Course 3: 08.03.2021

1.5 Group homomorphisms

Let us now define some special maps between groups. We denote by the same symbol operations in different arbitrary structures.

Definition 1.5.1 Let $(G,\cdot)$ and $(G',\cdot)$ be groups and let $f : G \to G'$. Then f is called a *(group) homomorphism* if

$$f(x \cdot y) = f(x) \cdot f(y), \quad \forall x, y \in G.$$

A group homomorphism $f : G \to G'$ is called *isomorphism* if it is bijective, *endomorphism* if $(G,\cdot) = (G',\cdot)$ and *automorphism* if it is bijective and $(G,\cdot) = (G',\cdot)$.

The sets of endomorphisms and automorphisms of a group G are denoted by $\mathrm{End}(G)$ and $\mathrm{Aut}(G)$ respectively.

We denote by $G \simeq G'$ or $G \cong G'$ the fact that two groups G and G' are isomorphic. Usually, we denote by 1 and $1'$ the identity elements in G and G' respectively.

Example 1.5.2 (a) Let $(G,\cdot)$ and $(G',\cdot)$ be groups and let $f : G \to G'$ be defined by $f(x) = 1'$, $\forall x \in G$. Then f is a homomorphism, called the *trivial homomorphism*.

(b) Let $(G,\cdot)$ be a group. Then the identity map $1_G : G \to G$ is an automorphism of G.

(c) Let $(G,\cdot)$ be a group and let $H \leq G$. Define $i : H \to G$ by $i(x) = x$, $\forall x \in H$. Then i is a homomorphism, called the *inclusion homomorphism*.

(d) Let $a \in \mathbb{Z}$ and let $t_a : \mathbb{Z} \to \mathbb{Z}$ be defined by $t_a(x) = ax$. Then t_a is a group homomorphism from the group $(\mathbb{Z},+)$ to itself.

(e) Let $n \in \mathbb{N}$ with $n \geq 2$. The map $f : \mathbb{Z} \to \mathbb{Z}_n$ defined by $f(x) = \widehat{x}$ is a group homomorphism between the groups $(\mathbb{Z},+)$ and $(\mathbb{Z}_n,+)$.

(f) Let $f : \mathbb{C}^* \to \mathbb{R}^*$ be defined by $f(z) = |z|$. Then f is a group homomorphism between $(\mathbb{C}^*,\cdot)$ and $(\mathbb{R}^*,\cdot)$. But $f : \mathbb{C} \to \mathbb{R}$ defined by $f(z) = |z|$ is not a group homomorphism between the groups $(\mathbb{C},+)$ and $(\mathbb{R},+)$.

(g) Let $n \in \mathbb{N}$, $n \geq 2$ and let $f : GL_n(\mathbb{R}) \to \mathbb{R}^*$ be defined by $f(A) = \det(A)$. Then f is a group homomorphism between the groups $(GL_n(\mathbb{R}),\cdot)$ and $(\mathbb{R}^*,\cdot)$.

(h) Let $(G,\cdot)$ be a group and $g \in G$. Let $i_g : G \to G$ be defined by

$$i_g(x) = g^{-1}xg.$$

Then i_g is an automorphism of $(G,\cdot)$, called the *inner automorphism* defined by g. The element $g^{-1}xg$ is called the *conjugate* of x by g.

Theorem 1.5.3 *(i) Let $f : G \to G'$ be a group isomorphism. Then $f^{-1} : G' \to G$ is again a group isomorphism.*

(ii) Let $f : G \to G'$ and $g : G' \to G''$ be group homomorphisms. Then $g \circ f : G \to G''$ is a group homomorphism.

Proof. (i) Clearly, f^{-1} is bijective. Now let $x', y' \in G'$. By the surjectivity of f, $\exists x, y \in G$ such that $f(x) = x'$ and $f(y) = y'$. Since f is a homomorphism, it follows that

$$f^{-1}(x' \cdot y') = f^{-1}(f(x) \cdot f(y)) = f^{-1}(f(x \cdot y)) = x \cdot y = f^{-1}(x') \cdot f^{-1}(y').$$

Therefore, f^{-1} is an isomorphism.

(ii) Let $x, y \in G$. We have:

$$(g \circ f)(x \cdot y) = (g(f(x \cdot y)) = g(f(x) \cdot f(y)) = g(f(x)) \cdot g(f(y)) = (g \circ f)(x) \cdot (g \circ f)(y)).$$

This shows that $g \circ f$ is a group homomorphism. □

Corollary 1.5.4 *Let $(G,\cdot)$ be a group. Then $(\mathrm{End}(G),\circ)$ is a monoid and its group of invertible elements is*

$$U(\mathrm{End}(G),\circ)=\mathrm{Aut}(G).$$

Theorem 1.5.5 *Let $f:G\to G'$ be a group homomorphism. Then:*
(i) $f(1)=1'$;
(ii) $(f(x))^{-1}=f(x^{-1})$, $\forall x\in G$.

