

§20

Group Homomorphisms

In Example 18.10(d), we have observed that the groups S_4/V_4 and S_3 have almost the same multiplication table. They have the same structure. In this paragraph, we study groups with the same structure.

20.1 Definition: Let G and G_1 be groups and let $\varphi: G \rightarrow G_1$ be a mapping from G into G_1 . If

$$(ab)\varphi = a\varphi.b\varphi \quad \text{for all } a,b \in G,$$

then φ is called a (*group*) *homomorphism*.

The equation $(ab)\varphi = a\varphi.b\varphi$ is paraphrased by saying that φ preserves multiplication or that φ preserves products. Loosely speaking, a homomorphism is a mapping under which the image of a product is the product of the images.

Here "products" might refer to different operations. For $a,b \in G$, the product $ab \in G$ is clearly the result of the binary operation of the group G , whereas $a\varphi, b\varphi \in G_1$ and $a\varphi.b\varphi \in G_1$ is the result of the binary operation of the group G_1 . This is implicit in the equation $(ab)\varphi = a\varphi.b\varphi$ which does not make any sense unless ab is the product of a,b in G and $a\varphi.b\varphi$ is the product of $a\varphi, b\varphi$ in G_1 .

More precisely, if \circ is the binary operation on G and if $*$ is the binary operation on G_1 , then $\varphi: G \rightarrow G_1$ is a homomorphism provided

$$(a \circ b)\varphi = a\varphi * b\varphi \quad \text{for all } a,b \in G.$$

20.2 Examples: (a) One homomorphism is very well known to the reader. It is the logarithm function

$$\log: \mathbb{R}^+ \rightarrow \mathbb{R}$$

from the group \mathbb{R}^+ of positive real numbers (under multiplication) into the group \mathbb{R} of all real numbers (under addition). The homomorphism property of the logarithm function is the well known identity

$$\log ab = \log a + \log b$$

that holds for all $a, b \in \mathbb{R}^+$.

(b) The determinant mapping

$$\det: GL(2, \mathbb{Q}) \rightarrow \mathbb{Q} \setminus \{0\}$$

is a homomorphism from $GL(2, \mathbb{Q})$ into the group of nonzero rational numbers under multiplication, for

$$\det AB = (\det A)(\det B)$$

for all $A, B \in GL(2, \mathbb{Q})$ by Theorem 17.9(1). The same thing is true for the mapping $\det: GL(2, K) \rightarrow K \setminus \{0\}$, where K is any arbitrary field.

(c) The sign mapping

$$\mathbb{E}: S_n \rightarrow \{1, -1\}$$

is a homomorphism from S_n into the multiplicative group $\{1, -1\}$ since

$$\mathbb{E}(\sigma\pi) = \mathbb{E}(\sigma)\mathbb{E}(\pi)$$

for all $\sigma, \pi \in S_n$ by Theorem 16.7.

(d) The absolute value function

$$\varphi: \mathbb{R} \setminus \{0\} \rightarrow \mathbb{R}^+$$

$$a \rightarrow |a|$$

is a homomorphism from the group of all nonzero real numbers (under multiplication) into the group of positive real numbers (under multiplication) since

$$(ab)\varphi = |ab| = |a||b| = a\varphi b\varphi$$

for all $a, b \in \mathbb{R} \setminus \{0\}$.

(e) The signum function

$$\text{sgn}: \mathbb{R} \setminus \{0\} \rightarrow \{1, -1\}$$

$$x \rightarrow \begin{cases} 1 & \text{if } x \text{ is positive} \\ -1 & \text{if } x \text{ is negative} \end{cases}$$

is a homomorphism from the group of nonzero real numbers into the group $\{1, -1\}$.

(f) Let G be a group. Then the identity mapping

$$\iota: G \rightarrow G$$

is a homomorphism from G into G since

$$(ab)\iota = ab = a\iota b\iota$$

for all $a, b \in G$. More generally, let H be a subgroup of G and let

$$\begin{aligned}\mu: H &\rightarrow G \\ h &\rightarrow h\end{aligned}$$

be the inclusion mapping (Example 3.2(a)). Then

$$(ab)\mu = ab = a\mu b\mu$$

for all $a, b \in H$. Hence μ is a homomorphism. Both ι and μ are one-to-one homomorphisms.

(g) Let $\varphi: G \rightarrow G_1$ be a group homomorphism and let $H \leq G$. Then the restriction

$$\varphi_H: H \rightarrow G_1$$

of φ to H (Example 3.2(i)) is a homomorphism from H into G_1 since

$$(ab)\varphi_H = (ab)\varphi = (a)\varphi(b)\varphi = (a)\varphi_H(b)\varphi_H$$

for all $a, b \in H$.

20.3 Lemma: Let $\varphi: G \rightarrow G_1$ be a homomorphism of groups.

(1) $1\varphi = 1$.

(2) $(a^{-1})\varphi = (a\varphi)^{-1}$ for all $a \in G$.

