6. Maps between groups

6.1 Group homomorphisms

Definition 6.1.1: Group homomorphism and isomorphism

Let $(G_1, \cdot_1)$ and $(G_2, \cdot_2)$ be groups. A function $\boxed{\psi : G_1 \to G_2}$ is a **group homomorphism** if it satisfies

1. $\boxed{\psi(e_1) = e_2}$
2. $\forall f, g \in G : \boxed{\psi(f \cdot_1 g) = \psi(f) \cdot_2 \psi(g)}$

If $\psi : G_1 \to G_2$ is **bijective** as well, it is called a **group isomorphism**.

Isomorphic Groups

Two groups $(G_1, \cdot_1)$ and $(G_2, \cdot_2)$ are called **isomorphic**
if there exists a group isomorphism (bijective homomorphism) $\psi : G_1 \to G_2$:

$$\boxed{(G_1, \cdot_1) \simeq (G_2, \cdot_2)}$$

Exercise 6.13: Composition of group homomorphisms

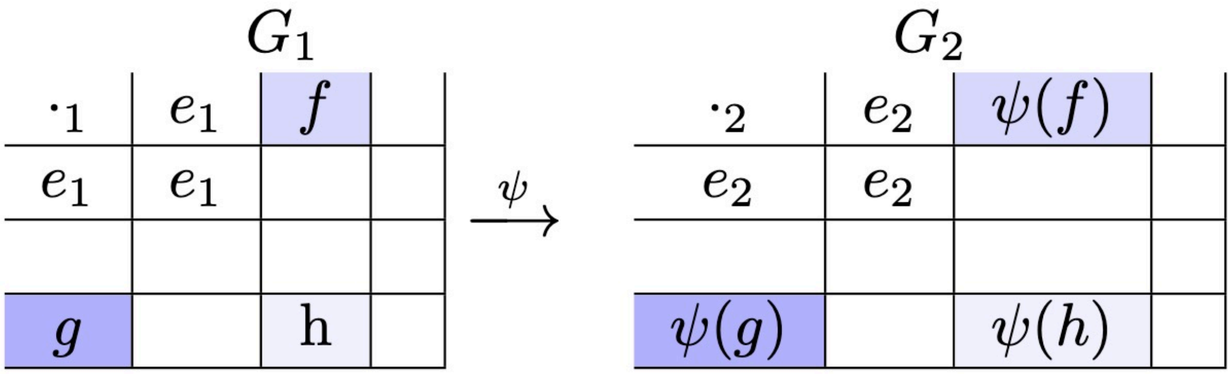
Let $(G_1, \cdot_1)$, $(G_2, \cdot_2)$ and $(G_3, \cdot_3)$ be groups and let $\psi_1 : G_1 \to G_2$ and $\psi_2 : G_2 \to G_3$ be group homomorphisms.

- The composition $\psi_2 \circ \psi_1 : G_1 \to G_3$ is also a group homomorphism.
- If both ψ_1 and ψ_2 are group **iso**morphisms, then $\psi_2 \circ \psi_1$ is also a group **iso**morphism

Exercise 6.18: Isomorphism as an equivalence relation

Being isomorphic is an equivalence relation on the set of all groups.

- Reflexive:
  - $\mathrm{id}_G : G \to G$ *is a group isomorphism (**automorphism**).*
- Symmetric
  - *If $\psi : G_1 \to G_2$ is a group isomorphism, then its inverse $\psi^{-1} : G_2 \to G_1$ is also a group isomorphism.*
- Transitive:
  - ***The composition of two group homomorphisms is again a group homomorphism**.*
  - $\psi_2 \circ \psi_1 : G_1 \to G_3$ is a group homomorphism if $\psi_1 : G_1 \to G_2$ and $\psi_2 : G_2 \to G_3$ are group homomorphisms.



$$h = f \cdot_1 g \qquad \text{and} \qquad \psi(h) = \psi(f) \cdot_2 \psi(g)$$

Note how similar the definition of a group **homomorphism** is to the definition of a group **action** (Def. 5.1.1).

