Linear Algebra 1

Lecture #6

Groups

Irena Penev

November 13, 2023

This lecture consists of two parts:

This lecture consists of two parts:

1. Monoids

This lecture consists of two parts:

1. Monoids
2. Groups

1. Monoids

1. Monoids

Definition

A *monoid* is an ordered pair $(S, \circ)$, where S is a set and $\circ$ is a binary operation on S (i.e. $\circ : S \times S \to S$), satisfying the following two axioms:

1. the operation $\circ$ is associative, i.e. $\forall a, b, c \in S$, we have that $a \circ (b \circ c) = (a \circ b) \circ c$;
2. there exists some $e \in S$, called the *identity element* of $(S, \circ)$, s.t. $\forall a \in S$, we have that $e \circ a = a$ and $a \circ e = a$.

1. Monoids

Definition

A *monoid* is an ordered pair $(S, \circ)$, where S is a set and $\circ$ is a binary operation on S (i.e. $\circ : S \times S \to S$), satisfying the following two axioms:

1. the operation $\circ$ is associative, i.e. $\forall a, b, c \in S$, we have that $a \circ (b \circ c) = (a \circ b) \circ c$;
2. there exists some $e \in S$, called the *identity element* of $(S, \circ)$, s.t. $\forall a \in S$, we have that $e \circ a = a$ and $a \circ e = a$.

Proposition 2.1.1

Every monoid has a unique identity element.

- Proof: Later!

1. Monoids

Definition

A *monoid* is an ordered pair $(S, \circ)$, where S is a set and $\circ$ is a binary operation on S (i.e. $\circ : S \times S \to S$), satisfying the following two axioms:

1. the operation $\circ$ is associative, i.e. $\forall a, b, c \in S$, we have that $a \circ (b \circ c) = (a \circ b) \circ c$;
2. there exists some $e \in S$, called the *identity element* of $(S, \circ)$, s.t. $\forall a \in S$, we have that $e \circ a = a$ and $a \circ e = a$.

Proposition 2.1.1

Every monoid has a unique identity element.

- Proof: Later!
- First, some examples.

Example 2.1.2

All the following are monoids:

1. $(\mathbb{N}_0, +)$;
2. $(\mathbb{Z}, +)$;
3. $(\mathbb{Q}, +)$;
4. $(\mathbb{R}, +)$;
5. $(\mathbb{C}, +)$.

In each of the above, 0 is the identity element.

Example 2.1.2

All the following are monoids:

1. $(\mathbb{N}_0, +)$;
2. $(\mathbb{Z}, +)$;
3. $(\mathbb{Q}, +)$;
4. $(\mathbb{R}, +)$;
5. $(\mathbb{C}, +)$.

In each of the above, 0 is the identity element.

- **Remark:** $(\mathbb{N}, +)$ is **not** a monoid, since it does not have an identity element.

Example 2.1.3

All the following are monoids ("$\cdot$" denotes multiplication):

1. $(\mathbb{N}_0, \cdot)$;
2. $(\mathbb{N}, \cdot)$;
3. $(\mathbb{Z}, \cdot)$;
4. $(\mathbb{Q}, \cdot)$;
5. $(\mathbb{R}, \cdot)$;
6. $(\mathbb{C}, \cdot)$.

In each of the above, 1 is the identity element.

Example 2.1.3

All the following are monoids ("$\cdot$" denotes multiplication):

1. $(\mathbb{N}_0, \cdot)$;
2. $(\mathbb{N}, \cdot)$;
3. $(\mathbb{Z}, \cdot)$;
4. $(\mathbb{Q}, \cdot)$;
5. $(\mathbb{R}, \cdot)$;
6. $(\mathbb{C}, \cdot)$.

In each of the above, 1 is the identity element.

Example 2.1.4

All the following are monoids ("$\cdot$" denotes multiplication):

1. $(\mathbb{N}, \cdot)$;
2. $(\mathbb{Z} \setminus \{0\}, \cdot)$;
3. $(\mathbb{Q} \setminus \{0\}, \cdot)$;
4. $(\mathbb{R} \setminus \{0\}, \cdot)$;
5. $(\mathbb{C} \setminus \{0\}, \cdot)$.

In each of the above, 1 is the identity element.

Proposition 2.1.1

Every monoid has a unique identity element.

Proof.

Proposition 2.1.1

Every monoid has a unique identity element.

Proof. Let $(S, \circ)$ be a monoid.

Proposition 2.1.1

Every monoid has a unique identity element.

Proof. Let $(S, \circ)$ be a monoid. By definition (in particular, by axiom 2), the monoid $(S, \circ)$ has an identity element; we must show that this identity element is unique. Suppose that e_1, e_2 are identity elements of $(S, \circ)$.

Proposition 2.1.1

Every monoid has a unique identity element.

Proof. Let $(S, \circ)$ be a monoid. By definition (in particular, by axiom 2), the monoid $(S, \circ)$ has an identity element; we must show that this identity element is unique. Suppose that e_1, e_2 are identity elements of $(S, \circ)$. Then

$$e_1 \quad \overset{(*)}{=} \quad e_1 \circ e_2 \quad \overset{(**)}{=} \quad e_2$$

where (*) follows from the fact that e_2 is the identity element of the monoid $(S, \circ)$, and (**) follows from the fact that e_1 is the identity element of the monoid $(S, \circ)$. So, the identity element of the monoid $(S, \circ)$ is unique. $\square$

2. Groups

2. Groups

Definition

A *group* is an ordered pair $(G, \circ)$, where G is a set and $\circ$ is a binary operation on G (i.e. $\circ : G \times G \to G$) that satisfy the following three axioms:

1. the operation $\circ$ is associative, i.e. $\forall a, b, c \in G$, we have that $a \circ (b \circ c) = (a \circ b) \circ c$;
2. there exists some $e \in G$, called the *identity element* of $(G, \circ)$, s.t. $\forall a \in G$, we have that $e \circ a = a$ and $a \circ e = a$;
3. $\forall a \in G$, $\exists a' \in G$, called the *inverse* of a, s.t. $a \circ a' = e$ and $a' \circ a = e$.

An *abelian group* is a group $(G, \circ)$ that satisfies the following additional axiom:

4. the operation $\circ$ is commutative, i.e. $\forall a, b \in G$, we have that $a \circ b = b \circ a$.

A *non-abelian* group is a group that is not abelian.

- **Remark:** Note that the first two axioms (axioms 1 and 2) from the definition of a group are precisely the monoid axioms.

- **Remark:** Note that the first two axioms (axioms 1 and 2) from the definition of a group are precisely the monoid axioms.
  - So, every group is a monoid.

- **Remark:** Note that the first two axioms (axioms 1 and 2) from the definition of a group are precisely the monoid axioms.
    - So, every group is a monoid.
    - By Proposition 2.1.1, it follows that the identity element e of a group is unique.

- **Remark:** Note that the first two axioms (axioms 1 and 2) from the definition of a group are precisely the monoid axioms.
    - So, every group is a monoid.
    - By Proposition 2.1.1, it follows that the identity element e of a group is unique.
    - In particular, the third axiom (axiom 3) makes sense.

