§ 7 - Homomorphisms & Isomorphisms

Throughout the course we have been interested in studying the structure of various groups G. In this section we will build a framework for deciding when the structures of two groups are identical.

Consider the groups $\mathbb{Z}_4 = \{0, 1, 2, 3\}$ and $\mathbb{Z}_8^* = \{1, 3, 5, 7\}$. On the surface these groups look different, but even at a structural level there are many ways to tell them apart:

- $\mathbb{Z}_4$ is cyclic; $\mathbb{Z}_8^*$ is not.
- $\mathbb{Z}_4$ has two elements of order 2; $\mathbb{Z}_8^*$ has three.

- $\mathbb{Z}_4$ has only one subgroup of order 2; $\mathbb{Z}_8^*$ has three

On the other hand, consider $\mathbb{Z}_4$ and $\mathbb{Z}_{10}^* = \{1,3,7,9\}$.

The elements may look different, but the structures are very similar:

- The groups are both cyclic of order 4.
- The groups have the same number of elements of any given order.
- The groups have the same subgroup structure.

Aside from how we label the elements, are there any differences between these groups structurally?

NO! The group structures are identical.

How could one prove this rigorously? First, we would need a way to "relabel" the elements in $\mathbb{Z}_4$ to elements in $\mathbb{Z}_{10}^*$. This can be accomplished by a bijection $\varphi : \mathbb{Z}_4 \longrightarrow \mathbb{Z}_{10}^*$.

Of course, a bijection is not enough! We need to relabel in a way that preserves the group structure of $\mathbb{Z}_4$. Specifically, we want the elements to multiply the same way both before and after relabelling. We need

$$\boxed{\varphi(a+b) = \varphi(a)\varphi(b) \quad \forall a,b \in \mathbb{Z}_4.}$$

In our case we can take $\varphi : \mathbb{Z}_4 \to \mathbb{Z}_{10}^*$

$\varphi(0) = 1$, $\varphi(1) = 3$, $\varphi(2) = 9$, $\varphi(3) = 7$.

This φ is bijective and preserves the group structure of $\mathbb{Z}_4$. For example:

$$\begin{cases} \varphi(1+2) = \varphi(3) = 7 \\ \varphi(1)\varphi(2) = 3 \cdot 9 = 7 \end{cases}$$

§7.1 - Definitions, Properties, & First Examples

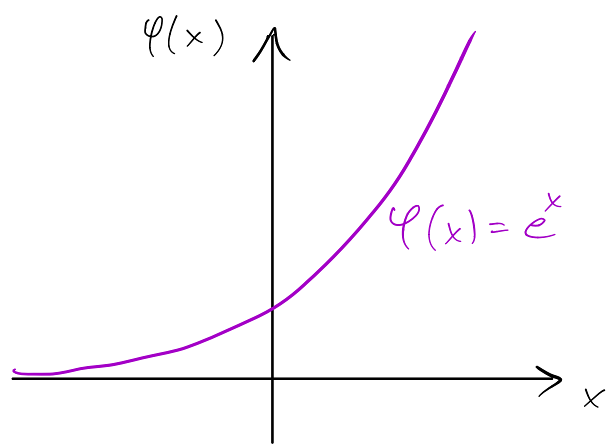
Definition: Let $(G, \cdot)$, $(H, *)$ be groups. A function $\varphi : G \longrightarrow H$ satisfying

$$\boxed{\varphi(a \cdot b) = \varphi(a) * \varphi(b) \quad \forall a, b \in G}$$

is called a (group) homomorphism. A homomorphism that is also bijective is called an isomorphism. If there is an isomorphism $\varphi: G \to H$, we say that G and H are isomorphic and we write $\boxed{G \cong H.}$

Ex 1: Consider the groups $(\mathbb{R}, +)$ and $(\mathbb{R}_{>0}, \cdot)$ where $\mathbb{R}_{>0} = \{x \in \mathbb{R} : x > 0\}$.

We know from Calculus that the function $\varphi: \mathbb{R} \to \mathbb{R}_{>0}$ given by $\varphi(a) = e^a$ is bijective (prove this!)



Also

$$\varphi(x+y) = e^{x+y} = e^x e^y = \varphi(x)\varphi(y),$$

So φ is a homomorphism. Consequently, φ is an isomorphism, so $(\mathbb{R},+) \cong (\mathbb{R}_{>0},\cdot)$.

For our next two examples, it will be helpful to recall the following result from §2.

Lemma 2.1: Let a be a group element.

