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 φ 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 $\mathrm{Aut}(G)$.

Before we show that $\mathrm{Aut}(G)$ 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 φ 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, $\varphi(e_G) = \varphi(xx^{-1}) = \varphi(x)\,\varphi(x^{-1}) = e_H$, which implies $\varphi(x^{-1}) = \varphi(x)^{-1}$. ⊣

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

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

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

⊣

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

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

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

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

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

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

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 ι on G is of course a bijective homomorphism from G to itself, and in fact, ι is the neutral element of $\big(\mathrm{Aut}(G), \circ\big)$.

(A2) Let $\varphi \in \mathrm{Aut}(G)$, and let φ^{-1} be such that for every $x \in G$, $\varphi\big(\varphi^{-1}(x)\big) = x$. It is obvious that $\varphi \circ \varphi^{-1} = \iota$ and it remains to show that φ^{-1} is a homomorphism: Since φ is a homomorphism, for all $x, y \in G$ we have

$$\varphi^{-1}(xy) = \varphi^{-1}\big(\underbrace{\varphi(\varphi^{-1}(x))}_{=x}\,\underbrace{\varphi(\varphi^{-1}(y))}_{=y}\big) = \varphi^{-1}\big(\varphi\big(\varphi^{-1}(x)\,\varphi^{-1}(y)\big)\big) = \varphi^{-1}(x)\,\varphi^{-1}(y)\,,$$

which shows that $\varphi^{-1} \in \mathrm{Aut}(G)$. ⊣

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

Theorem 6.4. Let $\varphi : G \to H$ be a homomorphism, then $\ker(\varphi) \trianglelefteq G$.

Proof. First we have to show that $\ker(\varphi) \leqslant G$: 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 $\ker(\varphi) \leqslant G$.
Now we show that $\ker(G) \trianglelefteq G$: Let $x \in G$ and $a \in \ker(\varphi)$, then

$$\varphi(xax^{-1}) = \varphi(x)\,\varphi(a)\,\varphi(x)^{-1} = \varphi(x)\,e_H\,\varphi(x)^{-1} = \varphi(x)\,\varphi(x)^{-1} = e_H\,,$$

thus, $xax^{-1} \in \ker(\varphi)$, which implies $\ker(\varphi) \trianglelefteq G$. ⊣

Let us give some examples of homomorphisms:

(1) The mapping

$$\begin{aligned} \varphi:\ (\mathbb{R},+) &\to (\mathbb{R}^+,\,\cdot\,) \\ x &\mapsto e^x \end{aligned}$$

is an isomorphism, and $\varphi^{-1} = \ln$.

(2) Let n be a positive integer. Then

$$\begin{aligned} \varphi:\ (\mathrm{O}(n),\,\cdot\,) &\to \big(\{1,-1\},\,\cdot\,\big) \\ A &\mapsto \det(A) \end{aligned}$$

is a surjective homomorphism and $\ker(\varphi) = \mathrm{SO}(n)$. Further, for $n = 1$, φ is even an isomorphism.

(3) The mapping

$$\begin{aligned} \varphi:\ \mathbb{R}^3 &\to \mathbb{R}^2 \\ (x,y,z) &\mapsto (x,z) \end{aligned}$$

is a surjective homomorphism and $\ker(\varphi) = \big\{(0,y,0) : y \in \mathbb{R}\big\}$.

(4) Let $n \geq 3$ be an integer, let $C_n = \{a^0, \ldots, a^{n-1}\}$, 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

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

then

$$\begin{array}{rccc} \varphi: & D_n & \to & \big(\{1,-1\},\,\cdot\,\big) \\ & x & \mapsto & \operatorname{sg}(x) \end{array}$$

is a surjective homomorphism.

(6) The mapping

$$\begin{array}{rccc} \varphi: & (\mathbb{Z}_{12},+) & \to & (\mathbb{Z}_{12},+) \\ & x & \mapsto & 4x \end{array}$$

is an endomorphism of $(\mathbb{Z}_{12},+)$, where $\ker(\varphi) = \{0,3,6,9\}$ and the image of φ is $\{0,4,8\}$.