- **Remark:** Note that the first two axioms (axioms 1 and 2) from the definition of a group are precisely the monoid axioms.
  - So, every group is a monoid.
  - By Proposition 2.1.1, it follows that the identity element e of a group is unique.
  - In particular, the third axiom (axiom 3) makes sense.
- **Terminology/Notation:** If the operation $\circ$ of the group $(G, \circ)$ is clear from context, then we may say that G is a group, rather than that $(G, \circ)$ is a group.

- **Remark:** Note that the first two axioms (axioms 1 and 2) from the definition of a group are precisely the monoid axioms.
  - So, every group is a monoid.
  - By Proposition 2.1.1, it follows that the identity element e of a group is unique.
  - In particular, the third axiom (axiom 3) makes sense.
- **Terminology/Notation:** If the operation $\circ$ of the group $(G, \circ)$ is clear from context, then we may say that G is a group, rather than that $(G, \circ)$ is a group.
  - However, this is only done if there is no chance of confusion, and so when in doubt, you should specify the operation.

- **Remark:** Note that the first two axioms (axioms 1 and 2) from the definition of a group are precisely the monoid axioms.
  - So, every group is a monoid.
  - By Proposition 2.1.1, it follows that the identity element e of a group is unique.
  - In particular, the third axiom (axiom 3) makes sense.
- **Terminology/Notation:** If the operation $\circ$ of the group $(G, \circ)$ is clear from context, then we may say that G is a group, rather than that $(G, \circ)$ is a group.
  - However, this is only done if there is no chance of confusion, and so when in doubt, you should specify the operation.
  - Sometimes, we say "G is a group under the operation $\circ$," which means exactly the same thing as "$(G, \circ)$ is a group."

Proposition 2.2.1

Each element of a group has a **unique** inverse.

- Proof: Later!

Proposition 2.2.1

Each element of a group has a **unique** inverse.

- Proof: Later!
- First, we introduce some notation and consider a few examples.

Proposition 2.2.1

Each element of a group has a **unique** inverse.

- Proof: Later!
- First, we introduce some notation and consider a few examples.

- **Notation:** Typically, the (unique) inverse of an element g of a group $(G, \circ)$ is denoted by g^{-1}.

Proposition 2.2.1

Each element of a group has a **unique** inverse.

- Proof: Later!
- First, we introduce some notation and consider a few examples.

- **Notation:** Typically, the (unique) inverse of an element g of a group $(G, \circ)$ is denoted by g^{-1}.
  - However, when the group operation is denoted by $+$ (note: this is typically done only if the group is abelian), then the inverse of an element g is denoted by $-g$.

Example 2.2.2

All the following are abelian groups:

1. $(\mathbb{Z}, +)$;
2. $(\mathbb{Q}, +)$;
3. $(\mathbb{R}, +)$;
4. $(\mathbb{C}, +)$.

In each of the above cases, the identity element is 0, and the inverse of a group element g is $-g$.[a]

[a] For example, in the group $(\mathbb{R}, +)$, the inverse of $\sqrt{13}$ is $-\sqrt{13}$.

Example 2.2.2

All the following are abelian groups:

1. $(\mathbb{Z}, +)$;
2. $(\mathbb{Q}, +)$;
3. $(\mathbb{R}, +)$;
4. $(\mathbb{C}, +)$.

In each of the above cases, the identity element is 0, and the inverse of a group element g is $-g$.[a]

[a] For example, in the group $(\mathbb{R}, +)$, the inverse of $\sqrt{13}$ is $-\sqrt{13}$.

- Note that the monoid $(\mathbb{N}_0, +)$ is **not** a group because elements other than 0 do not have inverses, and so axiom 3 from the definition of a group is not satisfied.

Example 2.2.3

All the following are abelian groups:

1. $(\mathbb{Q} \setminus \{0\}, \cdot)$;
2. $(\mathbb{R} \setminus \{0\}, \cdot)$;
3. $(\mathbb{C} \setminus \{0\}, \cdot)$.

In each of the above cases, the identity element is 1, and the inverse of a group element g is $g^{-1} = \frac{1}{g}$.[a]

[a] For example, in the group $(\mathbb{R} \setminus \{0\}, \cdot)$, the inverse of $\sqrt{13}$ is $\frac{1}{\sqrt{13}}$.

Example 2.2.3

All the following are abelian groups:

1. $(\mathbb{Q} \setminus \{0\}, \cdot)$;
2. $(\mathbb{R} \setminus \{0\}, \cdot)$;
3. $(\mathbb{C} \setminus \{0\}, \cdot)$.

In each of the above cases, the identity element is 1, and the inverse of a group element g is $g^{-1} = \frac{1}{g}$.[a]

[a] For example, in the group $(\mathbb{R} \setminus \{0\}, \cdot)$, the inverse of $\sqrt{13}$ is $\frac{1}{\sqrt{13}}$.

- **Remark:** Monoids $(\mathbb{Q}, \cdot)$, $(\mathbb{R}, \cdot)$, and $(\mathbb{C}, \cdot)$ are **not** groups because, in each of those cases, 0 does not have an inverse element.

Example 2.2.3

All the following are abelian groups:

1. $(\mathbb{Q} \setminus \{0\}, \cdot)$;
2. $(\mathbb{R} \setminus \{0\}, \cdot)$;
3. $(\mathbb{C} \setminus \{0\}, \cdot)$.

In each of the above cases, the identity element is 1, and the inverse of a group element g is $g^{-1} = \frac{1}{g}$.[a]

[a] For example, in the group $(\mathbb{R} \setminus \{0\}, \cdot)$, the inverse of $\sqrt{13}$ is $\frac{1}{\sqrt{13}}$.

- **Remark:** Monoids $(\mathbb{Q}, \cdot)$, $(\mathbb{R}, \cdot)$, and $(\mathbb{C}, \cdot)$ are **not** groups because, in each of those cases, 0 does not have an inverse element.
- Note also that $(\mathbb{Z} \setminus \{0\}, \cdot)$ is **not** a group because elements other than 1 and -1 do not have inverses.

Example 2.2.3

All the following are abelian groups:

1. $(\mathbb{Q} \setminus \{0\}, \cdot)$;
2. $(\mathbb{R} \setminus \{0\}, \cdot)$;
3. $(\mathbb{C} \setminus \{0\}, \cdot)$.

In each of the above cases, the identity element is 1, and the inverse of a group element g is $g^{-1} = \frac{1}{g}$.[a]

[a] For example, in the group $(\mathbb{R} \setminus \{0\}, \cdot)$, the inverse of $\sqrt{13}$ is $\frac{1}{\sqrt{13}}$.

- **Remark:** Monoids $(\mathbb{Q}, \cdot)$, $(\mathbb{R}, \cdot)$, and $(\mathbb{C}, \cdot)$ are **not** groups because, in each of those cases, 0 does not have an inverse element.
- Note also that $(\mathbb{Z} \setminus \{0\}, \cdot)$ is **not** a group because elements other than 1 and -1 do not have inverses.
- **Remark:** It might now seem that all groups are abelian. However, this is not the case: we will see examples of non-abelian groups later.

Proposition 2.2.1

Each element of a group has a **unique** inverse.

Proof.

Proposition 2.2.1

Each element of a group has a **unique** inverse.

Proof. Let $(G, \circ)$ be a group, and let e be its identity element.

Proposition 2.2.1

Each element of a group has a **unique** inverse.

