6. The Homomorphism Theorems

In this section, we investigate maps between groups which preserve the group-operations.

**Definition.** Let $G$ and $H$ be groups and let $\varphi : G \to H$ be a mapping from $G$ to $H$. Then $\varphi$ is called a **homomorphism** if for all $x, y \in G$ we have:

$$\varphi(xy) = \varphi(x) \varphi(y).$$

A homomorphism which is also bijective is called an **isomorphism**.

A homomorphism from $G$ to itself is called an **endomorphism**.

An isomorphism from $G$ to itself is called an **automorphism**, and the set of all automorphisms of a group $G$ is denoted by $\text{Aut}(G)$.

Before we show that $\text{Aut}(G)$ is a group under compositions of maps, let us prove that a homomorphism preserves the group structure.

**Proposition 6.1.** If $\varphi : G \to H$ is a homomorphism, then $\varphi(e_G) = e_H$ and for all $x \in G$, $\varphi(x^{-1}) = \varphi(x)^{-1}$.

**Proof.** Since $\varphi$ is a homomorphism, for all $x, y \in G$ we have $\varphi(xy) = \varphi(x) \varphi(y)$. In particular, $\varphi(y) = \varphi(e_G y) = \varphi(e_G) \varphi(y)$, which implies $\varphi(e_G) = e_H$. Further, $\varphi(e_G) = \varphi(x x^{-1}) = \varphi(x) \varphi(x^{-1}) = e_H$, which implies $\varphi(x^{-1}) = \varphi(x)^{-1}$. \(\square\)

**Corollary 6.2.** If $\varphi : G \to H$ is a homomorphism, then the image of $\varphi$ is a subgroup of $H$.

**Proof.** Let $a$ and $b$ be in the image of $\varphi$. We have to show that also $ab^{-1}$ is in the image of $\varphi$. If $a$ and $b$ are in the image of $\varphi$, then there are $x, y \in G$ such that $\varphi(x) = a$ and $\varphi(y) = b$. Now, by Proposition 6.1 we get

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

\(\square\)

**Proposition 6.3.** For any group $G$, the set $\text{Aut}(G)$ is a group under compositions of maps.

**Proof.** Let $\varphi, \psi \in \text{Aut}(G)$. First we have to show that $\varphi \circ \psi \in \text{Aut}(G)$: Since $\varphi$ and $\psi$ are both bijections, $\varphi \circ \psi$ is a bijection too, and since $\varphi$ and $\psi$ are both homomorphisms, we have

$$(\varphi \circ \psi)(xy) = \varphi(\psi(xy)) = \varphi(\psi(x) \psi(y)) = \varphi(\psi(x)) \varphi(\psi(y)) = (\varphi \circ \psi)(x) (\varphi \circ \psi)(y).$$

Hence, $\varphi \circ \psi \in \text{Aut}(G)$. Now, let us show that $(\text{Aut}(G), \circ)$ is a group:

(A0) Let $\varphi_1, \varphi_2, \varphi_3 \in \text{Aut}(G)$. Then for all $x \in G$ we have

$$(\varphi_1 \circ (\varphi_2 \circ \varphi_3))(x) = \varphi_1((\varphi_2 \circ \varphi_3)(x)) = \varphi_1(\varphi_2(\varphi_3(x))) = (\varphi_1 \circ \varphi_2)(\varphi_3(x)) = ((\varphi_1 \circ \varphi_2) \circ \varphi_3)(x),$$

which implies that $\varphi_1 \circ (\varphi_2 \circ \varphi_3) = (\varphi_1 \circ \varphi_2) \circ \varphi_3$, thus, “$\circ$” is associative.

(A1) The identity mapping $\iota$ on $G$ is of course a bijective homomorphism from $G$ to itself, and in fact, $\iota$ is the neutral element of $(\text{Aut}(G), \circ)$.