Proof. (i) We have $\forall x\in G$, $1\cdot x=x\cdot 1=x$, so that $f(1\cdot x)=f(x\cdot 1)=f(x)$. Since f is a homomorphism, it follows that

$$f(1)\cdot f(x)=f(x)\cdot f(1)=f(x)\,,$$

whence we get $f(1)=1'$ by multiplying by $(f(x))^{-1}$.

(ii) Let $x\in G$. Since $x\cdot x^{-1}=x^{-1}\cdot x=1$, f is a homomorphism and $f(1)=1'$, it follows that

$$f(x)\cdot f(x^{-1})=f(x^{-1})\cdot f(x)=1'\,.$$

Hence $(f(x))^{-1}=f(x^{-1})$. □

Let us now define two important sets related to a group homomorphism, that will be even subgroups.

Definition 1.5.6 Let $f:G\to G'$ be a group homomorphism. Then the set

$$\mathrm{Ker}f=\{x\in G\mid f(x)=1'\}$$

is called the *kernel* of the homomorphism f and the set

$$\mathrm{Im}f=\{f(x)\mid x\in G\}$$

is called the *image* of the homomorphism f.

Theorem 1.5.7 *Let $f:G\to G'$ be a group homomorphism. Then*

$$\mathrm{Ker}f\leq G \text{ and } \mathrm{Im}f\leq G'\,.$$

Proof. Since $f(1)=1'$, we have $1\in\mathrm{Ker}f\neq\emptyset$. Now let $x,y\in\mathrm{Ker}f$. Then $f(x)=f(y)=1'$. It follows that

$$f(xy^{-1})=f(x)f(y^{-1})=f(x)(f(y))^{-1}=1'\cdot 1'=1'\,,$$

hence $xy^{-1}\in\mathrm{Ker}f$. Therefore, $\mathrm{Ker}f\leq G$.

Since $1'=f(1)$, we have $1'\in\mathrm{Im}f\neq\emptyset$. Now let $x',y'\in\mathrm{Im}f$. Then $\exists x,y\in G$ such that $f(x)=x'$ and $f(y)=y'$. It follows that

$$x'y'^{-1}=f(x)(f(y))^{-1}=f(x)f(y^{-1})=f(xy^{-1})\in\mathrm{Im}f\,,$$

hence $x'y'^{-1}\in\mathrm{Im}f$. Therefore, $\mathrm{Im}f\leq G'$. □

More generally, we have the following property.

Theorem 1.5.8 *Let $f:G\to G'$ be a group homomorphism and let H be a subgroup of G. Then*

$$f(H)=\{f(x)\mid x\in H\}$$

is a subgroup of G'.

Proof. Since H is a subgroup of G, we have $H\neq\emptyset$, and thus $f(H)\neq\emptyset$. Now let $x',y'\in f(H)$. Then $x'=f(x)$ and $y'=f(y)$ for some $x,y\in H$. It follows that

$$x'y'^{-1}=f(x)(f(y))^{-1}=f(x)f(y^{-1})=f(xy^{-1})\in f(H),$$

hence $x'y'^{-1}\in f(H)$. Therefore, $f(H)\leq G'$. □

It is well-known that a group homomorphism (and even a function) $f:G\to G'$ is surjective if and only if $\mathrm{Im}f=G'$. We have a similar characterization of injective group homomorphisms by their kernel.

Theorem 1.5.9 *Let $f : G \to G'$ be a group homomorphism. Then*

$$\mathrm{Ker} f = \{1\} \Longleftrightarrow f \text{ is injective}.$$

Proof. $\Longrightarrow$. Suppose that $\mathrm{Ker} f = \{1\}$. Let $x, y \in G$ be such that $f(x) = f(y)$. Then

$$f(x)(f(y))^{-1} = 1',$$

whence it follows that $f(xy^{-1}) = 1'$, that is, $xy^{-1} \in \mathrm{Ker} f = \{1\}$. Hence $x = y$. Therefore, f is injective.

$\Longleftarrow$. Suppose that f is injective. Clearly, $\{1\} \subseteq \mathrm{Ker} f$. Now let $x \in \mathrm{Ker} f$. Then

$$f(x) = 1' = f(1),$$

whence $x = 1$. Hence $\mathrm{Ker} f \subseteq \{1\}$, so that $\mathrm{Ker} f = \{1\}$. □

Theorem 1.5.10 (Factorization by an injective group homomorphism) *Let $f : A \to B$ be a group homomorphism. Let $g : B' \to B$ be an injective group homomorphism with $\mathrm{Im}(f) \subseteq \mathrm{Im}(g)$. Then there exists a unique group homomorphism $h : A \to B'$ such that $f = g \circ h$.*

Proof. Let $a \in A$. Then $f(a) \in \mathrm{Im}(f) \subseteq \mathrm{Im}(g)$, hence there exists $b' \in B'$ such that $f(a) = g(b')$. If there exists $b'' \in B'$ such that $f(a) = g(b'')$, then we have $g(b') = g(b'')$, hence $b' = b''$ because g is injective. Hence for every $a \in A$, there exists a unique $b' \in B'$ such that $f(a) = g(b')$.