Proof. Let $(G, \circ)$ be a group, and let e be its identity element. Fix some $g \in G$.

Proposition 2.2.1

Each element of a group has a **unique** inverse.

Proof. Let $(G, \circ)$ be a group, and let e be its identity element. Fix some $g \in G$. By the definition of a group (and in particular, by axiom 3), g has an inverse in the group $(G, \circ)$; WTS it is unique.

Proposition 2.2.1

Each element of a group has a **unique** inverse.

Proof. Let $(G, \circ)$ be a group, and let e be its identity element. Fix some $g \in G$. By the definition of a group (and in particular, by axiom 3), g has an inverse in the group $(G, \circ)$; WTS it is unique. Let g_1 and g_2 be inverses of g in the group $(G, \circ)$. Then

$$\begin{array}{rcll} g_1 & = & g_1 \circ e & \text{because } e \text{ is the identity element of } (G, \circ) \\ & = & g_1 \circ (g \circ g_2) & \text{because } g_2 \text{ is an inverse of } g \\ & = & (g_1 \circ g) \circ g_2 & \text{because } \circ \text{ is associative} \\ & = & e \circ g_2 & \text{because } g_1 \text{ is an inverse of } g \\ & = & g_2 & \text{because } e \text{ is the identity element of } (G, \circ). \end{array}$$

We have now shown that $g_1 = g_2$. So, the inverse of g is unique. □

Proposition 2.2.4

Let $(G, \circ)$ be a group with identity element e. Then all the following hold (here, the inverse of a group element g is denoted by g^{-1}):

(a) $\forall a, b, c \in G$, if $a \circ b = a \circ c$, then $b = c$;

(b) $\forall a, b, c \in G$, if $b \circ a = c \circ a$, then $b = c$;

(c) $\forall a, b \in G$, $\exists! x \in G$ s.t. $a \circ x = b$;

(d) $\forall a, b \in G$, $\exists! x \in G$ s.t. $x \circ a = b$;

(e) $\forall a \in G$: $(a^{-1})^{-1} = a$;

(f) $\forall a, b \in G$: $(a \circ b)^{-1} = b^{-1} \circ a^{-1}$.

Proposition 2.2.4

Let $(G, \circ)$ be a group with identity element e. Then all the following hold (here, the inverse of a group element g is denoted by g^{-1}):

(a) $\forall a, b, c \in G$, if $a \circ b = a \circ c$, then $b = c$;

(b) $\forall a, b, c \in G$, if $b \circ a = c \circ a$, then $b = c$;

(c) $\forall a, b \in G$, $\exists! x \in G$ s.t. $a \circ x = b$;

(d) $\forall a, b \in G$, $\exists! x \in G$ s.t. $x \circ a = b$;

(e) $\forall a \in G$: $(a^{-1})^{-1} = a$;

(f) $\forall a, b \in G$: $(a \circ b)^{-1} = b^{-1} \circ a^{-1}$.

- We will prove (a), (c), (e), and (f).

Proposition 2.2.4

Let $(G, \circ)$ be a group with identity element e. Then all the following hold (here, the inverse of a group element g is denoted by g^{-1}):

(a) $\forall a, b, c \in G$, if $a \circ b = a \circ c$, then $b = c$;

(b) $\forall a, b, c \in G$, if $b \circ a = c \circ a$, then $b = c$;

(c) $\forall a, b \in G$, $\exists! x \in G$ s.t. $a \circ x = b$;

(d) $\forall a, b \in G$, $\exists! x \in G$ s.t. $x \circ a = b$;

(e) $\forall a \in G$: $(a^{-1})^{-1} = a$;

(f) $\forall a, b \in G$: $(a \circ b)^{-1} = b^{-1} \circ a^{-1}$.

- We will prove (a), (c), (e), and (f).
- The proof of (b) is similar to that of (a), and the proof of (d) is similar to that of (c).

(a) $\forall a, b, c \in G$, if $a \circ b = a \circ c$, then $b = c$

Proof of (a).

1. (a) $\forall a, b, c \in G$, if $a \circ b = a \circ c$, then $b = c$

Proof of (a). Fix $a, b, c \in G$, and assume that $a \circ b = a \circ c$.

(a) $\forall a, b, c \in G$, if $a \circ b = a \circ c$, then $b = c$

Proof of (a). Fix $a, b, c \in G$, and assume that $a \circ b = a \circ c$. Then

b	$=$	$e \circ b$	because e is the identity element of $(G, \circ)$
	$=$	$(a^{-1} \circ a) \circ b$	because $a^{-1} \circ a = e$
	$=$	$a^{-1} \circ (a \circ b)$	because $\circ$ is associative
	$=$	$a^{-1} \circ (a \circ c)$	because $a \circ b = a \circ c$
	$=$	$(a^{-1} \circ a) \circ c$	because $\circ$ is associative
	$=$	$e \circ c$	because $a^{-1} \circ a = e$
	$=$	c	because e is the identity element of $(G, \circ)$.

This proves (a). $\square$

(c) $\forall a, b \in G, \exists! x \in G$ s.t. $a \circ x = b$

Proof of (c).

(c) $\forall a, b \in G$, $\exists! x \in G$ s.t. $a \circ x = b$

Proof of (c). Fix $a, b \in G$. WTS $\exists! x \in G$ s.t. $a \circ x = b$.

(c) $\forall a, b \in G$, $\exists! x \in G$ s.t. $a \circ x = b$

Proof of (c). Fix $a, b \in G$. WTS $\exists! x \in G$ s.t. $a \circ x = b$.

For existence, we set $x := a^{-1} \circ b$, and we observe that

$$
\begin{aligned}
a \circ x &= a \circ (a^{-1} \circ b) && \text{because } x = a^{-1} \circ b \\
&= (a \circ a^{-1}) \circ b && \text{because } \circ \text{ is associative} \\
&= e \circ b && \text{because } a \circ a^{-1} = e \\
&= b && \text{becuase } e \text{ is the identity element of } (G, \circ).
\end{aligned}
$$

(c) $\forall a, b \in G$, $\exists! x \in G$ s.t. $a \circ x = b$

Proof of (c). Fix $a, b \in G$. WTS $\exists! x \in G$ s.t. $a \circ x = b$.

For existence, we set $x := a^{-1} \circ b$, and we observe that

$a \circ x$	$=$	$a \circ (a^{-1} \circ b)$	because $x = a^{-1} \circ b$
	$=$	$(a \circ a^{-1}) \circ b$	because $\circ$ is associative
	$=$	$e \circ b$	because $a \circ a^{-1} = e$
	$=$	b	becuase e is the identity element of $(G, \circ)$.

Uniqueness follows from (a). This proves (c). $\square$

(e) $\forall a \in G$: $(a^{-1})^{-1} = a$

Proof of (e).

- (e) $\forall a \in G$: $(a^{-1})^{-1} = a$

Proof of (e). Fix $a \in G$. It suffices to show that $a^{-1} \circ (a^{-1})^{-1} = a^{-1} \circ a$, for then (a) will guarantee that $(a^{-1})^{-1} = a$, which is what we need.

- (e) $\forall a \in G$: $(a^{-1})^{-1} = a$

Proof of (e). Fix $a \in G$. It suffices to show that $a^{-1} \circ (a^{-1})^{-1} = a^{-1} \circ a$, for then (a) will guarantee that $(a^{-1})^{-1} = a$, which is what we need.