(i) If $|a| = \infty$, then $\forall i,j \in \mathbb{Z}$, $a^i = a^j \Leftrightarrow i = j$

(ii) If $|a| = n < \infty$, then $\forall i,j \in \mathbb{Z}$, $a^i = a^j \Leftrightarrow n \mid (i-j)$

Ex 2: If $G = \langle a \rangle$ is an infinite cyclic group, then $G \cong \mathbb{Z}$. Indeed, consider the function $\varphi : \mathbb{Z} \longrightarrow G$ given by $\varphi(k) = a^k$.

Clearly φ is surjective, as

$$G = \langle a \rangle = \{a^k : k \in \mathbb{Z}\}.$$

Moreover, since

$$\varphi(k) = \varphi(m) \iff a^k = a^m$$
$$\iff k = m \quad (\text{Lemma } 2.1\ (i))$$

we have that φ is injective.

Finally, $\varphi(k+m) = a^{k+m} = a^k a^m = \varphi(k)\varphi(m)$

for all $k, m \in \mathbb{Z}$, so φ is a homomorphism.

Thus, φ is an isomorphism, so $\boxed{G \cong \mathbb{Z}.}$

Ex 3: If $G = \langle a \rangle = \{e, a, a^2, \ldots, a^{n-1}\}$ is a cyclic group of order $n < \infty$, then $G \cong \mathbb{Z}_n$.

Indeed, consider the map $\varphi : \mathbb{Z}_n \longrightarrow G$ given by $\varphi(k) = a^k$. As before, φ is surjective, and we can use Lemma 2.1 (ii) to show that φ is injective:

$$\varphi(k) = \varphi(m) \iff a^k = a^m$$
$$\iff n \mid (k-m)$$
$$\iff k = m \mod n$$
$$\iff k = m \text{ in } \mathbb{Z}_n.$$

The same proof in Ex 2. shows that φ is a homomorphism. We conclude that φ is an isomorphism, so $G \cong \mathbb{Z}_n$.

Consequences:

- $\mathbb{Z}_{18}^*$ is a cyclic group of order 6, so $\mathbb{Z}_{18}^* \cong \mathbb{Z}_6$.
- The group of n^{th} roots of unity in $\mathbb{C}^*$ is a

cyclic group of order n and hence $\cong \mathbb{Z}_n$.

- $3\mathbb{Z}$ is an infinite cyclic group, so $3\mathbb{Z} \cong \mathbb{Z}$.

(in fact, $n\mathbb{Z} \cong \mathbb{Z}$ for all $n \in \mathbb{Z} \setminus \{0\}$.)

Let us now investigate some of the properties of group isomorphisms.

Proposition 7.1: Let G, H, K be groups.

(i) If $G \cong H$ then $H \cong G$.

[In fact, if $\varphi : G \longrightarrow H$ is an isomorphism, then $\varphi^{-1} : H \longrightarrow G$ is also an isomorphism.]

(ii) If $G \cong H$ and $H \cong K$, then $G \cong K$.

Proof: (i) Let $\varphi: G \longrightarrow H$ be an isomorphism.

As an exercise, prove that $\varphi^{-1}: H \longrightarrow G$ is bijective. To see that φ is a homomorphism, let $h_1, h_2 \in H$, and choose $g_1, g_2 \in G$ such that $\varphi(g_1) = h_1$ and $\varphi(g_2) = h_2$. Thus, $\varphi^{-1}(h_i) = g_i$.

Note that since $\varphi(g_1 g_2) = \varphi(g_1)\varphi(g_2) = h_1 h_2$, we have $\varphi^{-1}(h_1 h_2) = g_1 g_2 = \varphi^{-1}(h_1)\varphi^{-1}(h_2)$.

$\therefore \varphi$ is a homomorphism (and hence an isomorphism)

(ii) Let $\varphi: G \rightarrow H$ and $\psi: H \longrightarrow K$ be isomorphisms. Then $\psi \circ \varphi: G \longrightarrow K$ is bijective (proven on A1) and a homomorphism.

Indeed, for if $g_1, g_2 \in G$, then

$$(\psi \circ \varphi)(g_1 g_2) = \psi(\varphi(g_1 g_2))$$
$$= \psi(\varphi(g_1)\varphi(g_2))$$
$$= \psi(\varphi(g_1))\psi(\varphi(g_2))$$
$$= (\psi \circ \varphi)(g_1)(\psi \circ \varphi)(g_2) \quad \blacksquare$$

Theorem 7.2 [Properties of Isomorphisms]

Let G, H be groups with identities e, e', respectively, and $\varphi : G \longrightarrow H$ a group isomorphism.

[Element Properties] Let $a, b \in G$.

1. $\varphi(e) = e'$
2. $\varphi(a^{-1}) = [\varphi(a)]^{-1}$
3. For all $n \in \mathbb{Z}$, $\varphi(a^n) = [\varphi(a)]^n$.
4. a, b commute $\iff$ $\varphi(a), \varphi(b)$ commute.

