4.1 Note: We recall the following terminology. Let \( X \) and \( Y \) be sets. When we say that \( f \) is a function or a map from \( X \) to \( Y \), written \( f : X \to Y \), we mean that for every \( x \in X \) there exists a unique corresponding element \( y = f(x) \in Y \). The set \( X \) is called the domain of \( f \) and the range or image of \( f \) is the set \( \text{Image}(f) = f(X) = \{ f(x) \mid x \in X \} \). For a set \( A \subseteq X \), the image of \( A \) under \( f \) is the set \( f(A) = \{ f(a) \mid a \in A \} \) and for a set \( B \subseteq Y \), the inverse image of \( B \) under \( f \) is the set \( f^{-1}(B) = \{ x \in X \mid f(x) \in B \} \).

For a function \( f : X \to Y \), we say \( f \) is one-to-one (written 1:1) or injective when for every \( y \in Y \) there exists at most one \( x \in X \) such that \( y = f(x) \), we say \( f \) is onto or surjective when for every \( y \in Y \) there exists at least one \( x \in X \) such that \( y = f(x) \), and we say \( f \) is invertible or bijective when \( f \) is 1:1 and onto, that is for every \( y \in Y \) there exists a unique \( x \in X \) such that \( y = f(x) \). When \( f \) is invertible, the inverse of \( f \) is the function \( f^{-1} : Y \to X \) defined by \( f^{-1}(y) = x \iff y = f(x) \).

For \( f : X \to Y \) and \( g : Y \to Z \), the composite \( g \circ f : X \to Z \) is given by \( (g \circ f)(x) = g(f(x)) \). Note that if \( f \) and \( g \) are both injective then so is the composite \( g \circ f \), and if \( f \) and \( g \) are both surjective then so is \( g \circ f \).

4.2 Definition: Let \( G \) and \( H \) be groups. A group homomorphism from \( G \) to \( H \) is a function \( \phi : G \to H \) such that
\[
\phi(ab) = \phi(a)\phi(b)
\]
for all \( a, b \in G \), or to be more precise, such that \( \phi(a \ast b) = \phi(a) \times \phi(b) \) for all \( a, b \in G \), where \( \ast \) is the operation on \( G \) and \( \times \) is the operation on \( H \). The kernel of \( \phi \) is the set
\[
\ker(\phi) = \phi^{-1}(e) = \{ a \in G \mid \phi(a) = e \}
\]
where \( e = e_H \) is the identity in \( H \), and the image (or range) of \( \phi \) is
\[
\text{Image}(\phi) = \phi(G) = \{ \phi(a) \mid a \in G \}.
\]
A group isomorphism from \( G \) to \( H \) is a bijective group homomorphism \( \phi : G \to H \). For two groups \( G \) and \( H \), we say that \( G \) and \( H \) are isomorphic and we write \( G \cong H \) when there exists an isomorphism \( \phi : G \to H \). An endomorphism of a group \( G \) is a homomorphism from \( G \) to itself. An automorphism of a group \( G \) is an isomorphism from \( G \) to itself. The set of all homomorphisms from \( G \) to \( H \), the set of all isomorphisms from \( G \) to \( H \), the set of all endomorphisms of \( G \), and the set of all automorphisms of \( G \) will be denoted by
\[
\text{Hom}(G,H), \text{Iso}(G,H), \text{End}(G), \text{Aut}(G).
\]

4.3 Remark: In algebra, we consider isomorphic groups to be (essentially) equivalent. The classification problem for finite groups is to determine, given any \( n \in \mathbb{Z}^+ \), the complete list of all groups, up to isomorphism, of order \( n \).
4.4 Example: The groups $U_{12}$ and $\mathbb{Z}_2^2$ are isomorphic. One way to see this is to compare their operation tables.

$\begin{array}{cccc}
1 & 5 & 7 & 11 \\
1 & 1 & 5 & 7 \\
5 & 5 & 1 & 11 \\
7 & 7 & 11 & 1 \\
11 & 11 & 7 & 5
\end{array}$

$\begin{array}{cccccc}
(0,0) & (0,1) & (1,0) & (1,1) \\
(0,0) & (0,0) & (0,1) & (1,0) & (1,1) \\
(0,1) & (0,1) & (0,0) & (1,1) & (1,0) \\
(1,0) & (1,0) & (1,1) & (0,0) & (0,1) \\
(1,1) & (1,1) & (1,0) & (0,1) & (0,0)
\end{array}$

We see that all the entries in these tables correspond under the map $\phi: U_{12} \rightarrow \mathbb{Z}_2^2$ given by $\phi(1) = (0,0)$, $\phi(5) = (0,1)$, $\phi(7) = (1,0)$ and $\phi(1,1) = (1,1)$, so $\phi$ is an isomorphism.