Since $(a^{-1})^{-1}$ is the inverse of a^{-1}, we know that $a^{-1} \circ (a^{-1})^{-1} = e$.

- (e) $\forall a \in G$: $(a^{-1})^{-1} = a$

Proof of (e). Fix $a \in G$. It suffices to show that $a^{-1} \circ (a^{-1})^{-1} = a^{-1} \circ a$, for then (a) will guarantee that $(a^{-1})^{-1} = a$, which is what we need.

Since $(a^{-1})^{-1}$ is the inverse of a^{-1}, we know that $a^{-1} \circ (a^{-1})^{-1} = e$.

On the other hand, since a^{-1} is the inverse of a, we have that $a^{-1} \circ a = e$.

(e) $\forall a \in G$: $(a^{-1})^{-1} = a$

Proof of (e). Fix $a \in G$. It suffices to show that $a^{-1} \circ (a^{-1})^{-1} = a^{-1} \circ a$, for then (a) will guarantee that $(a^{-1})^{-1} = a$, which is what we need.

Since $(a^{-1})^{-1}$ is the inverse of a^{-1}, we know that $a^{-1} \circ (a^{-1})^{-1} = e$.

On the other hand, since a^{-1} is the inverse of a, we have that $a^{-1} \circ a = e$.

Thus, $a^{-1} \circ (a^{-1})^{-1} = a^{-1} \circ a$.

(e) $\forall a \in G$: $(a^{-1})^{-1} = a$

Proof of (e). Fix $a \in G$. It suffices to show that $a^{-1} \circ (a^{-1})^{-1} = a^{-1} \circ a$, for then (a) will guarantee that $(a^{-1})^{-1} = a$, which is what we need.

Since $(a^{-1})^{-1}$ is the inverse of a^{-1}, we know that $a^{-1} \circ (a^{-1})^{-1} = e$.

On the other hand, since a^{-1} is the inverse of a, we have that $a^{-1} \circ a = e$.

Thus, $a^{-1} \circ (a^{-1})^{-1} = a^{-1} \circ a$. As explained above, this implies that $(a^{-1})^{-1} = a$. This proves (e). $\square$

(f) $\forall a, b \in G$: $(a \circ b)^{-1} = b^{-1} \circ a^{-1}$.

Proof of (f).

(f) $\forall a, b \in G$: $(a \circ b)^{-1} = b^{-1} \circ a^{-1}$.

Proof of (f). Fix $a, b \in G$.

- (f) $\forall a, b \in G$: $(a \circ b)^{-1} = b^{-1} \circ a^{-1}$.

Proof of (f). Fix $a, b \in G$. It suffices to prove the following:

(1) $(a \circ b) \circ (b^{-1} \circ a^{-1}) = e$;

(2) $(b^{-1} \circ a^{-1}) \circ (a \circ b) = e$.

(f) $\forall a, b \in G$: $(a \circ b)^{-1} = b^{-1} \circ a^{-1}$.

Proof of (f). Fix $a, b \in G$. It suffices to prove the following:

(1) $(a \circ b) \circ (b^{-1} \circ a^{-1}) = e$;

(2) $(b^{-1} \circ a^{-1}) \circ (a \circ b) = e$.

For (1), we observe that

$$\begin{aligned}
(a \circ b) \circ (b^{-1} \circ a^{-1}) &= a \circ (b \circ b^{-1}) \circ a && \text{because } \circ \text{ is associative} \\
&= a \circ e \circ a^{-1} && \text{because } b \circ b^{-1} = e \\
&= a \circ a^{-1} && \text{because } e \text{ is the identity element of } (G, \circ) \\
&= e && \text{because } a \circ a^{-1} = e.
\end{aligned}$$

(f) $\forall a, b \in G$: $(a \circ b)^{-1} = b^{-1} \circ a^{-1}$.

Proof of (f) (continued). For (2), we observe that

$$
\begin{aligned}
(b^{-1} \circ a^{-1}) \circ (a \circ b) &= b^{-1} \circ (a^{-1} \circ a) \circ b && \text{because } \circ \text{ is associative} \\
&= b^{-1} \circ e \circ b && \text{because } a^{-1} \circ a = e \\
&= b^{-1} \circ b && \text{because } e \text{ is the identity element of } (G, \circ) \\
&= e && \text{because } b^{-1} \circ b = e.
\end{aligned}
$$

(f) $\forall a, b \in G$: $(a \circ b)^{-1} = b^{-1} \circ a^{-1}$.

Proof of (f) (continued). We have now proven the following:

(1) $(a \circ b) \circ (b^{-1} \circ a^{-1}) = e$;

(2) $(b^{-1} \circ a^{-1}) \circ (a \circ b) = e$.

(f) $\forall a, b \in G$: $(a \circ b)^{-1} = b^{-1} \circ a^{-1}$.

Proof of (f) (continued). We have now proven the following:

(1) $(a \circ b) \circ (b^{-1} \circ a^{-1}) = e$;

(2) $(b^{-1} \circ a^{-1}) \circ (a \circ b) = e$.

It follows that $(a \circ b)^{-1} = b^{-1} \circ a^{-1}$. This proves (f). $\square$

Proposition 2.2.4

Let $(G, \circ)$ be a group with identity element e. Then all the following hold (here, the inverse of a group element g is denoted by g^{-1}):

(a) $\forall a, b, c \in G$, if $a \circ b = a \circ c$, then $b = c$;
(b) $\forall a, b, c \in G$, if $b \circ a = c \circ a$, then $b = c$;
(c) $\forall a, b \in G$, $\exists! x \in G$ s.t. $a \circ x = b$;
(d) $\forall a, b \in G$, $\exists! x \in G$ s.t. $x \circ a = b$;
(e) $\forall a \in G$: $(a^{-1})^{-1} = a$;
(f) $\forall a, b \in G$: $(a \circ b)^{-1} = b^{-1} \circ a^{-1}$.

- We now consider the case of $\mathbb{Z}_n$ and $\mathbb{Z}_p$.

- We now consider the case of $\mathbb{Z}_n$ and $\mathbb{Z}_p$.
- First of all, let us recall Fermat's Little Theorem.

- We now consider the case of $\mathbb{Z}_n$ and $\mathbb{Z}_p$.
- First of all, let us recall Fermat's Little Theorem.

Fermat's Little Theorem

If $p \in \mathbb{N}$ is a prime number and $a \in \mathbb{Z}_p \setminus \{0\}$, then $a^{p-1} = 1$.

- We now consider the case of $\mathbb{Z}_n$ and $\mathbb{Z}_p$.
- First of all, let us recall Fermat's Little Theorem.

Fermat's Little Theorem

If $p \in \mathbb{N}$ is a prime number and $a \in \mathbb{Z}_p \setminus \{0\}$, then $a^{p-1} = 1$.

Proposition 2.2.5

(a) For all positive integers n, $(\mathbb{Z}_n, +)$ is an abelian group whose identity element is $0 := [0]_n$.

(b) For all **prime** numbers p, $(\mathbb{Z}_p \setminus \{0\}, \cdot)$ is an abelian group whose identity element is $1 := [1]_p$.

Proposition 2.2.5

(a) For all positive integers n, $(\mathbb{Z}_n, +)$ is an abelian group whose identity element is $0 := [0]_n$.