It follows that we can define the function

$$h : A \to B', \quad h(a) = b',$$

where $b' \in B'$ is uniquely determined as above. We have $g(h(a)) = g(b') = f(a)$ for every $a \in A$. Hence $f = g \circ h$.

We show that h is a group homomorphism. Let $a_1, a_2 \in A$. Then there exist $b'_1, b'_2 \in B'$ unique such that $f(a_1) = g(b'_1)$ and $f(a_2) = g(b'_2)$. Hence $h(a_1) = b'_1$ and $h(a_2) = b'_2$. We have

$$f(a_1 + a_2) = f(a_1) + f(a_2) = g(b'_1) + g(b'_2) = g(b'_1 + b'_2).$$

It follows that

$$h(a_1 + a_2) = b'_1 + b'_2 = h(a_1) + h(a_2).$$

Thus h is a group homomorphism.

For uniqueness, suppose that there exists a homomorphism $h' : A \to B'$ such that $f = g \circ h'$. It follows that $g \circ h = g \circ h'$. For every $a \in A$, we have $g(h(a)) = g(h'(a))$, whence $h(a) = h'(a)$ by the injectivity of g. Hence $h = h'$. □

Theorem 1.5.11 (Factorization by a surjective group homomorphism) *Let $f : A \to B$ be a group homomorphism. Let $g : A \to A'$ be a surjective group homomorphism with $\mathrm{Ker}(g) \subseteq \mathrm{Ker}(f)$. Then there exists a unique group homomorphism $h : A' \to B$ such that $f = h \circ g$.*

Proof. Let $a' \in A'$. Since g is surjective, there exists $a \in A$ such that $g(a) = a'$. If there exists $a_0 \in A$ such that $g(a_0) = a'$, then we have $g(a) = g(a_0)$. It follows that $g(a - a_0) = 0$, hence $a - a_0 \in \mathrm{Ker}(g) \subseteq \mathrm{Ker}(f)$. Then $f(a - a_0) = 0$, hence $f(a) = f(a_0)$.

It follows that we can define the function

$$h : A' \to B, \quad h(a') = f(a),$$

where $f(a)$ is uniquely determined as above. We have $h(g(a)) = a$ for every $a \in A$. Hence $f = h \circ g$.

We show that h is a group homomorphism. Let $a'_1, a'_2 \in A'$. Then there exist $a_1, a_2 \in A$ such that $g(a_1) = a'_1$ and $g(a_2) = a'_2$. Hence $h(a'_1) = f(a_1)$ and $h(a'_2) = f(a_2)$. We have

$$g(a_1 + a_2) = g(a_1) + g(a_2) = a'_1 + a'_2.$$

It follows that

$$h(a'_1 + a'_2) = h(g(a_1 + a_2)) = f(a_1 + a_2) = f(a_1) + f(a_2) = h(a'_1) + h(a'_2).$$

Thus h is a group homomorphism.

For uniqueness, suppose that there exists a group homomorphism $h' : A' \to B$ such that $f = h' \circ g$. It follows that $h \circ g = h' \circ g$. For every $a' \in A'$, there is $a \in A$ such that $g(a) = a'$ by the surjectivity of g, which implies that $h(a') = h(g(a)) = h'(g(a)) = h'(a')$. Hence $h = h'$. □

Theorem 1.5.12 *Let $f : G \to G'$ be a group homomorphism and let $X \subseteq G$. Then*

$$f(< X >) =< f(X) > .$$

Proof. If $X = \emptyset$, then $f(< \emptyset >) = f(\{1\}) = \{f(1)\} = \{1'\} =< f(\emptyset) >$.

Now assume that $X \neq \emptyset$. We have seen that

$$< X >= \{x_1 x_2 \dots x_n \mid x_i \in X \cup X^{-1}, i = 1, \dots, n, n \in \mathbb{N}^*\}.$$

Since f is a group homomorphism, it follows that

$$f(< X >) = f(\{x_1 \dots x_n \mid x_i \in X \cup X^{-1}, i = 1, \dots, n, n \in \mathbb{N}^*\}) =$$

$$= \{f(x_1 \dots x_n) \mid x_i \in X \cup X^{-1}, i = 1, \dots, n, n \in \mathbb{N}^*\} =$$

$$= \{f(x_1) \dots f(x_n) \mid x_i \in X \cup X^{-1}, i = 1, \dots, n, n \in \mathbb{N}^*\} =< f(X) >,$$

which proves the theorem. □

Corollary 1.5.13 *Let $f : G \to G'$ be a group homomorphism and let $x \in G$. Then*

$$f(< x >) = \{f(x)^k \mid k \in \mathbb{Z}\}.$$

Proof. Recall that we have $< x >= \{x^k \mid k \in \mathbb{Z}\}$. By Theorem 1.5.12, it follows that

$$f(< x >) =< f(x) >= \{f(x)^k \mid k \in \mathbb{Z}\}),$$

as required. □