Recall:

- A normal subgroup of a group G is a subgroup $H \subseteq G$ such that for every $a \in G$ and $h \in H$ we have $aha^{-1} \in H$.
- We write $H \lhd G$ to denote that H is a normal subgroup of G.
- If $f\colon G \to K$ is a group homomorphism, then $\mathrm{Ker}(f) \lhd G$.

Theorem 14.1

Let G be a group and let $H \subseteq G$ be a subgroup. Then the following conditions are equivalent:

1) $H \lhd G$

2) For any $a \in G$ we have $aHa^{-1} = H$ where $aHa^{-1} = \{aha^{-1} \mid h \in H\}$.

3) For any $a \in G$ we have $aH = Ha$.

Proof. 1) $\Rightarrow$ 2) Choose $a \in G$. By the definition of a normal subgroup, for every $b \in G$ we have $bHb^{-1} \subseteq H$, so in particular $aHa^{-1} \subseteq H$.

Moreover, taking $b = a^{-1}$ we get $a^{-1}Ha \subseteq H$. This gives:

$$H = eHe^{-1} = (aa^{-1})H(aa^{-1})^{-1} = a(a^{-1}Ha)a^{-1} \subseteq aHa^{-1}$$

Thus we obtain $aHa^{-1} = H$.

2) $\Rightarrow$ 3) Let $a \in G$ and $h \in H$. Since $aHa^{-1} = H$, thus $aha^{-1} = h'$ for some $h' \in H$ and so $ah = h'a \in Ha$. This gives $aH \subseteq Ha$. Similarly, since $a^{-1}Ha = H$, we get $a^{-1}ha = h'$ for some $h' \in H$ and so $ha = ah'$. This implies that $Ha \subseteq aH$.

3) $\Rightarrow$ 1) Let $a \in G$ and $h \in H$. Since $aH = Ha$, there is $h' \in H$ such that $ah = h'a$, or equivalently $aha^{-1} = h'$. Thus $aha^{-1} \in H$ for any $a \in G$ and $h \in H$, which shows that $H \lhd G$. $\square$

Theorem 14.2

Let G be a group and $H \triangleleft G$. Let $a_1, a_2, b_1, b_2 \in G$ be elements such that $a_1H = a_2H$ and $b_1H = b_2H$. Then $(a_1b_1)H = (a_2b_2)H$.

Note. Theorem 14.2 is not true if $H \subseteq G$ is a subgroup of G which is not normal. Take, for example, the dihedral group D_4 and let $K = \{I, H\} \subseteq D_4$. We have

$$R_{90}K = D'K \quad \text{and} \quad R_{270}K = DK$$

On the other hand

$$\begin{aligned}(R_{90} \cdot R_{270})K &= IK = \{I, H\} \\ (D' \cdot D)K &= R_{180}K = \{R_{180}, V\}\end{aligned}$$

Thus $(R_{90} \cdot R_{270})K \neq (D' \cdot D)K$.

Proof of Theorem 14.2. Since $a_1H = a_2H$, we have $a_1 = a_2h$ for some $h \in H$. Similarly, since $b_1H = b_2H$, thus $b_1 = b_2h'$ for some $h' \in H$. This gives $a_1b_1 = a_2hb_2h'$.

Since H is a normal subgroup, we have $Hb_2 = b_2H$, so $hb_2 = b_2h''$ for some $h'' \in H$. Using this we obtain

$$a_1b_1 = a_2hb_2h' = a_2b_2h''h' \in a_2b_2H$$

This gives $a_1b_1H \subseteq a_2b_2H$. Analogously we can show that $a_2b_2H \subseteq a_1b_1H$, and so $a_2b_2H = a_1b_1H$. □

Definition 14.3

Let G be a group and let $H \triangleleft G$. The *quotient group* G/H is defined as follows:

- Elements of G/H are left cosets aH of H in G.
- Group operation: $aH \cdot bH = (ab)H$.
- The identity element: the coset $eH = H$.
- The inverse of aH: $a^{-1}H$.