4.5 Example: Let $G$ be a group and let $a \in G$. Then the map $\phi_a: \mathbb{Z} \rightarrow G$ given by $\phi_a(k) = a^k$ is a group homomorphism since $\phi_a(k + \ell) = a^{k+\ell} = a^k a^\ell = \phi_a(k) \phi_a(\ell)$.

The image of $\phi_a$ is

$$\text{Image}(\phi_a) = \{a^k | k \in \mathbb{Z}\} = \langle a \rangle$$

and the kernel of $\phi_a$ is

$$\text{Ker}(\phi_a) = \{k \in \mathbb{Z} | a^k = e\} = \begin{cases} \langle n \rangle = n\mathbb{Z}, & \text{if } |a| = n, \\ \langle 0 \rangle = \{0\}, & \text{if } |a| = \infty. \end{cases}$$

4.6 Example: Let $G$ be a group and let $a \in G$. If $|a| = \infty$ then the map $\phi_a: \mathbb{Z} \rightarrow \langle a \rangle$ given by $\phi_a(k) = a^k$ is an isomorphism, and if $|a| = n$ then the map $\phi_a: \mathbb{Z}_n \rightarrow \langle a \rangle$ given by $\phi_a(k) = a^k$ is an isomorphism (note that $\phi_a$ is well-defined because if $k = \ell \mod n$ then $a^k = a^\ell$ by Theorem 2.3). In each case, $\phi$ is a homomorphism since $a^{k+\ell} = a^k a^\ell$ and $\phi$ is bijective by Theorem 2.3.

4.7 Example: When $R$ is a commutative ring with 1, the map $\phi : GL_n(R) \rightarrow R^*$ given by $\phi(A) = \det(A)$ is a group homomorphism since $\det(AB) = \det(A) \det(B)$. The kernel is

$$\text{Ker}(\phi) = \{A \in GL_n(R) | \det(A) = 1\} = SL_n(R)$$

and the image is

$$\text{Image}(\phi) = \{ \det(A) | A \in GL_n(R) \} = R^*$$

since for $a \in R^*$ we have $\det(\text{diag}(a,1,1,\cdots,1)) = a$.

4.8 Example: The map $\phi : \mathbb{R} \rightarrow \mathbb{R}^+$ given by $\phi(x) = e^x$ is a group isomorphism since it is bijective and $\phi(x + y) = e^{x+y} = e^x e^y = \phi(x) \phi(y)$.

4.9 Example: The map $\phi : SO_2(\mathbb{R}) \rightarrow S^1$ given by $\phi(R_\theta) = e^{i\theta}$ is a group isomorphism.
4.10 Theorem: Let $G$ and $H$ be groups and let $\phi : G \to H$ be a group homomorphism. Then

1. $\phi(e_G) = e_H$,
2. $\phi(a^{-1}) = \phi(a)^{-1}$ for all $a \in G$,
3. $\phi(a^k) = \phi(a)^k$ for all $a \in G$ and all $k \in \mathbb{Z}$, and
4. For $a \in G$, if $|a|$ is finite then $|\phi(a)|$ divides $|a|$.

Proof: To prove (1), note that $\phi(e_G) = \phi(e_G e_G) = \phi(e_G) \phi(e_G)$ so $\phi(e_G) = e_H$ by cancellation. To prove (2) note that $\phi(a) \phi(a^{-1}) = \phi(aa^{-1}) = \phi(e_G) = e_H$, so $\phi(a)^{-1} = \phi(a^{-1})$ by cancellation. For part (3), note first that $\phi(a^0) = \phi(a)^0$ by part (1), and then note that when $k \in \mathbb{Z}^+$ we have $\phi(a^k) = \phi(aa \cdots a) = \phi(a) \phi(a) \cdots \phi(a) = \phi(a)^k$ and hence also $\phi(a^{-k}) = \phi((a^{-1})^k) = \phi(a^{-1})^k = (\phi(a)^{-1})^k = \phi(a)^{-k}$. For part (4) note that if $|a| = n$ then we have $\phi(a)^n = \phi(a^n) = \phi(e_G) = e_H$ and so $|\phi(a)|$ divides $n$ by Theorem 2.3.

