# Chapter 11 Homomorphisms of groups.

A homomorphism is what we get if we relax the requirement that an isomorphism be bijective (but still ask that the group structure is preserved).

**Definition**: A homomorphism between groups $G$ and $H$ is a map $\phi: G \to H$ satisfying

$$\phi(g_1 \cdot g_2) = \phi(g_1) * \phi(g_2)$$

for all $g_1, g_2 \in G$. (Here, $\circ$ is the operation in $G$ and $*$ is the operation in $H$).

The set $\phi(G) \subset H$ is called the homomorphic image (or just "image") of $G$ in $H$.

**Example**: Define a map $\phi: S_n \longrightarrow \mathbb{Z}_2$ by

$$\phi(\sigma) = \begin{cases} 0 & \text{if } \sigma \text{ is an even permutation} \\ 1 & \text{if } \sigma \text{ is an odd permutation.} \end{cases}$$

Then suppose $\sigma, \tau \in S_n$. Observe that the product $\sigma\tau$ is either even or odd according to the table:

| $\tau$ \ $\sigma$ | even | odd |
|---|---|---|
| even | even | odd |
| odd | odd | even |

Since the elements $0, 1 \in \mathbb{Z}_2$ behave the same way, we know that

$$\phi(\sigma\tau) = \phi(\sigma)\phi(\tau)$$

So that $\phi$ is a homomorphism.

<u>Example</u>: Let $G$ be any group, and choose $g \in G$. Define $\phi : \mathbb{Z}_{\cancel{n}} \longrightarrow G$ ~~(for arbitrary $n$)~~ by

$$\phi(r) = g^r \quad \cancel{0 \le r < n}$$

Then $\phi$ is a homomorphism since

$$\phi(m+n) = g^{m+n} = g^m \cdot g^n = \phi(m)\,\phi(n)$$

<u>Example</u>: Define

$$\phi : GL_2(\mathbb{R}) \longrightarrow \mathbb{R}^* \text{ by}$$

$\phi(A) = \det(A)$. Then since $\det(AB) = \det(A)\det(B)$, we have $\phi(AB) = \phi(A)\phi(B)$. So $\phi$ is a homomorphism.

<u>Example</u>: Define

$$\phi : \mathbb{Z} \longrightarrow \mathbb{Z}_n$$

by $\phi(r)$ = remainder of $r \bmod n$.

That is, write $r = i + kn$, and define

$\phi(r) = i \in \mathbb{Z}_n$. If $r = i + kn$ and $s = j + ln$

Then $\phi(r+s) = j+i \bmod n = i \bmod n + j \bmod n$

$$= \phi(r) + \phi(s),$$

so $\phi$ is a homomorphism.

<u>Example</u>: Define a map $\phi: \mathbb{R} \longrightarrow GL_3(\mathbb{R})$ (here, $(\mathbb{R},+)$)
by $\phi(r) = \begin{pmatrix} 1 & 0 & r \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$. Then we check:

$$\phi(r+s) = \begin{pmatrix} 1 & 0 & r+s \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \text{ while}$$

$$\phi(r)\phi(s) = \begin{pmatrix} 1 & 0 & r \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 & s \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & r+s \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix},$$

so $\phi(r+s) = \phi(s)\phi(r)$, and $\phi$ is a homomorphism.

<u>Proposition</u>: Let $\phi: G_1 \longrightarrow G_2$ be a homomorphism of groups. Then:

① If $e$ is the identity of $G_1$ then $\phi(e)$ is the identity of $G_2$

② For every $g \in G_1$ we have $\phi(g^{-1}) = (\phi(g))^{-1}$

③ If $H_1 \subset G_1$ is a subgroup, then $\phi(H_1)$ is a subgroup of $G_2$ (in particular $\phi(G_1)$ is a subgroup)

④ If $H_2 \subset G_2$ is a subgroup, then

$$\phi^{-1}(H_2) = \{ g \in G_1 \mid \phi(g) \in H_2 \} \text{ is a subgroup}$$

of $G_1$. Furthermore, if $H_2$ is normal in $G_2$ then $\phi^{-1}(H_2)$ is normal in $G_1$.

