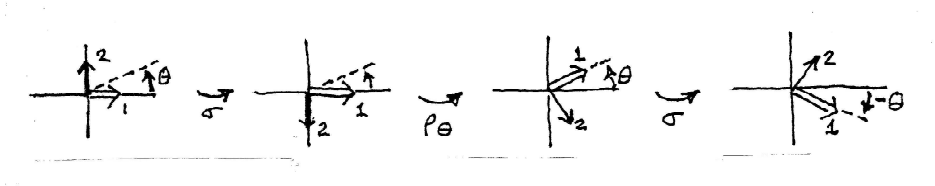

Figure 6.3. Action of $\sigma\rho_\theta\sigma$ on basis vectors in $\mathbb{R}^2$ shows that $\sigma\rho_\theta\sigma = \rho_\theta^{-1} = \rho_{-\theta}$.

the exponent one more time, leaving ρ_θ^k. Performing this "sign flip" i times yields

$$\rho_\theta^{(-1)^i k} = \begin{cases} \rho_\theta^k & \text{if } i \text{ is even} \\ \rho_\theta^{-k} & \text{if } i \text{ is odd} \end{cases}$$

Since ρ_θ and σ generate D_n the identities (18A) and (18B) imply that $N = \langle \rho_\theta \rangle$ is a *nomal* subgroup in D_n, as a consequence of the following general result.

***6.2.6A Exercise.** If elements $a_1, \ldots, a_n$ generate a group G, prove that a subgroup H is normal in $G \Leftrightarrow H$ is invariant under congugation by the generators of G:

$$a_i H a_i^{-1} = H \qquad \text{for all } 1 \le i \le n$$

Note: In practice it is much easier to verify normality by checking the action of a few generators, than to examine the action of an arbitrary group element. In the last example there were just two generators. □

Using the relations (18) we now show that every element of $D_n = \langle \rho_\theta, \sigma \rangle$ can be written uniquely in the form

$$\rho_\theta^k \sigma^\ell \qquad \text{where} \quad 0 \le k < n \text{ and } \ell = 0 \text{ or } 1$$

Since $\rho_\theta^n = \sigma^2 = I$, the operator ρ_θ^k depends only on the (mod n) congruence class of k, and it is convenient to think of this exponent as an element $k \in \mathbb{Z}_n$; likewise the exponent in σ^ℓ can be thought of as an element $\ell \in \mathbb{Z}_2$. Then the factorization of elements in D_n takes the form

(19) *Any element in the dihedral group D_n can be written uniquely in the form $\rho_\theta^k \sigma^\ell$ where $k \in \mathbb{Z}_n$ and $\ell \in \mathbb{Z}_2$.*

To prove this, we show that the set S of elements listed in (19) is already a group. Then, since $D_n = \langle \rho_\theta, \sigma \rangle \supseteq S$ and S is a subgroup containing the generators, the two sets must be equal and $D_n = S$ as claimed. Clearly $I \in S$, and $S \cdot S \subseteq S$ because

$$\begin{aligned} (\rho_\theta^k \sigma^\ell)(\rho_\theta^r \sigma^s) &= \rho_\theta^k \sigma^\ell \rho_\theta^r (\sigma^{-\ell}\sigma^\ell)\sigma^s = \rho_\theta^k (\sigma^\ell \rho_\theta^r \sigma^{-\ell})\sigma^{\ell+s} \\ &= \rho_\theta^k (\sigma^\ell \rho_\theta \sigma^{-\ell})^r \sigma^{\ell+s} \qquad \text{(conjugation by } \sigma^\ell \text{ is an automorphism)} \\ &= \rho_\theta^k \left(\rho_\theta^{(-1)^\ell}\right)^r \sigma^{\ell+s} \qquad \text{(by (18C))} \\ &= \rho_\theta^{k+(-1)^\ell r} \sigma^{\ell+s} \in S \end{aligned}$$

Finally $S^{-1} = S$, and S is a subgroup, because

$$\begin{aligned}(\rho_\theta^k\sigma^\ell)^{-1} &= \sigma^{-\ell}\rho_\theta^{-k} \\ &= \sigma^\ell\rho_\theta^{-k}\sigma^\ell\sigma^{-\ell} \qquad (\text{because } \sigma^{-\ell} = \sigma^\ell) \\ &= (\sigma^\ell\rho_\theta\sigma^\ell)^{-k}\sigma^{-\ell} \\ &= \left(\rho_\theta^{(-1)^\ell}\right)^{-k}\sigma^{-\ell} \qquad (\text{by (18C)}) \\ &= \rho_\theta^{-(-1)^\ell k}\sigma^{-\ell} \in S\end{aligned}$$

From (19) we see that D_n is a *finite* group of operators on the plane, with $|D_n| = 2n$. Summarizing these observations we have

6.2.7 Corollary (Multiplication Law in $\mathbf{D_n}$). *If two elements of D_n are written in factored form* (19)*, the group operations take the form*

(a) $(\rho_\theta^k\sigma^\ell)\cdot(\rho_\theta^r\sigma^s) = \rho_\theta^{k+(-1)^\ell r}\,\sigma^{\ell+s}$

(b) $(\rho_\theta^k\sigma^\ell)^{-1} = \rho_\theta^{-(-1)^\ell k}\sigma^{-\ell}$

for $k, r \in \mathbb{Z}_n$ and $\ell, s \in \mathbb{Z}_2$.

As for uniqueness, the identity $\rho_\theta^k\sigma^\ell = \rho_\theta^r\sigma^s$ implies $\rho_\theta^{k-r} = \sigma^{s-\ell}$. Unless both exponents are congruent to zero, the transformation on the left has determinant $+1$ while the one on the right has determinant -1, which is impossible.

We have now established that the subgroups $N = \langle\rho_\theta\rangle$ and $H = \langle\sigma\rangle$ have the properties (i) $N \cap H = (e)$, (ii) $NH = D_n$, and (iii) N is normal in D_n. Conjugation of an element $n \in N$ by an arbitrary element $g = \rho_\theta^r\sigma^s$ in D_n has the following effect.

$$g\rho_\theta^k g^{-1} = (\rho_\theta^r\sigma^s)\rho_\theta^k(\rho_\theta^r\sigma^s)^{-1} = \rho_\theta^r(\sigma^s\rho_\theta^k\sigma^{-s})\rho_\theta^{-r} = \rho_\theta^r\big(\rho_\theta^{(-1)^s k}\big)\rho_\theta^{-r} = \rho_\theta^{(-1)^s k}$$

and if g is an element $h \in H$ this becomes

$$\phi_h\big(\rho_\theta^k\big) = h\rho_\theta^k h^{-1} = \begin{cases} \rho_\theta^k & \text{if } h = e \\ \sigma\rho_\theta^k\sigma^{-1} = \rho_\theta^{-k} & \text{if } h = \sigma \end{cases} \tag{20}$$

Thus D_n is a semidirect product $\cong \mathbb{Z}_n \rtimes \mathbb{Z}_2$ under the action $H \times N \to N$ in (20). The nontrivial element $\sigma \in H$ acts as the inversion automorphism on N

$$J : \rho_\theta^k \to \big(\rho_\theta^k\big)^{-1} = \rho_\theta^{-k}$$

for all $k \in \mathbb{Z}_n$. $\square$

We now examine the geometric meaning of the symmetry operations $\rho_\theta^i\sigma$ in D_n.

6.2.8 Example ($\mathbf{D_n}$ as Symmetries of the Plane). In $G = D_n = N \rtimes H$ the geometric meaning of the elements $\rho_\theta^k \in N$ and the reflection $\sigma \in H$ is clear, but what about products of the form $\rho_\theta^k\sigma$, the elements in the "other" coset in $D_n = N \cup N\sigma$? They are all orientation-reversing because $\det(\rho_\theta^k\sigma) = \det\sigma = -1$. We will show that these are *reflections* across the lines of reflection symmetry shown in Figure 6.3A:

$$\rho_\theta^k\cdot\sigma = r_{\ell(k\theta/2)} = (\text{reflection across the line } \ell\big(k\cdot\frac{\theta}{2}\big)\,)$$

where $\ell(\phi)$ is the oriented line through the origin making an angle ϕ with the $+x$-axis.

Discussion: First consider $\rho_\theta\sigma$, whose action on basis vectors is shown in Figure 6.3B below. Compare this with the action of the reflection $r_{\ell(\theta/2)}$ across the line through the

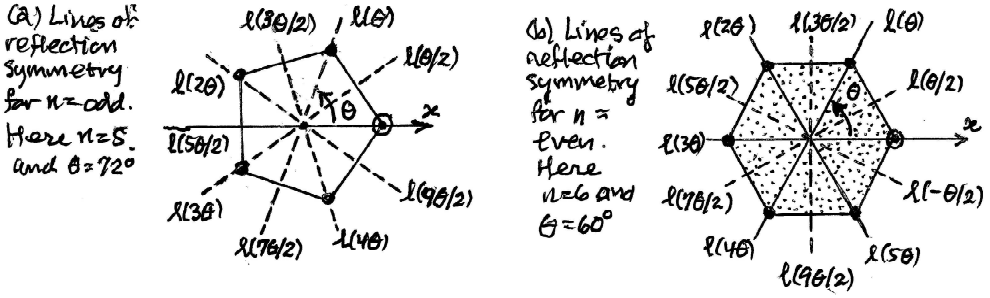

Figure 6.4A. Lines of reflection symmetry of an n-gon centered at the origin. (a) The situation for n odd: every line through a vertex passes through the midpoint of an opposite edge. (b) For even n we get two families of lines, passing through two opposite vertices or through the midpoints of opposite edges.

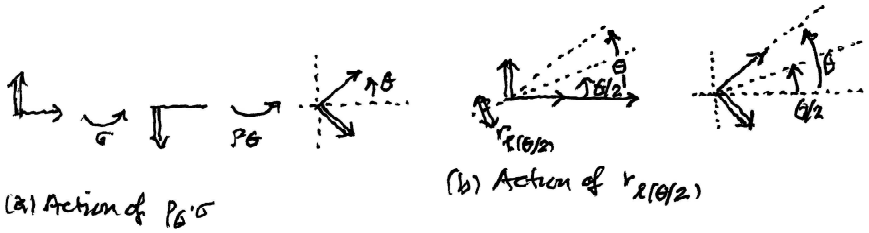

Figure 6.4B. The action on basis vectors of the operations $\rho_\theta\sigma$ and reflection $r_{\ell(\theta/2)}$ across a line making an angle $\theta/2$ with the $+x$-axis.

origin that makes an angle $\theta/2$ with the $+x$-axis. Both have the same action on basis vectors, so $\rho_\theta\sigma = r_{\ell(\theta/2)}$ as linear operators on $\mathbb{R}^2$.

But the same argument applies to rotation ρ_θ by *any* angle, in particular the angles $k\theta$ ($\theta = 2\pi/n$) corresponding to vertices of the n-gon, therefore

$$\rho_\theta^k\sigma = \rho_{k\theta}\sigma = r_{\ell(k(\theta/2))} \qquad \text{for all } k \in \mathbb{Z}$$

This accounts for all lines of reflection symmetry shown in Figure 6.4A, but there is a curious distinction between the cases $n =$ even and $n =$ odd.

As in Figure 6.4A, for even n there are two families of lines of reflection symmetry: lines $\ell(k\theta)$ through opposite vertices, and lines $\ell\big((k+\frac{1}{2})\theta\big)$ through midpoints of opposite edges. For odd n a radial line through a vertex also passes through the midpoint of the opposite edge. As we increment $k = 0, 1, 2, \ldots$ in this case the lines $\ell(k(\theta/2))$ cycle *twice* through the lines of reflection shown in Figure 6.4A(a). In either case, all lines of reflection symmetry are accounted for as elements of the coset $N\sigma$. This coset consists entirely of reflections, while N consists of orientation-preserving rotations (which have $\det = +1$). $\square$

6.2.8A Exercise. It is geometrically obvious that reflections have the property $R^2 = R \circ R = I$. Show by direct *algebraic* calculation that $\tau^2 = e$ for all τ in the coset $N\sigma$ in

D_n. $\square$

6.2.9 Exercise. In D_n explain why the group element

$$T = \rho_\theta^k \sigma \rho_\theta^{-k} \qquad (\text{with } k \not\equiv 0 \pmod{n})$$

is the reflection $\sigma_{_L}$ across the line through the origin that passes through the k^{th} vertex of the n-gon. (Label vertices $0, 1, 2, \ldots, n-1$ counterclockwise starting with the vertex on the positive x-axis).
Hint: Use the results in 6.2.8. Since $\det T = -1$ this is a reflection across some line $\ell(\phi)$ of fixed points. Find all $x \in \mathbb{R}^2$ such that $Tx = x$. $\square$

***6.2.10 Exercise.** For $n \geq 3$, what are the *geometric* actions on $\mathbb{R}^2$ corresponding to the following elements in D_n?

(a) $\rho_\theta \sigma$ and $\sigma \rho_\theta$.
(b) $\rho_\theta^k \sigma$ ($k \not\equiv 0 \bmod n$)
(c) $\rho_\theta^j \sigma \rho_\theta^{-j}$ ($j \not\equiv 0 \bmod n$)
(d) $\rho_{\pi/4} \sigma \rho_{-\pi/4}$ $\square$

***6.2.11 Exercise.** Determine the center $Z(D_n) = \{x \in D_n : gxg^{-1} = x \text{ for all } g \in G\}$ for $n \geq 3$.
Note: The answer will depend on whether n is even or odd. When $n = 2$ the group is abelian and the center is all of D_2.
Hint: By 3.1.46 an element $x = \rho^i \sigma^j$ is in the center of $D_n \Leftrightarrow x$ commutes with each of the generators ρ and σ of D_n. $\square$

6.2.12 Exercise. Determine all conjugacy classes in D_5 and in D_6.
Note: Recall that N (hence also its other coset $N\sigma$) are unions of whole conjugacy classes, so you might start by determining the classes contained in the normal subgroup. $\square$

6.2.13 Exercise. Use Exercise 6.2.12 to determine all normal subgroups in D_6 and in D_7.
Hint: Recall 5.4.2 and 5.4.6. $\square$

***6.2.14 Exercise.** Determine the conjugacy classes in D_n for arbitrary $n \geq 3$. Start by discussing the class $\mathcal{C}_\sigma = \{g\sigma g^{-1} : g \in D_n\}$.
Note: The answer is different for odd and even n. $D_2 \cong \mathbb{Z}_2 \times \mathbb{Z}_2$ is abelian and has trivial classes. $\square$

6.2.15 Example (The Group of Affine Mappings Aff(V)). The **affine mappings** on a finite dimensional vector space V are the bijective maps of the form

$$T(v) = A(v) + \mathbf{a} \qquad \text{where } A \text{ is a linear map and } \mathbf{a} \in V \tag{21}$$

It is easily seen that $T : V \to V$ is a bijection $\Leftrightarrow$ its linear part A is invertible $\Leftrightarrow \det(A) \neq 0$. It is also clear that the set of affine maps $\mathrm{Aff}(V)$ is a group under composition of operators since the composite

$$T \circ T'(v) = A(T'v) + a = A(A'v + a') + a = AA'(v) + (Aa' + a) = B(v) + b$$

is again invertible and affine. If we label $Tv = Av + a$ by the pair (a, A) the multiplication law in the affine group becomes

$$(a, A) \cdot (a', A') = \big(a + A(a')\,,\; AA'\big) \tag{22}$$

when expressed in these parameters.

Any affine map (21) is a composite $T = t_a \circ A$ where A is an invertible linear operator on V and $t_a : V \to V$ is the *pure translation* operator $t_a(v) = v + a$. The components A, a in (21) are uniquly determined, for if $A'v + a' = Av + a$ for all v then we have $A'v - Av = a - a'$. Taking $v = 0$ we get $a' = a$, and then $A'v = Av$ for all v, so $A' = A$ as operators on V. Within $G = \mathrm{Aff}(V)$ we find two natural subgroups

> TRANSLATIONS: $N = \{t_a : a \in V\}$. This subgroup is abelian because $t_a \circ t_{a'} = t_{a+a'}$ and since $a' \neq a \Rightarrow t_{a'} \neq t_a$, the map $j : a \mapsto t_a$ is an isomorphism between $(V, +)$ and the subgroup N in $(\mathrm{Aff}(V), \circ)$.
>
> INVERTIBLE LINEAR OPERATORS: $\mathrm{GL}(V) = \{A : \det(A) \neq 0\}$. This is the set of all invertible *linear* operators $A : V \to V$, which is obviously a subgroup in $\mathrm{Aff}(V)$.

We have just remarked that $G = N \cdot \mathrm{GL}(V)$. It is also clear that $N \cap \mathrm{GL}(V) = \{I\}$, where I is the identity operator on V. In fact, every linear operator A leaves the origin in V fixed, but a translation t_a does this only when $a = 0$ and $t_a = I$.