4.11 Theorem: Let $G$, $H$ and $K$ be groups. Let $\phi : G \to H$ and $\psi : H \to K$ be group homomorphisms. Then

1. the identity $I : G \to G$ given by $I(x) = x$ for all $x \in G$, is an isomorphism,
2. the composite $\psi \circ \phi : G \to K$ is a group homomorphism, and
3. if $\phi : G \to H$ is an isomorphism then so is its inverse $\phi^{-1} : H \to G$.

Proof: We prove part (3) and leave the proofs of (1) and (2) as an exercise. Suppose that $\phi : G \to H$ is an isomorphism. Let $\psi = \phi^{-1} : H \to G$. We know that $\psi$ is bijective, so we just need to show that $\psi$ is a homomorphism. Let $c,d \in H$. Let $a = \phi(c)$ and $b = \psi(d)$. Since $\phi$ is a homomorphism we have $\phi(ab) = \phi(a) \phi(b)$, and so

$$\psi(cd) = \psi(\phi(a) \phi(b)) = \psi(\phi(ab)) = ab = \psi(c) \psi(d).$$

4.12 Corollary: Isomorphism is an equivalence relation on the class of groups. This means that for all groups $G$, $H$ and $K$ we have

1. $G \cong G$,
2. if $G \cong H$ and $H \cong K$ then $G \cong K$, and
3. if $G \cong H$ then $H \cong G$.

4.13 Corollary: For a group $G$, $\text{Aut}(G)$ is a group under composition.

4.14 Theorem: Let $\phi : G \to H$ be a homomorphism of groups. Then

1. if $K \leq G$ then $\phi(K) \leq H$, in particular $\text{Image}(\phi) \leq H$,
2. if $L \leq H$ then $\phi^{-1}(L) \leq G$, in particular $\text{Ker}(\phi) \leq G$.

Proof: The proof is left as an exercise.

4.15 Theorem: Let $\phi : G \to H$ be a homomorphism of groups. Then

1. $\phi$ is injective if and only if $\text{Ker}(\phi) = \{e\}$, and
2. $\phi$ is surjective if and only if $\text{Image}(\phi) = H$.

Proof: The proof is left as an exercise.
4.16 Theorem: Let $\phi : G \to H$ be an isomorphism of groups. Then

1. $G$ is abelian if and only if $H$ is abelian,
2. for $a \in G$ we have $|\phi(a)| = |a|$,
3. $G$ is cyclic with $G = \langle a \rangle$ if and only if $H$ is cyclic with $H = \langle \phi(a) \rangle$,
4. for $n \in \mathbb{Z}^+$ we have $\{ a \in G | |a| = n \} = \{ b \in H | |b| = n \}$,
5. for $K \leq G$ the restriction $\phi : K \to \phi(K)$ is an isomorphism of groups, and
6. for any group $C$ we have $\{ K \leq G | K \cong C \} = \{ L \leq H | L \cong C \}$.

Proof: The proof is left as an exercise.

4.17 Example: Note that $\mathbb{Q}^* \ncong \mathbb{R}^*$ since $|\mathbb{Q}^*| \neq |\mathbb{R}^*|$. Similarly, $GL_3(\mathbb{Z}_2) \ncong S_5$ because $|GL_3(\mathbb{Z}_2)| = 168$ but $|S_5| = 120$.

4.18 Example: $\mathbb{C}^* \ncong GL_2(\mathbb{R})$ since $\mathbb{C}^*$ is abelian but $GL_n(\mathbb{R})$ is not. Similarly, $S_4 \ncong U_{35}$ because $U_{35}$ is abelian but $S_4$ is not.

4.19 Example: $\mathbb{R}^* \ncong \mathbb{C}^*$ since $\mathbb{C}^*$ has elements of order $n \geq 3$, for example $|i| = 4$ in $\mathbb{C}^*$, but $\mathbb{R}^*$ has no elements of order $n \geq 3$, indeed in $\mathbb{R}^*$, $|1| = 1$ and $|-1| = 2$ and for $x \neq \pm 1$ we have $|x| = \infty$.