Proof: ①: Suppose $e_G$ and $e_H$ are the identities in $G$ and $H$. Then

$$e_H \phi(e_G) = \phi(e_G) = \phi(e_G \cdot e_G) = \phi(e_G)\phi(e_G)$$

and so by cancelation, $e_H = \phi(e_G)$.

② For any element $g \in G$, we must show that $\phi(g^{-1})\phi(g) = \phi(g)\phi(g^{-1}) = e$, since this shows $\phi(g^{-1})$ serves as an inverse to $\phi(g)$.

Observe $\phi(g^{-1})\phi(g) = \phi(g^{-1}g) = \phi(e) = e$, so we're done.

③ Recall that $H \subset G$ is a subgroup if it is nonempty and $gh^{-1} \in H$ for all $g, h \in H$.

In our case, $\phi(H_1)$ is nonempty since $e \in \phi(H_1)$. On the other hand, suppose $x, y \in \phi(H_1)$. Choose $a, b \in H_1$ with $\phi(a) = x$ and $\phi(b) = y$. Then

$$xy^{-1} = \phi(a)(\phi(b))^{-1} = \phi(a)\phi(b^{-1}) = \phi(ab^{-1}),$$

and since $ab^{-1} \in H_1$ this shows $xy^{-1} \in \phi(H_1)$.

Thus $\phi(H_1)$ is a subgroup.

④ Suppose $H_2 \subset G_2$ is a subgroup, define $H_1 = \phi^{-1}(H_2)$.

Then $H_1 \neq \emptyset$ since $\phi^{-1}(e) = e \in H_1$.

Now let $a, b \in H_1$ be given. Then $\phi(a), \phi(b) \in H_2$, so ~~$\phi(ab$~~ $\phi(ab^{-1}) \in H_2$, since $\phi(ab^{-1}) = \phi(a)(\phi(b))^{-1}$.

Thus $ab^{-1} \in H_1$.

Finally, suppose $H_2$ is normal. Then let $g_1 \in G_1$ and $h \in H_1$ be given. Note that

$$\phi(ghg^{-1}) = \phi(g)\phi(h)(\phi(g))^{-1} \in H_2$$

since $H_2$ is normal. Thus $ghg^{-1} \in H_1$ by definition.

---

We already remarked that part 3 of the previous theorem shows that $\phi(G_1)$ is a subgroup. In fact, part 4 of the theorem says something more significant:

Since $\{e\} \subset H$ is a normal subgroup, part 4 of the theorem says that $\phi^{-1}(\{e\})$ is a normal subgroup of $G$ for any group $G$ and any $\phi: G \to H$.

<u>Definition</u>: Let $\phi: G \to H$ be a homomorphism. The normal subgroup

$$\phi^{-1}(\{e\}) = \{g \in G \mid \phi(g) = e\}$$

is called the <u>kernel</u> of $\phi$.

---

<u>Discussion</u>: Since the kernel of $\phi$ is a normal subgroup, homomorphisms can be used to define normal subgroups. So whenever we define $\phi: G \to H$,

"for free" we get a normal subgroup $N \lhd G$,
and a quotient $G/N$.

Question: What group is $G/N$? Is it isomorphic to something familiar?

Answer: Stay tuned for Algebra 2!

Given that every homomorphism gives a normal subgroup, we can expect simple groups to behave a certain way with respect to homomorphisms. To say exactly what happens, we prove:

Proposition: Let $\phi: G \longrightarrow H$ be a homomorphism. If kernel of $\phi$ is $\{e\}$, then $\phi$ is injective.