5. $|a| = |\varphi(a)|$

[Group Properties]

6. G is Abelian $\Longleftrightarrow$ H is Abelian.

7. G is cyclic $\Longleftrightarrow$ H is cyclic.

8. If $K \leq G$, then $\varphi(K) \leq H$.

9. $\varphi(Z(G)) = Z(H)$.

Proof:

1. $\varphi(e) = \varphi(ee) = \varphi(e)\varphi(e)$

$\Rightarrow \varphi(e) = e'$ by cancellation.

2. $aa^{-1} = e \Rightarrow \varphi(aa^{-1}) = \varphi(e) = e'$

$\Rightarrow \varphi(a)\varphi(a^{-1}) = e'$

$\Rightarrow \varphi(a)^{-1} = \varphi(a^{-1})$.

3. If $n=0 \Rightarrow$ done by 1.

If $n>0 \Rightarrow \varphi(a^n) = \varphi(a \cdot a \cdot \cdots a)$

$$= \varphi(a)\varphi(a) \cdots \varphi(a)$$

$$= [\varphi(a)]^n$$

If $n<0 \Rightarrow \varphi(a^n a^{-n}) = \varphi(e) = e'$

$$\Rightarrow \varphi(a^n)\varphi(a^{-n}) = e'$$

$$\Rightarrow \varphi(a^n)[\varphi(a)]^{-n} = e' \quad (\text{as } -n>0)$$

$\cdot\ [\varphi(a)]^n$

$$\Rightarrow \varphi(a^n) = [\varphi(a)]^n$$

4. If $ab = ba$ then

$$\varphi(a)\varphi(b) = \varphi(ab) = \varphi(ba) = \varphi(b)\varphi(a).$$

The reverse direction can be argued the same way using the isomorphism $\varphi^{-1}: H \to G$.

5. Note that $a^n = e \iff \varphi(a^n) = \varphi(e)$

$$\iff [\varphi(a)]^n = e'$$

So $a^n = e \iff [\varphi(a)]^n = e'$, and hence the smallest $n > 0$ making these equations true (if it exists) is the same for both.

i.e., $|a| = |\varphi(a)|$.

6. Follows immediately from 4.

7. Exercise.

8. Exercise.

9. Follows immediately from 4. ∎

Remark: Understanding what properties must be satisfied by an isomorphism is helpful when showing that two groups are NOT isomorphic.

Ex: $(\mathbb{Z},+) \not\cong (\mathbb{Q},+)$ ($\mathbb{Z}$ cyclic, $\mathbb{Q}$ not)

Ex: $(\mathbb{Q},+) \not\cong (\mathbb{Q}^*,\cdot)$ ($-1 \in \mathbb{Q}^*$ has order 2, but $\mathbb{Q}$ doesn't have any elements of order 2).

Homomorphisms

An isomorphism $\varphi: G \longrightarrow H$ preserves the group structure of G exactly. On the other hand, homomorphisms preserve some of the group structure, but perhaps not all of it.

Ex 1: Consider the map $\varphi: \mathbb{Z} \longrightarrow \mathbb{Z}_2$

$$n \longmapsto n \bmod 2.$$

This φ is a homomorphism:

$$\begin{aligned}\varphi(m+n) &= (m+n) \bmod 2 \\ &= (m \bmod 2) + (n \bmod 2) \\ &= \varphi(m) + \varphi(n)\end{aligned}$$

But φ is not an isomorphism, as it is not injective $(\varphi(0) = \varphi(2) = 0)$

Under this homomorphism, all even integers are collapsed to 0, while all odd integers are collapsed to 1.

Essentially, φ forgets everything about $\mathbb{Z}$

except "even vs. odd".

We measure the amount of group structure lost through a homomorphism by the size of its kernel.

Definition: If $\varphi : G \longrightarrow H$ is a group homomorphism, we define the kernel of φ to be the set

$$\boxed{\mathrm{Ker}(\varphi) = \{a \in G \mid \varphi(a) = e\}.}$$

In Ex 1, $\mathrm{Ker}\,\varphi = \{n \in \mathbb{Z} : n \bmod 2 = 0\}$

$$= 2\mathbb{Z}$$

It is also interesting to ask how much of H exhibits structure similar to G.

