Theorem 6.7 Let $\phi : G \to G'$ be an epimorphism where G and G' are two groups. Then the following are true:

(i) H is a subgroup of G and $\ker\phi \subset H \Rightarrow H = \phi^{-1}(\phi(H))$

(ii) The mapping $H \mapsto \phi(H)$ is a bijection between the family of subgroups of G containing $\ker\phi$ and the family of subgroups of G'; furthermore, normal subgroups of G correspond to normal subgroups of G'.

Proof: (i) Trivially, $H \subset \phi^{-1}(\phi(H))$. Let $x \in \phi^{-1}(\phi(H))$. Then

$\phi(x) \in \phi(H) \Rightarrow \phi(x) = \phi(h)$ (for some $h \in H$)

$\Rightarrow \phi(x)(\phi(h))^{-1} = e'$ (e' is the identity in G')

$\Rightarrow \phi(x)\phi(h^{-1}) = e'$

$\Rightarrow \phi(xh^{-1}) = e' \Rightarrow xh^{-1} \in \ker\phi$

$\Rightarrow xh^{-1} \in H$ as $\ker\phi \subset H$

$\Rightarrow (xh^{-1})h \in H$ as H is a subgroup

$\Rightarrow x \in H$

Thus $H \supseteq \phi^{-1}(\phi(H))$

(ii) Let H' be a subgroup of G'. Then $\phi^{-1}(H')$ is a subgroup of G by Theorem 6.5. and $\ker\phi \subset \phi^{-1}(H')$. Also $\phi(\phi^{-1}(H')) = H'$. So, the mapping $H \mapsto \phi(H)$ is surjective. Now let $\phi(H_1) = \phi(H_2)$ where H_1, H_2 are subgroups of G containing $\ker\phi$.

Then $\phi^{-1}(\phi(H_1)) = \phi^{-1}(\phi(H_2))$, So, by (i) $H_1 = H_2$

So, the mapping $H \mapsto \phi(H)$ is a bijection of G

Now if H be a normal subgroup, then $\phi(H)$ is a normal subgroup of G' by Theorem 6.6. Then Similarly, the mapping $H \mapsto \phi(H)$ gives a bijection between the normal subgroups of G and normal subgroups of G'

Theorem 6.8 (Cayley's theorem) A finite group G of order n is isomorphic to a subgroup of S_n

Proof: Let $G = \{a_1, a_2, \ldots, a_n\}$. Let a be an arbitrary element of G. Then the elements $aa_1, aa_2, \ldots, aa_n$ all belong to G and they are all distinct by cancellation. So, $\begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ aa_1 & aa_2 & \cdots & aa_n \end{pmatrix}$ is a permutation on the set $\{a_1, a_2, \ldots, a_n\}$. We denote this permutation by π_a

Let S_n be the symmetric group of all permutations on the set $\{a_1, a_2, \ldots, a_n\}$. Let us define a mapping $\phi : G \to S_n$ by $\phi(a_i) = \pi_{a_i}$ i.e.,

$\phi(a_i) = \begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ a_ia_1 & a_ia_2 & & a_ia_n \end{pmatrix}$. We prove that ϕ is a homomorphism, Let $a_i, a_j \in G$

$$\text{Then } \phi(a_ia_j) = \begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ a_ia_ja_1 & a_ia_ja_2 & & a_ia_ja_n \end{pmatrix}$$

$$= \begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ a_ia_1 & a_ia_2 & & a_ia_n \end{pmatrix} \begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ a_ja_1 & a_ja_2 & \cdots & a_ja_n \end{pmatrix}$$

$$= \phi(a_i)\,\phi(a_j)$$

So, ϕ is a homomorphism. Let $a \in \ker\phi$. Then

$$\phi(a) = \begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ a_1 & a_2 & & a_n \end{pmatrix} \Rightarrow \begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ aa_1 & aa_2 & & aa_n \end{pmatrix} = \begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ a_1 & a_2 & \cdots & a_n \end{pmatrix}$$

So, $aa_i = a_i$, $i = 1, 2, \ldots, n$

So $a = e$, e is the identity element G.

So, $\ker\phi = \{e\}$. So ϕ is injective

Now $\phi(G)$ is a subgroup of S_n. So, G is isomorphic to $\phi(G) = \{\pi_{a_1}, \pi_{a_2}, \cdots \pi_{a_n}\}$, a subgroup of S_n.

Theorem 6.9 Let G and G' be two groups and $\phi: G \to G'$ be an isomorphism. Then

(i) $o(a) = o(\phi(a))$ for every $a \in G$.

