

Dr. H. Joseph Straight
 SUNY Fredonia
Smokin' Joe's Catalog of Groups: Abelian Groups

Again, we consider the fundamental problem of cataloging all the groups of some given order n , up to isomorphism. The goal of this chapter is to state and prove the Fundamental Theorem of Finite Abelian Groups, which solves the subproblem of cataloging all the abelian groups of order n .

Recall that, if $(G, *)$ is a group and $(H, *)$ is a subgroup of $(G, *)$, then the set of distinct right cosets of H in G is a partition of G . We denote this set of cosets by G/H ; that is,

$$G/H = \{Hx \mid x \in G\}$$

We wish to define an operation \otimes on G/H so that $(G/H, \otimes)$ is a group. The obvious candidate is this: for $x_1, x_2 \in G$,

$$Hx_1 \otimes Hx_2 = H(x_1 * x_2)$$

It is not difficult to show that, if \otimes is well-defined, then:

1. \otimes is associative;
2. If e is the identity element of G , then $He = H$ is the identity element of G/H ;
3. If x^{-1} is the inverse of x in G , then Hx^{-1} is the inverse of Hx in G/H .

See Exercise 2. Thus, $(G/H, \otimes)$ will be a group provided the operation \otimes is well-defined on G/H .

The problem is that a given right coset of H in G may have different “names.” For example, if

$$G = D_4 = \{e, a, a^2, a^3, b, ab, a^2b, a^3b\}$$

(with $|a| = 4$, $|b| = 2$, $b \neq a^2$, and $ba = a^3b$) and $H = \langle b \rangle = \{e, b\}$, then:

$$\begin{aligned} H &= \{e, b\} = Hb \\ Ha &= \{a, a^3b\} = Ha^3b \\ Ha^2 &= \{a^2, a^2b\} = Ha^2b \\ Ha^3 &= \{a^3, ab\} = Hab \end{aligned}$$

Thus, Ha^3 and Hab refer to the same right coset. Hence, if \otimes is well-defined, then $Ha \otimes Ha^3$ should equal $Ha \otimes Hab$. However, note that

$$Ha \otimes Ha^3 = H(a * a^3) = He = H, \quad \text{whereas} \quad Ha \otimes Hab = H(a * ab) = Ha^2b = Ha^2$$

So $Ha \otimes Ha^3 \neq Ha \otimes Hab$, and it follows that \otimes is not well-defined in this case.

In the general case, suppose $x_1, x_2, x_3, x_4 \in G$ with $Hx_1 = Hx_3$ and $Hx_2 = Hx_4$. Then there exist $h_1, h_2, h_3, h_4 \in H$ such that

$$h_1 * x_1 = h_3 * x_3 \quad \text{and} \quad h_2 * x_2 = h_4 * x_4$$

In order for \otimes to be well-defined, we need $Hx_1 \otimes Hx_2 = Hx_3 \otimes Hx_4$. This will be true provided $Hx_1 \otimes Hx_2 = Hx_3 \otimes Hx_2$ and $Hx_3 \otimes Hx_2 = Hx_3 \otimes Hx_4$.

Let's check these. First,

$$\begin{aligned} Hx_1 \otimes Hx_2 &= H(x_1 * x_2) \\ &= H(h_1^{-1} * h_3 * x_3 * x_2) \\ &= H(x_3 * x_2) && \text{since } h_1^{-1} * h_3 \in H \\ &= Hx_3 \otimes Hx_2 \end{aligned}$$

So, no problem with that one. Next,

$$\begin{aligned} Hx_3 \otimes Hx_2 &= H(x_3 * x_2) \\ &= H(x_3 * h_2^{-1} * h_4 * x_4) \\ &= H(h * x_3 * x_4) && \text{provided } x_3H = Hx_3 \\ &= H(x_3 * x_4) \\ &= Hx_3 \otimes Hx_4 \end{aligned}$$

Thus, in order for \otimes to be well-defined, we need $xH = Hx$ for each $x \in G$; that is, for any element x of G , we need the left and right cosets xH and Hx to be the same set.

Definition 1: Let G be a group and let H be a subgroup of G . We call H a *normal subgroup* provided

$$xH = Hx$$

for every $x \in G$. We denote the fact that H is a normal subgroup of G by writing $H \triangleleft G$. ■

We remark that, if e is the identity element of G , then both $\{e\} \triangleleft G$ and $G \triangleleft G$; that is, both of the trivial subgroups of G are normal subgroups. For nontrivial subgroups, we often apply the following result.

Theorem 1 (Normal Subgroup Test): For any group G and any subgroup H of G , H is a normal subgroup of G if and only if

$$ghg^{-1} \in H$$

for any elements h and g with $h \in H$ and $g \in G$.

Proof: Let G be a group and let H be a subgroup of G .

For necessity, suppose for some elements h and g with $h \in H$ and $g \in G$ that $ghg^{-1} \notin H$. We claim that $gH \neq Hg$, and hence that H is not a normal subgroup. Suppose, to the contrary, that $gH = Hg$. Then $gh \in Hg$, and so there is some element $h' \in H$ such that $gh = h'g$. But then $ghg^{-1} = h' \in H$, a contradiction.

For sufficiency, assume that $ghg^{-1} \in H$ for any elements h and g with $h \in H$ and $g \in G$. To show that $H \triangleleft G$, it suffices to show that $gH = Hg$. Let $x \in gH$. Then $x = gh$ for some $h \in H$. Hence, $xg^{-1} = ghg^{-1} = h' \in H$. Thus, $x = h'g \in Hg$. This shows that $gH \subseteq Hg$. Using a similar argument, it can be shown that $Hg \subseteq gH$. Therefore, $gH = Hg$, as was to be shown. ■

The following corollary is an immediate consequence of Theorem 1. Recall that the *center* of a group G is the subgroup \mathcal{C} defined by

$$\mathcal{C} = \{h \in G \mid gh = hg \text{ for all } g \in G\}$$

Hence, if $h \in \mathcal{C}$ and $g \in G$, then

$$ghg^{-1} = (gh)g^{-1} = h(gg^{-1}) = h \in \mathcal{C}$$

Corollary 2: For any group G :

1. If G is abelian, then any subgroup H is a normal subgroup; that is, every subgroup of an abelian group is a normal subgroup.
2. The center \mathcal{C}_G of G is a normal subgroup of G . ■

There is an additional class of normal subgroups that occurs frequently enough to deserve special mention.