Definition: If $\varphi : G \to H$ is a group homomorphism, we define the image of φ to be the set

$$\boxed{\operatorname{im}(\varphi) = \varphi(G) = \{\varphi(a) : a \in G\}}.$$

In Ex 1, $\operatorname{im}(\varphi) = \{\varphi(n) : n \in \mathbb{Z}\}$

$$= \{n \bmod 2 : n \in \mathbb{Z}\} = \mathbb{Z}_2.$$

Ex 2: If $\varphi : G \longrightarrow H$ is a group isomorphism, then φ is a homomorphism with $\mathrm{Ker}(\varphi) = \{e\}$ and $\mathrm{im}(\varphi) = H$.

Ex 3: If $\varphi : G \longrightarrow H$ is given by $\varphi(a) = e$ for all $a \in G$, then φ is a homomorphism with $\mathrm{Ker}(\varphi) = G$, $\mathrm{im}(\varphi) = \{e\}$. We call φ the trivial homomorphism.

Ex 4: The absolute value function $|\cdot| : \mathbb{R}^* \longrightarrow \mathbb{R}^*$ is a homomorphism as $|ab| = |a||b|$. The kernel is $\{\pm 1\}$ and the image is $\mathbb{R}_{>0}$.

Ex 5: $\mathrm{sgn} : S_n \longrightarrow \mathbb{Z}_2$ given by

$$\mathrm{sgn}(\sigma) = \begin{cases} 0 & \text{if } \sigma \text{ even} \\ 1 & \text{if } \sigma \text{ odd} \end{cases}$$

is a group homomorphism:

$$\mathrm{sgn}(\sigma\tau) = \begin{cases} 0 & \text{if } \sigma\tau \text{ even} \\ 1 & \text{if } \sigma\tau \text{ odd} \end{cases}$$

$$= \begin{cases} 0 & \text{if } \mathrm{sgn}(\sigma) = \mathrm{sgn}(\tau) = 0 \text{ or} \\ & \quad \mathrm{sgn}(\sigma) = \mathrm{sgn}(\tau) = 1 \\ 1 & \text{if } \mathrm{sgn}(\sigma) = 0,\ \mathrm{sgn}(\tau) = 1 \text{ or} \\ & \quad \mathrm{sgn}(\tau) = 0,\ \mathrm{sgn}(\sigma) = 1. \end{cases}$$

$$= \mathrm{sgn}(\sigma) + \mathrm{sgn}(\tau).$$

We have $\mathrm{Ker}(\varphi) = A_n$, $\mathrm{im}(\varphi) = \mathbb{Z}_2$.

Ex 6: Vector spaces V and W are groups under addition, and a homomorphism $\varphi: V \longrightarrow W$ must satisfy

$$\varphi(v+v') = \varphi(v) + \varphi(v') \quad \forall v, v' \in V.$$

Thus, linear maps from V to W are homomorphisms. They are isomorphisms precisely when the corresponding matrix is non-singular.

Ex 7: The map $\varphi : \mathbb{R} \longrightarrow \mathbb{R}$ (under $+$) given by $\varphi(x) = x^2$ is NOT a homomorphism as $\varphi(x+y) = (x+y)^2 \neq x^2 + y^2 = \varphi(x) + \varphi(y)$.

Theorem 7.3 [Properties of Homomorphisms]

Let G and H be groups, $a, b \in G$, and $\varphi : G \longrightarrow H$ a homomorphism.

1. $\varphi(e) = e$

2. $\varphi(a^n) = [\varphi(a)]^n$ for all $n \in \mathbb{Z}$

   (In particular, $\varphi(a^{-1}) = [\varphi(a)]^{-1}$)

3. If $|a| < \infty$ then $|\varphi(a)|$ divides $|a|$.

4. $\operatorname{Ker} \varphi \trianglelefteq G$

5. $\varphi(a) = \varphi(b) \iff a \operatorname{Ker} \varphi = b \operatorname{Ker} \varphi$.

6. φ is injective $\iff \operatorname{Ker} \varphi = \{e\}$.

7. $\operatorname{im} \varphi \leq H$

8. φ is surjective $\iff \operatorname{im}(\varphi) = H$.

Proof: The arguments for 1. and 2. are the same as in Theorem 7.2.

3. If $|a| = n < \infty$, then

$$[\varphi(a)]^n = \varphi(a^n) = \varphi(e) = e$$

so $|\varphi(a)|$ divides $n = |a|$.

4. Exercise

5. Note that

$$\varphi(a) = \varphi(b) \iff \varphi(a)^{-1}\varphi(b) = e$$
$$\iff \varphi(a^{-1}b) = e$$
$$\iff a^{-1}b \in \operatorname{Ker}\varphi$$
$$\iff a \operatorname{Ker}\varphi = b \operatorname{Ker}\varphi.$$

6. Follows immediately from 7.

7. Exercise.

8. Obvious. $\blacksquare$

Just like in the case of isomorphisms, understanding the properties of homomorphisms helps us to determine what homomorphisms can exist between groups G and H.