(ii) G' is commutative if and only if G is commutative

(iii) G' is cyclic if and only if G is cyclic

Proof: (i) Case 1 Let $o(a) = n$. By Theorem 6.1 (iv), $o(\phi(a))$ is a divisor of n. We prove that $o(\phi(a)) = n$. If possible, let $o(\phi(a)) = m$ and $m < n$. Then $(\phi(a))^k = e'$, e' is the identity in G'

$\Rightarrow \phi(a^m) = \phi(e)$, e is the identity in G.

$\Rightarrow a^m = e$ [$\because \phi$ is injective]

This ~~Contradi~~ contradicts that $o(a) = n$. So, $o(\phi(a)) = n$

Case 2 Let $o(a)$ be infinite

we prove that $o(\phi(a))$ is also infinite. If possible, let $o(\phi(a)) = k$

Then $(\phi(a))^k = e' \Rightarrow \phi(a^k) = \phi(e) \Rightarrow a^k = e$. So, this implies that $o(a)$ is finite, a contradiction. So, $o(\phi(a))$ is infinite.

(ii) Let G' be commutative. Let $a, b \in G$.

$\phi(ab) = \phi(a)\phi(b) = \phi(b)\phi(a)$ (Since G' is commutative)

$= \phi(ba)$

So, $ab = ba$ as ϕ is injective. So, G is commutative

Other part follows from Theorem 6.4(i).

(iii) Let G' be cyclic and let $G' = \langle a' \rangle$. Since ϕ is surjective, $\exists\ a \in G$ such that $\phi(a) = a'$

Let $b \in G$. Then $\phi(b) = G'$. So, $\phi(b) = a'^r$ for some integer r.

So, $\phi(b) = (\phi(a))^r = \phi(a^r)$. So, $b = a^r$ [as ϕ is injective]

So, $G = \langle a \rangle$. So, G is cyclic. The other part follows from Theorem 6.4(ii)

Examples of Isomorphism:

1. Let G, G' be two groups and f is an isomorphism. Let $f: G \to G'$ be an isomorphism. Then f^{-1} is also an isomorphism

2. Let G, G', G'' be three groups and $f: G \to G'$ and $g: G' \to G''$ be two isomorphism Then $gof: G \to G'$ defined by $(gof)(x) = g(f(x))$ is an isomorphism.

3. Let n be a positive integer. Define a mapping $f: \mathbb{Z}_n \to \mathbb{Z}/n\mathbb{Z}$ by $f(\bar{a}) = a + n\mathbb{Z}$ for any $\bar{a} \in \mathbb{Z}_n$. Then $\bar{a} = \bar{b}$ if and only if n divides $a-b$ if and only if $a - b = nq$ for some $q \in \mathbb{Z}$, if and only if $a - b \in n\mathbb{Z}$ if and only if $a + n\mathbb{Z} = b + n\mathbb{Z}$ if and only $f(\bar{a}) = f(\bar{b})$. So, f is well defined and injective. From the definition of f, it follows that f is surjective.

Now $f(\bar{a} + \bar{b}) = f(\overline{a+b}) = a+b+n\mathbb{Z} = (a+n\mathbb{Z}) + (b+n\mathbb{Z})$

$= f(\bar{a}) + f(\bar{b})$. Thus f is an isomorphism.

4. Let $(\mathbb{R}, +)$ be the group of real numbers under addition and $(\mathbb{R}^+, \cdot)$ be the group of positive real numbers under multiplication. Define $f: \mathbb{R} \to \mathbb{R}^+$ by $f(a) = e^a$ for all $a \in \mathbb{R}$. Clearly f is well defined. Let $a, b \in \mathbb{R}$. Then $f(a+b) = e^{a+b} = e^a \cdot e^b = f(a) f(b)$ Hence f is a homomorphism. Suppose $f(a) = f(b) \Rightarrow e^a = e^b$ $\Rightarrow \log_e e^a = \log_e e^b \Rightarrow a = b$. So, f is injective. Let $b \in \mathbb{R}^+$ Then $\log_e b \in \mathbb{R}$ and $f(\log_e b) = e^{\log_e b} = b$. So, f is surjective. So, f is an isomorphism. So $(\mathbb{R}, +)$ and $(\mathbb{R}^+, \cdot)$ are isomorphic.

5. Symmetric group S_3 is not isomorphic with $(\mathbb{Z}_6, +)$ because $(\mathbb{Z}_6, +)$ is commutative but S_3 is not.

6. Consider the group $(\mathbb{Z}, +)$ and $(\mathbb{Q}, +)$. They are not isomorphic as $(\mathbb{Z}, +)$ is cyclic and $(\mathbb{Q}, +)$ is not cyclic.

