Properties of homomorphisms and isomorphisms. Cayley's theorem.

Key questions:

1. Homomorphisms of Groups
2. Example for Homomorphisms of Groups
3. Isomorphisms of Groups
4. Example for Isomorphisms of Groups
5. Correspondence Theorems
6. Example for Correspondence Theorems

Key phrases: Homomorphisms, Isomorphisms, Correspondence Theorems, vector space, classification of algebraic structures, isomorphism is the representation, commutative, subgroup, the kernel of *f*, noncommutative, nonisomorphic groups, cyclic group, the quotient group, inner automorphism of *G,* automorphisms of *G,* normal subgroup of *G*.

Introduction. One of the main uses of the concept of an isomorphism is the classification of algebraic structures−in particular, groups. Readers with some knowledge of linear algebra may recall that the concept of an isomorphism is used to completely characterize vector spaces with the same field of scalars in terms of a single integer, the dimension of the vector space. Another important use of an isomorphism is the representation of one algebraic structure by means of another. This is done in linear algebra, where it is shown that the vector space of all linear transformations from one finite dimensional vector space into another is isomorphic to a certain vector space of matrices.

Homomorphisms of Groups

In this section, we consider certain mappings between groups. These mappings will be defined in such a way as to preserve the algebraic structure of the groups involved. More precisely, suppose we are given a function f from a group G into a group $G1$, where $*1$ denotes the operation of $G1$. Let $a,b \in G$. Then under f, a corresponds to $f(a)$, b to $f(b)$, and $a * b$ to $f(a * b)$. If f is to preserve the operations of G and $G1$, $a * b$ must correspond to $f(a) *1 f(b)$. Since f is a function, this forces the requirement that $f(a * b) = f(a) *1 f(b)$.

Definition 1.1 Let $(G,*)$ and $(G1,*1)$ be groups and f a function from G into $G1$. Then f is called a homomorphism of G into $G1$ if for all $a,b \in G$,

$f(a * b) = f(a) *1 f(b)$.

Let the identity element of the group $G1$ be denoted by $e1$.

Define $f : G \to G1$ by $f(a) = e1$ for all $a \in G$. Since $f(a * b) = e1 = e1 *1 e1 = f(a) *1 f(b)$ for all $a,b \in G$, we find that f is a homomorphism from G into $G1$. This shows that there always exists a homomorphism from a group G into a group $G1$. This homomorphism is called the trivial homomorphism.

The identity map from G onto G is also a homomorphism.

Before we consider more examples of homomorphisms, let us prove some basic properties of homomorphisms.

Theorem 1.2 Let f be a homomorphism of a group G into a group $G1$. Then

(i) $f(e) = e1$.

(ii) $f(a-1) = f(a)-1$ for all $a \in G$.

(iii) If H is a subgroup of G, then $f(H) = \{f(h) \mid h \in H\}$ is a subgroup of $G1$.

(iv) If $H1$ is a subgroup of $G1$, then $f-1(H1) = \{g \in G \mid f(g) \in H1\}$ is a subgroup of G, and if $H1$ is a normal subgroup, then $f-1(H1)$ is a normal subgroup of G.

(v) If G is commutative, then $f(G)$ is commutative.

(vi) If $a \in G$ is such that $\circ(a) = n$, then $\circ(f(a))$ divides n.

Proof. (i) Since f is a homomorphism, $f(e)f(e) = f(ee) = f(e) = f(e)e1$. This implies that $f(e) = e1$ by the cancellation law.

(ii) Let $a \in G$. Then $f(a)f(a-1) = f(aa-1) = f(e) = e1$. Similarly, $f(a-1)f(a) = e1$. Since $f(a)$ has a unique inverse, $f(a-1) = f(a)-1$.

(iii) Let H be a subgroup of G. Then $e \in H$ and by (i), $f(e) = e1$. Thus, $e1 = f(e) \in f(H)$ and so $f(H)$ =6 $\emptyset$. Let $f(a),f(b) \in f(H)$, where $a,b \in H$. Since H is a subgroup, $ab-1 \in H$. Thus, $f(a)f(b)-1 = f(a)f(b-1) = f(ab-1) \in f(H)$. Hence, by Theorem 4.1.6, $f(H)$ is a subgroup of $G1$.

(iv) By (i), $e \in f-1(H1)$ and so $f-1(H1)$ =6 $\emptyset$. Let $a,b \in f-1(H1)$. Then $f(a)$, $f(b) \in H1$. Hence, $f(ab-1) = f(a)f(b-1) = f(a)f(b)-1 \in H1$ and so $ab-1 \in f-1(H1)$. Thus, by Theorem 4.1.6, $f-1(H1)$ is a subgroup of G. Suppose $H1$ is a normal subgroup of $G1$. Let $g \in G$.We now show that $gf-1(H1)g-1 \subseteq f-1(H1)$. Let $a \in gf-1(H1)g-1$. Then $a = gbg-1$ for some $b \in f-1(H1)$. Now $f(a) = f(gbg-1) = f(g)f(b)f(g-1) = f(g)f(b)f(g)-1 \in H1$ since $H1$ is a normal subgroup of $G1$ and $f(b) \in H1$. Hence, $a \in f-1(H1)$ and this shows that $gf-1(H1)g-1 \subseteq f-1(H1)$. Thus, $f-1(H1)$ is a normal subgroup of G.

(v) Suppose G is commutative. Let $f(a)$, $f(b) \in f(G)$. Then $f(a)f(b) = f(ab) = f(ba) = f(b)f(a)$. Hence, $f(G)$ is commutative.

(vi) Since $(f(a))n = f(an) = f(e) = e1$, we have $\circ(f(a))$ divides n by Theorem 2.1.46. ■

Definition 1.3 Let f be a homomorphism of a group G into a group $G1$. The kernel of f, written Ker f, is defined to be the set

Ker $f = \{a \in G \mid f(a) = e1\}$.

By Theorem 1.2, $e \in$ Ker f.

Example 1.4 Define the function f from $(\mathbb{Z},+)$ into $(\mathbb{Z}_n,+_n)$ by $f(a) = [a]$ for all $a \in \mathbb{Z}$. From the definition of f, it follows that f maps $\mathbb{Z}$ onto $\mathbb{Z}_n$. Let $a,b \in \mathbb{Z}$. Then

$$f(a + b) = [a + b] = [a] +_n [b] = f(a) +_n f(b).$$

Thus, f is a homomorphism of $\mathbb{Z}$ onto $\mathbb{Z}_n$. The above example shows that a nontrivial finite group may be an image of an infinite group under a homomorphism. By Theorem 1.2(v), a noncommutative group cannot be an image under a homomorphism of a commutative group. In the next example, we show that two finite groups G and $G1$ having same number of elements need not have a homomorphism from G onto $G1$.

Example 1.5 The groups $\mathbb{Z}_4 \times \mathbb{Z}_4$ and $\mathbb{Z}_8 \times \mathbb{Z}_2$ are commutative and each is of order 16. Suppose there exists a homomorphism f of $\mathbb{Z}_4 \times \mathbb{Z}_4$ onto $\mathbb{Z}_8 \times \mathbb{Z}_2$. Now $a = ([7],[0]) \in \mathbb{Z}_8 \times \mathbb{Z}_2$ and $\circ(a) = 8$. Since f is onto $\mathbb{Z}_8 \times \mathbb{Z}_2$, there exists $b \in \mathbb{Z}_4 \times \mathbb{Z}_4$ such that $f(b) = a$. By Theorem 1.2(vi), $\circ(f(b))$ divides $\circ(b)$. Since $\circ(f(b)) = 8$ and $\mathbb{Z}_4 \times \mathbb{Z}_4$ has elements of order 1,2, and 4 only, $\circ(f(b))$ cannot divide $\circ(b)$. This is a contradiction. Hence, there does not exist any homomorphism from $\mathbb{Z}_4 \times \mathbb{Z}_4$ onto $\mathbb{Z}_8 \times \mathbb{Z}_2$.

Definition 1.6 Let G and $G1$ be groups. A homomorphism $f : G \rightarrow G1$ is called an epimorphism if f is onto $G1$ and f is called a monomorphism if f is one-one. If there is an epimorphism f from G onto $G1$, then $G1$ is called a homomorphic image of G.

The homomorphism in Example 1.4 is an epimorphism, but not a monomorphism.