We claim that N is a normal subgroup in G, and hence we have a semidirect product $\mathrm{Aff}(V) = N \rtimes \mathrm{GL}(V)$. To see that $T t_a T^{-1} \in N$ for any $T \in \mathrm{Aff}(V)$ we first apply (21) to compute the inverse of any operator $Tv = Av + b$.

$$T^{-1}v = A^{-1}(v - b) = A^{-1}(v) - A^{-1}(b) \tag{23}$$

(Simply solve $w = Tv = Av + b$ for v in terms of w.) Next we compute the effect of conjugation by T on a translation t_a in the special case when $T = A$ is *linear* and $b = 0$. We get

$$A t_a A^{-1} = t_{A(a)} \qquad \text{for all } \ a \in V,\ A \in \mathrm{GL}(V) \tag{24}$$

because for every v we have

$$A t_a A^{-1}(v) = A(A^{-1}(v) + a) = AA^{-1}(v) + A(a) = v + A(a) = t_{A(a)}(v)$$

Thus, conjugating a translation t_a by a purely linear operator produces another translation as expected, but it is also useful to interpret (24) as saying

> *When we identify* $(V, +) \cong N$ *via the bijection* $j : a \mapsto t_a$*, the action of* $\mathrm{GL}(V)$ *on* N *by conjugation (which sends* $t_a \mapsto A t_a A^{-1}$*) gets identified with the usual action of the linear operator* A *on vectors in* V *(which sends* $a \mapsto A(a)$*).*

Now let T be any element in G.To see that $TNT^{-1} \subseteq N$ we write $T = t_b \circ A$ and compute the effect of conjugation; since $t_b^{-1} = t_{-b}$, equation (24) implies that

$$T t_a T^{-1} = t_b (A t_a A^{-1}) t_{-b} = t_b t_{A(a)} t_{-b} = t_{b + A(a) - b} = t_{A(a)}$$

Compare with (24): throwing in the translation component t_b has no effect because N is abelian and acts trivially on itself via conjugation. □

6.2.16 Exercise. Consider the lines of reflection symmetry of the regular hexagon shown in Figure 6.4(a). To which group elements in D_6 do the reflections r_{ℓ_1} and r_{ℓ_2} correspond? □

6.2.17 Exercise (The Degenerate case $n = 2$). When $n = 2$ the n-gon degenerates into a line segment, as shown in Figure 6.4(b). This shape has D_2 as its full symmetry group; notice that $\theta = \pi$.

(a) Identify the geometric meaning of each element e, ρ_θ, σ, $\rho_\theta \sigma$ in D_2.

(b) Verify that D_2 is *abelian.*

(c) The only groups of order 4 are $\mathbb{Z}_4$ and $\mathbb{Z}_2 \times \mathbb{Z}_2$. Which one is D_2? □

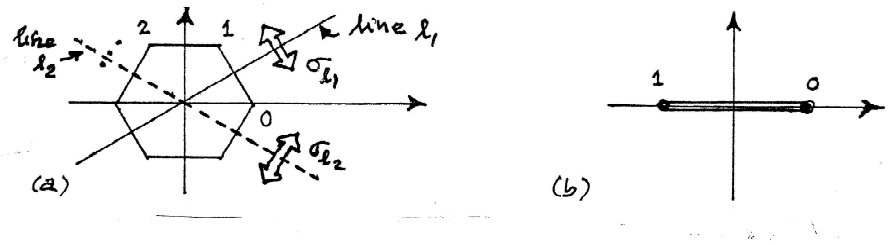

Figure 6.5. In (a) we show the reflection symmetriea σ_{ℓ_1} and σ_{ℓ_2} across lines ℓ_1, ℓ_2 passing through opposite vertices or midpoints of opposite edges of an n-gon. (b) The 2-gon degenerates to a line segment with two vertices.

6.2.18 Exercise. The *orthogonal group* $G = \mathrm{O}(n)$ is the group of matrices

$$\{A \in \mathrm{M}(n,\mathbb{R}) : A^{\mathrm{t}}A = I = AA^{\mathrm{t}}\} = \{A : A^{\mathrm{t}} = A^{-1}\}$$

The *special orthogonal group* is the subgroup $N = \mathrm{SO}(n) = \{A \in \mathrm{O}(n) : \det A = +1\}$.

(a) Verify that G and N are both groups.

(b) Prove that N is a normal subgroup in G.

(c) Prove that there are exactly two N-cosets in the quotient group G/H, and that $G/N \cong (\mathbb{Z}_2, +)$.

(d) Is G isomorphic to a *direct* product of $\mathrm{SO}(n)$ and $\mathbb{Z}_2$? Is G a *semidirect* product $\mathrm{SO}(n) \rtimes \mathbb{Z}_2$? Explain. $\square$

We close this section with a few case studies. In the first we shall complete the analysis of groups of order $|G| = 6$. We will examine more complicated groups at the end of Section 6.3 after introducing an important new tool, the *Sylow Theorems*.

6.2.19 Example (Groups of Order $|G| = 6$, Part II). By Cauchy's theorem 4.3.4 there exist cyclic subgroups H_2 and H_3 of order 2 and 3, and in 6.1.11 we showed that H_3 must be normal in G, $H_3 \cdot H_2 = G$ and $H_3 \cap H_2 = (e)$. Since $H_3 \cong \mathbb{Z}_3$ is normal and $H_2 \cong \mathbb{Z}_2$, G must be a semidirect product of $\mathbb{Z}_2$ acting on $\mathbb{Z}_3$.

Homomorphisms Φ from $H_2 \cong \mathbb{Z}_2$ into $\mathrm{Aut}(H_3) \cong \mathrm{Aut}(\mathbb{Z}_3, +)$ determine the possible actions. We have already determined the automorphisms of any finite cyclic group $G \cong \mathbb{Z}_n$. The group operation in $(\mathrm{Aut}(G), \circ)$ is composition of mappings $(\alpha \circ \beta)(x) = \alpha\big(\beta(x)\big)$, and in Theorem 3.5.3 we proved that $\mathrm{Aut}(\mathbb{Z}_n)$ is isomorphic to the group of multiplicative units $(\mathrm{U}_n, \cdot\,)$ in $\mathbb{Z}_n$ under the correspondence

$$\Phi : \mathrm{U}_n \to \mathrm{Aut}(\mathbb{Z}_n) \text{ that sends } [k] \in \mathrm{U}_n \text{ to } \phi_{[k]} = \left\{ \begin{array}{l} \text{the multiplication operator} \\ \phi_{[k]}\big([m]\big) = [k]\cdot[m] = [km] \end{array} \right.$$

This bijective correspondence is a group isomorphism because

$$\phi_{[k]\cdot[\ell]} = \phi_{[k]} \circ \phi_{[\ell]} \qquad \text{for all } [k], [\ell] \in \mathrm{U}_n$$

and $\phi_{[k]}$ is a bijection if $[k]$ is a unit in $\mathbb{Z}_n$.

In the present situation where $|G| = 6$, if a is the generator of H_2 the assigned automorphism $\Phi(a) = \phi_a$ in $\mathrm{Aut}(H_3)$ is determined by what it does to the generator b of H_3 because we have $\phi_a(b^i) = \big(\phi_a(b)\big)^i$ for all i. An automorphism cannot send an element $b \neq e$ to the identity element e, and since $H_3 = \{e, b, b^2 = b^{-1}\}$ the only places ϕ_a can send b are:

- $\phi_a(b) = b$. Then $\phi_a(b^i) = \big(\phi_a(b)\big)^i = b^i$ for all i, so that $\phi_a = I$ (the identity operator on the normal subgroup H_3). In this case $\Phi : H_2 \to \mathrm{Aut}(H_3)$ is the trivial homomorphism with $\Phi(H_2) = \{I\}$.
- $\phi_a(b) = b^2 = b^{-1}$. Then $\phi_a(b^i) = b^{-i}$ for all i and ϕ_a is the inversion automorphism $J(x) = x^{-1}$ on H_3. In this case Φ maps H_2 to the subgroup $\{\phi_e, \phi_a\} = \{I, J\}$ which must equal $\mathrm{Aut}(H_3)$ because

$$\mathrm{Aut}(\mathbb{Z}_3) \cong \mathrm{U}_3 = \{[1]_3, [2]_3\}, \text{ is a two-element group, isomorphic to } \mathbb{Z}_2\,.$$

Thus $\mathrm{Aut}(H_3) = \{I, J\}$ with $J^2 = I$.

In the following discussion we write $N = H_3, H = H_2$ and employ multiplicative notation for both groups, letting a be the generator of H with $o(a) = 2$. We have just seen that there are only two places $\Phi : H \to \mathrm{Aut}(N)$ can send the generator of $H = \langle a \rangle$.

GROUP $G^{(1)}$: Take $\Phi(a) = I$. Then all elements of H go to the identity map on N and the action of H on N is trivial. The multiplication rule for the semidirect product $G^{(1)}$ becomes the multiplication law for a *direct* product

$$\begin{aligned}(b^i, a^j) \cdot (b^k, a^\ell) &= \big(b^i \Phi(a^j)(b^k)\,,\, a^j a^\ell\big) \\ &= (b^{i+k}, a^{j+\ell})\end{aligned}$$

Thus $G^{(1)} = N \times H \cong \mathbb{Z}_3 \times \mathbb{Z}_2$, which by Chinese Remainder is $\cong \mathbb{Z}_6$.

GROUP $G^{(2)}$: Take $\Phi(a) = J$. Then $\Phi(a^k) = J^k$ for $k \in \mathbb{Z}_2$ and the multiplication law in $G^{(2)}$ is

$$(b^i, a^j) \cdot (b^k, a^\ell) = \big(b^i \cdot b^{(-1)^j k}\,,\, a^{j+\ell}\big) = \big(b^{i+(-1)^j k}\,,\, a^{j+\ell}\big) \tag{25}$$

because

$$\begin{aligned}(b^i, a^j) \cdot (b^k, a^\ell) &= \big(b^i \cdot \Phi(a^j)(b^k)\,,\, a^j \cdot a^\ell\big) \\ &= \big(b^i \cdot J^j(b^k)\,,\, a^{j+\ell}\big) = \big(b^i \cdot b^{(-1)^j k}\,,\, a^{j+\ell}\big) \\ &= (b^{i+(-1)^j k}, a^{j+\ell})\end{aligned}$$

Here $J^j(b^k) = b^{(-1)^j k}$ because each successive application of $J = \Phi(a)$ to b^k reverses the sign of the exponent.

The semidirect product in which $H \cong \mathbb{Z}_2$ acts by inversion on $N \cong \mathbb{Z}_n$ is precisely the dihedral group D_n, so $G^{(2)} \cong D_3$. This can also be seen by observing that the elements

$$\rho = (b, e) \quad \text{and} \quad \sigma = (e, a)$$

satisfy the identities

$$o(\rho) = 3 \qquad o(\sigma) = 2 \qquad \sigma\rho\sigma^{-1} = \rho^{-1}$$

characteristic of the dihedral groups because

$$\begin{aligned}\sigma\rho\sigma &= (e, a)(b, e)(e, a) = (e \cdot J(b), a \cdot e)(e, a) = (b^{-1}, a)(e, a) \\ &= (b^{-1} \cdot J(e), a \cdot a) = (b^{-1}, e) = \rho^{-1} \qquad (\text{since } a^2 = e)\end{aligned}$$

There are no other possibilities for groups of order 6. In particular since $\mathbb{Z}_3 \times \mathbb{Z}_2 \cong \mathbb{Z}_6$ by the CRT, the only *abelian* group of order 6 is $\mathbb{Z}_6$. Incidentally, we have indirectly proved that the permutation group S_3 is isomorphic to D_3 because both are noncommutative and of order 6, and up to isomorphism there is just one such group. $\square$

One can also rewrite the multiplication law for $G^{(2)} \cong D_3$ when the operations in N and H are written in additive form. Under the isomorphisms

$$\psi_1 : (\mathbb{Z}_3, +) \to N \qquad \psi_1([i]_3) = b^i \quad \text{for } [i]_3 \in \mathbb{Z}_3$$
$$\psi_2 : (\mathbb{Z}_2, +) \to H \qquad \psi_2([k]_2) = a^k \quad \text{for } [k]_2 \in \mathbb{Z}_2$$

the inversion map $J(b^i) = b^{-i}$ becomes the additive inversion map $J([i]_3) = -[i]_3$ on $\mathbb{Z}_3$. Then we can identify $G^{(2)}$ as $\mathbb{Z}_3 \times \mathbb{Z}_2$ equipped with the following multiplication law.

6.2.20 Exercise. Verify that the multiplication law in $G^{(2)} = (\mathbb{Z}_3, +) \rtimes (\mathbb{Z}_2, +)$ is given by

$$\begin{aligned} ([i],[j]) \cdot ([k],[\ell]) &= \big([i]_3 + J^j([k]_3)\,,\, [j+\ell]_2 \big) \\ &= \big([i + (-1)^j k]_3\,,\, [j+\ell]_2 \big) \quad \square \end{aligned}$$

Note the parallel between this and the multiplicative version (25). The identities in Exercise 6.2.20 are precisely those satisfied by the *exponents* in the multiplicative law (25). This correspondence is an immediate consequence of the exponent laws.

***6.2.21 Exercise.** Can you devise a bijective map $\psi : S_3 \to D_3$ that effects the isomorphism mentioned above?
Hint: What subgroups in S_3 might play the roles of $N = \{e, \rho_\theta, \rho_\theta^2\}$ and $H = \{e, \sigma\}$ in D_3? Keepin mind: N should be normal in S_3. $\square$

In any discussion of general semidirect products $N \rtimes H$ we have to address the following tasks

- Determine the elements in $\mathrm{Aut}(N)$. This can be difficult, but we already know how to do it if $N \cong \mathbb{Z}_n$ is cyclic because $\mathrm{Aut}(\mathbb{Z}_n, +) \cong (\mathrm{U}_n, \cdot\,)$, the multiplicative group of units in the ring $(\mathbb{Z}_n, +, \cdot\,)$, see 3.5.3.

- Determine all homomorphisms $\Phi : H \to \mathrm{Aut}(N)$. Here we use the fact that a homomorphism Φ is completely determined once we know where it sends the generators of H. This is particularly easy for a cyclic group $H = \langle a \rangle$.

  Not all assignments sending a to an automorphism $\phi_a \in \mathrm{Aut}(N)$ yield valid homomorphisms. If $\Phi : H \to \mathrm{Aut}(N)$ is to be a homomorphism we must have

  $$\Phi(a^k) = \big(\Phi(a)\big)^k = \phi_a^k \qquad (k \in \mathbb{Z}) \tag{26}$$

  Thus if $o(a) = n$, so $a^n = e$, the assignment $a \mapsto \phi_a$ must also satisfy the condition

  $$(\phi_a)^n = I \quad \text{(the identity map on } N)$$

  The map (26) is a well-defined homomorphism $\Leftrightarrow$ the assigned automorphism ϕ_a satisfies this "consistency condition." In turn, $(\phi_a)^n = I$ means that the order $o(\phi_a)$ as an element in $\mathrm{Aut}(N)$ must be a divisor of $n = o(a)$. No other assignments of ϕ_a are allowed

- Define a semidirect product group $G^{(\Phi)} = N \rtimes_\phi H$, letting

  $$(n,h) * (n',h') = (n \cdot \phi_h(n')\,,\, hh') \qquad \text{for all } (n,h) \in N \times H \tag{27}$$

In the previous example we ended up having to determine all homomorphisms

$$\Phi : (\mathbb{Z}_2, +) \to \mathrm{Aut}(\mathbb{Z}_3, +) \cong (\mathrm{U}_3, \cdot\,) \quad \big[\cong (\mathbb{Z}_2, +) \text{ since } |\mathrm{U}_3| = 2 \big]$$

That was easy because N and H were quite small, and both were cyclic. We will provide an explicit procedure for determining semidirect products in the (cyclic)$\rtimes$(cyclic) case.

Life gets more interesting if H has several generators, but there are some general guidelines for determining the assignments Φ : (generators) $\to \mathrm{Aut}(N)$ that yield homomorphisms $\Phi : H \to \mathrm{Aut}(N)$. We have already mentioned one constraint on such assignments:

- If $a \in H$ has order $o(a) = n$ and $\Phi(a) = \phi_a$ in $\mathrm{Aut}(N)$, the order $o(\phi_a)$ of the automorphism must be a divisor of n, so that $(\phi_a)^n = I$.

Other useful constraints on homomorphisms $\Phi : H \to \mathrm{Aut}(N)$ are forced by the Lagrange theorem.

- The order of the image group $\Phi(H)$ must divide the order of $\mathrm{Aut}(N)$.
- The order of the image group $\Phi(H)$ must also divide the order of H.

The first follows because $\Phi(H)$ is a subgroup in $\mathrm{Aut}(N)$; the second follows from Lagrange and the First Isomorphism Theorem because $\Phi(H) \cong H/\ker(\Phi)$ and

$$|H| = |\ker \Phi| \cdot |H/\ker \Phi| = |\ker \Phi| \cdot |\Phi(H)|$$

Sometimes these conditions by themselves force Φ to be trivial, with $\Phi(h) = \mathrm{id}_{_N}$ for all $h \in H$, and then the *direct* product $N \times H$ is the only possibility.

The Cyclic Case $\mathbb{Z}_n \rtimes \mathbb{Z}_m$. Since we are writing N and H in additive form it will be convenient to take the obvious additive generators for $N = \mathbb{Z}_n$ and $H = \mathbb{Z}_m$, namely $b = [1]_n$ and $a = [1]_m$.

