8.3 Example Recall that $U_n = \{z \in \mathbb{C} \mid z^n = 1\}$. Let $\phi : U_{28} \to U_4$ be given by $\phi(z) = z^7$. To check that ϕ is well defined, we see that if $z \in U_{28}$, then $z^{28} = 1$. Therefore, $(z^7)^4 = 1$, which implies that $z^7 \in U_4$. We check that ϕ is a homomorphism.

$$\phi(z_1 z_2) = (z_1 z_2)^7 = z_1^7 z_2^7 = \phi(z_1)\phi(z_2).$$

As in the previous example, ϕ maps the identity in U_{28}, in this case 1, to the identity 1 in U_4. Furthermore,

$$\phi(z^{-1}) = z^{-7} = (z^7)^{-1} = (\phi(z))^{-1}. \quad \blacktriangle$$

8.4 Definition Let $\phi : X \to Y$ and suppose that $A \subseteq X$ and $B \subseteq Y$. The set $\phi[A] = \{\phi(a) \mid a \in A\}$ is called the **image of A in Y under the mapping ϕ.** The set $\phi^{-1}[B] = \{a \in A \mid \phi(a) \in B\}$ is called the **inverse image of B under the mapping ϕ.** ■

The four properties of a homomorphism given in the theorem that follows are obvious in the case of an isomorphism since we think of an isomorphism as simply relabeling the elements of a group. However, it is not obvious that these properties hold for all homomorphisms whether or not they are one-to-one or onto maps. Consequently, we give careful proofs of all four properties.

8.5 Theorem Let ϕ be a homomorphism of a group G into a group G'.

1. If e is the identity element in G, then $\phi(e)$ is the identity element e' in G'.
2. If $a \in G$, then $\phi(a^{-1}) = \phi(a)^{-1}$.
3. If H is a subgroup of G, then $\phi[H]$ is a subgroup of G'.
4. If K' is a subgroup of G', then $\phi^{-1}[K']$ is a subgroup of G.

Loosely speaking, ϕ preserves the identity element, inverses, and subgroups.

Proof Let ϕ be a homomorphism of G into G'. Then

$$\phi(e) = \phi(ee) = \phi(e)\phi(e).$$

Multiplying on the left by $\phi(e)^{-1}$, we see that $e' = \phi(e)$. Thus $\phi(e)$ must be the identity element e' in G'. The equation

$$e' = \phi(e) = \phi(aa^{-1}) = \phi(a)\phi(a^{-1})$$

shows that $\phi(a^{-1}) = \phi(a)^{-1}$ for all $a \in G$.

Turning to Statement (3), let H be a subgroup of G, and let $\phi(a)$ and $\phi(b)$ be any two elements in $\phi[H]$. Then $\phi(a)\phi(b) = \phi(ab)$, so we see that $\phi(a)\phi(b) \in \phi[H]$; thus, $\phi[H]$ is closed under the operation of G'. The fact that $e' = \phi(e)$ and $\phi(a^{-1}) = \phi(a)^{-1}$ completes the proof that $\phi[H]$ is a subgroup of G'.

Going the other way for Statement (4), let K' be a subgroup of G'. Suppose a and b are in $\phi^{-1}[K']$. Then $\phi(a)\phi(b) \in K'$ since K' is a subgroup. The equation $\phi(ab) = \phi(a)\phi(b)$ shows that $ab \in \phi^{-1}[K']$. Thus $\phi^{-1}[K']$ is closed under the binary operation in G. Also, K' must contain the identity element $e' = \phi(e)$, so $e \in \phi^{-1}[K']$. If $a \in \phi^{-1}[K']$, then $\phi(a) \in K'$, so $\phi(a)^{-1} \in K'$. But $\phi(a)^{-1} = \phi(a^{-1})$, so we must have $a^{-1} \in \phi^{-1}[K']$. Hence $\phi^{-1}[K']$ is a subgroup of G. ◆

Let $\phi : G \to G'$ be a homomorphism and let e' be the identity element of G'. Now $\{e'\}$ is a subgroup of G', so $\phi^{-1}[\{e'\}]$ is a subgroup H of G by Statement (4) in Theorem 8.5. This subgroup is critical to the study of homomorphisms.