Example 1.7 Let $\mathbb{R}^*$ be the group of all nonzero real numbers under multiplication. Define $f : \mathbb{R}^* \rightarrow \mathbb{R}^*$ by $f(a) = |a|$. Now $f(ab) = |ab| = |a||b| = f(a)f(b)$, which implies that f is a homomorphism. Since $f(1) = 1 = f(-1)$ and $1 =6 -1$, f is not one-one. Also, from the definition of f, it follows that f is not onto $\mathbb{R}^*$. Hence, f is neither an epimorphism nor a monomorphism.

The following theorem gives a necessary and sufficient condition for a homomorphism to be a one-one mapping in terms of its kernel.

Theorem 1.8 Let f be a homomorphism of a group G into a group $G1$. Then f is one-one if and only if Ker $f = \{e\}$.

Proof. Suppose f is one-one. Let $a \in$ Ker f. Then $f(a) = e1 = f(e)$ by Theorem 1.2(i). Since f is one-one, we must have $a = e$. Hence, Ker $f = \{e\}$. Conversely, suppose that Ker $f = \{e\}$. Let $a,b \in G$. Suppose $f(a) = f(b)$. Then $f(ab-1) = f(a)f(b-1)$ $= f(a)f(b)-1 = e1$.

Thus, $ab-1 \in$ Ker $f = \{e\}$ and so $ab-1 = e$, i.e., $a = b$. This proves that f is one-one. ■

Theorem 1.9 Let f be a homomorphism of a group G into a group $G1$. Then Ker f is a normal subgroup of G.

Proof. Since $e \in$ Ker f, Ker f =6 ∅. Let a, $b \in$ Ker f. Then $f(ab-1) = f(a)f(b-1) =$ $f(a)f(b)-1 = e1(e1)-1 = e1e1 = e1$. Thus, $ab-1 \in$ Ker f and hence Ker f is a subgroup of G by Theorem 4.1.6. Let $a \in G$ and $h \in$ Ker f. Then $f(aha-1) = f(a)f(h)f(a-1) =$ $f(a)f(h)f(a)-1 = f(a)e1f(a)-1 = e1$. Therefore, $aha-1 \in$ Ker f. This proves that aKer $fa-1 \subseteq$ Ker f. Hence, Ker f is a normal subgroup of G by Theorem 4.4.3. ■

Example 1.10 Let $GL(2,\mathbb{R}) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \mid a,b,c,d \in \mathbb{R},\ ad-bc \neq 0 \right\}$ be the noncommutative group of Example 2.1.14. Let R∗ be the group of all nonzero real numbers under multiplication. Define $f : GL(2,$R) →R∗ by

$$f\left(\begin{bmatrix} a & b \\ c & d \end{bmatrix}\right) = ad - bc$$

for all $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in GL(2,\mathbb{R})$. Let $\begin{bmatrix} a & b \\ c & d \end{bmatrix}, \begin{bmatrix} u & v \\ w & s \end{bmatrix} \in GL(2,\mathbb{R})$. Now

$$\begin{aligned} f\left(\begin{bmatrix} a & b \\ c & d \end{bmatrix}\begin{bmatrix} u & v \\ w & s \end{bmatrix}\right) &= f\left(\begin{bmatrix} au+bw & av+bs \\ cu+dw & cv+ds \end{bmatrix}\right) \\ &= (au+bw)(cv+ds) - (av+bs)(cu+dw) \\ &= (ad-bc)(us-vw) \\ &= f\left(\begin{bmatrix} a & b \\ c & d \end{bmatrix}\right) f\left(\begin{bmatrix} u & v \\ w & s \end{bmatrix}\right). \end{aligned}$$

This proves that f is a homomorphism. To show that f is onto $\mathbb{R}^*$, *let* $a \in \mathbb{R}^*$. *Then* $\begin{bmatrix} a & 0 \\ 0 & 1 \end{bmatrix} \in GL(2, \mathbb{R})$ and

$f\left(\begin{bmatrix} a & 0 \\ 0 & 1 \end{bmatrix}\right) = a.$ Hence, f is onto R∗. Since $f\left(\begin{bmatrix} a & 0 \\ 0 & 1 \end{bmatrix}\right) = a = f\left(\begin{bmatrix} a & 1 \\ 0 & 1 \end{bmatrix}\right)$ *and* $\begin{bmatrix} a & 0 \\ 0 & 1 \end{bmatrix} \neq \begin{bmatrix} a & 1 \\ 0 & 1 \end{bmatrix}$,

f is not one-one.

The previous example shows that there may exist a homomorphism of a noncommutative group onto a commutative group.

Example 1.11 Consider $S3$ and the normal subgroup

$$H = \left\{\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}\right\}.$$

Define $f : S3 \to S3/H$ by for all $\pi \in S3$, $f(\pi) = \pi H$. Then

$f(\pi \circ \pi0) = (\pi \circ \pi0)H = (\pi H) \circ (\pi 0H) = f(\pi) \circ f(\pi0)$

for all $\pi, \pi0 \in S3$. Hence, f is a homomorphism. Also, Ker $f = \{\alpha \in S3 \mid \alpha H = H\} = \{\alpha \in S3 \mid \alpha \in H\} = H$.

In Theorem 1.9, we showed that if f is a homomorphism of a group into a group $G1$, then Ker f is a normal subgroup of G. In the following theorem, we show that every normal subgroup H of a group G induces a homomorphism g of G onto the quotient group G/H such that Ker $g = H$. We note that in Example 1.11, the conclusion did not depend on the nature of $S3$. The conclusion was made by use of general arguments. This also leads us to the following theorem.

Theorem 1.12 Let H be a normal subgroup of a group G. Define the function g from G onto the quotient group G/H by $g(a) = aH$ for all $a \in G$. Then g is a homomorphism of G onto G/H and Ker $g = H$. (The homomorphism g is called the natural homomorphism of G onto G/H.)

Proof. From the definition of g, it follows that g is a function from G onto G/H. To show g is a homomorphism, let $a, b \in G$. Then $g(ab) = (ab)H = (aH)(bH) =$

$g(a)g(b)$. Hence, g is a homomorphism of G onto G/H. Finally, we show that Ker $g = H$. Now $a \in$ Ker g if and only if $g(a) = eH$ if and only if $aH = eH$ if and only if $e-1a \in H$ if and only if $a \in H$. Thus, Ker $g = H$. ■

We now define a particular type of homomorphism between groups in order to introduce the important idea of groups being algebraically indistinguishable.

Definition 1.13 A homomorphism f of a group G into a group $G1$ is called an isomorphism of G onto $G1$ if f is one-one and onto $G1$. In this case, we write G ' $G1$ and say that G and $G1$ are isomorphic. An isomorphism of a group G onto G is called an automorphism.

For a group G, Aut(G), denotes the set of all automorphisms of G.

In the following theorem, we collect some properties of isomorphisms, which will be useful in determining whether given groups are isomorphic or not.

Theorem 1.14 Let f be an isomorphism of a group G onto a group $G1$. Then (i) $f-1 : G1 \to G$ is an isomorphism.

(ii) G is commutative if and only if $G1$ is commutative.

(iii) For all $a \in G$, $\circ(a) = \circ(f(a))$.

(iv) G is a torsion group if and only if $G1$ is a torsion group. (v) G is cyclic if and only if $G1$ is cyclic.

Proof. (i) Since f is one-one and onto $G1$, $f-1$ is one-one and onto G. Now we only need to verify that $f-1$ is a homomorphism. Let $u,v \in G1$. Then there exist $a,b \in G$ such that $f(a) = u$ and $f(b) = v$. This implies that $a = f-1(u)$, $b = f-1(v)$, and $uv = f(a)f(b) = f(ab)$. Thus, $f-1(uv) = ab = f-1(u)f-1(v)$ and so $f-1$ is a homomorphism. Hence, $f-1$ is an isomorphism.

(ii) Suppose G is commutative. Let $u,v \in G1$. Since f is onto $G1$, there exist $a,b \in G$ such that $f(a) = u$ and $f(b) = v$. Now $uv = f(a)f(b) = f(ab) = f(ba) = f(b)f(a) = vu$.

Thus, $G1$ is commutative. Conversely, suppose $G1$ is commutative. Let $a,b \in G$. Now

$f(ab) = f(a)f(b) = f(b)f(a) = f(ba)$.

Since f is one-one, we have $ab = ba$. This proves that G is commutative.