Example 6.1.5: A group action is a group homomorphism

Let $(G, \cdot)$ be a group with identity element e_1 that acts on the set A via $\varphi : G \to S_A$.

- Since $\varphi_{e_1} = \mathrm{id}_A$ and $\mathrm{id}_A = e_2$ is the identity element of S_A, we have $\varphi(e_1) = e_2$.
- For any $f, g \in G$ we have $\varphi_{g \cdot f} = \varphi_g \circ \varphi_f$ by definition of a group action.
  Since $\circ = \cdot_2$ is the group operation in S_A, we have $\varphi(g \cdot f) = \varphi(g) \cdot_2 \varphi(f)$.

We conclude: **any group action $\varphi : G \to S_A$ is a group homomorphism on S_A**

Lemma 5.1.2 (group actions preserve inverses) can be generalized to any group **homomorphism**:

Lemma 6.1.6: Group homomorphisms preserve inverses

Let $\psi : G_1 \to G_2$ be a group homomorphism. Then for any $f \in G_1$ we have

$$\boxed{\psi(f^{-1}) = (\psi(f))^{-1}}$$

Definition 6.1.7: Kernel of a group homomorphism

Let $\psi : G_1 \to G_2$ be a group homomorphism and let e_2 be the identity element of G_2.
Then we define the **kernel** of ψ as

$$\boxed{\mathrm{er}(\psi) := \{g \in G_1 \mid \psi(g) = e_2\}}$$

Kernel of $\psi : G_1 \to G_2$ always contains the identity element of G_1

Since ψ is a group homomorphism, we have $\psi(e_1) = e_2$. Therefore

$$e_1 \in \mathrm{er}(\psi)$$

If the kernel only contains the identity element, the homomorphism ψ is injective:

Lemma 6.1.8: Injectivity and kernel

Let $\psi : G_1 \to G_2$ be a group homomorphism. Then

$$\boxed{\psi \text{ is injective} \iff \mathrm{er}(\psi) = \{e_1\}}$$

We proved this in Exercise 6.14.

Group isomorphisms have trivial kernel

If $\psi : G_1 \to G_2$ is a group **iso**morphism, then ψ is bijective and therefore injective.
By Lemma 6.1.8, we have

$$\mathrm{er}(\psi) = \{e_1\}$$

Theorem 6.1.9: Kernel is a NORMAL subgroup

Let $\psi : G_1 \to G_2$ be a group homomorphism. Then

$$\mathrm{er}(\psi) \subseteq G_1 \text{ is a subgroup of } G_1$$

Moreover,

$$\forall f \in G_1 : \qquad \boxed{f \cdot_1 \mathrm{er}(\psi) = \mathrm{er}(\psi) \cdot_1 f}$$

In other words, the kernel is a **normal subgroup** of G_1 (Def. 6.1.10).

Definition 6.1.10: Normal subgroup

A subgroup H of a group $(G, \cdot)$ is called a **normal subgroup** if

$$\forall f \in G : \qquad \boxed{f \cdot H = H \cdot f}$$

In other words, all left cosets of H are equal to the corresponding right cosets.
In normal subgroups H, we have that $\forall h \in H, \forall g \in G$:

$$\boxed{g \cdot h \cdot g^{-1} \in H}$$

This last property is often used as an alternative definition of normal subgroups. Why does it hold?
Proof
Let $h \in H$ and $g \in G$ be arbitrary. Since H is a normal subgroup, we have

$$g \cdot H = H \cdot g.$$

This implies that there exists an element $h' \in H$ such that

$$g \cdot h = h' \cdot g.$$

Multiplying both sides from the right by g^{-1}, we obtain

$$g \cdot h \cdot g^{-1} = h' \cdot g \cdot g^{-1} = h' \cdot e = h' \in H.$$

The kernel is a normal subgroup

It follows directly from Theorem 6.1.9 and Definition 6.1.10 that the **kernel** of any group homomorphism $\psi : G_1 \to G_2$ is a **normal** subgroup of G_1.