When $N = (\mathbb{Z}_n, +)$ we know its automorphisms. As shown in 3.5.3,

$$\mathrm{Aut}(\mathbb{Z}_n, +) \text{ is isomorphic to the multiplicative group } (\mathrm{U}_n, \cdot\,) \text{ of units in } \mathbb{Z}_n$$

This isomorphism is effected by the map $\Phi : \mathrm{U}_n \to \mathrm{Aut}(\mathbb{Z}_n)$ that takes a multiplicative unit $[r]_n$ to the "multiplication operator" on $\mathbb{Z}_n$

$$\phi_{[r]_n} : [i]_n \to [r]_n[i]_n = [ri]_n \qquad \text{for } [i]_n \in \mathbb{Z}_n$$

Therefore, finding a homomorphism $\Phi : \mathbb{Z}_m \to \mathrm{Aut}(\mathbb{Z}_n)$ is equivalent to finding a homomorphism $\tilde{\Phi} : (\mathbb{Z}_m, +) \to (\mathrm{U}_n, \cdot\,)$. We work through the details below.

Notation in Semidirect Products $\mathbb{Z}_\mathbf{n} \rtimes \mathbb{Z}_\mathbf{m}$. Describing the group law in terms of the Cartesian product space $\mathbb{Z}_n \times \mathbb{Z}_m$ can be a bit confusing since integers are combined using the $(+)$ operation within $\mathbb{Z}_m$ and $\mathbb{Z}_n$; multiplied via $(\cdot)$ within the group of units U_n; and also multiplied in forming the actions $\mathrm{U}_n \times \mathbb{Z}_n \to \mathbb{Z}_n$,

$$\phi_{[r]} : [\ell] \to [r][\ell] = [r\ell] \qquad \text{for } [r] \in \mathrm{U}_n,\ [\ell] \in \mathbb{Z}_n$$

6.2.22 Proposition. *If $\Phi : (\mathbb{Z}_m, +) \to (\mathrm{U}_n, \cdot\,)$ is the homomorphism that sends the generator $a = [1]_m$ of $\mathbb{Z}_m$ to an element $b = [r]_n$ in U_n that satisfies the compatibility condition $b^m = [1]_n$, then the group operation in the semidirect product $\mathbb{Z}_n \rtimes \mathbb{Z}_m$ takes the form*

$$([i]_n, [j]_m) \cdot ([k]_n, [\ell]_m) = ([i + r^j k]_n\ ,\ [j + \ell]_m) \tag{28}$$

PROOF: Viewing $\mathbb{Z}_m$ as an additive group, the j^{th} "power" of the generator a is $j \cdot a = a + \ldots + a$, and since Φ is a homomorphism from an additive group to a multiplicative group $(\mathrm{Aut}(N), \circ)$ we get

$$\begin{aligned} \Phi\big([j]_m\big) \,=\, \Phi(j \cdot a) \;&=\; \Phi(a + \ldots + a) \\ &=\; \Phi(a) \circ \ldots \circ \Phi(a) \\ &=\; \Phi(a)^j = \big(\phi_{[r]}\big)^j = \phi_{[r]^j} = \phi_{[r^j]} \end{aligned}$$

Hence, (suppressing some subscripts m, n for clarity), we get

$$\begin{aligned}([i]_n, [j]_m) \cdot ([k]_n, [\ell]_m) &= \big([i] + \Phi(a)^j([k])\,,\, [j] + [\ell]\big) \\ &= \big([i] + \phi^j_{[r]}([k])\,,\, [j] + [\ell]\big) \\ &= ([i] + [r]^j[k]\,,\, [j + \ell]) \\ &= ([i + r^j k]_n\,,\, [j + \ell]_m)\end{aligned}$$

as claimed $\square$

We now turn to various computed examples.

6.2.23 Example. Determine the group of units $(\mathrm{U}_5, \cdot\,)$ and its isomorphism type. Then find all possible homomorphisms $\Phi : (\mathbb{Z}_3, +) \to (\mathrm{U}_5, \cdot\,)$. Describe the possible semidirect products $G = \mathbb{Z}_5 \rtimes \mathbb{Z}_3$.

Discussion: Obviously

$$\mathrm{Aut}(\mathbb{Z}_5, +) \cong \mathrm{U}_5 = \{[k] : \gcd(k, 5) = 1\} = \{[1], [2], [3], [4]\}$$

and $|\mathrm{U}_5| = 4$. There are two possibilities: $\mathrm{U}_5 \cong \mathbb{Z}_4$ or $\mathrm{U}_5 \cong \mathbb{Z}_2 \times \mathbb{Z}_2$. If we calculate the orders of a few elements in U_5 we find that $o([2]) = 4$, so $(\mathrm{U}_5, \cdot\,) \cong (\mathbb{Z}_4, +)$.

If $\Phi : \mathbb{Z}_3 \to \mathrm{U}_5$ is a homomorphism, the size $|\Phi(\mathbb{Z}_3)|$ of the image subgroup in U_5 must be a divisor of both 3 and 4. Since $\gcd(3, 4) = 1$ the range of Φ must be the trivial subgroup $\{[1]\}$ in U_5, so the only action $\mathbb{Z}_3 \times \mathbb{Z}_5 \to \mathbb{Z}_5$ by automorphisms is the trivial action. The direct product $\mathbb{Z}_5 \times \mathbb{Z}_3 \cong \mathbb{Z}_{15}$ is the only possible semidirect product. (Notice that we didn't need to know the structure of U_5 to see this!) $\square$

6.2.24 Example. Repeat the last example taking $N = \mathbb{Z}_9$ and $H = \mathbb{Z}_3$.

Discussion: Now $\mathrm{Aut}(N) = \mathrm{U}_9 = \{[1], [2], [4], [5], [7], [8]\}$ and $|\mathrm{U}_9| = 6$. Up to isomorphism there are just two groups of order $|G| = 6$, and since the group of units is abelian we see that $\mathrm{U}_9 \cong (\mathbb{Z}_6, +)$, without inspecting the orders of any elements in U_9. [In fact, $o([2]) = 6$ so $a = [2]$ is a cyclic generator of U_9.] However, it is useful to actually write down the orders $o(x)$ of elements in U_9 and the groups $\langle x \rangle$ they generate, see the Table below.

Table 6.1. Orders of elements in U_9 and the cyclic groups they generate.

x	$o(x)$	$\langle x \rangle$
[1]	1	1
[2]	6	1, 2, 4, 8, $16 \equiv 7$, $14 \equiv 5$
[4]	3	1, 4, $16 \equiv 7$
[5]	6	1, 5, $25 \equiv 7$, $35 \equiv 8$, $40 \equiv 4$, $20 \equiv 2$
[7]	3	1, 7, $49 \equiv 4$
[8]	2	1, $8 \equiv -1$

With this we can determine the possible homomorphisms $\Phi : \mathbb{Z}_3 \to \mathrm{U}_9$. Our only flexibility in defining Φ lies in specifying where Φ sends the generator $a = [1]$ of $H = \mathbb{Z}_3$. Since a has order 3 we can only send a to an element $b \in \mathrm{U}_9$ such that $b^3 = e$, and there are just three such elements: $b = [1], [4], [7]$. Each assignment yields an action of $\mathbb{Z}_3$ on $\mathbb{Z}_9$ and a semidirect product $\mathbb{Z}_9 \rtimes \mathbb{Z}_3$.

Group $G^{(1)}$: Φ sends a to $[1] \in \mathrm{U}_9$. Then $\Phi([j]_3) = \Phi(j \cdot a) = [1]^j = [1]$ for all j. The action of $\mathbb{Z}_3$ on $\mathbb{Z}_9$ is trivial and we get the *direct* product

$G^{(1)} \cong \mathbb{Z}_9 \times \mathbb{Z}_3$ (which, incidentally, is *not* $\cong \mathbb{Z}_{27}$. Why?).

GROUP $G^{(2)}$: Φ sends a to the element $[4]$ in U_9, which corresponds to the automorphism $\phi_{[4]} : [k] \to [4][k] = [4k]$ for all $[k] \in \mathbb{Z}_9$. By (28), the group law in the semidirect product is

$$([i]_9, [j]_3) \cdot ([k]_9, [\ell]_3) = ([i + 4^j k]_9\ ,\ [j + \ell]_3)$$

GROUP $G^{(3)}$: Φ sends a to the element $[7]$ in U_9, which corresponds to the automorphism $\phi_{[7]} : [k] \to [7][k] = [7k]$ for all $[k] \in \mathbb{Z}_9$. By (28), the group law in the semidirect product is

$$([i]_9, [j]_3) \cdot ([k]_9, [\ell]_3) = ([i + 7^j k]_9\ ,\ [j + \ell]_3)$$

The preceeding analysis shows that all semidirect products $\mathbb{Z}_9 \rtimes \mathbb{Z}_3$ are included in our list of groups $G^{(1)}, \ldots, G^{(3)}$; it does not, however, insure that the groups we have constructed are *distinct* up to isomorphism. Since $[7] = [4]^{-1}$ in $(\mathrm{U}_9, \cdot\,)$ there seems to be a strong symmetry between the multiplication laws in $G^{(2)}$ and $G^{(3)}$. In fact these groups ARE isomorphic, so there is *only one* nonabelian semidirect product of the form $\mathbb{Z}_9 \rtimes \mathbb{Z}_3$ $\square$

***6.2.25 Exercise.** Verify that the map $\psi : \mathbb{Z}_9 \times \mathbb{Z}_3 \to \mathbb{Z}_9 \times \mathbb{Z}_3$ given by

$$\psi([i], [j]) = ([1], [2j])$$

is an isomorphism from $G^{(3)}$ to $G^{(2)}$.
Note: ψ is obviously a bijection on the Cartesian product space $\mathbb{Z}_9 \times \mathbb{Z}_3$ because $[2]$ is a unit in $\mathbb{Z}_3$. $\square$

You might wonder how anyone ever came up with the map ψ that effects this isomorphism. Here is a clue: The products in $G^{(2)}$ and $G^{(3)}$ involve multipliers of the form 4^j and 7^j. The equation $4^x = 7$ in U_9 has $x = 2$ as a solution, and therefore $4^{2j} \equiv 7^j$ in $\mathbb{Z}_9$ for all $j \in \mathbb{Z}_3$.

***6.2.26 Exercise.** Describe all semidirect products $\mathbb{Z}_3 \rtimes \mathbb{Z}_3$ by finding all possible homomorphisms $\Phi : \mathbb{Z}_3 \to (\mathrm{U}_3, \cdot\,) \cong \mathrm{Aut}(\mathbb{Z}_3, +)$. $\square$

***6.2.27 Exercise.** Consider the automorphism group $\mathrm{Aut}(\mathbb{Z}_{20}, +) \cong (\mathrm{U}_{20}, \cdot\,)$.

(a) Determine the order of each element $x \in \mathrm{U}_{20}$ and make a chart listing all elements in the subgroup $H_x = \langle x \rangle$ it generates.

(b) By examining this chart decide whether the abelian group $(\mathrm{U}_{20}, \cdot\,)$ is isomorphic to

$$\mathbb{Z}_8 \qquad \mathbb{Z}_4 \times \mathbb{Z}_2 \qquad \text{or} \qquad \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2.$$

Why are these the only possibilities for an abelian group of order 8?

(c) Can there be any *nontrivial* homomorphisms $\Phi : (\mathbb{Z}_5, +) \to \mathrm{Aut}(\mathbb{Z}_{20}, +)$?

What does this tell you about the number of possible semidirect products of the form $\mathbb{Z}_{20} \rtimes \mathbb{Z}_5$? $\square$

***6.2.28 Exercise.** If $|G| = pq$ where $p, q > 1$ are primes and $p \neq q$, prove that G must be isomorphic to the abelian direct product $\mathbb{Z}_p \times \mathbb{Z}_q$. o
Hint: By the Cauchy theorems there exist cyclic subgroups H_p, H_q of order p, q; show that at least one of these must be normal in G.

***6.2.28 Exercise.**A Explain why the cyclic group $\mathbb{Z}_{pq}$ did not show up in Exercise 6.2.28, which purports to identify all groups of order $|G| = pq$ for primes $p \neq q$. What happens if we allow $p = q$? $\square$

The next example involves an abelian N that is not cyclic.

6.2.29 Exercise. Describe all automorphisms of the non-cyclic group $N = \mathbb{Z}_2 \times \mathbb{Z}_2$. Then describe all homomorphisms $\Phi : \mathbb{Z}_2 \to \mathrm{Aut}(N)$, and determine all possible semidirect products $N \rtimes \mathbb{Z}_2$.
Hint: $\mathrm{Aut}(N) \cong S_3$, the group of permutations of 3 objects. What 3 objects in $\mathbb{Z}_2 \times \mathbb{Z}_2$ could possibly be permuted by an automorphism of $\mathbb{Z}_2 \times \mathbb{Z}_2$? Which elements $\sigma \in S_3$ satisfy $\sigma^2 = e$? What are the corresponding automorphisms of $\mathbb{Z}_2 \times \mathbb{Z}_2$? □

6.2.30 Exercise. Make a table showing the orders $o(x)$ and generated subgroups $H_x = \langle x \rangle$ for all $x \in \mathrm{U}_{16}$.

(a) Use this to prove that $\mathrm{U}_{16} \cong \mathbb{Z}_4 \times \mathbb{Z}_2$.

(b) Explain why no two of the groups $\mathbb{Z}_8$, $\mathbb{Z}_4 \times \mathbb{Z}_2$, and $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ can be isomorphic.

(c) How many distinct semidirect products $\mathbb{Z}_{16} \rtimes \mathbb{Z}_7$. are there?

(d) How many distinct semidirect products $\mathbb{Z}_{16} \rtimes \mathbb{Z}_2$. are there? □

6.2.31 Exercise. Prove that a group of order $|G| = 35$ must be isomorphic to the direct product $\mathbb{Z}_7 \times \mathbb{Z}_5$. How do you reconcile this result with the existence of the cyclic group $\mathbb{Z}_{35}$ of order 35? □

The next two exercises on product groups will play an important role in a later discussion (Section 6.3) in which we shall describe all groups of order $|G| = 8$, a tricky case whose outcome is quite different from that when $|G| = 6$.

6.2.32 Exercise. If G is a group such that $o(x) = 2$ for all $x \neq e$, so $x^2 = e$ for all x, prove that G is abelian.
Hint: Recall the discussion of 6.1.10 where we proved that all groups of order $|G| = 4$ are abelian. □

6.2.33 Exercise. If G is a finite group such that $o(x) = 2$ for all $x \neq e$, use 6.2.32 to

(a) Prove that $|G| = 2^n$ for some $n \in \mathbb{N}$.

(b) Prove that
$$G \cong \mathbb{Z}_2 \times \ldots \times \mathbb{Z}_2 \qquad (n \text{ factors}) \quad \square$$

Group Extensions. Suppose $N \lhd G$ is a normal subgroup. Then there is a natural **exact sequence** of homomorphisms

$$e \longrightarrow N \xrightarrow{\phi_1 = \mathrm{id}} G \xrightarrow{\phi_2 = \pi} H = G/N \longrightarrow e \tag{29}$$

where $\pi : G \to G/N$ is the quotient map. Here "*exact*" means $\mathrm{range}(\phi_{i-1}) = \ker(\phi_i)$ at every step in the sequence, which is certainly true in (29) since id_N is one-to-one, π is surjective, and $\ker(\pi) = N$. The middle group G in (29) is called an **extension** of the group G/N by the group N. In some sense G is a composite of N and $H = G/N$, but additional information is needed to know how they are put together. Part of this information is obtained by noting that there is a natural group action $G \times N \to N$, given by $g \cdot n = \phi_g(n) = gng^{-1}$, which makes sense because $N \lhd G$. For each $g \in G$ the operator $\phi_g : N \to N$ is actually an *automorphism* of N, and it is easily checked that

(30) The map $\Phi : g \mapsto \phi_g$ is a homomorphism from G into the group of automorphisms $\mathrm{Aut}(N)$, so that $\phi_e = \mathrm{id}_N$, $\phi_{g_1 g_2} = \phi_{g_1} \circ \phi_{g_2}$, and $\phi_{g^{-1}} = (\phi_g)^{-1}$.

For any g the conjugation operators $\alpha_g(x) = gxg^{-1}$ are *inner* automorphism of G (recall Section 3.5). However, the restrictions $\phi_g = \alpha_g | N$ are not necessarily inner automorphisms of N because there might not be any element $b \in N$ such that conjugation by

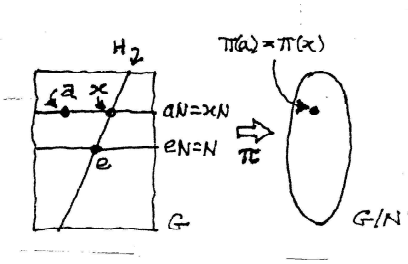

Figure 6.5. A cross-section H meets each coset in G/N in a single point, so the quotient map π restricts to an isomorphism from H to G/N, as shown.

b matches the restricted action of g on N. For instance, if N is abelian all inner automorphisms are *trivial*; but the restrictions $\phi_g = \alpha_g|N$ can be nontrivial because g lies outside of N.

Sometimes, if we are lucky, the sequence (29) *splits*: there is a subgroup $H \subseteq G$ that cross-sections the G/N cosets in the following sense. Then the action (30) is all we need to solve the problem of reassembling G from its components N and G/N: the semidirect product construction does the job.

