2. If $\varphi : G \to H$ is an isomorphism, prove that $|\varphi(x)| = |x|$ for all $x \in G$. Deduce that any two isomorphic groups have the same number of elements of order n for each $n \in \mathbb{Z}^+$. Is the result true if φ is only assumed to be a homomorphism?
3. If $\varphi : G \to H$ is an isomorphism, prove that G is abelian if and only if H is abelian. If $\varphi : G \to H$ is a homomorphism, what additional conditions on φ (if any) are sufficient to ensure that if G is abelian, then so is H?
4. Prove that the multiplicative groups $\mathbb{R} - \{0\}$ and $\mathbb{C} - \{0\}$ are not isomorphic.
5. Prove that the additive groups $\mathbb{R}$ and $\mathbb{Q}$ are not isomorphic.
6. Prove that the additive groups $\mathbb{Z}$ and $\mathbb{Q}$ are not isomorphic.
7. Prove that D_8 and Q_8 are not isomorphic.
8. Prove that if $n \neq m$, S_n and S_m are not isomorphic.
9. Prove that D_{24} and S_4 are not isomorphic.
10. Fill in the details of the proof that the symmetric groups S_Δ and S_Ω are isomorphic if $|\Delta| = |\Omega|$ as follows: let $\theta : \Delta \to \Omega$ be a bijection. Define
$$\varphi : S_\Delta \to S_\Omega \qquad \text{by} \qquad \varphi(\sigma) = \theta \circ \sigma \circ \theta^{-1} \quad \text{for all } \sigma \in S_\Delta$$
and prove the following:
    (a) φ is well defined, that is, if σ is a permutation of Δ then $\theta \circ \sigma \circ \theta^{-1}$ is a permutation of Ω.
    (b) φ is a bijection from S_Δ onto S_Ω. [Find a 2-sided inverse for φ.]
    (c) φ is a homomorphism, that is, $\varphi(\sigma \circ \tau) = \varphi(\sigma) \circ \varphi(\tau)$.

    Note the similarity to the *change of basis* or *similarity* transformations for matrices (we shall see the connections between these later in the text).
11. Let A and B be groups. Prove that $A \times B \cong B \times A$.
12. Let A, B, and C be groups and let $G = A \times B$ and $H = B \times C$. Prove that $G \times C \cong A \times H$.
13. Let G and H be groups and let $\varphi : G \to H$ be a homomorphism. Prove that the image of φ, $\varphi(G)$, is a subgroup of H (cf. Exercise 26 of Section 1). Prove that if φ is injective then $G \cong \varphi(G)$.
14. Let G and H be groups and let $\varphi : G \to H$ be a homomorphism. Define the *kernel* of φ to be $\{g \in G \mid \varphi(g) = 1_H\}$ (so the kernel is the set of elements in G which map to the identity of H, i.e., is the fiber over the identity of H). Prove that the kernel of φ is a subgroup (cf. Exercise 26 of Section 1) of G. Prove that φ is injective if and only if the kernel of φ is the identity subgroup of G.
15. Define a map $\pi : \mathbb{R}^2 \to \mathbb{R}$ by $\pi((x, y)) = x$. Prove that π is a homomorphism and find the kernel of π (cf. Exercise 14).
16. Let A and B be groups and let G be their direct product, $A \times B$. Prove that the maps $\pi_1 : G \to A$ and $\pi_2 : G \to B$ defined by $\pi_1((a, b)) = a$ and $\pi_2((a, b)) = b$ are homomorphisms and find their kernels (cf. Exercise 14).
17. Let G be any group. Prove that the map from G to itself defined by $g \mapsto g^{-1}$ is a homomorphism if and only if G is abelian.
18. Let G be any group. Prove that the map from G to itself defined by $g \mapsto g^2$ is a homomorphism if and only if G is abelian.
19. Let $G = \{z \in \mathbb{C} \mid z^n = 1 \text{ for some } n \in \mathbb{Z}^+\}$. Prove that for any fixed integer $k > 1$ the map from G to itself defined by $z \mapsto z^k$ is a surjective homomorphism but is not an isomorphism.