Proof of (a).

Proposition 2.2.5

(a) For all positive integers n, $(\mathbb{Z}_n, +)$ is an abelian group whose identity element is $0 := [0]_n$.

Proof of (a). Fix a positive integer n.

Proposition 2.2.5

(a) For all positive integers n, $(\mathbb{Z}_n, +)$ is an abelian group whose identity element is $0 := [0]_n$.

Proof of (a). Fix a positive integer n. The fact that $+$ ("addition") is an associative and commutative binary operation on $\mathbb{Z}_n$ follows from Proposition 0.2.11. The identity element of $\mathbb{Z}_n$ is $0 := [0]_n$.

Proposition 2.2.5

(a) For all positive integers n, $(\mathbb{Z}_n, +)$ is an abelian group whose identity element is $0 := [0]_n$.

Proof of (a). Fix a positive integer n. The fact that $+$ ("addition") is an associative and commutative binary operation on $\mathbb{Z}_n$ follows from Proposition 0.2.11. The identity element of $\mathbb{Z}_n$ is $0 := [0]_n$. For each element $[a]_n$ in $\mathbb{Z}_n$ (where $a \in \mathbb{Z}$), the additive inverse of $[a]_n$ is $[-a]_n = [n - a]_n$.

Proposition 2.2.5

(a) For all positive integers n, $(\mathbb{Z}_n, +)$ is an abelian group whose identity element is $0 := [0]_n$.

Proof of (a). Fix a positive integer n. The fact that $+$ ("addition") is an associative and commutative binary operation on $\mathbb{Z}_n$ follows from Proposition 0.2.11. The identity element of $\mathbb{Z}_n$ is $0 := [0]_n$. For each element $[a]_n$ in $\mathbb{Z}_n$ (where $a \in \mathbb{Z}$), the additive inverse of $[a]_n$ is $[-a]_n = [n - a]_n$. So, $(\mathbb{Z}_n, +)$ is an abelian group with identity element $[0]_n$. $\square$

Proposition 2.2.5

(b) For all **prime** numbers p, $(\mathbb{Z}_p \setminus \{0\}, \cdot)$ is an abelian group whose identity element is $1 := [1]_p$.

Proof of (b).

Proposition 2.2.5

(b) For all **prime** numbers p, $(\mathbb{Z}_p \setminus \{0\}, \cdot)$ is an abelian group whose identity element is $1 := [1]_p$.

Proof of (b). Fix a prime number p.

Proposition 2.2.5

(b) For all **prime** numbers p, $(\mathbb{Z}_p \setminus \{0\}, \cdot)$ is an abelian group whose identity element is $1 := [1]_p$.

Proof of (b). Fix a prime number p. By Proposition 0.2.11, we know that $\cdot$ ("multiplication") is an associative and commutative binary operation on $\mathbb{Z}_p$.

Proposition 2.2.5

(b) For all **prime** numbers p, $(\mathbb{Z}_p \setminus \{0\}, \cdot)$ is an abelian group whose identity element is $1 := [1]_p$.

Proof of (b). Fix a prime number p. By Proposition 0.2.11, we know that $\cdot$ ("multiplication") is an associative and commutative binary operation on $\mathbb{Z}_p$. However, the question is whether multiplication remains a binary operation on $\mathbb{Z}_p \setminus \{0\}$, that is, whether $\mathbb{Z}_p \setminus \{0\}$ is "closed under multiplication," that is, whether the product of two numbers in $\mathbb{Z}_p \setminus \{0\}$ is always another number in $\mathbb{Z}_p \setminus \{0\}$.

Proposition 2.2.5

(b) For all **prime** numbers p, $(\mathbb{Z}_p \setminus \{0\}, \cdot)$ is an abelian group whose identity element is $1 := [1]_p$.

Proof of (b). Fix a prime number p. By Proposition 0.2.11, we know that $\cdot$ ("multiplication") is an associative and commutative binary operation on $\mathbb{Z}_p$. However, the question is whether multiplication remains a binary operation on $\mathbb{Z}_p \setminus \{0\}$, that is, whether $\mathbb{Z}_p \setminus \{0\}$ is "closed under multiplication," that is, whether the product of two numbers in $\mathbb{Z}_p \setminus \{0\}$ is always another number in $\mathbb{Z}_p \setminus \{0\}$.

So, fix $a, b \in \mathbb{Z}$ s.t. $[a]_p$ and $[b]_p$ are both non-zero (in $\mathbb{Z}_p$), i.e. p divides neither a nor b.

Proposition 2.2.5

- (b) For all **prime** numbers p, $(\mathbb{Z}_p \setminus \{0\}, \cdot)$ is an abelian group whose identity element is $1 := [1]_p$.

Proof of (b). Fix a prime number p. By Proposition 0.2.11, we know that $\cdot$ ("multiplication") is an associative and commutative binary operation on $\mathbb{Z}_p$. However, the question is whether multiplication remains a binary operation on $\mathbb{Z}_p \setminus \{0\}$, that is, whether $\mathbb{Z}_p \setminus \{0\}$ is "closed under multiplication," that is, whether the product of two numbers in $\mathbb{Z}_p \setminus \{0\}$ is always another number in $\mathbb{Z}_p \setminus \{0\}$.

So, fix $a, b \in \mathbb{Z}$ s.t. $[a]_p$ and $[b]_p$ are both non-zero (in $\mathbb{Z}_p$), i.e. p divides neither a nor b. Since p is **prime**, p does not divide the product ab,

Proposition 2.2.5

- (b) For all **prime** numbers p, $(\mathbb{Z}_p \setminus \{0\}, \cdot)$ is an abelian group whose identity element is $1 := [1]_p$.

Proof of (b). Fix a prime number p. By Proposition 0.2.11, we know that $\cdot$ ("multiplication") is an associative and commutative binary operation on $\mathbb{Z}_p$. However, the question is whether multiplication remains a binary operation on $\mathbb{Z}_p \setminus \{0\}$, that is, whether $\mathbb{Z}_p \setminus \{0\}$ is "closed under multiplication," that is, whether the product of two numbers in $\mathbb{Z}_p \setminus \{0\}$ is always another number in $\mathbb{Z}_p \setminus \{0\}$.

So, fix $a, b \in \mathbb{Z}$ s.t. $[a]_p$ and $[b]_p$ are both non-zero (in $\mathbb{Z}_p$), i.e. p divides neither a nor b. Since p is **prime**, p does not divide the product ab, and consequently, $[a]_p[b]_p = [ab]_p \neq 0$.

Proposition 2.2.5

- (b) For all **prime** numbers p, $(\mathbb{Z}_p \setminus \{0\}, \cdot)$ is an abelian group whose identity element is $1 := [1]_p$.

Proof of (b). Fix a prime number p. By Proposition 0.2.11, we know that $\cdot$ ("multiplication") is an associative and commutative binary operation on $\mathbb{Z}_p$. However, the question is whether multiplication remains a binary operation on $\mathbb{Z}_p \setminus \{0\}$, that is, whether $\mathbb{Z}_p \setminus \{0\}$ is "closed under multiplication," that is, whether the product of two numbers in $\mathbb{Z}_p \setminus \{0\}$ is always another number in $\mathbb{Z}_p \setminus \{0\}$.

