Proof. The elements of $\overline{G}$ are the cosets of N, and they are also the fibres of the map φ (2.7.15). The map $\overline{\varphi}$ referred to in the theorem is the one that sends a nonempty fibre to its image: $\overline{\varphi}(\overline{x}) = \varphi(x)$. For any surjective map of sets $\varphi: G \to G'$, one can form the set $\overline{G}$ of fibres, and then one obtains a diagram as above, in which $\overline{\varphi}$ is the bijective map that sends a fibre to its image. When φ is a group homomorphism, $\overline{\varphi}$ is an isomorphism because $\overline{\varphi}(\overline{ab}) = \varphi(ab) = \varphi(a)\varphi(b) = \overline{\varphi}(\overline{a})\overline{\varphi}(\overline{b})$. □

Corollary 2.12.11 Let $\varphi: G \to G'$ be a group homomorphism with kernel N and image H'. The quotient group $\overline{G} = G/N$ is isomorphic to the image H'. □

Two quick examples: The image of the absolute value map $\mathbb{C}^\times \to \mathbb{R}^\times$ is the group of positive real numbers, and its kernel is the unit circle U. The theorem asserts that the quotient group $\mathbb{C}^\times/U$ is isomorphic to the multiplicative group of positive real numbers. The determinant is a surjective homomorphism $GL_n(\mathbb{R}) \to \mathbb{R}^\times$, whose kernel is the special linear group $SL_n(\mathbb{R})$. So the quotient $GL_n(\mathbb{R})/SL_n(\mathbb{R})$ is isomorphic to $\mathbb{R}^\times$.

There are also theorems called the Second and the Third Isomorphism Theorems, though they are less important.

Es giebt alſo ſehr viel verſchiedene Arten von Größen,
welche ſich nicht wohl herzehlen laßen;
und daher entſtehen die verſchiedene Theile der Mathematic,
deren eine jegliche mit einer beſondern Art von Größen beſchäftiget iſt.

—Leonhard Euler

EXERCISES

Section 1 Laws of Composition

1.1. Let S be a set. Prove that the law of composition defined by $ab = a$ for all a and b in S is associative. For which sets does this law have an identity?

1.2. Prove the properties of inverses that are listed near the end of the section.

1.3. Let $\mathbb{N}$ denote the set $\{1, 2, 3, \ldots, \}$ of natural numbers, and let $s: \mathbb{N} \to \mathbb{N}$ be the *shift* map, defined by $s(n) = n + 1$. Prove that s has no right inverse, but that it has infinitely many left inverses.

Section 2 Groups and Subgroups

2.1. Make a multiplication table for the symmetric group S_3.

2.2. Let S be a set with an associative law of composition and with an identity element. Prove that the subset consisting of the invertible elements in S is a group.

2.3. Let x, y, z, and w be elements of a group G.

(a) Solve for y, given that $xyz^{-1}w = 1$.

(b) Suppose that $xyz = 1$. Does it follow that $yzx = 1$? Does it follow that $yxz = 1$?

2.4. In which of the following cases is H a subgroup of G?

(a) $G = GL_n(\mathbb{C})$ and $H = GL_n(\mathbb{R})$.

(b) $G = \mathbb{R}^\times$ and $H = \{1, -1\}$.

(c) $G = \mathbb{Z}^+$ and H is the set of positive integers.

(d) $G = \mathbb{R}^\times$ and H is the set of positive reals.

(e) $G = GL_2(\mathbb{R})$ and H is the set of matrices $\begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix}$, with $a \neq 0$.

2.5. In the definition of a subgroup, the identity element in H is required to be the identity of G. One might require only that H have an identity element, not that it need be the same as the identity in G. Show that if H has an identity at all, then it is the identity in G. Show that the analogous statement is true for inverses.

2.6. Let G be a group. Define an *opposite group* G° with law of composition $a * b$ as follows: The underlying set is the same as G, but the law of composition is $a * b = ba$. Prove that G° is a group.

Section 3 Subgroups of the Additive Group of Integers

3.1. Let $a = 123$ and $b = 321$. Compute $d = \gcd(a, b)$, and express d as an integer combination $ra + bs$.

3.2. Prove that if a and b are positive integers whose sum is a prime p, their greatest common divisor is 1.

3.3. **(a)** Define the greatest common divisor of a set $\{a_1, \ldots, a_n\}$ of n integers. Prove that it exists, and that it is an integer combination of $a_1, \ldots, a_n$.