(7) For every $r \in \mathbb{Q}^*$, the mapping

$$\begin{array}{rccc} \varphi: & (\mathbb{Q},+) & \to & (\mathbb{Q},+) \\ & q & \mapsto & rq \end{array}$$

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, $\operatorname{Aut}(C_2 \times C_2)$ 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

$$(xN)\,(yN) = \big(x(\underbrace{yNy^{-1}}_{=N})\big)(yN) = (xy)(NN) = (xy)N\,.$$

⊣

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 $(xN)\,(yN)$ is well-defined: If $(xN) = (\tilde{x}N)$ and $(yN) = (\tilde{y}N)$, 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,

$$(xy)^{-1}(\tilde{x}\tilde{y}) = y^{-1}\,(\underbrace{x^{-1}\tilde{x}}_{\in N})\,\tilde{y} \;\in\; y^{-1}N\tilde{y} = \underbrace{y^{-1}N(y}_{=N}\,y^{-1})\tilde{y} = N(y^{-1}\tilde{y}) = N\,,$$

which implies $(xN)\,(yN) = (xy)N = (\tilde{x}\tilde{y})N = (\tilde{x}N)\,(\tilde{y}N)$.
Now, let us show that G/N is a group:

(A0) $(xN)\big((yN)\,(zN)\big) = \big(x(yz)\big)N = \big((xy)z\big)N = \big((xN)\,(yN)\big)(zN)$.

(A1) For all $x \in G$ we have

$$(eN)\,(xN) = (ex)N = xN\,,$$

therefore, $eN = N$ is the neutral element of G/N.

(A2) For all $x \in G$ we have

$$(xN)\,(x^{-1}N) = (xx^{-1})N = eN = N = (x^{-1}x)N = (x^{-1}N)\,(xN)\,,$$

therefore, $(xN)^{-1} = (x^{-1}N)$. ⊣

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

$$\begin{array}{rccc} \pi: & G & \to & G/N \\ & x & \mapsto & xN \end{array}$$

is a surjective homomorphism, called the natural homomorphism from G onto G/N, and $\ker(\pi) = N$.

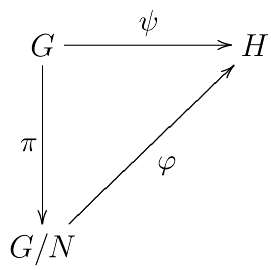
Proof. For all $x, y \in G$ we have $\pi(xy) = (xy)N = (xN)\,(yN) = \pi(x)\,\pi(y)$, thus, π is a homomorphism. Further, let $xN \in G/N$, then $\pi(x) = xN$, which shows that π is surjective. Finally, by Lemma 3.6 (c), $\ker(\pi) = \{x \in G : xN = N\} = N$. ⊣

By Theorem 6.4 we know that if $\varphi : G \to H$ 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 $\varphi : G \to H$ such that $N = \ker(\varphi)$.

Proof. Let $H = G/N$ and let φ be the natural homomorphism from G onto H. ⊣

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



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 φ is well-defined, a bijective homomorphism and unique.

φ 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 ψ is a homomorphism we have $e_H = \psi(x^{-1}y) = \psi(x)^{-1}\,\psi(y)$, which implies $\psi(x) = \psi(y)$. Therefore, $\varphi(xN) = \psi(x) = \psi(y) = \varphi(yN)$.

φ is a homomorphism: Let $xN, yN \in G/N$, then

$$\varphi\big((xN)(yN)\big) = \varphi\big((xy)N\big) = \psi(xy) = \psi(x)\,\psi(y) = \varphi(xN)\,\varphi(yN)\,.$$

φ is injective:

$$\begin{aligned} \varphi(xN) = \varphi(yN) \iff \psi(x) = \psi(y) \iff \\ \iff e_H = \psi(x)^{-1}\,\psi(y) = \psi(x^{-1})\,\psi(y) = \psi(x^{-1}y) \iff \\ \iff x^{-1}y \in N \iff xN = yN\,. \end{aligned}$$

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

φ is unique: Assume towards a contradiction that there exists an isomorphism $\tilde{\varphi} : G/N \to H$ different from φ 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

$$\psi(x) = (\tilde{\varphi} \circ \pi)(x) = \tilde{\varphi}\big(\pi(x)\big) = \tilde{\varphi}(xN) \neq \varphi(xN) = \varphi\big(\pi(x)\big) = (\varphi \circ \pi)(x) = \psi(x)\,,$$

a contradiction. ⊣

For example, let m be a positive integer and let $C_m = \{a^0, \dots, a^{m-1}\}$ be the cyclic group of order m. Further, let $\psi : \mathbb{Z} \to C_m$, where $\psi(k) := a^k$. Then ψ 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

$$\begin{aligned} \psi : \ (\mathrm{O}(n), \cdot\,) &\to \big(\{1, -1\}, \cdot\,\big) \\ A &\mapsto \det(A) \end{aligned}$$

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

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

$$\begin{aligned} \psi : \ (\mathrm{GL}(n)^+, \cdot\,) &\to (\mathbb{R}^+, \cdot\,) \\ A &\mapsto \det(A) \end{aligned}$$

is a surjective homomorphism with $\ker(\psi) = \mathrm{SL}(n)$, and thus, $\mathrm{GL}(n)^+/\,\mathrm{SL}(n)$ and $\mathbb{R}^+$ are isomorphic.