(3) $(a_1 a_2 \dots a_n)\varphi = (a_1\varphi)(a_2\varphi) \dots (a_n\varphi)$ for all $a_1, a_2, \dots, a_n \in G$, $n \in \mathbb{N}$, $n \geq 2$.

(4) $(a^n)\varphi = (a\varphi)^n$ for all $a \in G$, $n \in \mathbb{Z}$.

(5) If $o(a\varphi) = \infty$, then $o(a) = \infty$. If $o(a) = n \in \mathbb{N}$, then $o(a\varphi)$ divides n ; in particular, $o(a\varphi) \leq o(a)$.

Proof: (1) Here we use the same symbol "1" with two different meanings. In " 1φ ", 1 is the identity element of the group G . On the right hand side, 1 is the identity element of the group G_1 . A more accurate way of writing the claim is

$$(1_G)\varphi = 1_{G_1},$$

where 1_G is the identity element of G and 1_{G_1} is that of G_1 . For the homomorphisms in Examples 20.2(a)-(e), the assertion means

$$\log 1 = 0; \det \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = 1; \iota \text{ is an even permutation; } |1| = 1; 1 \text{ is positive}$$

respectively.

The proof is easy. We have $1\varphi = (1.1)\varphi = 1\varphi.1\varphi$, hence 1φ is the identity of G_1 by Lemma 7.3(1). One can also use $a\varphi 1\varphi = (a1)\varphi = a\varphi$ with some $a \in G$ to conclude $1\varphi = 1$.

(2) For any $a \in G$, we have $a\varphi(a^{-1}\varphi) = (aa^{-1})\varphi = 1\varphi = 1 = (a\varphi)(a\varphi)^{-1}$, hence $a^{-1}\varphi = (a\varphi)^{-1}$.

(3) We make induction on n . The case $n = 2$ is covered by the very definition of a homomorphism. Supposing the claim to be true for $n = k$, i.e., supposing $(a_1a_2 \dots a_k)\varphi = (a_1\varphi)(a_2\varphi) \dots (a_k\varphi)$ for all $a_1, a_2, \dots, a_k \in G$, we get

$$\begin{aligned} (a_1a_2 \dots a_k a_{k+1})\varphi &= ((a_1a_2 \dots a_k)a_{k+1})\varphi \\ &= (a_1a_2 \dots a_k)\varphi(a_{k+1})\varphi \\ &= (a_1\varphi)(a_2\varphi) \dots (a_k\varphi)(a_{k+1})\varphi \end{aligned}$$

and the claim is true for $n = k + 1$. Hence it is true for all $n \in \mathbb{N}$, $n \geq 2$.

(4) We prove $(a^n)\varphi = (a\varphi)^n$ for all $a \in G$, $n \in \mathbb{Z}$. If $n > 0$, this follows from (3) when we take $a_1 = a_2 = \dots = a_n = a$. If $n < 0$, this follows from (3) when we take $a_1 = a_2 = \dots = a_n = a^{-1}$. If $n = 0$, the claim is proved in (1).

(5) Suppose $o(a\varphi) = \infty$. If $o(a)$ were a natural number m , then we would obtain $a^m = 1$, so $(a\varphi)^m = (a^m)\varphi = 1\varphi = 1$ and $a\varphi$ would be of finite order by Lemma 11.4, a contradiction. Thus $o(a\varphi) = \infty$ implies $o(a) = \infty$.

Suppose $o(a) = n \in \mathbb{N}$. Then $a^n = 1$ and $(a\varphi)^n = (a^n)\varphi = 1\varphi = 1$, so $o(a\varphi) \mid n$ by Lemma 11.4 and Lemma 11.6.

□

Next we show that composition of homomorphisms is also a homomorphism.

20.4 Theorem: *Let $\varphi: G \rightarrow G_1$ and $\psi: G_1 \rightarrow G_2$ be group homomorphisms. Then the composition mapping*

$$\varphi\psi: G \rightarrow G_2$$

is a homomorphism from G into G_2

Proof: We are to show that $(ab)\varphi\psi = (a)\varphi\psi.(b)\varphi\psi$ for all $a, b \in G$. This follows immediately:

$$(ab)\varphi\psi = ((ab)\varphi)\psi \quad (\text{definition of } \varphi\psi)$$

$$\begin{aligned}
&= (a\varphi.b\varphi)\psi && (\varphi \text{ is a homomorphism}) \\
&= (a\varphi)\psi.(b\varphi)\psi && (\psi \text{ is a homomorphism}) \\
&= (a)\varphi\psi.(b)\varphi\psi && (\text{definition of } \varphi\psi)
\end{aligned}$$

for all $a, b \in G$. Hence $\varphi\psi$ is indeed a homomorphism. \square

20.5 Definition: Let $\varphi: G \rightarrow G_1$ be a group homomorphism. The set

$$\{a\varphi \in G_1; a \in G\} = \{b \in G_1; b = a\varphi \text{ for some } a \in G\}$$

of all images (under φ) of the elements of G is called the *image* of φ and is denoted by $Im \varphi$ or by $G\varphi$. The set

$$\{a \in G; a\varphi = 1\}$$

of all elements of the domain G that are mapped to the identity of the range group G_1 is called the *kernel* of φ and is written as $Ker \varphi$.

