from: Intro to Abstract Algebra, 2nd Edition
W. K. Nicholson J. Wiley (1999).

30. Let $G = \langle g \rangle$ where $|g| = n$. Given $g^k \in G$, show $\langle g^k \rangle = \langle g^d \rangle$, where $d = \gcd(k, n)$. [*Hint:* Theorem 3 §1.2.]
31. Let $G = \langle g \rangle$ be a cyclic group and let $A = \langle g^a \rangle$ and $B = \langle g^b \rangle$.
    (a) If $|g| = \infty$, show that $A \cap B = \langle g^m \rangle$, where $m = \text{lcm}(a, b)$.
    (b) If $|g| = n$, assume (Theorem 7) that $a|n$ and $b|n$. Show again that $A \cap B = \langle g^m \rangle$, where $m = \text{lcm}(a, b)$.
32. Show that the following conditions are equivalent for a finite group G.
    (1) G is cyclic and $|G| = p^n$, where p is a prime and $n \geq 0$.
    (2) If H and K are subgroups of G, either $H \subseteq K$ or $K \subseteq H$.
    [*Hint:* For (1) $\Rightarrow$ (2) use Theorem 7.]
33. If a group G has a finite number of subgroups, show that G must be finite.
34. Prove the **Chinese Remainder Theorem**. Let $n_1, n_2, \ldots, n_r$ be positive integers, relatively prime in pairs. Given integers $m_1, m_2, \ldots, m_r$, show that there exists $m \in \mathbb{Z}$ such that $m_i \equiv m \pmod{n_i}$ for each i. [*Hint:* Extend Exercise 25 to r groups.]
35. (a) Let $|a| = m$ and $|b| = n$ in a group G. If $ab = ba$, show that an element $c \in G$ exists, with $|c| = \text{lcm}(m, n)$. [*Hint:* Theorem 9 §1.2, Theorem 7, and Exercise 26(a).]
    (b) Let G be an abelian group and assume that G has an element of maximal order n (always true if G is finite). Show that $g^n = 1$ for all $g \in G$. [*Hint:* Part (a).]
36. Let m be the smallest positive integer such that $\sigma^m = \varepsilon$ for all $\sigma \in S_n$. Show that $m = \text{lcm}(2, 3, 4, 5, \ldots, n)$.
37. For a deck of $2n$ distinct cards, a "perfect shuffle" means cutting the deck into two equal halves and collating them as follows: If the cards were originally in the order $1, 2, 3, 4, \ldots, 2n$, they end up in the order $1, n+1, 2, n+2, \ldots, n, 2n$. In each case, determine the number of perfect shuffles required to bring the deck back into its original order.
    (a) $n = 4, 5, 6$, and 7
    (b) $n = 8, 9$, and 10
    (c) $n = 12$
    (d) $n = 26$ (a regular deck)

2.5 HOMOMORPHISMS AND ISOMORPHISMS

Mathematicians do not deal in objects, but in relations among objects; they are free to replace some objects by others so long as the relations remain unchanged. Content to them is irrelevant: they are interested in form only.

—Henri Poincaré

Up to this point we have paid no attention to mappings from one group to another. Most such mappings are of little interest; the interesting ones are those that *preserve* the group multiplication in the following sense: If G and G_1 are groups, a mapping $\alpha : G \to G_1$ is called a **homomorphism**[6] if

[6]Homomorphisms were first used explicitly (for permutation groups) by Jordan in 1870.

$$\alpha(ab) = \alpha(a) \cdot \alpha(b) \text{ for all } a \text{ and } b \text{ in } G.$$

Note that in this case the product ab is in G while $\alpha(a) \cdot \alpha(b)$ is in G_1.

Example 1. The mapping $\alpha : \mathbb{Z} \to \mathbb{Z}$ given by $\alpha(a) = 3a$ is a homomorphism of additive groups because $\alpha(a + b) = 3(a + b) = 3a + 3b = \alpha(a) + \alpha(b)$ for all $a, b \in \mathbb{Z}$.

Example 2. If a is an element of a group G, define the **exponent map** $\alpha : \mathbb{Z} \to \langle a \rangle$ by $\alpha(k) = a^k$ for all $k \in \mathbb{Z}$. Then α is an (onto) homomorphism because (as the operation in $\mathbb{Z}$ is addition)

$$\alpha(k + m) = a^{k+m} = a^k a^m = \alpha(k) \cdot \alpha(m) \qquad \text{for all } k, m \in \mathbb{Z}.$$

Example 3. Let $\mathbb{R}^+$ denote the group of positive real numbers under multiplication. The absolute value map $\alpha : \mathbb{C}^* \to \mathbb{R}^+$ given by $\alpha(z) = |z|$ for all $z \in \mathbb{C}^*$ is a homomorphism (in fact, onto) by virtue of the fact that $|zw| = |z||w|$ for all $z, w \in \mathbb{C}$.

Example 4. Let $GL_n(\mathbb{R})$ denote the general linear group of $n \times n$ invertible matrices over $\mathbb{R}$. The determinant map $GL_n(\mathbb{R}) \to \mathbb{R}^*$ given by $A \mapsto \det A$ is a homomorphism (onto) because $\det(AB) = \det A \det B$ for all matrices A and B (and $\det A \neq 0$ if A is invertible). If $n = 2$, determinants are defined explicitly in Appendix B.

Example 5. The identity map $1_G : G \to G$ is a homomorphism for any group G because $1_G(ab) = ab = 1_G(a) \cdot 1_G(b)$ for all a, b in G.

Example 6. For groups G and G_1, there is always at least one homomorphism from G to G_1, the **trivial homomorphism** $\alpha : G \to G_1$ defined by $\alpha(g) = 1$ for all $g \in G$.

