left coset and b_1, b_2 are in the same left coset, then a_1b_1 and a_2b_2 are in the same left coset. If this condition is satisfied for a subgroup $H \leq G$, we say that the operation on the left cosets of H is **induced** by the operation of G or that the operation of G **induces** an operation on the left cosets of H. In this case for any $a, b \in G$ we write

$$(aH)(bH) = (ab)H$$

to mean that the product of any element in aH multiplied by any element in bH must be in the left coset $(ab)H$.

12.2 Example We show that the operation $+$ in the group $\mathbb{Z}$ induces an operation on the cosets of $5\mathbb{Z} \leq \mathbb{Z}$. We first list the left cosets.

$$\begin{aligned} 5\mathbb{Z} &= \{\cdots - 10, -5, 0, 5, 10, \dots\} \\ 1 + 5\mathbb{Z} &= \{\cdots - 9, -4, 1, 6, 11, \dots\} \\ 2 + 5\mathbb{Z} &= \{\cdots - 8, -3, 2, 7, 12, \dots\} \\ 3 + 5\mathbb{Z} &= \{\cdots - 7, -2, 3, 8, 13, \dots\} \\ 4 + 5\mathbb{Z} &= \{\cdots - 6, -1, 4, 9, 14, \dots\} \end{aligned}$$

Let a_1 and a_2 be in the same left coset of $5\mathbb{Z}$. Then $a_2 = a_1 + 5r$ for some $r \in \mathbb{Z}$. We also let b_1, b_2 be in the same left coset of $5\mathbb{Z}$. Then $b_2 = b_1 + 5s$ for some $s \in \mathbb{Z}$. We compute $a_2 + b_2$.

$$\begin{aligned} a_2 + b_2 &= (a_1 + 5r) + (b_1 + 5s) \\ &= a_1 + 5r + b_1 + 5s \\ &= a_1 + b_1 + 5r + 5s && \textbf{(1)} \\ &= (a_1 + b_1) + 5(r + s) && \textbf{(2)} \\ &\in (a_1 + b_1) + 5\mathbb{Z} \end{aligned}$$

So $a_2 + b_2$ is in the same coset as $a_1 + b_1$, which says that addition in $\mathbb{Z}$ induces an operation on the five left cosets $5\mathbb{Z}, 1 + 5\mathbb{Z}, 2 + 5\mathbb{Z}, 3 + 5\mathbb{Z}, 4 + 5\mathbb{Z}$. Looking back at the calculations, we see that only properties shared by all groups were used in each step except in line (1) where we used the fact that $\mathbb{Z}$ is abelian. Furthermore, line (2) is not necessary since $5\mathbb{Z}$ is a subgroup of $\mathbb{Z}$ so we know that $5\mathbb{Z}$ is closed under addition. From this example, it appears that as long as G is an abelian group, the operation of G induces an operation on the left cosets of any subgroup of G. ▲

In Equation (1) of Example 12.2 we used the fact that $5r + b_1 = b_1 + 5r$. If we were doing the same computation in multiplicative notation and using any group G and subgroup H of G, this would correspond to $hb_1 = b_1h$. If the group G is not abelian, then this computation fails. However, we can weaken the abelian condition slightly and still get an induced operation on the left cosets. All we really need is that $hb_1 = b_1h'$ for some $h' \in H$. This happens when the left coset b_1H is the same set as the right coset Hb_1.

12.3 Definition Let H be a subgroup of G. We say that H is a **normal** subgroup of G if for all $g \in G$, $gH = Hg$. If H is a normal subgroup of G, we write $H \trianglelefteq G$. ■

Recall that Theorem 10.17 states that if $\phi : G \to G'$ is a group homomorphism and e' is the identity element in G', then $\text{Ker}(\phi) = \{g \in G \mid \phi(g) = e'\}$ has the property that left and right cosets of $\text{Ker}(\phi)$ are the same. So the kernel of any homomorphism is a normal subgroup.