Thus $Im \varphi \subseteq G_1$ and $Ker \varphi \subseteq G$. It is immediate from the definition of $Im \varphi$ that $Im \varphi \neq \emptyset$, for $G \neq \emptyset$. Also, $1 = 1_G \in Ker \varphi$ by Lemma 20.3(1), so $Ker \varphi \neq \emptyset$. We prove now that $Im \varphi$ is a subgroup of G_1 and that $Ker \varphi$ is a subgroup of G . In fact, $Ker \varphi$ is a normal subgroup of G . This is a very important fact.

20.6 Theorem: Let $\varphi: G \rightarrow G_1$ be a group homomorphism. Then

$$Im \varphi \leq G_1 \quad \text{and} \quad Ker \varphi \trianglelefteq G.$$

Proof: First we prove $Im \varphi \leq G_1$. We know $Im \varphi \neq \emptyset$. We use our subgroup criterion (Lemma 9.2).

(i) Let $x, y \in Im \varphi$. We are to show $xy \in Im \varphi$. Now $x, y \in Im \varphi$ means $x = a\varphi$, $y = b\varphi$ for some $a, b \in G$. Then $xy = (a\varphi)(b\varphi) = (ab)\varphi$ is the image (under φ) of an element in G , namely of $ab \in G$. So $xy \in Im \varphi$ and $Im \varphi$ is closed under multiplication.

(ii) Let $x \in Im \varphi$. We are to show $x^{-1} \in Im \varphi$. Now $x \in Im \varphi$ means $x = a\varphi$ for some $a \in G$. Then $x^{-1} = (a\varphi)^{-1} = a^{-1}\varphi$ is the image (under

φ) of an element in G , namely of $a^{-1} \in G$. So $x^{-1} \in \text{Im } \varphi$ and $\text{Im } \varphi$ is closed under taking inverses.

Thus $\text{Im } \varphi \leq G_1$.

Now we prove $\text{Ker } \varphi \trianglelefteq G$. First $\text{Ker } \varphi \leq G$. We know $\text{Ker } \varphi \neq \emptyset$. Compare the following with the proof of Theorem 17.12.

(i) For any $a, b \in \text{Ker } \varphi$, we have $a\varphi = 1 = b\varphi$, so $(ab)\varphi = (a\varphi)(b\varphi) = 1 \cdot 1 = 1$ and $ab \in \text{Ker } \varphi$. Thus $\text{Ker } \varphi$ is closed under multiplication.

(ii) For any $a \in \text{Ker } \varphi$, we have $a\varphi = 1$, so $a^{-1}\varphi = (a\varphi)^{-1} = 1^{-1} = 1$ and $a^{-1} \in \text{Ker } \varphi$. Thus $\text{Ker } \varphi$ is closed under taking inverses.

Therefore $\text{Ker } \varphi \leq G$. Now we prove that $\text{Ker } \varphi$ is a normal subgroup of G . Compare the following with Example 18.5(j).

We must show that $g^{-1}kg \in \text{Ker } \varphi$ for any $g \in G, k \in \text{Ker } \varphi$ (Lemma 18.2(1)). This is easy: if $k \in \text{Ker } \varphi$, then $k\varphi = 1$ and, for any $g \in G$,

$$(g^{-1}kg)\varphi = (g^{-1}\varphi)(k\varphi)(g\varphi) = (g\varphi)^{-1} \cdot 1 \cdot g\varphi = 1,$$

so $g^{-1}kg \in \text{Ker } \varphi$. Thus $\text{Ker } \varphi \trianglelefteq G$. □

The elements of a group which have the same image under a homomorphism make up a coset of the kernel of that homomorphism.

20.7 Lemma: Let $\varphi: G \rightarrow G_1$ be a group homomorphism. For any $a, b \in G$, there holds $a\varphi = b\varphi$ if and only if $(\text{Ker } \varphi)a = (\text{Ker } \varphi)b$.

Proof: Let $a, b \in G$. Then $a\varphi = b\varphi$ if and only if

$$\begin{aligned} (a\varphi)(b\varphi)^{-1} &= 1, & \text{so if and only if} \\ (a\varphi)(b^{-1}\varphi) &= 1, & \text{so if and only if} \\ (ab^{-1})\varphi &= 1, & \text{so if and only if} \\ ab^{-1} &\in \text{Ker } \varphi, & \text{so if and only if} \\ (\text{Ker } \varphi)a &= (\text{Ker } \varphi)b \end{aligned}$$

by Lemma 10.2(5). □

Since $\text{Ker } \varphi \trianglelefteq G$ by Theorem 20.6, we also have $a(\text{Ker } \varphi) = \{b \in G: b\varphi = a\varphi\}$. Alternatively, one may prove a lemma analogous to Lemma 20.7, stating that a and b have the same image under φ if and only if the left cosets $a(\text{Ker } \varphi)$ and $b(\text{Ker } \varphi)$ are equal, and combine it Lemma 20.7 to get $a(\text{Ker } \varphi) = (\text{Ker } \varphi)a$, thereby proving $\text{Ker } \varphi \trianglelefteq G$ anew.