6.2.34 Definition. *Let G be a group and N a normal subgroup, as in* (29)*. A subgroup H is a* **cross-section** *for G/N if each coset in G/N meets the set H in a single point; in particular, $H \cap N = (e)$. If such a subgroup exists we say that the sequence* (29) **splits**. *Such subgroups are generally not unique.*

The meaning of the cross-section property is shown in Figure 6.5. The idea is that

> *Every coset C in G/N has a unique representative x (i.e. $xN = C$) such that x lies in the cross-section subgroup H.*

Existence of such a representative follows because the coset C meets the set H; uniqueness follows because there is just one point in $C \cap H$. What all this means is that the quotient map $\pi : G \to G/N$ restricts to H to give a *bijective* homomorphism $\pi_{_H} : H \to G/N$, which implies that $H \cong G/N$ for any cross-section. In effect, cross-sections H are copies of the quotient group G/N embedded back inside G.

Various conditions are equivalent to existence of a cross-section. We summarize the possibilities in the next lemma.

6.2.35 Lemma. *Let G be a group, H a subgroup and N a normal subgroup. Then the following statements are equivalent*

(a) *The product set NH is equal to G and $N \cap H = (e)$*

(b) *Each $g \in G$ has a unique factorization $g = nh$ with $n \in N, h \in H$.*

(c) *H is a cross-section for G/N cosets*

These conditions are satisfied precisely when the sequence (29) *splits, and then we have $H \cong G/N$.*

REMARK: Notice that $NH = HN$ by normality of N, because every product nh can be rewritten as $nh = h(h^{-1}nh) = h'n'$. Thus each g also has a unique factorization as $g = h'n'$. To avoid notational mess later on we restrict attention to factorizations $g = nh$ in which the normal element lies on the left, even though cosets in G/N have the form

gN.

PROOF: For (c) $\Rightarrow$ (a), if H cross-sections cosets we get $H \cap N = (e)$ by looking at the coset $eN = N$. For any $x \in G$ the intersection $xN \cap H = (b)$ consists of a single point such that $xN = bN$. In particular there is some $n \in N$ such that $x = bn \in HN = NH$. Hence $G = NH$.

For (a) $\Rightarrow$ (b), every group element has *some* decomposition $g = nh$ because $G = NH$. If $g = nh = n'h'$, then $n^{-1}n' = h(h')^{-1}$ lies in $N \cap H = (e)$, so that $n = n'$ and $h = h'$. The decomposition is unique.

For (b) $\Rightarrow$ (c), unique factorization implies that $g = nh = h(h^{-1}nh) \in hN$. Hence $gN = hN$, so every coset in G/N has at least one representative in H. If we could find two representatives $h, h' \in H \cap gN$, we would then have

$$\begin{aligned} hN = gN = h'N &\Rightarrow h' = hn \text{ for some } n \in N \\ &\Rightarrow h^{-1}h' = n \in H \cap N = (e) \\ &\Rightarrow n = e \text{ and } h' = h \end{aligned}$$

Therefore each coset meets H in a single point, as required. $\square$

Obviously condition (a) means G is a semidirect product of the form $N \rtimes H$, and we can reconstruct G once we know how elements $h \in H$ act as automorphisms $\phi_h = \alpha_h|N$ on the normal subgroup N. In the next section we will see that among groups of order $|G| = 8$ there is one (the group Q_8 of *unit quaternions*) that is a *non-split* extension of $G/N \cong \mathbb{Z}_2$ by $N \cong \mathbb{Z}_4$. For non-split extensions an entirely new theory of *group cohomology* is needed to see how the subgroups N and G/N combine to reconstruct G.

Here is an example of a non-split extension. Although it involves an infinite group, it illustrates the sort of obstructions that can prevent the existence of a *subgroup* that cross-sections the N-cosets in G. The quaternion group Q_8 to be discussed in Section 6.3 is a finite group exhibiting similar behavior.

6.2.36 Example. If we take $G = \mathbb{R}$ and $N = \mathbb{Z}$, the extension $e \to \mathbb{Z} \to \mathbb{R} \to G/N \to e$ *does not* split, so G is not a semidirect product of N and H. To see why, recall that G/N is isomorphic to the circle group $S^1 = \{z \in \mathbb{C} : |z| = 1\}$. In fact (as in 3.3.3), the homomorphism $\phi : (\mathbb{R}, +) \to (S^1, \cdot)$ given by the exponential map $\phi(t) = e^{2\pi it}$ has kernel $\ker \phi = \mathbb{Z}$, and hence by the First Isomorphism Theorem 3.1.13 the map ϕ factors through the quotient map $\pi : \mathbb{R} \to \mathbb{R}/\mathbb{Z}$ to give an *isomorphism* $\tilde{\phi} : (\mathbb{R}/\mathbb{Z}, +) \to (S^1, \cdot)$ as shown in Figure 6.5 at right.

$$\begin{array}{ccc} \mathbb{R} & \xrightarrow{\phi} & (S^1, \cdot) \\ \pi \downarrow & \nearrow_{\tilde{\phi}} & \\ \mathbb{R}/\mathbb{Z} & & \end{array}$$

Figure 6.6. The induced map $\tilde{\phi}$ is an isomorphism such that $\tilde{\phi} \circ \pi = \phi$ (diagram commutes).

Arguing by contradiction, we now show that no *subgroup* H in $\mathbb{R}$ can cross-section the cosets $x + \mathbb{Z}$ in $\mathbb{R}/\mathbb{Z}$. Suppose such an H actually exists. Consider any rational value $0 < \theta < 1$. Then $m\theta \in \mathbb{Z}$ for some $m \in \mathbb{N}$, and hence $1 = \phi(m\theta) = \phi(\theta)^m$. But H is a cross-section for $\mathbb{R}/\mathbb{Z}$-cosets, so there is some $x \in H$ such that $x + \mathbb{Z} = \theta + \mathbb{Z}$. Therefore $x - \theta \in \mathbb{Z}$, $mx - m\theta \in \mathbb{Z}$, and then $\phi(mx) = \phi(m\theta) = 1$ because $\ker \phi = \mathbb{Z}$. But if H is a cross-section we also know that the restricted homomorphism $\phi_{_H} : H \to S^1$ is a *bijection*, and hence an isomorphism of groups. Since $x \in H \Rightarrow mx = x + \ldots + x \in H$, the only way to get $\phi(mx) = 1$ is to have $mx = 0$ because $\phi : H \to S^1$ is one-to-one and we already have $\phi(0) = 1$. This in turn implies that $x = 0$, which is impossible because it would imply that $\theta \equiv x \equiv 0 \pmod 1$ and hence that θ is an integer contrary to our choice of $0 < \theta < 1$. Conclusion: no *subgroup* can cross-section the cosets in $\mathbb{R}/\mathbb{Z}$. $\square$

6.3 The Sylow theorems.

A group is called a p-**group** if its order is some power p^s of a prime $p > 1$. If G is a nontrivial finite group, its order $|G| = n$ will have various prime divisors $p_i > 1$ with multiplicities $n_i \geq 1$ such that $|G| = \prod_{i=1}^{r} p_i^{n_i}$. We now show that the pattern of subgroups in G is keyed to these prime divisors and their multiplicities. The connection is revealed in the three "Sylow Theorems" presented below.

6.3.1 Definition. *Let G be a nontrivial finite group whose order has $n = \prod_{i=1}^{r} p_i^{n_i}$ as its prime factorization. A subgroup $H \subseteq G$ is a p_i-**group** if its order is some power of p_i. It is a* **Sylow** *p_i-**subgroup** if its order is as large as possible, namely $|H| = p_i^{n_i}$. For any prime $p > 1$ we write $\mathrm{Syl}_p(G)$ to indicate the collection of all Sylow p-subgroups in G. Unless p is a divisor of $|G|$ this collection will be empty; otherwise $\mathrm{Syl}_p(G)$ might contain several distinct Sylow p-subgroups for each divisor p.*

The main point of the Sylow theorems is that $\mathrm{Syl}_p(G)$ is *not* empty if p divides $|G|$, and this observation is a robust starting point if we wish to unravel the structure of a given finite group.

6.3.2 Theorem (The Sylow Theorems). *Let G be a nontrivial finite group of order $n = \prod_{i=1}^{r} p_i^{n_i}$. Then for each prime factor p_i*

(a) *G contains a subgroup S_{p_i} that has exactly $p_i^{n_i}$ elements.*

(b) *If S_{p_i} is a fixed Sylow p_i-subgroup, any subgroup H whose order is a power of p_i can be conjugated to lie within S_{p_i} – i.e. there is some $g \in G$ such that $gHg^{-1} \subseteq S_p$. In particular all Sylow p_i-subgroups are conjugates of one another.*

(c) *The number of distinct Sylow p_i-subgroups is equal to $1 + mp_i$ for some m, so their number is congruent to $1 \,(mod\ p_i)$. The number of p_i-Sylow subgroups must also be a divisor of $|G|$.*

For each prime divisor $p > 1$, all the Sylow p-subgroups are isomorphic since they are conjugates.

Proof: For (a) we start with the *abelian* case, working by induction on $n = |G|$ with $n > 1$. For $n = 2$ we have $G \cong \mathbb{Z}_2$; $p = 2$ is the only divisor and G itself is the Sylow 2-subgoup. So, we may assume $n > 2$ and $p > 1$ is one of its prime divisors, say with p^k the largest power dividing n. By Cauchy's theorem 4.3.5, G contains a cyclic subgroup $H \cong \mathbb{Z}_p$, and if the multiplicity of p as a divisor of $|G|$ is one we are done: H is a Sylow p-subgroup. Otherwise $k > 1$, p^k divides $|G|$, and $H \lhd G$ since G is assumed abelian. Thus p^{k-1} divides $|G/H|$ because $|G| = |G/H| \cdot |H| = |G/H| \cdot p$, and p^{k-1} is the largest power that can divide $|G/H|$. By the Induction Hypothesis G/H contains a Sylow p-subgroup $\overline{S}_p$ with $|\overline{S}_p| = p^{k-1}$ whose pullback S_p in G under the quotient map is the desired Sylow p-subgroup because $|S_p| = |\overline{S}_p| \cdot |H| = p^k$. That proves the abelian version of (a).

For general groups G we again use induction on $n = |G|$ to prove (a), and again the case $n = 2$ is trivial (not to mention abelian). So, assume $n > 2$ and that $p > 1$ is a prime divisor whose largest power in n is p^k. If G is nonabelian some of its conjugacy classes will be nontrivial. The class equation 4.3.1 says

$$|G| = |Z(G)| + \sum_{x \in S'} |C_x| = |Z(G)| + \sum_{x \in S'} \frac{|G|}{|Z_G(x)|}$$

where S' is a set of representatives for the nontrivial conjugacy classes C_x in G, and $Z_G(x) = \{g \in G : gx = xg\}$ is the centralizer of x (the stabilizer $\mathrm{Stab}_G(x)$ when we let G act on itself by conjugation). If there is a nontrivial class C_x such that $|Z_G(x)|$ is divisible by p^k, then p^k is also the largest power of p that can possibly divide $|Z_G(x)|$ because

$Z_G(x) \subseteq G$. Clearly $|Z_G(x)| < |G|$ if C_x is nontrivial, so by the inductive hypothesis this subgroup would already contain a Sylow p-group for G.

Otherwise the multiplicity of p in $|Z_G(x)|$ is $< k$ for *every* nontrivial class. Since $|Z_G(x)|$ is not divisible by p^k, $|C_x| = |G|/|Z_G(x)|$ must be divisible by p for every nontrivial class. By the class equation the number of elements in the center $Z(G)$ must then be divisible by p and hence $|Z(G)|$ must include a factor of the form p^s for some $1 \leq s \leq k$. If $s = k$ then p^k is the largest power of p that could possibly divide the order of $Z(G) \subseteq G$, so the Sylow p-subgroups of the abelian group $Z(G)$ have order p^k and any Sylow p-subgroup for $Z(G)$ is also a Sylow p-subgroup for G. Applying the abelian result to $Z(G)$ yields a Sylow subgroup of G in the case $s = k$.

If $s < k$ consider the quotient group G/H_p where H_p is a Sylow subgroup of the center $Z(G)$, with $|H_p| = p^s$. [Any subgroup of the center $Z(G)$ is normal in G, so the quotient *is* a group.] Induction applies to this quotient, whose order involves the prime factor p^{k-s}. Therefore the (abelian) quotient contains a Sylow p-subgroup $\overline{S}_p$ of this order. The pullback S_p in G has order p^k since we factor out a group of order p^s to get $\overline{S}_p$. This S_p is the desired Sylow p-subgroup in G and the proof of (a) is complete.

To prove (b) and (c) we use the following instructive lemma about actions $G \times X \to X$ of p-groups on finite spaces X.

6.3.3 Lemma. *Let X be a finite set acted on by p-group G. Let*

$$X^G = \mathrm{Fix}_G(X) = \{x \in X : g \cdot x = x, \ \textit{all } g \in G\}$$

be the set of G-fixed points in X. Then $|X^G| \equiv |X|$ (mod p). In particular fixed points must exist if $|X| \not\equiv 0$ (mod p).

Proof: The set X^G is obviously G-invariant and so is the difference set $X \sim X^G$, which must then be a union of disjoint nontrivial G-orbits. The cardinality $|G|/|\mathrm{Stab}_G(x)|$ of any such orbit is a divisor of $|G|$ and so must be a power p^s with $s \geq 1$. Hence $|\mathcal{O}|$ is congruent to 0 (mod p) for every nontrivial orbit $\mathcal{O}$ in X. But then the same must be true for the union $X \sim X^G$ of these orbits, which means

$$|X| = |X \sim X^G| + |X^G| \equiv |X^G| \pmod{p}$$

as claimed. □

In (b), if $|G| = p^m$ the group is already a Sylow subgroup and there is nothing to prove. Otherwise, let $n = p^k m$ with $\gcd(m, p^k) = 1$. Fix a Sylow p-group S_p and let H be a subgroup whose order is a power of p. Consider the permutation action $H \times X \to X$ on the coset space $X = G/S_p$. Then $|S_p| = p^k$ and $|X| = |G/S_p| = m \not\equiv 0$ (mod p), so by 6.3.3 there is at least one fixed point xS_p in X. But then $HxS_p = xS_p \Rightarrow x^{-1}HxS_p = S_p \Rightarrow x^{-1}Hx \subseteq S_p$ and we're done.

For (c) we fix a Sylow p-subgroup S_p and look at the group action $S_p \times X \to X$ of S_p by conjugation on the set $X = \mathrm{Syl}_p$ of *all* Sylow p-groups in G. By (b), the action of G on X by conjugation is transitive, but thye action of the smaller group $S_p \subseteq G$ yields various smaller orbits in X. The base point S_p is a fixed point for the action $S_p \times X \to X$. We claim that there are no other, one-point orbits and then (c) follows because

$$|X| = \#(p\text{-Sylow}) = 1 + (\text{a multiple of } p)$$

by Lemma 6.3.3.

In fact, if If there were another fixed point $H \in X$ this subgroup would be normalized by S_p in the sense that $gHg^{-1} = H$ for $g \in S_p$. Thus S_p is contained in the *normalizer* of H: the subgroup $N = N_G(H) = \{g \in G : gHg^{-1} = H\}$. Hence S_p and H are Sylow p-subgroups of N, and by (b) there exists some $n \in N$ such that $S_p = nHn^{-1}$. By definition of N this makes $S_p = H$, so S_p is the only fixed point in X as claimed.

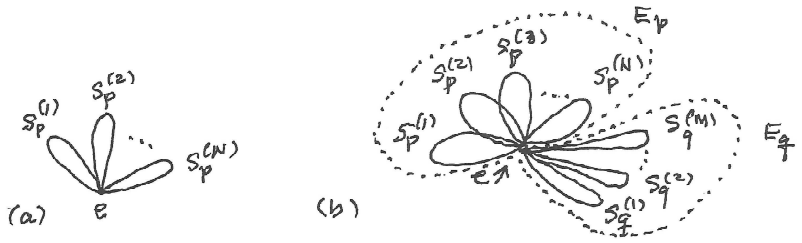

Figure 6.7. If prime divisor p of $|G|$ has multiplicity 1, the Sylow p-subgroups $S_p^{(1)}, \ldots, S_p^{(N)}$ are "essentially disjoint" as indicated in (a), so their union has cardinality $|E_p| = N(p-1)+1$. If p, q are different prime divisors, the unions E_p, E_q of the corresponding Sylow subgroups are essentially disjoint, as in (b), *even if p and q have multiplicities greater than* 1 (in which case the individual $S_p^{(i)}$ might have nontrivial overlap). Thus $|E_p \cup E_q| = |E_p| + |E_q| - 1$.

Finally, let P be any base point in $\mathrm{Syl}_p(G)$. By (b) the action $G \times \mathrm{Syl}_p \to \mathrm{Syl}_p$ is transitive so $|\mathrm{Syl}_p| = |G|/|\mathrm{Stab}_G(P)|$ and $|G|$ is a multiple of $|\mathrm{Syl}_p|$, as claimed. □

In 4.3.5 (Cauchy theorem) we proved that if p is a divisor of $n = |G|$ then there are elements in G such that $o(x) = p$. If p^k is the largest power dividing n, one can generalize the Sylow theorems to prove that there exist subgroups of order p^r for every $1 \le r \le k$.