Example 7. Let $G = G_1 \times G_2$ be a direct product of groups. We define

$$\pi_1 : G \to G_1 \quad \text{by} \quad \pi_1(g_1, g_2) = g_1$$
$$\sigma_1 : G_1 \to G \quad \text{by} \quad \sigma_1(g_1) = (g_1, 1)$$

Then π_1 is an onto homomorphism as the reader can verify (called the **projection** onto G_1), and σ_1 is a one-to-one homomorphism (called the **injection** of G_1 into G). Similarly there is a projection onto G_2, and an injection of $G_2 \to G$.

Example 8. If $\alpha : G \to H$ and $\beta : H \to K$ are homomorphisms, show that the composite map $\beta\alpha : G \to K$ is also a homomorphism.

Solution. This is because, for all a and b in G,

$$\beta\alpha(ab) = \beta[\alpha(ab)] = \beta[\alpha(a)\cdot\alpha(b)] = \beta[\alpha(a)]\cdot\beta[\alpha(b)] = \beta\alpha(a)\cdot\beta\alpha(b). \quad \square$$

A homomorphism $\alpha : G \to G_1$ is a mapping that preserves the operation in the sense that $\alpha(ab) = \alpha(a)\alpha(b)$ for all a and b in G. Theorem 1 shows that α also preserves the identity, inverses, and powers.

Theorem 1. *Let $\alpha : G \to G_1$ be a homomorphism. Then:*
(1) $\alpha(1) = 1$. *(α preserves the identity element)*
(2) $\alpha(g^{-1}) = \alpha(g)^{-1}$ *for all* $g \in G$. *(α preserves inverses)*
(3) $\alpha(g^k) = \alpha(g)^k$ *for all* $g \in G$ *and* $k \in \mathbb{Z}$. *(α preserves powers)*

Proof. (1). Here $\alpha(1)\cdot\alpha(1) = \alpha(1^2) = \alpha(1)$, so cancellation in G_1 gives (1).
(2). From (1), $\alpha(g^{-1})\cdot\alpha(g) = \alpha(g^{-1}g) = \alpha(1) = 1$, which gives (2).
(3). If $k = 0$ then $\alpha(g^0) = \alpha(1) = 1 = [\alpha(g)]^0$ by (1). If (3) holds for some $k \geq 0$, then

$$\alpha(g^{k+1}) = \alpha(gg^k) = \alpha(g)\cdot\alpha(g^k) = \alpha(g)\cdot[\alpha(g)]^k = [\alpha(g)]^{k+1}.$$

Hence (3) holds for $k \geq 0$ by induction. If $k < 0$, write $k = -m$, $m > 0$. Then (2) and the preceding calculation give

$$\alpha(g^k) = \alpha[(g^m)^{-1}] = [\alpha(g^m)]^{-1} = [\alpha(g)^m]^{-1} = [\alpha(g)]^k.$$

Thus $[\alpha(g)]^k = \alpha(g^k)$ for all $k \in \mathbb{Z}$. ■

Corollary. *Let $\alpha : G \to H$ be a homomorphism. If $g \in G$ has finite order, then $\alpha(g)$ also has finite order, and $|\alpha(g)|$ divides $|g|$.*

Proof. If $|g| = n$ then $g^n = 1$, so $\alpha(g)^n = \alpha(g^n) = \alpha(1) = 1$. Hence $|\alpha(g)|$ divides n by Theorem 2 §2.4. ■

Let G and G_1 denote groups. In order to show that two mappings $\alpha : G \to G_1$ and $\beta : G \to G_1$ are equal, we must verify that $\alpha(g) = \beta(g)$ holds for all $g \in G$. However, if α and β are homomorphisms, this need only be checked for all g in some generating set for G.

Theorem 2. *Let $\alpha : G \to G_1$ and $\beta : G \to G_1$ be homomorphisms and assume that $G = \langle X\rangle$ generated by a subset X. Then*

$$\alpha = \beta \quad \textit{if and only if} \quad \alpha(x) = \beta(x) \quad \textit{for all } x \in X.$$

Proof. If $\alpha = \beta$, the condition is obvious. If the condition holds, let $g \in G$ and write (Theorem 8 §2.4) $g = x_1^{k_1}x_2^{k_2}\cdots x_n^{k_n}$, where $x_i \in X$ and $k_i \in \mathbb{Z}$ for each i. Then Theorem 1 gives

$$\alpha(g) = \alpha(x_1)^{k_1}\alpha(x_2)^{k_2}\cdots\alpha(x_n)^{k_n} = \beta(x_1)^{k_1}\beta(x_2)^{k_2}\cdots\beta(x_n)^{k_n} = \beta(g).$$

As $g \in G$ was arbitrary, this shows that $\alpha = \beta$. ■

Theorem 2 shows that a group homomorphism $\alpha : G \to G_1$ is completely determined by its effect on a generating set for G. This is useful because many groups are generated by a relatively small number of elements.

Example 9. Show that there are at most six homomorphisms $S_3 \to C_6$.

Solution. As in Example 8 §2.2 we write $S_3 = \{1, \sigma, \sigma^2, \tau, \tau\sigma, \tau\sigma^2\}$ where $|\sigma| = 3$, $|\tau| = 2$, and $\sigma\tau\sigma = \tau$, and write $C_6 = \langle c\rangle$, $|c| = 6$. Because $S_3 = \langle\sigma, \tau\rangle$, Theorem 2 shows that a homomorphism $\alpha : S_3 \to C_6$ is determined by the choice of $\alpha(\sigma)$ and $\alpha(\tau)$ in C_6. Now $\alpha(\sigma)^3 = \alpha(\sigma^3) = \alpha(1) = 1$, so the order $|\alpha(\sigma)|$ of $\alpha(\sigma)$ is 1 or 3. Hence there are three choices for $\alpha(\sigma)$: $1, c^2$, or c^4. Similarly, $\alpha(\tau)^2 = 1$, so $\alpha(\tau)$ must be either 1 or c^3. Thus there are at most $3\cdot 2 = 6$ choices in all. □

We hasten to note that *not* all the choices in Example 9 correspond to actual homomorphisms. In fact, there are *only two* homomorphisms from S_3 to C_6, and we return to this example later (see Example 9 §2.10).