It follows from Lemma 20.7 that φ is a one-to-one homomorphism if and only if $\text{Ker } \varphi$ has only one element. We give a direct proof of this.

20.8 Theorem: *Let $\varphi: G \rightarrow G_1$ be a group homomorphism. Then φ is one-to-one if and only if $\text{Ker } \varphi = 1$.*

Proof: Here 1 is the trivial subgroup of G (Example 18.5(a)). We prove φ is not one-to-one if and only if $\text{Ker } \varphi \neq 1$.

If φ is not one-to-one, then there are $a, b \in G$ with $a\varphi = b\varphi$ and $a \neq b$. We obtain then $1 = a\varphi.(a\varphi)^{-1} = a\varphi.(b\varphi)^{-1} = a\varphi.b^{-1}\varphi = (ab^{-1})\varphi$, with $ab^{-1} \neq 1$. Thus $1 \neq ab^{-1} \in \text{Ker } \varphi$ and $\text{Ker } \varphi \neq 1$.

Conversely, if $\text{Ker } \varphi \neq 1$, then there is an $a \in \text{Ker } \varphi$ with $a \neq 1$. Then we have $a\varphi = 1 = 1\varphi$ and $a \neq 1$. So φ is not one-to-one. \square

We can determine whether a homomorphism is one-to-one by examining its kernel. A homomorphism φ is one-to-one if and only if $\text{Ker } \varphi = 1$. Also, we can determine whether a homomorphism is onto by examining its image. A homomorphism φ is onto if and only if $\text{Im } \varphi$ is the whole range. Homomorphisms which are both one-to-one and onto will have a name.

20.9 Definition: A group homomorphism $\varphi: G \rightarrow G_1$ is called an *isomorphism* if it is one-to-one and onto. If there is an isomorphism from G onto G_1 , we say G is *isomorphic to* G_1 , and write $G \cong G_1$. If G is not isomorphic to G_1 , we write $G \not\cong G_1$.

20.10 Examples: (a) The logarithm function is well known to be a one-to-one function onto the set of real numbers. Thus

$$\log: \mathbb{R}^+ \rightarrow \mathbb{R}$$

is an isomorphism.

(b) For any group G , the identity mapping

$$i: G \rightarrow G$$

is an isomorphism.

(c) Let G be a group. Then

$$\begin{aligned} \varphi: G &\rightarrow G/1 \\ g &\rightarrow \{g\} \end{aligned}$$

is an isomorphism from G onto $G/1$ (see Example 18.10(a)). Thus $G \cong G/1$.

(d) The mapping

$$\begin{aligned} \varphi: S_3 &\rightarrow S_4/V_4 \\ \sigma &\rightarrow V_4\sigma \end{aligned}$$

(where, on the right hand side, σ is the permutation in S_4 that fixes 4 and maps 1,2,3 as $\sigma \in S_3$ does) is an homomorphism. This is evident from the tables in Example 18.10(d). Also, φ is clearly one-to-one and onto. So φ is an isomorphism and $S_3 \cong S_4/V_4$.

An isomorphism, being one-to-one and onto, has an inverse mapping. It is natural to ask if the inverse of an isomorphism is an isomorphism. Also, is it true that composition of two isomorphisms is an isomorphism?

20.11 Lemma: Let $\varphi: G \rightarrow G_1$ and $\psi: G_1 \rightarrow G_2$ be group isomorphisms.

(1) The composition $\psi\varphi: G \rightarrow G_2$ is an isomorphism from G onto G_2 .

(2) The inverse $\varphi^{-1}: G_1 \rightarrow G$ of φ is an isomorphism from G_1 onto G .

Proof: (1) The composition $\psi\varphi$ is a homomorphism by Theorem 20.4. It is one-to-one and onto by Theorem 3.13. So $\psi\varphi$ is an isomorphism.