Note: In analyzing the structure of groups, special interest attaches to the p-groups, for which $|G| = p^k$, so it is worth noting that

A finite group G is a p-group $\Leftrightarrow$ the order of each element is a power of p.

Implication ($\Rightarrow$) is trivial (Lagrange). For the converse ($\Leftarrow$), if some prime $q \neq p$ appeared in the prime decomposition of $|G|$, then by 4.3.5 there would be a cyclic subgroup of order q, which is impossible. □

By 6.3.2(b), a Sylow p-subgroup is normal in G if and only if there is just one such subgroup. Sometimes we can determine when this happens using 6.3.2(c), and in any case a lot can be learned about the pattern of Sylow subgroups by looking at intersections of conjugates $S_p \cap gS_pg^{-1}$ with Lagrange and the Sylow theorems in mind. For instance, suppose p has multiplicity 1 in the prime factorization of $n = |G|$. Then the distinct Sylow p-subgroups $S_p^{(1)}, \ldots, S_p^{(N)}$ all have order p and by Lagrange their pairwise intersections are trivial. Hence their union has cardinality $N(p-1)+1$, which cannot exceed $|G|$. This and the requirement that $N \equiv 1 \pmod{p}$ can put serious constraints on the $S_p^{(i)}$. The idea is shown in Figure 6.6(a).

Another useful counting principle concerns the unions $E_p = \bigcup_{i=1}^{N} S_p^{(i)}$ and $E_q = \bigcup_{j=1}^{M} S_q^{(j)}$ of all the p-Sylow and q-Sylow subgroups in G, where p, q are distinct prime divisors of $|G|$. The subgroups in E_p, E_q have orders $|S_p^{(i)}| = p^k$ and $|S_q^{(j)}| = q^\ell$ where $k, \ell \in \mathbb{N}$. Hence $\gcd(p^k, q^\ell) = 1$, which implies that $S_p^{(i)} \cap S_q^{(j)} = (e)$ for all i, j. That forces the "blobs" E_p and E_q to be *essentially disjoint* in the sense that $E_p \cap E_q = (e)$, because any $x \in E_p \cap E_q$ would lie in the intersection of a p-Sylow and a q-Sylow subgroup. Obviously the union of these blobs must fit inside G, so that $|E_p \cup E_q| = |E_p| + |E_q| - 1 \le |G|$, see Figure 6.7(b). (There must also be room outside $E_p \cup E_q$

for Sylow subgroups associated with *other* prime divisors of n.) These constraints also provide useful information about the pattern of Sylow subgroups in G.

6.3.4 Example (Groups of Order 28). Let G be an arbitrary group of order $|G| = 28 = 7 \cdot 2^2$. If H_7 is a 7-Sylow subgroup then $|H_7| = 7$ and $N = \#(\text{7-Sylow subgroups})$ can only equal 1, 8, 15, 22 ($\leq |G| = 28$). In fact $N = 1$ because other values do not divide $|G| = 28$. Thus the 7-Sylow subgroup $H_7 \cong (\mathbb{Z}_7, +)$ is normal in G and there is just one such subgroup.

The 2-Sylow subgroups H_2 all have order $|H_2| = 2^2 = 4$. As shown in Section 6.2, all groups of order 4 are abelian and isomorphic to $\mathbb{Z}_4$ (cyclic) or $\mathbb{Z}_2 \times \mathbb{Z}_2$. The number of 2-Sylow subgroups can only be $N = 1, 3, 5, 7, ...$; only 1 and 7 are divisors of $|G| = 28$, so $\#(\text{2-Sylow subgroups})$ is either 1 or 7. Fix a 2-Sylow subgroup H_2. Then $H_2 \cap H_7 = (e)$ since $\gcd(4, 7) = 1$; it follows that $|H_7 \cdot H_2| = 28$ and $G = H_7 H_2$. Thus G is a semidirect product $H_7 \rtimes H_2 = \mathbb{Z}_7 \rtimes H_2$.

Case 1: $H_2 \cong \mathbb{Z}_4$. Identifying $H_2 = (\mathbb{Z}_4, +)$, consider the standard generator $a = [1]_4$ of $\mathbb{Z}_4$. We must determine all homomorphisms $\Phi : \mathbb{Z}_4 \to (\mathrm{U}_7, \cdot) \cong \mathrm{Aut}(\mathbb{Z}_7, +)$. Since $\mathrm{U}_7 = \{[1], [2], [3], \ldots, [6]\}$ is abelian and $|\mathrm{U}_7| = 6$ it follows from 6.2.19 that $\mathrm{U}_7 \cong (\mathbb{Z}_6, +)$. We won't need this specific information below, but what we do need is a list of the orders of the elements in U_7, and the groups $\langle x \rangle$ they generate, so we can decide which elements $b \in \mathrm{U}_7$ may be assigned as images $\Phi(a)$ of the generator of H_2. The orders are listed in the table at right. Since $4 \cdot a = [0]$ in $\mathbb{Z}_4 \Rightarrow \Phi(a)^4 = [1]$ in U_7 we musts have $o(\Phi(a)) = 1, 2$, or 4. The only valid assignments are $\Phi(a) = [1]$ or $[6] = [-1]$, which correspond to multiplication operators $\phi_{[1]}$ (identity map) and $\phi_{[-1]}$ (inversion) on $\mathbb{Z}_7$.

x	**o(x)**	**Subgroup** $\langle x \rangle$
[1]	$\boxed{1}$	1
[2]	3	1, 2, 4
[3]	6	all of U_7
[4]	3	1, 4, 2
[5]	6	all of U_7
[6]	$\boxed{2}$	$1, 6 \equiv -1$

Data Table for U_7. Orders that are divisors of 4 are "boxed."

Case 1A: $\Phi(a) = \phi_{[1]} = \mathrm{id}_{\mathbb{Z}_7}$. This yields the trivial action of $H_2 = \mathbb{Z}_4$ on $N = \mathbb{Z}_7$; the corresponding group is the direct product $G^{(1)} = \mathbb{Z}_7 \times \mathbb{Z}_4 \cong \mathbb{Z}_{28}$.

Case 1B: $\Phi(a) = \phi_{[-1]} = J$ (the inversion automorphism on $\mathbb{Z}_7$). The automorphisms corresponding to the various elements in $\mathbb{Z}_4 = \{j \cdot a : 0 \leq j < 4\}$ are $\Phi(j \cdot a) = \Phi(a)^j = J^j$, so that

$$\Phi([0]_4) = I \qquad \Phi([1]_4) = J \qquad \Phi([2]_4) = J^2 = I \qquad \Phi([3]_4) = J^3 = J$$

In Proposition 6.2.22 we showed that the multiplication law in the resulting semidirect product $G^{(2)} = H_7 \rtimes H_2 \cong \mathbb{Z}_7 \rtimes \mathbb{Z}_4$ takes the form

$$([i]_7, [j]_4) \cdot ([k]_7, [\ell]_4) = ([i + (-1)^j k]_7\,,\, [j + \ell]_4) \tag{31}$$

6.3.5 Exercise (Multiplicative Version of (31)). Suppose we specify generators a, u and write H_2 and H_7 in multiplicative notation, so that $H_2 = \{e, a, a^2, a^3\}$ and $H_7 = \{e, u, u^2, \ldots, u^6\}$. Prove that the multiplication law in $G^{(2)} = H_7 \rtimes H_2$ then takes the form

$$\begin{aligned} (u^i, a^j) \star (u^k, a^\ell) &= \left(u^i \Phi(a)^j(u^k)\,,\, a^{j+\ell}\right) \\ &= \left(u^{i+(-1)^j k}, a^{j+\ell}\right) \end{aligned} \tag{32}$$

in which the *exponents* $i, k \in \mathbb{Z}_7$ and $j, \ell \in \mathbb{Z}_4$ satisfy (31).
Note: In multiplicative notation, $\Phi(a) = \phi_a$ is the operator that maps u^j to u^{-j} for all

$0 \le j < 7$. Furthermore, $\Phi(a^i) = \Phi(a)^i$. $\square$

CASE 2: $H_2 = \mathbb{Z}_2 \times \mathbb{Z}_2$. The analysis is complicated by the fact that the acting group is not cyclic. It will be convenient to write H_2 multiplicatively, as $H_2 = \{e, u, v, w\}$ where

$$u^2 = v^2 = w^2 = e \quad \text{and} \quad uv = w,\ vw = u,\ wu = v$$

Obviously H_2 is the internal direct product of the two subgroups $\langle u \rangle \cong \langle v \rangle \cong \mathbb{Z}_2$. Consequently each element $g \in H_2$ has a unique factorization in the form $g = u^i v^j$ with $i, j \in \mathbb{Z}_2$. As always, a homomorphism $\Phi : H_2 \to (\mathrm{U}_7, \cdot\,)$ is determined by where it sends the generators u, v. Furthermore $K = \Phi(H_2)$ can only have cardinality that divides both $|\mathrm{Aut}(N)| = |\mathrm{U}_7| = 6$ and $|H_2| = 4$, so $|K| = 1$ or 2.

CASE 2A: $|K| = 1$. Then H_2 acts trivially on H_7 and we have a direct product $G^{(3)} = \mathbb{Z}_7 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ (which is $\cong \mathbb{Z}_{14} \times \mathbb{Z}_2$ by Chinese Remainder theorem).

CASE 2B: $|K| = 2$. Then $|\ker \Phi| = |H_2|/|K| = 2$, so any such Φ must "kill" e and exactly one other element (sending both to [1] in U_7). By relabeling the points u, v in H_2 we may assume $K = \{e, u\}$; then since $w = uv$ we get $\Phi(u) = I$ and

$$\Phi(w) = \Phi(u)\Phi(v) = \Phi(v) \qquad \text{with} \qquad \Phi(v) \neq [1] \text{ in } \mathrm{U}_7$$

Since $v^2 = e$ the image $\Phi(v)$ can only be an element x in U_7 such that $x^2 = [1]$, and since $\Phi(v) \neq [1]$ the only choice is $\Phi(v) = [6] = [-1]$. This corresponds to the inversion automorphism $J = \phi_{[-1]}$ on $\mathbb{Z}_7$, so in this case Φ is fully determined:

$$\Phi(e) = \Phi(u) = I \qquad \Phi(v) = \Phi(w) = J$$

Let us label the resulting semidirect product as $G^{(4)}$.

Writing both $H_2 = \{u^i v^j : i, j \in \mathbb{Z}_2\}$ and $H_7 = \langle a \rangle$ in multiplicative form, the multiplication law in $G^{(4)} = H_7 \rtimes H_2 = \mathbb{Z}_7 \rtimes (\mathbb{Z}_2 \times \mathbb{Z}_2)$ becomes

$$\begin{aligned}
(a^k, u^i v^j) \star (a^\ell, u^r v^s) &= (a^k \Phi(u^i v^j)(a^\ell)\,,\ u^{i+r} v^{j+s}) \\
&= (a^k \Phi(u)^i \Phi(v)^j (a^\ell)\,,\ u^{i+r} v^{j+s}) \\
&= (a^k \Phi(v)^j (a^\ell)\,,\ u^{i+r} v^{j+s}) \qquad (\text{since } \Phi(u) = I) \\
&= (a^{k+(-1)^j \ell}\,,\ u^{i+r} v^{j+s})
\end{aligned} \tag{33}$$

for $k, \ell \in \mathbb{Z}_7$ and $i, j, r, s \in \mathbb{Z}_2$. $\square$

It would seem that we have produced four distinct groups such that $|G| = 28$, but appearances sometimes deceive. How do we know there isn't some "accidental" isomorphism $G^{(i)} \cong G^{(j)}$ despite the differences in the way the groups are constructed? The answer is: Without further investigation, we don't! Obviously $\mathbb{Z}_{28} \ncong \mathbb{Z}_{14} \times \mathbb{Z}_2$ (why?), and an abelian group can't be isomorphic to a nonabelian group, so the only interesting possibility is that $G^{(2)} \cong G^{(4)}$. To disprove this we might compare various structural properties of the two groups – e.g. highest orders of elements, the sizes and isomorphism types of the centers, the number and size of the conjugacy classes, etc – all of which can be computed once the group law on the Cartesian product set $H_7 \times H_2$ is in hand. In fact (see below) $G^{(2)}$ and $G^{(4)}$ are *not* isomorphic.

There also seems to be a "missing" group of order 28, namely the dihedral group D_{14}. Where does it appear in the list $G^{(1)}, \ldots, G^{(4)}$?

A look at the way $G^{(4)}$ was constructed shows that the element $u \in H_2 \subseteq G^{(4)}$ acts trivially on the normal subgroup H_7. This action is just conjugation by u, $\phi_u(n) = unu^{-1}$ restricted to elements $n \in H_7$, so u commutes with all $n \in H_7$. Since u also commutes with everyone in the abelian subgroup H_2 it follows that u commutes with

all $g \in G^{(4)} = H_7H_2$. Thus the cyclic subgroup $U = \langle u \rangle \cong \mathbb{Z}_2$ is in the center of $G^{(4)}$. Obviously $U \cap H_7 = (e)$, so the product set $M = U \cdot H_7$ is a normal subgroup of order 14 in $G^{(4)}$, and is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_7 \cong \mathbb{Z}_{14}$. On the other hand, every element of $G^{(4)}$ has a unique factorization $g = xy$ with $x \in H_7, y \in H_2$. From this it follows easily that the element $v \in H_2$ lies outside of M, and since $o(v) = 2$ the subgroup $V = \langle v \rangle \cong \mathbb{Z}_2$ has the properties $V \cap M = (e),\ MV = G^{(4)},\ M \lhd G^{(4)}$. This allows us to recognize $G^{(4)}$ as a semidirect product $M \rtimes V \cong \mathbb{Z}_{14} \rtimes \mathbb{Z}_2$.

In fact, $G^{(4)}$ is the missing dihedral group. The possible semidirect products $\mathbb{Z}_{14} \rtimes \mathbb{Z}_2$ correspond to homomorphisms $\Phi : \mathbb{Z}_2 \to \mathrm{U}_{14} \cong \mathrm{Aut}(\mathbb{Z}_{14}, +)$. But the group of units $\mathrm{U}_{14} = \{[1], [3], [5], [9], [11], [13]\}$ is abelian and has order 6, hence $\mathrm{U}_{14} \cong \mathbb{Z}_6$; only the elements $x = [1]$ and $x = [13] = [-1]$ in U_{14} satisfy the compatibility condition $x^2 = \Phi(a)^2 = [1]$, so the only possible assignments of the generator $v \in V \cong \mathbb{Z}_2$ to elements in $\mathrm{Aut}(\mathbb{Z}_{14}) \cong \mathrm{U}_{14}$ are

$$\begin{aligned} \Phi(v) &= \phi_{[1]} = \mathrm{id}_M \\ \Phi(v) &= \phi_{[-1]} = J \quad \text{(inversion automorphism on } M = \mathbb{Z}_{14}) \end{aligned}$$

The first would make $G^{(4)}$ an abelian direct product $\mathbb{Z}_{14} \times \mathbb{Z}_2$ already accounted for; the second choice yields the dihedral group $G^{(4)} \cong D_{14}$, as it was originally defined.

Is $G^{(2)} \cong G^{(4)}$? This cannot be decided by comparing the centers because $|Z(G)| = 2$ in both cases. However, consider the possible orders of elements in these groups. $G^{(2)}$ contains an element $g = a$ of order $o(g) = 4$, but there is no such element in $G^{(4)} \cong D_{14}$. In fact, writing elements in D_{14} as $\rho_\theta^i \sigma^j$ we know that elements in $\langle \rho_\theta \rangle \cong \mathbb{Z}_{14}$ cannot have order 4 because 4 is not a divisor of 14. But elements of the form $\rho_\theta^k \sigma$ are reflections and have order 2 because

$$(\rho_\theta^k \sigma) \cdot (\rho_\theta^k \sigma) = \rho_\theta^k (\sigma \rho_\theta^k \sigma) = \rho_\theta^k \cdot \rho_\theta^{-k} = e$$

Therefore the two groups can't be isomorphic. □

6.3.5A Exercise. Write u, a for the generators of $H_7 \cong \mathbb{Z}_7$ and $H_2 \cong \mathbb{Z}_4$ and write the multiplication law in multiplicative form, as in (32). Elements of $G^{(2)} = H_7 \rtimes H_2$ have unique factorizations $u^i a^j$ where $i \in \mathbb{Z}_7, j \in \mathbb{Z}_4$.