12.4 Example The subgroup of even permutations $A_n \leq S_n$ is normal since A_n is the kernel of the homomorphism $\text{sgn} : S_n \to \{1, -1\}$. ▲

12.5 Example If $H \leq G$ and G is an abelian group, then H is a normal subgroup of G. ▲

12.6 Example Let $H = \{A \in \mathrm{GL}(n, \mathbb{R}) \mid \det(A) = 1\}$. The determinant map satisfies $\det(AB) = \det(A)\det(B)$, which means that the determinant map is a homomorphism, $\det : \mathrm{GL}(n, \mathbb{R}) \to \mathbb{R}^*$. Thus $H = \mathrm{Ker}(\det)$, which says that $H \trianglelefteq \mathrm{GL}(n, \mathbb{R})$. This subgroup H is called the **special linear group** and it is denoted by $\mathrm{SL}(n, \mathbb{R})$. ▲

12.7 Theorem Let H be a subgroup of a group G. Then left coset multiplication is well defined by the equation

$$(aH)(bH) = (ab)H$$

if and only if H is a normal subgroup of G.

Proof Suppose first that $(aH)(bH) = (ab)H$ does give a well-defined binary operation on left cosets. Let $a \in G$. We want to show that aH and Ha are the same set. We use the standard technique of showing that each is a subset of the other.

Let $x \in aH$. Choosing representatives $x \in aH$ and $a^{-1} \in a^{-1}H$, we have $(xH)(a^{-1}H) = (xa^{-1})H$. On the other hand, choosing representatives $a \in aH$ and $a^{-1} \in a^{-1}H$, we see that $(aH)(a^{-1}H) = eH = H$. Using our assumption that left coset multiplication by representatives is well defined, we must have $xa^{-1} = h \in H$. Then $x = ha$, so $x \in Ha$ and $aH \subseteq Ha$. We leave the symmetric proof that $Ha \subseteq aH$ to Exercise 26.

We turn now to the converse: If H is a normal subgroup, then left coset multiplication by representatives is well-defined. Due to our hypothesis, we can simply say *cosets,* omitting *left* and *right*. Suppose we wish to compute $(aH)(bH)$. Choosing $a \in aH$ and $b \in bH$, we obtain the coset $(ab)H$. Choosing different representatives $ah_1 \in aH$ and $bh_2 \in bH$, we obtain the coset ah_1bh_2H. We must show that these are the same cosets. Now $h_1b \in Hb = bH$, so $h_1b = bh_3$ for some $h_3 \in H$. Thus

$$(ah_1)(bh_2) = a(h_1b)h_2 = a(bh_3)h_2 = (ab)(h_3h_2)$$

and $(ab)(h_3h_2) \in (ab)H$. Therefore, ah_1bh_2 is in $(ab)H$. ◆

Theorem 12.7 shows that we have an operation on the left cosets of $H \leq G$ induced by the operation on G if and only if H is a normal subgroup of G. We next verify that this operation makes G/H, the cosets of H in G, a group.

12.8 Corollary Let H be a normal subgroup of G. Then the cosets of H form a group G/H under the binary operation $(aH)(bH) = (ab)H$. ▲

Proof Computing, $(aH)[(bH)(cH)] = (aH)[(bc)H] = [a(bc)]H$, and similarly, we have $[(aH)(bH)](cH) = [(ab)c]H$, so associativity in G/H follows from associativity in G. Because $(aH)(eH) = (ae)H = aH = (ea)H = (eH)(aH)$, we see that $eH = H$ is the identity element in G/H. Finally, $(a^{-1}H)(aH) = (a^{-1}a)H = eH = (aa^{-1})H = (aH)(a^{-1}H)$ shows that $a^{-1}H = (aH)^{-1}$. ◆

12.9 Definition The group G/H in the preceding corollary is the **factor group** (or **quotient group**) of G by H. ■

12.10 Example Since $\mathbb{Z}$ is an abelian group, $n\mathbb{Z}$ is a normal subgroup. Corollary 12.8 allows us to construct the factor group $\mathbb{Z}/n\mathbb{Z}$. For any integer m, the division algorithm says that $m = nq + r$ for some $0 \leq r < n$. Therefore, $m \in r + n\mathbb{Z}$. So $\mathbb{Z}/n\mathbb{Z} = \{k + n\mathbb{Z} \mid 0 \leq k < n\}$. Thus $\langle 1 + n\mathbb{Z}\rangle = \mathbb{Z}/n\mathbb{Z}$, which implies that $\mathbb{Z}/n\mathbb{Z}$ is cyclic and isomorphic with $\mathbb{Z}_n$. ▲

