Definition 11.1

Let G, H be groups. A group homomorphism is a function

$$f\colon G \to H$$

which for any $a, b \in G$ satisfies $f(a \cdot b) = f(a) \cdot f(b)$

Theorem 11.2

Let $f\colon G \to H$ be a groups homomorphism. Then:

- $f(e_G) = e_H$ where e_G and e_H are the identity elements in G and H, respectively.
- $f(a^{-1}) = f(a)^{-1}$ for any $a \in G$.

Proof. 1) We have

$$f(e_G) = f(e_G \cdot e_G) = f(e_G) \cdot f(e_G)$$

This gives:

$$e_H = f(e_G) \cdot f(e_G)^{-1} = (f(e_G) \cdot f(e_G)) \cdot f(e_G)^{-1} = f(e_G)$$

2) We have

$$e_H = f(e_G) = f(a \cdot a^{-1}) = f(a) \cdot f(a^{-1})$$

which gives:

$$f(a)^{-1} = f(a)^{-1} \cdot e_H = f(a)^{-1} \cdot (f(a) \cdot f(a^{-1})) = f(a^{-1})$$

$\square$

Example. For $n \geq 2$ take the function $f\colon \mathbb{Z} \to \mathbb{Z}_n$ given by $f(k) = k \mod n$. Then f is a group homomorphism.

Example. Recall that for $n \geq 1$, the general linear group $GL(n, \mathbb{R})$ is a group that consists of $n \times n$ invertible matrices with matrix multiplication as the group operation. Recall also that $\mathbb{R}^*$ is the group of non-zero real numbers with multiplication. For an invertible matrix A its determinant is a non-zero number $\det A$. Moreover, $\det AB = (\det A) \cdot (\det B)$. This means that the determinant defines a homomorphism of groups

$$\det\colon GL(n, \mathbb{R}) \to \mathbb{R}^*$$

Example. Let S_n be the symmetric group on n letters and let $\text{sign}\colon S_n \to \mathbb{Z}_2$ be defined by

$$\text{sign}(\alpha) = \begin{cases} 0 & \text{is } \alpha \text{ is an even permutation} \\ 1 & \text{is } \alpha \text{ is an odd permutation} \end{cases}$$

This gives a homomorphism of groups.

Example. For a group G, consider the function $f\colon G \to G$ given by $f(a) = a^{-1}$. In general this function is not a homomorphism. For example, take $G = S_3$, the symmetric group on 3 letters, let $\alpha, \beta \in S_3$ be given by $\alpha = (1, 2)$, $\beta = (2, 3)$. Then we have:

$$f(\alpha \circ \beta) = ((1, 2) \circ (2, 3))^{-1} = (2, 3)^{-1} \circ (1, 2)^{-1} = (2, 3) \circ (1, 2) = (1, 3, 2)$$
$$f(\alpha) \circ f(\beta) = (1, 2)^{-1} \circ (2, 3)^{-1} = (1, 2) \circ (2, 3) = (1, 2, 3)$$

and so $f(\alpha \circ \beta) \neq f(\alpha) \circ f(\beta)$

On the other hand, if G is an abelian group then for any $a, b \in G$ we get

$$f(ab) = (ab)^{-1} = b^{-1}a^{-1} = a^{-1}b^{-1} = f(a)f(b)$$

Thus for an abelian group $f(a) = a^{-1}$ defines a homomorphism.

Example. Recall that by $\mathbb{R}$ we denote the group of all real numbers with addition and by $\mathbb{R}^*$ the group of non-zero real numbers with multiplication. Define $g\colon \mathbb{R} \to \mathbb{R}^*$ by $g(a) = 2^a$. For $a, b \in \mathbb{R}$ we have

$$g(a + b) = 2^{a+b} = 2^a \cdot 2^b = g(a) \cdot g(b)$$

This means that g is a homomorphism of groups.

Example. For any group G and an element $a \in G$ there is exactly one homomorphism $f\colon \mathbb{Z} \to G$ such that $f(1) = a$. This homomorphism if given by $f(m) = a^m$.

Example. For any group G the identity function $\text{id}_G\colon G \to G$, given by $\text{id}_G(a) = a$ for all $a \in G$ is a homomorphism.

Theorem 11.3

Let $f\colon G \to H$ be a homomorphism of groups and let $a \in G$. If $|a| < \infty$ then $|f(a)|$ divides $|a|$.

Proof. If $|a| = n$ then
$$f(a)^n = f(a^n) = f(e_G) = e_H$$
This means that $|f(a)|$ divides n (see Theorem 6.3). □

Example. Let G be a group and let $a \in G$ be an element such that $|a| = n$. Then for each $k = 1, 2, \dots$ there is exactly one homomorphism $f\colon \mathbb{Z}_{kn} \to G$ such that $f(1) = a$. This homomorphism is given by $f(m) = a^m$.

Definition 11.4

Let $f\colon G \to H$ be a group homomorphism. The *kernel of f* is the subset of G defined by
$$\mathrm{Ker}(f) = \{g \in G \mid f(g) = e\}$$
The *image of f* is the subset of H given by
$$\mathrm{Im}(f) = \{f(g) \mid g \in G\}$$

Theorem 11.5

If $f\colon G \to H$ is a homomorphism of groups then $\mathrm{Ker}(f)$ is a subgroup of G and $\mathrm{Im}(f)$ is a subgroup of H.