Theorem 3: For any finite group G of even order, if H is a subgroup of G and

$$2|H| = |G|$$

then H is a normal subgroup of G .

Proof: Let G be a finite group of even order and let H be a subgroup of G such that $2|H| = |G|$; that is $|G : H| = 2$. Then, for any $x \in H$, $xH = H = Hx$. Also, for any $x \in G - H$, $xH = G - H = Hx$, since both $\{H, xH\}$ and $\{H, Hx\}$ are partitions of G . It follows from Definition 1 that $H \triangleleft G$. ■

Example 1: Find all the nontrivial normal subgroups of D_6 .

Solution: Recall that

$$D_6 = \langle r, s \mid |r| = 6, |s| = 2, s \neq r^3, sr = r^5s \rangle$$

The nontrivial subgroups of D_6 are:

$$\begin{aligned} H_1 &= \langle r \rangle = \{e, r, r^2, r^3, r^4, r^5\} \\ H_2 &= \{e, r^2, r^4, s, r^2s, r^4s\} \cong D_3 \\ H_3 &= \{e, r^2, r^4, rs, r^3s, r^5s\} \cong D_3 \\ H_4 &= \{e, r^3, s, r^3s\} \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \\ H_5 &= \{e, r^3, rs, r^4s\} \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \\ H_6 &= \{e, r^3, r^2s, r^5s\} \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \\ H_7 &= \langle r^2 \rangle = \{e, r^2, r^4\} & H_8 &= \langle r^3 \rangle = \{e, r^3\} \\ H_9 &= \langle s \rangle = \{e, s\} & H_{10} &= \langle rs \rangle = \{e, rs\} \\ H_{11} &= \langle r^2s \rangle = \{e, r^2s\} & H_{12} &= \langle r^3s \rangle = \{e, r^3s\} \\ H_{13} &= \langle r^4s \rangle = \{e, r^4s\} & H_{14} &= \langle r^5s \rangle = \{e, r^5s\} \end{aligned}$$

Each of H_1 , H_2 , and H_3 has index 3 in D_6 , and hence are normal by Theorem 3. Also, H_8 is the center of D_6 , and hence is normal by Corollary 2.

For H_7 , note that $sr^2s^{-1} = r^4$ and $sr^4s^{-1} = r^2$. It follows (see Exercise 4) that $H_7 \triangleleft D_6$.

For H_4 , note that

$$rsr^{-1} = rsr^5 = r(rs) = r^2s \notin H_4$$

Thus, H_4 is not a normal subgroup. By similar reasoning, it can be shown that none of the subgroups H_5 , H_6 , H_9 , H_{10} , H_{11} , H_{12} , H_{13} , H_{14} is a normal subgroup of D_6 . Therefore, D_6 has precisely five nontrivial normal subgroups: H_1 , H_2 , H_3 , H_7 , and H_8 . ■

Definition 2: Let $(G, *)$ be a group and let H be a normal subgroup of G . Then $(G/H, \otimes)$ is a group, with the operation \otimes defined by

$$Hx_1 \otimes Hx_2 = H(x_1 * x_2) \quad \clubsuit$$

The group G/H is called the **factor group** (or **quotient group**) of G by H . ■

Let G be a group and let $H \triangleleft G$. We make the following remarks:

1. If e is the identity element of G , then

$$G/\{e\} \cong G \quad \text{and} \quad G/G \cong \mathbb{Z}_1$$

That is, the factor group G/H is not very interesting when H is a trivial subgroup of G .

2. If G is finite, then

$$|G/H| = |G : H| = \frac{|G|}{|H|}$$

3. If G is abelian, then G/H is abelian.

4. If x has finite order in G , then Hx has finite order in G/H , and the order of Hx in G/H is a factor of the order of x in G — see Exercise 6.

With regard to the last remark, we have two possible interpretations for the notation $|Hx|$ — it could mean the cardinality of the coset Hx , or it could mean the order of the element Hx in the factor group G/H . Since the cardinality of Hx is generally not an issue (it is the same as the cardinality of H), we will take $|Hx|$ to mean the order of Hx in the factor group G/H , unless explicitly stated otherwise.

If the operation for G is considered to be a form of “multiplication,” then we will, as usual, use juxtaposition to denote the operation in G and the operation in G/H . That is, we will write \clubsuit as

$$(Hx_1)(Hx_2) = H(x_1x_2)$$

On the other hand, if the operation in G is considered to be a form of “addition,” then we’ll write \clubsuit as

$$(H + x_1) + (H + x_2) = H + (x_1 + x_2)$$

Example 2: Refer to Example 1. Find:

- | | |
|---------------|---------------|
| (a) D_6/H_1 | (b) D_6/H_2 |
| (c) D_6/H_7 | (d) D_6/H_8 |

Solution: Before getting into the details, we compute the orders of these four factor groups. Note that

$$|D_6/H_1| = 2 = |D_6/H_2|, \quad |D_6/H_7| = 4, \quad \text{and} \quad |D_6/H_8| = 6$$

(a) Since D_6/H_1 has order 2, it is isomorphic to \mathbb{Z}_2 . We note that

$$D_6/H_1 = \{H_1, H_1s\}$$

Of course, if you answered that $D_6/H_1 = \{H_1r, H_1r^2s\}$, you are not wrong, since $H_1 = H_1r$ and $H_1s = H_1r^2s$.