Because the **kernel is a normal subgroup**, we can prove that a subgroup H of a group G is normal by identifying it as the kernel of a suitable group homomorphism $\psi : G \to G_2$.

Definition: Image of a group homomorphism

Let $\psi : G_1 \to G_2$ be a group homomorphism. Then we define the **image** of ψ as

$$\boxed{\mathrm{im}(\psi) := \{\psi(g) \mid g \in G_1\} \subseteq G_2}$$

Note that the image is **never empty**, since e_2 is always in it:

$$e_1 \in G_1 \implies \psi(e_1) \overset{\Delta}{=} \boxed{e_2 \in \mathrm{im}(\psi)}.$$

Exercise 6.15: The image is a subgroup of G_2

Let $\psi : G_1 \to G_2$ be a group homomorphism. Then

$$\mathrm{im}(\psi) \subseteq G_2 \text{ is a subgroup of } G_2.$$

Isomorphic groups and element order

Let $(G_1, \cdot_1) \simeq (G_2, \cdot_2)$ be isomorphic via the group isomorphism $\varphi : G_1 \to G_2$.
Then for any $g \in G_1$

$$\boxed{\mathrm{ord}(g) = \mathrm{ord}(\varphi(g))}$$

So a group isomorphism maps elements to elements of the same order.
We can thus **check if an isomorphism can exist between two groups by comparing the orders of their elements.**

Proof.

Let $\mathrm{ord}(g) = n$ for $g \in G_1$.

$$\varphi(g)^n = \underbrace{\varphi(g) \cdot_2 \ldots \cdot_2 \varphi(g)}_{n} \overset{(2)}{=} \varphi(g \cdot_1 \ldots \cdot_1 g) = \varphi(g^n) \overset{\mathrm{ord}(g)=n}{=} \varphi(e_1) \overset{(1)}{=} e_2.$$

We conclude that $\varphi(g)^n = e_2$, so because of Lemma 3.1.12, $\mathrm{ord}(\varphi(g))$ divides n.
Now we show that n is the smallest such positive integer.

Assume there exists a positive integer $m < n$ such that $\varphi(g)^m = e_2$.
Then, by similar reasoning as above, we have $\varphi(g^m) = e_2$.

Now we see that

$$\varphi \text{ is injective} \overset{\text{Lemma 6.1.8}}{\implies} \mathrm{er}(\varphi) = \{e_1\} \implies g^m = e_1$$

But we assumed that $\mathrm{ord}(g) = n$ and that $m < n$. This gives a contradiction, since the order is by definition the smallest positive integer such that $g^{\mathrm{ord}(g)} = e_1$.
Therefore, no such m can exist and we conclude that $\mathrm{ord}(\varphi(g)) = n$.

6.2 Quotient groups

We will show that a **normal** subgroup (with left cosets = right cosets) $H \subseteq G$ of a group $(G, \cdot)$ can be used to construct a new group, called the **quotient group** G/H.

📖 **Definition 6.2.1:**

Let $(G, \cdot)$ be a group and $H \subseteq G$ be a **normal** subgroup of G we define

$$\boxed{G/H := \{f \cdot H \mid f \in G\}} = \{H \cdot f \mid f \in G\}$$

as the **set of all cosets** of H in G.
Its size $|G/H|$ is called the **index** of H in G and denoted by $[G : H]$.

Using multiplication of subsets (Def. 4.2.1), we can define a **group operation** $\cdot$ on G/H:

$$(fH) \cdot (gH) := \{k \cdot \ell \mid k \in fH, \ell \in gH\}$$

where $fH, gH \in G/H$.

📖 **Definition 6.2.2**

Let $(G, \cdot)$ be a group and $H \subseteq G$ be a normal subgroup of $(G, \cdot)$.
Let $C, D \in G/H$ be two cosets of H in G.
Suppose that $f \in C$ and $g \in D$ are arbitrary representatives of C and D, respectively.