Isomorphisms

We have shown that there are two *distinct* groups of order 4: the cyclic group and the noncyclic Klein group. Determining how to distinguish between distinct groups leads to the notion of isomorphic groups. Roughly speaking, the two groups are isomorphic if they are the same except for notation.

As an illustration, consider the groups $G = \{1, -1\}$ and $\mathbb{Z}_4^* = \{1, 3\}$. The two Cayley tables are

G	1	-1
1	1	-1
-1	-1	1

$\mathbb{Z}_4^*$	1	3
1	1	3
3	3	1

Clearly, they are alike. In fact, because the way the identity multiplies is always specified, we can describe both by saying that the nonidentity element squares to 1. A more precise comparison can be given as follows: The mapping $\sigma : G \to \mathbb{Z}_4^*$ given by

$$\sigma(1) = 1 \quad \text{and} \quad \sigma(-1) = 3$$

is a bijection, and we can obtain the entire Cayley table for $\mathbb{Z}_4^*$ from that of G by replacing a with $\sigma(a)$ for every a in G. In other words, the two groups are the same except for notation; we obtain $\mathbb{Z}_4^*$ from G by changing symbols.

This works in general. If G and G_1 are groups and $\sigma : G \to G_1$ is a bijection, we ask when the Cayley table for G_1 results from applying σ to every element of the table for G. This transformation is shown in the diagram.

$$\begin{array}{c|ccc} G & \cdots & b & \cdots \\ \hline \vdots & & & \\ a & & ab & \\ \vdots & & & \end{array} \qquad \begin{array}{c|ccc} G_1 & \cdots & \sigma(b) & \cdots \\ \hline \vdots & & & \\ \sigma(a) & & \sigma(ab) & \\ \vdots & & & \end{array}$$

Hence the condition is that $\sigma(ab) = \sigma(a)\sigma(b)$ for all a and b in G, that is that σ is a homomorphism. In general, if G and G_1 are groups, a mapping $\sigma : G \to G_1$ is called an **isomorphism** if σ is a bijection (one-to-one and onto) which is also a homomorphism. When an isomorphism exists from G to G_1 we say that G is **isomorphic** to G_1 and write $G \cong G_1$.

Hence, if $\sigma : G \to G_1$ is an isomorphism, the group G_1 is just G with the change of notation $g \mapsto \sigma(g)$. As in the preceding illustration, G and G_1 are the same group except for the symbols used. It is useful to think of isomorphic groups as two different realizations of the same (abstract) group. (The term *isomorphism* comes from *isos*, meaning *equal*, and *morphe*, meaning *shape*.)

Example 10. The set $2\mathbb{Z} = \{2k \mid k \in \mathbb{Z}\}$ of even integers is an additive group, in fact a subgroup of $\mathbb{Z}$. Show that $\mathbb{Z} \cong 2\mathbb{Z}$.

Solution. The function $\sigma : \mathbb{Z} \to 2\mathbb{Z}$ given by $\sigma(k) = 2k$ is clearly onto, and σ is one-to-one because $\sigma(k) = \sigma(m)$ implies $k = m$. Finally, σ is a homomorphism because

$$\sigma(k+m) = 2(k+m) = 2k + 2m = \sigma(k) + \sigma(m)$$

for all k and m in $\mathbb{Z}$. Thus σ is an isomorphism, so $\mathbb{Z} \cong 2\mathbb{Z}$. □

Note that the argument in Example 10 shows that $\mathbb{Z} \cong n\mathbb{Z}$ for *any* nonzero integer n.

Example 11. If $G = \left\{ \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix} \middle| n \in \mathbb{Z} \right\}$, show that G is a group using matrix multiplication, and that $\mathbb{Z} \cong G$.

Solution. G is closed because $\begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & m \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & n+m \\ 0 & 1 \end{bmatrix}$ is in G for all n and m in $\mathbb{Z}$. The identity matrix $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ is also in G. Finally, for $\begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix}$ in G, we have $\begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix}^{-1} = \begin{bmatrix} 1 & -n \\ 0 & 1 \end{bmatrix} \in G$. Hence G is a subgroup of $GL_2(\mathbb{Z})$. Now define $\sigma : \mathbb{Z} \to G$ by $\sigma(n) = \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix}$ for all n in $\mathbb{Z}$. This map is clearly onto and one-to-one, and given m and n in $\mathbb{Z}$, we have

$$\sigma(m+n) = \begin{bmatrix} 1 & m+n \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & m \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix} = \sigma(m) \cdot \sigma(n).$$

Hence σ preserves the operations and so is an isomorphism. □

Clearly, $G \cong G$ for any group G (the identity map $G \to G$ is an isomorphism). However, even though two groups are isomorphic, they sometimes appear to be quite different. For example, the group $\mathbb{C}^*$ of all nonzero complex numbers is known to be isomorphic to the circle group $\mathbb{C}^0$ of complex numbers on the unit circle[7]. Here is a less spectacular example.

Example 12. Show that $\mathbb{R} \cong \mathbb{R}^+$, where $\mathbb{R}$ is additive and $\mathbb{R}^+$ is multiplicative.

