Chapter 6

Defn: An isomorphism from a group \( G \) to a group \( \overline{G} \) is a one-to-one and onto function \( \phi : G \to \overline{G} \) that preserves the group operation, meaning

\[ \forall a, b \in G \quad \phi(a \cdot b) = \phi(a) \phi(b) \]

binary operation for \( G \) \quad binary operation for \( \overline{G} \)

If there is an isomorphism from \( G \) onto \( \overline{G} \), we say \( G \) and \( \overline{G} \) are isomorphic and write \( G \cong \overline{G} \)

Note:
- If binary operation on \( G \) is written as addition, the left-hand side of \((*)\) should be written \( \phi(a+b) \)
- If the binary operation on \( \overline{G} \) is written as addition, the right-hand side of \((*)\) should be written \( \phi(a) + \phi(b) \)

Isomorphic groups are considered to be "the same" or "identical" but expressed differently.

Ex: Let \( G \) be a group and \( a \in G \)

1. If \( a \) has infinite order then \( \langle a \rangle \cong \mathbb{Z} \)

   since the map \( \phi(a^k) = k \) is a bijection
   and \( \phi(a^k \cdot a^m) = \phi(a^{k+m}) = k+m = \phi(a^k) + \phi(a^m) \)
If a has order $n$ then $\langle a \rangle \cong \mathbb{Z}_n$ since the function $\phi : \langle a \rangle \to \mathbb{Z}_n$ given by $\phi(a^k) = k \text{ mod } n$ is one-to-one and onto and (by Thm 4.1) if $j = k + m \text{ mod } n$
then $\phi(a^k a^m) = \phi(a^{k+m}) = k + m \text{ mod } n$

$= (k \text{ mod } n) + (m \text{ mod } n)$

$= \phi(a^k) + \phi(a^m)$

Ex: The group $\mathbb{R}$ (with usual addition) is isomorphic to the group $(0, \infty)$ (with multiplication).
An isomorphism is $\phi(x) = e^x$ (here $e = \text{Euler's constant} = 2.71...$)

* $\phi$ is one-to-one because if $x \neq y$, say $x < y$, then $e^x < e^y$ so $e^x \neq e^y$

* $\phi$ is onto since for every $y \in (0, \infty)$ we have

  $\phi(\ln y) = e^{\ln y} = y$

* $\phi$ preserves the group operation:

  $\phi(x+y) = e^{x+y} = e^x \cdot e^y = \phi(x) \cdot \phi(y)$

Thm 6.1 (Cayley's Thm): Every group is isomorphic to a group of permutations.

pf: let $G$ be a group. For each $g \in G$ define

$T_g : G \to G$ by

$T_g(x) = gx$
Claim 1: $T_g$ is a permutation of $G$

We just have to check that $T_g$ is one-to-one and onto.

(one-to-one) Suppose $x, y \in G$ and $T_g(x) = T_g(y)$. Then

$$g \cdot x = T_g(x) = T_g(y) = g \cdot y$$

and by left-cancellation $x = y$.

(onto) Consider any $y \in G$. Setting $x = g^{-1} y$ we have

$$T_g(x) = g \cdot x = g(g^{-1} y) = (gg^{-1}) y = ey = y$$

$\square$ (Claim 1)

We will show that $\bar{G}$ is a subgroup of the group of all permutations of $G$ and that $\phi$ is an isomorphism.

Now set $\bar{G} = \{ T_g : g \in G \}$ and define $\phi : G \to \bar{G}$ by $\phi(g) = T_g$.

Claim 2: $\phi$ is one-to-one and onto

The definition of $\bar{G}$ shows $\phi$ is onto.

Next suppose $g \neq h \in G$. Then

$$T_g(e) = ge = g \neq h = he = T_h(e)$$

and hence $\phi(g) = T_g \neq T_h = \phi(h)$.

So $\phi$ is one-to-one

$\square$ (Claim 2)

Claim 3: for all $g, h \in G$, $\phi(gh) = \phi(g) \phi(h)$

Recall that $\phi(gh), \phi(g),$ and $\phi(h)$ are all functions from $G$ to $G$, and that $\phi(g) \circ \phi(h)$ is the composition of $\phi(g)$ with $\phi(h)$.
We check that \( \phi(gh) \) and \( \phi(g) \phi(h) \)
are equal by checking that for every input they give the same output:

For any \( x \in G \) we have
\[
\phi(gh)(x) = T_{gh}(x) = ghx
\]
\[
= g(hx) = T_g(hx) = T_g(T_h(x))
\]
\[
= (T_g T_h)(x)
\]

Thus \( \phi(gh) = \phi(g) \phi(h) \)
\( \phi \) (Claim 3)

Claim 4: \( G \) is a subgroup of the group of permutations of \( G \)

We'll apply Two-Step Subgroup Test.
We have \( T_e \in G \) so \( G \neq \emptyset \).