We define the **product** of the cosets C and D as

$$C \cdot D := (f \cdot g)H$$

Note that this coset is independent of the choice of representatives f and g.

Let f, f' be two representatives of the coset C (i.e., $fH = f'H$).
Let g, g' be two representatives of the coset D (i.e., $gH = g'H$).
We must show that:

$$(f' \cdot g')H = (f \cdot g)H$$

Step 1: Express representatives using H
Since f' and f are in the same coset, f' must equal f multiplied by some element of H:

$$f' = f \cdot h_1 \quad \text{for some } h_1 \in H$$

Similarly for g' and g:

$$g' = g \cdot h_2 \quad \text{for some } h_2 \in H$$

Step 2: Examine the product $f' \cdot g'$
Substitute the expressions from Step 1:

$$f' \cdot g' = (f \cdot h_1) \cdot (g \cdot h_2)$$

We CANNOT simply swap $h_1 \cdot g \to g \cdot h_1$
Even though H is **normal**, G is not necessarily abelian!

Step 3: Utilize Normality of H
We need to group f and g together. To do this, we must commute h_1 and g.
Since H is a normal subgroup, we know that $Hg = gH$.
Thus, for any $h_1 \in H$, there exists an $h_3 \in H$ such that:

$$h_1 \cdot g = g \cdot h_3$$

Step 4: Substitution and Conclusion
Substitute $g \cdot h_3$ back into the main equation:

$$\begin{aligned} f' \cdot g' &= f \cdot (g \cdot h_3) \cdot h_2 \\ &= (f \cdot g) \cdot (h_3 \cdot h_2) \end{aligned}$$

Since H is a subgroup, $h_3 \cdot h_2 \in H$. Let $h_{ne} = h_3 \cdot h_2$.

$$f' \cdot g' = (f \cdot g) \cdot h_{ne}$$

Because $f' \cdot g'$ differs from $f \cdot g$ only by an element in H, they generate the same coset:

$$(f' \cdot g')H = (f \cdot g)H$$

Utilizing normality

Given an element $h_1 \cdot g \in H \cdot g$, we **cannot** simply swap h_1 and g to get an element in the coset $g \cdot H$. However, since H is a **normal** subgroup, we know that $Hg = gH$.
Thus, for any $h_1 \in H$, there exists an $h_3 \in H$ such that

$$h_1 \cdot g = g \cdot h_3.$$

Notation: representatives of cosets

If $C \in G/H$ is a coset of the normal subgroup H in G, then any $f \in C$ is called a **representative** of the coset C.

Restated Definition 6.2.2:
If f is a representative of a coset $C \in G/H$ and g is a representative of a coset $D \in G/H$, then $C \cdot D$ is again a coset of H in G (and thus $C \cdot D \in G/H$) and $f \cdot g$ is a representative of $C \cdot D$.

Definition 6.2.3: Quotient group

Let $(G, \cdot)$ be a group, $H \subseteq G$ a **normal** subgroup of G and G/H the set of all cosets of H in G (Def. 6.2.1). Then the multiplication of cosets

$$\boxed{(fH) \cdot (gH) := (f \cdot g)H} \quad (Def.\ 6.2.2)$$

gives rise to a **group structure** on $(G/H, \cdot)$.

We can explicitly write out the group operations to clarify how they work. Let $\cdot_G$ be the group operation in $(G, \cdot_G)$ (with **normal** subgroup H) and $\cdot_{G/H}$ be the group operation in the quotient group $(G/H, \cdot_{G/H})$. Then

$$(fH) \cdot_{G/H} (gH) = (f \cdot_G g)H.$$

We can see that

1. The composition of left (right) cosets is again a left (right) coset.
2. The representative of the composition is the composition of the representatives.