Solution. Define $\sigma : \mathbb{R} \to \mathbb{R}^+$ by $\sigma(r) = e^r$, where e^x is the exponential function. To show that σ is one-to-one, let $\sigma(r) = \sigma(s)$, where $r, s \in \mathbb{R}$. Then $e^r = e^s$ so, if $\ln x$ denotes the natural logarithm, $r = \ln(e^r) = \ln(e^s) = s$. Thus σ is one-to-one. If $t \in \mathbb{R}^+$, then $t > 0$, so $\ln t \in \mathbb{R}$ and $\sigma(\ln t) = e^{\ln t} = t$. Hence σ is onto. Finally,

$$\sigma(r+s) = e^{r+s} = e^r e^s = \sigma(r) \cdot \sigma(s) \qquad \text{for all } r \text{ and } s \text{ in } \mathbb{R}$$

which shows that σ is an isomorphism. □

Example 13. Let $G = \langle a \rangle$ be a cyclic group. Show that:
(1) If $|G| = n$, then $G \cong \mathbb{Z}_n$.
(2) If $|G| = \infty$, then $G \cong \mathbb{Z}$.

Solution. If $|G| = n$, then $|a| = n$, so we define $\sigma : \mathbb{Z}_n \to G$ by $\sigma(\bar{k}) = a^k$. We must show that this mapping is well defined. But Theorem 2 §2.4 gives

$$\bar{k} = \bar{m} \quad \Leftrightarrow \quad k \equiv m \pmod{n} \quad \Leftrightarrow \quad a^k = a^m$$

so σ is well defined (and one-to-one). Since σ is clearly onto, it remains to verify that it is a homomorphism:

$$\sigma(\bar{k} + \bar{m}) = \sigma(\overline{k+m}) = a^{k+m} = a^k a^m = \sigma(\bar{k}) \cdot \sigma(\bar{m}).$$

Hence σ is an isomorphism, proving (1). The proof of (2) is similar and we leave it as Exercise 14. □

Example 14. For the group $\mathbb{R}$ (under addition), the mapping $\alpha : \mathbb{R} \to \mathbb{R}$ given by $\alpha(r) = 2r + 1$ is onto and one-to-one as is easily verified, but it is *not* an isomorphism; for example, $\alpha(1+1) = 5$ but $\alpha(1) + \alpha(1) = 6$.

[7] See, for instance, Clay, J.R., "The punctured plane is isomorphic to the unit circle," *J. Number Theory*, 1, (1964), pp. 500–501.

Verifying that a particular mapping is an isomorphism requires checking three things: that it is onto; that it is one-to-one; and that it is operation-preserving. Although a particular mapping $\alpha : G \to G_1$ may fail one of these tests, the groups G and G_1 could very well be isomorphic (see Example 14). Conversely, showing that G and G_1 are *not* isomorphic entails showing that *no* isomorphism exists from G to G_1. Examples 15 and 16 illustrate this situation.

Example 15. Show that $\mathbb{Q}$ is not isomorphic to $\mathbb{Q}^*$.

Solution. Suppose that $\sigma : \mathbb{Q} \to \mathbb{Q}^*$ is an isomorphism. Then σ is onto, so let $q \in \mathbb{Q}$ satisfy $\sigma(q) = 2$, and write $\sigma(\frac{1}{2}q) = a$. The fact that σ is a homomorphism then gives

$$a^2 = \sigma(\tfrac{1}{2}q) \cdot \sigma(\tfrac{1}{2}q) = \sigma(\tfrac{1}{2}q + \tfrac{1}{2}q) = \sigma(q) = 2.$$

But there is no rational number a that satisfies $a^2 = 2$ (Example 3 §0.1), so no such isomorphism σ can exist. □

Example 16. Let G and H be cyclic groups with $|G| = 9$ and $|H| = 3$. Show that G and $H \times H$ are not isomorphic, even though both groups have order 9.

Solution. If $G = \langle a \rangle$ then $a^3 \neq 1$. On the other hand *every* element x of $H \times H$ satisfies $x^3 = 1$ (as this holds in H). This would not occur if $G \cong H \times H$ because the two Cayley tables would then be the same except for notation. □

Example 16 points to an important feature of isomorphisms: They preserve **structural properties** of groups, that is, properties that depend only on the Cayley table of a group and not on the way the group is described. The property that $x^3 = 1$ for every element of $H \times H$ in Example 16 is clearly a structural property, so it must be enjoyed by any group isomorphic to $H \times H$. Because G does not have this property, it cannot be isomorphic to $H \times H$. We can often show that two groups are *not* isomorphic by exhibiting a structural property of one that is not shared by the other.

The following list contains several examples of structural properties of a group G.

(1) G has order n.
(2) G is finite.
(3) G is abelian.
(4) G is cyclic.
(5) G has no element of order n.
(6) G has exactly m elements of order n.

The reader can likely add to this list. The above discussion is summarized in the following theorem.

Theorem 3. *If $G \cong H$ are isomorphic groups and G has a structural property, then H also has that structural property.*

Thus if G is abelian or cyclic, and if $G \cong H$, then H is abelian or cyclic. The reader should verify these facts directly using an isomorphism $\sigma : G \to H$.