12.11 Example Consider the abelian group $\mathbb{R}$ under addition, and let $c \in \mathbb{R}^+$. The cyclic subgroup $\langle c \rangle$ of $\mathbb{R}$ contains as elements

$$\cdots - 3c, -2c, -c, 0, c, 2c, 3c, \cdots .$$

Every coset of $\langle c \rangle$ contains just one element x such that $0 \leq x < c$. If we choose these elements as representatives of the cosets when computing in $\mathbb{R}/\langle c \rangle$, we find that we are computing their sum modulo c as discussed for the computation in $\mathbb{R}_c$ in Section 3. For example, if $c = 5.37$, then the sum of the cosets $4.65 + \langle 5.37 \rangle$ and $3.42 + \langle 5.37 \rangle$ is the coset $8.07 + \langle 5.37 \rangle$, which contains $8.07 - 5.37 = 2.7$, which is $4.65 +_{5.37} 3.42$. Working with these coset elements x where $0 \leq x < c$, we thus see that the group $\mathbb{R}_c$ of Section 3 is isomorphic to $\mathbb{R}/\langle c \rangle$ under an isomorphism ψ where $\psi(x) = x + \langle c \rangle$ for all $x \in \mathbb{R}_c$. Of course, $\mathbb{R}/\langle c \rangle$ is then also isomorphic to the circle group U of complex numbers of magnitude 1 under multiplication. ▲

We have seen that the group $\mathbb{Z}/\langle n \rangle$ is isomorphic to the group $\mathbb{Z}_n$, and as a set, $\mathbb{Z}_n = \{0, 1, 3, 4, \cdots, n-1\}$, the set of nonnegative integers less than n. Example 12.11 shows that the group $\mathbb{R}/\langle c \rangle$ is isomorphic to the group $\mathbb{R}_c$. In Section 3, we choose the notation $\mathbb{R}_c$ rather than the conventional $[0, c)$ for the half-open interval of nonnegative real numbers less than c. We did that to bring out now the comparison of these factor groups of $\mathbb{Z}$ with these factor groups of $\mathbb{R}$.

Homomorphisms and Factor Groups

We learned that the kernel of any homomorphism $\phi : G \to G'$ is a normal subgroup of G. Do all normal subgroups arise in this way? That is, for any normal subgroup $H \trianglelefteq G$, is there a group homomorphism $\phi : G \to G'$ for some group G' such that H is the kernel of G? The answer to the question is yes as we see in Theorem 12.12.

12.12 Theorem Let H be a normal subgroup of G. Then $\gamma : G \to G/H$ given by $\gamma(x) = xH$ is a homomorphism with kernel H.

Proof Let $x, y \in G$. Then

$$\gamma(xy) = (xy)H = (xH)(yH) = \gamma(x)\gamma(y),$$

so γ is a homomorphism. Since $xH = H$ if and only if $x \in H$, we see that the kernel of γ is indeed H. ◆

Since the kernel of any homomorphism $\phi : G \to G'$ is a normal subgroup, it is natural to ask how the factor group $G/\text{Ker}(\phi)$ is related to G'. Theorem 12.12 and the next example illustrate that there is a very strong connection.

