Chapter 11
Group Homomorphisms

A homomorphism is a function between groups satisfying a few natural properties. A homomorphism that is both one to one and onto is an isomorphism. This chapter presents different isomorphism theorems which are important tools for proving further results. The first isomorphism theorem, that will be the second theorem to be proven after the factor theorem, is easier to motivate, since it will help us in computing quotient groups. Cayley's Theorem states that a permutation group of a group is isomorphic to the given group.

11.1 Homomorphisms and Their Properties

Here are the Cayley tables for a cyclic group of order 4 and U_{10}:

$\cdot$	e	a	a^2	a^3
e	e	a	a^2	a^3
a	a	a^2	a^3	e
a^2	a^2	a^3	e	a
a^3	a^3	e	a	a^2

$\cdot$	1	3	7	9
1	1	3	7	9
3	3	9	1	7
7	7	1	9	3
9	9	7	3	1

There is obvious sense in which these two groups are "the same". Indeed, we can obtain the right table from the left table by replacing e, a, a^2 and a^3 with 1, 7, 9 and 3, respectively. Then, although the two groups look different, they are essentially the same. We may think of saying two groups are the same if it is possible to obtain one of them from the other by substitution as above. One way to implement a substitution is to use a function. In a sense, a function is a thing which substitutes its output for its input. We will define what it means for two groups to be the same by using certain kinds of functions between groups. These functions are called group homomorphisms; a special kind of homomorphism, called an isomorphism, will be

B. Davvaz, *A First Course in Group Theory*,
https://doi.org/10.1007/978-981-16-6365-9_11

used to define sameness for groups. The term homomorphism comes from the Greek words homo, "like", and morphe, "form".

Definition 11.1 Let G and H be groups. A function $f : G \to H$ is called a *homomorphism* if

$$f(ab) = f(a)f(b),$$

for all $a, b \in G$. Here, the multiplication in ab is in G and the multiplication in $f(a)f(b)$ is in H.

This definition can be visualized as shown in Fig. 11.1. The pairs of dashed arrows represent the group operations.

A short description of a homomorphism is that it preserve the operation of G. The set of all homomorphism from G to H is denoted by $Hom(G, H)$. This set is always non-empty because it contains the *zero homomorphism*, the homomorphism which sends every elements of G to the identity element of H.

In the definition of homomorphism, we assumed multiplicative notation for the operations in both G and H. If the operation in one or both is something else, we must adjust the definition accordingly. For instance, see Table 11.1.

Before working out some facts about homomorphisms, we present some examples.

Example 11.2 For any pair of groups G and H, one can always define the trivial homomorphism. This is the rather uninteresting function that maps every element of the domain to the identity element in the range.

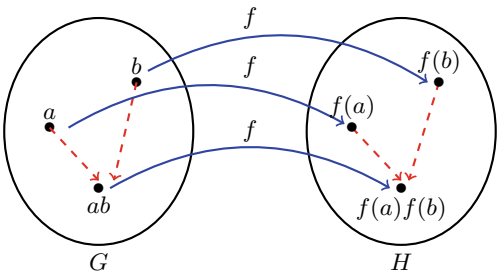


Fig. 11.1 Homomorphism between two groups

Table 11.1 Operations of groups in a homomorphism

Operation in G	Operation in H	Homomorphism definition
$+$	$+$	$f(x + y) = f(x) + f(y)$
$+$	$\cdot$	$f(x + y) = f(x) \cdot f(y)$
$\cdot$	$+$	$f(x \cdot y) = f(x) + f(y)$
$\star$	$\times$	$f(x \star y) = f(x) \times f(y)$

Example 11.3 Let $\mathbb{Z}$ be the group of integers under addition and $\mathbb{Z}_n$ be the group of integers under addition modulo n. If we define $f : \mathbb{Z} \to \mathbb{Z}_n$ by $f(x)$ equals to remainder of x on division by n, then n is a homomorphism.

Example 11.4 If $G = \langle a \rangle$, then $f : \mathbb{Z} \to G$ defined by $f(m) = a^m$ is a homomorphism.

Example 11.5 Let H denote the group $\{1, -1\}$ under multiplication (the 1 and -1 here are just the ordinary numbers, H is a group of order 2). We may define a function f from the group $\mathbb{Z}$ of integers under addition to H by

$$f(n) = \begin{cases} 1 & \text{if } n \text{ is even} \\ -1 & \text{if } n \text{ is odd.} \end{cases}$$

Then f is a homomorphism.

Example 11.6 The logarithm function is homomorphism from the group of positive real numbers under multiplication, to the group of all real numbers under addition.

Example 11.7 Let the circle group H consists of all complex numbers z such that $|z| = 1$. We can define a homomorphism f from the additive group of real numbers $\mathbb{R}$ to H by $f(\theta) = \cos\theta + i \sin\theta$. Geometrically, we are simply wrapping the real line around the circle in a group-theoretic fashion.

Example 11.8 Let $\mathbb{R}[x]$ denote the group of all polynomials with real coefficients under addition. For any $p \in \mathbb{R}[x]$, let p' denote the derivative of p. Then, the function $p \mapsto p'$ is a homomorphism from $\mathbb{R}[x]$ to itself.

Example 11.9 Let $G = C([0, 1])$ be the additive group of all continuous real-valued functions. Then, the integration function from G to $\mathbb{R}$ given by $f \mapsto \int_0^1 f(x)dx$ is a homomorphism.

Theorem 11.10 *If G and H are groups and $f : G \to H$ is a homomorphism, then*

(1) $f(e) = e$, where e on the left is the identity in G and e on the right is the identity in H;
(2) $f(a^{-1}) = f(a)^{-1}$, for all $a \in G$.

Proof (1) Since $ee = e$, it follows that $f(e)f(e) = f(e) = f(ee) = f(e) = f(e)e$. So, by cancellation property in H, we obtain $f(e) = e$.

(2) Let $a \in G$ be an arbitrary element. Since $f(aa^{-1}) = f(e) = e$, it follows that $f(a)f(a^{-1}) = e$, and so by the definition of inverse, we conclude that $f(a^{-1}) = f(a)^{-1}$. ■

Informally, we can speak about a homomorphism as a function that respects structure. A homomorphism of groups "respects" the property of the identity element, multiplication, and inversion.

Theorem 11.11 *If G and H are groups and $f : G \to H$ is a homomorphism, then*

(1) For any integer n and $a \in G$, $f(a^n) = f(a)^n$;
(2) For any $a \in G$, if the order of a is finite, then $o\big(f(a)\big) | o(a)$.

Proof (1) It follows from the first part of Theorem 11.10 trivially when $n = 0$, and by mathematical induction for $n > 0$. If $n < 0$, then put $m = -n$. Hence, we obtain

$$f(a^n) = f(a^{-m}) = f\big((a^m)^{-1}\big) = f(a^m)^{-1} = f(a)^{-m} = f(a)^n.$$

(2) If $o(a) = n$, then $a^n = e$, and so we obtain $f(a^n) = f(e) = e$. This implies that $f(a)^n = e$. Thus, we conclude that $o(f(a)|n$. ■

Remark 11.12 If the operation of H is addition, then the property (1) in Theorem 11.11 becomes $f(a^n) = nf(a)$. If both the operation of G and H are addition, then the property (1) becomes $f(na) = nf(a)$.

Example 11.13 We want to determine all homomorphisms from $\mathbb{Z}_{24}$ to $\mathbb{Z}_{18}$. Suppose that $f : \mathbb{Z}_{24} \to \mathbb{Z}_{18}$ be a homomorphism. For every non-negative integer m, we have

$$f(\overline{m}) = f(\underbrace{\overline{1} + \overline{1} + \cdots + \overline{1}}_{m \text{ times}}) = \underbrace{f(\overline{1}) + f(\overline{1}) + \cdots + f(\overline{1})}_{m \text{ times}} = mf(\overline{1}),$$

for all $0 \leq m \leq 23$. This means that a homomorphism f is completely determined by the value $f(\overline{1})$. Let $f(\overline{1}) = \overline{n}$, where $0 \leq n \leq 17$. In additive group $\mathbb{Z}_{18}$, we can write

$$\overline{24n} = \overline{24}\overline{n} = \overline{24}f(\overline{1}) = f(\overline{24}) = f(\overline{0}).$$

Since any homomorphism maps the identity to identity, it follows that $f(\overline{0}) = \overline{0}$. Hence, $\overline{24n} = \overline{0}$. This yields that $18|24n$ or $3|4n$. Since $(3, 4) = 1$, it follows that $3|n$, and so we conclude that $n \in \{0,\ 3,\ 6,\ 9,\ 12,\ 15\}$. Therefore, any homomorphism must send $\overline{1}$ to $\overline{3k}$, for $k = 0, 1, \ldots, 5$. This shows that there exist at most six possible homomorphisms from $\mathbb{Z}_{24}$ to $\mathbb{Z}_{18}$, namely $f_0, f_1, \ldots, f_5$, where $f_k(\overline{m}) = \overline{3km}$, for every $k = 0, 1, \ldots, 5$.

Now, we investigate that for each $0 \leq k \leq 5$, f_k is well defined. Assume that $m, m' \in \mathbb{Z}$ such that $\overline{m} = \overline{m'}$ in $\mathbb{Z}_{24}$. Then, we have $24|m - m'$, and so $3km - 3km'$ is a multiple of 72. It follows that $3km - 3km'$ is a multiple of 18. Thus, $\overline{3km} = \overline{3km'}$ or $f_k(\overline{m}) = f_k(\overline{m'})$.

In the rest, we show that f_k is a homomorphism. If $m, m' \in \mathbb{Z}$, then we have

$$\begin{aligned} f_k(\overline{m} + \overline{m'}) &= f_k(\overline{m + m'}) = \overline{3k(m + m')} \\ &= \overline{3km} + \overline{3km'} = f(\overline{m}) + f(\overline{m'}). \end{aligned}$$

Therefore, each f_k is a homomorphism from $\mathbb{Z}_{24}$ to $\mathbb{Z}_{18}$.

Since homomorphisms preserve the group operation, it should not be a surprise that they preserve many group properties.

Theorem 11.14 *Let G and H be groups and $f : G \to H$ be a homomorphism.*

(1) The image of a subgroup of G is a subgroup of H. In particular, $f(G)$ (or another notation, Imf) is a subgroup of H;
(2) The inverse image of a subgroup of H is a subgroup of G.

Proof (1) Let A be a subgroup of G. Since $e = f(e) \in f(A)$, it follows that $f(A)$ is non-empty. Let $f(a)$ and $f(b)$ be two arbitrary elements of $f(A)$. Then, we have $f(a)f(b)^{-1} = f(ab^{-1})$. Since A is a subgroup, it follows that $ab^{-1} \in A$. Therefore, we conclude that $f(a)f(b)^{-1} \in f(A)$, and so $f(A)$ is a subgroup of H.

(2) Let B be a subgroup of H. Again, since $f(e) = e \in B$, it follows that $e \in f^{-1}(B)$. Hence, $f^{-1}(B)$ is non-empty. Assume that x and y are two arbitrary elements of $f^{-1}(B)$. Then, we have $f(x) \in B$ and $f(y) \in B$. Since B is a subgroup, it follows that $f(x)f(y)^{-1} \in B$, and so $f(xy^{-1}) \in B$. Therefore, we conclude that $xy^{-1} \in f^{-1}(B)$. This completes the proof. ■

Theorem 11.15 *Let G and H be groups and $f : G \to H$ be a homomorphism. If $A \trianglelefteq G$ and $B \trianglelefteq H$, then $f(A) \trianglelefteq f(G)$ and $f^{-1}(B) \trianglelefteq G$.*

Proof By Theorem 11.14, we know that $f(A) \leq f(G)$ and $f^{-1}(B) \leq G$.

Now, let $f(a) \in f(A)$ and $f(x) \in f(G)$ be arbitrary. Then, we can write $f(x)f(a)f(x)^{-1} = f(xax^{-1})$. Since $A \trianglelefteq G$, it follows that $xax^{-1} \in A$. So, we conclude that $f(x)f(a)f(x)^{-1} \in f(A)$. This shows that $f(A) \trianglelefteq f(G)$.

Finally, suppose that $x \in G$ and $y \in f^{-1}(B)$ are arbitrary. Then, we have $f(x) \in H$ and $f(y) \in B$. Since $B \trianglelefteq H$, it follows that $f(x)f(y)f(x)^{-1} \in B$, or equivalently $f(xyx^{-1}) \in B$. This implies that $xyx^{-1} \in f^{-1}(B)$, and so $f^{-1}(B) \trianglelefteq G$. ■

The following is an important concept for homomorphisms.