(iii) Let $a \in G$. By induction, it follows that for all positive integers n, $f(an) = (f(a))n$. Since f is one-one, for all $b \in G$, $f(b) = e1$ if and only if $b = e$. Hence, $an = e$ if and only if $(f(a))n = e1$. Thus, a is of finite order if and only if $f(a)$ is of finite order. Suppose $\circ(a) = m$ and $\circ(f(a)) = n$. Since $am = e$, $(f(a))m = e1$. By Theorem 2.1.46, n divides m. Also, $(f(a))n = e1$ implies that $an = e$. Hence, m divides n. Since m and n are both positive integers and m divides n and n divides m, it follows that $m = n$.

(iv) This follows immediately by (iii).

(v) Suppose G is cyclic. Then $G = \text{h}a\text{i}$ for some $a \in G$. Since $f(a) \in G1$, $\text{h}f(a)\text{i} \subseteq G1$. Let $b \in G1$. Since f is onto $G1$, there exists $c \in G$ such that $f(c) = b$. Now $c = an$ for some $n \in \mathbb{Z}$. Thus,

$b = f(c) = f(an) = (f(a))n \in \text{h}f(a)\text{i}$.

Hence, $G1 = \text{h}f(a)\text{i}$ and so $G1$ is cyclic. The converse follows since $f{-}1$ is an isomorphism. ■

In order to develop a feel for two groups being algebraically indistinguishable, let us consider two sets S and $S0$ such that there is a one-one function f of S onto $S0$. Then in a set-theoretic sense, S and $S0$ are the same sets "under f". For instance, let A and B be subsets of S. Then $f(A)$ and $f(B)$ are corresponding subsets of $S0$. Now $f(A\cap B) = f(A)\cap f(B)$ and $f(A\cup B) = f(A)\cup f(B)$; that is, union and intersection are preserved under f. Other purely set-theoretic operations can be seen to be preserved under f also. Now suppose binary operations $*$ and $*0$ are defined on S and $S0$, respectively, so that $(S,*)$ and $(S0,*0)$ are groups. Now even though S and $S0$ are the same sets "under f," they need not be the same as groups, i.e., f may not preserve operations. We have seen that the requirement for *f* to preserve operations is that *f*(*a* ∗ *b*) = *f*(*a*) ∗0 *f*(*b*) for all *a, b* ∈ *S*.

We now consider examples of groups that are isomorphic and examples of groups that are not isomorphic.

Example 1.15 Let *n* be a positive integer. Define *f* from Z*n* into Z/h*n*i by for all [*a*] ∈Z*n*, *f*([*a*]) = *a*+h*n*i. Then [*a*] = [*b*] if and only if *n* | (*a* − *b*) if and only if *a* − *b* = *nq* for some *q* ∈Z if and only if *a* − *b* ∈ h*n*i if and only if *a*+ h*n*i = *b* +h*n*i if and only if *f*([*a*]) = *f*([*b*]). Therefore, we find that *f* is a one-one function. From the definition of *f*, it follows that *f* maps Z*n* onto Z/h*n*i. Now *f*([*a*]+*n* [*b*]) = *f*([*a*+*b*]) = (*a*+*b*)+h*n*i = (*a*+h*n*i)+ (*b* + h*n*i) = *f*([*a*]) + *f*([*b*]). Thus, *f* is an isomorphism of Z*n* onto Z/h*n*i.

Example 1.16 Consider the sets *G* = {*e,a,b,c*} and *G*1 = {1, −1, *i*, −*i*}. Define ∗ and · on *G* and *G*1, respectively, by means of the following operation tables.

– – –

Now *G*1 is a cyclic group generated by *i*. *G* is also a group. However, since *aa* = *e*, *bb* = *e*, and *cc* = *e*, no element of *G* has order 4 and so *G* is not cyclic. Thus, *G* and *G*1 are not isomorphic.

Example 1.17 Let (R,+) be the group of real numbers under addition and (R+,·) be the group of positive real numbers under multiplication. Define *f* : R→R+ by *f*(*a*) = *ea* for all *a* ∈R. Clearly *f* is well defined. Let *a,b* ∈R. Then *f*(*a* + *b*) = *ea*+*b* = *eaeb* = *f*(*a*)*f*(*b*). Hence, *f* is a homomorphism. Suppose *f*(*a*) = *f*(*b*). Then *ea* = *eb* and so log*e* *ea* = log*e* *eb*. This implies that *a* = *b*, whence *f* is one-one. Let *b* ∈R+. Then log*e* *b* ∈R and *f*(log*e* *b*) = *e*log*eb* = *b*. Thus, *f* is onto R+. Consequently, *f* is an isomorphism of (R,+) onto (R+,·).

Example 1.18 Consider the groups (Z,+) and (Q,+). By Worked-Out Exercise 1 (page 80), (Q,+) is not cyclic. Since (Z,+) is cyclic and (Q,+) is not cyclic, (Z,+) is not isomorphic to (Q,+) by Theorem 1.14(*v*).

Example 1.19 The group $(\mathbb{Q},+)$ is not isomorphic to $(\mathbb{Q}^*,\cdot)$ since every nonidentity element of $(\mathbb{Q},+)$ is of infinite order while -1 is a nonidentity element of $(\mathbb{Q}^*,\cdot)$ which is of finite order.

Let us now characterize finite and infinite cyclic groups.

Theorem 1.20 Every finite cyclic group of order n is isomorphic to $(\mathbb{Z}_n,+_n)$ and every infinite cyclic group is isomorphic to $(\mathbb{Z},+)$.

Proof. Let $(\langle a\rangle,*)$ be a cyclic group of order n. Let $G = \langle a\rangle$. Define the function $f : G \to \mathbb{Z}_n$ by for all $a^i \in G$, $f(a^i) = [i]$. Now $a^i = a^j$ if and only if $a^{j-i} = e$ if and only if $n \mid (j - i)$ if and only if $[i] = [j]$ (Exercise 11, page 23) if and only if $f(a^i) = f(a^j)$. Thus, f is a one-one function. Now

$$f(a^ia^j) = f(a^{i+j}) = [i + j] = [i] +_n [j] = f(a^i) +_n f(a^j).$$

Since f is one-one and G and $\mathbb{Z}_n$ are finite with same number of elements, f is onto $\mathbb{Z}_n$. Hence, $G \simeq \mathbb{Z}_n$.

Now let $G = \langle a\rangle$ be an infinite cyclic group. Define the function $f : G \to \mathbb{Z}$ by $f(a^i) = i$ for all $i \in \mathbb{Z}$. Since $a^i = a^j$ if and only if $a^{i-j} = e$ if and only if $i - j = 0$ (since a is of infinite order) if and only if $i = j$, we have that f is a one-one function of G into $\mathbb{Z}$. From the definition of f, f is onto $\mathbb{Z}$. Now

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

Hence, $G \simeq \mathbb{Z}$. ■

Corollary 1.21 Any two cyclic groups of the same order are isomorphic. ■

From the above corollary, it follows that there is only one (up to isomorphism) cyclic group having a prescribed order.

In Example 1.16, we saw that there are at least two nonisomorphic groups of order 4. We now show that these are exactly two nonisomorphic groups of order 4.

Let G be a group of order 4 which is not cyclic. (Example 1.16 shows that such a group exists.) Then no element of G can have order 4, for if $a \in G$ has order 4, then

$e,a,a2,a3$ would be distinct elements of G and thus G would be cyclic, i.e., G = hai. This is contrary to the assumption that G is not cyclic. Let $G = \{e,a,b,c\}$. Since the order of every element of G divides the order of G, a, b, and c have order 2. If $ab = a$, then $b = e$, a contradiction. Thus, ab =6 a. Similarly, ab =6 b. Suppose $ab = e$, then $a(ab) = ae$. Therefore, $b = a$ since $a2 = e$, a contradiction. Thus, $ab = c$. Similarly, $ba = c$. Hence, $ab = ba$. By similar arguments, we have $ac = b = ca$ and $bc = a = cb$. Thus, we find that G is a commutative group and its operation table is given by the table in Example 1.16. Consequently, there is essentially one group of order 4 which is not cyclic. This is the Klein 4-group. Since all cyclic groups of the same orders are isomorphic, we thus have exactly two nonisomorphic groups of order 4, namely, the Klein 4-group and the cyclic group of order 4. We have thus proved the following result.

Theorem 1.22 There are only two groups of order 4 (up to isomorphism), a cyclic group of order 4 and $K4$ (Klein 4-group).

