Chapter 6

Defn An <u>isomorphism</u> 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

(*) $\forall a,b \in G \quad \underbrace{\phi(ab)}_{\text{binary operation for } G} = \underbrace{\phi(a)\phi(b)}_{\text{binary operation for } \overline{G}}$

If there is an isomorphism from G onto $\overline{G}$, we say G and $\overline{G}$ are isomorphic and write $G \approx \overline{G}$

<u>Note</u>:
- If the 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.

<u>Ex</u>: Let G be a group and $a \in G$

① If a has infinite order then $\langle a \rangle \approx \mathbb{Z}$ since the map $\phi(a^k) = k$ is a bijection and $\phi(a^k a^m) = \phi(a^{k+m}) = k+m = \phi(a^k)+\phi(a^m)$

② If a has order n then $\langle a \rangle \approx \mathbb{Z}_n$ since the function $\phi: \langle a \rangle \to \mathbb{Z}_n$ given by $\phi(a^k) = k \bmod n$ is one-to-one and onto and (by Thm 4.1) if $j = k+m \bmod n$

then $\phi(a^k a^m) = \phi(a^{k+m}) = k+m \bmod n$

$= (k \bmod n) + (m \bmod n)$

binary operation in $\mathbb{Z}_n$

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

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 = Euler's constant $= 2.71\ldots$)

- ϕ is one-to-one because if $x \neq y$, say $x < y$, then $e^x < e^y$ so $e^x \neq e^y$
- ϕ is onto since for every $y \in (0, \infty)$ we have $\phi(\ln y) = e^{\ln y} = y$
- ϕ 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

$$gx = T_g(x) = T_g(y) = gy$$

and by left-cancellation $x = y$.
(Onto) Consider any $y \in G$. Setting $x = g^{-1}y$ we have

$$T_g(x) = gx = g(g^{-1}y) = (gg^{-1})y = ey = y \quad \square \text{(Claim 1)}$$

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

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

Claim 2: ϕ is one-to-one and onto

The definition of $\overline{G}$ shows ϕ 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 ϕ 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 $\phi(g)\phi(h)$ 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

$$\phi(gh)(x) = T_{gh}(x) = ghx$$
$$= g(hx) = T_g(hx) = T_g(T_h(x))$$
$$= (T_g T_h)(x)$$
$$= (\phi(g)\phi(h))(x)$$

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

<u>Claim 4</u>: $\overline{G}$ is a subgroup of the group of permutations of G

We'll apply Two-Step Subgroup Test.
We have $T_e \in \overline{G}$ so $\overline{G} \neq \emptyset$.

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

Lastly, consider any $T_g \in \overline{G}$. Then $T_{g^{-1}} \in \overline{G}$ 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 $\square$ (Claim 4)

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

Thm 6.2 If ϕ is an isomorphism from G onto $\overline{G}$ then

1. ϕ 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. $a, b \in G$ commute $\Leftrightarrow$ $\phi(a), \phi(b)$ commute
4. $G = \langle a \rangle \Leftrightarrow \overline{G} = \langle \phi(a) \rangle$
5. (order of a) = (order of $\phi(a)$) for all $a \in G$
6. (# solutions of $x^k = b$ in G) = (# solutions of $x^k = \phi(b)$ in $\overline{G}$)
7. G and $\overline{G}$ have exactly the same number of elements of every order

Pf: ① $\bar{e}\phi(e) = \phi(e) = \phi(ee) = \phi(e)\phi(e)$

since $\bar{e}$ identity in $\overline{G}$; since $e = ee$; since ϕ preserves group operation

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

② $\phi(a^{-1})\phi(a) = \phi(a^{-1}a) = \phi(e) \overset{①}{=} \bar{e}$

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

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

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

Can continue by induction.

③ HW 6

④ ($\Rightarrow$) ϕ is onto so $\overline{G} = \phi(G) = \phi(\langle a \rangle) = \phi(\{a^n : n \in \mathbb{Z}\}) \overset{②}{=} \{\phi(a)^n : n \in \mathbb{Z}\} = \langle \phi(a) \rangle$

($\Leftarrow$) $\phi(\langle a\rangle) = \{\phi(a^n) : n\in\mathbb{Z}\} \overset{2}{=} \{\phi(a)^n : n\in\mathbb{Z}\} = \langle\phi(a)\rangle = \bar{G}$

Since ϕ 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 $\square$

Thm 6.3: If ϕ is an isomorphism from G onto $\bar{G}$ then:

① ϕ^{-1} is an isomorphism from $\bar{G}$ onto G

② G abelian $\Leftrightarrow$ $\bar{G}$ abelian

③ G cyclic $\Leftrightarrow$ $\bar{G}$ cyclic

④ K a subgroup of G $\Rightarrow$ $\phi(K)$ a subgroup of $\bar{G}$

⑤ $\bar{K}$ a subgroup of $\bar{G}$ $\Rightarrow$ K subgroup of G

⑥ $\phi(Z(G)) = Z(\bar{G})$

Pf: ① exercise

② By ③ of previous Thm

③ By ④ of previous Thm

④ exercise (HW 6?)

⑤ follows from ① and ④

⑥ By ③ of previous Thm $\square$

Defn 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: $\phi:\mathbb{Z}\to\mathbb{Z}$ defined by $\phi(k) = -k$ is an automorphism of $\mathbb{Z}$.

~~Defn~~ **Lemma**: Let G be a group and $a \in G$. The map $\phi_a : G \to G$ defined by
$$\phi_a(g) = aga^{-1}$$
is an automorphism of G

Pf: (one-to-one) Suppose $\phi_a(x) = \phi_a(y)$. Then
$$axa^{-1} = \phi_a(x) = \phi_a(y) = aya^{-1}$$
By applying left and right cancelation 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 $x, y \in G$
$$\phi_a(xy) = axya^{-1} = axeya^{-1} = (axa^{-1})(aya^{-1}) = \phi_a(x)\phi_a(y)$$
$\square$

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

Thm 6.4: $Aut(G)$ and $Inn(G)$ are groups under the operation of composition of functions

Pf for $Aut(G)$: (Associativity) Composition of functions is always associative

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

(Inverses) If $\phi : G \to G$ is an automorphism of G, then so is ϕ^{-1}. $\square$

Thm 6.5: For all $n>0$, $Aut(\mathbb{Z}_n) \approx U(n)$

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

Note: If $\alpha \in Aut(\mathbb{Z}_n)$ then (by Thm 6.2 ④) $\mathbb{Z}_n = \langle \alpha(1) \rangle$ since $\mathbb{Z}_n = \langle 1 \rangle$. So by Cor. 4 of Thm 4.2 $\gcd(n, \alpha(1)) = 1$ and hence $\alpha(1) \in U(n)$. So T maps to $U(n)$

(T is one-to-one) Suppose $T(\alpha) = T(\beta)$ for some $\alpha, \beta \in Aut(\mathbb{Z}_n)$. Then $\alpha(1) = T(\alpha) = T(\beta) = \beta(1)$. By Thm 6.2 ② for every $k \in \mathbb{Z}_n$ we have

$$\alpha(k) = \alpha(\underbrace{1+1+\cdots+1}_{k}) = \alpha(1)+\alpha(1)+\cdots+\alpha(1)$$
$$= \beta(1)+\beta(1)+\cdots+\beta(1) = \beta(\overbrace{1+1+\cdots+1}^{k}) = \beta(k)$$

Therefore $\alpha = \beta$.

(T is onto) Consider any $r \in U(n)$. Let $s \in U(n)$ be the inverse of r. Define $\alpha: \mathbb{Z}_n \to \mathbb{Z}_n$ by $\alpha(k) = rk \bmod n$. Then $\alpha \in Aut(\mathbb{Z}_n)$ since:

(α one-to-one) if $\alpha(k) = \alpha(m)$ then $rk \bmod n = rm \bmod n$ so

$$k = 1\cdot k \bmod n = (sr)k \bmod n = s(rk) \bmod n$$
$$= s(rm) \bmod n = (sr)m \bmod n = 1\cdot m \bmod n = m$$

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

$$\alpha(sk \bmod n) = rsk \bmod n = 1\cdot k \bmod n = k$$

(α preserves group op.)

addition in $\mathbb{Z}_n$

$$\alpha(k+m) = r(k+m) \bmod n = (rk \bmod n) + (rm \bmod n) = \alpha(k) + \alpha(m)$$

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

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

$$T(\alpha\beta) = (\alpha\beta)(1) = \alpha(\beta(1)) = \alpha(\underbrace{1 + 1 + \cdots + 1}_{\beta(1)}) = \overbrace{\alpha(1) + \alpha(1) + \cdots + \alpha(1)}^{\beta(1)} = \alpha(1)\beta(1) = T(\alpha)T(\beta) \quad \square$$