Theorem 4. *Let G, G_1, and G_2 denote groups.*
(1) *The identity map $1_G : G \to G$ is an isomorphism for every group G.*
(2) *If $\sigma : G \to G_1$ is an isomorphism, the inverse mapping $\sigma^{-1} : G_1 \to G$ is also an isomorphism.*
(3) *If $\sigma : G \to G_1$ and $\tau : G_1 \to G_2$ are isomorphisms, their composite $\tau\sigma : G \to G_2$ is also an isomorphism.*

Proof. (1) is clear, and (3) follows from Theorem 3 §0.3 and Example 8. Turning to (2), the inverse mapping $\sigma^{-1} : G_1 \to G$ exists because σ is a bijection, and σ^{-1} is also a bijection (see Theorem 5 §0.3). It remains to show that σ^{-1} is a homomorphism. If g_1 and h_1 are in G_1, write $g = \sigma^{-1}(g_1)$ and $h = \sigma^{-1}(h_1)$. Then $\sigma(g) = g_1$ and $\sigma(h) = h_1$, so

$$\sigma^{-1}(g_1 h_1) = \sigma^{-1}[\sigma(g) \cdot \sigma(h)] = \sigma^{-1}[\sigma(gh)] = gh = \sigma^{-1}(g_1) \cdot \sigma^{-1}(h_1).$$

Therefore σ^{-1} is an isomorphism. ■

Corollary 1. *The isomorphic relation $\cong$ is an equivalence for groups. That is:*
(1) *$G \cong G$ for every group G.*
(2) *If $G \cong G_1$ then $G_1 \cong G$.*
(3) *If $G \cong G_1$ and $G_1 \cong G_2$ then $G \cong G_2$.*

Proof. Each of (1), (2), and (3) follows from the corresponding item in Theorem 4. ■

As an illustration of Corollary 1, we show that if G and H are both cyclic of order n then $G \cong H$. Indeed $G \cong \mathbb{Z}_n$ and $H \cong \mathbb{Z}_n$ by Example 13, so $G \cong H$ by Corollary 1. The reader should give a direct proof along the lines of Example 13.

Corollary 2. *If G is a group, the set of all isomorphisms $G \to G$ forms a group under composition.*

Proof. The isomorphisms $G \to G$ are a subset of the group S_G of all bijections $G \to G$, and Theorem 4 shows that they are a subgroup of S_G. ■

If G is a group, an isomorphism $G \to G$ is called an **automorphism** of G. The group of all automorphisms is denoted $\operatorname{aut} G$ and is called the **automorphism group** of G.

Example 17. If G is abelian, the mapping $\sigma : G \to G$ defined by $\sigma(g) = g^{-1}$ for all $g \in G$ is an automorphism of G. We leave the verification to the reader.

Example 18. If G is any group and $a \in G$, define $\sigma_a : G \to G$ by $\sigma_a(g) = aga^{-1}$ for all $a \in G$. Show that:
(1) σ_a is an automorphism of G for all a in G.
(2) $\{\sigma_a \mid a \in G\}$ is a subgroup of $\operatorname{aut} G$.

Solution. We leave verification that σ_a is one-to-one and onto for all $a \in G$ to the reader. If $g, h \in G$ we have

$$\sigma_a(g) \cdot \sigma_a(h) = aga^{-1} \cdot aha^{-1} = ag1ha^{-1} = agha^{-1} = \sigma_a(gh).$$

Hence σ_a is an automorphism of G, proving (1). If $b \in G$, then

$$\sigma_a\sigma_b(g) = \sigma_a(bgb^{-1}) = a(bgb^{-1})a^{-1} = abg(ab)^{-1} = \sigma_{ab}(g)$$

for all $g \in G$, so $\sigma_a\sigma_b = \sigma_{ab}$. Because $\sigma_1 = 1_G$, this implies that $\sigma_a^{-1} = \sigma_{a^{-1}}$ (verify), so the set $\{\sigma_a \mid a \in G\}$ is a subgroup of $\operatorname{aut} G$ by the Subgroup Test. This is (2). □

If G is a group and $a \in G$, the automorphism $\sigma_a : G \to G$ in Example 18 is called the **inner automorphism** of G determined by a. The group of all inner automorphisms of G is denoted $\operatorname{inn} G$. Because each inner automorphism $\sigma_a : G \to G$ is given explicitly in terms of a, the group $\operatorname{inn} G = \{\sigma_a \mid a \in G\}$ is routinely determined. By contrast, the group $\operatorname{aut} G$ can be difficult to determine. We do one simple case in Example 19 below.

Because it is a homomorphism, every isomorphism preserves the identity, inverses, and powers. But isomorphisms also preserve the order of an element (compare with the Corollary to Theorem 1).

Theorem 5. *Let $\sigma : G \to G_1$ be an isomorphism. Then $|\sigma(g)| = |g|$ for all $g \in G$.*

Proof. It suffices to show that $g^k = 1$ if and only if $[\sigma(g)]^k = 1$. If $g^k = 1$, then $[\sigma(g)]^k = \sigma(g^k) = \sigma(1) = 1$ by Theorem 1. Conversely, if $[\sigma(g)]^k = 1$, then $\sigma(g^k) = [\sigma(g)]^k = 1^k = 1 = \sigma(1)$. Hence $g^k = 1$ because σ is one-to-one. ■

Example 19. If G is cyclic of order 6, show that $\operatorname{aut} G = \{1_G, \lambda\}$, where $\lambda(g) = g^{-1}$ for all $g \in G$.