Since every cyclic group is commutative and every group of prime order is cyclic, it follows that that if a group is noncommutative, then it must have order at least 6. Indeed, the symmetric group $S3$ is noncommutative and of order 6. Since all cyclic groups of the same order are isomorphic and since every group of prime order is cyclic, there is exactly one group of order 1, 2, 3, 5 (up to isomorphism), respectively. We have seen that there are two nonisomorphic groups of order 4. In the next theorem, we show that there are only two (up to isomorphism) nonisomorphic groups of order 6.

Theorem 1.23 There are only two (up to isomorphism) groups of order 6.

Proof. The group Z6 is a cyclic group of order 6 and $S3$ is a noncommutative group of order 6. Note that Z6 is not isomorphic to $S3$. To show that there are only two (up to isomorphism) nonisomorphic groups of order 6, we will show that any group of order 6 is isomorphic to either Z6 or $S3$.

Let G be a group of order 6. Since $|G|$ is even, there exists $a \in G$, $a \neq e$ such that $a^2 = e$. If $x^2 = e$ for all $x \in G$, then G is commutative and for any two distinct nonidentity elements a and b, $\{e,a,b,ab\}$ is a subgroup of G. Since $|G| = 6$, G has no subgroups of order 4. Hence, there exists $b \in G$ such that $b^2 \neq e$, i.e., $b \neq e$ and $\circ(b) \neq 2$. Since $\circ(b) \mid 6$, $\circ(b) = 6$ or 3. If $\circ(b) = 6$, then $G = \langle b \rangle$ is a cyclic group of order 6 and $G \simeq Z_6$. Suppose G is not cyclic. Then $\circ(b) = 3$. Let $H = \{e,b,b^2\}$. Then H is a subgroup of G of index 2. Thus, H is a normal subgroup of G. Clearly $a \notin H$. Now $G = H \cup aH$ and $H \cap aH = \emptyset$. Hence, $G = \{e,b,b^2,a,ab,ab^2\}$. Now $aba^{-1} \in H$ since H is normal and $b \in H$. Therefore, $aba^{-1} = e$ or $aba^{-1} = b$ or $aba^{-1} = b^2$. If $aba^{-1} = e$, then $b = e$, which is a contradiction. If $aba^{-1} = b$, then $ab = ba$. Since $\circ(a)$ and $\circ(b)$ are relatively prime and $ab = ba$, $\circ(ab) = \circ(a) \cdot \circ(b) = 6$. Thus, G is cyclic, a contradiction. Hence, $aba^{-1} = b^2$. Thus, $G = \langle a,b \rangle$, where $\circ(a) = 2$, $\circ(b) = 3$, and $aba^{-1} = b^2$. It is now easy to see that $G \simeq S_3$. ■

We conclude this section by proving Cayley's theorem, which says that any group can be realized as a permutation group.

Theorem 1.24 (Cayley) Any group G is isomorphic to some subgroup of the group $(S(G),\circ)$ of all permutations of the set G.

Proof. Let a be an element of a group G. Define the function $f_a : G \to G$ by for all $b \in G$, $f_a(b) = ab$. Then $b = c$ if and only if $ab = ac$ if and only if $f_a(b) = f_a(c)$. Thus, f_a is a one-one function of G into G. For any $b \in G$, $f_a(a^{-1}b) = a(a^{-1}b) = b$.

So we find that f_a maps G onto G. Hence, f_a is a permutation of G. This implies that $f_a \in S(G)$. Let $F(G) = \{f_a \mid a \in G\}$. Then $F(G)$ is a subset of the set $S(G)$of all permutations on G Define $g : G \to S(G)$ by for all $a \in G$, $g(a) = f_a$. Then $a = b$ if and only if $ac = bc$ for all $c \in G$ if and only if $f_a(c) = f_b(c)$ for all $c \in G$ if and only if $f_a = f_b$ if and only if $g(a) = g(b)$. This proves that g is a one-one function of G into $F(G)$. Clearly g maps G onto $F(G)$. Now $g(ab) = f_{ab}$ and $g(a) \circ g(b) = f_a \circ f_b$. Also, for all $c \in G$,

$f_{ab}(c) = (ab)c = a(bc) = f_a(bc) = f_a(f_b(c)) = (f_a \circ f_b)(c)$.

Thus, $f_{ab} = f_a \circ f_b$. Hence, $g(ab) = g(a) \circ g(b)$ and so g is a homomorphism.This implies that $F(G)$ is a subgroup and G is isomorphic to this subgroup.

Cayley's theorem is another example of a representation theorem. However, Cayley realized that the best way of studying general problems in group theory was not necessarily by the use of permutations.

Worked-Out Exercises

♦ Exercise 1 Let $f : G \to G1$ be an epimorphism of groups. If H is a normal subgroup of G, then show that $f(H)$ is a normal subgroup of $G1$.

Solution: By Theorem 1.2, we find that $f(H)$ is a subgroup of $G1$. Let $g1 \in G1$. Since f is onto $G1$, there exists $g \in G$ such that $f(g) = g1$. Let $a \in g1f(H)g1{-}1 = f(g)f(H)f(g){-}1$. Then $a = f(g)f(h)f(g){-}1 = f(ghg{-}1)$ for some $h \in H$. Since H is a normal subgroup of G, $ghg{-}1 \in H$ and so $a \in f(H)$. Thus, $g1f(H)g1{-}1 \subseteq f(H)$. Hence, $f(H)$ is a normal subgroup of $G1$.

♦ Exercise 2 Let G and H be finite groups such that $\gcd(|G|,|H|) = 1$. Show that the trivial homomorphism is the only homomorphism from G into H.

Solution: Let $f : G \to H$ be a homomorphism and let $a \in G$. We show that every element of G is mapped onto the identity element of H, i.e., $f(a) = eH$ for all $a \in G$, where eH denotes the identity element of H. Now $\circ(a) \mid |G|$ and $\circ(f(a)) \mid |H|$. Also, by Theorem 1.2, $\circ(f(a)) \mid \circ(a)$. Hence, $\circ(f(a)) \mid |G|$. Since $|G|$ and $|H|$ are relatively prime, $\circ(f(a)) = 1$, proving $f(a) = eH$. Thus, f is the trivial homomorphism.

♦ Exercise 3 Show that the group (Q,+) is not isomorphic to (Q/Z,+).

Solution: In (Q,+), every nonzero element is of infinite order. Let $\frac{p}{q} + \mathbb{Z} \in \mathbb{Q}/\mathbb{Z}$, where $p,q \in$Z and $q = 06$. Then

$q(\frac{p}{q} + \mathbb{Z}) = p + \mathbb{Z} = \mathbb{Z}$. This shows that every element of Q/Z is of finite order. Hence, (Q,+) is not isomorphic

to (Q/Z,+).

Exercise 4 Show that R∗, the group of all nonzero real numbers under multiplication, is not isomorphic to C∗, the group of all nonzero complex numbers under multiplication.

Solution: In the group C∗, i is an element of order 4. But R∗ does not contain any element of order 4. Hence, by Theorem 1.14, R∗ is not isomorphic to C∗.

♦ Exercise 5 Find all homomorphisms from Z6 into Z4.

Solution: Z6 = h[1]i. Let f : Z6 → Z4 be a homomorphism. For any [a] ∈ Z6, f([a]) = af([1]) shows that f is completely known if f([1]) is known. Now ◦(f([1])) divides ◦([1]) and 4, i.e., ◦(f([1])) divides 6 and 4. Hence, ◦(f([1])) = 1 or 2. Thus, f([1]) = [0] or [2]. If f([1]) = [0], then f is the trivial homomorphism which maps every element to [0]. On the other hand, f([1]) = [2] implies that f([a]) = [2a] for all [a] ∈Z6. Thus, f([a] + [b]) = f([a + b]) = [2(a + b)] = [2a + 2b] = [2a] + [2b] = f([a]) + f([b]), proving that the mapping f : Z6 →Z4 defined by f([a]) = [2a] for all [a] ∈Z6 is a homomorphism. Hence, there are two homomorphisms from Z6 into Z4.

Exercise 6 Let G be a finite commutative group. Let n ∈Z be such that n and |G| are relatively prime. Show that the function φ : G → G defined by $\varphi(a)$ = an for all a ∈ G is an isomorphism of G onto G.