Definition 11.16 The *kernel* of a homomorphism f from a group G to a group H is the set $\{x \in G \mid f(x) = e\}$. The kernel of f is denoted by $Kerf$.

Example 11.17 Let $D(\mathbb{R})$ be the additive group of all differentiable functions, $f : \mathbb{R} \to \mathbb{R}$, with continuous derivative. Let $C(\mathbb{R})$ be the additive group of all continuous functions $f : \mathbb{R} \to \mathbb{R}$. Suppose that $F : D(\mathbb{R}) \to C(\mathbb{R})$ be defined by $F(f) = df/dx$. Then

(1) F is a homomorphism;
(2) $KerF = \{f \in D(\mathbb{R}) \mid df/dx = 0\}$, which is the set of all constant functions.

The following is a fundamental theorem about the kernel of a homomorphism.

Theorem 11.18 *If G and H are groups and $f : G \to H$ is a homomorphism, then $Kerf$ is a normal subgroup of G.*

Proof Since $f(e) = e$, it follows that $Kerf$ is non-empty. Now, we suppose that a and b are two arbitrary elements of $Kerf$. Then, we have $f(a) = e$ and $f(b) = e$. Consequently, we get $f(ab^{-1}) = f(a)f(b)^{-1} = ee^{-1} = e$. This shows that $ab^{-1} \in Kerf$ and so $Kerf$ is a subgroup of G. On the other hand, for any $x \in G$, we have $f(xax^{-1}) = f(x)f(a)f(x)^{-1} = f(x)ef(x)^{-1} = e$. This yields that $xax^{-1} \in Kerf$. Therefore, we deduce that $Kerf$ is also a normal subgroup of G. ■

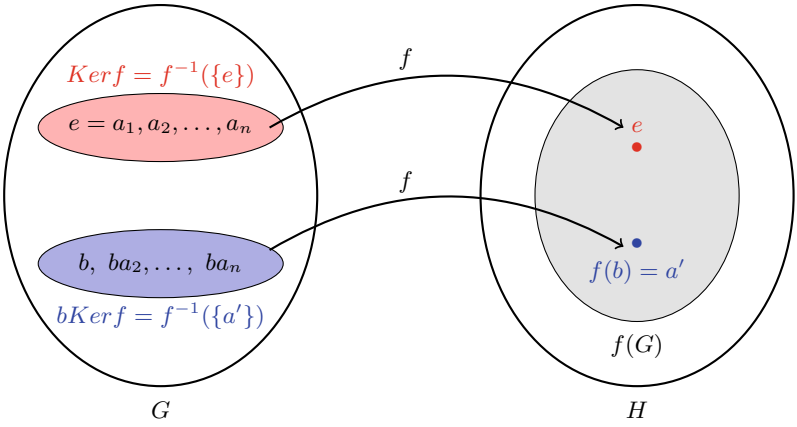


Fig. 11.2 Illustration for the kernel

Theorem 11.19 *If G and H are groups and $f : G \to H$ is a homomorphism, then*

(1) $f(a) = f(b)$ if and only if $aKerf = bKerf$;
(2) If $f(b) = a'$, then $f^{-1}(\{a'\}) = \{x \in G \mid f(x) = a'\} = bKerf$. Look at the illustration in Fig. 11.2.

Proof (1) We have

$$\begin{aligned} f(a) = f(b) &\Leftrightarrow f(b)^{-1} f(a) = e \Leftrightarrow f(b^{-1}a) = e \\ &\Leftrightarrow b^{-1}a \in Kerf \Leftrightarrow aKerf = bKerf. \end{aligned}$$

(2) We must show that $f^{-1}(\{a'\}) \subseteq bKerf$ and $bKerf \subseteq f^{-1}(\{a'\})$. To demonstrate the first inclusion, assume that $x \in f^{-1}(\{a'\})$ is an arbitrary element. Then, we have $f(x) = a'$, and so $f(x) = f(b)$. Now by part (1), we conclude that $xKerf = bKerf$, and hence $x \in bKerf$.

To prove the second inclusion, suppose that $x \in Kerf$ is an arbitrary element. Then, we have $f(bx) = f(b)f(x) = a'e = a'$ or $bx \in f^{-1}(\{a'\})$. This completes the proof. ■

Theorem 11.20 *Let G and H be groups and $f : G \to H$ be a homomorphism. Then, f is one to one if and only if $Kerf = \{e\}$.*

Proof Suppose that f is one to one. If $x \in Kerf$, then $f(x) = e$. On the other hand, we always have $f(e) = e$. Now, since $f(x) = f(e)$ and f is one to one, it follows that $x = e$. This proves that $Kerf = \{e\}$.

Conversely, let $Kerf = \{e\}$ and assume that a and b are elements of G such that $f(a) = f(b)$. Then, $f(a)f(b)^{-1} = e$, or equivalently $f(ab^{-1}) = e$. This means that $ab^{-1} \in Kerf = \{e\}$, and so $a = b$. Hence, f is a one to one function. ■

Exercises

1. Let X be a non-empty set of generators of G. Let $f : G \to H$ and $g : G \to H$ be homomorphisms. If for every $x \in X$, $f(x) = g(x)$, prove that $f = g$.
2. Let G and H be groups and $f : G \to H$ be a homomorphism. Show that $f([x, y]) = [f(x), f(y)]$, for all $x, y \in G$.
3. Describe all the homomorphisms from $\mathbb{Z}_{12}$ to itself.
4. Let $f : \mathbb{Z}_8 \to \mathbb{Z}_{32}$ be a homomorphism such that $f(1) = 4$. Compute $f(5)$. What is the kernel of f?
5. Show that there is a homomorphism from S_n to $\mathbb{Z}_2$ whose kernel is A_n.
6. Determine all homomorphisms from $\mathbb{Z}$ onto S_3. Determine all homomorphisms from $\mathbb{Z}$ to S_3.
7. Find all group homomorphisms from $\mathbb{Z}_4$ into $\mathbb{Z}_{10}$.
8. How many homomorphisms are there from $\mathbb{Z}_{20}$ onto $\mathbb{Z}_8$?
9. If G is a finitely generated group by a set with n elements and H is a finite group, prove that $|Hom(G, H)| \leq |H|^n$.
10. If f is a homomorphism from $\mathbb{Z}_{30}$ onto a group of order 5, determine the kernel of f.
11. Let G and H be groups and $f : G \to H$ be an onto homomorphism. If X is a subset of G that generates G, show that $f(X)$ generates H.
12. Find a homomorphism f from U_{30} to U_{30} with kernel $\{\overline{1}, \overline{11}\}$ and $f(\overline{7}) = \overline{7}$.
13. Let $\mathbb{Z}[x]$ be the group of polynomials in x with integer coefficients under addition. Prove that the function from $\mathbb{Z}[x]$ into $\mathbb{Z}$ given by $f(x) \mapsto f(3)$ is a homomorphism. Give a geometrical description of the kernel of this homomorphism.
14. Prove that the function from $\mathbb{R}$ under addition to $GL_2(\mathbb{R})$ that takes x to

$$\begin{bmatrix} \cos x & \sin x \\ -\sin x & \cos x \end{bmatrix}$$

    is a homomorphism. What is the kernel of this homomorphism?
15. Let G be a subgroup of some dihedral group. For each $x \in G$, we define

$$f(x) = \begin{cases} 1 & \text{if } x \text{ is a rotation} \\ -1 & \text{if } x \text{ is a reflection.} \end{cases}$$

    Prove that f is a homomorphism from G to the multiplicative group $\{1, -1\}$. What is the kernel?
16. (a) Let $n \geq 5$ and $m \geq 3$. Suppose that m is not divisible by 3. Let $f : S_n \to D_m$ be a homomorphism. Prove that A_n is contained in the kernel of f. How many homomorphisms $S_n \to D_m$ are there?
    (b) Let $n \geq 5$ and $m \geq 3$ be arbitrary, so m may be divisible by 3. How many homomorphisms $S_n \to D_m$ are there?

11.2 Isomorphism Theorems

We wish to have a way to determine if two groups have similar properties. The advantage of this is that if we could tell that two groups G and H have similar properties and we already know all the properties of G, then we would immediately know all the properties of H. The tool which will allow us to do this is called an isomorphism, from the Greek words "isos" which mean "same" and "morphe" which means "form".

Definition 11.21 Let G and H be groups. A function $f : G \to H$ is said to be an *isomorphism* if the following conditions are satisfied:

(1) f is a homomorphism;
(2) f is one to one;
(3) f is onto.

If there is an isomorphism from G onto H, we say that G and H are *isomorphic* and write $G \cong H$.

Example 11.22 If G is a group, then the identity function $id : G \to G$ defined by $id(x) = x$, for all $x \in G$, is an isomorphism.

Example 11.23 The group of real numbers $\mathbb{R}$ under addition and positive real numbers $\mathbb{R}^+$ under multiplication are isomorphic. Indeed, if we consider $f : \mathbb{R} \to \mathbb{R}^+$ by $f(x) = e^x$, then for every real numbers a and b we have $f(a + b) = e^{a+b} = e^a e^b = f(a)f(b)$. So, f is a homomorphism. Moreover, by the well-known results of calculus, f is one to one and onto.

An injective (or one to one) homomorphism is called a *monomorphism* and a surjective (or onto) homomorphism is called an *epimorphism*. Of course a bijective homomorphism is what we have been calling an isomorphism. A group H is said to be a *homomorphic image* of a group G, if there exists an epimorphism from G onto H.

Let G and H be groups and $f : G \to H$ be a homomorphism. Clearly, we have

(1) f is a monomorphism if and only if $Kerf = \{e\}$;
(2) f is an epimorphism if and only if $Imf = H$;
(3) f is an isomorphism if and only if $Kerf = \{e\}$ and $Imf = H$.

How do we demonstrate that two groups G and H are not isomorphic, if this is the case? A structural property of a group is one that must be shared by any isomorphic group. It is not concerned with names or some other non-structural characteristics of the elements. In order to prove that two groups G and H are not isomorphic, one needs to demonstrate that there is no isomorphism from G onto H. Usually, in practice, this is much easier than it sounds in general, and is accomplished by finding some structural property that holds in one group, but not in the other.

Example 11.24 $\mathbb{Z}_6 \ncong S_3$ because $\mathbb{Z}_6$ is abelian and S_3 is not abelian.

Example 11.25 The dihedral group D_{12} is not isomorphic to S_4 because D_{12} has 13 elements of order 2 (12 reflections and the rotation for π), while S_4 has only 9 such elements (transpositions and product of disjoint transpositions).

Lemma 11.26 *Let G and H be groups and $f : G \to H$ be an isomorphism. Then, $f^{-1} : H \to G$ is also an isomorphism.*

Proof Since f is a bijective function, by Theorem 5.5, it follows that f^{-1} exists and it is a bijective function from H onto G. So, it remains to be seen that f^{-1} is a homomorphism. Assume that x and y are arbitrary elements of H. Then, there exist $a, b \in G$ such that $f(a) = x$ and $f(b) = y$. This yields that $a = f^{-1}(x)$ and $b = f^{-1}(y)$. Hence, we can write $xy = f(a)f(b) = f(ab)$, and so $f^{-1}(xy) = ab$. This shows that $f^{-1}(xy) = f^{-1}(x)f^{-1}(y)$. Therefore, f^{-1} is a homomorphism. ■

Lemma 11.27 *If $f : G \to H$ and $g : H \to K$ are isomorphisms between groups, then so is the function $g \circ f$.*

Proof By Theorem 5.6, gof is a bijective function from G onto K. To check that $g \circ f$ is a homomorphism, let a and b be arbitrary elements of G. Then, we obtain

$$\begin{aligned}(g \circ f)(ab) &= g\big(f(ab)\big) = g\big(f(a)f(b)\big) \\ &= g\big(f(a)\big)g\big(f(b)\big) = (g \circ f)(a)(g \circ f)(b),\end{aligned}$$

where we used in turn the facts that f and g are homomorphisms. Therefore, $g \circ f$ is an isomorphism. ■

Theorem 11.28 *The relation of isomorphism between groups is an equivalence relation on the family of all groups.*

Proof The result follows by Lemmas 11.26 and 11.27. ■

Lemma 11.29 *Let G and H be two cyclic groups of the same order. Then, G and H are isomorphic.*

Proof Suppose that $G = \langle a \rangle$ and $H = \langle b \rangle$. If $x \in G$, then $x = a^i$, for some integer i. Define $f : G \to H$ by $f(x) = b^i$.

We first have to check that f is well defined. If G is infinite, then so is H and every element of G may be uniquely represented in the form a^i. Thus, f is automatically well defined in this case. Now, assume that G has order n, and suppose that $x = a^j$, too. We have to check that $b^i = b^j$.