For any two elements in \( G \), say \( T_g \) and \( T_h \),
we have (by Claim 3) that
\[
T_g T_h = \phi(g) \phi(h) = \phi(gh) = T_{gh} \in G
\]
so \( T_g T_h \in G \).

Lastly, consider any \( T_g \in G \). Then \( T_g^{-1} \in G \)
and (by Claim 3)
\[
T_g^{-1} T_g = \phi(g^{-1}) \phi(g) = \phi(g^{-1} g) = \phi(e) = T_e
\]
and similarly \( T_g T_g^{-1} = T_e \) (the identity).
So $T_{g^{-1}}$ is the inverse to $T_g$, and clearly $T_{g^{-1}} \in \overline{G}$. We conclude $\overline{G}$ is a subgroup. (Claim 4)

By Claim 4 $\overline{G}$ is a group of permutations, and by Claims 2 and 3 $\phi : G \rightarrow \overline{G}$ is an isomorphism.

**Theorem 6.2.** If $\phi$ is an isomorphism from $G \rightarrow \overline{G}$ then

1. $\phi$ takes identity of $G$ to identity of $\overline{G}$
2. $\phi(a^n) = \phi(a)^n$ for all $a \in G$, $n \in \mathbb{Z}$
3. If $a, b \in G$ commute $\iff \phi(a), \phi(b)$ commute
4. $G = \langle a \rangle \iff \overline{G} = \langle \phi(a) \rangle$
5. (order of $a$) = (order of $\phi(a)$) for all $a \in G$
6. (# solutions of $x^k = b$ in $G$) = (# solutions of $x^k = d(b)$ in $\overline{G}$)
7. $G$ and $\overline{G}$ have exactly the same number of elements of every order

**Proof:**

1. $\overline{e} \phi(e) = \phi(e) = \phi(\overline{ee}) = \phi(\overline{e}) \phi(\overline{e})$

   Since $\overline{e}$ is identity in $\overline{G}$, $e = \overline{ee}$ since $\phi$ preserves group operation.

   Applying right-cancelation above, we get $\overline{e} = \phi(e)$.

2. $\phi(a^{-1}) \phi(a) = \phi(a^{-1}a) = \phi(\overline{e}) = \overline{e}$

   So $\phi(a^{-1}) = \phi(a)^{-1}$. Also

   $\phi(a^2) = \phi(aa) = \phi(a) \phi(a) = \phi(a)^2$

   $\phi(a^{-2}) = \phi(a^{-1}a^{-1}) = \phi(a^{-1}) \phi(a^{-1}) = \phi(a)^{-2}$. Can continue by induction.

3. HW $\overline{e}$

4. ($\Rightarrow$) $\phi$ is onto so $\overline{G} = \phi(G) = \phi(\langle a \rangle) = \phi(\langle a^n \mid n \in \mathbb{Z} \rangle) = \langle \phi(a)^n \mid n \in \mathbb{Z} \rangle = \langle \phi(a) \rangle$
\( \text{Thm 6.3: If } \phi \text{ is an isomorphism from } G \text{ onto } \overline{G} \text{ then:} \)

1. \( \phi^{-1} \) is an isomorphism from \( \overline{G} \) onto \( G \)
2. \( G \) abelian \( \iff \) \( \overline{G} \) abelian
3. \( G \) cyclic \( \iff \) \( \overline{G} \) cyclic
4. \( K \) a subgroup of \( G \) \( \Rightarrow \) \( \phi(K) \) a subgroup of \( \overline{G} \)
5. \( \overline{K} \) a subgroup of \( \overline{G} \) \( \Rightarrow \) \( K \) subgroup of \( G \)
6. \( \phi(\langle a \rangle) = \langle \phi(a) \rangle = G \)

Since \( \phi \) is one-to-one we must have: \( \langle a \rangle = G \)

5. Follows from 1 and 2
6. Follows from 2
7. Follows from 5

\( \square \)

**Def:** An isomorphism from \( G \) onto itself is called an automorphism of \( G \). The set of all automorphisms of \( G \) is denoted \( \text{Aut}(G) \).