Identity element of the quotient group

Let $(G, \cdot)$ be a group, $H \subseteq G$ a **normal** subgroup of G and $(G/H, \cdot)$ the quotient group.

$$\boxed{e_{G/H} = e_G \cdot H = H}$$

Proof

By definition of the identity element in a group, we have to show that

$$(fH) \cdot H = fH = H \cdot (fH)$$

Using the definition of the group operation in the quotient group, we have

$$(fH) \cdot H = (fH) \cdot (e_G H) \overset{\Delta}{=} (f \cdot e_G)H = fH$$

and

$$H \cdot (fH) = (e_G H) \cdot (fH) \stackrel{\Delta}{=} (e_G \cdot f)H = fH.$$

Inverse of a left coset in the quotient group

Let $(G, \cdot)$ be a group, $H \subseteq G$ a **normal** subgroup of G and $(G/H, \cdot)$ the quotient group.

$$\forall f \in G: \qquad \boxed{(fH)^{-1} = (f^{-1})H}$$

Proof

By definition of the inverse element in a group, we have to show that

$$(fH) \cdot (f^{-1}H) = e_{G/H} = H = (Hf^{-1}) \cdot (fH)$$

Using the definition of the group operation in the quotient group, we have

$$(fH) \cdot (f^{-1}H) = (f \cdot f^{-1})H = e_G H = H.$$

and the proof is completely analogous for the right side.

Exercise 6.16

Let $(G, \cdot)$ be a group. Then for the quotient group by the trivial normal subgroup $\{e_G\}$ we have

$$\boxed{(G/\{e_G\}, \cdot) \simeq (G, \cdot)}$$

by the isomorphism

$$\psi : G/\{e_G\} \to G, \quad \psi(f \cdot \{e_G\}) := f$$

Exercise 6.16

If $\psi : G_1 \to G_2$ is an **injective** homomorphism, then

$$\boxed{(G_1, \cdot_{G_1}) \simeq (\operatorname{im}(\psi), \cdot_{G_2})}$$

by the isomorphism theorem and the isomorphism

$$\psi : G_1/\{e_1\} \to \operatorname{im}(\psi), \quad \psi(g \cdot \{e_1\}) = \psi(g \cdot \{e_1\}) = g$$

Where $\operatorname{er}(\psi) = \{e_1\}$ because ψ is injective (Lemma 6.1.8).
It follows from the isomorphism theorem (Theorem 6.3.1) that

$$(G_1/\operatorname{er}(\psi), \cdot_{G_1}) \simeq (\operatorname{im}(\psi), \cdot_{G_2})$$

and from Exercise 6.16 that

$$(G_1/\{e_1\}, \cdot_{G_1}) \simeq (G_1, \cdot_{G_1}).$$

Combining both results gives the desired isomorphism (since composition of isomorphisms is again an isomorphism, Exercise 6.18).

Group Automorphisms

A group isomorphism $\psi : G \to G$ from a group $(G, \cdot)$ to itself is called a **group automorphism**.
The set of all group automorphisms of $(G, \cdot)$ is denoted by $\mathrm{Aut}(G)$.

$$(\mathrm{Aut}(G), \circ) \text{ is a group}$$

where $\circ$ is the composition of functions.

Proof

- We already showed in Exercise 6.18 that the **composition of two group homomorphisms is again a group homomorphism.**
- The identity function $\mathrm{id}_G : G \to G$ is a group automorphism (Exercise 6.18).
- The inverse of a group automorphism is again a group automorphism (Exercise 6.18).
- Composition of functions is associative (function composition is associative by Lemma 2.1.2)

6.3 The isomorphism theorem

Theorem 6.3.1: The isomorphism theorem

Let $\psi : G_1 \to G_2$ be a group homomorphism. Then the map

$$\boxed{\psi : \begin{cases} G_1/\mathrm{er}(\psi) \to \mathrm{im}(\psi) \\ g \cdot \mathrm{er}(\psi) \mapsto \psi(g) \end{cases}}$$

is a group **isomorphism**. In other words,

$$\boxed{\left(G_1/\mathrm{er}(\psi), \cdot_{G_1/\mathrm{er}(\psi)}\right) \simeq (\mathrm{im}(\psi), \cdot_{G_2})}$$