Since $a^i = a^j$, it follows that $a^{i-j} = e$, and so $m|i - j$. Since $|H| = m$, it follows that $i - j = k|H|$, for some integer k. Consequently, we can write $b^{i-j} = b^{k|H|} = \big(b^{|H|}\big)^k = e$. This shows that $b^i = b^j$. Therefore, we conclude that f is well defined. Now, let a^i and a^j be two elements of G. Then, we have

$$f(a^i a^j) = f(a^{i+j}) = b^{i+j} = b^i b^j = f(a^i)f(a^j).$$

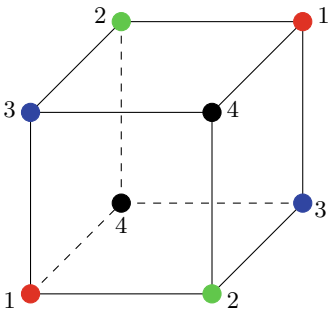


Fig. 11.3 Vertices of the cube with the same number are endpoints of the four diagonals of the cube

This means that f is a homomorphism. Moreover, the function $g : H \to G$ defined by $g(b^i) = a^i$ is the inverse of f, and so f is a one-to-one correspondence. This completes the proof. ■

Corollary 11.30 *Any infinite cyclic group is isomorphic to the additive group* $\mathbb{Z}$. *Any finite cyclic group of order* n *is isomorphic to* $\mathbb{Z}_n$, *the additive group of modulo* n.

Proof The result follows directly from Lemma 11.29. ■

Example 11.31 (*The Rotation Group of a Cube*) A cube has 8 vertices, 12 edges, and 6 faces (see Fig. 11.3), each of which is a square. The cube has exactly 24 rotational symmetries, which comprise:

(1) 1 trivial rotation or the identity symmetry;
(2) 9 non-trivial rotations (by $\pi/2$, π and $3\pi/2$) about 3 axes joining the centers of opposite faces;
(3) 8 non-trivial rotations (by $2\pi/3$ and $4\pi/3$) about the 4 great diagonals;
(4) 4 non-trivial rotations (by π) about the 4 axes joining the midpoints of opposite edges.

Since the group of rotations of a cube has the same order as S_4, we need only prove that the group of rotations is isomorphic to a subgroup of S_4. We number the vertices of the cube from 1 to 4, and where opposite vertices are given the same number. Now a cube has 4 diagonals and any rotation induces a permutation of these diagonals. But we cannot just assume that different rotations correspond to different rotations. Observe that vertices with the same number are endpoints of the four diagonals of the cube. We can number the diagonals according to their endpoints. The permutations of the numbers of vertices in the front face of the cube correspond to permutations of the diagonals. Therefore, there is a one to one correspondence between the rotations of the cube and the permutations of the diagonals of the cube. The composition of rotations coincides with the product of permutations and so the group of rotations of a cube is isomorphic to the symmetric group S_4. We see two perpendicular axes where $\pi/2$ rotations give the permutations $\sigma = (1\,2\,3\,4)$ and $\tau = (1\,4\,3\,2)$. These induce the

subgroup $\{id,\ \sigma,\ \sigma^2,\ \sigma^3,\ \tau^2,\ \tau^2\sigma,\ \tau^2\sigma^2,\ \tau^2\sigma^3\}$ and the subgroup $\{id,\ \sigma\tau,\ (\sigma\tau)^2\}$. Consequently, the rotations induce all 24 permutations since $24 = (8, 3)$.

There are three theorems, formulated by E. Noether, describing the relationship between factor groups, normal subgroups and homomorphisms. These theorems are based on a basic result on homomorphisms presented in the following lemma.

Lemma 11.32 *If N is a normal subgroup of a group G, then the canonical map $\pi : G \to G/N$, given by $\pi(a) = aN$, is an onto homomorphism with kernel N.*

Proof Clearly, we have $\pi(ab) = abN = aNbN = \pi(a)\pi(b)$, for all $a, b \in G$. Moreover, since every element of G/N is of the form aN, for some $a \in G$, it follows that π is onto. Finally, for each $a \in G$, we have $a \in Ker\pi$ if and only if $\pi(a) = aN = N$ if and only if $a \in N$. ■

Theorem 11.33 *Let G and H be groups and $f : G \to H$ be a homomorphism and suppose that N is a normal subgroup of G satisfies $N \leq Kerf$. Then, there exists a unique homomorphism $g : G/N \to H$ which satisfies $g \circ \pi = f$.*

Proof Let aN be a left coset of N in G. Choose any $x \in aN$, then $x = ay$, for some $y \in N$. Moreover, we have $f(x) = f(ay) = f(a)f(y) = f(a)e = f(a)$, because $N \leq Kerf$. Therefore, f has the same effect on every element of the coset aN. So, if we define $g : G/N \to H$ by $g(aN) = f(a)$, for all $a \in G$, then g is well defined. Now, assume that aN and bN are arbitrary elements of G/N. Then, we have

$$g(aNbN) = g(abN) = f(ab) = f(a)f(b) = g(aN)g(bN).$$

Hence, g is a homomorphism such that $g \circ \pi = f$. At the end, we prove the uniqueness. Suppose that $g, g' : G/N \to H$ are homomorphisms which satisfy $g \circ \pi = f$ and $g' \circ \pi = f$. Then, we have $g\big(\pi(a)\big) = g'\big(\pi(a)\big)$, for all $a \in G$. Since π is onto, any element of G/N has the form $\pi(a)$, for some $a \in G$. Thus, we conclude that $g = g'$. This completes the proof. ■

Theorem 11.34 (First Isomorphism Theorem) *Let G and H be groups and $f : G \to H$ be a homomorphism. Then, there exists an isomorphism $g : G/Kerf \to Imf$ such that $g \circ \pi = f$. In particular, if f is onto, then $G/Kerf \cong H$. In this case, we say the diagram presented in Fig. 11.4 is commutative.*

Proof Since Imf is a subgroup of H, without loss of generality we may assume that $H = Imf$. With $N = Kerf$ we conclude that by Theorem 11.33 that there is an onto homomorphism $g : G/N \to Imf$ given by $g(aN) = f(a)$, for all $a \in G$. Since $Kerg = \{aN \mid f(a) = e\} = \{aN \mid a \in N\} = \{N\}$, it follows that g is one to one. This completes our proof. ■

Theorem 11.34 also is called the *fundamental theorem of homomorphism*, and it is one of the most basic theorems in group theory.

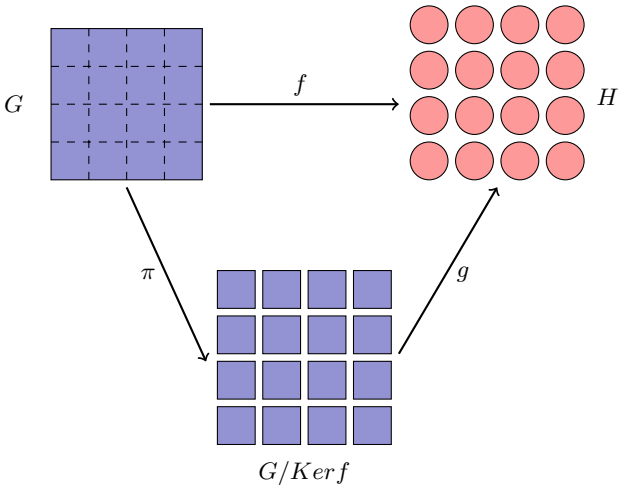
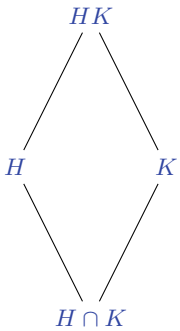


Fig. 11.4 Commutative diagram for the first isomorphism theorem

Fig. 11.5 The second isomorphism theorem



Example 11.35 Let $f : \mathbb{Z} \to \mathbb{Z}_n$ be the homomorphism defined in Example 11.3. We obtain $Imf = \mathbb{Z}_n$ and $Kerf = n\mathbb{Z}$, and so we conclude that $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$.

Example 11.36 The function $f : \mathbb{R} \to \mathbb{C}^*$ given by $f(x) = e^{2\pi xi}$, for all $x \in \mathbb{R}$, is a homomorphism. We obtain $Imf = \{z \in \mathbb{C} \mid |z| = 1\} := S^1$, the unit complex numbers and $Kerf = \mathbb{Z}$. Therefore, we can write $\mathbb{R}/\mathbb{Z} \cong S^1$.

Theorem 11.37 (Second Isomorphism Theorem) *Let G be a group and H, N be subgroups of G. If $N \trianglelefteq G$, then $H \cap N$ is normal in H and $H/(H \cap N) \cong HN/N$.*

The second isomorphism theorem can be represented pictorially as in Fig. 11.5.

Proof Since N is a normal subgroup of G, it follows that $NH = HN$, and so HN is a subgroup of G and also we have $N \leq HN$. Moreover, for every $x \in HN$, there exist $h \in H$ and $n \in N$ such that $xNx^{-1} = hnNn^{-1}h^{-1} = hNh^{-1} = N$. This yields

that $N \trianglelefteq HN$. Now, we define a function $f : H \to HN/N$ by $f(h) = hN$, for all $h \in H$. Clearly, f is a homomorphism. Consider $xN \in HN/N$, where $x \in HN$. Then, $x = hn$, for some $h \in H$ and $n \in N$. Hence, we have $xN = hnN = hN = f(h)$. This shows that f is onto. Now, by the first isomorphism theorem, we obtain $H/Kerf \cong HN/N$. If we can establish that $Kerf = H \cap N$, we shall obtain that $H \cap N$ is a normal subgroup of H and $H/(H \cap N) \cong HN/N$. Indeed, we have

$$\begin{aligned} Kerf &= \{h \in H \mid f(h) = N\} = \{h \in H \mid hN = N\} \\ &= \{h \in H \mid h \in N\} = H \cap N. \end{aligned}$$

This completes the proof. ■

Theorem 11.38 (Third Isomorphism Theorem) *Let H and N be normal subgroups of a group G such that $N \leq H$. Then, H/N is a normal subgroup of G/N and $(G/N)\big/(H/N) \cong G/H$.*

Proof We define $f : G/N \to G/H$ by $f(aN) = aH$, for every $a \in G$. Since f is defined on cosets, we should check that f is well defined. To begin with, if $aN = bN$, then $a^{-1}b \in N$. Since $N \leq H$, it follows that $a^{-1}b \in H$ or $aH = bH$. This shows that f is well defined. For every aN and bN in G/N, we have $f(aNbN) = f(abN) = abH = aHbH = f(aN)f(bN)$. Hence, f is a homomorphism. Clearly, f is onto, for if $aH \in G/H$, then $f(aN) = aH$. Furthermore, we have

$$\begin{aligned} Kerf &= \{aN \in G/N \mid f(aN) = H\} = \{aN \in G/N \mid aH = H\} \\ &= \{aN \in G/N \mid a \in H\} = H/N, \end{aligned}$$

as required. The result now follows by the first isomorphism theorem. ■

We may picture the third isomorphism theorem as illustration in Fig. 11.6.

Exercises

1. Find a group which is isomorphic to one of its proper subgroups.
2. Let $G = \mathbb{R} \setminus \{-1\}$ and define a binary operation on G by $a \star b = a + b + ab$. Prove that G is a group under this operation. Show that $(G, \star)$ is isomorphic to the multiplicative group of non-zero real numbers.
3. Prove that
   (a) The multiplication groups $\mathbb{R}^*$ and $\mathbb{C}^*$ are not isomorphic;
   (b) The additive groups $\mathbb{R}$ and $\mathbb{Q}$ are not isomorphic;
   (c) The additive groups $\mathbb{Z}$ and $\mathbb{Q}$ are not isomorphic;
4. Prove that every cyclic group of finite order n is isomorphic to the multiplicative group of all complex nth roots of 1.