12.13 Example **(Reduction Modulo *n*)** Let $\phi : \mathbb{Z} \to \mathbb{Z}_n$ be defined by letting $\phi(m)$ be the remainder when m is divided by n. We check that ϕ is a group homomorphism. Let $m_1, m_2 \in \mathbb{Z}$ and suppose that the division algorithm gives us

$$m_1 = nq_1 + r_1 \qquad \text{and}$$
$$m_2 = nq_2 + r_2.$$

Then $m_1 + m_2 = n(q_1 + q_2) + r_1 + r_2$. If $r_1 + r_2 < n$, then

$$\phi(m_1 + m_2) = r_1 + r_2 = \phi(m_1) +_n \phi(m_2).$$

On the other hand, if $r_1 + r_2 \geq n$, then $m_1 + m_2 = n(q_1 + q_2 + 1) + (r_1 + r_2 - n)$ and $0 \leq r_1 + r_2 - n < n$, which implies

$$\phi(m_1 + m_2) = r_1 + r_2 - n = \phi(m_1) +_n \phi(m_2).$$

The kernel of ϕ is the set of all the multiples of n, $n\mathbb{Z}$. So $\mathbb{Z}/\text{Ker}(\phi) = \mathbb{Z}/n\mathbb{Z}$, which is isomorphic to $\mathbb{Z}_n$. ▲

The previous example is a special case of the Fundamental Homomorphism Theorem.

12.14 Theorem **(The Fundamental Homomorphism Theorem)** Let $\phi : G \to G'$ be a group homomorphism with kernel H. Then $\phi[G]$ is a group, and $\mu : G/H \to \phi[G]$ given by $\mu(gH) = \phi(g)$ is an isomorphism. If $\gamma : G \to G/H$ is the homomorphism given by $\gamma(g) = gH$, then $\phi(g) = \mu \circ \gamma(g)$ for each $g \in G$.

Proof Theorem 8.5 says that $\phi[G]$ is a subgroup of G'. Theorem 10.17 shows that the map $\mu : G/H \to \phi[G]$ is well defined. We show μ is a homomorphism. Let $aH, bH \in G/H$. Then $\mu((aH)(bH)) = \mu((ab)H) = \phi(ab) = \phi(a)\phi(b) = \mu(aH)\mu(bH)$. Since ϕ maps G onto $\phi[G]$, μ maps G/H onto $\phi[G]$. To show that μ is one-to-one, we compute the kernel of μ. Since $\mu(aH) = \phi(a)$, the kernel of μ is $\{aH \mid \phi(a) = e'\}$. But $\phi(a) = e'$ if and only if $a \in \text{Ker}(\phi) = H$. So $\text{Ker}(\mu) = \{H\}$ which is the trivial subgroup of G/H. By Corollary 10.19 μ is one-to-one, which completes the proof that μ is an isomorphism.

We next turn to the final statement of the theorem. Let $g \in G$. Then

$$\phi(g) = \mu(gH) = \mu(\gamma(g)) = \mu \circ \gamma(g).$$

◆

The Fundamental Homomorphism Theorem is sometimes called the First Isomorphism Theorem. As the name suggests, there are other related theorems. In fact we will prove two others, the Second Isomorphism Theorem and the Third Isomorphism Theorem, in Section 16.

Theorem 12.14 states that $\phi(g) = \mu \circ \gamma(g)$. This can be visualized in Figure 12.15. If we start with an element $g \in G$, and map it to $\phi(g)$, we get the same result as first mapping g to $\gamma(g)$ and then mapping $\gamma(g)$ to $\mu \circ \gamma(g)$. When we have a situation like this, we say that the map ϕ can be *factored* as $\phi = \mu \circ \gamma$.

The isomorphism μ in Theorem 12.14 is referred to as a *natural* or *canonical* isomorphism, and the same adjectives are used to describe the homomorphism γ. There may be other isomorphisms and homomorphisms for these same groups, but the maps μ and γ have a special status with ϕ and are uniquely determined by Theorem 12.14.

In summary, every homomorphism with domain G gives rise to a factor group G/H, and every factor group G/H gives rise to a homomorphism mapping G into G/H. Homomorphisms and factor groups are closely related. We give an example indicating how useful this relationship can be.

$$\begin{tikzcd}
G \arrow[rr, "\phi"] \arrow[dr, "\gamma_K"'] & & \phi[G] \\
& G/K \arrow[ur, dashed, "\mu\text{ (isomorphism)}"'] &
\end{tikzcd}$$

12.15 Figure