(a) Verify that conjugation of $g = u^k a^\ell$ by $x = u^i a^j$ takes the form

$$xgx^{-1} = (u^i a^j)(u^k a^\ell)(a^{-j} u^{-i}) = u^{\{\, i[1-(-1)^\ell] + k(-1)^j \,\}}$$

for all $i \in \mathbb{Z}_7, j \in \mathbb{Z}_4$

(b) Prove that $xgx^{-1} = g$ for all x if and only if $[k]_7 = 0$ in $\mathbb{Z}_7$ and $\ell = [0]_4$ or $\ell = [2]_4$ in $\mathbb{Z}_4$, so that $Z(G^{(2)}) = \{e, a^2\}$ has order 2. □

6.3.5B Exercise. Show that, up to isomorphism, $G = (\mathbb{Z}_{15}, +)$ is the only group of order $|G| = 15$.
Hints: First show G is abelian by examining the pattern of p-Sylow subgroups. Then show G is isomorphic to the direct product $\mathbb{Z}_5 \times \mathbb{Z}_3$. □

6.3.5C Exercise. Discuss the number and nature of the 3-Sylow and 5-Sylow subgroups of a group whose order is $|G| = 225 = 3^2 \cdot 5^2$. □

6.3.5D Exercise. If $|G| = 30$ use the Sylow theorems to prove that the 3-Sylow and 5-Sylow subgroups are both normal in G, and that G is a semidirect product $G \cong \mathbb{Z}_{15} \rtimes \mathbb{Z}_2$.
Hints: Recall 6.3.5B above. □

6.3.5E Exercise. If a group has order $|G| = 231 = 11 \cdot 7 \cdot 3$, prove that the 11-Sylow subgroup is normal and must lie in the *center* of G. □

6.3.5F Exercise. Consider the automorphism group $G = \mathrm{Aut}(\mathbb{Z}_{25}, +) \cong (\mathrm{U}_{25}, \cdot)$

(a) What is the order of G? Is it cyclic? What are the orders of its Sylow subgroups?

(b) What are the distinct isomorphism types of the Sylow subgroups in G and how many distinct subgroups of each type are there?

(c) Exhibit an explicit subgroup in G of each Sylow type. (List the elements in U_{25} that belong to it.)

Notes: U_{25} is abelian. You might want to determine a few subgroups $H_a = \langle a \rangle$ generated by elements $a \in \mathrm{U}_{25}$, but you won't have to do this for all 20 elements in order to answer these questions. □

6.3.5G Exercise. If a group G has order p^2q where p, q are primes, prove that G must have a *proper* normal subgroup, and hence cannot be simple group. □

Abelian Groups and the Sylow Theorems. If G is a finite *abelian* group the Sylow theorems provide an explicit and natural direct product decomposition. This is not the final answer if we want to know the detailed structure of a finite abelian group, but it is a big step in that direction. The proof uses the fact that in an abelian group all Sylow p-subgroups are automatically normal, and hence by Theorem 6.3.1(b) there is *just one* Sylow p-subgroup for each prime divisor of the order when G is nontrivial.

6.3.6 Theorem. *A finite* ABELIAN *group is isomorphic to a direct product* $S_{p_1} \times \ldots \times S_{p_r}$ *where* $n = \prod_{i=1}^{r} p_i^{n_i}$ *is the prime decomposition of the order* $n = |G|$ *and* S_{p_i} *is the unique Sylow* p_i*-subgroup in* G *of order* $p_i^{n_i}$*. This direct product decomposition is canonical: the subgroups* S_{p_i} *are uniquely determined, as are the primes* p_i *and their exponents* n_i*.*

NOTE: The components S_{p_i} *need not* be cyclic groups (which would make them $\cong \mathbb{Z}_{p_i^{n_i}}$). For instance, if $p = 2$ we might have $S_2 = \mathbb{Z}_2 \times \mathbb{Z}_4$ or $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ which cannot be isomorphic to the cyclic group $\mathbb{Z}_8$ of the same size. (Why?) Determining the fine structure of the components S_{p_i} would require further effort, leading to the *Fundamental Structure Theorem* for finitely generated abelian groups. The coarse decomposition 6.3.6 is the first step in that direction. □

PROOF: Let's write S_i for the unique Sylow p_i-subgroup. For each index $1 \le i \le r$ the product set $H_i = \prod_{j=1}^{i} S_j$ is a normal subgroup (G being abelian). We now apply Lagrange's theorem and the counting principle 3.4.7 to show by induction that its order is $|H_i| = \prod_{j=1}^{i} p_j^{n_j}$ for each $i = 1, 2 \ldots$ Obviously $|H_1| = |S_1| = p_1^{n_1}$. When $i = 2$ the order of the subgroup $H_1 \cap S_2 = S_1 \cap S_2$ must divide both $p_1^{n_1}$ and $p_2^{n_2}$, and hence this intersection is trivial; it follows immediately from 3.4.7 that $H_2 = H_1 S_1$ has cardinality

$$|H_1| \cdot |S_2| / |H_1 \cap S_2| = p_1^{n_1} p_2^{n_2}$$

At the next stage we have $H_3 = H_2 S_3$ and $H_2 \cap S_3$ is again trivial because these subgroups have different prime divisors; applying 3.4.7 we get $|H_3| = |H_2| \cdot |S_3| = p_1^{n_1} p_2^{n_2} p_3^{n_3}$. Continuing inductively we prove our claim.

This already implies that G is a direct product. In fact, since $|G| = |H_r|$ we see that G is equal to the product set $S_1 S_2 \ldots S_r$. It remains only to check uniqueness of the factorization: if $a_1 a_2 \ldots a_r = e$ with $a_i \in S_i$, then each $a_i = e$. Multiplying on the right by a_r^{-1} we get

$$a_r^{-1} = a_1 \ldots a_{r-1}$$

with $a_r^{-1} \in S_r$ and the right hand product in H_{r-1}. Since $S_r \cap H_{r-1} = (e)$ we have $a_r = e$ and $a_1 \ldots a_{r-1} = e$. By similar reasoning we get $a_{r-1} = e$, etc. Thus every element in G has a unique decomposition of the form $a_1 a_2 \ldots a_r$ and G is the internal direct product of its Sylow subgroups. □

Essentially, this result says that to understand the structure of any finite abelian group it

suffices to analyze the abelian p-groups – those with just one prime divisor and $|G| = p^k$ for some $k > 0$.

More on Non-Abelian G. In order for the Sylow subgroups to be useful indicators of the overall structure for noncommutative G they should be *pervasive* in G. Here's what that means.

6.3.7 Lemma. *Let G be a nontrivial finite group and let S be the subgroup generated by all the Sylow subgroups in G:*

$$S = \left\langle \bigcup \{H : H \in \mathrm{Syl}_{p_i}(G), 1 \le i \le r\} \right\rangle$$

where the $p_i > 1$ are the prime divisors of $|G|$. Then S is all of G.

PROOF: The result has already been established in 6.3.6 when G is abelian. We argue by induction on $n = |G|$. The result is trivial when $n = 2$ and $G = \mathbb{Z}_2$, so we may assume that $n > 2$ and that the theorem is true for all groups of order at most $n - 1$.

If $S \neq G$, there exist elements $a \notin S$. The cyclic subgroup $M = \langle a \rangle$ must have order $|M| = m$ that divides $|G| = n$, which means that only the p_i can appear in the prime factorization of m. Let p be one of those primes. Any Sylow p-subgroup for M will have order p^s for some $s \le n_i$ (if $p = p_i$). By Theorem 6.3.1(a-b), every such subgroup must be contained in one of the Sylow p-subgroups for G. Therefore the product of the Sylow subgroups in M is contained in S. But by definition M is abelian and hence (by 6.3.6) is the product of its Sylow subgroups, which means $a \in M \subseteq S$. That is impossible since we are assuming a lies outside S. Conclusion: we actually have $G = S$, as claimed. □

A Case Study: The Groups of Order 12. The following analysis of the groups of order 12 will draw upon almost everything discussed so far.

6.3.8 Example (Groups of Order 12). Classify all groups of order $|G| = 12$ up to isomorphism. Identify all semidirect products in this family. Are they all direct or semidirect products of smaller groups?

DISCUSSION: There are Sylow subgroups H_p for the prime divisors $p = 2, 3$, with $|H_2| = 4$ and $|H_3| = 3$; thus $H_3 \cong \mathbb{Z}_3$ while H_2 could be either $\mathbb{Z}_4$ or $\mathbb{Z}_2 \times \mathbb{Z}_2$ (abelian). We obviously have $H_2 \cap H_3 = (e)$ and $|H_2 \cdot H_3| = 4 \cdot 3/|H_2 \cap H_3| = 12$, so that $H_2H_3 = G$. Now let E_p be the union of all conjugates of H_p. Then $E_2 \cap E_3 = (e)$ because all intersections $H_p \cap H_q$ are trivial when $p \neq q$. (Recall Figure 6.6 and the discussion preceding Example 6.3.4.)

By the Sylow theorems we have

$$\#(\text{Sylow 2-subgroups}) = 1 \text{ (if } H_2 \lhd G\text{), and } = 3 \text{ otherwise}$$
$$\#(\text{Sylow 3-subgroups}) = 1 \text{ (if } H_3 \lhd G\text{), and } = 4 \text{ otherwise}$$

If H_3 is *not* normal the union of its conjugates has cardinality $|E_3| = 4(3 - 1) + 1 = 9$ because distinct conjugates of H_3 intersect only at the identity. In this situation, the other Sylow subgroup H_2 must be normal, otherwise the union E_2 would involve at least 3 distinct copies of H_2. Since $|H_2^{(i)} \cap H_2^{(j)}| \le 2$ whether $H_2 \cong \mathbb{Z}_4$ or $\mathbb{Z}_2 \times \mathbb{Z}_2$, the set $E_2 \sim \{e\}$ would contain at least 4 points and $E_2 \cup E_3$ would contain more than 12 points. We conclude that

At least one of the subgroups H_2, H_3 must be normal in G

and hence every G of order 12 can be realized as a semidirect product. We will employ the Chinese Remainder Theorem 6.1.26 in our analysis of these products.

CASE 1: BOTH H_2, H_3 NORMAL. Then G is the abelian direct product $H_2 \times H_3$. The possible distinct isomorphism types are

GROUP $G^{(1)}$: $\mathbb{Z}_3 \times \mathbb{Z}_4 \cong \mathbb{Z}_{12}$ (by Chinese Remainder)

GROUP $G^{(2)}$: $\mathbb{Z}_3 \times (\mathbb{Z}_2 \times \mathbb{Z}_2) \cong \mathbb{Z}_6 \times \mathbb{Z}_2$ not $\cong \mathbb{Z}_{12}$. (Why?)

CASE 2: ONLY H_3 IS NORMAL. Then G is a semidirect product $\mathbb{Z}_3 \rtimes \mathbb{Z}_4$ or $\mathbb{Z}_3 \rtimes (\mathbb{Z}_2 \times \mathbb{Z}_2)$.

CASE 2A: If $H_2 = \mathbb{Z}_4$, let us write both H_2 and $H_3 \cong \mathbb{Z}_3$ in additive notation. Then G is determined by some homomorphism

$$\Phi : \mathbb{Z}_4 \to \mathrm{Aut}(\mathbb{Z}_3, +) \cong (\mathrm{U}_3, \cdot\,) \quad \big[\, \cong (\mathbb{Z}_2 +) \text{ since } |\mathrm{U}_3| = 2 \,\big]$$

The only possible assignments for the additive cyclic generator $a = [1]_4$ in $\mathbb{Z}_4$ are $\Phi(a) =$ id (in which case G is one of the abelian groups already listed), or $\Phi(a)$ is the inversion map $J([k]) = -[k]$, $[k] \in \mathbb{Z}_3$. Then we we get a new group of order 12.

GROUP $G^{(3)}$. This group is the the semidirect product $\mathbb{Z}_3 \rtimes \mathbb{Z}_4$ whose multiplication operation has been described in (28) of proposition 6.2.20:

$$\begin{aligned} ([i]_3, [j]_4) \star ([k]_3, [\ell]_4) &= \big([i] + \Phi(a)^j([k]) \,,\, [j] + [\ell] \big) \\ &= \big([i + (-1)^j k]_3 \,,\, [j + \ell]_4 \big) \end{aligned} \tag{34}$$

for all $[i], [k] \in \mathbb{Z}_3$ and $[j], [\ell] \in \mathbb{Z}_4$.

Note that $\Phi(e)$ and $\Phi(2 \cdot a) = \Phi(a)^2$ are equal to I and $\Phi(a), \Phi(3 \cdot a) = \Phi(a)^3$ are both equal to J.

6.3.9 Exercise. In terms of generators and relations, $G^{(3)}$ is generated by elements x, y which satisfy the relations

$$x^3 = e \qquad y^4 = e \qquad yx = x^2 y \;\; (\text{or } yxy^{-1} = x^{-1})$$

Verify this claim. Which elements in $\mathbb{Z}_3 \rtimes \mathbb{Z}_4$ should be identified with x and y? □

CASE 2B: If $H_2 = \mathbb{Z}_2 \times \mathbb{Z}_2$ let's write both H_2 and H_3 in multiplicative form

$$\begin{aligned} H_2 &= \{u^i v^j : i, j \in \mathbb{Z}_2\} = \{e, u, v, uv\} \qquad \text{with } u^2 = v^2 = (uv)^2 = e \\ H_3 &= \{e, a, a^2\} \qquad \text{with } a^3 = e \end{aligned}$$

as in 6.3.4. Since $\mathrm{Aut}(H_3) \cong \mathrm{Aut}(\mathbb{Z}_3, +) \cong (\mathrm{U}_3, \cdot\,) \cong (\mathbb{Z}_2, +)$, any *nontrivial* homomorphism $\Phi : H_2 \to \mathrm{Aut}(H_3)$ will have a kernel $\ker(\Phi)$ of index 2 in H_2. By changing our labeling of elements u, v in H_2 if necessary, we may assume that Φ is the map

$$\Phi(e) = \Phi(u) = I \qquad \Phi(v) = \Phi(uv) = J \text{ (Inversion map } J : a^i \to a^{-i} \text{ on } H_3)$$

with $\langle u \rangle$ acting trivially on H_3. The multiplication law for the resulting semidirect product $G^{(4)} = H_3 \rtimes H_2$ then takes the form

$$\begin{aligned} (a^k, u^i v^j) \star (a^\ell, u^r v^s) &= (a^k \Phi(u^i v^j)(a^\ell) \,,\, u^{i+r} v^{j+s}) \\ &= (a^k J^j(a^\ell) \,,\, u^{i+r} v^{j+s}) \\ &= (a^{k + (-1)^j \ell} \,,\, u^{i+r} v^{j+s}) \end{aligned} \tag{35}$$

for all exponents $i, j, r, s \in \mathbb{Z}_2$ and $k, \ell \in \mathbb{Z}_4$.

This is a familiar group in disguise.

GROUP $G^{(4)}$. Up to isomorphism, this semidirect product $\mathbb{Z}_3 \rtimes (\mathbb{Z}_2 \times \mathbb{Z}_2)$ is the dihedral group D_6

In fact, the element $u \in H_2$ is central in G because $\Phi(u) = I$, and it generates a subgroup $Z = \langle u \rangle \cong \mathbb{Z}_2$ such that $Z \cap H_3 = (e)$. Thus $N = H_3 \cdot Z$ is a subgroup isomorphic to $\mathbb{Z}_3 \times \mathbb{Z}_2 \cong \mathbb{Z}_6$ that is normal in G, with index $|G/N| = 2$. The element v in H_2 generates a copy of $\mathbb{Z}_2$ transverse to N. It is easy to check that the element $\rho = au$ is a cyclic generator for N and that $\sigma = v$, with $o(\sigma) = 2$, satisfies the dihedral relation $\sigma\rho\sigma^{-1} = \rho^{-1}$. It follows that $G^{(4)} \cong D_6$ as claimed.

CASE 3: ONLY H_2 IS NORMAL. If $H_2 \cong \mathbb{Z}_4$ then $G = H_2 \rtimes H_3$ is determined by by some homomorphism $\Phi : H_3 \cong \mathbb{Z}_3 \to \mathrm{Aut}(\mathbb{Z}_4, +) \cong (\mathrm{U}_4, \cdot\,) \cong (\mathbb{Z}_2, +)$. Since $\gcd(2, 3) = 1$, Φ must be trivial and we get nothing new: a direct product $\mathbb{Z}_4 \times \mathbb{Z}_3 \cong \mathbb{Z}_{12}$.

If $H_2 \cong \mathbb{Z}_2 \times \mathbb{Z}_2$ we again employ multiplicative notation for both H_2 and H_3, as in Case 2B. Important insight is achieved if we relabel elements of $H_2 = \{u^i v^j : i, j \in \mathbb{Z}_2\}$ as

$$x_0 = e, \quad x_1 = u, \quad x_2 = v, \quad x_3 = uv$$

Observe that $x_i^2 = e$ and $x_i x_{i+1} = x_{i+2} = x_{i-1}$ for $1 \le i \le 3$ when subscripts are reckoned (mod 3). (Thus for instance, $x_1 x_2 = uv = x_3, x_2 x_3 = v \cdot uv = u = x_1$ etc.) It is not hard to see that every element in $\mathrm{Aut}(H_2)$ permute the x_i leaving e fixed, and all permutations of the set $\{1, 2, 3\}$ are accounted for.