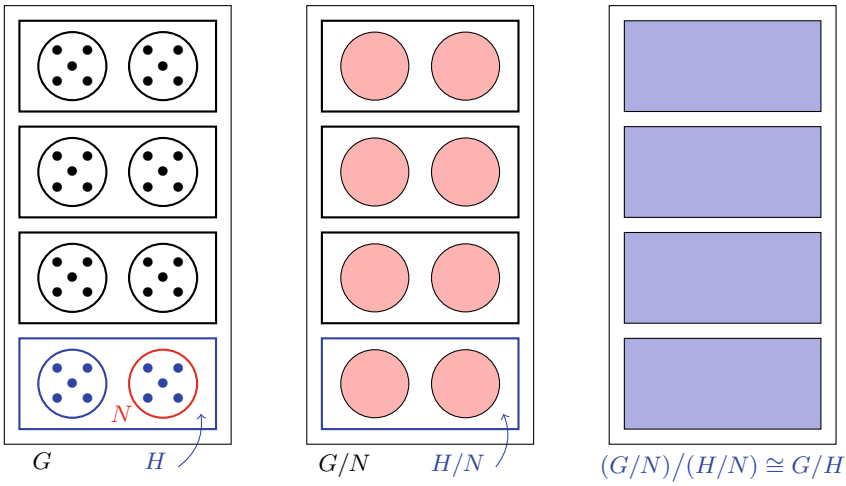


Fig. 11.6 Illustration for the third isomorphism theorem

5. Let $1 \leq n \leq 3$. Prove that any two groups containing exactly n elements are isomorphic.
6. If G is a non-abelian group of order 6, prove that $G \cong S_3$.
7. Let X_1 and X_2 be two sets. Suppose that there exists a one to one correspondence between X_1 and X_2. Show that there exists an isomorphism of S_{X_1} onto S_{X_2}.
8. Prove that any group of order 4 is isomorphic to the group $\mathbb{Z}_4$ or to the group $K = \{id,\ (1\ 2)(3\ 4),\ (1\ 3)(2\ 4),\ (1\ 4)(2\ 3)\}$.
9. Is $\mathbb{Q}/\mathbb{Z} \cong \mathbb{Q}$?
10. Show that the groups $\mathbb{Q}/\mathbb{Z}$ and $\mathbb{R}/\mathbb{Q}$ can not be isomorphic.
11. Let $f, g : \mathbb{R} \to \mathbb{R}$ be real valued functions defined by $f(x) = 1/x$ and $g(x) = (x-1)/x$. Then, f and g generate a group G with the operation given by function composition. Prove that $G \cong S_3$.
12. Let X be a non-empty set and $G = \{f \mid f : X \to \mathbb{Z}_2\}$. Show that

    (a) G is a group addition of functions;
    (b) $\mathcal{P}(X)$ is a group under the binary operation

$$A \triangle B = (A \cup B) - (A \cap B);$$

    (c) $(\mathcal{P}(X), \triangle) \cong (G, +)$.

13. Show that the nth roots of unity are isomorphic to $\mathbb{Z}_n$.
14. Show that to each positive integer n there exist only a finite number of pairwise non-isomorphic groups of order n.
15. Let G be a non-abelian group. Prove that the group of automorphisms of G is not cyclic.

16. Prove that D_4 and Q_8 are not isomorphic.
17. Show that U_{17} is isomorphic to Z_{16}.
18. Show that the three groups $\mathbb{Z}_6$, U_9 and U_{18} are isomorphic to each other.
19. How many pairwise non-isomorphic groups can you find which are homomorphic images of S_3?
20. Suppose that for each prime p, $\mathbb{Z}_p$ is the homomorphic image of a group G. What can we say about $|G|$?
21. Prove that $GL_2(\mathbb{Z}_2) \cong S_3$.
22. Show that D_4 is isomorphic to the subgroup of all lower triangular matrices in $GL_3(\mathbb{Z}_2)$.
23. Show that $SL_2(\mathbb{Z}_3)$ is not isomorphic to S_4.
24. Explain why S_n ($n \geq 3$) contains a subgroup isomorphic to D_n.
25. For real numbers a and b with $a \neq 0$, define $f_{ab} : \mathbb{R} \to \mathbb{R}$ by $f_{ab}(x) = ax + b$, for all $x \in \mathbb{R}$. Let $G = \{f_{ab} \mid a, b \in \mathbb{R} \text{ and } a \neq 0\}$ and $N = \{f_{1b} \mid b \in \mathbb{R}\}$. Prove that N is a normal subgroup of G and G/N is isomorphic to the group of non-zero real numbers under multiplication.
26. Let $G = \{z \in \mathbb{C} \mid z^n = 1, \text{ for some positive integer } n\}$. Prove that for any fixed integer $k > 1$, the function f from G to itself defined by $f(z) = z^k$, for all $z \in G$, is an onto homomorphism but is not an isomorphism.
27. Let a group G contain two normal subgroups K and N. Let H be a subgroup of G. Prove that $HK/K \cong HN/N$ if $H \cap K = H \cap N$.
28. In the group $GL_2(\mathbb{Z}_3)$, let

$$H = \left\langle \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} -1 & 1 \\ 1 & 1 \end{bmatrix} \right\rangle.$$

    Prove that $H \cong Q_8$ and $H \trianglelefteq GL_2(\mathbb{Z}_3)$.
29. Let G be a group, and suppose that S be any set for which there exists a bijective function $f : G \to S$. Define a binary operation on S by setting $a \cdot b = f\big(f^{-1}(a) f^{-1}(b)\big)$, for all $a, b \in S$. Prove that S is a group under this binary operation, and that f is actually a group isomorphism.
30. Let G be defined as all formal symbols $x^i y^j$, $i = 0,\ 1$ and $j = 0, 1, \ldots, n-1$, where we assume

$$\begin{aligned} &x^i y^j = x^{i'} y^{j'} \ \Leftrightarrow\ i = i',\ j = j', \\ &x^2 = y^n = e,\ n > 2, \\ &xy = y^{-1} x. \end{aligned}$$

    (a) Find the form of the product $(x^i y^j)(x^k y^l)$ as $x^r y^s$;
    (b) Prove that G is non-abelian of order $2n$;
    (c) If n is odd, prove that the center of G is $\{e\}$, while if n is even the center of G is larger than $\{e\}$;
    (d) Can you interpret this group as the dihedral group of order $2n$.

11.3 Cayley's Theorem

Our next subject is a classic theorem of Cayley. The proof of this theorem is not difficult, and it is a good exercise in group theory as it uses many concepts previously studied. Then, an important generalization of it is given.

Theorem 11.39 (Cayley's Theorem) *Let G be a given group. Then, there exists a set X such that G is isomorphic to a permutation group on X.*

Proof We choose the set X consisting of all the elements of G. For each element $a \in G$, let ρ_a be a function on X defined by the formula

$$\rho_a(x) = xa,$$

for all $x \in X$. It follows that ρ_a is a permutation on X. Furthermore, the associative law proves

$$\rho_{ab} = \rho_a \circ \rho_b,$$

for all $a, b \in G$. Thus, the function ρ is a homomorphism from G into the symmetric group S_X. Clearly, ρ_a is the identity function on X if and only if $a = e$. This means that ρ is one to one. Hence, G is isomorphic to the image $\rho(G)$ which is a permutation group on X. ■

If a group G is isomorphic to a subgroup of a group H, we say G *embeds* in H. In this case there is an embedding (another word for one to one homomorphism) $G \hookrightarrow H$ which identifies G with its image in H. So, Cayley's Theorem says that every finite group embeds in a symmetric group.

Theorem 11.40 (Generalized Cayley's Theorem) *Let H be a subgroup of a group G, and X be the set of all left cosets of H in G. Then, there exists a homomorphism from G into the permutation group S_X whose kernel is the largest normal subgroup of G that is contained in H.*

Proof Suppose that $H \leq G$ and $X = \{xH \mid x \in G\}$. Note that X need not be a group itself. If a is a fixed element of G, we define $\theta_a : X \to X$ by $\theta_a(xH) = axH$, for all $x \in G$. Simulating the proof of Theorem 11.39, we find that $\theta_a \in S_X$ and $\theta_{ab} = \theta_a\theta_b$. This shows that the function $f : G \to S_X$ defined by $f(a) = \theta_a$ is a homomorphism of G into S_X. Next, we identify the kernel of f. We have

$$\begin{aligned}
Kerf &= \{a \in G \mid f(a) = \theta_e\} \\
&= \{a \in G \mid \theta_a(xH) = \theta_e(xH), \text{ for all } x \in G\} \\
&= \{a \in G \mid axH = xH, \text{ for all } x \in G\} \\
&= \{a \in G \mid x^{-1}axH = H, \text{ for all } x \in G\} \\
&= \{a \in G \mid x^{-1}ax \in H, \text{ for all } x \in G\} \\
&= \{a \in G \mid a \in xHx^{-1}, \text{ for all } x \in G\} \\
&= \bigcap_{x \in G} xHx^{-1} \leq H.
\end{aligned}$$

Now, we claim that from this characterization of $Kerf$, $Kerf$ must be the largest normal subgroup of G which is contained in H. To prove this, suppose that N is a normal subgroup of G contained in H. Using $N \leq H$, it is immediate that $N = xNx^{-1} \subseteq xHx^{-1}$, for all $x \in G$. Thus, we conclude that

$$N \leq \bigcap_{x \in G} xHx^{-1} = Kerf.$$

This completes the proof. ■

Note that Theorem 11.40 reduces to Cayley's Theorem in the special case of $H = \{e\}$.

In Theorem 3.56, we proved that a Cayley table is a Latin square, i.e., the rows and columns are permutation of one another. However, the associative law is not easy to discern by the naked eye. In Theorem 3.57, we studied a method for the verification of the associative law. Now, by using a method similar the proof of Cayley's Theorem, we give another procedure for verification of the associative law.

Theorem 11.41 *A Latin square is a Cayley table if composite of two rows is some row in the table.*

Proof We use $1, 2, \ldots, n$ to denote the entries in a Latin square and a_{ij} denote the entry at the ith row and the jth column. In order to prove the statement, it remains to check if associative law holds in the set $G = \{1, 2, \ldots, n\}$ with the binary operation $\star$ defined by the given Latin square. We assume 1 is the identity element.

Simulating the proof of Theorem 11.39, we define $\sigma : G \to S_n$ by $\sigma(j) = \sigma_j$ such that $i\sigma_j = a_{ij} = i \star j$, for all $i, j \in G$. The right cancellation law guarantees that σ_j is indeed in S_n. Although G is a set for all we know, S_G is a group. Associative law in G amounts to the relation $\sigma_i\sigma_j = \sigma_{i\star j}$, for all $i, j \in G$. If that is true, then $\sigma(G)$ is a subgroup of S_G. Conversely, if $\sigma(G)$ is a subgroup of S_G, then the associative law holds, for we claim that $\sigma_i\sigma_j$, which is σ_k, for some $k \in G$, is indeed $\sigma_{i\star j}$. To see this, we show that k must be $i \star j$. Toward this end, consider $1\sigma_i\sigma_j$ and $1\sigma_k$. The former is equal to $(1 \star i)\sigma_j = i\sigma_j = i \star j$, while the later is equal to $1 \star k = k$. Hence, it reduces to check if $\sigma(G)$ is a subgroup of S_G. Since S_G is a finite group, we need only to check that if the multiplication of any two permutations in $\sigma(G)$ is still a permutation in $\sigma(G)$. This can be achieved by checking the row of the Latin square. ■

Example 11.42 As a quick test, examine the following two Latin squares of order 4. One of these turns out to be a Latin square that we can get from a group, while the other does not. Which is which?

x	a	b	c
c	x	a	b
b	c	x	a
a	b	c	x

x	a	b	c	d
a	d	c	x	b
b	x	a	d	c
c	b	d	a	x
d	c	x	b	a

It is easy to check that the first square can be the Cayley table for the group $\mathbb{Z}_4$, if we consider $x = \overline{0}$, $a = \overline{1}$, $b = \overline{2}$ and $c = \overline{3}$.

The second table seems so different. Assume that it is a Cayley table of a group. Then, for some ordering $[\sigma_1,\ \sigma_2,\ \sigma_3,\ \sigma_4,\ \sigma_5]$ of our group elements and another ordering $[\tau_1,\ \tau_2,\ \tau_3,\ \tau_4,\ \tau_5]$, we have

$\cdot$	τ_1	τ_2	τ_3	τ_4	τ_5
σ_1	x	a	b	c	d
σ_2	a	d	c	x	b
σ_3	b	x	a	d	c
σ_4	c	b	d	a	x
σ_5	d	c	x	b	a

One of the $\sigma_1,\ \sigma_2,\ \sigma_3,\ \sigma_4,\ \sigma_5$ is the identity element. One of the five rows of the table must be $[\tau_1,\ \tau_2,\ \tau_3,\ \tau_4,\ \tau_5]$. In particular, we can actually assume that our top row is formed by taking σ_1^{-1} and acting to each element of $[x,\ a,\ b,\ c,\ d]$, because the row $[x,\ a,\ b,\ c,\ d]$ is just multiplying $[\tau_1,\ \tau_2,\ \tau_3,\ \tau_4,\ \tau_5]$ to σ_1, i.e., $[\tau_1\sigma_1,\ \tau_2\sigma_1,\ \tau_3\sigma_1,\ \tau_4\sigma_1,\ \tau_5\tau_4] = [x,\ a,\ b,\ c,\ d]$, or equivalently, $[\tau_1,\ \tau_2,\ \tau_3,\ \tau_4,\ \tau_5] = [x\sigma_1^{-1},\ a\sigma_1^{-1},\ b\sigma_1^{-1},\ c\sigma_1^{-1},\ d\sigma_1^{-1}]$. We can think of these as permutations of the row $[x,\ a,\ b,\ c,\ d]$. For example, the row corresponding to σ_2, can be considered as the permutation

$$\sigma_2 = \begin{pmatrix} x & a & b & c & d \\ a & d & c & x & b \end{pmatrix}.$$

Similarly, the row corresponding to σ_3, gives us the following permutation:

$$\sigma_3 = \begin{pmatrix} x & a & b & c & d \\ b & x & a & d & c \end{pmatrix}.$$

If we consider the product of σ_2 and σ_3, then we obtain

$$\sigma_2\sigma_3 = \begin{pmatrix} x & a & b & c & d \\ a & d & c & x & b \end{pmatrix}\begin{pmatrix} x & a & b & c & d \\ b & x & a & d & c \end{pmatrix} = \begin{pmatrix} x & a & b & c & d \\ x & c & d & b & a \end{pmatrix}.$$

Exercises

1. How many ways are there to embed $\mathbb{Z}_4$ in S_4?
2. How many ways are there to embed D_4 in S_4?
3. Let G be a group and H be a subgroup of G. Let $X = \{Ha \mid a \in G\}$ be the set of all right cosets of H in G. Define, for $b \in G$, $T_b : X \to X$ by $T_b(Ha) = Hab^{-1}$.