22
(A2) Let \( \varphi \in \operatorname{Aut}(G) \), and let \( \varphi^{-1} \) be such that for every \( x \in G \), \( \varphi(\varphi^{-1}(x)) = x \). It is obvious that \( \varphi \circ \varphi^{-1} = \iota \) and it remains to show that \( \varphi^{-1} \) is a homomorphism: Since \( \varphi \) is a homomorphism, for all \( x, y \in G \) we have
\[
\varphi^{-1}(xy) = \varphi^{-1}\left(\varphi(\varphi^{-1}(x)) \varphi(\varphi^{-1}(y))\right) = \varphi^{-1}\left(\varphi(\varphi^{-1}(x) \varphi^{-1}(y))\right) = \varphi^{-1}(x) \varphi^{-1}(y),
\]
which shows that \( \varphi^{-1} \in \operatorname{Aut}(G) \).

\[\text{Definition.}\] If \( \varphi : G \to H \) is a homomorphism, then \( \{ x \in G : \varphi(x) = e_H \} \) is called the kernel of \( \varphi \) and is denoted by \( \ker(\varphi) \).

\[\text{Theorem 6.4.}\] Let \( \varphi : G \to H \) be a homomorphism, then \( \ker(\varphi) \leq G \).

\[\text{Proof.}\] First we have to show that \( \ker(\varphi) \leq G \): If \( a, b \in \ker(\varphi) \), then
\[
\varphi(ab^{-1}) = \varphi(a) \varphi(b)^{-1} = \varphi(a) \varphi(b^{-1}) = e_H e_H^{-1} = e_H,
\]
thus, \( ab^{-1} \in \ker(\varphi) \), which implies \( \ker(\varphi) \leq G \).

Now we show that \( \ker(G) \leq G \): Let \( x \in G \) and \( a \in \ker(\varphi) \), then
\[
\varphi(xax^{-1}) = \varphi(x) \varphi(a) \varphi(x)^{-1} = \varphi(x) x_H \varphi(x)^{-1} = \varphi(x) \varphi(x)^{-1} = e_H,
\]
thus, \( xax^{-1} \in \ker(\varphi) \), which implies \( \ker(\varphi) \leq G \).

Let us give some examples of homomorphisms:

1. The mapping
\[
\varphi : (\mathbb{R}, +) \to (\mathbb{R}^+, \cdot) \quad x \mapsto e^x
\]
is an isomorphism, and \( \varphi^{-1} = \ln \).

2. Let \( n \) be a positive integer. Then
\[
\varphi : (O(n), \cdot) \to (\{1, -1\}, \cdot) \quad A \mapsto \det(A)
\]
is a surjective homomorphism and \( \ker(\varphi) = \text{SO}(n) \). Further, for \( n = 1 \), \( \varphi \) is even an isomorphism.

3. The mapping
\[
\varphi : \mathbb{R}^3 \to \mathbb{R}^2 \quad (x, y, z) \mapsto (x, z)
\]
is a surjective homomorphism and \( \ker(\varphi) = \{(0, y, 0) : y \in \mathbb{R}\} \).

4. Let \( n \geq 3 \) be an integer, let \( C_n = \{a^n, \ldots, a^{n-1}\} \), and let \( \rho \in D_n \) be the rotation through \( 2\pi/n \). Then \( \varphi : C_n \to D_n \), defined by \( \varphi(a^k) := \rho^k \) is an injective homomorphism from \( C_n \) into \( D_n \). Thus, \( C_n \) is isomorphic to a subgroup of \( D_n \).
(5) Let \( n \geq 3 \) be an integer. For any \( x \in D_n \), let
\[
\text{sg}(x) = \begin{cases} 
1 & \text{if } x \text{ is a rotation}, \\
-1 & \text{if } x \text{ is a reflection}, 
\end{cases}
\]
then
\[
\varphi : D_n \to (\{1,-1\}, \cdot)
\]
\[
x \mapsto \text{sg}(x)
\]
is a surjective homomorphism.