Ex: How many homomorphisms are there from $\mathbb{Z}_8$ to $\mathbb{Z}_6$?

Note that since $\mathbb{Z}_8$ is cyclic, any homomorphism $\varphi: \mathbb{Z}_8 \to \mathbb{Z}_6$ will be completely determined by $\varphi(1)$:

Given $k \in \mathbb{Z}_8$, $\varphi(k) = \underbrace{\varphi(1) + \varphi(1) + \cdots + \varphi(1)}_{k \text{ times}}$

$= k\varphi(1)$

What do we know about $\varphi(1)$? Well, its order must divide $|1| = 8$ by property 3. Also, $\varphi(1) \in \mathbb{Z}_6$, so by Lagrange, $|\varphi(1)|$ divides $|\mathbb{Z}_6| = 6$.

$\therefore |\varphi(1)|$ divides $\gcd(8,6) = 2$

$\Rightarrow |\varphi(1)| = 1$ or 2.

If $|\varphi(1)| = 1$, then $\varphi(1) = 0$ and hence φ is the trivial homomorphism.

If $|\varphi(1)| = 2$, then $\varphi(1) = 3$ and hence $\varphi(k) = 3k \bmod 6$ for $k \in \mathbb{Z}$.

These conditions on $\varphi: \mathbb{Z}_8 \to \mathbb{Z}_6$ are necessary, but are they sufficient? In particular, is $\varphi(k) = 3k \bmod 6$ really a homomorphism?

Clearly
$$\varphi(k+m) = 3(k+m) \bmod 6$$
$$= (3k \bmod 6) + (3m \bmod 6)$$
$$= \varphi(k) + \varphi(m),$$

but is this function even well-defined? If $k \equiv m \bmod 8$, then $8 \mid k-m$ so $k = m + 8t$ for some $t \in \mathbb{Z}$. Thus,
$$\varphi(k) = \varphi(m+8t)$$
$$= 3(m+8t) \bmod 6$$

$$= 3m + \underbrace{24t}_{=0 \bmod 6} \mod 6$$

$$= 3m \mod 6 \quad = \varphi(m). \qquad \text{Yes!}$$

Something like $\psi : \mathbb{Z}_8 \to \mathbb{Z}_6$ given by $\psi(k) = 2k \mod 6$, however, is not:

e.g. $1 = 9 \mod 8$, but

$$\left.\begin{aligned} \psi(1) &= 2 \mod 6 \\ \psi(9) &= 18 = 0 \mod 6 \end{aligned}\right\} \text{different.}$$

Thus, ψ is not a well-defined map, so it isn't a homomorphism.

This begs the question:

What are the homomorphisms $\varphi : \mathbb{Z}_n \to \mathbb{Z}_m$?

1. All homomorphisms $\varphi: \mathbb{Z}_n \longrightarrow \mathbb{Z}_m$ must be of the form $\varphi(x) = ax$ where $a = \varphi(1)$.

2. Every such φ satisfies the homomorphism property: $\varphi(x+y) = \varphi(x) + \varphi(y)$.

3. Which of these φ's are well-defined?

Necessary: $0 = \varphi(0) = \varphi(n) = an$, so

$$an = 0 \mod m.$$

Exercise: Prove that this condition is sufficient. That is, $\varphi: \mathbb{Z}_n \longrightarrow \mathbb{Z}_m$ is given by $\varphi(x) = ax$ is well-defined if and only if $an \equiv 0 \mod m$.

Remark: If $\varphi : G \longrightarrow H$ is a group homomorphism, then $\operatorname{Ker}\varphi \trianglelefteq G$ (Theorem 7.3). It turns out that every normal subgroup arises in this way!

Theorem 7.4: Let G be a group and $N \trianglelefteq G$. Then there is a group H and homomorphism $\varphi : G \longrightarrow H$ such that $N = \operatorname{Ker}\varphi$.

Proof: Define $H = G/N$ and $\varphi : G \longrightarrow G/N$ by $\varphi(a) = aN$. Then φ is a homomorphism and $\operatorname{Ker}\varphi = N$. ■

§7.2 - Isomorphism Theorems

In this section we will use our basic understanding of homomorphisms and isomorphisms to prove some strong structural results.

1. The First Isomorphism Theorem (The big one!)

Suppose that $\varphi : G \longrightarrow H$ is a group homomorphism, but perhaps not an isomorphism. The map φ may fail to be an isomorphism because it is (a) not surjective, or

(b) not injective.

Are there some simple changes that can be made to G and H to turn φ into an isomorphism?