(a) Prove that the function $f : G \to S_X$ defined by $f(b) = T_b$, for all $b \in G$, is a homomorphism;
(b) Describe $Kerf$;
(c) Show that $Kerf$ is the largest normal subgroup of G lying in H.

4. Show that the function $f : S_n \to A_{n+2}$ given by

$$f(\sigma) = \begin{cases} \sigma & \text{if } \sigma \text{ is even} \\ \sigma(n+1\ n+2) & \text{if } \sigma \text{ is odd,} \end{cases}$$

is an isomorphism between S_n and a subgroup of A_{n+2}. Deduce that every finite group is isomorphic to a subgroup of A_{n+2}.
5. Show that, for $n \leq 4$, any Latin square of order n can be obtained from the Cayley table of a group by permuting rows, columns, and symbols; but this is not true for $n = 5$.

11.4 Automorphisms

A homomorphism of a group G into itself is called an *endomorphism*. The identity function is clearly an endomorphism. The set of all endomorphism from G to itself is denoted by $End(G)$.

Definition 11.43 By an *automorphism* of a group G, we shall mean an isomorphism of G onto itself.

Lemma 11.44 *Let G be a group and $a \in G$ is a fixed element of G. If a function $\phi_a : G \to G$ is defined by $\phi_a(x) = axa^{-1}$, for every $x \in G$, then ϕ_a is an automorphism of G.*

Proof Assume that x and y are arbitrary elements of G. Then, we have $\phi_a(x)\phi_a(y) = (axa^{-1})(aya^{-1} = a(xy)a^{-1} = \phi_a(xy)$. So, ϕ_a is a homomorphism. Now, we investigate that ϕ_a is a bijective function. In fact, if $\phi_a(x) = \phi_a(y)$, then $axa^{-1} = aya^{-1}$, and so $x = y$. This shows that ϕ_a is one to one. On the other hand, for each $y \in G$, we can write $\phi_a(a^{-1}ya) = aa^{-1}yaa^{-1} = y$. This means that ϕ_a is onto. ■

The function ϕ_a is called the *inner automorphism* by a.

Let $Aut(G)$ denote the set of all automorphisms of G. For the product of elements of $Aut(G)$, we can use the composition of functions.

Theorem 11.45 *If G is a group, then $Aut(G)$ is also a group.*

Proof Note that the identity function belongs to $Aut(G)$. Since the resultant composition for functions is in general associative, it follows that the composition in $Aut(G)$ is also associative. Now, the result follows immediately from Lemmas 11.26 and 11.27. ■

$Aut(G)$ is called the *group of automorphism* of G.

Theorem 11.46 *The set of all inner automorphisms is a normal subgroup of $Aut(G)$, which is written $Inn(G)$.*

Proof Clearly, the identity function lies in $Inn(G)$ as $id(x) = x = exe^{-1} = \phi_e(x)$, for all $x \in G$. Now, let a, b and x be arbitrary elements of G. We can write $\phi_a \circ \phi_b(x) = \phi_a(bxb^{-1}) = abxb^{-1}a^{-1} = (ab)x(ab)^{-1} = \phi_{ab}(x)$. This means that

$$\phi_a \circ \phi_b = \phi_{ab}. \tag{11.1}$$

Thus, $\phi_a \circ \phi_b \in Inn(G)$. Moreover, using (11.1), we can write $\phi_a \circ \phi_{a^{-1}} = \phi_{a^{-1}} \circ \phi_a = \phi_e$. This implies that $(\phi_a)^{-1} = \phi_{a^{-1}} \in Inn(G)$. Hence, we conclude that $Inn(G)$ is a subgroup of $Aut(G)$. To prove that $Inn(G)$ is a normal subgroup of $Aut(G)$, let $\phi_a \in Inn(G)$ and $f \in Aut(G)$ be arbitrary elements. Then, for any $x \in G$, we have

$$\begin{aligned}(f \circ \phi_a \circ f^{-1})(x) &= f \circ \phi_a\big(f^{-1}(x)\big) = f\big(af^{-1}(x)a^{-1}\big) \\ &= f(a)f\big(f^{-1}(x)\big)f(a^{-1}) = f(a)xf(a)^{-1} = \phi_{f(a)}(x).\end{aligned}$$

This shows that $f \circ \phi_a \circ f^{-1} \in Inn(G)$, and so $Inn(G) \trianglelefteq Aut(G)$. ■

Definition 11.47 $Inn(G)$ is called the *group of inner automorphisms* of G. If G is abelian, then $Inn(G) = \{e\}$. An automorphism of G which is not inner is called *outer*. The factor group $Out(G) = Aut(G)/Inn(G)$ is called the *group of outer automorphisms* of G even although its elements are not automorphism.

Theorem 11.48 *The group of inner automorphisms of G is isomorphic to the quotient group $G/Z(G)$, where $Z(G)$ is the center of G.*

Proof We define $f : G \to Inn(G)$ by $f(a) = \phi_a$, for all $a \in G$. Then, we can write $f(ab) = \phi_{ab} = \phi_a \circ \phi_b = f(a)f(b)$, for all $a, b \in G$. This means that f is a homomorphism. Since each element of $Inn(G)$ is of the form ϕ_a, it follows that f is onto. Hence, by applying the first isomorphism theorem, we obtain $G/Kerf \cong Inn(G)$. Now, the result follows if we show that $Kerf = Z(G)$. An element a of G lies in the kernel K if and only if $\phi_a = id$, i.e., $a^{-1}xa = x$, for all $x \in G$. This yields that $Kerf = Z(G)$. ■

Theorem 11.49 *Let $G = \langle a \rangle$ be a cyclic group, and suppose that f is an endomorphism of G. Then, f is an automorphism if and only if $f(a)$ is a generator of G.*

Proof Suppose that f is an automorphism of G. Let x be an arbitrary element of G. Since f is onto, it follows that there is an element $y \in G$ such that $f(y) = x$. On the other hand, since $y \in \langle a \rangle$, it follows that $y = a^n$, for some integer n. So, we have $x = f(y) = f(a^n) = f(a)^n$. This shows that $G = \langle f(a) \rangle$.

Conversely, assume that $G = \langle f(a) \rangle$. We must show that f is bijective. Let $y \in G$

be an arbitrary element. Then, $y = f(a)^k$, for some integer k. Hence, we obtain $y = f(a^k)$, and so we conclude that f is onto. To prove that f is one to one, we consider the following two cases:

Case 1: Let G be finite. Then, f is clearly one to one.

Case 2: Let G be infinite, and suppose that $f(x) = f(y)$. Then, $f(a^i) = f(a^j)$, where $a^i = x$ and $a^j = y$, for some integers i and j. So, we can write $f(a)^i = f(a)^j$, or equivalently $f(a)^{i-j} = e$. Since G is infinite, it follows that $i = j$, and so $x = y$. Consequently, f is one to one. ■

Theorem 11.50 *If G is an infinite group, then $Aut(G)$ is of order 2.*

Proof The result follows from Theorem 11.49 and the fact that the number of generators of an infinite cyclic group is 2. ■

Theorem 11.51 *If $G = \langle a \rangle$ is a finite cyclic group of order n, then $Aut(G) \cong U_n$.*

Proof Since G is finite, by Corollary 4.33, the number of generators of G is $\varphi(n)$. This yields that $|Aut(G)| = \varphi(n)$. Suppose that $f : G \to G$ be an automorphism of G. Then, we have $f(a) = a^k$, for some integer k. Since $f(a)$ is a generator of G, it follows that $k < n$ and $(k, n) = 1$. Now, we define $\theta : Aut(G) \to U_n$ by $\theta(f) = \overline{k}$, for all $f \in Aut(G)$. Let f and g be two elements of $Aut(G)$ such that $f(a) = a^k$ and $g(a) = a^l$, for some integers k and l. So, we have $(f \circ g)(a) = f(a^l) = a^{kl}$. Therefore, we obtain $\theta(f \circ g) = \overline{kl} = \overline{k}\,\overline{l} = \theta(f)\theta(g)$. This shows that θ is a homomorphism. Now, if $\theta(f) = \theta(g)$, then $\overline{k} = \overline{l}$. This implies that $n|k - l$. Since $k < n, l < n$, $(k, n) = 1$ and $(l, n) = 1$, we conclude that $k = l$, and so $f = g$. This proves that f is one to one. Finally, since $|Aut(G)| = |U_n| = \varphi(n)$, it follows that θ is onto. Therefore, θ is an isomorphism. ■

Theorem 11.52 *If G is a group of order p^n, then $|Aut(G)| = p^n(p - 1)$.*

Proof It follows directly from Theorem 11.51. ■

Exercises

1. Find all of the automorphisms of $\mathbb{Z}_8$.
2. Prove that $a + ib \mapsto a - ib$ is an automorphism of $\mathbb{C}^*$.
3. Prove that $Aut(S_3) \cong S_3$.
4. What are the inner automorphisms of the quaternion group Q_8? Is $Inn(G) = Aut(G)$ in this case?
5. Prove that $Aut(D_4) \cong D_4$ and yet D_4 has outer automorphism.
6. Prove that $Aut(A_5) \cong S_5$.
7. Let G be any group. Prove that the function f from G to itself defined by $f(a) = a^{-1}$, for all $a \in G$, is an automorphism if and only if G is abelian.

8. If G is a group such that $Aut(G)$ is the trivial group, prove that G is abelian and every element of G is of order 2.
9. If $G \cong H$, prove that $Aut(G) \cong Aut(H)$ and $Inn(G) \cong Inn(H)$.
10. Find two non-isomorphic groups G and H such that $Aut(G) \cong Aut(H)$.
11. Prove that every finite group having more than two elements has a non-trivial automorphism.
12. If an automorphism fixes more than half of the elements of a finite group, prove that it is the identity automorphism.
13. Let G be a group and $f : G \to G$ defined by $f(x) = x^n$, for all $x \in G$, be an automorphism. Prove that for each $a \in G$, we have $a^{n-1} \in Z(G)$.
14. Prove that if G is a group in which every non-identity element is of order 2, then G has a non-trivial automorphism.
15. Let G be the group of order 9 generated by elements a and b, where $a^3 = b^3 = e$. Find all the automorphisms of G.
16. Prove that the group of inner automorphisms of the symmetric group S_n ($n \geq 3$) is isomorphic to S_n.
17. Prove that every automorphism of S_4 is inner. What is the order of the group of automorphisms of S_4?
18. Let G be the additive group of numbers of the form mp^n, where m and n are integers and p is a fixed prime. Describe $End(G)$ and $Aut(G)$.
19. Prove that if G is a finite non-cyclic abelian group, then $Aut(G)$ is not abelian.
20. Let f be an automorphism of a finite group G with the property that $f(x) = x$ if and only if $x = e$. Suppose further that $f^2 = id$, the identity element of $Aut(G)$. Show that G is abelian.
    Hint: First prove that every $a \in G$ can be represented as $x^{-1} f(x)$, for some $x \in G$.

11.5 Characteristic Subgroups

Recall that a subgroup of a group G is normal if it is invariant under conjugation. Now, conjugation is just a special case of an automorphism of G.

Definition 11.53 Let G be a group and H be a subgroup of G. We say that H is a *characteristic subgroup* of G, if for every automorphism f of G, $f(H) = H$.