(b) Likewise, $D_6/H_2 = \{H_2, H_2r\}$ is isomorphic to \mathbb{Z}_2 .

(c) Since D_6/H_7 has order 4, it is isomorphic to either \mathbb{Z}_4 or to $\mathbb{Z}_2 \times \mathbb{Z}_2$. First, note that $H_7r = \{r, r^3, r^5\} \in D_6/H_7$. Let's find $|H_7r|$ (the order of H_7r):

$$(H_7r)^2 = (H_7r)(H_7r) = H_7r^2 = H_7$$

Thus, $|H_7r| = 2$ and $\langle H_7r \rangle = \{H_7, H_7r\}$. Next, note that $s \notin H_7 \cup H_7r$, so $H_7s \neq H_7$ and $H_7s \neq H_7r$. Since the order of s in D_6 is 2, it follows from remark 4 above that $|H_7s| = 2$. Note that $H_7s = \{s, r^2s, r^4s\}$. Likewise, $H_7(rs) = \{rs, r^3s, r^5s\}$ has order 2 in D_6/H_7 . Therefore, $D_6/H_7 \cong \mathbb{Z}_2 \times \mathbb{Z}_2$. The complete operation table for D_6/H_7 is shown below.

	H_7	H_7r	H_7s	H_7rs
H_7	H_7	H_7r	H_7s	H_7rs
H_7r	H_7r	H_7	H_7rs	H_7s
H_7s	H_7s	H_7rs	H_7	H_7r
H_7rs	H_7rs	H_7s	H_7r	H_7

(d) **Exercise:** Show that $D_6/H_8 \cong D_3$. ■

Example 3: Consider the group $(\mathbb{Z}, +)$ and the subgroup $(8\mathbb{Z}, +)$, with

$$8\mathbb{Z} = \{\dots, -16, -8, 0, 8, 16, \dots\}$$

(the set of multiples of 8). Since the group \mathbb{Z} is abelian, $8\mathbb{Z} \triangleleft \mathbb{Z}$. What can we say about the factor group $\mathbb{Z}/8\mathbb{Z}$?

Solution: Since \mathbb{Z} is abelian, $\mathbb{Z}/8\mathbb{Z}$ is abelian by remark 3 above. Using left cosets rather than right cosets (which we can do, since $8\mathbb{Z} \triangleleft \mathbb{Z}$), we note that the distinct left cosets of $8\mathbb{Z}$ in \mathbb{Z} are:

$$\begin{aligned} 8\mathbb{Z} &= \{\dots, -16, -8, 0, 8, 16, \dots\} \\ 1 + 8\mathbb{Z} &= \{\dots, -15, -7, 1, 9, 17, \dots\} \\ 2 + 8\mathbb{Z} &= \{\dots, -14, -6, 2, 10, 18, \dots\} \\ 3 + 8\mathbb{Z} &= \{\dots, -13, -5, 3, 11, 19, \dots\} \\ 4 + 8\mathbb{Z} &= \{\dots, -12, -4, 4, 12, 20, \dots\} \\ 5 + 8\mathbb{Z} &= \{\dots, -11, -3, 5, 13, 21, \dots\} \\ 6 + 8\mathbb{Z} &= \{\dots, -10, -2, 6, 14, 22, \dots\} \\ 7 + 8\mathbb{Z} &= \{\dots, -9, -1, 7, 15, 23, \dots\} \end{aligned}$$

Thus, $\mathbb{Z}/8\mathbb{Z}$ is an abelian group of order 8, and thus is isomorphic to one of \mathbb{Z}_8 , $\mathbb{Z}_4 \times \mathbb{Z}_2$, or $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$.

We claim that $\mathbb{Z}/8\mathbb{Z} = \langle 1 + 8\mathbb{Z} \rangle$, and hence that $\mathbb{Z}/8\mathbb{Z} \cong \mathbb{Z}_8$. To see this, note that

$$\begin{aligned}(1 + 8\mathbb{Z})^2 &= (1 + 8\mathbb{Z}) + (1 + 8\mathbb{Z}) = 2 + 8\mathbb{Z} \\(1 + 8\mathbb{Z})^3 &= (1 + 8\mathbb{Z}) + (1 + 8\mathbb{Z})^2 = 3 + 8\mathbb{Z} \\&\vdots \\(1 + 8\mathbb{Z})^7 &= (1 + 8\mathbb{Z}) + (1 + 8\mathbb{Z})^6 = 7 + 8\mathbb{Z} \\(1 + 8\mathbb{Z})^8 &= (1 + 8\mathbb{Z}) + (1 + 8\mathbb{Z})^7 = 8\mathbb{Z}\end{aligned}$$

■

Generalizing Example 3, if n is an integer with $n > 1$, then

$$\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$$

Now let's see how factor groups can help us determine all the groups of some given order n , up to isomorphism. We begin with the fundamental theorem of finite abelian groups.

Theorem 4: Let n be a positive integer and let G be an abelian group of order n . Then either G is isomorphic to \mathbb{Z}_n (the cyclic group of order n), or G is isomorphic to a direct product of cyclic groups; in particular:

$$G \cong \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_k}$$

where n_1, n_2, \dots, n_k are positive integers, each greater than 1, such that

$$n = n_1 n_2 \cdots n_k \quad \text{and} \quad n_k \mid \cdots \mid n_2 \mid n_1$$

that is, for each integer i , $1 \leq i < k$, n_i is a multiple of n_{i+1} .

■

Before proving Theorem 4, let's give an example to get a better feel for what the theorem is saying.

Example 4: List the abelian groups of order 72, up to isomorphism.

Solution: Essentially, Theorem 4 says that any abelian group G of order 72 is a direct product of cyclic groups. If there is a single factor in this direct product, then $G \cong \mathbb{Z}_{72}$.