Solution: Let a,b ∈ G. Now $\varphi(ab)$ = $(ab)n$

= $anbn$ (since G is commutative) = $\varphi(a)\varphi(b)$.

This implies that φ is a homomorphism. Let $\varphi(a)$ = $\varphi(b)$. Then an = bn and so (ab−1)n = e. Therefore, ◦(ab−1) divides n. Since ◦(ab−1) divides |G| and n and |G| are relatively prime, ◦(ab−1) = 1. This implies that ab−1 = e, i.e., a = b, proving that φ is one-one. Since G is a finite group and φ is one-one, φ is onto G. Hence, φ is an isomorphism of G onto G.

♦ Exercise 7 (a) Let G be a group and f : G → G be defined by $f(a)$ = an for all a ∈ G, where n is a positive integer. Suppose f is an isomorphism. Prove that an−1 ∈ $Z(G)$ for all a ∈ G.

(b) Let G be a group and $f : G \to G$ defined by for all $a \in G$, $f(a) = a3$ be an isomorphism. Prove that G is commutative.

Solution:(a) Let $a,b \in G$. Then $f(a-1ba) = (a-1ba)n = a-1bna$. Thus,

$a-nbnan = f(a-1)f(b)f(a) = f(a-1ba) = a-1bna.$

Hence, $a-(n-1)\ bn\ an-1 = bn$ or $(a-(n-1)ban-1)n = bn$. Thus, $f(a-(n-1)ban-1) = f(b)$. Since f is one-one, $a-(n-1)ban-1 = b$. Hence, $an-1b = ban-1$, proving that $an-1 \in Z(G)$.

(b) By (a), $a2 \in Z(G)$ for all $a \in G$. Let $a,b \in G$. Then $f(ab) = (ab)3 = ab(ab)2 = a(ab)2b = aababb = a2bab2 = ba2b2a = bb2a2a = b3a3 = f(b)f(a) = f(ba)$. Hence, $ab = ba$ since f is one-one. Thus, G is commutative.

2. Isomorphism and Correspondence Theorems

In this section, we continue our study of isomorphisms. Our objective is to prove the fundamental theorem of homomorphisms, the isomorphism theorems, and the correspondence theorem. These theorems show us the relationship between homomorphisms and quotient groups.

Theorem 2.1 Let f be a homomorphism of a group G onto a group $G1$, H be a normal subgroup of G such that $H \subseteq \text{Ker } f$, and g be the natural homomorphism of G onto G/H. Then there exists a unique homomorphism h of G/H onto $G1$ such that $f = h \circ g$. Furthermore, h is one-one if and only if $H = \text{Ker } f$.

Proof. Define $h : G/H \to G1$ by $h(aH) = f(a)$

for all $aH \in G/H$.

Now $aH = bH$ implies $b-1a \in H \subseteq \text{Ker } f$ and so $f(b-1a) = e1$ or $f(a) = f(b)$. Hence, $h(aH) = h(bH)$ and so h is well defined. Let $a \in G$. Then

$(h \circ g)(a) = h(g(a)) = h(aH) = f(a).$

Therefore, $h \circ g = f$. Since f maps G onto $G1$, h must map G/H onto $G1$. Now

$h((aH)(bH)) = h((ab)H) = f(ab) = f(a)f(b) = h(aH)h(bH).$

Hence, h is a homomorphism of G/H onto $G1$ satisfying $f = h \circ g$. To prove the uniqueness part, let us assume $f = h0 \circ g$ for some homomorphism $h0$ from G/H onto $G1$. Then

$$h(aH) = f(a) = (h0 \circ g)(a) = h0(g(a)) = h0(aH)$$

for all $aH \in G/H$ and so $h = h0$. Hence, h is the only homomorphism of G/H onto $G1$ such that $f = h \circ g$.

Suppose h is one-one. Let $a \in \text{Ker } f$. Then $f(a) = e1$ and so $h(aH) = e1$. Since $h(eH) = e1$ and h is one-one, $aH = eH$. Thus, $a \in H$ and so $\text{Ker } f \subseteq H$. By hypothesis, $H \subseteq \text{Ker } f$ and so $H = \text{Ker } f$. Conversely, assume $H = \text{Ker } f$. Suppose $h(aH) = h(bH)$. Then $f(a) = f(b)$ or $f(b-1a) = e1$. Thus, $b-1a \in \text{Ker } f = H$ and so $aH = bH$, proving that h is one-one. ■

From Theorem 2.1, it follows that if $H = \text{Ker } f$, then h is an isomorphism and hence $G/\text{Ker } f$ is isomorphic to $G1$, i.e., every homomorphism of a group G onto a group $G1$ induces an isomorphism of $G/\text{Ker } f$ onto $G1$. This result plays a fundamental role in group theory. It is known as the fundamental theorem of homomorphisms for groups. This result is also called the first isomorphism theorem for groups. Considering the importance of this theorem, we state it in its general form and also give a direct proof of it.

Theorem 2.2 (First Isomorphism Theorem) Let f be a homomorphism of a group G into a group $G1$. Then $f(G)$ is a subgroup of $G1$ and

$$G/\text{Ker } f \,' f(G).$$

Proof. By Theorem 1.2, $f(G)$ is a subgroup of $G1$. Let $H = \text{Ker } f$. Define $h : G/H \rightarrow f(G)$ by

$$h(aH) = f(a)$$

for all $aH \in G/H$. Now $aH = bH$ if and only if $b-1a \in H = \text{Ker } f$ if and only if $f(b-1a) = e1$ if and only if $f(b-1)f(a) = e1$ if and only if $f(a) = f(b)$. Thus, h is a one-one function. Let $x \in f(G)$. Then $x = f(b)$ for some $b \in G$. Therefore, $h(bH) = f(b) = x$.

This shows that h is onto $f(G)$. Finally, $h(aHbH) = h(abH) = f(ab) = f(a)f(b) = h(aH)h(bH)$ for all $aH,bH \in G/H$, proving that h is a homomorphism. Consequently, $G/\mathrm{Ker} f$ ' $f(G)$. ■

In the following example we illustrate the first isomorphism theorem.

Example 2.3 Let f be the homomorphism of (Z,+) onto (Z3,+3) defined by $f(n) = [n]$ for all $n \in$ Z. Let g be the natural homomorphism of Z onto Z/h6i. Now h6i is a normal subgroup of Z and h6i ⊂ h3i = Ker f. Thus, there exists a homomorphism h of Z/h6i onto Z3 such that $f = h \circ g$. The homomorphism h is defined by $h(n$ + h6i) = $[n]$.

Recall that a group G1 is called a homomorphic image of a group G if there exists a homomorphism of G onto G1.

From Theorem 2.1 and Corollary 2.2, we find that for each normal subgroup N of a group G, G/N is a homomorphic image of G, and for each homomorphic image G1, there exists a normal subgroup N of G such that G/N ' G1.

Example 2.4 The group S3 has (up to isomorphism) only three homomorphic images. This follows from the fact that S3 has only three normal subgroups. The homomorphic images are S3, Z1, and Z2 since $\{e\}$, S3, and $\{e,(1\ 2\ 3),(1\ 3\ 2)\}$ are the only normal subgroups of S3 and S3 ' $S3/\{e\}$, Z1 ' $S3/S3$, and Z2 ' $S3/\{e,(1\ 2\ 3),(1\ 3\ 2)\}$.

Theorem 2.5 Let G1 be a homomorphic image of a group G. Then the following assertions hold.

(i) If G is cyclic, then G1 is cyclic.

(ii) If G is commutative, then G1 is commutative.

(iii) If G1 contains an element of order n and $|G|$ is finite, then G contains an element of order n.

■

Note that the result in Theorem 2.5(iii) does not hold if $|G|$ is not finite. For example, Z6 is a homomorphic image of Z; Z6 contains an element of order 3, but Z has no element of order 3.

Theorem 2.6 (Second Isomorphism Theorem) Let H and K be subgroups of a group G with K normal in G. Then

$H/(H \cap K)$ ' $(HK)/K$.

We illustrate the second isomorphism theorem with the help of the following example.

Theorem 2.8 Let f be a homomorphism of a group G onto a group $G1$, H be a normal subgroup of G such thatThen there exists a unique isomorphism$H \supseteq$ Ker f, and g, $g0$ be the natural homomorphisms of$h$ of G/H onto G /f(GHonto) such thatG/H and$g0 \circ Gf$ 1=onto$h \circ g.G1/f(H)$, respectively.