8.6 Definition Let $\phi : G \to G'$ be a homomorphism of groups. The subgroup $\phi^{-1}[\{e'\}] = \{x \in G \mid \phi(x) = e'\}$ is the **kernel of ϕ**, denoted by $\text{Ker}(\phi)$. ■

We will use the kernel of a homomorphism when we define the alternating group later in this section.

Another extreme is to let $H = G$ in Statement (3) of Theorem 8.5. In this case, the theorem says that $\phi[G]$ is a subgroup of G'. We use this in the proof of Cayley's Theorem.

8.7 Example In Example 8.2, the homomorphism $\phi : \mathbb{R} \to U$ is defined by $\phi(x) = \cos(2\pi x) + i\sin(2\pi x) = e^{2\pi ix}$. The kernel of ϕ is the set of integers since $\cos(2\pi x) + i\sin(2\pi x) = 1$ if and only if x is an integer.

Let n be a positive integer. Then $\left\langle \frac{1}{n} \right\rangle$ is a subgroup of $\mathbb{R}$ and

$$\begin{aligned}\phi\left[\left\langle \frac{1}{n} \right\rangle\right] &= \phi\left[\left\{ \frac{m}{n} \mid m \in \mathbb{Z} \right\}\right] \\ &= \{\cos(2\pi m/n + i\sin(2\pi m/n)) \mid m \in \mathbb{Z}\} \\ &= U_n.\end{aligned}$$

▲

8.8 Example Let $\phi : \mathbb{Z}_n \to D_n$ be given by $\phi(k) = \rho^k$. We check that ϕ is a homomorphism. Let $a, b \in \mathbb{Z}_n$. If $a + b < n$, then $a +_n b = a + b$, so $\phi(a +_n b) = \phi(a + b) = \rho^{a+b} = \rho^a\rho^b = \phi(a)\phi(b)$. If $a + b \geq n$, then $\phi(a +_n b) = \phi(a + b - n) = \rho^{a+b-n} = \rho^a\rho^b\rho^{-n} = \rho^a\rho^b = \phi(a)\phi(b)$. The image $\phi[\mathbb{Z}_n]$ is $\langle\rho\rangle$. ▲

Cayley's Theorem

Each of the groups we have seen so far is isomorphic to a subgroup of permutations on some set. For example, $\mathbb{Z}_n$ is isomorphic with the cyclic group $\langle(1, 2, 3, \ldots, n)\rangle \leq S_n$. The dihedral group D_n is defined to be the permutations in $S_{\mathbb{Z}_n}$ with the property that the line segment between vertices i and j is an edge in P_n, a regular n-gon, if and only if the line segment between the images of i and j is also an edge. The infinite group $\mathrm{GL}(n, \mathbb{R})$ can be thought of as invertible linear transformations of $\mathbb{R}^n$. Each element of $\mathrm{GL}(n, \mathbb{R})$ permutes the vectors in $\mathbb{R}^n$, which makes $\mathrm{GL}(n, \mathbb{R})$ isomorphic with a permutation group on vectors in $\mathbb{R}^n$. We refer to a subgroup of a permutation group as a **group of permutations**. Cayley's Theorem states that any group is isomorphic with a group of permutations.

At first Cayley's Theorem seems like a remarkable result that could be used to understand all groups. In fact, this is a nice and intriguing classic result. Unfortunately, approaching group theory by trying to determine all possible permutation groups is not feasible. On the other hand, Cayley's theorem does show the strength and generality of permutation groups and it deserves a special place in group theory for that reason. For example, if we wish to find a counterexample to a conjecture about groups, provided that there is one, it will occur in a permutation group.

It may seem a mystery how we could start with an arbitrary group and come up with a permutation group that is isomorphic with the given group. The key is to think about the group table. Each row contains each element of the group exactly once. So each row defines a permutation of the elements of the group by placing the table head as the top row in the two-row representation of a permutation and placing the row corresponding to an element a in the group as the bottom row. Table 8.9 is the group table for D_3. Note that the permutation obtained using the row $\mu\rho$ is

$$\begin{pmatrix} \iota & \rho & \rho^2 & \mu & \mu\rho & \mu\rho^2 \\ \mu\rho & \mu\rho^2 & \mu & \rho^2 & \iota & \rho \end{pmatrix}.$$