**Ex:** \( \phi : \mathbb{Z} \rightarrow \mathbb{Z} \) defined by \( \phi(k) = -k \) is an automorphism of \( \mathbb{Z} \).
**Lemma: Let G be a group and \( a \in G. \)**

The map \( \phi_a : G \rightarrow G \) defined by
\[
\phi_a(g) = aga^{-1}
\]
is an automorphism of \( G \)

**Pf:** (one-to-one) Suppose \( \phi_a(x) = \phi_a(y) \). Then
\[
x \cdot a \cdot a^{-1} = \phi_a(x) = \phi_a(y) = y \cdot a \cdot a^{-1}
\]
By applying left and right cancellation laws we obtain \( x = y \)

(onto) For any \( x \in G \) we have
\[
\phi_a(a^{-1}xa) = a(a^{-1}xa)a^{-1} = (aa^{-1})x(aa^{-1}) = exe = x
\]
(preserves group operation) For any \( x, y \in G \)
\[
\phi_a(xy) = axya^{-1} = axeya^{-1} = axey(ay)a^{-1} = \phi_a(x) \phi_a(y)
\]

**Defn:** The function \( \phi_a \) is called the **inner automorphism** of \( G \) induced by \( a \). We define
\[
\text{Inn}(G) = \{ \phi_a : a \in G \} \subseteq \text{Aut}(G)
\]

**Thm 6.4:** \( \text{Aut}(G) \) and \( \text{Inn}(G) \) are groups under the operation of composition of functions

**Pf for \( \text{Aut}(G) \):** (Associativity) Composition of functions is always associative

(Identity) The identity map from \( G \) to \( G \) is an automorphism

(Involution) If \( \phi : G \rightarrow G \) is an automorphism of \( G \), then so is \( \phi^{-1} \). \( \Box \)
Thm 6.5: For all $n > 0$, $\text{Aut}(\mathbb{Z}_n) \cong \mathbb{U}(n)$

PF: Define $T: \text{Aut}(\mathbb{Z}_n) \rightarrow \mathbb{U}(n)$ by $T(\alpha) = \alpha(1)$.

Note: If $\alpha \in \text{Aut}(\mathbb{Z}_n)$ then (by Thm 6.2(b))

$\mathbb{Z}_n = \langle \alpha(1) \rangle$ since $\mathbb{Z}_n = \langle 1 \rangle$. So by

Cor. 4 of Thm 4.2 gcd($n, \alpha(1)$) = 1

and hence $\alpha(1) \in \mathbb{U}(n)$. So $T$ maps to $\mathbb{U}(n)$

($T$ is one-to-one) Suppose $T(\alpha) = T(\beta)$ for some $\alpha, \beta \in \text{Aut}(\mathbb{Z}_n)$. Then $\alpha(1) = T(\alpha) = T(\beta) = \beta(1)$.

By Thm 6.2(c) for every $k \in \mathbb{Z}_n$ we have

$\alpha(k) = \alpha(1+1+\cdots+1) = \alpha(1)+\alpha(1)+\cdots+\alpha(1)$

$\alpha(k) = \beta(1)+\beta(1)+\cdots+\beta(1) = \beta(1+1+\cdots+1) = \beta(k)$

Therefore $\alpha = \beta$.

($T$ is onto) Consider any $r \in \mathbb{U}(n)$. Let $s \in \mathbb{U}(n)$ be the inverse of $r$.

Define $\alpha: \mathbb{Z}_n \rightarrow \mathbb{Z}_n$ by $\alpha(k) = rk \text{ mod } n$. Then $\alpha \in \text{Aut}(\mathbb{Z}_n)$ since:

(o one-to-one) if $\alpha(k) = \alpha(m)$ then $rk \text{ mod } n = rm \text{ mod } n$ so

$k = 1 \cdot k \text{ mod } n = (sr)k \text{ mod } n = s(rk) \text{ mod } n$

$s(rkm) = (sr)k \text{ mod } n = 1 \cdot km = m$

(o onto) for any $k \in \mathbb{Z}_n$ we have

$\alpha(srk \text{ mod } n) = rsk \text{ mod } n = 1 \cdot k \text{ mod } n = k$

($\alpha$ preserves group op.)

$\alpha(k+m) = r(k+m) \text{ mod } n = (rk \text{ mod } n) + (rm \text{ mod } n) = \alpha(k) + \alpha(m)$

Clearly, $T(\alpha) = r(1) = r$. 

(T preserves group operation) If $\alpha, \beta \in \text{Aut}(\mathbb{Z}_n)$ then

\[
T(\alpha \beta)(n) = (\alpha \beta)(\alpha(n)) = \alpha(\beta(n)) = \alpha\left(\frac{n}{1+\frac{1}{\beta(n)}}\right)
\]

\[
= \alpha(n) + \alpha(1) + \cdots + \alpha(1) = \alpha(n) = T(\alpha)T(\beta)
\]