1.33. Let G be a group and let $a \in G$.

(i) For each $a \in G$, prove that the functions $L_a\colon G \to G$, defined by $x \mapsto a * x$ (called ***left translation*** by a), and $R_a\colon G \to G$, defined by $x \mapsto x * a^{-1}$ (called ***right translation*** by a), are bijections.

(ii) For all $a, b \in G$, prove that $L_{a*b} = L_a \circ L_b$ and $R_{a*b} = R_a \circ R_b$.

(iii) For all a and b, prove that $L_a \circ R_b = R_b \circ L_a$.

1.34. Let G denote the multiplicative group of positive rationals. What is the identity of G? If $a \in G$, what is its inverse?

1.35. Let n be a positive integer and let G be the multiplicative group of all nth roots of unity; that is, G consists of all complex numbers of the form $e^{2\pi ik/n}$, where $k \in \mathbb{Z}$. What is the identity of G? If $a \in G$, what is its inverse? How many elements does G have?

1.36. Prove that the following four permutations form a group $\mathbf{V}$ (which is called the ***4-group***):

$$1; \qquad (1\ 2)(3\ 4); \qquad (1\ 3)(2\ 4); \qquad (1\ 4)(2\ 3).$$

1.37. Let $\hat{\mathbb{R}} = \mathbb{R} \cup \{\infty\}$, and define $1/0 = \infty$, $1/\infty = 0$, $\infty/\infty = 1$, and $1 - \infty = \infty = \infty - 1$. Show that the six functions $\hat{\mathbb{R}} \to \hat{\mathbb{R}}$, given by x, $1/x$, $1 - x$, $1/(1 - x)$, $x/(x - 1)$, $(x - 1)/x$, form a group with composition as operation.

EXERCISES

1.38. (i) Write a multiplication table for S_3.

(ii) Show that S_3 is isomorphic to the group of Exercise 1.37. (*Hint.* The elements in the latter group permute $\{0, 1, \infty\}$.)

1.39. Let $f: X \to Y$ be a bijection between sets X and Y. Show that $\alpha \mapsto f \circ \alpha \circ f^{-1}$ is an isomorphism $S_X \to S_Y$.

1.40. Isomorphic groups have the same number of elements. Prove that the converse is false by showing that $\mathbb{Z}_4$ is not isomorphic to the 4-group $\mathbf{V}$ defined in Exercise 1.36.

1.41. If isomorphic groups are regarded as being the same, prove, for each positive integer n, that there are only finitely many distinct groups with exactly n elements.

1.42. Let $G = \{x_1, \ldots, x_n\}$ be a set equipped with an operation $*$, let $A = [a_{ij}]$ be its multiplication table (i.e., $a_{ij} = x_i * x_j$), and assume that G has a (two-sided) identity e (that is, $e * x = x = x * e$ for all $x \in G$).

(i) Show that $*$ is commutative if and only if A is a symmetric matrix.

(ii) Show that every element $x \in G$ has a (two-sided) inverse (i.e., there is $x' \in G$ with $x * x' = e = x' * x$) if and only if the multiplication table A is a ***Latin square***; that is, no $x \in G$ is repeated in any row or column (equivalently, every row and every column of A is a permutation of G.)

(iii) Assume that $e = x_1$, so that the first row of A has $a_{1i} = x_i$. Show that the first column of A has $a_{i1} = x_i^{-1}$ for all i if and only if $a_{ii} = e$ for all i.

(iv) With the multiplication table as in (iii), show that $*$ is associative if and only if $a_{ij}a_{jk} = a_{ik}$ for all i, j, k.

1.43. (i) If $f: G \to H$ and $g: H \to K$ are homomorphisms, then so is the composite $g \circ f: G \to K$.

(ii) If $f: G \to H$ is an isomorphism, then its inverse $f^{-1}: H \to G$ is also an isomorphism.

(iii) If $\mathscr{C}$ is a class of groups, show that the relation of isomorphism is an equivalence relation on $\mathscr{C}$.

