Course 3

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 $f : G \to G'$ be a function. 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 $(G,\cdot) = (G',\cdot)$;
- *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 $t_a(x) = a \cdot x$. 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 $(\mathbb{Z}_n, +)$. The map $f : \mathbb{Z} \to n\mathbb{Z}$ defined by $f(x) = nx$ is a group isomorphism between the groups $(\mathbb{Z}, +)$ and $(n\mathbb{Z}, +)$.

(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

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

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

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

(ii) Let $(G,\cdot)$, $(G',\cdot)$ and $(G'',\cdot)$ be groups, and 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* $(G, \cdot)$ *and* $(G', \cdot)$ *be groups, and 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 $(G, \cdot)$ and $(G', \cdot)$ be groups, and 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* $(G, \cdot)$ *and* $(G', \cdot)$ *be groups, and 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

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

hence $x \cdot y^{-1} \in \mathrm{Ker}f$. 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

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

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

More generally, we have the following property.

Theorem 1.5.8 *Let $(G, \cdot)$ and $(G', \cdot)$ be groups, and 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

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

because $x \cdot y^{-1} \in H$. Hence $x' \cdot y'^{-1} \in f(H)$. 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 $(G, \cdot)$ and $(G', \cdot)$ be groups, and 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 we have:

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

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

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

Proof. If $X = \emptyset$, then we have:

$$f(< \emptyset >) = f(\{1\}) = \{f(1)\} = \{1'\} = < f(\emptyset) > .$$

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

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

Since f is a group homomorphism, it follows that

$$\begin{aligned} f(< X >) &= f(\{x_1 \cdot x_2 \cdot \ldots \cdot x_n \mid x_i \in X \cup X^{-1}, i = 1, \ldots, n, n \in \mathbb{N}^*\}) \\ &= \{f(x_1 \cdot x_2 \cdot \ldots \cdot x_n) \mid x_i \in X \cup X^{-1}, i = 1, \ldots, n, n \in \mathbb{N}^*\} \\ &= \{f(x_1) \cdot f(x_2) \cdot \ldots \cdot f(x_n) \mid x_i \in X \cup X^{-1}, i = 1, \ldots, n, n \in \mathbb{N}^*\} \\ &= < f(X) >, \end{aligned}$$

which proves the theorem. □

Corollary 1.5.11 *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 1.5.10, it follows that

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

as required. □

Example 1.5.12 Let us show that

$$\mathrm{End}(\mathbb{Z},+)=\{t_a \mid a\in\mathbb{Z}\},$$

$$\mathrm{Aut}(\mathbb{Z},+)=\{t_1,t_{-1}\},$$

where $\forall a\in\mathbb{Z}$, $t_a:\mathbb{Z}\to\mathbb{Z}$ is defined by $t_a(n)=a\cdot n$.

We show the first equality by double inclusion.

First, let $f\in\mathrm{End}(\mathbb{Z},+)$. For every $n\in\mathbb{N}^*$, we have:

$$f(n)=f(\underbrace{1+\cdots+1}_{n\text{ times}})=\underbrace{f(1)+\cdots+f(1)}_{n\text{ times}})=f(1)\cdot n,$$

$$f(-n)=-f(n)=-f(1)\cdot n=f(1)\cdot(-n).$$

Also, we have $f(0)=f(1)\cdot 0$. Hence for every $n\in\mathbb{Z}$, we have $f(n)=f(1)\cdot n=t_{f(1)}(n)$. Thus $f=t_{f(1)}\in\{t_a\mid a\in\mathbb{Z}\}$.

Now let $a\in\mathbb{Z}$. For every $m,n\in\mathbb{Z}$, we have:

$$t_a(m+n)=a(m+n)=am+an=t_a(m)+t_a(n).$$

Hence $t_a\in\mathrm{End}(\mathbb{Z},+)$

In view of the second equality, note that $\mathrm{Aut}(\mathbb{Z},+)$ consists of the bijective endomorphisms of $(\mathbb{Z},+)$. Now let $a\in\mathbb{Z}$ be such that $t_a\in\mathrm{Aut}(\mathbb{Z},+)$. By the surjectivity of t_a, there is $b\in\mathbb{Z}$ such that $t_a(b)=1$, that is, $ab=1$. But this implies that $a\in\{-1,1\}$. Note that $t_1=1_{\mathbb{Z}}$ and $t_{-1}(n)=-n$ for every $n\in\mathbb{Z}$. Finally, it is easy to see that $t_1,t_{-1}\in\mathrm{Aut}(\mathbb{Z},+)$.

Example 1.5.13 (a) Let us show that the groups $(\mathbb{Z}_4,+)$ and $(\mathbb{Z}_5^*,\cdot)$ are isomorphic.

Consider $f:\mathbb{Z}_4\to\mathbb{Z}_5^*$ defined by $f(\hat{x})=2^x \bmod 5$. Note first that f is a well-defined function. Indeed, if $\hat{x}=\hat{y}$, then $x-y=4k$ for some $k\in\mathbb{Z}$, whence $2^x\equiv 2^{y+4k}\equiv 2^y\cdot 2^{4k}\equiv 2^y \pmod 5$.

One shows that f is a group isomorphism. Note that $g:\mathbb{Z}_4\to\mathbb{Z}_5^*$ defined by $f(\hat{x})=4^x \bmod 5$ is a group homomorphism, but not an isomorphism.

(b) Let us show that the groups $(\mathbb{Z},+)$ and $(\mathbb{Q},+)$ are not isomorphic.

If there is a group isomorphism $f:\mathbb{Q}\to\mathbb{Z}$ between them, then there is $r\in\mathbb{Q}$ such that $f(r)=1$. But then we have:

$$1=f(r)=f\left(\frac{r}{2}+\frac{r}{2}\right)=f\left(\frac{r}{2}\right)+f\left(\frac{r}{2}\right)=2f\left(\frac{r}{2}\right),$$

whence $f(\frac{r}{2})=\frac{1}{2}\notin\mathbb{Z}$, a contradiction.