(b) Prove that if the greatest common divisor of $\{a_1, \ldots, a_n\}$ is d, then the greatest common divisor of $\{a_1/d, \ldots, a_n/d\}$ is 1.

Section 4 Cyclic Groups

4.1. Let a and b be elements of a group G. Assume that a has order 7 and that $a^3b = ba^3$. Prove that $ab = ba$.

4.2. An nth root of unity is a complex number z such that $z^n = 1$.

(a) Prove that the nth roots of unity form a cyclic subgroup of $\mathbb{C}^\times$ of order n.

(b) Determine the product of all the nth roots of unity.

4.3. Let a and b be elements of a group G. Prove that ab and ba have the same order.

4.4. Describe all groups G that contain no proper subgroup.

4.5. Prove that every subgroup of a cyclic group is cyclic. Do this by working with exponents, and use the description of the subgroups of $\mathbb{Z}^+$.

4.6. **(a)** Let G be a cyclic group of order 6. How many of its elements generate G? Answer the same question for cyclic groups of orders 5 and 8.

(b) Describe the number of elements that generate a cyclic group of arbitrary order n.

4.7. Let x and y be elements of a group G. Assume that each of the elements x, y, and xy has order 2. Prove that the set $H = \{1, x, y, xy\}$ is a subgroup of G, and that it has order 4.

4.8. **(a)** Prove that the elementary matrices of the first and third types (1.2.4) generate $GL_n(\mathbb{R})$.

(b) Prove that the elementary matrices of the first type generate $SL_n(\mathbb{R})$. Do the 2×2 case first.

4.9. How many elements of order 2 does the symmetric group S_4 contain?

4.10. Show by example that the product of elements of finite order in a group need not have finite order. What if the group is abelian?

4.11. **(a)** Adapt the method of row reduction to prove that the transpositions generate the symmetric group S_n.

(b) Prove that, for $n \geq 3$, the three-cycles generate the alternating group A_n.

Section 5 Homomorphisms

5.1. Let $\varphi: G \to G'$ be a surjective homomorphism. Prove that if G is cyclic, then G' is cyclic, and if G is abelian, then G' is abelian.

5.2. Prove that the intersection $K \cap H$ of subgroups of a group G is a subgroup of H, and that if K is a normal subgroup of G, then $K \cap H$ is a normal subgroup of H.

5.3. Let U denote the group of invertible upper triangular 2×2 matrices $A = \begin{bmatrix} a & b \\ 0 & d \end{bmatrix}$, and let $\varphi: U \to \mathbb{R}^\times$ be the map that sends $A \rightsquigarrow a^2$. Prove that φ is a homomorphism, and determine its kernel and image.

5.4. Let $f: \mathbb{R}^+ \to \mathbb{C}^\times$ be the map $f(x) = e^{ix}$. Prove that f is a homomorphism, and determine its kernel and image.

5.5. Prove that the $n \times n$ matrices that have the block form $M = \begin{bmatrix} A & B \\ 0 & D \end{bmatrix}$, with A in $GL_r(\mathbb{R})$ and D in $GL_{n-r}(\mathbb{R})$, form a subgroup H of $GL_n(\mathbb{R})$, and that the map $H \to GL_r(\mathbb{R})$ that sends $M \rightsquigarrow A$ is a homomorphism. What is its kernel?

5.6. Determine the center of $GL_n(\mathbb{R})$.

Hint: You are asked to determine the invertible matrices A that commute with every invertible matrix B. Do not test with a general matrix B. Test with elementary matrices.

Section 6 Isomorphisms

6.1. Let G' be the group of real matrices of the form $\begin{bmatrix} 1 & x \\ & 1 \end{bmatrix}$. Is the map $\mathbb{R}^+ \to G'$ that sends x to this matrix an isomorphism?

6.2. Describe all homomorphisms $\varphi: \mathbb{Z}^+ \to \mathbb{Z}^+$. Determine which are injective, which are surjective, and which are isomorphisms.

6.3. Show that the functions $f = 1/x$, $g = (x-1)/x$ generate a group of functions, the law of composition being composition of functions, that is isomorphic to the symmetric group S_3.

6.4. Prove that in a group, the products ab and ba are conjugate elements.

6.5. Decide whether or not the two matrices $A = \begin{bmatrix} 3 & \\ & 2 \end{bmatrix}$ and $B = \begin{bmatrix} 1 & 1 \\ -2 & 4 \end{bmatrix}$ are conjugate elements of the general linear group $GL_2(\mathbb{R})$.