1

$$\begin{tikzcd} G \arrow[r, "f"] \arrow[d, "g"'] & G_1 \arrow[d, "g'"] \\ G/H \arrow[r, "h"] & G_1/f(H) \end{tikzcd}$$

■

Corollary 2.9 (Third Isomorphism Theorem) Let $H1$, $H2$ be normal subgroups of a group G such that $H1 \subseteq H2$. Then

$(G/H1)/(H2/H1)$ ' $G/H2$.

$$\begin{tikzcd} G \arrow[r, "f"] \arrow[d] & G/H_1 \arrow[d] \\ G/H_2 \arrow[r] & (G/H_1)/(H_2/H_1) \end{tikzcd}$$

Proof. Make the following substitutions in Theorem 2.8: $G/H1$ for $G1$, $H2$ for H, and $(G/H1)/(H2/H1)$ for $G1/f(H)$, where in this case f is the natural homomorphism of G onto $G/H1$. Note that $f(H2) = H2/H1$.

■

We can at times determine the subgroups of a group $G1$ from a group G whose subgroups are known if there is a homomorphism f of G onto $G1$. For if such an f exists, the following result says that the subgroups of $G1$ can be determined from the subgroups of G which contain Ker f.

Theorem 2.11 (Correspondence Theorem) Let f be a homomorphism of a group G onto a group $G1$. Then f induces a one-one inclusion preserving correspondence between the subgroups of G containing Ker f and the subgroups of $G1$. In fact, if H and K are corresponding subgroups of G and $G1$, respectively, then H is a normal subgroup of G if and only if K is a normal subgroup of $G1$.

Corollary 2.12 Let N be a normal subgroup of a group G. Then every subgroup of G/N is of the form K/N, where K is a subgroup of G that contains N. Also, K/N is a normal subgroup of G/N if and only if K is a normal subgroup of G.

we fiProof.nd that this homomorphism induces a one-one mappingLet $g : G \to G/N$ be the natural homomorphism. If$g*$ between the subgroups of$a \in G$, then $g(a) = aN$. From Theorem$G$ which contain Ker2.11, $g = N$ and the subgroups of G/N. Let H be a subgroup of G/N. Then there exists a subgroup K of G such that $N \subseteq K$ and $H = g*(K) = \{g(a) \mid a \in K\} = K/N$. The last part follows from Theorem 2.11. ■

The following example illustrates the correspondence theorem.

In the remainder of this section, we consider all isomorphisms of a group G onto itself. Recall that Aut(G) is the set of all automorphisms of G.

Theorem 2.14 Let G be a group. Then $(\mathrm{Aut}(G), \circ)$ is a group, where $\circ$ denotes the composition of functions.

Theorem 2.15 Let G be a group and $a \in G$. Define $\theta a : G \to G$ by $\theta a(b) = aba-1$ for all $b \in G$. Then (i) $\theta a \in \mathrm{Aut}(G)$,

((iiiii))$\theta(a\theta a\circ)\theta-b1==\theta\theta aba-$for all$1,a,b \in G$,

(iv) for all $\alpha \in \mathrm{Aut}(G)$, $\alpha \circ \theta a \circ \alpha-1 = \theta\alpha(a)$.

Proof. (i) Let $c,d \in G$. Suppose $c = d$. Then $aca-1 = ada-1$ or $\theta a(c) = \theta a(d)$. Therefore, θa is well defined. Now $\theta a(cd) = a(cd)a-1 = (aca-1)(ada-1) = \theta a(c)\theta a(d)$. This shows that θa is a homomorphism. Also, $c = \theta a(a-1ca)$, proving that θa is onto G. Suppose $\theta a(c) = \theta a(d)$. Then $aca-1 = ada-1$ and so $c = d$. Thus, θa is one-one. Consequently, $\theta a \in \mathrm{Aut}(G)$.

(ii) Let $a,b \in G$. Then $(\theta a \circ \theta b)(c) = \theta a(\theta b(c)) = \theta a(bcb-1) = a(bcb-1)a-1 = (ab)c(ab)-1 = \theta ab(c)$ for all $c \in G$. Hence, $\theta a \circ \theta b = \theta ab$.

(iii) Note that $\theta a \circ \theta a-1 = \theta aa-1 = \theta e = iG$ and $\theta a-1 \circ \theta a = \theta a-1a = \theta e = iG$. Thus, $(\theta a)-1 = \theta a-1$.

(iv) Let $\alpha \in \mathrm{Aut}(G)$. Now $(\alpha \circ \theta a \circ \alpha-1)(b) = \alpha(\theta a(\alpha-1(b))) = \alpha(a\alpha-1(b)a-1) = \alpha(a)\alpha(\alpha-1(b))\alpha(a-1) = \alpha(a)b(\alpha(a))-1 = \theta\alpha(a)(b)$ for all $b \in G$. Hence, $\alpha \circ \theta a \circ \alpha-1 = \theta\alpha(a)$. ■

The automorphism θa of Theorem 2.15 is called an inner automorphism of G. We denote by $\mathrm{Inn}(G)$ the set of all inner automorphisms of G.

Theorem 2.16 Let G be a group. Then $\mathrm{Inn}(G)$ is a normal subgroup of $\mathrm{Aut}(G)$.

Proof. Since $iG = \theta e \in \mathrm{Inn}(G)$, $\mathrm{Inn}(G) =6 \emptyset$. By Theorem 2.15(i), $\mathrm{Inn}(G) \subseteq \mathrm{Aut}(G)$. Let $\theta a,\theta b \in \mathrm{Inn}(G)$. Then $\theta a \circ\theta-b\ 1 = \theta a \circ\theta b-1 = \theta ab-1 \in \mathrm{Inn}(G)$. Hence, $\mathrm{Inn}(G)$ is a subgroup of $\mathrm{Aut}(G)$ by Theorem 4.1.6. Let $\alpha \in \mathrm{Aut}(G)$. Then by Theorem 2.15(iv), $\alpha \circ \theta a \circ \alpha-1 = \theta\alpha(a) \in \mathrm{Inn}(G)$. Hence, $\mathrm{Inn}(G)$ is a normal subgroup of $\mathrm{Aut}(G)$. ■

Theorem 2.17 Let G be a group and H be a subgroup of G. Then

$\frac{N(H)}{C(H)} \simeq$ a subgroup of $\mathrm{Aut}(H)$, where $N(H) = \{x \in G \mid xHx^{-1} = H\}$ is the normalizer of H and $C(H) = \{x \in G \mid xhx^{-1} = h$ for all $h \in H\}$ is the centralizer of H.

Proof. Define $f : N(H) \to \mathrm{Aut}(H)$ by for all $a \in N(H)$,

$f(a) = \theta_a |_H$.

Then f is well defined. Let $a_1, a_2 \in N(H)$. Then $f(a_1a_2) = \theta_{a_1a_2}|_H = \theta_{a_1}|_H \circ \theta_{a_2}|_H = f(a_1) \circ f(a_2)$. Thus, f is a homomorphism. Now

$$\begin{aligned} \mathrm{Ker}\, f &= \{a \in G \mid f(a) = i_H\} \\ &= \{a \in G \mid \theta_a = i_H\} \\ &= \{a \in G \mid \theta_a(b) = i_H(b) \text{ for all } b \in H\} \\ &= \{a \in G \mid aba^{-1} = b \text{ for all } b \in H\} \end{aligned}$$

$= \{a \in G \mid ab = ba$ for all $b \in H\} = C(H)$.

Thus, by the first isomorphism theorem, we have the desired result. ■

Corollary 2.18 Let G be a group. Then

$\frac{G}{Z(G)} \simeq \mathrm{Inn}(G)$.

Proof. Let $H = G$ in Theorem 2.17. Then we have $N(G) = G$ and $C(G) = Z(G)$. ■

Worked-Out Exercises

♦ Exercise 1 Find all homomorphic images of the additive group Z.