Note. By Lagrange Theorem 13.6 we have

$$|G/H| = [G : H] = \frac{|G|}{|H|}$$

Example. Take 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

One can check that the subgroup $K = \{I, R_{180}\}$ is a normal subgroup of D_4. The quotient group D_4/K has 4 elements:

$$\begin{aligned}
IK &= R_{180}K = \{I, R_{180}\}\\
R_{90}K &= R_{270}K = \{R_{90}, R_{270}\}\\
HK &= VK = \{H, K\}\\
DK &= D'K = \{D, D'\}
\end{aligned}$$

The multiplication table of D_4/K is as follows:

$\circ$	IK	$R_{90}K$	HK	DK
IK	IK	$R_{90}K$	HK	DK
$R_{90}K$	$R_{90}K$	IK	DK	HK
HK	HK	DK	IK	$R_{90}K$
DK	DK	HK	$R_{90}K$	IK

Recall that every group of order 4 is isomorphic either to $\mathbb{Z}_4$ or $\mathbb{Z}_2 \times \mathbb{Z}_2$. Since all elements of D_4/K are of order 2, we obtain that $D_4/K \cong \mathbb{Z}_2 \times \mathbb{Z}_2$

Example. If G is a cyclic group every subgroup $H \subseteq G$ is normal, since G is abelian. Moreover, if $G = \langle a \rangle$ then every element of G/H is of the form $a^k H = (aH)^k$ for some $k \in \mathbb{Z}$. This means that G/H is a cyclic group, $G/H = \langle aH \rangle$. If $[G : H] = n$ then $G/H \cong \mathbb{Z}_n$

Recall that if $f\colon G \to H$ is a homomorphism, then by Corollary 11.11 $\mathrm{Ker}(f)$ is a normal subgroup of G, so the quotient group $G/\mathrm{Ker}(f)$ exists.

Theorem 14.4 (First Isomorphism Theorem)

Let $f\colon G \to H$ be a homomorphisms of groups which is onto. Then

$$H \cong G/\mathrm{Ker}(f)$$

Example. Take the homomorphism $f\colon \mathbb{Z} \to \mathbb{Z}_n$ given by $f(k) = k \mod n$. This homomorphism is onto and

$$\mathrm{Ker}(f) = \{k \mid k \mod n = 0\} = \{nl \mid l \in \mathbb{Z}\}$$

Denote this subgroup of $\mathbb{Z}$ by $n\mathbb{Z}$. By Theorem 14.4 we obtain $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$.

Example. Recall that $\mathbb{R}^*$ denote the group of non-zero real numbers with multiplication. Take the determinant homomorphism

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

This homomorphism is onto and

$$\mathrm{Ker}(\det) = \{A \in GL(n, \mathbb{R}) \mid \det A = 1\} = SL(n, \mathbb{Z})$$

Thus we obtain $GL_n(n, \mathbb{R})/SL(n, \mathbb{R}) \cong \mathbb{R}^*$.

Proof of Theorem 14.4. Let $b \in H$. Since f is onto, there is $a \in G$ such that $f(a) = b$. Recall that by Corollary 11.8 we have

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

It follows that we have a well-defined function $\bar{f}\colon G/\mathrm{Ker}(f) \to H$ given by $\bar{f}(g\mathrm{Ker}(f)) = f(g)$. We will show that this function is an isomorphism of groups.

First, notice that the function $\bar{f}$ is a homomorphism:

$$\begin{aligned} \bar{f}(a_1\mathrm{Ker}(f) \cdot a_2\mathrm{Ker}(f)) &= \bar{f}(a_1a_2\mathrm{Ker}(f)) \\ &= f(a_1a_2) \\ &= f(a_1) \cdot f(a_2) \\ &= \bar{f}(a_1\mathrm{Ker}(f)) \cdot \bar{f}(a_2\mathrm{Ker}(f)) \end{aligned}$$

Next, the function $\bar{f}$ is onto, since f is onto. It remains to show that $\bar{f}$ is 1-1, i.e. that $\mathrm{Ker}(\bar{f}) = \{e\mathrm{Ker}(f)\}$. Assume then that $\bar{f}(g\mathrm{Ker}(f)) = e$. This means that $f(g) = e$, so $g \in Ker(f)$. But in such case $g\mathrm{Ker}(f) = e\mathrm{Ker}(f)$. $\square$

Corollary 14.5

For any normal subgroup K of a group G there exists a homomorphism $f: G \to H$ such that $\mathrm{Ker}(f) = K$.

Proof. Take $H = G/K$ and define f by $f(a) = aK$. $\square$