If there are two factors in the direct product, then $G \cong \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2}$ with $72 = n_1 n_2$, $n_2 > 1$, and n_1 a multiple of n_2 . So, we simply need to figure out the nontrivial ways to factor 72 (that is, don't use $72 \cdot 1$) so that the first factor is a multiple of the second factor. Doing so yields the following groups:

$$\mathbb{Z}_{36} \times \mathbb{Z}_2, \quad \mathbb{Z}_{24} \times \mathbb{Z}_3, \quad \mathbb{Z}_{12} \times \mathbb{Z}_6$$

Note that the group $\mathbb{Z}_{18} \times \mathbb{Z}_4$ is not listed. The simple reason, in view of the theorem, is that 18 is not a multiple of 4. The more subtle reason is this: in $\mathbb{Z}_{18} \times \mathbb{Z}_4$, the element $(1, 1)$ has order

$$\text{lcm}(18, 4) = 36$$

Thus, in fact, $\mathbb{Z}_{18} \times \mathbb{Z}_4 \cong \mathbb{Z}_{36} \times \mathbb{Z}_2$.

Next, we consider when there are three factors in the direct product. Here, we need to express 72 as $n_1 n_2 n_3$, with $n_3 > 1$, n_2 a multiple of n_3 , and n_1 a multiple of n_2 . Doing so yields the following groups:

$$\mathbb{Z}_{18} \times \mathbb{Z}_2 \times \mathbb{Z}_2 \quad \text{and} \quad \mathbb{Z}_6 \times \mathbb{Z}_6 \times \mathbb{Z}_2$$

What about four factors? We leave it as an exercise to show that there is no way to factor 72 as $n_1 n_2 n_3 n_4$ such that $n_4 > 1$, n_3 is a multiple of n_4 , n_2 is a multiple of n_3 , and n_1 is a multiple of n_2 .

In conclusion, up to isomorphism, there are precisely six abelian groups of order 72:

$$\mathbb{Z}_{72}, \quad \mathbb{Z}_{36} \times \mathbb{Z}_2, \quad \mathbb{Z}_{24} \times \mathbb{Z}_3, \quad \mathbb{Z}_{12} \times \mathbb{Z}_6, \quad \mathbb{Z}_{18} \times \mathbb{Z}_2 \times \mathbb{Z}_2, \quad \mathbb{Z}_6 \times \mathbb{Z}_6 \times \mathbb{Z}_2$$

■

Proof of Theorem 4: The proof is by induction on n . We already know that, if $n = 1$ or n is prime, then there is a unique abelian group of order n up to isomorphism, namely, \mathbb{Z}_n , so this anchors the induction.

Let n be an integer, $n \geq 4$, and assume the result of the theorem holds for any abelian group G' of order n' , $1 \leq n' < n$. Let G be an abelian group of order n with identity e . We first present an algorithm for expressing G as an internal direct product of subgroups of G .

Step 1. Select an element a_1 in G of maximum order n_1 , and let $H_1 = \langle a_1 \rangle$. If $H_1 = G$, then G is cyclic and we're done. If not, then let $G_1 = H_1$, let $i = 1$, and proceed to the next step.

Step 2. Select an element a_{i+1} in G of maximum order n_{i+1} such that

$$G_i \cap \langle a_{i+1} \rangle = \{e\}$$

(Exercise: Show that this can always be done.) Let $H_{i+1} = \langle a_{i+1} \rangle$ and $G_{i+1} = G_i H_{i+1} = H_1 \cdots H_i H_{i+1}$. If $G_{i+1} = G$, stop; otherwise, increment i and repeat Step 2.

Now then, suppose the algorithm terminates with $G = G_k = H_1 H_2 \cdots H_k$, $k \geq 2$. Then

$$H_1 \cap H_2 \cap \cdots \cap H_k = \{e\}$$

and so G is the internal direct product of H_1, H_2, \dots, H_k . It follows that $n = n_1 n_2 \cdots n_k$. We claim that G is isomorphic to

$$\mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_k}$$

with $n = n_1 n_2 \cdots n_k$ and n_i is a multiple of n_{i+1} for each integer $i, 1 \leq i < k$. It turns out that the orders n_1, n_2, \dots, n_k are those found by the algorithm, but for now let's just assume that $n_1 = |H_1|$, let $G' = H_2 \cdots H_k$, and let $n' = |G'|$.

Then G' is an abelian group of order less than n , and it follows by the induction hypothesis that G' is isomorphic to a direct product of cyclic groups, say

$$\mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_k}$$

with $n' = n_2 \cdots n_k$ and n_i is a multiple of n_{i+1} for each integer $i, 2 \leq i < k$. (Note: It is possible that $k = 2$, in which case G' is cyclic.) Let ϕ' denote the isomorphism.

Since $G = H_1 G'$ with $H_1 \cap G' = \{e\}$, we know that an element x in G can be uniquely expressed as a product of the form $a_1^t g$ with $0 \leq t < n_1$ and $g \in G'$. We define $\phi : G \rightarrow \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_k}$ by

$$\phi(x) = (t, \phi'(g))$$

(Technically, the image of ϕ is $\mathbb{Z}_{n_1} \times (\mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_k})$, but hey, close enough!) It is straightforward to show that ϕ is an isomorphism; see Exercise 14.

To complete the proof, it remains to show that n_1 is a multiple of n_2 . Suppose, to the contrary, that this is not the case, and let $a_2 = \phi^{-1}(0, 1, 0, \dots, 0)$. Then

$$\begin{aligned} |a_1 a_2| &= |\phi(a_1 a_2)| \\ &= |\phi(a_1) + \phi(a_2)| \\ &= |(1, 1, 0, \dots, 0)| \\ &= \text{lcm}(n_1, n_2, 1, \dots, 1) > n_1 \end{aligned}$$

This contradicts the choice of a_1 as an element of G with maximum order, and thus completes the proof. ■

Example 5: The group U_{56} is abelian. To what direct product of cyclic groups is it isomorphic?