(6) The mapping
\[
\varphi : (\mathbb{Z}_{12}, +) \to (\mathbb{Z}_{12}, +)
\]
\[
x \mapsto 4x
\]
is an endomorphism of \((\mathbb{Z}_{12}, +)\), where \( \ker(\varphi) = \{0, 3, 6, 9\} \) and the image of \( \varphi \) is \( \{0, 4, 8\} \).

(7) For every \( r \in \mathbb{Q}^* \), the mapping
\[
\varphi : (\mathbb{Q}, +) \to (\mathbb{Q}, +)
\]
\[
q \mapsto rq
\]
is an automorphism of \((\mathbb{Q}, +)\).

(8) Let \( C_2 \times C_2 = \{e, a, b, c\} \), then every permutation of \( \{a, b, c\} \) is a bijective homomorphism from \( C_2 \times C_2 \) to itself. Hence, \( \text{Aut}(C_2 \times C_2) \) is isomorphic to \( S_3 \) (or to \( D_3 \)).

In order to define an operation on the set \( G/N \), where \( N \trianglelefteq G \), we need the following:

**FACT 6.5.** If \( N \trianglelefteq G \), then for all \( x, y \in G \), \( (xN)(yN) = (xy)N \).

**Proof.** Since \( N \) is a normal subgroup of \( G \), we have
\[
(xN)(yN) = \left( x \underbrace{(yNy^{-1})}_{=N} \right)(yN) = (xy)(NN) = (xy)N.
\]
\[\Box\]

This leads to the following:

**PROPOSITION 6.6.** If \( N \trianglelefteq G \), then the set \( G/N = \{xN : x \in G\} \) is a group under the operation \((xN)(yN) := (xy)N\).
Proof. First we have to show that the operation \((x N) (y N)\) is well-defined: If \((x N) = (\tilde{x} N)\) and \((y N) = (\tilde{y} N)\), then, by Lemma 3.6 (d), \(x^{-1}\tilde{x}, y^{-1}\tilde{y} \in N\). Now, since \(N\) is a normal subgroup of \(G\),
\[
(xy)^{-1}(\tilde{x}\tilde{y}) = y^{-1}(x^{-1}\tilde{x})\tilde{y} \in y^{-1}N\tilde{y} = y^{-1}N(y^{-1}\tilde{y}) = N\,
\]
which implies \((x N) (y N) = (xy)N = (\tilde{x} N) (\tilde{y} N)\).

Now, let us show that \(G/N\) is a group:
(A0) \((x N)((y N) (z N)) = (x(yz))N = ((xy) z)N = ( (x N) (y N))(z N)\).
(A1) For all \(x \in G\) we have
\[
(e N) (x N) = (ex)N = xN,
\]
therefore, \(e N = N\) is the neutral element of \(G/N\).
(A2) For all \(x \in G\) we have
\[
(x N)(x^{-1} N) = (xx^{-1}) N = eN = N = (x^{-1} x) N = (x^{-1} N)(x N),
\]
therefore, \((x N)^{-1} = (x^{-1} N)\). ⊟

For example, let \(C\) be the cube-group and let \(N\) be the normal subgroup of \(C\) which is isomorphic to \(C_2 \times C_2\). Then, by Proposition 6.6, \(C/N\) is a group, and in fact, \(C/N\) is isomorphic to \(S_3\) (see Hw9.Q41).

Lemma 6.7. If \(N \trianglelefteq G\), then
\[
\pi : G \rightarrow G/N \quad x \mapsto xN
\]
is a surjective homomorphism, called the natural homomorphism from \(G\) onto \(G/N\), and \(\ker(\pi) = N\).