Solution. Both 1_G and (as G is abelian) λ are automorphisms of G. If $\sigma : G \to G$ is any automorphism, we show $\sigma = 1_G$ or $\sigma = \lambda$. Write $G = \langle a \rangle$, where $|a| = 6$. Theorem 1(3) shows that the choice of $\sigma(a)$ completely determines σ. We have $|\sigma(a)| = |a| = 6$ by Theorem 5, so $\sigma(a) = a$, or $\sigma(a) = a^5 = a^{-1}$. If $g \in G$, write $g = a^k$ for some $k \in \mathbb{Z}$, so that

$$\sigma(g) = \sigma(a^k) = [\sigma(a)]^k.$$

If $\sigma(a) = a$, this shows that $\sigma(g) = a^k = g$ for all $g \in G$, that is $\sigma = 1_G$. If $\sigma(a) = a^{-1}$, it shows that $\sigma(g) = (a^{-1})^k = (a^k)^{-1} = g^{-1}$ for all $g \in G$, that is, $\sigma = \lambda$. □

Cayley's Theorem

We conclude this section with a proof of a theorem of Cayley (proved in 1878) that every finite group is isomorphic to a group of permutations. If X is a nonempty set, recall that S_X denotes the group of all permutations of X (bijections $X \to X$) under composition. We need one simple observation about these permutation groups: If a bijection $\sigma : X \to Y$ exists then $S_X \cong S_Y$. Indeed, if $\lambda \in S_X$ we have

$$Y \xrightarrow{\sigma^{-1}} X \xrightarrow{\lambda} X \xrightarrow{\sigma} Y$$

so $\sigma\lambda\sigma^{-1} \in S_Y$. But then $\varphi : S_X \to S_Y$ given by $\varphi(\lambda) = \sigma\lambda\sigma^{-1}$ is an isomorphism, as can be readily verified. In particular $S_X \cong S_n$ whenever $|X| = n$.

Now let G be a group. We noted earlier that each row of the Cayley table of G is a permutation of G in the sense that each element appears exactly once. Since the row of $a \in G$ is $\{ag \mid g \in G\}$, this is just the assertion that $g \mapsto ag$ is a bijection $G \to G$. This is the connection that Cayley noticed between the groups G and S_G.

Theorem 6. ***Cayley's Theorem.*** *Every group G of order n is isomorphic to a subgroup of S_n.*

Proof. By the preceding discussion, there is an isomorphism $\varphi : S_G \to S_n$, so it suffices to find an isomorphism $\theta : G \to G_1$, where G_1 is a subgroup of S_G [then $\varphi(G_1) = \{\varphi(x) \mid x \in G_1\}$ is a subgroup of S_n and $\varphi\theta : G \to \varphi(G_1)$ is an isomorphism]. If $a \in G$, define $\tau_a : G \to G$ by $\tau_a(g) = ag$ for all $g \in G$. Then it is easy to verify that τ_a is a bijection (so $\tau_a \in S_G$) and that $\tau_1 = 1_G$, $\tau_a^{-1} = \tau_{a^{-1}}$, and $\tau_{ab} = \tau_a\tau_b$ for $a, b \in G$. These relations imply that $G_1 = \{\tau_a \mid a \in G\}$ is a subgroup of S_G, so define $\theta : G \to G_1$ by $\theta(a) = \tau_a$ for all $a \in G$. Then θ is clearly onto; it is also one-to-one because $\tau_a = \tau_b$ implies that $a = \tau_a(1) = \tau_b(1) = b$. Finally, $\tau_{ab} = \tau_a\tau_b$ implies that θ is a homomorphism, and hence an isomorphism. ■

Cayley's Theorem shows that every abstract group of order n is (up to isomorphism) a subgroup of S_n. Hence, to study the groups of order n, we need only study the symmetric group S_n. At first this approach seens to be an advantage because S_n consists of concrete mappings that can be analyzed using tools (such as cycle factorization and parity) not available in an abstract group. However, these symmetric groups are extremely large, so a subgroup of order n is lost in S_n, (for example, $|S_{10}| = 10! = 3,628,800$). However, in Section 8.3 we give a generalization of Cayley's Theorem that cuts down the size of the symmetric group and so provides more information about G.

Arthur Cayley (1821–1895)

Cayley showed his mathematical talent at an early age, quickly excelling at school. After some initial reluctance, his merchant father sent him to Cambridge at the age of 17. During the following eight years he read the works of the masters and published more than 20 papers on topics that would occupy him for the rest of his life. In addition, he developed broad interests in literature (he read Greek, German, and French, as well as English), architecture, and painting (he demonstrated talent in watercolors) and became an enthusiastic hiker and mountaineer.

At the age of 25, with no position as a mathematician in view, he undertook legal training and was admitted to the bar three years later. He earned a comfortable living as a lawyer but resisted the temptation to make a lot of money so as to free himself to do mathematics. And do it he did, publishing nearly 300 papers in 14 years. Finally, in 1863, he accepted the Sadlerian professorship at Cambridge and remained there for the rest of his life, valued for his administrative and teaching skills, as well as for his scholarship.

Although Cayley introduced the concept of an abstract group, his main accomplishments lay elsewhere. With his lifelong friend J. J. Sylvester, he founded the theory of invariants; he was one of the first to consider geometry of more than three dimensions; and he initiated matrix algebra and the theory of determinants. He also wrote on quaternions, the theory of equations, dynamics, and astronomy. He continued working until his death, leaving 966 papers filling 13 volumes of 600 pages each.