Solution: The order of U_{56} is $\phi(56) = \phi(2^3 \cdot 7) = \phi(2^3)\phi(7) = 2^2 \cdot 6 = 2^3 \cdot 3 = 24$. Since $56 = 2^3 \cdot 7$ is not a prime power or twice a prime power, we know that U_{56} is not cyclic. Hence, U_{56} is isomorphic to one of the following abelian groups of order 24:

$$\mathbb{Z}_{12} \times \mathbb{Z}_2 \quad \text{or} \quad \mathbb{Z}_6 \times \mathbb{Z}_2 \times \mathbb{Z}_2$$

Checking the prime elements in U_{56} , we find that, for any $p \in \{3, 5, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 51, 53\}$,

$$p^6 = 1$$

It follows that, for any $x \in U_{56}$, $x^6 = 1$. For instance, let $x = 33$. Then

$$33^6 = (3 \cdot 11)^6 = 3^6 \cdot 11^6 = 1 \cdot 1 = 1$$

Hence, U_{56} has no elements of order 12, and so $U_{56} \cong \mathbb{Z}_6 \times \mathbb{Z}_2 \times \mathbb{Z}_2$.

If we follow the algorithm given in the proof of Theorem 6.4, we might choose $a_1 = 3$, $a_2 = 13$, and $a_3 = 29$. ■

The abelian groups U_n , $n \geq 2$, are important, so we provide an additional result concerning their structure. Define

$$\lambda(n) = \max\{|x| \mid x \in U_n\}$$

that is, $\lambda(n)$ is the maximum order among the elements of U_n . This function is known as *Carmichael's lambda function*, and $\lambda(n)$ is also called the *least universal exponent for n* , since $\lambda(n)$ is the smallest positive integer t with the property that

$$x^t = 1$$

for every element $x \in U_n$. We have the following result for computing λ .

Theorem 5: Let n and k be positive integers. Then:

1. $\lambda(2) = 1$ and $\lambda(4) = 2$.
2. $\lambda(2^k) = 2^{k-2}$ for $k \geq 3$.
3. If n is an odd prime power — that is, if $n = p^k$ for some odd prime p , then $\lambda(n) = \phi(n) = p^{k-1}(p-1)$.
4. If $n = n_1 n_2$ with $1 < n_1, n_2 \leq n$ and $\gcd(n_1, n_2) = 1$, then

$$\lambda(n) = \text{lcm}(\lambda(n_1)\lambda(n_2))$$
■

Example 6: Both U_{45} and U_{72} are abelian groups of order 24. Thus, by Theorem 4, each of these groups is isomorphic to

$$\mathbb{Z}_{24} \quad \text{or} \quad \mathbb{Z}_{12} \times \mathbb{Z}_2 \quad \text{or} \quad \mathbb{Z}_6 \times \mathbb{Z}_2 \times \mathbb{Z}_2$$

Apply Theorem 5 to determine which one.

Solution: For U_{45} , we have that

$$\lambda(45) = \lambda(5 \cdot 9) = \text{lcm}(\lambda(5), \lambda(9)) = \text{lcm}(\phi(5), \phi(9)) = \text{lcm}(4, 6) = 12$$

Therefore, $U_{45} \cong \mathbb{Z}_{12} \times \mathbb{Z}_2$.

For U_{72} , we have that

$$\lambda(72) = \lambda(8 \cdot 9) = \text{lcm}(\lambda(8), \lambda(9)) = \text{lcm}(2, 6) = 6$$

Therefore, $U_{72} \cong \mathbb{Z}_6 \times \mathbb{Z}_2 \times \mathbb{Z}_2$. ■

Next, we prove an important result concerning groups of order p^2 , with p a prime.

Theorem 6: Let G be a nonabelian group with center \mathcal{C}_G . Then G/\mathcal{C}_G is not cyclic.

Proof: Let G be a nonabelian group with center $\mathcal{C} = \mathcal{C}_G$ and suppose, to the contrary, that G/\mathcal{C}_G is cyclic. Then G/\mathcal{C}_G has a generator, say $\mathcal{C}b$, with $b \in G - \mathcal{C}$. Letting t denote the order $\mathcal{C}b$, we see that the distinct right cosets of \mathcal{C} in G are

$$\mathcal{C}, \quad \mathcal{C}b, \quad \mathcal{C}b^2, \quad \dots, \quad \mathcal{C}b^{t-1}$$

Let g_1 and g_2 be two arbitrary elements of G . Then $g_1 = z_1b^i$ and $g_2 = z_2b^j$ for some $z_1, z_2 \in \mathcal{C}$ and some integers i and j between 0 and $t - 1$. Hence,

$$g_1g_2 = (z_1b^i)(z_2b^j) = \dots = (z_2b^j)(z_1b^i) = g_2g_1$$

But this means that G is abelian, contradicting our assumption that G is not abelian. This completes the proof.

Exercise: Fill in the missing steps above. Hint: Use the fact that both z_1 and z_2 are in the center of G , and $b^ib^j = b^jb^i$. ■

Example 7: Let G be a nonabelian group of order 12. What can be said about G/\mathcal{C}_G ?

Solution: Well, since G is nonabelian, $\mathcal{C} = \mathcal{C}_G$ is a proper subgroup of G . Hence, the order of $\mathcal{C} = 1, 2, 3, 4,$ or 6 .

If $|\mathcal{C}| = 6$, then $|G/\mathcal{C}| = 2$, and it follows that $G/\mathcal{C} \cong \mathbb{Z}_2$. However, this is ruled out by Theorem 6. A similar argument can be used to show that $|\mathcal{C}| \neq 4$.