(2) For any $x,y \in G_1$, we must show $(xy)\varphi^{-1} = x\varphi^{-1}.y\varphi^{-1}$. Since φ is onto, there are $a,b \in G$ such that $a\varphi = x$ and $b\varphi = y$. Now a and b are unique

with this property, for φ is one-to-one, and $a = x\varphi^{-1}$, $b = y\varphi^{-1}$. This is the definition of the inverse mapping. Since φ is a homomorphism, we have

$$(ab)\varphi = a\varphi.b\varphi = xy$$

Hence, by definition of φ^{-1} , we get $ab = (xy)\varphi^{-1}$. Thus

$$(xy)\varphi^{-1} = ab = x\varphi^{-1}.y\varphi^{-1}$$

and this holds for all $x,y \in G_1$. So $\varphi^{-1}:G_1 \rightarrow G$ is a homomorphism. As it is one-to-one and onto by Theorem 3.17(1), φ^{-1} is an isomorphism. \square

From Example 20.10(b) and Lemma 20.11, we see that

$$\begin{aligned} G &\cong G \\ \text{if } G &\cong G_1, \text{ then } G_1 \cong G \\ \text{if } G &\cong G_1 \text{ and } G_1 \cong G_2, \text{ then } G \cong G_2 \end{aligned}$$

for any groups G,G_1,G_2 . We are tempted to say that \cong is an equivalence relation on the set of all groups. It is true indeed that \cong is an equivalence relation, but we must avoid the phrase "the set of all groups". This phrase leads to logical difficulties. For more information about this point, the reader is referred to the appendix.

Since $G \cong G_1$ implies $G_1 \cong G$, it is legitimate to say G and G_1 are isomorphic when G is isomorphic to G_1 .

We are not interested in the nature of the elements in a group. The essential thing is the algebraic structure of the group. If $G \cong G_1$, then any algebraic property of G is immediately carried over to G_1 . For this reason, we do not distinguish between isomorphic groups. For example, any two cyclic groups of the same order are easily seen to be isomorphic. By abuse of language, we call any cyclic group of order $n \in \mathbb{N}$ *the* cyclic group of order n , and write C_n for it. Likewise, any two dihedral groups of order $2n$ are isomorphic, and we speak of *the* dihedral group of order $2n$, and write D_{2n} for it.

We saw in Theorem 20.6 that the kernel of any homomorphism is a normal subgroup of the domain. We show now conversely that any normal subgroup of G is the kernel of some homomorphism from G . Into which group? Since we are given only a normal subgroup of G , the only

range group that we can construct out of G and its normal subgroup is the factor group with respect to that normal subgroup.

20.12 Theorem: Let $N \trianglelefteq G$. Then the mapping

$$\begin{aligned} \nu: G &\rightarrow G/N \\ a &\rightarrow Na \end{aligned}$$

is a homomorphism. It is onto G/N and $\text{Ker } \nu = N$.

Proof: ν is a homomorphism, for $(ab)\nu = N(ab) = Na.Nb = a\nu.b\nu$ for all a, b in G , by the very definition of multiplication in G/N . Obviously, any element Na of G/N is the image of $a \in G$ under ν , so ν is onto. Finally

$$\begin{aligned} \text{Ker } \nu &= \{a \in G: a\nu = \text{identity of } G/N\} \\ &= \{a \in G: a\nu = N1\} \\ &= \{a \in G: Na = N\} \\ &= \{a \in G: a \in N\} && \text{(Lemma 10.2(2))} \\ &= N. && \square \end{aligned}$$

20.13 Definition: Let $N \trianglelefteq G$. The mapping $\nu: G \rightarrow G/N$ is called the
 $a \rightarrow Na$
natural (or canonical) homomorphism from G onto G/N .

20.14 Theorem: Let $N \trianglelefteq G$. Then there is a homomorphism $\varphi: G \rightarrow G_1$ with $\text{Ker } \varphi = N$.

Proof: N is the kernel of the natural homomorphism $\nu: G \rightarrow G/N$ by Theorem 20.12. □

The coincidence of kernels with normal subgroups shows that normal subgroups, factor groups and homomorphisms are closely related. Theorem 20.12 describes the relation between $N \trianglelefteq G$, G/N and the natural homomorphism $\nu: G \rightarrow G/N$. We prove next that any homomorphism φ is connected in the same way to $\text{Ker } \varphi$ and $G/\text{Ker } \varphi$ as ν is connected to N

and G/N . This is done by showing that φ is essentially a natural homomorphism.

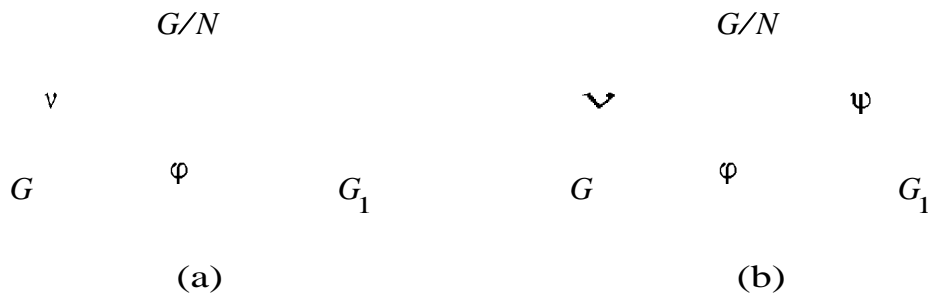
20.15 Theorem (Fundamental theorem on homomorphisms):

Let

$\varphi: G \rightarrow G_1$ be a homomorphism of groups. Let $N = \text{Ker } \varphi$, which is normal in G by Theorem 20.6, and let $v: G \rightarrow G/N$ be the associated natural homomorphism.