To make φ surjective, let's replace H with $\text{im}(\varphi)$ (i.e., remove the extra parts of H)

To make φ injective, let's replace G with $G/\text{Ker}\,\varphi$ (i.e., collapse the kernel to a point)

The resulting map is an isomorphism from $G/\text{Ker}\,\varphi$ to $\text{im}(\varphi)$!

<u>Theorem 7.5</u> (First Isomorphism Theorem):

If $\varphi : G \longrightarrow H$ is a group homomorphism, then $G/\text{Ker}\,\varphi \cong \text{im}(\varphi)$.

Proof: Define $\psi : G/\ker\varphi \longrightarrow \mathrm{im}(\varphi)$ by

$$\psi(a\cdot \ker\varphi) = \varphi(a).$$

Claim: ψ is an isomorphism.

Note that

$$\psi(a\cdot\ker\varphi) = \psi(b\cdot\ker\varphi) \iff \varphi(a) = \varphi(b)$$

$$\iff a\ker\varphi = b\ker\varphi$$

Thus, ψ is well-defined and injective.

We have that $\mathrm{im}(\psi) = \{\psi(a\cdot\ker\varphi) : a \in G\}$

$$= \{\varphi(a) : a\in G\} = \mathrm{im}(\varphi),$$

so ψ is surjective. Finally,

$$\psi((a\cdot\ker\varphi)(b\cdot\ker\varphi)) = \psi(ab\ker\varphi)$$

$$= \varphi(ab)$$

$$= \varphi(a)\varphi(b)$$

$$= \psi(a \cdot \ker\varphi) \cdot \psi(b \cdot \ker\varphi)$$

Thus, ψ is a homomorphism. We conclude that ψ is an isomorphism, so $G/\ker\varphi \cong \mathrm{im}(\varphi)$ $\blacksquare$

Ex 1: The absolute value function $|\cdot| : \mathbb{R}^* \longrightarrow \mathbb{R}^*$ is a homomorphism with kernel $\{\pm 1\}$ and image $\mathbb{R}_{>0} = \{x \in \mathbb{R} : x > 0\}$. By the First Isomorphism Theorem, $\boxed{\mathbb{R}^*/\{\pm 1\} \cong \mathbb{R}_{>0}.}$

Ex 2:
$$\mathrm{sgn} : S_n \longrightarrow \mathbb{Z}_2$$
$$\sigma \longmapsto \begin{cases} 0 & \text{if } \sigma \text{ odd} \\ 1 & \text{if } \sigma \text{ odd} \end{cases}$$

is a homomorphism with $\ker(\mathrm{sgn}) = A_n$ and $\mathrm{im}(\mathrm{sgn}) = \mathbb{Z}_2$. By the First

Isomorphism Theorem, $\boxed{S_n/A_n \cong \mathbb{Z}_2.}$

Suppose that G is a finite group. Together with Lagrange's Theorem, the First Isomorphism Theorem reveals the following exciting fact:

Corollary 7.6: Let G be a finite group, and suppose that $\varphi : G \longrightarrow H$ is a group homomorphism. Then $|G| = |\operatorname{Ker}\varphi| \cdot |\operatorname{im}\varphi|$.

Proof: By the First Isomorphism Theorem, $G/\operatorname{Ker}\varphi \cong \operatorname{im}\varphi$. Thus,

$$|\operatorname{im}\varphi| = |G/\operatorname{Ker}\varphi| = |G|/|\operatorname{Ker}\varphi| \qquad \blacksquare$$

Ex: By Example 1 above, $|S_n| = |A_n| \cdot |\mathbb{Z}_2|$.

This means that $n! = |A_n| \cdot 2$, and hence we get a new proof that $|A_n| = n!/2$.

2. Correspondence Theorem

Let G be a group and $N \trianglelefteq G$. Here we investigate the connection between the subgroups of G/N and the subgroups of G.

First note that if $H \leq G$ and $N \subseteq H$, then $N \trianglelefteq H$ (verify). Thus, $H/N \leq G/N$. Indeed,

- $eN \in H/N$, so $H/N \neq \emptyset$
- If $h_1N, h_2N \in H/N$, then

$$h_1 N \cdot h_2 N = \underbrace{(h_1 h_2)}_{\in H} N \in H/N.$$

- If $hN \in H/N$, then

$$(hN)^{-1} = \underbrace{h^{-1}}_{\in H} N \in H/N.$$

Thus, $H/N \leq G/N$ by the subgroup test.

So, if $H \leq G$, then we get a subgroup H/N of G/N for free. But in fact, every subgroup of G/N arises in this way:

$$\boxed{\text{If } K \leq G/N, \text{ then } K = H/N \text{ for some } H \leq G \text{ with } N \subseteq H.}$$

You will prove this fact on Assignment 5.