So, fix $a, b \in \mathbb{Z}$ s.t. $[a]_p$ and $[b]_p$ are both non-zero (in $\mathbb{Z}_p$), i.e. p divides neither a nor b. Since p is **prime**, p does not divide the product ab, and consequently, $[a]_p[b]_p = [ab]_p \neq 0$. So, multiplication is indeed a binary operation on $\mathbb{Z}_p \setminus \{0\}$.

Fermat's Little Theorem

If $p \in \mathbb{N}$ is a prime number and $a \in \mathbb{Z}_p \setminus \{0\}$, then $a^{p-1} = 1$.

Proposition 2.2.5

(b) For all **prime** numbers p, $(\mathbb{Z}_p \setminus \{0\}, \cdot)$ is an abelian group whose identity element is $1 := [1]_p$.

Proof of (b) (continued).

Fermat's Little Theorem

If $p \in \mathbb{N}$ is a prime number and $a \in \mathbb{Z}_p \setminus \{0\}$, then $a^{p-1} = 1$.

Proposition 2.2.5

(b) For all **prime** numbers p, $(\mathbb{Z}_p \setminus \{0\}, \cdot)$ is an abelian group whose identity element is $1 := [1]_p$.

Proof of (b) (continued). The identity element of $(\mathbb{Z}_p \setminus \{0\}, \cdot)$ is $1 := [1]_p$.

Fermat's Little Theorem

If $p \in \mathbb{N}$ is a prime number and $a \in \mathbb{Z}_p \setminus \{0\}$, then $a^{p-1} = 1$.

Proposition 2.2.5

(b) For all **prime** numbers p, $(\mathbb{Z}_p \setminus \{0\}, \cdot)$ is an abelian group whose identity element is $1 := [1]_p$.

Proof of (b) (continued). The identity element of $(\mathbb{Z}_p \setminus \{0\}, \cdot)$ is $1 := [1]_p$.

Moreover, by Fermat's Little Theorem, each number $a \in \mathbb{Z}_p \setminus \{0\}$ has a multiplicative inverse, namely, a^{p-2}.

Fermat's Little Theorem

If $p \in \mathbb{N}$ is a prime number and $a \in \mathbb{Z}_p \setminus \{0\}$, then $a^{p-1} = 1$.

Proposition 2.2.5

(b) For all **prime** numbers p, $(\mathbb{Z}_p \setminus \{0\}, \cdot)$ is an abelian group whose identity element is $1 := [1]_p$.

Proof of (b) (continued). The identity element of $(\mathbb{Z}_p \setminus \{0\}, \cdot)$ is $1 := [1]_p$.

Moreover, by Fermat's Little Theorem, each number $a \in \mathbb{Z}_p \setminus \{0\}$ has a multiplicative inverse, namely, a^{p-2}.

This proves that $(\mathbb{Z}_p \setminus \{0\}, \cdot)$ is indeed an abelian group. $\square$

Proposition 2.2.5

(a) For all positive integers n, $(\mathbb{Z}_n, +)$ is an abelian group whose identity element is $0 := [0]_n$.

(b) For all **prime** numbers p, $(\mathbb{Z}_p \setminus \{0\}, \cdot)$ is an abelian group whose identity element is $1 := [1]_p$.

Proposition 2.2.5

1. (a) For all positive integers n, $(\mathbb{Z}_n, +)$ is an abelian group whose identity element is $0 := [0]_n$.
2. (b) For all **prime** numbers p, $(\mathbb{Z}_p \setminus \{0\}, \cdot)$ is an abelian group whose identity element is $1 := [1]_p$.

- **Remark:** If n is a positive integer that is not prime, then $(\mathbb{Z}_n \setminus \{0\}, \cdot)$ is **not** a group.

Proposition 2.2.5

(a) For all positive integers n, $(\mathbb{Z}_n, +)$ is an abelian group whose identity element is $0 := [0]_n$.

(b) For all **prime** numbers p, $(\mathbb{Z}_p \setminus \{0\}, \cdot)$ is an abelian group whose identity element is $1 := [1]_p$.

- **Remark:** If n is a positive integer that is not prime, then $(\mathbb{Z}_n \setminus \{0\}, \cdot)$ is **not** a group.
  - Indeed, if $n = 1$, then $\mathbb{Z}_n \setminus \{0\}$ is empty and therefore not a group under any operation (no group is empty, since it must, at a minimum, contain an identity element).

Proposition 2.2.5

1. (a) For all positive integers n, $(\mathbb{Z}_n, +)$ is an abelian group whose identity element is $0 := [0]_n$.
2. (b) For all **prime** numbers p, $(\mathbb{Z}_p \setminus \{0\}, \cdot)$ is an abelian group whose identity element is $1 := [1]_p$.

- **Remark:** If n is a positive integer that is not prime, then $(\mathbb{Z}_n \setminus \{0\}, \cdot)$ is **not** a group.
  - Indeed, if $n = 1$, then $\mathbb{Z}_n \setminus \{0\}$ is empty and therefore not a group under any operation (no group is empty, since it must, at a minimum, contain an identity element).
  - On the other hand, if $n \geq 2$ is a composite number, say $n = pq$ for some integers $p, q \geq 2$, then we have that $[p]_n, [q]_n \in \mathbb{Z}_n \setminus \{0\}$, but $[p]_n[q]_n = [pq]_n = [n]_n = 0$, and it follows that $\mathbb{Z}_n \setminus \{0\}$ is not closed under multiplication, i.e. multiplication is not a binary operation on $\mathbb{Z}_n \setminus \{0\}$.

- We now consider some groups of vectors and matrices.

- We now consider some groups of vectors and matrices.
- Let $\mathbb{F}$ be a field.
    - Since we have not formally studied fields yet, let us assume for now that $\mathbb{F}$ is one of the following: $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, or $\mathbb{Z}_p$ (where p is a prime number).
    - However, the examples that we consider work for all fields, not just the four listed above.

- We now consider some groups of vectors and matrices.
- Let $\mathbb{F}$ be a field.
  - Since we have not formally studied fields yet, let us assume for now that $\mathbb{F}$ is one of the following: $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, or $\mathbb{Z}_p$ (where p is a prime number).
  - However, the examples that we consider work for all fields, not just the four listed above.
- It is obvious that $(\mathbb{F}^{n\times m}, +)$ is an abelian group whose identity element is the zero matrix $O_{n\times m}$.
  - The (additive) inverse of a matrix $\left[\begin{array}{c} a_{i,j} \end{array}\right]_{n\times m}$ in the group $(\mathbb{F}^{n\times m}, +)$ is the matrix $\left[\begin{array}{c} -a_{i,j} \end{array}\right]_{n\times m}$ (i.e. the $n \times m$ matrix whose i,j-th entry is $-a_{i,j}$ for all indices $i \in \{1,\dots,n\}$ and $j \in \{1,\dots,m\}$).