4.20 Example: Determine whether $U_{35} \cong \mathbb{Z}_{24}$.

Solution: In $U_{35}$ we have

\[
\begin{array}{cccccccccccc}
 k & 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\
2^k & 1 & 2 & 4 & 8 & 16 & 32 & 29 & 23 & 11 & 22 & 9 & 18 & 1
\end{array}
\]

We notice that $U_{35}$ has at least two elements of order 2, namely 29 and 34, but $\mathbb{Z}_{24}$ has only one element of order 2, namely 12. Thus $U_{35} \ncong \mathbb{Z}_{24}$.

4.21 Theorem: Let $a, b \in \mathbb{Z}^+$ with $\gcd(a, b) = 1$. Then

1. $\mathbb{Z}_{ab} \cong \mathbb{Z}_a \times \mathbb{Z}_b$ and
2. $U_{ab} \cong U_a \times U_b$.

Proof: We prove part (2) (the proof of part (1) is similar). Define $\phi : U_{ab} \to U_a \times U_b$ by $\phi(k) = (k, k)$. This map $\phi$ is well-defined because if $k = \ell \mod ab$ then $k = \ell \mod a$ and $k = \ell \mod b$ and because if $\gcd(k, ab) = 1$ so that $k \in U_{ab}$ then $\gcd(k, a) = \gcd(k, b) = 1$. Also, $\phi$ is a group homomorphism since $\phi(k\ell) = (k\ell, k\ell) = (k, k)(\ell, \ell) = \phi(k)\phi(\ell)$. Finally note that $\phi$ is bijective by the Chinese Remainder Theorem, indeed $\phi$ is onto because given $k \in U_a$ and $\ell \in U_b$ there exists $x \in \mathbb{Z}$ with $x = k \mod a$ and $x = \ell \mod b$ and we then have $\gcd(x, a) = \gcd(k, a) = 1$ and $\gcd(x, b) = \gcd(\ell, b) = 1$ so that $\gcd(x, ab) = 1$, that is $x \in U_{ab}$, and $\phi$ is 1:1 because this solution $x$ is unique modulo $ab$.

4.22 Corollary: If $n = \prod_{i=1}^{\ell} p_i^{k_i}$ where the $p_i$ are distinct primes and each $k_i \in \mathbb{Z}^+$ then

\[
\phi(n) = \prod_{i=1}^{\ell} (p_i^{k_i} - p_i^{k_i - 1}) = n \cdot \prod_{i=1}^{\ell} \left(1 - \frac{1}{p_i}\right).
\]
**4.23 Definition:** Let $G$ be a group. For $a \in G$, we define **left multiplication** by $a$ to be the map $L_a : G \to G$ given by

$$L_a(x) = ax \text{ for } x \in G.$$  

Note that $L_e = I$ (since $L_e(x) = ex = x = I(x)$ for all $x \in G$) and $L_aL_b = L_{ab}$ since $L_a(L_b(x)) = L_a(br) = abx = L_{ab}(x)$ for all $x \in G$. Similarly, we define **right-multiplication** by $a$ to be the map $R_a : G \to G$ given by $R_a(x) = ax$ for $x \in G$. Also, we define **conjugation** by $a$ to be the map $C_a : G \to G$ by

$$C_a(x) = axa^{-1} \text{ for } x \in G.$$  

The map $L_a : G \to G$ is not necessarily a group homomorphism since $L_a(xy) = a(xy)$ while $L_a(x)L_a(y) = axay$. On the other hand, the map $C_a : G \to G$ is a group homomorphism because $C_a(xy) = axya^{-1} = axa^{-1}aya^{-1} = C_a(x)C_a(y)$. Indeed $C_a$ is an automorphism of $G$ because it is invertible with $C_a^{-1} = C_{a^{-1}}$. An automorphism of $G$ of the form $C_a$ is called an **inner automorphism** of $G$. The set of all inner automorphisms of $G$ is denoted by Inn($G$), so we have

$$\text{Inn}(G) = \{C_a | a \in G\}.$$  

Note that $\text{Inn}(G) \leq \text{Aut}(G)$ because $I = C_e$, $C_aC_b = C_{ab}$ and $C_a^{-1} = C_{a^{-1}}$. Note that when $H \leq G$, the restriction of the conjugation map $C_a$ gives an isomorphism from $H$ to the group

$$C_a(H) = aHa^{-1} = \{aha^{-1} | h \in H\} \cong H.$$  

The isomorphic groups $H$ and $C_a(H) = aHa^{-1}$ are called **conjugate** subgroups of $G$.