Theorem 7.7 (Correspondence Theorem)

Let G be a group and $N \trianglelefteq G$. Then

$$\{K \leq G/N\} = \{H/N : H \leq G \text{ and } N \subseteq H\}.$$

Moreover, $H/N \subseteq H'/N \iff H \subseteq H'$.

<u>Ex:</u> The subgroups of S_n/A_n are given by H/A_n where $H \leq S_n$ and $A_n \subseteq H$. The only such H are $H = A_n$ or $H = S_n$ (for if $A_n \subsetneq H$, then $|H| > \frac{n!}{2}$, and hence $|H| = n!$ as $|H|$ divides $|S_n|$.)

Thus, the subgroups of S_n/A_n are

$A_n/A_n = \{A_n\}$ (trivial) and S_n/A_n (whole group)

This makes sense, as $S_n/A_n \cong \mathbb{Z}_2$ and the only subgroups of $\mathbb{Z}_2$ are $\{0\}$ and $\{0,1\} = \mathbb{Z}_2$.

When coupled with the First Isomorphism theorem, the correspondence theorem says the following:

$\boxed{\text{If } \varphi : G \longrightarrow H \text{ is a group homomorphism, then } G/\ker\varphi \cong \mathrm{im}(\varphi), \text{ and hence the subgroups of } \mathrm{im}(\varphi) \text{ are in bijection with the subgroups of } G \text{ containing } \ker\varphi.}$

§7.3 - Automorphisms

An isomorphism $\varphi : G \longrightarrow G$ is called an **automorphism** of G. The set of all automorphisms of G is denoted by $\underline{Aut(G)}$.

Ex 1: The identity automorphism $id : G \longrightarrow G$ is given by $\varphi(a) = a$ for all $a \in G$.

Ex 2: Consider the map $\varphi : \mathbb{C} \longrightarrow \mathbb{C}$ given by

$\varphi(z) = \overline{z}$ (i.e., $\varphi(a+ib) = \overline{a+ib} = a-ib$).

Then $\varphi \in Aut(\mathbb{C})$.

Ex 3: Let G be a group and fix some $a \in G$. Consider $\varphi_a : G \longrightarrow G$ given by $\varphi_a(b) = aba^{-1}$.

φ_a is called an inner automorphism of G, and the set of all inner automorphisms is denoted by $\mathrm{Inn}(G)$.

Remark: $\mathrm{Inn}(G) = \{id\} \iff G$ is Abelian

To see that φ_a is an automorphism, note that

$$\varphi_a(bc) = a(bc)a^{-1} = ab(a^{-1}a)ca^{-1}$$

$$= (aba^{-1})(aca^{-1}) = \varphi_a(b)\varphi_a(c),$$

and φ_a is bijective as it is left-multiplication by a and right-multiplication by a^{-1}.

For a concrete example, fix $S \in GL_n(\mathbb{R})$ and consider $\varphi_S : GL_n(\mathbb{R}) \longrightarrow GL_n(\mathbb{R})$. Then

$\varphi_s(A) = SAS^{-1}$ (similarity, i.e. change of basis!)

Remark: As the above example suggests, an automorphism of G should be viewed as a way to view G from a different perspective.

Theorem 7.8 Let G be a group. Then $\mathrm{Aut}(G)$ is a group under function composition and $\mathrm{Inn}(G) \trianglelefteq \mathrm{Aut}(G)$.

Proof: As an exercise, prove that $\mathrm{Aut}(G)$ is a group with identity $\mathrm{id} : G \longrightarrow G$.

Note that $\mathrm{id} = \varphi_e \in \mathrm{Inn}(G)$, so $\mathrm{Inn}(G) \neq \emptyset$.

If $\varphi_a, \varphi_b \in \mathrm{Inn}(G)$, then for all $x \in G$,

$$\varphi_a \varphi_b(x) = \varphi_a(bxb^{-1}) = a(bxb^{-1})a^{-1} = \varphi_{ab}(x)$$

so $\varphi_a \varphi_b = \varphi_{ab} \in \mathrm{Inn}(G)$. Finally, one can check that $\varphi_a^{-1} = \varphi_{a^{-1}} \in \mathrm{Inn}(G)$, so $\mathrm{Inn}(G) \leq \mathrm{Aut}(G)$ by the subgroup test.