7. Consider the group $(\mathbb{Q}, +)$ and $(\mathbb{Q}^*, \cdot)$ where $(\mathbb{Q}^*, \cdot)$ is the group of non-zero rationals with respect to multiplication. They are not isomorphic since every non-identity element of $(\mathbb{Q}, +)$ is of infinite order while -1 is a non-identity element of $(\mathbb{Q}^*, \cdot)$ which is of finite order (of order 2)

Theorem 6.10 Every finite cyclic group of order n is isomorphic to $(\mathbb{Z}_n, +)$ and every infinite cyclic group is isomorphic to $(\mathbb{Z}, +)$

Proof Let G be a cyclic group of order n and $G = \langle a \rangle$. Define the mapping $f: G \to \mathbb{Z}_n$ by $f(a^i) = \bar{i}$, for each $a^i \in G$. Now $a^i = a^j$ if and only if $a^{j-i} = e$ (e is the identity element in G) if and only if n divides $j-i$ if and only if $\bar{i} = \bar{j}$ if and only if $f(a^i) = f(a^j)$. So, f is well defined and injective. Now $f(a^i a^j) = f(a^{i+j}) = \overline{i+j} = \bar{i} + \bar{j} = f(a^i) + f(a^j)$ for $a^i, a^j \in G$. So f is a homomorphism. Since f is injective and G and $\mathbb{Z}_n$ are finite with same number of elements, f is surjective. Hence f is an isomorphism. Hence G is isomorphic to $(\mathbb{Z}_n, +)$.

Now let $G = \langle a \rangle$ be an infinite cyclic group. Define the mapping $\phi: G \to \mathbb{Z}$ by $\phi(a^i) = i$ for each $a^i \in G$. Since $a^i = a^j$ if and only if $a^{i-j} = e$ (e is the identity in G) if and only if $i - j = 0$ (since a is of infinite order) if and only if $i = j$. So, ϕ is well defined and injective. From the definition of f, f is surjective. Now $f(a^i a^j) = f(a^{i+j}) = \overline{i+j} = f(a^i) + f(a^j)$. Hence G is isomorphic to $\mathbb{Z}$.

Corollary: Any two cyclic groups of the same order are isomorphic

From the above corollary, it follows that there is only one (up to isomorphism) cyclic group having a prescribed order.

Worked out exercises: 1. Show that there are only two groups of order 4 up to isomorphism, a cyclic group of order 4 and other is Klein's 4-group.

Proof: Let G be a group of order 4 which is not cyclic. Then no element of G can have order 4, otherwise, it would be cyclic. Let $G = \{e, a, b, c\}$. Since the order of every element of G divides the order of G, a, b and c have order 2 (as e is the identity element). If $ab = a$, then $b = e$, a contradiction. Thus $ab \neq a$. Similarly $ab \neq b$. Suppose $ab = e$, then $a(ab) = ae$. So, $b = a$ as $a^2 = e$, a contradiction. Thus $ab \neq e$. So, $ab = c$. Similarly $ba = c$. Hence $ab = ba$. By similar arguments $ac = b = ca$ and $bc = a = cb$. Thus, we see that G is a commutative group and whose composition table is given below

	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Consequently, there is essentially one group of order 4 which is not cyclic. This is Klein's 4-group. Since all cyclic groups of the same orders are isomorphic, we thus have exactly two non-isomorphic groups of order 4, namely, Klein's 4-group and the cyclic group of order 4.

Exercise 2. Let G and H be finite groups such that $\gcd(o(G), o(H)) = 1$. Show that the trivial homomorphism is homomorphism from G into H.

Proof: Let $f: G \to H$ be a homomorphism and $a \in G$. Now $o(a)$ divides $o(G)$ and $o(f(a))$ divides $o(H)$. Also by Theorem 6.1, (iv), $o(f(a))$ divides $o(a)$. Hence $o(f(a))$ divides $o(G)$. Since $o(G)$ and $o(H)$ are relatively prime, $o(f(a)) = 1$, proving $f(a) = e$, e is the identity in G. So, $f(a) = e$, $\forall a \in G$. Hence f is the trivial homomorphism.

3. Show that the group $(\mathbb{Q}, +)$ is not isomorphic to $(\mathbb{Q}/\mathbb{Z}, +)$

Proof: In $(\mathbb{Q}, +)$, every non-zero element is of infinite order. Let $p/q + \mathbb{Z} \in \mathbb{Q}/\mathbb{Z}$, where $p, q \in \mathbb{Z}$ and $q \neq 0$. Then

$q\left(\frac{p}{q} + \mathbb{Z}\right) = p + \mathbb{Z} = \mathbb{Z}$. This shows that every element of $\mathbb{Z}$ is of finite order. Hence, $(\mathbb{Q}, +)$ is not isomorphic to $(\mathbb{Q}/\mathbb{Z}, +)$

Note: If two groups G and G' are isomorphic, we write $G \simeq G'$

Theorem 6.11 Let H be a normal subgroup of a group G. Then $\theta: G \to G/H$ defined by $\theta(x) = xH$, $x \in G$ is an onto homomorphism with kernel H.