**4.24 Example:** As an exercise, find $\text{Inn}(D_4)$ and show that $\text{Inn}(D_4) \neq \text{Aut}(D_4)$.

**4.25 Example:** Let $G$ be a finite set with $|G| = n$. Let $S = \{1, 2, \cdots, n\}$ and let $f : G \to S$ be a bijection. The map $C_f : \text{Perm}(G) \to S_n$ given by $C_f(g) = fgf^{-1}$ is a group isomorphism. Indeed, $C_f$ is well-defined since when $g \in \text{Perm}(G)$ the map $fgf^{-1}$ is invertible with $(fgf^{-1})^{-1} = fg^{-1}f^{-1}$, and $C_f$ is a group homomorphism since $C_f(gh) = fghf^{-1} = fgf^{-1}fhf^{-1} = C_f(g)C_f(h)$, and $C_f$ is bijective with inverse $C_{f^{-1}} = C_{f^{-1}}$.

**4.26 Theorem:** (Cayley’s Theorem) Let $G$ be a group.

1. $G$ is isomorphic to a subgroup of $\text{Perm}(G)$.
2. If $|G| = n$ then $G$ is isomorphic to a subgroup of $S_n$.

**Proof:** Define $\phi : G \to \text{Perm}(G)$ by $\phi(a) = L_a$. Note that $L_a \in \text{Perm}(G)$ because $L_a$ is invertible with inverse $L_a^{-1} = L_{a^{-1}}$. Also, $\phi$ is a group homomorphism because $\phi(ab) = L_{ab} = L_aL_b$ and $\phi$ is injective because $L_a = I \implies a = e$ (indeed if $L_a = I$ then $a = ae = L_a(e) = I(e) = e$). Thus $\phi$ is an isomorphism from $G$ to $\phi(G)$, which is a subgroup of $\text{Perm}(G)$.

Now suppose that $|G| = n$, say $f : G \to \{1, 2, \cdots, n\}$ is a bijection. Then the map $C_f \circ \phi$ is an injective group homomorphism (where $C_f(g) = fgf^{-1}$, as above), and so $G$ is isomorphic to $C_f(\phi(G))$ which is a subgroup of $S_n$.  

19
4.27 Example: Show that $\text{Hom}(\mathbb{Z}, G) = \{ \phi_a | a \in G \}$, where $\phi_a(k) = a^k$.

Solution: Let $\phi \in \text{Hom}(\mathbb{Z}, G)$. Let $a = \phi(1)$. Then for all $k \in \mathbb{Z}$ we have $\phi(k) = \phi(k \cdot 1) = \phi(1)^k = a^k$, and so $\phi = \phi_a$. On the other hand, note that for $a \in G$ the map $\phi_a$ given by $\phi_a(k) = a^k$ is a group homomorphism because $\phi_a(k + l) = a^{k+l} = a^ka^l = \phi_a(k)\phi_a(l)$.

4.28 Example: Show that $\text{Hom}(\mathbb{Z}_n, G) = \{ \phi_a | a \in G, a^n = e \}$, where $\phi_a(k) = a^k$.

Solution: Let $\phi \in \text{Hom}(\mathbb{Z}_n, G)$. Let $a = \phi(1)$. Then for all $k \in \mathbb{Z}$ we have $\phi(k) = \phi(k \cdot 1) = \phi(1)^k = a^k$ so that $\phi = \phi_a$, and we have $a^n = \phi(n) = \phi(0) = e$. On the other hand, note that for $a \in G$ with $a^n = e$, the map $\phi_a$ is well-defined because if $k = l \mod n$ the $a^k = a^l$ and it is a homomorphism because $a^{k+l} = a^ka^l$.

4.29 Example: As an exercise, describe $\text{Hom}(\mathbb{Z}_n \times \mathbb{Z}_m, G)$.

4.30 Example: As an exercise, describe $\text{Hom}(D_n, G)$.