Solution: Let H be a homomorphic image of (Z,+). There exists a homomorphism f of Z onto H. By the first isomorphism theorem, Z/Ker f ' H. Since Ker f is a subgroup of Z, Ker $f = n$Z for some integer $n \geq 0$. Hence, H ' Z/nZ for some integer $n \geq 0$. On the other hand, for any $n \geq 0$, nZ is a subgroup of Z and since Z is commutative, nZ is a normal subgroup of Z. There exists a natural homomorphism f from Z onto Z/nZ given by $f(m) = m+n$Z for all $m \in$Z. This shows that Z/nZ is a homomorphic image of Z for all $n \geq 0$. Consequently, the homomorphic images of Z are the groups (up to isomorphism) Z/nZ, $n \geq 0$. Now for $n = 0$, Z/nZ ' Z and for $n >$

0, Z/nZ ' Z_n (Exercise 2, page 111). Therefore, we conclude that the homomorphic images of Z are the cyclic groups Z and Z_n, $n > 0$.

♦ Exercise 2 If there exists an epimorphism of a finite group G onto the group Z_8, show that G has normal subgroups of index 4 and 2.

Solution: Let $f : G \to Z_8$ be an epimorphism. Then by the first isomorphism theorem, $G/\mathrm{Ker}\, f$ ' Z_8. Hence, $G/\mathrm{Ker}\, f$ is a cyclic group of order 8. Thus, $G/\mathrm{Ker}\, f$ has a normal subgroup H_1 of order 4 and a normal subgroup H_2 of order 2. By the correspondence theorem, there exist normal subgroups N_1 and N_2 of G such that $\mathrm{Ker}\, f \subseteq N_1$, $\mathrm{Ker}\, f \subseteq N_2$, $N_1/\mathrm{Ker}\, f = H_1$, and $N_2/\mathrm{Ker}\, f = H_2$. Thus,

$$8 = |G/\mathrm{Ker}\, f| = [G : \mathrm{Ker}\, f] = [G : N_1][N_1 : \mathrm{Ker}\, f] = [G : N_1]4.$$

This implies that $[G : N_1] = 2$. Similarly, $[G : N_2] = 4$.

♦ Exercise 3 Show that $4Z/12Z$ ' Z_3.

Solution: Define $f : 4Z \to Z_3$ by $f(4n) = [n]$ for all $4n \in 4Z$. One can show that f is an epimorphism. Then from the first isomorphism theorem, $4Z/\mathrm{Ker}\, f$ ' Z_3. Now $\mathrm{Ker}\, f = \{4n \in 4Z \mid f(4n) = [0]\} = \{4n \in 4Z \mid [n] = [0]\} = 12Z$.

♦ Exercise 4 Let G be a finite group and f be an automorphism of G such that for all $a \in G$, $f(a) = a$ if and only if $a = e$. Show that for all $g \in G$, there exists $a \in G$ such that $g = a^{-1}f(a)$.

Solution: Let $G = \{a_1, a_2, \ldots, a_n\}$. Let $S = \{a_1^{-1}f(a_1), \ldots, a_n^{-1}f(a_n)\}$. Then $S \subseteq G$. Next, we show that all elements of S are distinct. Now $a_i^{-1}f(a_i) = a_j^{-1}f(a_j)$ if and only if $f(a_i)f(a_j)^{-1} = a_ia_j^{-1}$ if and only if $f(a_ia_j^{-1}) = a_ia_j^{-1}$ if and only if $a_ia_j^{-1} = e$ if and only if $a_i = a_j$. This shows that all elements of S are distinct and so $|S| = n$. Thus, $S = G$. Let $g \in G$. Then $g \in S$. Hence, $g = a^{-1}f(a)$ for some $a \in G$.

♦ Exercise 5 Let G be a finite group and f be an automorphism of G such that for all $a \in G$, $f(a) = a$ if and only if $a = e$. Suppose that $f^2 = i_G$, where i_G denotes the identity map. Prove that G is commutative.

Solution: Let $g \in G$. By Worked-Out Exercise 4, $g = a-1f(a)$ for some $a \in G$. Then $g = iG(g) = f2(a-1f(a)) = f(f(a-1f(a))) = f(f(a-1)f2(a)) = f(f(a)-1a) = f(g-1)$. This implies that $f(g) = g-1$ for all $g \in G$. Let $a,b \in G$. Then $(ab)-1 = f(ab) = f(a)f(b) = a-1b-1 = (ba)-1$ and so $ab = ba$. Hence, G is commutative.

♦ Exercise 6 Let H be a subgroup of index 2 in a finite group G. If the order of H is odd and every element of $G\backslash H$ is of order 2, prove that H is commutative.

Solution: Since $[G : H] = 2$, H is a normal subgroup of G. Now $G = H \cup Hg$, where $g /\in H$. Then $\circ(g) = 2$. Define $f : G \to G$ by for all $a \in G$, $f(a) = gag-1$. Then f is an automorphism of G. Now $f2(a) = f(f(a)) = f(gag-1) = g(gag-1)g-1 = g2ag-2 = a$ since $g2 = e$. Hence, $f2 = iG$. Since H is a normal subgroup of G, $f(h) = aha-1 \in H$ for all $h \in H$. Thus, f is also an automorphism of H. Let $h \in H$. Suppose $f(h) = h$. Then $ghg-1 = h$ or $gh = hg$. Since $gh /\in H$, $\circ(gh) = 2$. Therefore, $h2 = g2h2 = (gh)2 = e$. Since the order of H is odd, $h2 = e$ implies that $h = e$. Hence, $f(h) = h$ if and only $h = e$. Thus, f is an automorphism of H such that $f2 = iG$ and $f(h) = h$ if and only if $h = e$. By Worked-Out Exercise 5, H is commutative.

Test questions and assignments

1. Exercises

1. Determine whether the indicated function f is a homomorphism from the first group into the second group.

If f is a homomorphism, determine its kernel.

(a) $f(a) = a^2$; $(R^+,\cdot)$, $(R^+,\cdot)$ for all $a \in R^+$.

(b) $f(a) = 2$; $(R,+)$, $(R ,\cdot)$ for all $a \in R$.

(c) $f(a) = |a|$;$(R\backslash\{0\},\cdot)$, $(R^+,\cdot)$ for all $a \in R\backslash\{0\}$.

(d) $f(a) = a + 1$; $(Z,+)$, $(Z,+)$ for all $a \in Z$.

(e) $f(a) = 2a$; $(Z,+)$, $(Z,+)$ for all $a \in Z$.

(f) $f([a]) = [5a]$,$(Z8,+)$, $[Z8,+]$

2. Find all homomorphisms from Z into Z. How many homomorphisms are onto?

3. Find all homomorphisms from Z onto Z6.

4. Find all homomorphisms from Z8 into Z12 and from Z20 into Z10.

5. Show that Q*, the group of all nonzero rational numbers under multiplication, is not isomorphic to R*, the group of all nonzero real numbers under multiplication.

6. Show that (Q,+) is not isomorphic to (R,+).

7. Show that (Z,+) is not isomorphic to (R,+).

8. Let G be a group. Define the function $f : G \to G$ by for all $a \in G$, $f(a) = a^{-1}$. Prove that f is a homomorphism if and only if G is commutative.

9. Let G = {(a,b) | a,b ∈ R, b 6= 0}. Then (G,∗) is a noncommutative group under the binary operation (a,b)∗(c,d) = (a+bc,bd+) for all (a,b),(+c,d) ∈ G. Let H = {(a,b) ∈ G | a = 0} and K = {(a,b) ∈ G | b > 0}. Show that H ∩ K ' (R ,·), where (R ,·) is the group of all positive real numbers under multiplication.

10. (a) Let f be a homomorphism from a cyclic group of order 8 onto a cyclic group of order 4. Determine Ker f.

(b) Let f be a homomorphism from a cyclic group of order 8 onto a cyclic group of order 2. Determine Ker f.

11. Prove that a homomorphic image of a cyclic group is cyclic.

12. Show that S_3 and Z6 are not isomorphic groups, but for every proper subgroup A of S_3 there exists a proper subgroup B of Z6 such that A ' B.

13. Let G, H, and K be groups. Suppose that the functions $f : G \to H$ and $g : H \to K$ are homomorphisms. Prove that $g \circ f : G \to K$ is also a homomorphism.

14. Let G and H be groups. Define the function $f : G\times H \to G$ by for all $(a,b) \in G\times H$, $f((a,b)) = a$. Prove that f is a homomorphism from $G \times H$ onto G. Determine Ker f.

15. Let $f : G \to H$ be an isomorphism of groups. Prove that $f^{-1} : H \to G$ is also an isomorphism.

16. Let G, H, and K be groups. Prove that

(a) G × H ' H × G.

(b) If G ' H and H ' K, then G ' K.

(c) G × (H × K) ' (G × H) × K.