To see that $\mathrm{Inn}(G) \trianglelefteq \mathrm{Aut}(G)$, let $\varphi_a \in \mathrm{Inn}(G)$ and $\psi \in \mathrm{Aut}(G)$. For $x \in G$, we have

$$\begin{aligned}(\psi \circ \varphi_a \circ \psi^{-1})(x) &= \psi(\varphi_a(\psi^{-1}(x))) \\ &= \psi(a\psi^{-1}(x)a^{-1}) \\ &= \psi(a)\,x\,\psi(a)^{-1} = \varphi_{\psi(a)}(x).\end{aligned}$$

Thus, $\psi \circ \varphi_a \circ \psi^{-1} = \varphi_{\psi(a)} \in \mathrm{Inn}(G)$, so $\psi\,\mathrm{Inn}(G)\,\psi^{-1} \subseteq \mathrm{Inn}(G)$ for all ψ. By the normal subgroup test, $\text{Inn}(G) \trianglelefteq \text{Aut}(G)$. ■

Let's see if we can compute $\text{Aut}(G)$ for a familiar family of groups: $\mathbb{Z}_n$

Ex: What is $\text{Aut}(\mathbb{Z}_6)$?

Note that if $\varphi \in \text{Aut}(\mathbb{Z}_6)$, then

$|\varphi(1)| = |1| = 6$, so $\varphi(1) = 1$ or 5.

Since
$$\varphi(k) = \varphi(\underbrace{1+1+\cdots+1}_{k \text{ times}})$$
$$= \underbrace{\varphi(1) + \varphi(1) + \cdots + \varphi(1)}_{k \text{ times}} = k\,\varphi(1),$$

it follows that for all $k \in \mathbb{Z}_6$,

$\underline{\varphi(k) = k \bmod 6}$ or $\underline{\varphi(k) = 5k \bmod 6}$

Both of these homomorphisms are well-defined, as $6 \cdot 1 = 0 \mod 6$ and $6 \cdot 5 = 0 \mod 6$.

Consequently, $\boxed{\mathrm{Aut}(\mathbb{Z}_6) = \left\{ \begin{array}{l} k \mapsto k \mod 6, \\ k \mapsto 5k \mod 6 \end{array} \right\}}$

Observe that the automorphisms of $\mathbb{Z}_6$ correspond to the elements $1, 5 \in \mathbb{Z}_6$ (i.e., the elements of $\mathbb{Z}_6^*$). This correspondence occurs for other n as well.

<u>Theorem 7.9</u>: For any integer $n \geq 2$,

$$\mathrm{Aut}(\mathbb{Z}_n) \cong \mathbb{Z}_n^*.$$

Proof: Define $\Psi : \text{Aut}(\mathbb{Z}_n) \longrightarrow \mathbb{Z}_n^*$ by $\Psi(\varphi) = \varphi(1)$. Note that since $|\varphi(1)| = |1| = n$ for any $\varphi \in \text{Aut}(\mathbb{Z}_n)$, it follows that $\varphi(1)$ is a generator for $\mathbb{Z}_n$ and hence $\varphi(1) \in \mathbb{Z}_n^*$. Thus, the codomain of Ψ is correct.

We will show that Ψ is an isomorphism. First, note that for $\varphi_1, \varphi_2 \in \text{Aut}(\mathbb{Z}_n)$,

$$\begin{aligned}
\Psi(\varphi_1\varphi_2) &= (\varphi_1\varphi_2)(1) \\
&= \varphi_1(\varphi_2(1)) \\
&= \varphi_1(\underbrace{1+1+\cdots+1}_{\varphi_2(1) \text{ times}})
\end{aligned}$$

$$= \underbrace{\varphi_1(1) + \varphi_1(1) + \cdots + \varphi_1(1)}_{\varphi_2(1) \text{ times}}$$

$$= \varphi_1(1)\,\varphi_2(1) \quad = \Psi(\varphi_1)\,\Psi(\varphi_2).$$

Consequently, Ψ is a homomorphism.

To see that Ψ is injective, suppose that

$\Psi(\varphi_1) = \Psi(\varphi_2)$, so $\varphi_1(1) = \varphi_2(1)$.

Then for any $k \in \mathbb{Z}_n$,

$$\varphi_1(k) = k\,\varphi_1(1) = k\,\varphi_2(1) = \varphi_2(k)$$

and hence $\varphi_1 = \varphi_2$. Thus, Ψ is injective.

To see that Ψ is surjective, fix $a \in \mathbb{Z}_n^*$

and define $\varphi : \mathbb{Z}_n \longrightarrow \mathbb{Z}_n$ by

$\varphi(k) = ak \bmod n$. We leave it as an exercise to verify that φ is a well-defined automorphism of $\mathbb{Z}_n$ and $\Psi(\varphi) = a$. Consequently, Ψ is surjective.

$\therefore \Psi$ is an isomorphism, so $\mathrm{Aut}(\mathbb{Z}_n) \cong \mathbb{Z}_n^*$.

$\blacksquare$