Example 11.54 Let G be a group. Then, G itself and the identity subgroup $\{e\}$ are characteristic subgroups of G.

Example 11.55 The center of any group is a characteristic subgroup. Indeed, let $f \in Aut(G)$ be arbitrary. Pick $z \in Z(G)$, then z commutes with every element of G. Pick an element $a \in G$. Since f is onto, it follows that $a = f(b)$, for some $b \in G$. Hence, we can write

$$af(z) = f(b)f(z) = f(bz) = f(zb) = f(z)f(b) = f(z)a.$$

Since a is arbitrary, it follows that $f(z)$ commutes with every element of G, and so $f(z) \in Z(G)$. Consequently, we get $f\big(Z(G)\big) \subseteq Z(G)$. Applying the same result to the inverse of f, we obtain $f^{-1}\big(Z(G)\big) \subseteq Z(G)$. This implies that $Z(G) \subseteq f\big(Z(G)\big)$. Therefore, we have $f\big(Z(G)\big) = Z(G)$, and this shows that $Z(G)$ is a characteristic subgroup of G.

Example 11.56 Derived subgroup G' of a group G is a characteristic subgroup of G, since for every $f \in AUt(G)$ and $a, b \in G$, we have $f([a, b]) = [f(a), f(b)]$.

Example 11.57 If H is the only subgroup of G of order m, then it must be characteristic, because $f(H)$, for all $f \in Aut(G)$, is again a subgroup of G of order m.

Note that f restricted to H a characteristic subgroup (denoted by $f|_H$) is an automorphism of H (it is an endomorphism by definition of H being characteristic).

Here are a few immediate properties of characteristic subgroups.

Theorem 11.58 *Let G be a group, and let H, K be subgroups of G.*

(1) If H is characteristic in K and K is characteristic in G, then H is characteristic in G (being characteristic is transitive);
(2) If H is characteristic in K, and K is normal in G, then H is normal in G.

Proof (1) Note that by assumption $H \leq K \leq G$. Let f be an automorphism of G. Since K is characteristic in G, it follows that $f(K) = K$ by definition, and so $f|_K$ is an automorphism of K. Now, since H is characteristic in K, it follows that $f|_K(H) = H$. But $f|_K$ is just the restriction of f (recall $H \leq K$), and hence $f(H) = H$.

(2) Consider the automorphism of K given by $k \mapsto aka^{-1}$, $a \in G$, which is well defined since K is normal in G. For any choice of a, we get a different automorphism of K, which will always preserve H, because H is characteristic in K. Consequently, $aHa^{-1} \subseteq H$. This shows that H is normal in G. ■

Theorem 11.59 *Let G be a finite group and N be a normal subgroup of G. If $(|N|, [G : N]) = 1$, then N is a characteristic subgroup of G.*

Proof Suppose that $|N| = m$, $[G : N] = n$ and $(m, n) = 1$. Then, we conclude that $|G| = mn$. Let $f \in Aut(G)$ be an arbitrary automorphism. Since N is a normal subgroup of G, it follows that $Nf(N)$ is a subgroup of G. Moreover, we have

$$|Nf(N)| = \frac{|N|\,|f(N)|}{|N \cap f(N)|}.$$

Assume that $k = |N \cap f(N)|$. Since $|N| = |f(N)| = m$, it follows that $|Nf(N)| = m^2/k$. Since $Nf(N) \leq G$, it follows that $|Nf(N)| \big| |G|$, or equivalently $m^2/k | mn$. Since $(m, n) = 1$, it follows that $m = k$. Hence, we obtain $|N \cap f(N)| = |N|$. This yields that $N \cap f(N) = N$, and so $N \subseteq f(N)$. Finally, we conclude that $N = f(N)$, and this completes the proof. ■

Exercises

1. Prove that every subgroup of a cyclic group is characteristic.
2. Give an example of a group G containing a normal subgroup that is not a characteristic subgroup.
   Hint: Let G be abelian.
3. If H is a characteristic subgroup of a group G, prove that $C_G(H)$ is also a characteristic subgroup of G.
4. Let G be a finitely generated group and let H be a subgroup of G with finite index. Show that there is a subgroup K of H that is characteristic in G and has finite index in G.
5. Let G be a group and H, K be subgroups of G. If H is a characteristic subgroup of G and $H \subseteq K \subseteq G$, prove that K/H is a characteristic subgroup of G/H implies that K is a characteristic subgroup of G.

11.6 Another View of Linear Groups

Let V be a finite dimensional vector space over a field $\mathbb{F}$. The set of all invertible transformations of V to V is denoted by $GL(V, \mathbb{F})$. This set has a group structure under composition of transformations. On the other hand, in Sect. 7.1, we applied the notation $GL_n(\mathbb{F})$ for the general linear group, the group of $n \times n$ invertible matrices.

Theorem 11.60 *Let V be a finite vector space of dimension n over a field $\mathbb{F}$ with ordered basis $\{v_1, \ldots, v_n\}$. Then the map $\theta : GL(V, \mathbb{F}) \to GL_n(\mathbb{F})$ corresponding to this basis is an isomorphism of groups.*

Proof The result immediately follows by the properties of linear transformation. ■

Hence, since $GL(V, \mathbb{F}) \cong GL_n(\mathbb{F})$, we can consider the elements of general linear group as invertible matrices as well as invertible linear operators on V. The special linear group $SL_n(\mathbb{F})$ is the set of all matrices $A \in GL_n(\mathbb{F})$ such that $\det(A) = 1$. We note that if V is a finite vector space of dimension n over a field $\mathbb{F}$ with ordered basis $\{v_1, \ldots, v_n\}$, and if $\theta : GL(V, \mathbb{F}) \to GL_n(\mathbb{F})$ is as above, then the set

$$\{T \in GL(V, \mathbb{F}) \mid \det\big(\theta(T)\big) = 1\}$$

is independent of the choice of the basis. This subset is the subgroup $\theta^{-1}\big(SL(n, \mathbb{F})\big)$, and we denote it by $SL(V, \mathbb{F})$. It is clear that $SL(V, \mathbb{F}) \cong SL_n(\mathbb{F})$.

Theorem 11.61 *If $\mathbb{F}$ is a finite field with q elements, then*

$$|SL_n(\mathbb{F})| = q^{\binom{n}{2}} \prod_{i=2}^{n} (q^i - 1).$$

Proof Let $\mathbb{F}^*$ be the multiplicative group of $\mathbb{F}$. We define $f : GL_n(\mathbb{F}) \to \mathbb{F}^*$ by $f(A) = \det(A)$, for all $A \in GL_n(\mathbb{F})$. It is easy to check that f is an onto homomorphism. Moreover, we see that $Ker f = SL_n(\mathbb{F})$. So, by the first isomorphism theorem, we conclude that

$$\frac{GL_n(\mathbb{F})}{SL_n(\mathbb{F})} \cong \mathbb{F}^*.$$

This implies that $|SL_n(\mathbb{F})| = |GL_n(\mathbb{F})| \cdot |\mathbb{F}^*|$. Now, by Theorem 7.32, the result follows. ■

Definition 11.62 (*Projective Linear Groups*) Let $\mathbb{F}$ be a field and n a positive integer. The set $Z = \{aI_n \mid a \in \mathbb{F}^*\}$ of scalar matrices is a normal subgroup of $GL_n(\mathbb{F})$. The *projective general linear group* over $\mathbb{F}$ is defined by

$$PGL_n(\mathbb{F}) = \frac{GL_n(\mathbb{F})}{Z},$$

and the *projective special linear group* over $\mathbb{F}$ is defined by

$$PSL_n(\mathbb{F}) = \frac{SL_n(\mathbb{F})}{SL_n(\mathbb{F}) \cap Z} \cong \frac{SL_n(\mathbb{F})Z}{Z}.$$

The projective groups are obtained from the corresponding ordinary linear groups by identifying matrices that are scalar multiples of each other.

An *automorphism of a field* $\mathbb{F}$ is a one to one function σ from $\mathbb{F}$ onto itself such that $\sigma(a + b) = \sigma(a) + \sigma(b)$ and $\sigma(ab) = \sigma(a)\sigma(b)$, for all $a, b \in \mathbb{F}$. Let $Aut(\mathbb{F})$ be the set of all automorphism of $\mathbb{F}$. We denote $\sigma(a) := a^\sigma$.

Lemma 11.63 *If $\mathbb{F}$ is a field, then $Aut(\mathbb{F})$ is a group under composition of functions.*

Proof It is straightforward. ■

Definition 11.64 Let V be a finite dimensional vector space on a field $\mathbb{F}$. A function $T : V \to V$ is called a *semi-linear transformation* on V with associated field automorphism $\sigma \in Aut(\mathbb{F})$, if $T(v_1 + v_2) = T(v_1) + T(v_2)$ and $T(cv_1) = c^\sigma T(v_1)$, for all $v_1, v_2 \in V$ and $c \in \mathbb{F}$.

Example 11.65 Let $V = \mathbb{C}^n$ be the vector space of dimension n over $\mathbb{C}$, and σ be an automorphism of $\mathbb{C}$ defined by $(a + bi)^\sigma = a - bi$, for all $a + bi \in \mathbb{C}$. Then, $T : V \to V$ with $T(a_1 + b_1 i, \ldots, a_n + b_n i) = (a_1 - b_1 i, \ldots, a_n - b_n i)$, for all $a_1 + b_1 i, \ldots a_n + b_n i \in \mathbb{C}$, is a semi-linear transformation.

Let V be a vector space on a field $\mathbb{F}$. We denote $\Gamma L(V, \mathbb{F})$ the set of all invertible semi-linear transformations.

Theorem 11.66 *$\Gamma L(V, \mathbb{F})$ is a group under composition of semi-linear transformations.*

Proof It is straightforward. ■

The group $\Gamma L(V, \mathbb{F})$ is called the *semi-linear group*. Also, the group

$$P\Gamma L(V, \mathbb{F}) = \frac{\Gamma L(V, \mathbb{F})}{Z\big(\Gamma L(V, \mathbb{F})\big)}$$

is called the *projective semi-linear group*. If $dimV = n$, then we write $\Gamma L_n(\mathbb{F})$ and $P\Gamma L_n(\mathbb{F})$, respectively.

Corollary 11.67 *$GL(V, \mathbb{F})$ is a normal subgroup of $\Gamma L(V, \mathbb{F})$ and we have*

$$\frac{\Gamma L(V, \mathbb{F})}{GL(V, \mathbb{F})} \cong Aut(\mathbb{F}).$$

Proof We define $\theta : \Gamma L(V, \mathbb{F}) \to Aut(\mathbb{F})$ by $\theta(T) = \sigma$, where σ is the associated field automorphism of T. It is clear that θ is an onto homomorphism with $Ker\theta = GL(V, \mathbb{F})$. This completes the proof. ■

Exercises

1. Prove that
   (a) $PSL_n(\mathbb{F}) \trianglelefteq PGL_n(\mathbb{F}) \trianglelefteq P\Gamma L_n(\mathbb{F})$;
   (b) $\dfrac{P\Gamma L_n(\mathbb{F})}{PGL_n(\mathbb{F})} \cong Aut(\mathbb{F})$.
2. Let $\mathbb{F}_q$ be a finite field with q elements. Prove that
   (a) $PSL_2(\mathbb{F}_2) \cong SL_2(\mathbb{F}_2) \cong GL_2(\mathbb{F}_2) \cong S_3$;
   (b) $PSL_2(\mathbb{F}_3) \cong A_4$.
3. Show that the set of all matrices of the form

$$\begin{bmatrix} \pm 1 & k \\ 0 & 1 \end{bmatrix},$$

   is a group isomorphic to D_n, where all entries in the matrix are in $\mathbb{Z}_n$.
4. Let $\mathbb{C}^\infty$ be the complex plane augmented by an extra point ∞. Let $a, b, c, d \in \mathbb{C}$ be such that $ad - bc \neq 0$. Define $f : \mathbb{C}^\infty \to \mathbb{C}^\infty$ by

$$\text{if } c \neq 0, \text{ then } \begin{cases} f(z) = \dfrac{az + b}{cz + d} \text{ if } z \neq \infty,\ z \neq -\dfrac{d}{c} \\ f\Big(-\dfrac{d}{c}\Big) = \infty \\ f(\infty) = \dfrac{a}{c}, \end{cases}$$

and by

$$\text{if } c = 0, \text{ then } \begin{cases} f(z) = \dfrac{az+b}{d} \text{ if } z \neq \infty, \\ f(\infty) = \dfrac{a}{c}. \end{cases}$$

Show that under composition these functions form a group G and G is a homomorphic image of $GL_2(\mathbb{C})$.