Proof. For all \(x, y \in G\) we have \(\pi(xy) = (xy)N = (x N) (y N) = \pi(x) \pi(y)\), thus, \(\pi\) is a homomorphism. Further, let \(x N \in G/N\), then \(\pi(x) = xN\), which shows that \(\pi\) is surjective. Finally, by Lemma 3.6 (c), \(\ker(\pi) = \{ x \in G : x N = N \} = N\). ⊟

By Theorem 6.4 we know that if \(\varphi : G \rightarrow H\) is a homomorphism, then \(\ker(\varphi) \trianglelefteq G\). On the other hand, by Lemma 6.7, we get the following:

Corollary 6.8. If \(N \trianglelefteq G\), then there exists a group \(H\) and a homomorphism \(\varphi : G \rightarrow H\) such that \(N = \ker(\varphi)\).

Proof. Let \(H = G/N\) and let \(\varphi\) be the natural homomorphism from \(G\) onto \(H\). ⊟

Theorem 6.9 (First Isomorphism Theorem). Let \(\psi : G \rightarrow H\) be a surjective homomorphism, let \(N = \ker(\psi) \trianglelefteq G\) and let \(\pi : G \rightarrow G/N\) be the natural homomorphism from \(G\) onto \(G/N\). Then there is a unique isomorphism \(\varphi : G/N \rightarrow H\) such that \(\psi = \varphi \circ \pi\). In other words, the following diagram “commutes”:

\[
\begin{array}{c}
G \\
\downarrow \pi \\
G/N \quad \psi \quad \varphi \\
\downarrow \pi \\
H
\end{array}
\]
**Proof.** Define \( \varphi : G/N \to H \) by stipulating \( \varphi(xN) := \psi(x) \) (for every \( x \in G \)). Then \( \psi = \varphi \circ \pi \) and it remains to be shown that \( \varphi \) is well-defined, a bijective homomorphism and unique.

\( \varphi \) is well-defined: If \( xN = yN \), then \( x^{-1}y \in N \) (by Lemma 3.6(d)). Thus, since \( N = \ker(\psi) \), \( \psi(x^{-1}y) = e_H \) and since \( \psi \) is a homomorphism we have \( e_H = \psi(x^{-1}y) = \psi(x)^{-1}\psi(y) \), which implies \( \psi(x) = \psi(y) \). Therefore, \( \varphi(xN) = \psi(x) = \psi(y) = \varphi(yN) \).

\( \varphi \) is a homomorphism: Let \( xN, yN \in G/N \), then

\[
\varphi((xN)(yN)) = \varphi((xy)N) = \psi(xy) = \psi(x)\psi(y) = \varphi(xN)\varphi(yN).
\]

\( \varphi \) is injective:

\[
\varphi(xN) = \varphi(yN) \iff \psi(x) = \psi(y) \iff e_H = \psi(x)^{-1}\psi(y) = \psi(x^{-1}y) = \psi(x^{-1})\psi(y) = \psi(x^{-1}y) \iff x^{-1}y \in N \iff xN = yN.
\]

\( \varphi \) is surjective: Since \( \psi \) is surjective, for all \( z \in H \) there is an \( x \in G \) such that \( \psi(x) = z \), thus, \( \varphi(xN) = z \).

\( \varphi \) is unique: Assume towards a contradiction that there exists an isomorphism \( \tilde{\varphi} : G/N \to H \) different from \( \varphi \) such that \( \tilde{\varphi} \circ \pi = \psi \). Then there is a coset \( xN \in G/N \) such that \( \tilde{\varphi}(xN) \neq \varphi(xN) \), which implies

\[
\psi(x) = (\tilde{\varphi} \circ \pi)(x) = \tilde{\varphi}(\pi(x)) = \tilde{\varphi}(xN) \neq \varphi(xN) = \varphi(\pi(x)) = (\varphi \circ \pi)(x) = \psi(x),
\]

a contradiction. \( \square \)