Exercises 2.5

1. In each case show that α is a homomorphism and determine if it is onto or one-to-one.

   (a) $\alpha : \mathbb{R} \to GL_2(\mathbb{R})$ given by $\alpha(r) = \begin{bmatrix} 1 & r \\ 0 & 1 \end{bmatrix}$ for all r in $\mathbb{R}$.
   (b) $\alpha : G \to G \times G$ given by $\alpha(g) = (g, g)$ for all g in the group G.
2. Verify that π_1 and σ_1 are homomorphisms in Example 7, and that π_1 is onto and σ_1 is one-to-one.
3. If G is any group, define $\alpha : G \to G$ by $\alpha(g) = g^{-1}$. Show that G is abelian if and only if α is a homomorphism.
4. If $m \in \mathbb{Z}$ is fixed and G is an abelian group, show that $\alpha : G \to G$ is a homomorphism where we define $\alpha(a) = a^m$ for all $a \in G$.
5. Let σ_a be the inner automorphism of G determined by a. If $\alpha : G \to \operatorname{inn} G$ is defined by $\alpha(a) = \sigma_a$ for all $a \in G$, show that α is a homomorphism. What is $\alpha(a)$ if $a \in Z(G)$?
6. Show that there are exactly two homomorphisms $\alpha : C_6 \to C_4$. [*Hint:* Example 9.]
7. If $n \geq 1$, give an example of a group homomorphism $\sigma : G \to G_1$ and an element $g \in G$ such that $|g| = \infty$ but $|\alpha(g)| = n$.
8. (a) Describe all group homomorphisms $\mathbb{Z} \to \mathbb{Z}$.
   (b) How many are onto?
9. If $\alpha : G \to G_1$ is a homomorphism, show that $K = \{g \in G \mid \alpha(g) = 1\}$ is a subgroup of G (called the *kernel* of α).
10. If $\alpha : G \to G_1$ is a homomorphism, show that $\operatorname{im} \alpha = \alpha(G) = \{\alpha(g) \mid g \in G\}$ is a subgroup of G_1.
11. If $\alpha : G \to G_1$ is an onto homomorphism and $G = \langle a \rangle$, show that $G_1 = \langle \alpha(a) \rangle$.
12. In each case determine whether $\alpha : G \to G_1$ is an isomorphism. Support your answer.
   (a) $G = G_1 = \mathbb{R}$, $\alpha(x) = 2x$ (b) $G = G_1 = \mathbb{Z}$, $\alpha(n) = 2n$
   (c) $G = G_1 = \mathbb{Z}_5^*$, $\alpha(g) = g^2$ (d) $G = G_1 = \mathbb{Z}_5^*$, $\alpha(g) = g^3$
   (e) $G = G_1 = \mathbb{Z}_7$, $\alpha(g) = 2g$ (f) $G = G_1 = \mathbb{Z}_8$, $\alpha(g) = 2g$
   (g) $G = G_1 = \mathbb{R}^+$, $\alpha(g) = g^2$ (h) $G = \mathbb{R}$, $G_1 = \mathbb{R}^+$, $\alpha(g) = |g|$
   (i) $G = 2\mathbb{Z}$, $G_1 = 3\mathbb{Z}$, $\alpha(2k) = 3k$ (j) $G = G_1 = \mathbb{R}$, $\alpha(g) = ag$, $a \neq 0$
13. Show that
$$G = \left\{ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}, \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \right\}$$
   is a subgroup of $GL_2(\mathbb{Z})$ isomorphic to $\{1, -1, i, -i\}$.
14. If G is an infinite cyclic group, show that $G \cong \mathbb{Z}$.
15. Show that $\sigma : \mathbb{C}^* \to \mathbb{C}^*$ is an automorphism if $\sigma(z) = \bar{z}$ for all $z \in \mathbb{C}$ ($\bar{z}$ denotes the complex conjugate of z).
16. If g and h are elements of a group G, show that $\langle gh \rangle \cong \langle hg \rangle$.
17. If G is a group of order 2, show that $G \times G \cong K_4$.
18. If $G \cong G_1$ and $H \cong H_1$, show that $G \times H \cong G_1 \times H_1$.

19. (a) If $\sigma : G \to G_1$ is an isomorphism, show that $Z(G_1) = \sigma[Z(G)]$, where $\sigma[Z(G)] = \{\sigma(z) \mid z \in Z(G)\}$.
(b) If $\sigma : G \to G_1$ is an onto homomorphism and $G = \langle a \rangle$ is cyclic, show that $G_1 = \langle \sigma(a) \rangle$.
20. Write $n\mathbb{Z} = \{nk \mid k \in \mathbb{Z}\}$. Show that $n\mathbb{Z} \cong m\mathbb{Z}$ whenever $n \neq 0$ and $m \neq 0$.
21. Show that $\mathbb{Z}_{10}^*$ is not isomorphic to $\mathbb{Z}_{12}^*$.
22. Show that $\mathbb{R}$ is not isomorphic to $\mathbb{R}^*$.
23. Show that the circle group $\mathbb{C}^0 = \{z \in \mathbb{C} \mid |z| = 1\}$ is not isomorphic to $\mathbb{R}^*$.
24. Find two nonisomorphic groups of order n^2 for any integer $n \geq 2$.
25. Are the additive groups $\mathbb{Z}$ and $\mathbb{Q}$ isomorphic? Support your answer.
26. Show that $\mathbb{Z}_{14}^* \cong \mathbb{Z}_{18}^*$.
27. If $G = \langle a \rangle$ and $G_1 = \langle b \rangle$, where $|a| = |b| = 6$, describe all isomorphisms $G \to G_1$.
28. Show that $\mathbb{R}^+ \times \mathbb{C}^0 \cong \mathbb{C}^*$, where $\mathbb{C}^0 = \{z \in \mathbb{C} \mid |z| = 1\}$ is the circle group.
29. Define $\tau_{a,b} : \mathbb{R} \to \mathbb{R}$ by $\tau_{a,b}(x) = ax + b$ for all $x \in \mathbb{R}$, and let $G_1 = \{\tau_{a,b} \mid a, b \in \mathbb{R},\ a \neq 0\}$. Let $G = \left\{ \begin{bmatrix} a & b \\ 0 & 1 \end{bmatrix} \middle| a, b \in \mathbb{R},\ a \neq 0 \right\}$. Show that G and G_1 are subgroups of $GL_2(\mathbb{R})$ and $S_{\mathbb{R}}$, respectively, and that $G \cong G_1$.
30. If $G = \left\{ \begin{bmatrix} a & b \\ -b & a \end{bmatrix} \middle| a, b \in \mathbb{R},\ a \text{ and } b \text{ not both } 0 \right\}$, show that G is a subgroup of $M_2(\mathbb{R})^*$ and that $G \cong \mathbb{C}^*$.
31. In each case, find $\operatorname{aut} G$, where $G = \langle a \rangle$ is cyclic of order n.
(a) $n = 2$ (b) $n = 3$
32. If $\sigma : X \to Y$ is a bijection, where X and Y are sets, show that $S_X \cong S_Y$. (See the discussion preceding Theorem 5).
33. If G is infinite cyclic, determine $\operatorname{aut} G$.
34. If G is a group such that $Z(G) = \{1\}$, show that $G \cong \operatorname{inn} G$. [*Hint:* $g \mapsto \sigma_g$.]
35. Let $z \in Z(G)$ and let G^z denote the set G with a new operation $a * b = abz^{-1}$. Show that G^z is a group and $G^z \cong G$.
36. If G is a group and $g \in G$, let $S(g) = \{\sigma \in \operatorname{aut} G \mid \sigma(g) = g\}$.
(a) Show that $S(g)$ is a subgroup of $\operatorname{aut} G$ for all $g \in G$.
(b) If $g_1 = \tau(g)$, $\tau \in \operatorname{aut} G$, show that $S(g)$ and $S(g_1)$ are conjugate subgroups of $\operatorname{aut} G$.
37. In a group G, write $a \sim b$ if $b = gag^{-1}$ for some $g \in G$ (a is *conjugate* to b).
(a) Show that $\sim$ is an equivalence relation on G.
(b) Determine which elements of G have singleton equivalence classes.
38. If $G = \langle X \rangle$ and $\sigma : G \to G_1$ is an onto homomorphism, show that $G_1 = \langle \sigma(X) \rangle$, where $\sigma(X) = \{\sigma(x) \mid x \in X\}$.
39. Show that $\mathbb{Z}_{15}^* \cong \mathbb{Z}_{16}^*$.