6.3.10 Exercise. Prove that every permutation σ of the integers $\{1, 2, 3\}$ yields an automorphism α of $\mathbb{Z}_2 \times \mathbb{Z}_2 = \{e, x_1, x_2, x_3\}$ such that

$$\alpha(e) = e, \quad \alpha(x_i) = x_{\sigma(i)} \quad \text{for } 1 \le i \le 3$$

Verify that the correspondence $\sigma \in S_3 \mapsto \tau \in \mathrm{Aut}(H_2)$ is bijective and an isomorphism of groups.
Hint: For the last part recall 6.2.26. □

Thus we obtain a natural identification of $\mathrm{Aut}(H_2)$ with the permutation group S_3 on three elements. A homomorphism $\Phi : \mathbb{Z}_3 \to \mathrm{Aut}(H_2) \cong S_3$ must carry the cyclic generator $a \in H_3$ to a permutation $\Phi(a) = \sigma$ such that $\sigma^3 = e$ so $o(\sigma) = 1$ or 3. The case $\sigma = e$ is uninteresting since it yields the trivial action, so we must assign $\Phi(a) = (123)$ or else $\Phi(a) = (132) = (123)^{-1}$. Both choices yield isomorphic semidirect products since they differ only in the way we label nontrivial elements in H_2, so we may as well take $\Phi(a) = (123)$, which corresponds to the automorphism $\Phi(a) : H_2 \to H_2$

$$\Phi(a)(e) = e \qquad \Phi(a)(u) = v, \qquad \Phi(a)(v) = uv, \qquad \Phi(a)(uv) = u$$

of H_2. The new group $G^{(5)} = H_2 \rtimes H_3 \cong (\mathbb{Z}_2 \times \mathbb{Z}_2) \rtimes \mathbb{Z}_3$ has the following multiplication law

$$(u^i v^j, a^k) \star (u^r v^s, a^\ell) = (u^i v^j \cdot \Phi(a)^k (u^r v^s)\,,\, a^{k+\ell}) \tag{36}$$

for exponents $i, j, r, s \in \mathbb{Z}_2$ and $k, \ell \in \mathbb{Z}_4$.

The role of the permutation (123) in this group law becomes clearer when we label elements in H_2 as e, x_1, x_2, x_3. Then $\Phi(a)x_i = x_{i+1}$ and $\Phi(a)^k x_i = x_{i+k}$ if we reckon subscripts (mod 3), and the multiplication law (36) takes the form

$$\begin{aligned}
(e, a^k) \star (e, a^\ell) &= (e, a^{k+\ell}) \\
(e, a^k) \star (x_i, a^\ell) &= (e \cdot \Phi(a)^k (x_i)\,,\, a^{k+\ell}) \\
&= (x_{i+k}, a^{k+\ell}) \\
(x_i, a^k) \star (e, a^\ell) &= (x_i \cdot \Phi(a)^k (e)\,,\, a^{k+\ell}) \\
&= (x_i, a^{k+\ell}) \\
(x_i, a^k) \star (x_j, a^\ell) &= (x_i \cdot \Phi(a)^k (x_j)\,,\, a^{k+\ell}) \\
&= (x_i x_{j+k}, a^{k+\ell})
\end{aligned}$$

To evaluate the last type of product we might need to make a 4×4 multiplication table for elements of H_2; there is no simple algebraic formula $m = m(i,j)$ for rewriting products $x_i x_j$ in the form x_m with $1 \le i,j,m \le 3$. (The formula $x_i x_{i+1} = x_{i+2}$ only applies when $j = i \pm 1$.)

We have identified a new group. We claim that

> GROUP $G^{(5)}$: The semidirect product $H_2 \rtimes H_3 \cong (\mathbb{Z}_2 \times \mathbb{Z}_2) \rtimes \mathbb{Z}_3$ with multiplication law (36) is isomorphic to the group of even permutations A_4. It is also the group of orientation-preserving symmetries of the regular tetrahedron.

A regular tetrahedron $\mathbf{T} \subseteq \mathbb{R}^3$ centered at the origin is unusual in that every permutation of its four vertices corresponds to an orthogonal linear transformation (rigid motion) in $\mathbb{R}^3$ that maps the tetrahedron to itself. It can be shown by convexity arguments that there are no other rigid-motion symmetries of this solid, so the full symmetry group of rigid motions of the tetrahedron is $\cong S_4$. In this picture, the even permutations A_4 correspond to the subgroup of orientation-preserving symmetries, which are the rotations about axes passing through a vertex and the midpoint of the opposite face. The full group S_4 includes some reflections across planes passing through the origin. Obviously $|A_4| = 12$ while $|S_4| = 24$.

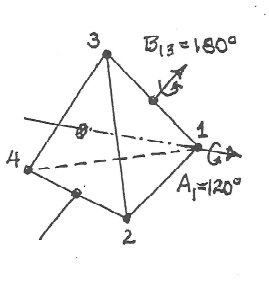

Figure 6.8 A regular tetrahedron centered at the origin. We show: rotation A_1 by 120° about an axis through vertex 1, and B_{13} by 180° about an axis through midpoints of opposite edges.

To see why the group described in (36) is isomorphic to A_4, regarded as the symmetry group of the tetrahedron $\mathbf{T}$, consider the tetrahedron shown in Figure 6.8 with vertices labeled $1,2,3,4$. Any 22-cycle, such as $(12)(34)$, corresponds to a 180° rotation about an axis passing through the midpoints of opposite edges. We have previously shown (Chapter 5) that the Klein Viergroup

$$N = \{e\} \cup \{\text{all three 2,2-cycles}\}$$

is a normal subgroup in S_4 isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$. For each axis passing through a vertex and the center of the opposite face, we get a subgroup of order 3 (one of the four Sylow 3-subgroups H_3) consisting of $0°, 120°$, and 240° rotations about this axis. For example the subgroup $\{e, (123), (132)\}$ corresponds to rotations about the axis passing through vertex 4 and the center of the opposite face. With these geometric descriptions in mind, it is not hard to see how to identify elements in our abstract model (36) with the correct geometric operations on $\mathbf{T}$. $\square$

6.3.11 Exercise. Explain why the five groups $G^{(1)}, \ldots, G^{(5)}$ of order 12 are pairwise

non-isomorphic. □

We take up one last example to show that the Sylow theorems do not always yield a definitive analysis, and that as the order of G increases we begin to encounter groups that are *not* semidirect products – i.e. they arise as extensions $e \to N \to G \to G/N \to e$ that do not split.

6.3.12 Example (Groups of Order 8). These are all p-groups so the Sylow theorems are not much help; however by (3.2.5, 3.2.6) we know G has nontrivial center $Z = Z(G)$, which can only have order $2, 4, 8$. If $|Z| = 8$ the group is abelian and the distinct possibilities are $G = \mathbb{Z}_8$, $\mathbb{Z}_4 \times \mathbb{Z}_2$, $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ in view of the following result.

6.3.13 Lemma. *If G is abelian with $|G| = 8$ then G is isomorphic to $\mathbb{Z}_8$, $\mathbb{Z}_4 \times \mathbb{Z}_2$, or $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$.*

Proof: If the maximum order of an element is $o(x) = 8$ then $G \cong \mathbb{Z}_8$. If the maximum is 4, say for $x = a$, then $A = \langle a \rangle \cong \mathbb{Z}_4$. Suppose there exists some $b \notin A$ such that $o(b) = 2$. Then $B = \langle b \rangle \cong \mathbb{Z}_2$ is transverse to A, $A \cap B = (e)$, $AB = G$, and since G is abelian it is a direct product $\cong \mathbb{Z}_4 \times \mathbb{Z}_2$.

Otherwise we have $o(b) = 4$ for all $b \notin A$ and $B \cong \mathbb{Z}_4$, but now we must have $|A \cap B| = 2$ (because $|G| = |A| \cdot |B| = 16$ if $A \cap B = (e)$). The only subgroup of $\mathbb{Z}_4$ with order 2 is $\{[0]_4, [2]_4\}$, whose nontrivial element has order 2. That means a^2 and b^2 are the only elements of A and B of order 2, and we must have $a^2 = b^2$, $a^{-2} = a^2, b^{-2} = b^2$, and $A \cap B = \{e, a^2\}$. Now look at the powers of the element ab: we get $e, ab, (ab)^2 = a^2b^2 = a^2a^{-2} = e$. Since $b \notin A \Rightarrow ab \notin A$ we have found an element outside of A with order 2. Contradiction. This case cannot arise. □

If $|Z| = 4$ then $G/Z \cong \mathbb{Z}_2$. Since G/Z is *cyclic* and Z is central in G, G must be abelian (why?). Contradiction. Thus $|Z|$ cannot equal 4when G is nonabelian.

***6.3.14 Exercise**. If G is a finite group and Z a subgroup such that (i) Z is central (so $zg = gz$ for all $z \in Z, g \in G$), and (ii) G/Z is cyclic, prove that G must be abelian. □

Assuming $|Z| = 2$, let x be an element of highest order in G. We can only have $o(x) = 2$ or 4 (G is abelian if $o(x) = 8$). In the first case all elements $y \neq e$ would have order 2 and $G \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ (see Exercises 6.2.28 - 29). Abelian G have already been dealt with, so we must have $o(x) = 4$ and $N = \langle x \rangle$ is isomorphic to $\mathbb{Z}_4$; the following elementary result shows that N is also normal in G.

***6.3.15 Exercise**. Let G be a group and H a subgroup of index $|G/H| = 2$. Prove that H is automatically normal in G.
Hint: If $a \notin H$ what can you say about the left and right cosets aH and Ha? □

We now have an extension

$$e \longrightarrow N \cong \mathbb{Z}_4 \longrightarrow G \longrightarrow Q = G/N \cong \mathbb{Z}_2 \longrightarrow e$$

and the real issue is whether it splits.

If it does there is a subgroup $Q = \langle y \rangle \cong \mathbb{Z}_2$ transverse to G/N cosets and we have a semidirect product $N \times_\phi Q$. We saw in 1.3.2 that $\mathrm{Aut}(\mathbb{Z}_4, +) \cong (\mathrm{U}_4, \cdot\,) \cong (\mathbb{Z}_3, +)$. The only possible homomorphisms $\Phi : \mathbb{Z}_2 \to \mathrm{Aut}(N)$ must map the nontrivial element $y \in Q$ to either

(a) $\Phi(y) = \mathrm{id}_N$, in which case G is an abelian direct product $\mathbb{Z}_4 \times \mathbb{Z}_2$, a possibility we have already excluded.

(b) $\Phi(y)$ = the inversion map, which takes $[k]_4$ to $-[k]_4 = [4-k]_4$ in $\mathbb{Z}_4$.
In this case:

$$x^4 = e, \qquad y^2 = e, \qquad yxy = yxy^{-1} = \Phi(y)(x) = x^{-1}$$

Obviously this G is isomorphic to the the dihedral group D_4.

In the non-split case we claim that G is the group of **unit quaternions** $Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$ in which the elements ± 1 are central, $-i = (-1)i, \ldots, -k = (-1)k$ and

$$(-1)^2 = 1 \qquad i^2 = j^2 = k^2 = ijk = -1$$

from which we get other familiar relations such as $ij = k = -ji, jk = i = -kj$, and $ki = j = -ik$. Given Q_8 it is easy to check that its center is $Z(Q_8) = \{1, -1\}$ and that $N = \langle j \rangle = \{1, j, -1, -j\}$ is a cyclic normal subgroup $\cong \mathbb{Z}_4$. But as you can easily check, the only elements $g \in Q_8$ such that $g^2 = 1$ are ± 1, which already lie in N; thus the extension Q_8 of $G/N \cong \mathbb{Z}_2$ by $N \cong \mathbb{Z}_4$ cannot split.

It remains to check by hand that, up to an isomorphism, Q_8 is the only possibile non-split extension of $\mathbb{Z}_4$ by $\mathbb{Z}_2$. Taking an $x \in G$ that generates a cyclic normal subgroup $N \cong \mathbb{Z}_4$, let y be any element lying outside N, so that $G = \langle x, y \rangle$. Since our extension does not split we cannot have $o(y) = 2$, but $y^2 \equiv e \pmod{N}$ so $y^2 \in \{x, x^2, x^3 = x^{-1}\}$. The first and last possibilities are excluded: if, say, $y^2 = x$ then $y^3 = xy = yx$ and G would be abelian. Hence our generators x, y satisfy

$$o(x) = o(y) = 4 \qquad y \notin N = \langle x \rangle \qquad y^2 = x^2$$

Let us write "$-\mathbf{1}$" for the element $x^2 = y^2$ and "$\mathbf{1}$" for the identity element in G. Then $(-\mathbf{1})^2 = \mathbf{1}$ and $-\mathbf{1}$ is central in G (because $(-\mathbf{1})x = x^2x = x(-\mathbf{1})$, and likewise for y). Next observe that $z = xy$ satisfies $z^2 = -\mathbf{1}$. To see this, first note that $xy \notin N$ but $(xy)^2 \in N$. If $xyxy = x$ then $yxy = e$ and $x = y^2 = x^2$, which is impossible; likewise we get $xyxy \neq x^3$. So, we must have $(xy)^2 = x^2$ – i.e. $xyz = xy(xy) = -\mathbf{1}$. We conclude that $G \cong Q_8$ when we identify with $1, i, j, k$ with $\mathbf{1}, x, y, z$ and $-\mathbf{1} = x^2 = y^2, -i = (-\mathbf{1})i = x^3, -j = (-\mathbf{1})j = y^3, -k = (-\mathbf{1})k = z^3$. □

To summarize: the only groups of order 8 are $Q_8, D_4, \mathbb{Z}_8, \mathbb{Z}_4 \times \mathbb{Z}_2$, and $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$.

Deciding whether an extension $e \to N \to G \to G/N \to e$ splits can be difficult. Even if N and G/N are cyclic, the extension need not split – the group Q_8 of quaternion units being one counterexample.

Keeping in mind that $G \cong \mathbb{Z}_p$ for any group of prime order $p > 1$, we have now identified all groups of order $|G| \leq 13$ except for those of orders 9 and 10. You might try your hand at filling in these gaps.

6.3.16 Exercise. If $|G| = 9$ prove that

(a) G is abelian

(b) G is isomorphic to $\mathbb{Z}_9$ or $\mathbb{Z}_3 \times \mathbb{Z}_3$.

Explain why the groups in (b) are not isomorphic. □

6.3.17 Exercise. Determine all groups of order $|G| = 10$ □

6.4 Types of Groups: Simple, Solvable, Nilpotent.

A group is **simple** if it contains no proper normal subgroups, which is to say it has no proper quotients G/N; by this definition, the trivial group is simple. In view of Cauchy's theorem 4.3.5, the only other simple finite abelian groups are $(\mathbb{Z}_p, +)$ where $p > 1$ is prime. Noncommutative examples include the alternating groups A_n, consisting of all even permutations in the full permutation group S_n on n objects. The fact that A_n is

simple for $n \geq 5$ is of great importance in Galois' theory of equations; S_n itself is not simple because it always has A_n as a proper normal subgroup.

Complementary to the simple groups we have the *solvable* and *nilpotent* groups. For any G, finite or not, two descending series of normal subgroups can be defined in terms of *commutators* $[x, y] = xyx^{-1}y^{-1}$. If A, B are subgroups we define $[A, B]$ to be the subgroup generated by all commutators formed from elements of A and B:

$$[A, B] = \left\langle\, xyx^{-1}y^{-1} : x \in A,\, y \in B \,\right\rangle \tag{37}$$

The **commutator subgroup** $[G, G]$ obtained by taking $A = B = G$ is of particular importance. First, it is a normal subgroup, but in fact it is a *characteristic subgroup*, which means it is invariant under *all* $\alpha \in \mathrm{Aut}(G)$. This follows because the image of a commutator $[x, y]$ under any automorphism α has the form

$$\alpha([x, y]) = [\alpha(x), \alpha(y)] \qquad \text{for all } x, y \in G \tag{38}$$

and again is a commutator. Second, the quotient $G/[G, G]$ is abelian because we are factoring out all relations associated with noncommutativity of G. In fact, the commutator group is the smallest normal subgroup such that G/N is abelian.

6.4.1 Exercise. Suppose S is a subset of a group G and $H = \langle S \rangle$ is the subgroup it generates. If $\phi : G \to G$ is a homomorphism that maps S into itself, prove that ϕ leaves the generated subgroup invariant too – i.e. $\phi(H) \subseteq H$.
Hint: Recall that $\langle S \rangle$ is defined to be the smallest subgroup in G that contains S. It is also described as $\langle S \rangle = \{a_1 a_2 \ldots a_r : r < \infty \text{ and } a_i \in S \cup S^{-1}\}$, the set of all "words" of finite length each of whose letters is of the form s or s^{-1}. The latter viewpoint might be congenial in proving that $\phi(H) \subseteq H$. □

6.4.2 Exercise. If $\alpha \in \mathrm{Aut}(G)$ and $x, y \in G$, verify the identity (38) and then use it to prove that the commutator subgroup $[G, G]$ is a **characteristic subgroup** in G (a subgroup invariant under all $\alpha \in \mathrm{Aut}(G)$).
Hint: Use the previous exercise. □

6.4.3 Exercise. If G is any group and N any normal subgroup, prove that G/N is abelian if and only if $N \supseteq [G, G]$. □

Thus $N = [G, G]$ is the smallest normal subgroup in G such that G/N is abelian. Obviously G is abelian $\Leftrightarrow$ $[G, G]$ is trivial.

We now define the **upper/lower derived series** to be the descending series of subgroups shown in Figure 6.8. Both series begin with G followed by $D^1(G) = D_1(G) = [G, G]$. In order to understand these definitions it would be useful to verify that in the right hand series we have $D_{k+\ell}(G) = D_k(D_\ell(G))$. This is almost obvious (by induction on k); it is *not* true for the series on the left.