For example, let \( m \) be a positive integer and let \( C_m = \{a^0, \ldots, a^{m-1}\} \) be the cyclic group of order \( m \). Further, let \( \psi : \mathbb{Z} \to C_m \), where \( \psi(k) := a^k \). Then \( \psi \) is a surjective homomorphism from \( \mathbb{Z} \) to \( C_m \) and \( \ker(\psi) = m\mathbb{Z} \). Thus, by Theorem 6.9, \( \mathbb{Z}/m\mathbb{Z} \) and \( C_m \) are isomorphic and the isomorphism \( \varphi : \mathbb{Z}/m\mathbb{Z} \to C_m \) is defined by \( \varphi(k + m\mathbb{Z}) := a^k \).

Let us consider some other applications of Theorem 6.9:

(1) Let \( n \) be a positive integer. Then

\[
\psi : (O(n), \cdot) \to (\{1, -1\}, \cdot)
\]

\[
A \mapsto \det(A)
\]

is a surjective homomorphism with \( \ker(\psi) = SO(n) \), and thus, \( O(n)/SO(n) \) and \( \{1, -1\} \) are isomorphic (where \( \{1, -1\} \cong C_2 \)).

(2) Let \( n \) be a positive integer and let \( GL(n)^+ = \{A \in GL(n) : \det(A) > 0\} \). Then

\[
\psi : (GL(n)^+, \cdot) \to (\mathbb{R}^+, \cdot)
\]

\[
A \mapsto \det(A)
\]

is a surjective homomorphism with \( \ker(\psi) = SL(n) \), and thus, \( GL(n)^+/SL(n) \) and \( \mathbb{R}^+ \) are isomorphic.
(3) The mapping
\[ \psi : (\mathbb{C}^*, \cdot) \rightarrow (\mathbb{R}^+, \cdot) \]
\[ z \mapsto |z| \]
is a surjective homomorphism with \( \ker(\psi) = \mathbb{U} = \{z \in \mathbb{C} : |z|\} \), and thus, \( \mathbb{C}^*/\mathbb{U} \) and \( \mathbb{R}^+ \) are isomorphic.

(4) The mapping
\[ \psi : \mathbb{R}^3 \rightarrow \mathbb{R}^2 \]
\[ (x, y, z) \mapsto (x, z) \]
is a surjective homomorphism with \( \ker(\psi) = \{(0, y, 0) : y \in \mathbb{R} \} \cong \mathbb{R} \), and thus, \( \mathbb{R}^3/\mathbb{R} \) and \( \mathbb{R}^2 \) are isomorphic.

(5) The mapping
\[ \psi : (\mathbb{Z}_{12}, +) \rightarrow (\mathbb{Z}_{3}, +) \]
\[ x \mapsto x \pmod{3} \]
is a surjective homomorphism with \( \ker(\psi) = \{0, 3, 6, 9\} = 3\mathbb{Z}_{12} \), and thus, \( \mathbb{Z}_{12}/3\mathbb{Z}_{12} \) and \( \mathbb{Z}_{3} \) are isomorphic.

**Theorem 6.10 (Second Isomorphism Theorem).** Let \( N \trianglelefteq G \) and \( K \trianglelefteq G \). Then

1. \( KN = NK \trianglelefteq G \).
2. \( N \trianglelefteq KN \).
3. \( (N \cap K) \trianglelefteq K \).
4. The mapping
\[ \varphi : K/(N \cap K) \rightarrow KN/N \]
\[ x(N \cap K) \mapsto xN \]
is an isomorphism.

**Proof.** (1) This is Theorem 5.8.

(2) Since \( KN \subseteq G \) and \( N \subseteq KN \), \( N \trianglelefteq KN \). Hence, since \( N \trianglelefteq G \), \( N \trianglelefteq KN \).

(3) Let \( x \in K \) and \( a \in N \cap K \). Then \( xax^{-1} \) belongs to \( K \), since \( x, a \in K \), but also to \( N \), since \( N \trianglelefteq G \), thus, \( xax^{-1} \in N \cap K \).