If $|\mathcal{C}| = 3$, then $|G/\mathcal{C}| = 4$. Again, by Theorem 6, it is impossible to have $G/\mathcal{C} \cong \mathbb{Z}_4$. Hence, $G/\mathcal{C} \cong K$, the Klein-four group.

If $|\mathcal{C}| = 2$, then $|G/\mathcal{C}| = 6$. Again, having $G/\mathcal{C} \cong \mathbb{Z}_6$ is ruled out by Theorem 6. Hence, $G/\mathcal{C} \cong D_3$. This is what actually happens when $G = D_6$ or $G = T$.

Finally, of course, if $|\mathcal{C}| = 1$, then $G/\mathcal{C} \cong G$. This is what actually happens when $G = A_4$. ■

Given a group G and a subgroup H of G , we know from Theorem 1 that $H \triangleleft G$ if and only if

$$ghg^{-1} \in H$$

for any elements h and g with $h \in H$ and $g \in G$. This suggests fixing an element $x \in G$ and looking at the set

$$\{gxg^{-1} \mid g \in G\}$$

This set is called the *conjugacy class* of x , and we want to show that the distinct conjugacy classes form a partition of G .

Recalling that partitions come from equivalence relations, we define the relation \sim on G by

$$x \sim y \leftrightarrow y = gxg^{-1} \text{ for some } g \in G$$

This relation is called *conjugacy*.

Example 8: Show that conjugacy is an equivalence relation on a group G . That is, show that conjugacy is:

- (a) reflexive: $x \sim x$ for any $x \in G$.
- (b) symmetric: For all $x, y \in G$, if $x \sim y$, then $y \sim x$
- (c) transitive: For all $x, y, z \in G$, if $x \sim y$ and $y \sim z$, then $x \sim z$.

Exercise: Show (a), (b), and (c). ■

Recall that, when we have an equivalence relation \sim on a set X , then the set of distinct equivalence classes is a partition of X , where the equivalence class containing x is

$$[x] = \{y \in X \mid x \sim y\} = \{y \in X \mid y \sim x\}$$

In the case of the conjugacy relation on a group G , the equivalence class containing x is

$$[x] = \{y \in G \mid x \sim y\} = \{gxg^{-1} \mid g \in G\}$$

We make the following remarks:

1. If e is the identity element of G , then $[e] = \{e\}$.
2. If g commutes with x , then $gxg^{-1} = x$. Hence, in computing $[x]$, we can ignore those elements g that commute with x ; in particular we can ignore $g \in \langle x \rangle$.
3. If \mathcal{C}_G denotes the center of G , then

$$x \in \mathcal{C}_G \leftrightarrow [x] = \{x\}$$

Hence, the notion of conjugacy is interesting only when the group G is nonabelian.

Example 9: Let's work out the conjugacy classes for several small nonabelian groups, namely:

- (a) D_3
- (b) D_4
- (c) Q

Solution: For (a), recall that

$$D_3 = \langle r, s \mid |r| = 3, |s| = 2, sr = r^2s \rangle$$

As remarked, $[e] = \{e\}$, and e is the only element in the center of D_3 . Let's find $[r]$:

$$\begin{aligned} srs^{-1} &= srs = r^2s^2 = r^2 \\ (rs)r(rs)^{-1} &= r(srs^{-1})r^{-1} = r(r^2)r^{-1} = r^2 \\ (r^2s)r(r^2s)^{-1} &= r^2(srs^{-1})(r^2)^{-1} = r^2(r^2)r = r^2 \end{aligned}$$

Hence, $[r] = \{r, r^2\} = [r^2]$. Next, let's find $[s]$:

$$\begin{aligned} rsr^{-1} &= rsr^2 = r(sr)r = r(r^2s)r = sr = r^2s \\ r^2s(r^2)^{-1} &= r^2sr = r^2(r^2s) = rs \end{aligned}$$

It follows that $[s] = \{s, rs, r^2s\}$. Therefore, using conjugacy classes, we obtain the following partition of D_3 :

$$D_3 = [e] \cup [r] \cup [s] = \{e\} \cup \{r, r^2\} \cup \{s, rs, r^2s\}$$

For (b), recall that

$$D_4 = \langle r, s \mid |r| = 4, |s| = 2, s \neq r^2, sr = r^3s \rangle$$

As mentioned in Example 1, the center of $D_4 = \{e, r^2\}$, so that $[e] = \{e\}$ and $[r^2] = \{r^2\}$. Let's find $[r]$:

$$\begin{aligned} srs^{-1} &= srs = r^3s^2 = r^3 \\ (rs)r(rs)^{-1} &= r(srs^{-1})r^{-1} = r(r^3)r^{-1} = r^3 \\ (r^2s)r(r^2s)^{-1} &= r^2(srs^{-1})(r^2)^{-1} = r^2(r^3)r^2 = r^3 \\ (r^3s)r(r^3s)^{-1} &= r^3(srs^{-1})(r^3)^{-1} = r^3(r^3)r = r^3 \end{aligned}$$

Hence, $[r] = \{r, r^3\}$. Next, let's find $[s]$:

$$\begin{aligned} rsr^{-1} &= rsr^3 = r(sr)r^2 = r(r^3s)r^2 = sr^2 = r^2s \\ r^3s(r^3)^{-1} &= r^3sr = r^3(r^3s) = r^2s \\ (rs)s(rs)^{-1} &= rsr^{-1} = rsr^3 = r^2s \\ (r^3s)s(r^3s)^{-1} &= r^3sr = r^2s \end{aligned}$$

Hence, $[s] = \{s, r^2s\}$. It follows from the remarks made above that $[rs] = \{rs, r^3s\}$.