17. Let G and H be groups. Let f : G → H be a homomorphism of G onto H. Show that if G = hSi for some subset S of G, then H = hf(S)i.

18. Let G be a simple group and ψ : S_n → G be an epimorphism for some positive integer n. Prove that G ' S_k for some k ≤ n.

19. Which of the following statements are true? Justify.

(a) A cyclic group with more than one element may be a homomorphic image of a noncyclic group.

(b) There does not exist a nontrivial homomorphism from a group G of order 5 into a group H of order 4.

(c) The group (Z,+) is isomorphic to (Q,+).

(d) There exists a monomorphism from a group of order 20 into a group of order 70.

(e) There exists an epimorphism of (R,+) onto (Z,+).

(f) There does not exist any epimorphism of (Q,+) onto (Z,+).

(g) If f and g are two epimorphisms of a group G onto a group H such that Ker f = Ker g, then f = g.

(h) (Z × Z,+) is a cyclic group.

(i) The group (Z,+) is a homomorphic image of (Q,+).

2. Exercises

1. For any positive integer n, prove that Z/nZ'Zn.

2. For any two positive integers m and n prove that mZ/mnZ'Zn.

3. Let G be a group and A and B be normal subgroups of G such that A ' B. Show by an example that G/A 6' G/B.

4. Let G be the group of symmetries of the square and K_4 the Klein 4-group. Show that the mapping $f : G \rightarrow K_4$ defines a homomorphism of G onto K_4, where $f(r_{180}) = f(r_{360}) = e$, $f(r_{90}) = f(r_{270}) = a$, $f(h) = f(v) = b$, $f(d_1) = f(d_2) = c$.

5. In Exercise 6, exhibit the one-one inclusion preserving correspondence between the subgroups of G containing Z(G) and the subgroups of K_4.

6. Let G and K_4 be as in Exercise 6. Let g be the natural homomorphism of G onto G/Z(G), where Z(G) is the center of G. Prove that Z(G) = Ker f and exhibit the isomorphism h of G/Z(G) onto K_4 such that $f = h \circ g$.

7. Show that Z8 is not a homomorphic image of Z1

8. Show that Z9 is not a homomorphic image of Z3 × Z3.

9. Show that if there exists an epimorphism from a finite group G onto the group Z15, then G has normal subgroups of indices 5 and 3, respectively.

10. Partition the following collection of groups into subcollections of groups such that any two groups in thesame subcollection are isomorphic.

(i) (Z,+), (ii) (Z6,+), (iii) (Z2,+), (iv) S_2, (v) S_6, (vi) (17Z,+), (vii) (3Z,+), (vii) (Q,+), (ix) (R,+), (x)(R^*,·), (xi) (R^+,·), (xii) (Q^*,·), (xiii) (C^*,·), (xiv) (hπi,·), where R^* denotes the set of nonzero real numbers, Q^* denotes the set of nonzero rational numbers, C^* denotes the set of nonzero real numbers, R^+ denotes the set of positive real numbers, and (hπi,·) is the cyclic subgroup of (R^+,·) generated by π.

13. Determine Aut(S_4).

14. Let G be a cyclic group of order n and φ be the Euler φ-function. Prove that |Aut(G)| = φ(n).

15. Let G be a group such that Z(G) = {e}. Prove that Z(Aut(G)) = {e}.

16. Let G be a group and H be a subgroup of G. H is called a characteristic subgroup of G if f(H) ⊆ H for all f ∈ Aut(G).

(a) Show that every characteristic subgroup of G is a normal subgroup of G.

(b) Give an example of a group G and a subgroup H such that H is a normal subgroup of G, but H is not a characteristic subgroup of G.

(c) Show that Z(G) is a characteristic subgroup of G.

(d) Let H and K be characteristic subgroups of G. Show that HK and $H \cap K$ are characteristic subgroups of G.

(e) Let H and K be subgroups of G such that $H \subseteq K$. Show that if K is a normal subgroup of G and H is a characteristic subgroup of G, then H is a normal subgroup of G.

(f) Let H and K be subgroups of G such that $H \subseteq K$. Show that if H is a characteristic subgroup of K and K is a characteristic subgroup of G, then H is a characteristic subgroup of G.

(g) Suppose G is cyclic. Show that every subgroup of G is a characteristic subgroup of G.

17. Show that the only characteristic subgroups of (Q,+) are {0} and Q.

18. Which of the following statements are true? Justify.

(a) Any epimorphism of Z onto Z is an isomorphism.

(b) Any epimorphism of a group G onto G is an isomorphism.

(c) The quotient group 4Z/64Z has five subgroups.

(d) Z5 has five homomorphic images.

(e) 2Z/6Z is a subgroup of Z/6Z.

(f) There exist four subgroups of Z which contain 10Z as a subgroup.

(g) Let G and H be two groups, A be a normal subgroup of G, and B be a normal subgroup of H. If G ' H and A ' B, then G/A ' H/B.

Exercises

1. Show that $I_3 = \{1,2,3\}$ is a S_3-set, where the left action is defined by $\sigma a = \sigma(a)$ for all $\sigma \in S_3$, $a \in I_3$. Find all distinct orbits of S_3. Find G_1, G_2, and G_3.

2. Let H be a subgroup of order 11 and index 4 of a group G. Prove that H is a normal subgroup of G.

3. Let H be a subgroup of a group G of index n. If H does not contain any nontrivial normal subgroups of G, prove that H is isomorphic to a subgroup of S_n.

4. Let G = GL(2,R) and S = R^2. Show that S is a G-set under the left action defined by

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}(x, y) = (ax + by,\ cx + dy)$$

for all $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in G,\ (x, y) \in \mathbb{R}^2$.

5. Let G be a group of order 77 acting on a set S of 20 elements. Show that G must have a fixed point.

6. Let G be a group. The left action of G on the set G is defined by conjugation, i.e., $(g,x) \rightarrow gxg^{-1}$ for all $g,x \in G$. Show that the kernel of the homomorphism $\psi : G \rightarrow A(G)$ induced by this action is Z(G).

7. Let G be a group of order 80 such that G has a subgroup of order 16. Show that G is not a simple group.

8. Show that a group of order 22 is not a simple group.

9. Show that there are no simple groups of orders 6, 10, 14, 26, 34, and 58.

10. Show that a group of order 8 cannot be a simple group.

11. Show that a simple group of order 63 cannot contain a subgroup of order 21.

12. Let G be a group of order 70 such that G has a subgroup of order 14. Show that G has a nontrivial normal subgroup.

Literature

1	Ayupov A.Sh., Omirov B.A., Xudoyberdiev A.X., Haydarov F.H. Algebra va sonlar nazariyasi, Toshkent, «Tafakkur bo‘stoni», 296 bet, 2019 y.
2	Xojiyev J.X. Faynleyb A.S. Algebra va sonlar nazariyasi kursi, Toshkent, «O’zbekiston», 2001 y.
3	Sh.A.Ayupov, B.A.Omirov, A.X.Xudoyberdiyev. ABSTRAKT ALGEBRA (o‘quv qo‘llanma), T., “Universitet”, 2021.
4	Malik D.S., Mordeson J.N., Sen M.K., Fundamentals of abstract algebra.- WCB McGrew-Hill, 1997, p.636.
5	Proskuryakov I.L. Sbornik zadach po lineynoy algebre. «Nauka», 2005 g.
6	G.G‘aymnazarov, O.G.Gaimnazarov, X.R.Umarov, Algebra va sonlar nazariyasidan masalalar yechish. GuDU, 2024.
7	Ғаймназаров Г., Гаимназаров О. Алгебра ва сонлар назариясидан масалалар ечиш. Тошкент, “Фан технология” 2015 й.
8	Kostrikin A.I. Vvedenie v algebru, M., «Nauka», 1977 g.
9	Buxshtab A.A. Teoriya chisel. M.: Prosvehenie,1966.-384s
10	Nesterenko Yu.V. Teoriya chisel. 2008
11	Hardy G.H., Wright E. M. An introduction to the Theory of Numbers. -6th.ed., Oxford University Press. -2008. -480 p.

Information sources

1. http://www.ziyonet.uz/
2. http://www.allmath.ru/
3. http://www.mcce.ru/
4. http://lib.mexmat.ru/
5. http://www.webmath.ru/

6. http://www.exponenta.ru/
7. http://www.intuit.ru/
8. Gulduportal.uz
9. https://unilibrary.uz