(4) Let \( \psi : K \rightarrow KN/N \) be defined by stipulating \( \psi(k) := kN \). Then \( \psi \) is a surjective homomorphism and \( \ker(\psi) = \{k \in K : k \in N\} = N \cap K \).

Consider the following diagram:

\[ \begin{array}{ccc}
K & \xrightarrow{\psi} & KN/N \\
\downarrow{\pi} & & \downarrow{\varphi} \\
K/(N \cap K) & & \\
\end{array} \]

Since \( \psi \) is a surjective homomorphism, by Theorem 6.9, \( \varphi \) is an isomorphism. \( \dashv \)
For example, let $m$ and $n$ be two positive integers. Then $m\mathbb{Z}$ and $n\mathbb{Z}$ are normal subgroups of $\mathbb{Z}$, and by Theorem 6.10, $m\mathbb{Z}/(m\mathbb{Z}\cap n\mathbb{Z})$ and $(m\mathbb{Z} + n\mathbb{Z})/n\mathbb{Z}$ are isomorphic. In particular, for $m = 6$ and $n = 9$ we have $m\mathbb{Z} \cap n\mathbb{Z} = 18\mathbb{Z}$ and $m\mathbb{Z} + n\mathbb{Z} = 3\mathbb{Z}$. Thus, $6\mathbb{Z}/18\mathbb{Z}$ and $3\mathbb{Z}/9\mathbb{Z}$ are isomorphic, in fact, both groups are isomorphic to $C_3$.

**Theorem 6.11 (Third Isomorphism Theorem).** Let $K \trianglelefteq G$, $N \trianglelefteq G$, and $N \trianglelefteq K$. Then $K/N \trianglelefteq G/N$ and

$$
\varphi : \frac{G}{K} \rightarrow \frac{G/N}{K/N},
$$

$$
xK \mapsto (xN)(K/N)
$$

is an isomorphism.

**Proof.** First we show that $K/N \trianglelefteq G/N$. So, for any $x \in G$ and $k \in K$, we must have $(xN)(kN)(xN)^{-1} \in K/N$:

$$
(xN)(kN)(xN)^{-1} = xNkNx^{-1}N = xNkx^{-1}xNx^{-1}N = xNx^{-1} = xKx^{-1} = xNkx^{-1}N = Nk'N = k'NN = k'N \in K/N.
$$

Let

$$
\psi : G \rightarrow \frac{G/N}{K/N},
$$

$$
x \mapsto (xN)(K/N)
$$

Then $\psi$ is a surjective homomorphism and $\ker(\psi) = \{x \in G : xN \in K/N\} = K$.

Consider the following diagram:

$$
\begin{array}{ccc}
G & \xrightarrow{\psi} & \frac{G/N}{K/N} \\
\pi \downarrow & & \varphi \downarrow \\
G/K & &
\end{array}
$$

Since $\psi$ is a surjective homomorphism, by Theorem 6.9, $\varphi$ is an isomorphism. \hfill \dashrightarrow

For example, let $m$ and $n$ be two positive integers such that $m \mid n$. Then $m\mathbb{Z}$ and $n\mathbb{Z}$ are normal subgroups of $\mathbb{Z}$, $n\mathbb{Z} \trianglelefteq m\mathbb{Z}$, and by Theorem 6.11,

$$
\frac{\mathbb{Z}/m\mathbb{Z}}{\mathbb{Z}/n\mathbb{Z}} \cong \frac{\mathbb{Z}/m\mathbb{Z}}{m\mathbb{Z}/n\mathbb{Z}}.
$$

In particular, for $m = 6$ and $n = 18$,

$$
\mathbb{Z}_6 \cong \frac{\mathbb{Z}/18\mathbb{Z}}{6\mathbb{Z}/18\mathbb{Z}},
$$

and in fact, both groups are isomorphic to $C_6$. 