Previously.

- Subgroups generated by one or more elements of a group
- Cyclic groups
- The order of an element
- Subgroup lattices

This Section.

- Mappings between groups
- Homomorphisms
- Isomorphisms
- Image
- Kernel
- Automorphisms

Goal. Study "sensible" functions from one group to another.

Definition. Let $(G, *)$ and $(H, \diamond)$ be groups. Then a mapping $\phi\colon G \to H$ is a `[group] homomorphism` if $\phi(g_1 * g_2) = \phi(g_1) \diamond \phi(g_2)$ for all $g_1, g_2 \in G$.

Exercise 1. Consider the groups $\mathbb{Z}$ and $2\mathbb{Z}$ and the map $\phi : \mathbb{Z} \to 2\mathbb{Z}$ defined by $\phi(n) = -2n$ for all $n \in \mathbb{Z}$.
Show that ϕ is a homomorphism.

Example. The `trivial homomorphism`,

$$\phi\colon G \to H, \quad \phi(g) = e_H \ \forall g \in G$$

Remark. We might leave operations out and write

$$\phi(ab) = \phi(a)\phi(b).$$

Exercise 2. Let $H = \{\varepsilon, (1\ 2)\}$ and $G = S_3$. Define $\pi : H \to G$ by $\pi(\sigma) = \sigma$ for all $\sigma \in H$. Show that π is a homomorhpism.

Exercise 3. $G = (\mathbb{Z}_2, +)$, $H = (\mathbb{Z}_5^*, \cdot)$

$$\phi\colon \mathbb{Z}_2 \to \mathbb{Z}_5^*, \quad \phi(\overline{0}_2) = \overline{0}_5 \text{ and } \phi(\overline{1}_2) = \overline{4}_5.$$

Answer each of the following to verify that ϕ is a homomorphism:

(a) Is $\phi(\overline{0}_2 + \overline{0}_2)$ equal to $\phi(\overline{0}_2) \cdot \phi(\overline{0}_2)$?

(b) Is $\phi(\overline{0}_2 + \overline{1}_2)$ equal to $\phi(\overline{0}_2) \cdot \phi(\overline{1}_2)$?

(c) Is $\phi(\overline{1}_2 + \overline{0}_2)$ equal to $\phi(\overline{1}_2) \cdot \phi(\overline{0}_2)$?

(d) Is $\phi(\overline{1}_2 + \overline{1}_2)$ equal to $\phi(\overline{1}_2) \cdot \phi(\overline{1}_2)$?

Exercise 4. Let $\sigma \in S_4$. Define $\phi : S_4 \to S_4$ by $\phi(\tau) = \sigma\tau\sigma^{-1}$ for all $\tau \in S_4$. Show that ϕ is a homomorhism by showing that $\phi(\tau_1\tau_2) = \phi(\tau_1)\phi(\tau_2)$ for all $\tau_1, \tau_2 \in S_4$.

Definition. A homomorphism that is both injective and surjective is called an `isomorphism`. If an isomorphism exists from G to H, we call G and H `isomorphic` and we write $G \cong H$ (`$G\cong H$`).

Example. Considering the homomorphism from before, $\phi\colon \mathbb{Z} \to 2\mathbb{Z}$ defined by $\phi(n) = -2n$ for all $n \in \mathbb{Z}$. Show that ϕ is:

- (One-to-One)

- (Onto)

Therefore $\mathbb{Z} \cong 2\mathbb{Z}$.

Exercise 5. Let $G = (\mathbb{R}, +)$ and $H = (\mathbb{R}_{>0}, \cdot)$. Define $\phi \colon G \to H$ by

$$\phi(x) = e^x \ \forall x \in \mathbb{R}.$$

(a) Is ϕ a homomorphism?

(b) Is ϕ one-to-one?

(c) Is ϕ onto?

(d) Is ϕ an isomorphism?

Exercise 6. Show that $\mathbb{Z}_3 \cong C_3$ (here $C_3 = \{1, a, a^2\}$).

Properties of Homomorphisms

Theorem 2.5.1. Let $\phi \colon G \to H$ be a group homomorphism. Then

(a) $\phi(e_G) = e_H$ (ϕ preserves identities)

(b) $\phi(g^{-1}) = \phi(g)^{-1} \ \forall g \in G$ (ϕ preserves inverses)

(c) $\phi(g^k) = \phi(g)^k \ \forall g \in G, k \in \mathbb{Z}$ (ϕ preserves powers)

Corollary. Let $\phi\colon G \to H$ be a homomorphism. If $g \in G$ has $|g| = n < \infty$, then $|\phi(g)| < \infty$. Moreover $|\phi(g)|$ divides $|g|$.

Example. $\phi\colon \mathbb{Z}_8 \to \mathbb{Z}_4$, $\phi(\overline{a}_8) = \overline{a}_4$

Warning: A map $\phi\colon \mathbb{Z}_n \to \mathbb{Z}_m$ with $\phi(\overline{a}_n) = \overline{a}_m$ only exists if $m \mid n$.

Exercise 7. Show $(\mathbb{Z}_4, +) \cong (\{1, -1, i, -i\}, \cdot)$ by writing down a group isomorphism.

Exercise 8. Show $\mathbb{Z}_4$ has a subgroup isomorphic to $\mathbb{Z}_2$. (Meaning there is an isomorphism between that subgroup and $\mathbb{Z}_2$.)

Exercise 9. Give some reason why...