5. Give an example of an outer automorphism of a group G which maps each conjugate class of G onto itself.
Hint: Take

$$G = \left\{ \begin{bmatrix} 1 & a \\ 0 & b \end{bmatrix} \mid a, b \in \mathbb{Z}_8 \text{ and } (b, 8) = 1 \right\}.$$

Show that G is a group under matrix multiplication. Define $f : G \to G$ by

$$f\left(\begin{bmatrix} 1 & a \\ 0 & b \end{bmatrix} \right) = \begin{bmatrix} 1 & a + \dfrac{b^2-1}{2} \\ 0 & b \end{bmatrix}.$$

11.7 Worked-Out Problems

Problem 11.68 Let G and H be finite groups such that $(|G|, |H|) = 1$, prove that the only homomorphism from G to H is the zero homomorphism.

Solution Suppose that f is a homomorphism from G to H. By the first isomorphism theorem, we can write $G/Kerf \cong Imf$. Since $Kerf \leq G$, it follows that $|Kerf| \big| |G|$. Consequently, we get $(|G/Kerf|, |H|) = 1$. Analogously, since $Imf \leq H$, it follows that $|Imf| \big| |H|$. Hence, we conclude that $|G/Kerf| = |Imf| = 1$. This yields that $G = Kerf$. Therefore, f sends every element of G to the identity element of H, and this means that f is the zero homomorphism. ■

Problem 11.69 If G is a perfect group, prove that the center of $G/Z(G)$ is trivial.

Solution For convenience we set $H = Z(G)$. Assume that the center of G/H is non-trivial. This means that there is an element $aH \in Z\big(G/H\big)$ such that $a \notin H$. Since $aH \in Z\big(G/H\big)$, it follows that $aHxH = xHaH$, for all $xH \in G/H$. This implies that $axH = xaH$, or equivalently $a^{-1}x^{-1}ax \in H$. Now, we can define a function $f : G \to H$ by $f(x) = a^{-1}x^{-1}ax$, for all $x \in G$. We show that f is a homomorphism. Let x and y be elements of G. Then, we find that

$$\begin{aligned} f(xy) &= a^{-1}(xy)^{-1}a(xy) = a^{-1}y^{-1}x^{-1}axy \\ &= (a^{-1}y^{-1}ay)y^{-1}(a^{-1}x^{-1}ax)y \\ &= (a^{-1}x^{-1}ax)(a^{-1}y^{-1}ay) = f(x)f(y). \end{aligned}$$

Thus, f is a homomorphism. By the first isomorphism theorem, we have $G/Kerf \cong Imf \leq H$. As H is abelian, we conclude that $G/Kerf$ is abelian. Consequently,

by Theorem 10.4, we obtain $G' \subseteq Kerf$. Since G is perfect, we have $G = G'$, which implies that $G = Kerf$. Now, if $G = Kerf$, then $f(x) = e$, for all $x \in G$. So, we obtain $a^{-1}x^{-1}ax = e$ or $ax = xa$. This shows that $a \in H$, which is a contradiction. Therefore, we conclude that $aH = H$ or $a \in H$. This proves that $Z\big(G/H\big) = \{H\}$. ■

Problem 11.70 Suppose that

(1) G and H are groups and G is finite;
(2) $f : G \to H$ is a homomorphism;
(3) A and B are subgroups of G such that $G = AB$ and $(|A|, |B|) = 1$.

Prove that for each normal subgroup N of G, $N = (N \cap A)(N \cap B)$.

Solution Let $\pi : G \to G/N$ be the canonical map. Since π is onto, it follows that $\pi(G) = G/N$. Then, we have

$$\begin{aligned}
&\pi(G) = \pi(AB) = \pi(A)\pi(B) = G/N,\\
&\pi(A) = \{\pi(a) \mid a \in A\} = \{aN \mid a \in A\} = (AN)/N,\\
&\pi(B) = \{\pi(b) \mid b \in B\} = \{bN \mid b \in B\} = (BN)/N.
\end{aligned}$$

Thus, we conclude that

$$\frac{G}{N} = \Big(\frac{AN}{N}\Big)\Big(\frac{BN}{N}\Big).$$

On the other hand, by the second isomorphism theorem, we have

$$\frac{A}{A \cap N} \cong \frac{AN}{N} \text{ and } \frac{B}{B \cap N} \cong \frac{BN}{N}.$$

So, we deduce that

$$\Big|\frac{AN}{N}\Big| \Big||A| \text{ and } \Big|\frac{BN}{N}\Big| \Big||B|.$$

Since $(|A|, |B|) = 1$, it follows that $(|(AN)/N|, |(BN)/N|) = 1$. Hence, we obtain

$$\frac{AN}{N} \cap \frac{BN}{N} = \{N\} \text{ and } A \cap B = \{e\}.$$

Now, we can write $|G| = |AB| = |A|\,|B|$ and

$$\Big|\frac{G}{N}\Big| = \Big|\frac{AN}{N}\Big|\,\Big|\frac{BN}{N}\Big| = \frac{|A|\,|B|}{|A \cap N|\,|B \cap N|} = \frac{|G|}{|A \cap N|\,|B \cap N|}.$$

This implies that

$$|N| = |A \cap N|\,|B \cap N|. \tag{11.2}$$

Moreover, since $A \cap N \leq N$ and $B \cap N \leq N$, we have

$$(A \cap N)(B \cap N) \leq N. \tag{11.3}$$

Now, by (11.2) and (11.3), we conclude that $N = (A \cap N)(B \cap N)$. ■

Problem 11.71 Prove that there are only two groups of order 6, one is cyclic and another is isomorphic to S_3.

Solution Suppose that G is a group of order 6. Since there exist 5 non-identity elements and $x \leftrightarrow x^{-1}$ is a one to one correspondence between the elements of G and their inverses, it follows that there exists a non-identity element $a \in G$ such that $o(a) = 2$.

Let G be abelian and $H = \langle a \rangle$. Then, we have $|G/H| = 3$, which implies that G/H is cyclic. Assume that $G/H = \langle bH \rangle$, for some $b \in G$. Since $o(bH)|o(b)$, it follows that $o(b) = 3$ or 6. If $o(b) = 6$, then G is cyclic. If $o(b) = 3$, then since $ab = ba$ and $\big(o(a), o(b)\big) = 1$, it follows that $o(ab) = 6$. Hence, again in this case we deduce that G is a cyclic group generated by ab.

Now, assume that G is non-abelian. Then, all non-identity elements of G can not be of order 2. Thus, there exists $c \in G$ such that $o(c) = 3$ and $ac \neq ca$. Take $N = \langle c \rangle$. Since $[G : N] = 2$, it follows that N is a normal subgroup of G. Hence, we get $aca^{-1} \in N$. This yields that $aca^{-1} = c$ or $aca^{-1} = c^2$. Since $ac \neq ca$, we conclude that $aca^{-1} = c^2$, or $ca = ac^3$. On the other hand, we know that a can not be in N, so we can write $G = N \cup aN = \{e,\ c,\ c^2,\ a,\ ac,\ ac^2\}$. Now, it is a routine verification to check that the function $f : G \to S_3$ given by $f(e) = id$, $f(a) = (1\ 2)$, $f(c) = (1\ 2\ 3)$, $f(c^2) = (1\ 3\ 2)$, $f(ac) = (2\ 3)$ and $f(ac^2) = (1\ 3)$ is an isomorphism. This completes the proof. ■

Problem 11.72 Prove that any non-abelian group of order 8 is either D_4 or Q_8.

Solution Suppose that G is a non-abelian group of order 8. Since G is non-abelian, it follows that G is not cyclic. So, G don't have any element of order 8. If every non-identity element of G is of order 2, then again G must be abelian. Hence, there is a non-identity element $a \in G$ such that the order of a is neither 8 nor 2. Since $o(a)\big||G|$, it follows that $o(a) = 4$. If $N = \langle a \rangle$, then $[G : N] = 2$, and so $N \trianglelefteq G$. Take $b \in G$ such that $b \notin N$. Then, we obtain

$$G = N \cup bN = \{e,\ a,\ a^2,\ a^3,\ b,\ ba,\ ba^2,\ ba^3\}.$$

This yields that $G = \langle a, b \rangle$. Since G is non-abelian, it follows that $ab \neq ba$. Since $N \trianglelefteq G$, it follows that $bab^{-1} \in N$. Moreover, $o(bab^{-1} = o(a) = 4$. In the subgroup N, the only element of order 4 other than a is a^3, so we conclude that $bab^{-1} = a^3 = a^{-1}$. Now, G/N is of order 2, so $(bN)^2 = N$, or equivalently $b^2 \in \{e,\ a,\ a^2,\ a^3\}$. If $b^2 = a$ or $b^2 = a^3$, then $o(b) = 8$. This is impossible, because G is non-abelian. Thus, we conclude that $b^2 = e$ or $b^2 = a^2$. If $b^2 = e$, then G is D_4 (see Exercise 30 in Sect. 11.2). If $b^2 = a$, then G is the quaternion group. ■

Problem 11.73 Let G be a group and H be a subgroup of G. Prove that $N_G(H)/C_G(H)$ is isomorphic to a subgroup of $Aut(H)$.

Solution Define $\theta : N_G(H) \to Aut(H)$ by $\theta(a) = \theta_a$, for all $a \in N_G(H)$, in which $\theta_a(h) = aha^{-1}$, for all $h \in H$. Since $a \in N_G(H)$, it follows that $aHa^{-1} = H$. This shows that $\theta_a(h) \in H$. Moreover, we observe that θ_a is a bijective homomorphism from H onto itself, and so $\theta_a \in Aut(H)$. Now, it is easy to check that θ is a homomorphism with $Ker\theta = C_G(H)$. At the end, the result follows by the first isomorphism theorem. ■

Problem 11.74 Let G be a finite group and suppose that automorphism f sends more than three-quatres of the elements of G onto their inverses. Prove that $f(x) = x^{-1}$, for all $x \in G$ and that G is abelian.

Solution Set $A = \{a \in G \mid f(a) = a^{-1}\}$. If $x \in A$, then $|A \cup xA| = |A| + |xA| - |A \cap xA|$. Since $A \cup xA \subseteq G$, it follows that $|A \cup xA| \leq |G|$. Since the function $h : A \to xA$ defined by $f(a) = xa$, for all $a \in A$, is a one to one correspondence, it follows that $|G| \geq |A \cup xA| = |A| + |A| - |A \cap xA|$. This implies that $|G| > 3|G|/4 + 3|G|/4 - |A \cap xA|$ or $|A \cap xA| > |G|/2$. Now, assume that xa_1 and xa_2 are two elements of $A \cap xA$, then $f(xa_i) = f(x)f(a_i) = x^{-1}a_i^{-1}$ and $f(xa_i) = (xa_i)^{-1} = a_i^{-1}x^{-1}$. Hence, we conclude that $a_i^{-1}x^{-1} = x^{-1}a_i^{-1}$, which implies that x and a_i commute. Since there are more than $|G|/2$ elements in $A \cap xA$, it follows that $|C_G(x)| > |G|/2$. Now, by Lagrange's theorem, we must have $G = C_G(x)$, and this yields that $x \in Z(G)$. Since this is true for all $x \in A$, it follows that $A \subseteq Z(G)$. Thus, we obtain $3|G|/4 < |A| \leq |Z(G)|$. This shows that $G = Z(G)$, because $Z(G)$ is a subgroup of G. Consequently, G is abelian. So, A is a subgroup of G such that $3|G|/4 < |A|$. By Lagrange's theorem we deduce that $G = A$. ■

Problem 11.75 Prove that an automorphism of S_n which sends transpositions to transpositions is an inner automorphism.

Solution Suppose that $f : S_n \to S_n$ be an automorphism mapping transpositions to transpositions. For two distinct transpositions we can consider two cases:

(1) $(a\ b)(c\ d)$, which is of order 2;
(2) $(a\ b)(a\ c) = (a\ b\ c)$, which is of order 3.

Therefore, we can say that f maps any pair of disjoint transpositions to a pair of disjoint transpositions. Let $f\big((1\ 2)\big) = (r\ s)$ and suppose that $3 \leq x \leq n$. Since $(1\ 2)(1\ x)$ is a cycle of length 3, it follows that

$$f\big((1\ 2)(1\ x)\big) = f\big((1\ 2)\big)f\big((1\ x)\big) = (r\ s)f\big((1\ x)\big).$$

Hence, $f\big((1\ x)\big)$ moves either r or s. Without loss of generality, we may suppose that it moves r. Consequently, we can write $f\big((1\ x)\big) = (r\ t)$, for some t different from r and s.

Now, we claim that for each $y \neq 1$, we have $f\big((1\ y)\big) = (r\ u)$, for some $1 \leq u \leq n$ and different from r.