Then there is a one-to-one homomorphism $\psi: G/N \rightarrow G_1$ such that $v\psi = \varphi$.

[This theorem may be summarized in a diagram. The hypothesis is the diagram (a) below. The claim is that there is a one-to-one homomorphism ψ such that both paths from G to G_1 ($v\psi$ and φ) in diagram (b) have the same effect.



The equation $v\psi = \varphi$ can be regarded as a factorization of φ . Since the path $v\psi$ passes through $G/\text{Ker } \varphi$, we say φ factors through $G/\text{Ker } \varphi$.

Proof: We must find a suitable $\psi: G/N \rightarrow G_1$. We want $\varphi = v\psi$, so that $a\varphi = a(v\psi) = (av)\psi = (Na)\psi$. So we define

$$\begin{aligned} \psi: G/N &\rightarrow G_1 \\ Na &\rightarrow a\varphi \end{aligned}$$

In order to find the image of any coset of N under ψ , we have to choose an element a from that coset, which can be done, generally speaking, in many ways. So we have to make sure that ψ is a well defined function. Thus we have to show

$$\text{for all } a, b \in G, \quad Na = Nb \implies (Na)\psi = (Nb)\psi.$$

From the definition of $N = \text{Ker } \varphi$ and of ψ , we see that this implication is equivalent to

$$\text{for all } a, b \in G, \quad (\text{Ker } \varphi)a = (\text{Ker } \varphi)b \implies a\varphi = b\varphi,$$

and this is true by Lemma 20.7. Thus ψ is indeed a well defined mapping.

ψ is a homomorphism. This is verified easily:

$$\begin{aligned} (Na.Nb)\psi &\stackrel{?}{=} (Na)\psi.(Nb)\psi && \text{for all } a, b \in G \\ (Nab)\psi &\stackrel{?}{=} (Na)\psi.(Nb)\psi && \text{for all } a, b \in G \\ (ab)\varphi &\stackrel{?}{=} a\varphi.b\varphi && \text{for all } a, b \in G \end{aligned}$$

Since φ is a homomorphism, the last line is true. Hence ψ is a homomorphism.

ψ is one-to-one. To prove this, we need only show $\text{Ker } \psi = \{N\}$ (see Theorem 20.8; N is the identity of G/N). We observe

$$\begin{aligned} \text{Ker } \psi &= \{Na \in G/N: (Na)\psi = 1 = 1_{G_1}\} \\ &= \{Na \in G/N: a\varphi = 1\} \\ &= \{Na \in G/N: a \in \text{Ker } \varphi\} \\ &= \{Na \in G/N: a \in N\} \\ &= \{N\} \end{aligned}$$

by Lemma 10.2(2) and ψ is one-to-one.

From the definition of ψ , we have $a(v\psi) = (av)\psi = (Na)\psi = a\varphi$ for all $a \in G$, so $v\psi = \varphi$.

This completes the proof. □

20.16 Theorem: *Let $\varphi: G \rightarrow G_1$ be a group homomorphism. Then*

$$G/\text{Ker } \varphi \cong \text{Im } \varphi.$$

In more detail: there is an isomorphism $\varphi': G/\text{Ker } \varphi \rightarrow \text{Im } \varphi$ such that $v\varphi'\mu = \varphi$, where $v: G \rightarrow G/\text{Ker } \varphi$ is the natural homomorphism and $\mu: \text{Im } \varphi \rightarrow G_1$ is the inclusion homomorphism (Example 20.2(f)). This means that the diagram

$$\begin{array}{ccc}
 G & \xrightarrow{\varphi} & G_1 \\
 \nu \downarrow & & \uparrow \mu \\
 G/\text{Ker } \varphi & & \text{Im } \varphi
 \end{array}$$

can be so completed with a homomorphism φ' that both paths $\nu\varphi'\mu$ and φ

$$\begin{array}{ccc}
 G & \xrightarrow{\varphi} & G_1 \\
 \nu \downarrow & & \uparrow \mu \\
 G/\text{Ker } \varphi & \xrightarrow{\varphi'} & \text{Im } \varphi
 \end{array}$$

have the same effect.