The horizontal inclusions shown in Figure 6.9 follow by an easy inductive argument from the fact that $A' \supseteq A \Rightarrow [A', B] \supseteq [A, B]$. A recursive argument based on Exercises 6.4.1-2 shows that all subgroups in Figure 6.9 are normal, and in fact are characteristic subgroups in G. For example, we know that $D^1(G) = [G, G]$ is characteristic by 6.4.2. The next derived group $D^2(G)$ is generated by commutators $[g, a]$ such that $g \in G$ and $a \in D^1(G)$; but an automorphism $\alpha \in \mathrm{Aut}(G)$ maps generators to generators in $D^2(G)$ because $\alpha([g, a]) = [\alpha(g), \alpha(a)] \in [G, D^1(G)]$. Hence by 6.4.1 the subgroup $D^2(G)$ is invariant under α. Similar arguments, which we omit, show that all the subgroups $D^k(G)$ and $D_k(G)$ are invariant under *all* automorphisms of G.

6.4.4 Exercise. Fill in the details needed to show

(a) $A' \supset A \Rightarrow [A', B] \supseteq [A, B]$

$$
\begin{array}{ccc}
G & & G \\
\cup & & \cup \\
D^1(G) = [G,G] & = & D_1(G) = [G,G] \\
\cup & & \cup \\
D^2(G) = [G, D^1(G)] & \supseteq & D_2(G) = [D_1(G), D_1(G)] \\
\cup & & \cup \\
D^3(G) = [G, D^2(G)] & \supseteq & D_3(G) = [D_2(G), D_2(G)] \\
\cup & & \cup \\
\vdots & & \vdots \\
\cup & & \cup \\
D^{k+1}(G) = [G, D^k(G)] & \supseteq & D_{k+1}(G) = [D_k(G), D_k(G)] \\
\cup & & \cup \\
\vdots & & \vdots \\
\text{Upper Derived Series} & & \text{Lower Derived Series}
\end{array}
$$

Figure 6.9. The two derived series for G.

(b) The inclusions shown in Figure 6.9 are valid

(c) The $D^k(G)$ are all characteristic subgroups in G.

(d) The $D_k(G)$ are all characteristic subgroups in G.

(e) $D_{k+\ell}(G) = D_k(D_\ell(G))$ for all $k, \ell \geq 1$.

(f) If $H \subseteq G$ then $D^k(H) \subseteq D^k(G)$ and $D_k(H) \subseteq D_k(G)$. $\square$

It is possible that one or both series stabilize after a finite number of steps, so that

$$G \supseteq D^1(G) \supseteq \ldots \supseteq D^k(G) = D^{k+1}(G) = \ldots$$

or

$$G \supseteq D_1(G) \supseteq \ldots \supseteq D_k(G) = D_{k+1}(G) = \ldots,$$

Clearly, once two successive groups are equal, say $D^k(G) = D^{k+1}(G)$, then all later subgroups are the same. Furthermore if G is finite the subgroups must "stabilize." When this happens the repeating stable subgroup need not be trivial; for example the alternating group A_n ($n \geq 5$) has no proper normal subgroups and is nonabelian, so the lower derived series for the permutation group is $S_n \supseteq A_n = A_n = \ldots$.

For infinite groups these descending series might not stabilize at all, as is true for the free group F_2 on two generators. [One can, with some effort, prove that F_2 is *residually nilpotent* in the sense that $\bigcap_{k=1}^{\infty} D^k(F_2) = (e)$.]

Two important classes of groups are defined by the properties of their derived series.

6.4.5 Definition. A group G is **nilpotent** if the upper derived series is eventually trivial, and G is **solvable** if the lower derived series becomes trivial in finitely many steps. Obviously (nilpotent) $\Rightarrow$ (solvable), but the converse fails. $\square$

6.4.6 Exercise. The **affine group** of the line $G = \mathrm{Aff}(2, \mathbb{R})$ consists of the operators

$$T_{(a,b)} : \mathbb{R} \to \mathbb{R} \text{ with } a > 0, b \in \mathbb{R} \qquad T_{(a,b)}(x) = ax + b$$

which form a group under composition.

(a) Verify that G is a group and work out formulas for computing

(i) $T_{(a,b)} \circ T_{(a',b')}$, and (ii) $T_{(a,b)}^{-1}$.

(b) Verify that $N = \{T_{(1,b)} : b \in \mathbb{R}\}$ is a normal subgroup isomorphic to $\mathbb{R}$ and that $G/N \cong \mathbb{R}$. *Hint:* The exponential map identifies $(\mathbb{R}, +)$ with the multiplicative group of numbers $a > 0$.

(c) Compute the derived group $[G, G]$ and verify that G is solvable.

(d) Show that the center $Z(G)$ is trivial, and that G is not nilpotent.

Note: This group is often referred to as the "$ax + b$ group," for obvious reasons. □

6.4.7 Exercise. The 3×3 **Heisenberg group** can be described as the set of upper triangular matrices

$$G = \left\{ \begin{bmatrix} 1 & x & z \\ 0 & 1 & y \\ 0 & 0 & 1 \end{bmatrix} : x, y, z \in \mathbb{R} \right\}$$

We shall label group elements by the symbol strings (x, y, z)

(a) In terms of these parameters compute the form of the product $(x, y, z) * (x', y', z') = \ldots$ of two group elements and the inverse $(x, y, z)^{-1} = \ldots$.

(b) Show that $Z(G) = \{(0, 0, z) : z \in \mathbb{R}\}$ and identify the commutator subgroup $[G, G]$.

Then verify that G is nilpotent. □

We now list some basic combinatorial facts about these groups. The first is just an exercise in understanding the definitions.

6.4.8 Exercise. Show that any homomorphism $\phi : G \to G'$ preserves the various derived subgroups:

(i) $\phi(D^k(G)) = D^k(\phi(G)) \subseteq D^k(G')$

(ii) $\phi(D_k(G)) = D_k(\phi(G)) \subseteq D_k(G')$

for all $k = 1, 2, \ldots$.
Hint: Use Exercise 6.4.1 and induction on the index k. □

It follows almost immediately that all homomorphic images and all subgroups of nilpotent (or solvable) groups are again nilpotent (or solvable). [For quotients, apply Exercise 6.4.8. For any subgroup H we have $[H, H] \subseteq [G, G]$, and then inductively we get $[H, D^k(H)] \subseteq [G, D^k(G)]$ and $[H, D_k(H)] \subseteq [G, D_k(G)]$ for $k = 1, 2, \ldots$. Thus $D^{r+1}(G) = (e) \Rightarrow D^{r+1}(H) = (e)$, and similarly for the lower derived series.] As a corollary we obtain a basic combinatorial result:

6.4.9 Lemma. *If $N \lhd G$ is a normal subgroup of a group G, giving us the sequence of homomorphisms*

$$e \longrightarrow N \xrightarrow{\text{id}} G \xrightarrow{\pi} G/N \longrightarrow e \quad ,$$

then G is solvable if and only if G/N and N are solvable.

Proof: We have just discussed ($\Rightarrow$), and conversely if $\pi : G \to G/N$ is the quotient homomorphism, solvability of G/N insures that $D_{n+1}(G/N) = (e)$ for some n. Exercise 6.4.8 insures that $\pi(D_{n+1}(G)) = D_{n+1}(G/N) = (e)$, and hence $D_{n+1}(G) \subseteq N$. Taking k so $D_{k+1}(N) = (e)$ we get $D_{k+n+2}(G) = D_{k+1}(D_{n+1}(G)) \subseteq D_{k+1}(N) = (e)$. □

Nilpotent groups do not share this property, see Exercise 6.4.6 where $N \cong \mathbb{R}$ and $G/N \cong \mathbb{R}$ are nilpotent (abelian) but G is not nilpotent. But for solvable groups there is an even stronger result which sheds light on how they are put together.

6.4.10 Lemma. *A group G is solvable if there exist subgroups*

$$G = G_0 \supseteq G_1 \supseteq \ldots \supseteq G_r \supseteq G_{r+1} = (e)$$

such that

(i) *G_{j+1} is a normal subgroup in G_j for each j,*

(ii) *Each quotient G_j/G_{j+1} is solvable.*

In particular G is solvable if the quotients are all abelian. Conversely, if G is solvable such sequences exist and the subgroups can be chosen so each quotient is abelian.

PROOF: The previous remarks show that we can work backward up the chain $G \supseteq D_1(G) \supseteq D_2(G) \supseteq \ldots$, successively verifying solvability of $G_r, G_{r-1}, \ldots$. Starting from the top, Exercise 6.4.3 shows that $G/D_1(G) = G/[G,G]$ is abelian, but since $D_2(G) = D_1(D_1(G)) = [D_1(G), D_1(G)]$ we see that $D_1(G)/D_2(G)$ is abelian, etc. □

Nilpotent groups, unlike solvable groups, always have nontrivial centers. In fact, if $D^r(G) \neq (e)$ and $D^{r+1}(G) = [G, D^r(G)] = (e)$, we see that $D^r(G)$ is a nontrivial central subgroup in G. Central subgroups play a prominent role in the nilpotent analog of 6.4.10.

6.4.11 Lemma. *A group G is nilpotent if there there is a subgroup N such that* (i) *N is central in G, and* (ii) *G/N is nilpotent.*

PROOF: All subgroups of the center $Z(G_j)$ are normal in G_j, so G/N is a bona-fide group. Now observe that $D^{r+1}(G/N) = (e)$ for some r and that $D^{r+1}(G/N) = \pi(D^{r+1}(G))$ under the quotient map π. Thus $D^{r+1}(G) \subseteq N = \ker \pi$, and since N is central in G we get $D^{r+2}(G) = [G, D^{r+1}(G)] \subseteq [G, N] = (e)$. Thus G is nilpotent. □

For other conditions leading to nilpotence of G see 6.4.13 below.

One useful consequence of 6.4.11 is the fact that nonabelian finite groups always include sizeable nilpotent subgroups, namely their Sylow p-subgroups.

6.4.12 Corollary. *If $|G| = p^k$ for some prime then G is nilpotent.*

PROOF: If $k = 1$ then $G \cong \mathbb{Z}_p$, so assume $k > 1$. Then the center $Z(G)$ is nontrivial and $|G/Z(G)| = p^r$ for some $r < k$. By induction $G/Z(G)$ is nilpotent, and since $Z(G)$ is central G must be nilpotent too. □

Nilpotent groups are the next best thing to being abelian; solvable groups also have some commutative aspects, but the connection is more tenuous. The pervasive role of "centers" in nilpotent groups is revealed by noting that there is a third canonical series of subgroups in any group G, the **ascending central series** $Z(G) \subseteq Z^{(2)} \subseteq Z^{(3)} \subseteq \ldots$ defined as follows.

$$
\begin{aligned}
Z^{(1)} &= Z(G) \quad \text{(the center of } G\text{)} \\
Z^{(2)} &= \{x \in G : xy \equiv yx \pmod{Z(G)}, \text{ all } y \in G\} \\
Z^{(3)} &= \{x \in G : xy \equiv yx \pmod{Z^{(2)}}, \text{ all } y \in G\} \\
&\vdots \\
Z^{(k+1)} &= \{x \in G : xy \equiv yx \pmod{Z^{(k)}}\} \\
&\vdots
\end{aligned}
\tag{39}
$$

The group $Z^{(2)}$ is often referred to as the *second center* of G; it is just the pullback to G of the center in the quotient group $G/Z(G)$. (The center of the quotient need not be trivial.) Obviously, $Z^{(k)} \subseteq Z^{(k+1)}$ at every step, and if equality holds at the k^{th} step it holds at every later step. We note without proof the following characterization of nilpotent groups in terms of the ascending central series.

6.4.13 Theorem. *A group G is nilpotent if and only if we have $Z^{(k)} = G$ for some*

$k = 1, 2, \ldots$.

Nilpotent groups are particularly amenable to study via inductive arguments. Indeed, 6.4.11 and 6.4.13 provide us with two inductive strategies:

1. Run up the ascending central series $(e) \subseteq Z(G) \subseteq \ldots$ hoping to prove some result by examining the abelian group $Z(G)$ and the smaller nilpotent group $G/Z(G)$.
2. Examine the descending derived series, $G \supseteq [G,G] \supseteq \ldots$ hoping to prove some result by examining the abelian group $G/[G,G]$ and the smaller nilpotent group $[G,G]$. In this connection it is worth noting that *any* intermediate subgroup $G \supseteq H \supseteq [G,G]$ is automatically nilpotent and normal in G, and G/H is abelian.

6.4.14 Example. The permutation groups S_2, S_3, S_4 are solvable. For $n \geq 5$ the alternating group $A_n = \{\sigma \in S_n : \mathrm{sgn}(\sigma) = +1\}$ is simple and is the only proper normal subgroup in S_n. Hence S_n is not solvable for $n \geq 5$.

Discussion: Assume $n \geq 5$. In 5.3.5 – 5.3.7 we indicated why A_n is the only proper normal subgroup in S_n, and showed that A_n is simple. The lower commutator series for S_n terminates prematurely, with

$$S_n \supseteq D_1(S_n) = [S_n, S_n] = A_n = D_2(S_n) = D_3(S_n) = \ldots$$

so S_n is not solvable. In fact, since the signature map $\mathrm{sgn} : S_n \to \{\pm 1\}$ is a homomorphism we get $\mathrm{sgn}(xyx^{-1}y^{-1}) = \mathrm{sgn}(x)\mathrm{sgn}(y)\mathrm{sgn}(x)^{-1}\mathrm{sgn}(y)^{-1} = 1$ for every commutator of elements in S_n. Thus $[S_n, S_n] \subseteq A_n$. But S_n is not abelian, so the the commutator subgroup $[S_n, S_n]$ is nontrivial and normal in S_n, and hence in A_n. Thus it is either all of A_n and $D_1(S_n) = [S_n, S_n] = A_n$ as shown above. At the next step in the commutator sequence, A_n is nonabelian so $D_2(S_n) = [A_n, A_n]$ is nontrivial, and it is a normal subgroup *in* A_n. As such, it must equal A_n. From here on the commutator sequence repeats.

For $n = 2, 3, 4$ we know that $S_2 \cong \mathbb{Z}_2$ is abelian, hence solvable. In Example 5.4.1 we showed that $S_3/A_3 \cong \mathbb{Z}_2$ and that $A_3 \cong \mathbb{Z}_3$, so S_3 is solvable by 6.4.10. In 5.4.4 we showed that S_4 contains the abelian Klein Viergroup $V_4 \cong \mathbb{Z}_2 \times \mathbb{Z}_2$ as a normal subgroup, and that $S_4/A_4 \cong \mathbb{Z}_2$, $A_4/V_4 \cong \mathbb{Z}_3$. Applying 6.4.10 again we conclude that S_4 is solvable. □

One goal of group theory has been to classify the finite simple groups up to isomorphism. Nilpotent and solvable groups are generally far from simple, owing to the presence of various series of normal subgroups. It is easy to see that the only simple solvable groups are abelian, and they are the cyclic groups $(\mathbb{Z}_p, +)$ where $p > 1$ is a prime. Here we can only mention a remarkable theorem proved by W. Feit and J. Thompson in the 1970's that opened the way for the successful classification of all finite simple groups in the 1980's.

6.4.15 Theorem. *If G is a finite group of odd order, then G is solvable. Hence all nonabelian finite simple groups have order divisible by* 2.

The proof ran some 250 pages and occupied an entire issue of *Pacific Journal of Mathematics*. Note that the only *abelian* simple groups are $(\mathbb{Z}_p, +)$ for primes $p > 1$; these have *odd* order p, except for $p = 2$.

The structure of non-simple groups can be quite complicated, even though they are in some sense assembled by combining simple groups. Nevertheless, certain structural features can be identified by recalling that the product set $N = N_1N_2$ formed from

two normal subgroups is again a normal subgroup. First notice that if both groups are solvable, so is the product. In fact, by the Second Isomorphism Theorem for quotients 3.3.14 we have a sequence of homomorphisms

$$e \longrightarrow N_1 \xrightarrow{\text{id}} N \xrightarrow{\pi} N/N_1 \cong N_2/N_1 \cap N_2 \longrightarrow e$$

and the middle group is solvable if the end groups are (Lemma 6.4.9). Thus a group G always contains a unique *largest* solvable normal subgroup R, which is sometimes referred to as the **solvable radical** of G. The quotient G/R contains no normal solvable subgroups at all, although there will certainly be non-normal abelian and solvable subgroups in it, for instance cyclic subgroups.

6.4.16 Exercise. For any $n \geq 3$ determine the center $Z(G)$ of the dihedral group $G = D_n$.
Hint: The answer will depend on whether n is even or odd. □

6.4.17 Exercise. Compute the commutator subgroup $[G, G]$ for the dihedral group $G = D_n$, $n \geq 3$. Is D_n nilpotent for any n? Solvable? □

6.4.18 Exercise. In the cases where the center of D_n is nontirival, does the extension

$$e \to Z(D_n) \to D_n \to D_n/Z(D_n) \to e$$

split – i.e. is D_n a semidirect product with its center as the normal subgroup? □

6.4.19 Exercise. Compute the commutator subgroup $[G, G]$ of the quaternion group $G = Q_8$ of Example 6.3.10. Is Q_8 nilpotent? Solvable? □