Therefore, using conjugacy classes, we obtain the following partition of D_4 :

$$D_4 = [e] \cup [r] \cup [r^2] \cup [s] \cup [rs] = \{e\} \cup \{r, r^3\} \cup \{r^2\} \cup \{s, r^2s\} \cup \{rs, r^3s\}$$

(c) **Exercise:** Work out the conjugacy classes for the quaternion group Q . ■

Let G be a finite nonabelian group and let $x \in G$. We have noted that, in computing $[x]$, we can ignore those elements $g \in G$ that commute with x . This set of elements has a name. It is called the *centralizer of x in G* , and is denoted by $\mathcal{C}_G(x)$, or simply by \mathcal{C}_x if the group under consideration is understood.

Exercise: Show that \mathcal{C}_x is a subgroup of G .

Our next result relates the cardinality of the conjugacy class containing x to the index of the centralizer of x .

Theorem 7: Let G be a finite nonabelian group and let $x \in G$. Then

$$|[x]| = |G : \mathcal{C}_x| = \frac{|G|}{|\mathcal{C}_x|}$$

In words, the cardinality of the conjugacy class for x is equal to the index in G of the centralizer of x .

Proof: Recall that $|G : \mathcal{C}_x|$ is the number of left cosets of \mathcal{C}_x in G . Thus, to show that $|[x]|$ is equal to $|G : \mathcal{C}_x|$, it suffices to construct a bijection from $[x]$ to the set of left cosets of \mathcal{C}_x . We do this by mapping the conjugate gxg^{-1} of x to the left coset $g\mathcal{C}_x$.

First, since two conjugates of x can be the same element of G , we need to show that the mapping is well-defined. Well, for $g_1, g_2 \in G$,

$$\begin{aligned} g_1xg_1^{-1} = g_2xg_2^{-1} &\leftrightarrow g_2^{-1}g_1xg_1^{-1}g_2 = x \\ &\leftrightarrow g_2^{-1}g_1x(g_2^{-1}g_1)^{-1} = x \\ &\leftrightarrow g_2^{-1}g_1 \in \mathcal{C}_x \\ &\leftrightarrow g_1\mathcal{C}_x = g_2\mathcal{C}_x \end{aligned}$$

This shows that the mapping is well-defined, and also that it is one-to-one. The mapping is clearly onto, since the preimage of the left coset $g\mathcal{C}_x$ is the conjugate gxg^{-1} of x . This completes the proof. ■

The result of Theorem 7 can be written in the form

$$|[x]| |\mathcal{C}_x| = |G| \quad \blacklozenge$$

Thus, we see that, for a finite group, the cardinality of any conjugacy class is a factor of the order of G . Of course, \diamond is trivial when x belongs to the center of G , for in this case $[x] = \{x\}$ and $\mathcal{C}_x = G$.

Keep in mind that the distinct conjugacy classes of G form a partition of G . Hence, if G is a finite nonabelian group, we can write

$$|G| = \sum |[x]|$$

where the sum is over the distinct conjugacy classes of G . Letting \mathcal{C} be the center of G , we can then split the sum on the right into two sums:

$$|G| = \sum_{x \in \mathcal{C}} |[x]| + \sum_{x \notin \mathcal{C}} |[x]|$$

Of course, each term in the first sum is 1, and so the first sum is simply the order of \mathcal{C} . This yields the following important result.

Theorem 8 (Class Equation): Let G be a finite nonabelian group, let \mathcal{C} be the center of G , and, for $x \in G$, let \mathcal{C}_x be the centralizer of x . Then

$$|G| = |\mathcal{C}| + \sum |[x]| = |\mathcal{C}| + \sum |G : \mathcal{C}_x| \quad \heartsuit$$

where both sums are over the distinct conjugacy classes of G containing more than one element (that is, over those elements $x \in G - \mathcal{C}$). ■

The class equation is especially useful when the order a nonabelian group G is a power of some prime p — such groups are termed *p-groups*.

Corollary 9: Let p be a prime and let G be a nonabelian group with order a power of p . Then the center \mathcal{C} of G contains at least p elements.

Proof: Under the assumption that p is a prime and that the order of G is a power of p , consider the class equation \heartsuit . Note that p is a factor of $|G|$ and p is a factor of each term in the summation on the right-hand side (by relation \diamond). Thus, p must be a factor of $|\mathcal{C}|$, as well. ■

Corollary 10: Any group with order the square of a prime is abelian.

Proof: Let p be a prime and let G be a group of order p^2 . Suppose, to the contrary, that G is nonabelian. Then, by Corollary 6.9, the center \mathcal{C} of G has order p . But then $G/\mathcal{C} \cong \mathbb{Z}_2$, in violation of Theorem 6.5. This completes the proof. ■

We have noted that, up to isomorphism, there are two groups of order 4, \mathbb{Z}_4 and $\mathbb{Z}_2 \times \mathbb{Z}_2$, and two groups of order 9, \mathbb{Z}_9 and $\mathbb{Z}_3 \times \mathbb{Z}_3$. In light of Theorem 4 and Corollary 10, we can generalize. For any prime p , there are two groups of order p^2 , up to isomorphism:

$$\mathbb{Z}_{p^2} \quad \text{and} \quad \mathbb{Z}_p \times \mathbb{Z}_p$$

Additional Exercises

1. Determine the normal subgroups of D_4 .
2. Let $(G, *)$ be a group and let $(H, *)$ be a normal subgroup. Define the operation \otimes on the set G/H of right cosets of H in G by

$$Hx_1 \otimes Hx_2 = H(x_1 * x_2)$$

- (a) Show that \otimes is associative.
- (b) Let e denote the identity element of $(G, *)$. Show that $H = He$ is the identity element of $(G/H, \otimes)$.
- (c) For $x \in G$, let x^{-1} denote the inverse of x in $(G, *)$. Show that Hx^{-1} is the inverse of Hx in $(G/H, \otimes)$.

3. Determine the normal subgroups of Q .
4. Let G be a group and suppose G has a finite generating set $\{a_1, a_2, \dots, a_k\}$. Let H be a subgroup of G . Show that H is a normal subgroup of G if and only if

$$a_i h a_i^{-1} \in H$$

for each i , $1 \leq i \leq k$.