Proof: Suppose the kernel is $\{e\}$ and $\phi(g) = \phi(h)$ for some $g, h \in G$. Then $\phi(g)\phi(h)^{-1} = e$

$$\Rightarrow \phi(gh^{-1}) = e.$$

So $gh^{-1}$ is in the kernel, forcing $gh^{-1} = e$.

$$\Rightarrow g = h.$$

Corollary: If $G$ is a simple group and $\phi: G \to H$ is a homomorphism, then either $\phi(G) = \{e\}$ or $\phi$ is injective.

Proof: Since $G$ is simple, there are only two possibilities for the kernel of $\phi$: $G$ and $\{e\}$.

If the kernel is $G$ then $\phi(G)=\{e\}$, and if the kernel is $\{e\}$ then $\phi$ is injective by the previous lemma.

# Chapter 16 Rings.

We now introduce a new object of study, which has two binary operations.

Definition: A nonempty set $R$ is a ring if there exist two binary operations on $R$, one denoted by $+$ and the other $\cdot$, such that:

① $a+b=b+a$ for all $a,b\in R$

② $(a+b)+c=a+(b+c)$ for all $a,b,c\in R$

③ There is an element $0\in R$ such that
$$a+0=0+a=a \quad \text{for all } a\in R$$

④ For every element $a\in R$ there exists an element $-a\in R$ such that $a+(-a)=0$.

⑤ $a(bc)=(ab)c$ for all $a,b,c\in R$

⑥ $a(b+c)=ab+ac$ and $(a+b)c=ac+bc$ for all $a,b,c\in R$.

Remarks: The easiest way to remember these axioms is to remember that ①-④ simply specify that $(R,+)$ is an abelian group. The last two insist that the multiplication on $R$ is associate and distributes over $+$.

Alternative definition of a ring:

A ring is an abelian group $(R,+)$ equipped with a second binary operation, which we denote by multiplication, satisfying:

(i) $a(bc)=(ab)c$ for all $a,b,c \in R$

(ii) $a(b+c) = ab+ac$ and $(a+b)c = ac+bc$ for all $a,b,c \in R$.

The definition of a ring can be modified in many ways. Here are the modifiers we need to know for this class:

Definition: If there exists an element $1 \in R$ that serves as a multiplicative identity for $R$:

$$a \cdot 1 = 1 \cdot a = a \quad \text{for all } a \in R$$

then $R$ is called a ring with unity or a ring with identity.

Def: If $R$ is a ring and $ab=ba$ for all $a,b \in R$, then $R$ is called a commutative ring.

Definition: If $R$ is a commutative ring with identity, then $R$ is called an integral domain if $ab=0$ implies $a=0$ or $b=0$ for all $a,b \in R$.

Definition: A ring $R$ with identity is called a division ring if every element has a multiplicative inverse, i.e. for all $a \in R$ there exists $a^{-1}$ satisfying

$$a \cdot a^{-1} = 1 = a^{-1} \cdot a .$$

A commutative division ring is called a field.

---

We can summarize this long list of definitions as follows:

$$
\begin{tikzcd}
 & \text{Rings} \arrow[dl, "\text{add identity}"'] \arrow[dr, "\text{make multiplication commutative}"] & \\
\text{Ring with unity} \arrow[dd, "\text{add multiplicative inverses}"] \arrow[drr, "\text{make multiplication commutative}"] & & \text{commutative ring} \arrow[d, "\text{add identity}"] \\
 & & \text{commutative ring with unity.} \arrow[d, "ab=0 \Rightarrow a=0 \text{ or } b=0"] \\
\text{division ring} \arrow[d, "\text{make multiplication commutative}"] & & \text{integral domain} \arrow[dll, "\text{add multiplicative inverses.}"] \\
\text{fields} & &
\end{tikzcd}
$$

Note: This may seem like a lot, but we'll work on this terminology for weeks. Moreover, this is just a small sample of the terminology in algebra 2, 3 & 4.

## Chapter 11 exercises:

1, 2, 3, 4, 8, 9, 10, 11, 12

## Chapter 16 exercises (more to come later)

1, 2 (note that 2 shows that subrings can have an identity even though the bigger ring does not).