40. Show that $\operatorname{aut}(\mathbb{Z}_n \times \mathbb{Z}_n) \cong GL_n(\mathbb{Z}_n)$. [*Hint:* If $\sigma \in \operatorname{aut}(\mathbb{Z}_n \times \mathbb{Z}_n)$, let $\sigma(1, 0) = (a, b)$ and $\sigma(0, 1) = (c, d)$, and show that σ acts as right multiplication by $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$.]
41. Let X be a nonempty set and let $F(X)$ denote the set of all functions $\lambda : X \to \mathbb{R}$. Given $\lambda, \mu \in F(X)$, define $\lambda + \mu : X \to \mathbb{R}$ by $(\lambda + \mu)(x) = \lambda(x) + \mu(x)$ for all $x \in X$.
(a) Show that $F(X)$ is an abelian group using this operation.
(b) If $X = \{1, 2, 3\}$, show that $F(X) \cong \mathbb{R} \times \mathbb{R} \times \mathbb{R}$.
42. If M and M_1 are monoids, a mapping $\sigma : M \to M_1$ is called a **monoid isomorphism** if it is onto, one-to-one, and satisfies $\sigma(1) = 1$ and $\sigma(xy) = \sigma(x) \cdot \sigma(y)$ for all $x, y \in M$. If a monoid isomorphism $M \to M_1$ exists, show that $M^* \cong M_1^*$, where M^* denotes the group of units of the monoid M.
43. If M is a monoid, let $E(M)$ denote the set of all mappings $\alpha : M \to M$ that satisfy the condition $\alpha(xy) = \alpha(x) \cdot y$ for all $x, y \in M$.
(a) Show that $E(M)$ is a monoid under composition.
(b) Given $a \in M$, define $\alpha_a : M \to M$ by $\alpha_a(x) = ax$ for all $X \in m$. Show that $\alpha_a \in E(M)$.
(c) Show that $\{\alpha_a \mid a \in M\}$ is a monoid under composition and find a monoid isomorphism (see Exercise 42) $\sigma : M \to \{\alpha_a \mid a \in M\}$. This is a version of Cayley's Theorem for monoids.
44. Let M be a commutative monoid ($xy = yx$ for all $x, y \in M$) and assume that M is *cancellative*: $xy = xz$ in M implies that $y = z$. Show that M is isomorphic to a submonoid of a group. (A submonoid of a monoid M means a subset of M, closed under the operation of M and containing the unity of M.) [*Hint:* Define $\equiv$ on $M \times M$ by $(x, y) \equiv (x', y')$ if $xy' = x'y$. Show that $\equiv$ is an equivalence on $M \times M$ and write the equivalence class of (x, y) as a *fraction* x/y. Show that these fractions form an abelian group.]

2.6 COSETS AND LAGRANGE'S THEOREM

He [Lagrange] would set to mathematics all the little themes on physical inquiries which his friends brought him, much as Schubert set to music any stray rhyme that took his fancy.

—Herbert Westron Turnbull

In this section we prove one of the most important theorems about finite groups, Lagrange's Theorem, which asserts that the order of a subgroup of a finite group G is a divisor of $|G|$. This has far-reaching consequences as we shall see. The proof of the theorem involves counting elements of G and depends on the following basic notion.

Let H be a subgroup of a group G. If $a \in G$ we identify two subsets of G:

$$Ha = \{ha \mid h \in H\} \text{ — the } \textbf{right coset} \text{ of } H \textbf{ generated} \text{ by } a.$$
$$aH = \{ah \mid h \in H\} \text{ — the } \textbf{left coset} \text{ of } H \textbf{ generated} \text{ by } a.$$