5. Determine the normal subgroups of D_5 .
6. Let G be a group and let H be a normal subgroup of G . Prove that, if x has finite order in G , then Hx has finite order in G/H , and the order of Hx in G/H is a factor of the order of x in G .
7. Determine the normal subgroups of A_4 .
8. Is Theorem 5 sufficient to determine, for any n , the structure of U_n as a direct product of cyclic groups?
9. With its usual presentation, the center of D_4 is $\mathcal{C} = \{e, r^2\}$. Describe the factor group D_4/\mathcal{C} .
10. Let G be a group and let H be a subgroup of G . For $g \in G$, define

$$gHg^{-1} = \{ghg^{-1} \mid h \in H\}$$

This set is called the *conjugate of H by g* . Show that H is a normal subgroup of G if and only if $gHg^{-1} = H$ for every $g \in G$.

11. With its usual presentation, the center of Q is $C = \{e, a^2\}$. Describe the factor group Q/C .

12. Apply Theorem 4 to show that, if G is an abelian group of order n , and if, for some prime p and some positive integer k , p^k is a factor of n , then G contains a subgroup of order p^k .

13. For $n \in \mathbb{Z}^+ - \{1\}$, recall that $n\mathbb{Z}$ denotes the set of multiples of n :

$$n\mathbb{Z} = \{\dots -3n, -2n, -n, 0, n, 2n, 3n, \dots\}$$

Since \mathbb{Z} is abelian, $n\mathbb{Z}$ is a normal subgroup of $(\mathbb{Z}, +)$. Show that the factor group $\mathbb{Z}/n\mathbb{Z}$ is isomorphic to \mathbb{Z}_n .

14. With reference to the proof of Theorem 4, verify that the mapping $\phi : G \rightarrow \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \dots \times \mathbb{Z}_{n_k}$ defined by

$$\phi(x) = (t, \phi'(g))$$

is an isomorphism.

15. Each of the following is a noncyclic abelian group of order 8. Determine whether it is isomorphic to $\mathbb{Z}_4 \times \mathbb{Z}_2$ or to $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$.

(a) U_{16}

(b) U_{20}

(c) U_{24}

16. List, up to isomorphism, all the abelian groups of order:

(a) 800

(b) 27783

17. Each of the following is an abelian group of order 12. Determine whether it is isomorphic to \mathbb{Z}_{12} or to $\mathbb{Z}_6 \times \mathbb{Z}_2$.

(a) U_{13}

(b) U_{28}

(c) U_{36}

18. List, up to isomorphism, the abelian groups of order 720.

19. Each of the following is a noncyclic abelian group of order 16. Determine whether it is isomorphic to $\mathbb{Z}_8 \times \mathbb{Z}_2$, or to $\mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_2$, or to $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$.

(a) U_{32}

(b) U_{40}

(c) U_{48}

20. Let n be a positive integer, $n > 1$, and suppose n has the canonical factorization

$$n = q_1^{t_1} q_2^{t_2} \cdots q_k^{t_k}$$

where $q_1 < q_2 < \dots < q_k$ are distinct primes and $t_1, t_2, \dots, t_k \in \mathbb{Z}^+$. Let $t = \max(t_1, t_2, \dots, t_k)$ and, for $1 \leq i \leq k$, let $p(t_i, t)$ be the number of partitions of t_i having t parts, with parts equal to zero allowed. For example, there are 5 partitions of 4 having 5 parts, with parts equal to zero allowed:

$$\begin{array}{lll} 4 + 0 + 0 + 0 + 0 & 3 + 1 + 0 + 0 + 0 & 2 + 2 + 0 + 0 + 0 \\ 2 + 1 + 1 + 0 + 0 & 1 + 1 + 1 + 1 + 0 & \end{array}$$

Show that the number of abelian groups of order n , up to isomorphism, is

$$\prod_{i=1}^k p(t_i, t)$$

Hint: Show that there is a one-to-one correspondence between k -tuples of the form (P_1, P_2, \dots, P_k) , with P_i a partition of t_i into t parts (with parts equal to zero allowed) and the distinct abelian groups of order n . When $n = 27783 = 3^4 7^3$, for example, we have $k = 2, t = 4, t_1 = 4$, and $t_2 = 3$. The pair of partitions

$$(2 + 1 + 1 + 0, 3 + 0 + 0 + 0)$$

of $t_1 = 4$ and $t_2 = 3$ into 4 parts corresponds to the direct product

$$\mathbb{Z}_{3^{2 \cdot 7^3}} \times \mathbb{Z}_{3^{1 \cdot 7^0}} \times \mathbb{Z}_{3^{1 \cdot 7^0}} \times \mathbb{Z}_{3^{0 \cdot 7^0}} \cong \mathbb{Z}_{3087} \times \mathbb{Z}_3 \times \mathbb{Z}_3$$

21. Let G be a group and let H be a normal subgroup of G . Prove or disprove: If H and G/H are both abelian, then G is abelian.
22. Consider the group G of nonzero real numbers under multiplication.
 - (a) Show that $N = \mathbb{R}^+$ is a normal subgroup of G .
 - (b) Show that $H = \{-1, 1\}$ is a subgroup of G .
 - (c) Show that $G/N \cong H$.
23. Are the groups U_{20} and U_{24} isomorphic? Explain.
24. Let G be a finite nonabelian group and consider the relation \sim of conjugacy on G . For $x, y \in G$, show that:
 - (a) If $x \sim y$, then $|x| = |y|$.
 - (b) If $x \sim y$, with $gxg^{-1} = y$ for $g \in G$, then $(y^k g)x(y^k g)^{-1} = y$ for any $k \in \mathbb{Z}^+$.
19. Apply the results of Exercise 24 to redo (more efficiently!) Example 9.