Proof: We use the homomorphism $\psi: G/N \rightarrow G_1$ of Theorem 20.15, where $N = \text{Ker } \varphi$. Obviously,

$$\text{Im } \psi = \{(Na)\psi: Na \in G/N\} = \{a\varphi: a \in G\} = \text{Im } \varphi$$

and since ψ is one-to-one, ψ is an isomorphism from $G/\text{Ker } \varphi$ onto $\text{Im } \psi = \text{Im } \varphi$. We observe

$$a(\nu\psi\mu) = (a\nu)(\psi\mu) = (Na)(\psi\mu) = ((Na)\psi)\mu = (a\varphi)\mu = a\varphi$$

for all $a \in G$, as μ maps any element of $\text{Im } \varphi$ to itself. Hence $\nu\psi\mu = \varphi$. The theorem follows when we write φ' in place of ψ . \square

According to Theorem 20.16, any homomorphism $\varphi: G \rightarrow G_1$ is factored into three homomorphisms ν, φ', μ :

$$G \xrightarrow{\nu} G/\text{Ker } \varphi \xrightarrow{\varphi'} \text{Im } \varphi \xrightarrow{\mu} G_1$$

where (a) ν is onto $G/\text{Ker } \varphi$; (b) φ' is one-to-one and onto $\text{Im } \varphi$ and (c) μ is one-to-one. So $\nu\varphi'$ is onto and $\varphi'\mu$ is one-to-one (Theorem 3.11). Hence, if φ fails to be onto, it is only due to the fact that μ is not onto. Also, if φ fails to be one-to-one, it is only due to the fact that ν is not one-to-one. We see that any homomorphism φ is essentially an isomorphism φ' , "diluted" by a natural homomorphism which (eventually) accounts for its failure to be one-to-one and by an inclusion mapping which (eventually) accounts for its failure to be onto. In fact, φ is one-to-one if and only if the associated natural homomorphism $\nu: G \rightarrow G/\text{Ker } \varphi$ is one-to-one and φ is onto if and only if the associated inclusion mapping $\mu: \text{Im } \varphi \rightarrow G_1$ is onto.

20.17 Examples: (a) Let $\langle a \rangle = \{a^n: n \in \mathbb{Z}\}$ be a cyclic group. The mapping

$$\begin{aligned}\psi: \mathbb{Z} &\rightarrow \langle a \rangle \\ n &\rightarrow a^n\end{aligned}$$

is a homomorphism from the additive group \mathbb{Z} into $\langle a \rangle$, because

$$(m+n)\psi = a^{n+m} = a^m a^n = m\psi \cdot n\psi$$

for all $m, n \in \mathbb{Z}$. From Theorem 20.16, we obtain

$$\mathbb{Z}/\text{Ker } \psi \cong \text{Im } \psi.$$

The homomorphism ψ is onto by definition of $\langle a \rangle$, hence $\text{Im } \psi = \langle a \rangle$ and

$$\mathbb{Z}/\text{Ker } \psi \cong \langle a \rangle.$$

We see that any cyclic group is isomorphic to a factor group of \mathbb{Z} . In order to get more information, we distinguish two cases, where $\langle a \rangle$ has finite or infinite order.

First suppose that $\langle a \rangle$ has finite order $k \in \mathbb{N}$. Then $o(a) = k$ and

$$\begin{aligned}\text{Ker } \psi &= \{n \in \mathbb{Z}: n\psi = 1 = a^0\} \\ &= \{n \in \mathbb{Z}: a^n = 1\} \\ &= \{n \in \mathbb{Z}: o(a) | n\} && \text{(Lemma 11.6)} \\ &= k\mathbb{Z}.\end{aligned}$$

Thus $\mathbb{Z}/k\mathbb{Z} \cong \langle a \rangle$. We see that any cyclic group of order k is isomorphic to $\mathbb{Z}/k\mathbb{Z}$. Consequently, any two cyclic groups of order k are isomorphic to each other. For this reason, we speak of *the* cyclic group of order k .

In the second case, suppose $\langle a \rangle$ has infinite order. Then

$$\begin{aligned}\text{Ker } \psi &= \{n \in \mathbb{Z}: n\psi = 1 = a^0\} \\ &= \{n \in \mathbb{Z}: a^n = 1\} \\ &= \{0\} && \text{(Lemma 11.5)}\end{aligned}$$

and so $\mathbb{Z}/\{0\} \cong \langle a \rangle$. From $\mathbb{Z}/\{0\} \cong \mathbb{Z}$ (Example 20.10(c)), we infer $\mathbb{Z} \cong \langle a \rangle$. We see that any infinite cyclic group is isomorphic to \mathbb{Z} . Consequently, any two cyclic groups of infinite order are isomorphic. For this reason, we speak of *the* infinite cyclic group.

(b) The determinant homomorphism (Example 20.2(b))

$$\det: GL(2, \mathbb{Q}) \rightarrow \mathbb{Q} \setminus \{0\}$$

is onto $\mathbb{Q} \setminus \{0\}$, because any $a \in \mathbb{Q} \setminus \{0\}$ is the determinant of $\begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix}$ in $GL(2, \mathbb{Q})$. Thus $Im \det = \mathbb{Q} \setminus \{0\}$. Also

$$ker \det = \{A \in GL(2, \mathbb{Q}) : \det A = 1\} = SL(2, \mathbb{Q}).$$

From Theorem 20.16, we obtain

$$GL(2, \mathbb{Q})/SL(2, \mathbb{Q}) \cong \mathbb{Q} \setminus \{0\}.$$

In the same way, $GL(2, K)/SL(2, K) \cong K \setminus \{0\}$

for any field K .