1.44. Let G be a group, let X be a set, and let $f: G \to X$ be a bijection. Show that there is a unique operation on X so that X is a group and f is an isomorphism.

1.45. If k is a field, denote the columns of the $n \times n$ identity matrix E by $\varepsilon_1, \ldots, \varepsilon_n$. A ***permutation matrix*** P over k is a matrix obtained from E by permuting its columns; that is, the columns of P are $\varepsilon_{\alpha 1}, \ldots, \varepsilon_{\alpha n}$ for some $\alpha \in S_n$. Prove that the set of all permutation matrices over k is a group isomorphic to S_n. (*Hint.* The inverse of P is its transpose P^t, which is also a permutation matrix.)

1.46. Let $\mathbf{T}$ denote the ***circle group***: the multiplicative group of all complex numbers of absolute value 1. For a fixed real number y, show that $f_y: \mathbb{R} \to \mathbf{T}$, given by $f_y(x) = e^{iyx}$, is a homomorphism. (The functions f_y are the only *continuous* homomorphisms $\mathbb{R} \to \mathbf{T}$.)

1.47. If a is a fixed element of a group G, define $\gamma_a: G \to G$ by $\gamma_a(x) = a * x * a^{-1}$ (γ_a is called ***conjugation*** by a).

(i) Prove that γ_a is an isomorphism.
(ii) If $a, b \in G$, prove that $\gamma_a \gamma_b = \gamma_{a*b}$.[4]

1.48. If G denotes the multiplicative group of all complex nth roots of unity (see Exercise 1.35), then $G \cong \mathbb{Z}_n$.

1.49. Describe all the homomorphisms from $\mathbb{Z}_{12}$ to itself. Which of these are isomorphisms?

1.50. (i) Prove that a group G is abelian if and only if the function $f: G \to G$, defined by $f(a) = a^{-1}$, is a homomorphism.
(ii) Let $f: G \to G$ be an isomorphism from a finite group G to itself. If f has no nontrivial fixed points (i.e., $f(x) = x$ implies $x = e$) and if $f \circ f$ is the identity function, then $f(x) = x^{-1}$ for all $x \in G$ and G is abelian. (*Hint.* Prove that every element of G has the form $x * f(x)^{-1}$.)

1.51 **(Kaplansky).** An element a in a ring R has a ***left quasi-inverse*** if there exists an element $b \in R$ with $a + b - ba = 0$. Prove that if every element in a ring R except 1 has a left quasi-inverse, then R is a division ring. (*Hint.* Show that $R - \{1\}$ is a group under the operation $a \circ b = a + b - ba$.)

1.52. (i) If G is the multiplicative group of all positive real numbers, show that $\log: G \to (\mathbb{R}, +)$ is an isomorphism. (*Hint*: Find a function inverse to log.)
(ii) Let G be the additive group of $\mathbb{Z}[x]$ (all polynomials with integer coefficients) and let H be the multiplicative group of all positive rational numbers. Prove that $G \cong H$. (*Hint.* Use the Fundamental Theorem of Arithmetic.)

Having solved Exercise 1.52, the reader may wish to reconsider the question when one "knows" a group. It may seem reasonable that one knows a group if one knows its multiplication table. But addition tables of $\mathbb{Z}[x]$ and of H are certainly well known (as are those of the multiplicative group of positive reals and the additive group of all reals), and it was probably a surprise that these groups are essentially the same. As an alternative answer to the question, we suggest that a group G is "known" if it can be determined, given any other group H, whether or not G and H are isomorphic.

[4] It is easy to see that $\delta_a: G \to G$, defined by $\delta_a(x) = a^{-1} * x * a$, is also an isomorphism; however, $\delta_a \delta_b = \delta_{b*a}$. Since we denote the value of a function f by $f(x)$, that is, the symbol f is on the left, the isomorphisms γ_a are more natural for us than the δ_a. On the other hand, if one denotes $\delta_a(x)$ by x^a, then one has put the function symbol on the right, and the δ_a are more convenient: $x^{a*b} = (x^a)^b$. Indeed, many group theorists nowadays put all their function symbols on the right!