(a) $K_4 \not\cong (\mathbb{Z}_4, +)$

(b) $S_3 \not\cong C_6$

(c) $(\mathbb{Z}_{12}, +) \not\cong (\mathbb{Q}^+, \cdot)$

Exercise 10. Is $(2\mathbb{Z}, +) \cong (3\mathbb{Z}, +)$?

Image of a Homomorphism

Definition. Let $\phi\colon G \to H$ be a group homomorphism.
The image of ϕ is denoted $\phi(G)$ or $\mathrm{im}(\phi)$ and is defined to be the set

$$\{\phi(g) \in H \mid g \in G\} = \{h \in H \mid \exists g \in G \text{ s.t. } \phi(g) = h\}.$$

Corollary of Thm 2.5.1. Let $\phi\colon G \to H$ be a homomorphism. Then $\mathrm{im}(\phi) \leq H$.

Exercise 11. Consider $\phi\colon \mathbb{Z} \to GL_2(\mathbb{R})$ defined by

$$\phi(n) = \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix}.$$

(a) Show that ϕ is a homomorphism.

(b) Verify $\mathrm{im}(\phi) = \left\{ \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix} : n \in \mathbb{Z} \right\}$. (Call this set H.)

(c) Conclude H is a group.

Isomorphisms are Equivalence Relations

Theorem 2.5.3. Let G, H, and K denote groups.

1. The identity map $id_G \colon G \to G$ is an isomorphism for every group G.

2. If $\sigma \colon G \to H$ is an isomorphism then the inverse mapping $\sigma^{-1} \colon H \to G$ is an isomorphism.

3. If $\sigma \colon G \to H$ and $\tau \colon H \to K$ are isomorphisms then $\tau\sigma \colon G \to K$ is an isomorphism.

Corollary 1. This isomorphism relation, $\cong$ is an equivalence relation on groups. That is, for all groups G, H, and K,

1. $G \cong G$,

2. if $G \cong H$, then $H \cong G$, and

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

Group of Homomorphisms

Corollary. If G is a group, then the set of all isomorphisms $G \to G$ forms a group under composition.

Proof. Notice that the set of all isomorphisms $G \to G$ is a subset of S_G. Therefore we can use the subgroup test. Theorem 2.5.3 completes the proof. $\square$

Question 12. How does Theorem 2.5.3 show that we have (1) Non-empty, (2) Closure, (3) Inverses?

Definition. Let G be a group.

1. An automorphism of G is an isomorphism from G to itself.
2. The set $\mathrm{Aut}(G)$ is the set of all automorphisms of G.

Note. The previous Corollary says $\mathrm{Aut}(G) \leq S_G$, so $\mathrm{Aut}(G)$ is a group.

Exercise 13. (a) If G is abelian, then $\phi\colon G \to G$ defined by $\phi(g) = g^{-1}$ is an automorphism of G.

i. Verify ϕ is a homomorphism.
ii. Check ϕ is injective.
iii. Check ϕ is surjective.

(b) Let $G = S_3$ (which is not abelian). Show that ϕ from (a) is not a homomorphism.

Exercise 14. Compute the automorphism group of the cyclic group of order 6.
$\mathbb{Z}_6 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}\}$

(a) Show that $\lambda : \mathbb{Z}_6 \to \mathbb{Z}_6$ defined by $\lambda(\overline{n}) = -\overline{n}$ is an automorphism of $\mathbb{Z}_6$.

(b) Verify that if $\phi : \mathbb{Z}_6 \to \mathbb{Z}_6$ is an automorphism, then $\phi(\overline{1}) = \overline{1}$ or $\phi(\overline{1}) = \overline{5}$.

(c) Conclude that $\mathrm{Aut}(\mathbb{Z}_6) = \{id_{\mathbb{Z}_6}, \lambda\}$.

(d) Discuss why $\mathrm{Aut}(\mathbb{Z}_6) \cong \mathbb{Z}_2$.

Exercise 15. Let G be a group and $a \in G$.
Define $\sigma_a \colon G \to G$ by $\sigma_a(g) = aga^{-1}$.
We call σ_a an `inner automorphism of` G.

(a) Verify σ_a is a homomorphism.

(b) Check σ_a is injective.

(c) Check σ_a is surjective.

Definition. The set $\mathrm{Inn}(G) = \{\sigma_a | a \in G\}$ is the set of all inner autmorphisms of G.

Exercise 16. Prove that $\mathrm{Inn}(G) \leq \mathrm{Aut}(G)$.

(a) Find a fixed $a \in G$ for which $\sigma_a = id_G$.

(b) If $\sigma_a, \sigma_b \in \mathrm{Inn}(G)$ what c satisfies $\sigma_a\sigma_b = \sigma_c$?

(c) For each $\sigma_a \in \mathrm{Inn}(G)$ what might be σ_a^{-1}?

Kernel of a Homomorphism

Definition. Let $\phi\colon G \to H$ be a group homomorphism.
The `kernel of` ϕ is denoted $\ker(\phi)$ and is defined to be the set

$$\{g \in G \mid \phi(g) = e_H\}.$$

Exercise 17. Let $\phi : G \to H$ be a homomorphism. Prove that $\ker(\phi) \leq G$.

Exercise 18. Let $\phi : \mathbb{Z} \to \mathbb{Z}_5$ be defined by $\phi(n) = \overline{n}$. Computer $\ker(\phi)$.