(3) The mapping

$$\begin{array}{rcl} \psi: \; (\mathbb{C}^*, \cdot\,) & \to & (\mathbb{R}^+, \cdot\,) \\ z & \mapsto & |z| \end{array}$$

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

$$\begin{array}{rcl} \psi: \quad \mathbb{R}^3 & \to & \mathbb{R}^2 \\ (x, y, z) & \mapsto & (x, z) \end{array}$$

is a surjective homomorphism with $\ker(\psi) = \big\{(0, y, 0) : y \in \mathbb{R}\big\} \cong \mathbb{R}$, and thus, $\mathbb{R}^3/\mathbb{R}$ and $\mathbb{R}^2$ are isomorphic.

(5) The mapping

$$\begin{array}{rcl} \psi: \; (\mathbb{Z}_{12}, +) & \to & (\mathbb{Z}_3, +) \\ x & \mapsto & x \pmod 3 \end{array}$$

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 $K \leqslant G$. Then

(1) $KN = NK \leqslant G$.
(2) $N \trianglelefteq KN$.
(3) $(N \cap K) \trianglelefteq K$.
(4) The mapping

$$\begin{array}{rcl} \varphi: \; K/(N \cap K) & \to & KN/N \\ x(N \cap K) & \mapsto & xN \end{array}$$

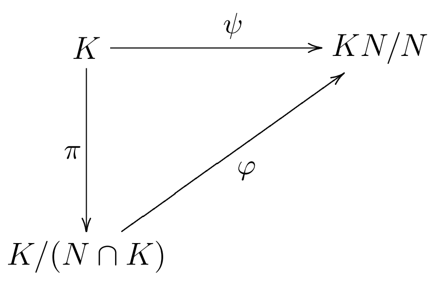
is an isomorphism.

Proof. (1) This is Theorem 5.8.

(2) Since $KN \leqslant G$ and $N \subseteq KN$, $N \leqslant KN$. 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 $\psi : K \to KN/N$ be defined by stipulating $\psi(k) := kN$. Then ψ is a surjective homomorphism and $\ker(\psi) = \{k \in K : k \in N\} = N \cap K$.
Consider the following diagram:



Since ψ is a surjective homomorphism, by Theorem 6.9, φ is an isomorphism. ⊣

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

$$\begin{array}{rccc} \varphi: & G/K & \to & G/N \big/ K/N \\ & xK & \mapsto & (xN)(K/N) \end{array}$$

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 $(xN)(kN)(xN)^{-1} \in K/N$:

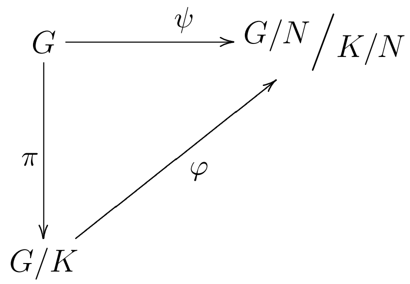
$$(xN)(kN)(xN)^{-1} = xNkNx^{-1}N = xNkx^{-1}\underbrace{xNx^{-1}}_{=N}N =$$

$$= xNkx^{-1}N = \underbrace{xNx^{-1}}_{=N}\underbrace{xkx^{-1}}_{=:k'\in K}N = Nk'N = k'NN = k'N \in K/N\,.$$

Let

$$\begin{array}{rccc} \psi: & G & \to & G/N \big/ K/N \\ & x & \mapsto & (xN)(K/N) \end{array}$$

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



Since ψ is a surjective homomorphism, by Theorem 6.9, φ is an isomorphism. ⊣

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,

$$\mathbb{Z}/m\mathbb{Z} \;\cong\; \mathbb{Z}/n\mathbb{Z}\big/ m\mathbb{Z}/n\mathbb{Z}\,.$$

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

$$\mathbb{Z}_6 \;\cong\; \mathbb{Z}_{18}\big/ 6\mathbb{Z}/18\mathbb{Z}\,,$$

and in fact, both groups are isomorphic to C_6.