- We now consider some groups of vectors and matrices.
- Let $\mathbb{F}$ be a field.
  - Since we have not formally studied fields yet, let us assume for now that $\mathbb{F}$ is one of the following: $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, or $\mathbb{Z}_p$ (where p is a prime number).
  - However, the examples that we consider work for all fields, not just the four listed above.
- It is obvious that $(\mathbb{F}^{n\times m},+)$ is an abelian group whose identity element is the zero matrix $O_{n\times m}$.
  - The (additive) inverse of a matrix $\left[\begin{array}{c} a_{i,j} \end{array}\right]_{n\times m}$ in the group $(\mathbb{F}^{n\times m},+)$ is the matrix $\left[\begin{array}{c} -a_{i,j} \end{array}\right]_{n\times m}$ (i.e. the $n\times m$ matrix whose i,j-th entry is $-a_{i,j}$ for all indices $i\in\{1,\dots,n\}$ and $j\in\{1,\dots,m\}$).
- In particular, $(\mathbb{F}^n,+)$ is an abelian group (with identity element $\mathbf{0}$).
  - We are using the fact that, by definition, $\mathbb{F}^n=\mathbb{F}^{n\times 1}$.

- More interestingly, consider the set $\mathrm{GL}_n(\mathbb{F})$ of all **invertible** matrices in $\mathbb{F}^{n \times n}$.

- More interestingly, consider the set $\mathrm{GL}_n(\mathbb{F})$ of all **invertible** matrices in $\mathbb{F}^{n \times n}$.
- $\mathrm{GL}_n(\mathbb{F})$ is a group under matrix multiplication, called the *general linear group of degree n over the field* $\mathbb{F}$.
  - The identity element of $\mathrm{GL}_n(\mathbb{F})$ is the identity matrix I_n, and the inverse of a matrix A in $\mathrm{GL}_n(\mathbb{F})$ is the matrix A^{-1} (the usual matrix inverse).

- More interestingly, consider the set $\mathrm{GL}_n(\mathbb{F})$ of all **invertible** matrices in $\mathbb{F}^{n \times n}$.
- $\mathrm{GL}_n(\mathbb{F})$ is a group under matrix multiplication, called the *general linear group of degree n over the field* $\mathbb{F}$.
    - The identity element of $\mathrm{GL}_n(\mathbb{F})$ is the identity matrix I_n, and the inverse of a matrix A in $\mathrm{GL}_n(\mathbb{F})$ is the matrix A^{-1} (the usual matrix inverse).
- The group $\mathrm{GL}_1(\mathbb{F})$ is abelian (because multiplication is commutative in the field $\mathbb{F}$).

- More interestingly, consider the set $\mathrm{GL}_n(\mathbb{F})$ of all **invertible** matrices in $\mathbb{F}^{n\times n}$.
- $\mathrm{GL}_n(\mathbb{F})$ is a group under matrix multiplication, called the *general linear group of degree n over the field* $\mathbb{F}$.
  - The identity element of $\mathrm{GL}_n(\mathbb{F})$ is the identity matrix I_n, and the inverse of a matrix A in $\mathrm{GL}_n(\mathbb{F})$ is the matrix A^{-1} (the usual matrix inverse).
- The group $\mathrm{GL}_1(\mathbb{F})$ is abelian (because multiplication is commutative in the field $\mathbb{F}$).
- However, for $n \geq 2$, the group $\mathrm{GL}_n(\mathbb{F})$ is **not** abelian.
  - We check this for $n = 2$.
  - The general case of $n \geq 2$ is discussed in the Lecture Notes.

- Consider the following two matrices in $\mathbb{F}^{2\times 2}$:

$$A_2 := \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, \qquad B_2 := \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}.$$

- Consider the following two matrices in $\mathbb{F}^{2\times 2}$:

$$A_2 := \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, \qquad B_2 := \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}.$$

- Both of these matrices have rank 2, and so by the Invertible Matrix Theorem, they are both invertible and therefore belong to $\mathrm{GL}_2(\mathbb{F})$.

- Consider the following two matrices in $\mathbb{F}^{2\times 2}$:

$$A_2 := \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, \qquad B_2 := \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}.$$

- Both of these matrices have rank 2, and so by the Invertible Matrix Theorem, they are both invertible and therefore belong to $\mathrm{GL}_2(\mathbb{F})$.
- However, we have that
  - $A_2 B_2 = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} 1+1 & 1 \\ 1 & 1 \end{bmatrix}$,
  - $B_2 A_2 = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 1+1 \end{bmatrix}$.

- Consider the following two matrices in $\mathbb{F}^{2\times 2}$:

$$A_2 := \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, \qquad B_2 := \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}.$$

- Both of these matrices have rank 2, and so by the Invertible Matrix Theorem, they are both invertible and therefore belong to $\mathrm{GL}_2(\mathbb{F})$.
- However, we have that
  - $A_2 B_2 = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} 1+1 & 1 \\ 1 & 1 \end{bmatrix}$,
  - $B_2 A_2 = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 1+1 \end{bmatrix}$.
- Since $1 + 1 \neq 1$, we see that $A_2 B_2 \neq B_2 A_2$.

- Consider the following two matrices in $\mathbb{F}^{2\times 2}$:

$$A_2 \quad := \quad \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, \qquad B_2 \quad := \quad \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}.$$

- Both of these matrices have rank 2, and so by the Invertible Matrix Theorem, they are both invertible and therefore belong to $\mathrm{GL}_2(\mathbb{F})$.
- However, we have that
  - $A_2 B_2 = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} 1+1 & 1 \\ 1 & 1 \end{bmatrix}$,
  - $B_2 A_2 = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 1+1 \end{bmatrix}$.
- Since $1 + 1 \neq 1$, we see that $A_2 B_2 \neq B_2 A_2$.
- So, $\mathrm{GL}_2(\mathbb{F})$ is not abelian.

- Consider the following two matrices in $\mathbb{F}^{2\times 2}$:

$$A_2 \; := \; \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, \qquad B_2 \; := \; \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}.$$

- Both of these matrices have rank 2, and so by the Invertible Matrix Theorem, they are both invertible and therefore belong to $\mathrm{GL}_2(\mathbb{F})$.
- However, we have that
  - $A_2 B_2 = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} 1+1 & 1 \\ 1 & 1 \end{bmatrix}$,
  - $B_2 A_2 = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 1+1 \end{bmatrix}$.
- Since $1 + 1 \neq 1$, we see that $A_2 B_2 \neq B_2 A_2$.
- So, $\mathrm{GL}_2(\mathbb{F})$ is not abelian.
- This construction is not hard to generalize to $n \geq 2$ (see the Lecture Notes).

- **Remark:** The fact that

$$1 + 1 \neq 1$$

is obviously true for the fields that we are familiar with.

- **Remark:** The fact that
$$1+1 \neq 1$$
is obviously true for the fields that we are familiar with.
- But in fact, this is true in **any** field $\mathbb{F}$, not just those that we have seen so far, and it essentially follows from the fact that
$$1 \neq 0$$
(which is true for any field).

- **Remark:** The fact that

$$1 + 1 \neq 1$$

is obviously true for the fields that we are familiar with.

- But in fact, this is true in **any** field $\mathbb{F}$, not just those that we have seen so far, and it essentially follows from the fact that

$$1 \neq 0$$

(which is true for any field).

- On the other hand,

$$1 + 1 + 1 = 1$$

is true in some fields (for example, it is true for the field $\mathbb{Z}_2$).

Definition

A *subgroup* of a group $(G, \circ)$ is a group $(H, \diamond)$ s.t. $H \subseteq G$ and for all $a, b \in H$, we have that $a \diamond b = a \circ b$.[a] If $(H, \diamond)$ is a subgroup of $(G, \circ)$, then we write $(H, \diamond) \leq (G, \circ)$.