(c) The sign homomorphism

$$\mathbb{E}: S_n \rightarrow \{1, -1\} = C_2$$

is onto C_2 when $n \geq 2$, because $\mathbb{E}(i) = 1$ and $\mathbb{E}((12)) = -1$. Hence $Im \mathbb{E} = C_2$. As $Ker \mathbb{E} = \{\sigma \in S_n : \mathbb{E}(\sigma) = 1\} = A_n$ by definition, the relation

$$S_n / Ker \mathbb{E} \cong Im \mathbb{E}$$

yields

$$S_n / A_n \cong C_2.$$

(d) Consider the absolute value homomorphism

$$\begin{aligned} \varphi: \mathbb{R} \setminus \{0\} &\rightarrow \mathbb{R}^+ \\ a &\rightarrow |a| \end{aligned}$$

Here $Im \varphi = \{|a| : a \in \mathbb{R} \setminus \{0\}\} = \mathbb{R}^+$ and $Ker \varphi = \{a \in \mathbb{R} \setminus \{0\} : |a| = 1\} = \{1, -1\} = C_2$. Thus

$$S_n / Ker \varphi \cong Im \varphi$$

gives

$$(\mathbb{R} \setminus \{0\}) / C_2 \cong \mathbb{R}^+.$$

(e) The mapping

$$\begin{aligned} \varphi: \mathbb{R} &\rightarrow \mathbb{C} \setminus \{0\} \\ x &\rightarrow e^{2\pi xi} \end{aligned}$$

is a homomorphism from the additive group \mathbb{R} into $\mathbb{C} \setminus \{0\}$:

$$(x + y)\varphi = e^{2\pi(x+y)i} = e^{2\pi xi} e^{2\pi yi} = x\varphi \cdot y\varphi$$

for all $x, y \in \mathbb{R}$. We have $\mathbb{R}/\text{Ker } \varphi \cong \text{Im } \varphi$. The reader may verify that

$$\text{Im } \varphi = \{z \in \mathbb{C} : |z| = 1\}.$$

As for the kernel,

$$\begin{aligned} \text{Ker } \varphi &= \{x \in \mathbb{R} : e^{2\pi xi} = 1\} \\ &= \{x \in \mathbb{R} : \cos 2\pi x + i \sin 2\pi x = 1\} \\ &= \{x \in \mathbb{R} : \cos 2\pi x = 1, \sin 2\pi x = 0\} \\ &= \mathbb{Z}. \end{aligned}$$

Thus

$$\mathbb{R}/\mathbb{Z} \cong \{z \in \mathbb{C} : |z| = 1\},$$

where \mathbb{R}/\mathbb{Z} is an additive, the right hand side is a multiplicative group.

Exercises

1. Show that the mapping $\exp: \mathbb{R} \rightarrow \mathbb{R}^+$ is an isomorphism.

$$x \rightarrow e^x$$
2. Determine whether the mapping $x \rightarrow \log(\log x)$ is a homomorphism.
3. Find an isomorphism from $\mathbb{Q} \setminus \{0\}$ under multiplication onto the group of Example 7.4(a).
4. Find an isomorphism from \mathbb{Z} under addition onto the group of Example 7.4(b).
5. Let $\varphi_i: G_i \rightarrow G_{i+1}$ be homomorphisms of groups, where $i = 1, 2, \dots, n$. Show that $\varphi_1 \varphi_2 \dots \varphi_n$ is a homomorphism from G_1 onto G_{n+1} . Prove a corresponding result for isomorphisms.
6. Let $\varphi: G \rightarrow G_1$ be an isomorphism. Prove that $o(a) = o(a\varphi)$ for all $a \in G$.
7. Let $\varphi: G \rightarrow G_1$ be a homomorphism. Show that $a\varphi = b\varphi$ if and only if $a(\text{Ker } \varphi) = b(\text{Ker } \varphi)$, where a, b are arbitrary elements of G .
8. Prove directly that any two cyclic groups of the same order are isomorphic.
9. Prove that any two dihedral groups of the same order are isomorphic.

10. Imitating Example 20.17(a), show that any dihedral group is isomorphic to a factor group of D_∞ .
11. Show that a factor group of a dihedral group is either dihedral or cyclic.
12. Let $n \in \mathbb{N}$ and let X be a set with n elements. Prove that $S_X \cong S_n$.
13. Prove that $(\mathbb{R} \setminus \{0\})/\mathbb{R}^+ \cong C_2$.
14. Let $\varphi: G \rightarrow G_1$ be a homomorphism, let K be a normal subgroup of G such that $K \leq \text{Ker } \varphi$, and let $v: G \rightarrow G/K$ be the associated natural homomorphism. Show that there is a homomorphism $\psi: G/K \rightarrow G_1$ such that $v\psi = \varphi$ and $\text{Ker } \psi = (\text{Ker } \varphi)/K$. What happens when we drop the condition $K \leq \text{Ker } \varphi$?