Proof. Exercise. □

Example. Let $f\colon \mathbb{Z} \to \mathbb{Z}_n$, $f(k) = (k \mod n)$. Then $\mathrm{Im}(f) = \mathbb{Z}_n$ and $\mathrm{Ker}(f) = \{nq \mid q \in \mathbb{Z}\}$. This subgroup of $\mathbb{Z}$ is often denoted by $n\mathbb{Z}$.

Example. Take the determinant homomorphism $\det\colon GL(n, R) \to \mathbb{R}^*$. Then $\mathrm{Im}(\det) = \mathbb{R}^*$. Also, $\mathrm{Ker}(\det) = \{A \in GL(n, \mathbb{R}) \mid \det A = 1\}$ This group is called the *special linear group* and it is denoted by $SL(n, \mathbb{R})$.

Example. For the homomorphism $\mathrm{sign}\colon S_n \to \mathbb{Z}_2$ we have $\mathrm{Im}(\mathrm{sign}) = \mathbb{Z}_2$ and $\mathrm{Ker}(\mathrm{sign}) = A_n$, where A_n is the alternating group.

Example. Let G be an abelian group and let $f\colon G \to G$ be given by $f(a) = a^{-1}$. Then $\mathrm{Im}(f) = G$ and $\mathrm{Ker}(f) = \{e\}$.

Example. Let $g\colon \mathbb{R} \to \mathbb{R}^*$, $g(a) = 2^a$. Then $\mathrm{Im}(g) = \mathbb{R}^+$ and $\mathrm{Ker}(g) = \{0\}$.

Theorem 11.6

If $f\colon G \to H$ is a homomorphism then $f(a) = f(b)$ if and only if $b = ak$ for some $k \in \mathrm{Ker}(f)$.

Proof. If $f(a) = f(b)$ then

$$e = f(a)^{-1}f(b) = f(a^{-1})f(b) = f(a^{-1}b)$$

so $a^{-1}b \in Ker(f)$. Taking $k = a^{-1}b$ we then get $ak = a(a^{-1}b) = b$. Conversely, if $k \in \mathrm{Ker}(f)$ then $f(ak) = f(a)f(k) = f(a)e = f(a)$. □

Corollary 11.7

A homomorphism of groups $f\colon G \to H$ is 1-1 if and only if $\mathrm{Ker}(f) = \{e\}$.

Corollary 11.8

If $f\colon G \to H$ is a homomorphism of groups, and $f(a) = b$ for some $a \in G$, $b \in H$ then

$$f^{-1}(b) = \{ak \mid k \in Ker(f)\ \}$$

Note. If G is a group and $H \subseteq G$ is a subgroup, then there exists a homomorphism

$$f\colon K \to G$$

such that $\mathrm{Im}(f) = H$ Indeed, we can take $f\colon H \to G$, $f(a) = a$.

We will show, however that, in general, not for every subgroup $H \subseteq G$ there is a homomorphism $f\colon G \to K$ such that $H = \mathrm{Ker}(f)$.

Theorem 11.9

Let $f\colon G \to H$ is a homomorphism of groups then $g \in \mathrm{Ker}(f)$ if and only if for each $a \in G$ we have $aga^{-1} \in \mathrm{Ker}(f)$.

Proof. Since $f(g) = e$ we obtain:

$$f(aga^{-1}) = f(a)f(g)f(a^{-1}) = f(a)ef(a)^{-1} = f(a)f(a)^{-1} = e$$

and so $gag^{-1} \in \mathrm{Ker}(f)$. □

Definition 11.10

Let G be a group. We say that a subgroup $H \subseteq G$ is a *normal subgroup* of G if for any $h \in H$ and $g \in G$ we have $ghg^{-1} \in H$.

We write $H \triangleleft G$ to denote that H is a normal subgroup of G.

Corollary 11.11

If $f\colon G \to H$ is a homomorphism of groups then $\mathrm{Ker}(f)$ is a normal subgroup of G.

Proof. This follows from Theorem 11.9. □

Example. G is an abelian group then any subgroup $H \subseteq G$ is normal since for $h \in H$ and $g \in G$ we have

$$ghg^{-1} = gg^{-1}h = h \in H$$

Example. Recall that the alternating group A_n is a subgroup of the symmetric group S_n consisting of all even permutations. This subgroup is normal, since if α is an even permutation and β is any permutation then $\beta \circ \alpha \circ \beta^{-1}$ is an even permutation.

Example. Consider the dihedral group D_4:

$\circ$	I	R_{90}	R_{180}	R_{270}	H	V	D	D'
I	I	R_{90}	R_{180}	R_{270}	H	V	D	D'
R_{90}	R_{90}	R_{180}	R_{270}	I	D'	D	H	V
R_{180}	R_{180}	R_{270}	I	R_{90}	V	H	D'	D
R_{270}	R_{270}	I	R_{90}	R_{180}	D	D'	V	H
H	H	D	V	D'	I	R_{180}	R_{90}	R_{270}
V	V	D'	H	D	R_{180}	I	R_{270}	R_{90}
D	D	H	D'	V	R_{270}	R_{90}	I	R_{180}
D'	D'	V	D	H	R_{90}	R_{270}	R_{180}	I

The set $\{I, V\}$ is a subgroup of D_4. However, this is not a normal subgroup since, for example, we have

$$DVD^{-1} = DVD = R_{90}D = H$$

and $H \notin \{I, V\}$.

Exercise. Check that the subgroup of rotations $G = \{I, R_{90}, R_{180}, R_{270}\}$ is a normal subgroup of D_4.

Note. We will see later that for any normal subgroup $H \triangleleft G$ there is a homomorphism $f\colon G \to K$ such that $\mathrm{Ker}(f) = H$.