Proof: By definition, θ is a surjective or onto. Let $x, y \in G$

Then $\theta(xy) = xyH = xHyH = \theta(x)\theta(y)$. So θ is a homomorphism.

Now $x \in \ker\theta \Leftrightarrow \theta(x) = H \Leftrightarrow xH = H \Leftrightarrow x \in H$

So $\ker\theta = H$.

So, θ is a onto homomorphism whose kernel is H.

Note: θ is said to be the natural (or canonical) homomorphism from G onto G/H.

Theorem 6.12 (First Isomorphism Theorem) Let $\phi: G \to G'$ be a homomorphism of a group G onto a group G'. Then

$$G/\ker\phi \simeq G'$$

Proof: ~~Let $\gamma : G/\ker\phi$~~ Let $K = \ker\phi$. Define $\gamma : G/K \to G'$ by $\gamma(xK) = \phi(x)$ for any $xK \in G/K$

Now $xK = yK \Leftrightarrow x^{-1}y \in K \Leftrightarrow \phi(x^{-1}y) = e'$ (e' is the identity in G')

$\Leftrightarrow \phi(x^{-1})\phi(y) = e' \Leftrightarrow (\phi(x))^{-1}\phi(y) = e \Leftrightarrow \phi(x) = \phi(y) \Leftrightarrow \gamma(xK) = \gamma(yK)$

Hence γ is well defined and injective.

Let $y \in G'$. As ϕ is onto, $\exists\ x \in G$, such that $\phi(x) = y$

So, $\gamma(xK) = \phi(x) = y$. Hence γ is surjective or onto.

Now $\gamma(xKyK) = \gamma(xyK) = \phi(xy) = \phi(x)\phi(y)$ [As ϕ is a homomorphism]

$= \gamma(xK)\gamma(yK)$

Hence γ is a homomorphism. So, γ is an isomorphism

So, $G/K \simeq G'$ or, $G/\ker\phi \simeq G'$.

Theorem 6.13 (Second Isomorphism Theorem). Let H and N be subgroups of a group G and N is a normal subgroup of G.

Then $H/H\cap N \simeq HN/N$

Proof: Since N is a normal subgroup of G, $HN = NH$ is a subgroup of G. and N is a normal subgroup of HN.

Consider the mapping $\phi : H \to HN/N$ given by $\phi(h) = hN$, for $h \in H$.

In fact, ϕ is the restriction of the natural homomorphism $\theta : G \to G/N$ to H. Hence $\ker\phi = H\cap N$. Moreover, ϕ is surjective by definition. Hence by First isomorphism theorem, $H/H\cap N \simeq HN/N$.

Theorem 6.14 (Third Isomorphism Theorem). Let H and K be normal subgroups of a group G, and $K \subset H$. Then

$$(G/K)/(H/K) \simeq G/H$$

Proof: Consider the mapping $\phi : G/K \to G/H$ defined by $\phi(xK) = xH$, $xK \in G/K$. Now $xK = yK \Rightarrow x^{-1}y \in K \Rightarrow x^{-1}y \in H$ (as $K \subset H$) $\Rightarrow xH = yH \Rightarrow \phi(xK) = \phi(yK)$

So, ϕ is well defined. By definition, ϕ is surjective.

Now, $\phi(xKyK) = \phi(xyK) = xyH = xHyH = \phi(xK)\phi(yK)$ for $xK, yK \in G/K$. So, ϕ is a homomorphism and it is onto.

Also, $\ker\phi = \{xK \in G/K : \phi(xK) = H\} = \{xK \in G/K : xH = H\}$
$= \{xK \in G/K : x \in H\} = H/K$

So, by First isomorphism Theorem, $(G/K)/(H/K) \cong G/H$.

Automorphism An isomorphism of a Group G onto itself is said to be an automorphism

Examples 1. Let G be a group. The identity mapping on G is an automorphism G. This is called the identity automorphism

2. Let G be an abelian group. The mapping $\phi : G \to G$ defined by $\phi(a) = a^{-1}$, $a \in G$ is an automorphism

3. Let $G = (\mathbb{C}, +)$ be the group of complex numbers with respect to addition. Then $f : G \to G$ defined by $f(z) = \bar{z}$ is an automorphism.

Theorem 6.15 The set of all automorphisms of a group forms a group under the mapping composition.

Proof: Let G be a group and A(G) be the set of all automorphisms of G. Let $f, g, h \in A(G)$ Then $fo(goh) = (fog)oh$ as composition of mapping is associative. The identity automorphism is the identity element of A(G). Also for each $f \in A(G)$, the inverse mapping $f^{-1} \in A(G)$ and f^{-1} plays the role of inverse element of f in A(G). So A(G) is a group

Theorem 6.16 Let G be a group and the mapping $f : G \to G$ is defined by $f(x) = x^{-1}$, $x \in G$. Then f is an automorphism if and only if G is abelian.

Proof: Do it yourself.