If $y = 2$ or $y = x$, the claim is true.

If $y \neq 2$ and $y \neq x$, then both permutations $(1\ y)(1\ 2)$ and $(1\ y)(1\ x)$ are cycles

of length 3, so are their images under f. As $f\big((1\ 2)\big) = (r\ s)$ and $f\big((1\ x)\big) = (r\ t)$, if $f\big((1\ y)\big)$ is not moving r, then it must move both s and t. Since $f\big((1\ y)\big)$ is a transposition, it follows that $f\big((1\ y)\big) = (s\ t)$. It is easy to see that $(r\ s)(r\ t)(s\ t) = (r\ t)$, and so $f^{-1}\big((r\ s)\big)f^{-1}\big((r\ t)\big)f^{-1}\big((s\ t)\big) = f^{-1}\big((r\ t)\big)$. Consequently, we get $(1\ 2)(1\ x)(1\ y) = (1\ x)$. Since $y \notin \{1,\ 2,\ x\}$ and $x \neq y$, we obtain a contradiction. Therefore, we conclude that $f\big((1\ y)\big)$ must move r, and hence $f\big((1\ y)\big) = (r\ u)$, for some $1 \leq u \leq n$ and different from r.

Now, we define $\sigma \in S_n$ as follows:

$$y\sigma = \begin{cases} r & \text{if } y = 1 \\ u & \text{if } y \neq 1, \end{cases}$$

where u is the unique element for which $f\big((1\ y)\big) = (r\ u)$. Also, assume that $g : S_n \to S_n$ denote the conjugation by σ. For every y we obtain

$$g^{-1}\big(f\big((1\ y)\big)\big) = g^{-1}\big(r\ u)\big) = \sigma(r\ u)\sigma^{-1} = (1\ y).$$

This means that $g^{-1}f$ fixes all permutations of the form $(1\ y)$, for all y. Since $(a\ b) = (1\ b)(1\ a)(1\ b)$, for all a and b, it follows that $g^{-1}f$ fixes every permutation of S_n. Thus, we obtain $f = g$. This completes the proof. ■

Problem 11.76 A group G is *complete* if it is centerless and every automorphism of G is inner. If $n \neq 2$ and $n \neq 6$, prove that S_n is complete.

Solution Let $C(k)$ denote the the conjugate class in S_n consisting of all products of k disjoint transpositions. We know that a permutation in S_n is of order 2 if and only if it belongs in some $C(k)$. So, if $f \in Aut(S_n)$, then $f\big(C(1)\big) = \big(C(k)\big)$, for some positive integer k. We claim that if $n \neq 6$, then $|C(1)| \neq |C(k)|$, for $k \neq 1$. Assuming this, then $f\big(C(1)\big) = C(1)$, and Problem 11.76 completes the proof.

Clearly, we have $C(1) = n(n-1)/2$. In order to count the elements of $C(k)$, we observe that there exist

$$\frac{n(n-1)}{2} \cdot \frac{(n-2)(n-3)}{2} \cdot \ldots \cdot \frac{(n-2k-2)(n-2k+1)}{2}.$$

k-tuples of disjoint transpositions. Since disjoint transpositions commute and there are $k!$ orderings obtained from any k-tuples, we obtain

$$|C(k)| = \frac{n(n-1)(n-2)\ldots(n-2k+1)}{k!2^k}.$$

Now, the question whether $|C(1)| = |C(k)|$ leads to the question whether there is some $k > 1$ such that

$$(n-2)(n-3)\ldots(n-2k+1) = k!2^k. \tag{11.4}$$

Since the right side of (11.4) is positive, it follows that $n \geq 2k$. Hence, we have

$$(n-2)(n-3)\dots(n-2k+1) \geq (2k-2)(2k-3)\dots(2k-2k+1)$$
$$= (2k-2)!.$$

Moreover, by mathematical induction, we find that if $k \leq 4$, then $(2k-2)! > k!2^{k-1}$. Consequently, (11.4) is true if $k = 2$ or $k = 3$. If $k = 2$, then the right side of (11.4) is 4 and it is easy to see that equality never holds. So, we suppose that $k = 3$. Since $n \geq 2k$, it follows that $n \geq 6$. If $n > 6$, then the left side of (11.4) is greater than or equal to $5 \cdot 4 \cdot 3 \cdot 2 = 120$, while the right side of (11.4) is 24. Therefore, we have proved that if $n \neq 6$, then $|C(1)| \neq |C(k)|$, for all $k > 1$, as desired. ■

Remark 11.77 $S_2 \cong \mathbb{Z}_2$ is not complete because it has a center. We shall see in future that S_6 is not complete too.

Problem 11.78 Let H be a subgroup of a group $G \leq GL_n(\mathbb{C})$. If the set

$$\{[x, y] \mid x \in G \text{ and } y \in H\}$$

is a set of order m, prove that $[G : C_G(H)] \leq m^{n^2}$.

Solution If $y \in H$, then y has at most m conjugate $x^{-1}yx = y[x, y]^{-1}$ in G (where $x \in G$). Therefore, we have

$$[G : C_G(y)] \leq m.$$

Suppose that $L(H) = \{c_1h_1 + \dots + c_mh_m \mid c_i \in \mathbb{C} \text{ and } h_i \in H\}$. If we define addition and multiplication by scalars in an obvious manner for elements in $L(H)$, then $L(H)$ is a vector space over $\mathbb{C}$. The set of all $n \times n$ matrices with entries in $\mathbb{C}$ is a vector space over $\mathbb{C}$ containing $L(H)$ as a subspace. Since the former space has dimension n^2, it follows that the dimension $L(H)$ is at most n^2. Assume that $dim L(H) = k \leq n^2$. Then, we can find elements $y_1, \dots, y_k$ in H which form a basis for $L(H)$. Consequently, we have

$$C_G(H) = \bigcap_{i=1}^{k} C_G(y_i).$$

So, we have

$$[G : C_G(H)] = [G : \bigcap_{i=1}^{k} C_G(y_i)] \leq \prod_{i=1}^{k} [G : C_G(y_i)] \leq m^{n^2}.$$

This completes the proof. ■

11.8 Supplementary Exercises

1. Let G be a group, and let S be any set for which there exists a one to one and onto function $f : G \to S$. We define a binary operation on S by setting $xy = f\left(f^{-1}(x)f^{-1}(y)\right)$, for all $x, y \in S$. Prove that S is a group under this operation, and that f is actually a group isomorphism.
2. Let G be a group of order 12. Show that either G has a normal subgroup of order 3 or G is isomorphic to A_4.
3. Let $f : G_1 \to G_2$ be an onto homomorphism. Let H_1 be a normal subgroup of G_1 and suppose that $f(H_1) = H_2$. Prove or disprove that $G_1/H_1 \cong G_2/H_2$.
4. Let N_1 and N_2 be two normal subgroups of G. Prove or disprove that
   (a) $N_1 \cong N_2$ implies $G/N_1 \cong G/N_2$;
   (b) $G/N_1 \cong G/N_2$ implies $N_1 \cong N_2$.
5. Let H be the subgroup of $GL_2(\mathbb{Z}_3)$ as follows:

$$H = \left\{ \begin{bmatrix} a & b \\ 0 & 1 \end{bmatrix} \in GL_2(\mathbb{Z}_3) \mid a, b \in \mathbb{Z}_3,\ a \neq 0 \right\}.$$

   Show that H is isomorphic to the symmetric group S_3.
6. Show that the subgroup $\{id,\ (1\ 2)(3\ 4),\ (1\ 3)(2\ 4),\ (1\ 4)(2\ 3)\}$ of A_4 is isomorphic to the group of plane symmetries of a chessboard.
7. Show that to each positive integer n there exist only a finite number of pairwise non-isomorphic groups of order n.
8. Prove that distinct automorphisms of the symmetric group S_4 induce distinct automorphisms of the alternating subgroup A_4. What is the order of the group of automorphisms of A_4?
9. Let G and H be groups, $f : G \to H$ be a homomorphism with kernel N, and K be a subgroup of G. Prove that $f^{-1}\big(f(K)\big) = KN$. Hence, $f^{-1}\big(f(K)\big) = K$ if and only if $N \leq K$.
10. If G is metabelian and $f : G \to H$ is a homomorphism, prove that $f(G)$ is metabelian.
11. Prove that
    (a) If G is a non-abelian group, $Aut(G)$ can not be cyclic;
    (b) There is no finite group G for which $Aut(G)$ is cyclic of odd order greater than 1.
12. Show that if G is a group with trivial center ($Z(G) = \{e\}$), then its group of automorphisms, $Aut(G)$, is also a group with trivial center.
    Hint: Let $f \in Z(Aut(G))$. For any $a \in G$, let $\phi_a \in Inn(G)$. Then $f \circ \phi_a = \phi_a \circ f$ (Why?). Use this to show that for any $x \in G$, $a^{-1}f(a) \in C_G(f(x))$. Infer the result from this.
13. Suppose that $Z(G) = \{e\}$ and $Inn(G)$ is a characteristic subgroup of $Aut(G)$. Show that any automorphism of A is inner.

14. Let G be a group and H a normal subgroup of G with the property that $[G : H] = 4$. Let K be an arbitrary subgroup of G. Show that if the factor group $K/K \cap H$ is non-trivial, then it is isomorphic to either $\mathbb{Z}_2$, or $\mathbb{Z}_4$, or K_4.
15. Let H be a subgroup of G. Prove that the factor group $N_G(H)/C_G(H)$ is isomorphic to a subgroup of $Aut(H)$.
16. Prove that if $G \cong H$, then $G' \cong H'$ and $Z(G) \cong Z(H)$.
17. Suppose that G_1 and G_2 are finite perfect groups such that $G_1/Z(G_1) \cong G_2/Z(G_2)$. Prove that there exists a finite perfect group G and subgroups $H_1, H_2 \leq Z(G)$ with $G/Z(G) \cong G_i/Z(G_i)$ and $G/H_i \cong G_i$, for $i = 1, 2$.
18. Show that no group can have its automorphism group cyclic of odd order.
19. Let G be a finite group. If $k(G)$ is the number of conjugate classes of G, show that

    (a) $k(G) = 2$ if and only if $G \cong \mathbb{Z}_2$;
    (b) $k(G) = 3$ if and only if $G \cong \mathbb{Z}_3$ or $G \cong S_3$;
    (c) What can you say about finite groups with 4 or 5 conjugate classes?

20. Let p be a prime and $Z(p^\infty)$ be the following subset of the group $\mathbb{Q}/\mathbb{Z}$:

$$Z(p^\infty) = \{\overline{a/b} \in \mathbb{Q}/\mathbb{Z} \mid a, b \in \mathbb{Z} \text{ and } b = p^i \text{ for some } i \geq 0\},$$

    where $\overline{a/b} = a/b + \mathbb{Z}$. Show that

    (a) $Z(p^\infty)$ is an infinite group under the addition operation of $\mathbb{Q}/\mathbb{Z}$;
    (b) Every element of $Z(p^\infty)$ has finite order p^n for some $n \geq 0$;
    (c) If at least one element of a subgroup H of $Z(p^\infty)$ has order p^k, and no element of H has order greater than p^k, then H is a cyclic subgroup generated by $\overline{1/p^k}$, whence $H \cong \mathbb{Z}_{p^k}$;
    (d) The only proper subgroups of $Z(p^\infty)$ are the cyclic groups $\langle\overline{1/p^n}\rangle$ $(n = 1, 2, \ldots)$;
    (e) If $x_1, x_2, \ldots$ are elements of an abelian group G such that $o(x_1) = p$, $px_2 = x_1$, $px_3 = x_2, \ldots, px_{n+1} = x_n, \ldots$, then the subgroup generated by x_i's $(i \geq 1)$ is isomorphic to $Z(p^\infty)$;
    (f) If H is a proper subgroup of $Z(p^\infty)$, then $Z(p^\infty)/H \cong Z(p^\infty)$.

21. If G has order $n > 1$, prove that

$$|Aut(G)| \leq \prod_{i=0}^{k} (n - 2^i),$$

    where $k = [\log_2(n - 1)]$.
22. Find a finite group G with a normal subgroup N such that $|Aut(N)| > |Aut(G)|$.
23. Let G be a group of order pq, where p and q are distinct prime numbers, and if G has a normal subgroup of order p and a normal subgroup of order q, prove that G is cyclic.
24. Let G be a group of order pq, where $p > q$ are primes. Prove that

(a) G has a subgroup of order p and a subgroup of order q;
(b) If $q \not| p-1$, then G is cyclic;
(c) Given two primes p and q with $q|p-1$, there exists a non-abelian group of order pq;
(d) Any two non-abelian groups of order pq are isomorphic.