Proof. As we already know, there is a homomorphism θ of $\bar{G}$ onto $\bar{G}/\bar{N}$ defined by $\theta(\bar{g}) = \bar{N}\bar{g}$. We define the mapping $\psi: G \to \bar{G}/\bar{N}$ by $\psi(g) = \bar{N}\phi(g)$ for all $g \in G$. To begin with, ψ is onto, for if $\bar{g} \in \bar{G}$, $\bar{g} = \phi(g)$ for some $g \in G$, since ϕ is onto, so the typical element $\bar{N}\bar{g}$ in $\bar{G}/\bar{N}$ can be represented as $\bar{N}\phi(g) = \psi(g)$.

If $a, b \in G$, $\psi(ab) = \bar{N}\phi(ab)$ by the definition of the mapping ψ. However, since ϕ is a homomorphism, $\phi(ab) = \phi(a)\phi(b)$. Thus $\psi(ab) = \bar{N}\phi(a)\phi(b) = \bar{N}\phi(a)\bar{N}\phi(b) = \psi(a)\psi(b)$. So far we have shown that ψ is a homomorphism of G onto $\bar{G}/\bar{N}$. What is the kernel, T, of ψ? Firstly, if $n \in N$, $\phi(n) \in \bar{N}$, so that $\psi(n) = \bar{N}\phi(n) = \bar{N}$, the identity element of $\bar{G}/\bar{N}$, proving that $N \subset T$. On the other hand, if $t \in T$, $\psi(t) =$ identity element of $\bar{G}/\bar{N} = \bar{N}$; but $\psi(t) = \bar{N}\phi(t)$. Comparing these two evaluations of $\psi(t)$, we arrive at $\bar{N} = \bar{N}\phi(t)$, which forces $\phi(t) \in \bar{N}$; but this places t in N by definition of N. That is, $T \subset N$. The kernel of ψ has been proved to be equal to N. But then ψ is a homomorphism of G onto $\bar{G}/\bar{N}$ with kernel N. By Theorem 2.7.1 $G/N \approx \bar{G}/\bar{N}$, which is the first part of the theorem. The last statement in the theorem is immediate from the observation (following as a consequence of Theorem 2.7.1) that $\bar{G} \approx G/K$, $\bar{N} \approx N/K$, $\bar{G}/\bar{N} \approx (G/K)/(N/K)$.

Problems

1. In the following, verify if the mappings defined are homomorphisms, and in those cases in which they are homomorphisms, determine the kernel.
   (a) G is the group of nonzero real numbers under multiplication, $\bar{G} = G$, $\phi(x) = x^2$ all $x \in G$.
   (b) $G, \bar{G}$ as in (a), $\phi(x) = 2^x$.
   (c) G is the group of real numbers under addition, $\bar{G} = G$, $\phi(x) = x + 1$ all $x \in G$.
   (d) $G, \bar{G}$ as in (c), $\phi(x) = 13x$ for $x \in G$.
   (e) G is any abelian group, $\bar{G} = G$, $\phi(x) = x^5$ all $x \in G$.
2. Let G be any group, g a fixed element in G. Define $\phi: G \to G$ by $\phi(x) = gxg^{-1}$. Prove that ϕ is an isomorphism of G onto G.
3. Let G be a finite abelian group of order $o(G)$ and suppose the integer n is relatively prime to $o(G)$. Prove that every $g \in G$ can be written as $g = x^n$ with $x \in G$. (*Hint:* Consider the mapping $\phi: G \to G$ defined by $\phi(y) = y^n$, and prove this mapping is an isomorphism of G onto G.)
4. (a) Given any group G and a subset U, let $\hat{U}$ be the smallest subgroup of G which contains U. Prove there is such a subgroup $\hat{U}$ in G. ($\hat{U}$ is called the *subgroup generated by* U.)

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!