Here, $G_1/\mathrm{er}(\psi)$ is the quotient group of G_1 by the kernel of ψ:

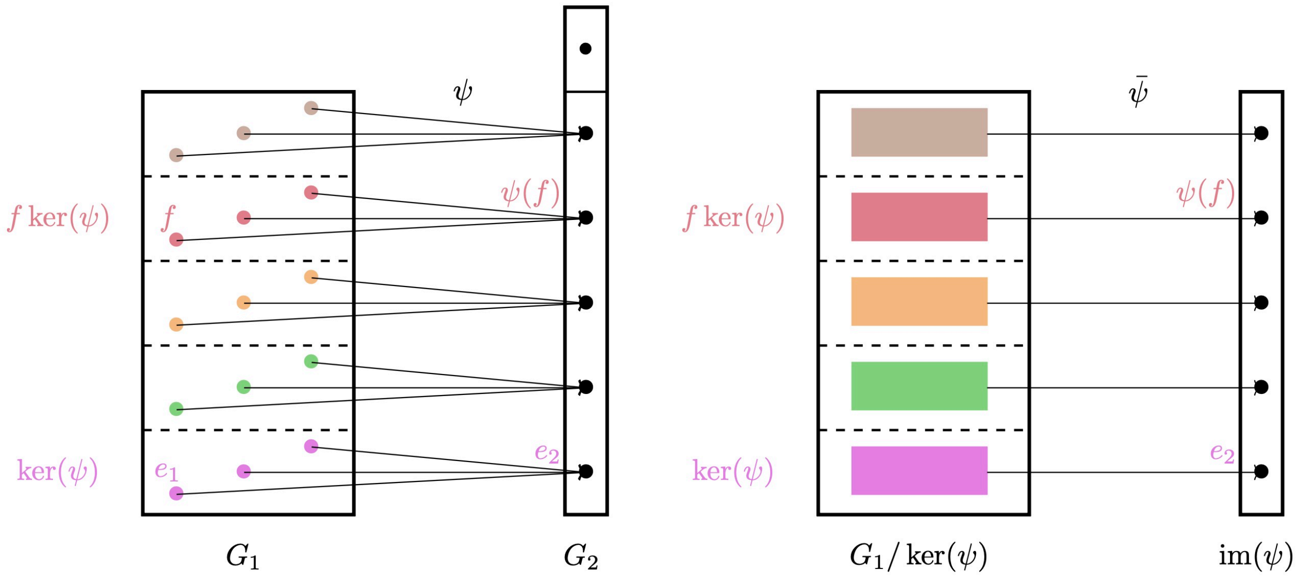
- $\mathrm{er}(\psi) \subseteq G_1$ is a **normal** subgroup of G_1 by Theorem 6.1.9.
- $G_1/\mathrm{er}(\psi)$ is thus a **quotient** group (Def. 6.2.3).
- $|G_1/\mathrm{er}(\psi)| = [G_1 : \mathrm{er}(\psi)]$ is the index of $\mathrm{er}(\psi)$ in G_1 (Def. 6.2.1).
- By Langrange's theorem (Theorem 4.3.3), if G **is finite**, then

$$|G_1/\mathrm{er}(\psi)| = [G_1 : \mathrm{er}(\psi)] = \frac{|G_1|}{|\mathrm{er}(\psi)|}.$$

'Well-defined' map

To show that a map $f : A \to B$ is **well-defined**, one has to show that $\forall a, b \in A$:

$$a = b \implies f(a) = f(b)$$



ψ
$f\ker(\psi)$
f
$\psi(f)$
$\ker(\psi)$
e_1
e_2
G_1
G_2
$\bar{\psi}$
$f\ker(\psi)$
$\psi(f)$
$\ker(\psi)$
e_2
$G_1/\ker(\psi)$
$\mathrm{im}(\psi)$