[a] Here, $\diamond$ is the restriction of $\circ$ to H, and it is important that $a \diamond b = a \circ b \in H$ for all $a, b \in H$ (otherwise, H is not "closed under" $\diamond$, which means that $\diamond$ is not a binary operation on H, and in particular, $(H, \diamond)$ is not a group).

- Normally, we do not notationally distinguish between $\diamond$ and $\circ$, and we speak about $(H, \circ)$ being a subgroup of $(G, \circ)$, where it is understood from context that the operation $\circ$ from $(H, \circ)$ is the restriction of the the binary operation $\circ$ on G to H.

Example 2.2.6

Every group $(G, \circ)$ has at least two subgroups: $(G, \circ)$ and $(\{e\}, \circ)$, where e is the identity element of G.

Example 2.2.6

Every group $(G, \circ)$ has at least two subgroups: $(G, \circ)$ and $(\{e\}, \circ)$, where e is the identity element of G.

Example 2.2.7

$(\mathbb{Z}, +) \leq (\mathbb{Q}, +) \leq (\mathbb{R}, +) \leq (\mathbb{C}, +)$.

Example 2.2.6

Every group $(G, \circ)$ has at least two subgroups: $(G, \circ)$ and $(\{e\}, \circ)$, where e is the identity element of G.

Example 2.2.7

$(\mathbb{Z}, +) \leq (\mathbb{Q}, +) \leq (\mathbb{R}, +) \leq (\mathbb{C}, +)$.

Example 2.2.8

$(\mathbb{Q} \setminus \{0\}, \cdot) \leq (\mathbb{R} \setminus \{0\}, \cdot) \leq (\mathbb{C} \setminus \{0\}, \cdot)$.

Theorem 2.2.9

Let $(G, \circ)$ be a group with identity element e, and with the inverse of an element $a \in G$ denoted by a^{-1}. Then for all $H \subseteq G$, we have that $(H, \circ)$ is a subgroup of $(G, \circ)$ iff all the following hold:

1. $e \in H$;
2. H is closed under $\circ$, that is, $\forall a, b \in H$: $a \circ b \in H$;
3. H is closed under inverses, that is, $\forall a \in H$: $a^{-1} \in H$.

Proof.

Theorem 2.2.9

Let $(G, \circ)$ be a group with identity element e, and with the inverse of an element $a \in G$ denoted by a^{-1}. Then for all $H \subseteq G$, we have that $(H, \circ)$ is a subgroup of $(G, \circ)$ iff all the following hold:

(i) $e \in H$;

(ii) H is closed under $\circ$, that is, $\forall a, b \in H$: $a \circ b \in H$;

(iii) H is closed under inverses, that is, $\forall a \in H$: $a^{-1} \in H$.

Proof. Fix $H \subseteq G$. Suppose first that (i), (ii), and (iii) hold.

Theorem 2.2.9

Let $(G, \circ)$ be a group with identity element e, and with the inverse of an element $a \in G$ denoted by a^{-1}. Then for all $H \subseteq G$, we have that $(H, \circ)$ is a subgroup of $(G, \circ)$ iff all the following hold:

(i) $e \in H$;

(ii) H is closed under $\circ$, that is, $\forall a, b \in H$: $a \circ b \in H$;

(iii) H is closed under inverses, that is, $\forall a \in H$: $a^{-1} \in H$.

Proof. Fix $H \subseteq G$. Suppose first that (i), (ii), and (iii) hold.
By (ii), the binary operation $\circ$ on G can be restricted to H (so that it becomes a binary operation on H).

Theorem 2.2.9

Let $(G, \circ)$ be a group with identity element e, and with the inverse of an element $a \in G$ denoted by a^{-1}. Then for all $H \subseteq G$, we have that $(H, \circ)$ is a subgroup of $(G, \circ)$ iff all the following hold:

(i) $e \in H$;

(ii) H is closed under $\circ$, that is, $\forall a, b \in H$: $a \circ b \in H$;

(iii) H is closed under inverses, that is, $\forall a \in H$: $a^{-1} \in H$.

Proof. Fix $H \subseteq G$. Suppose first that (i), (ii), and (iii) hold. By (ii), the binary operation $\circ$ on G can be restricted to H (so that it becomes a binary operation on H). The fact that $\circ$ is associative in $(H, \circ)$ follows simply from the fact that $\circ$ is inherited from the group $(G, \circ)$, where it is associative.

Theorem 2.2.9

Let $(G, \circ)$ be a group with identity element e, and with the inverse of an element $a \in G$ denoted by a^{-1}. Then for all $H \subseteq G$, we have that $(H, \circ)$ is a subgroup of $(G, \circ)$ iff all the following hold:

1. (i) $e \in H$;
2. (ii) H is closed under $\circ$, that is, $\forall a, b \in H$: $a \circ b \in H$;
3. (iii) H is closed under inverses, that is, $\forall a \in H$: $a^{-1} \in H$.

Proof. Fix $H \subseteq G$. Suppose first that (i), (ii), and (iii) hold. By (ii), the binary operation $\circ$ on G can be restricted to H (so that it becomes a binary operation on H). The fact that $\circ$ is associative in $(H, \circ)$ follows simply from the fact that $\circ$ is inherited from the group $(G, \circ)$, where it is associative. By (i), H contains an identity element, and by (iii), every element of H has an inverse in $(H, \circ)$.

Theorem 2.2.9

Let $(G, \circ)$ be a group with identity element e, and with the inverse of an element $a \in G$ denoted by a^{-1}. Then for all $H \subseteq G$, we have that $(H, \circ)$ is a subgroup of $(G, \circ)$ iff all the following hold:

(i) $e \in H$;

(ii) H is closed under $\circ$, that is, $\forall a, b \in H$: $a \circ b \in H$;

(iii) H is closed under inverses, that is, $\forall a \in H$: $a^{-1} \in H$.

Proof (continued). Suppose, conversely, that $(H, \circ)$ is a subgroup of $(G, \circ)$.

Theorem 2.2.9

Let $(G, \circ)$ be a group with identity element e, and with the inverse of an element $a \in G$ denoted by a^{-1}. Then for all $H \subseteq G$, we have that $(H, \circ)$ is a subgroup of $(G, \circ)$ iff all the following hold:

(i) $e \in H$;

(ii) H is closed under $\circ$, that is, $\forall a, b \in H\colon\ a \circ b \in H$;

(iii) H is closed under inverses, that is, $\forall a \in H\colon\ a^{-1} \in H$.

Proof (continued). Suppose, conversely, that $(H, \circ)$ is a subgroup of $(G, \circ)$. Then (ii) holds, because $\circ$ (properly restricted) is a binary operation on H.

Theorem 2.2.9

Let $(G, \circ)$ be a group with identity element e, and with the inverse of an element $a \in G$ denoted by a^{-1}. Then for all $H \subseteq G$, we have that $(H, \circ)$ is a subgroup of $(G, \circ)$ iff all the following hold:

(i) $e \in H$;

(ii) H is closed under $\circ$, that is, $\forall a, b \in H\colon\ a \circ b \in H$;

(iii) H is closed under inverses, that is, $\forall a \in H\colon\ a^{-1} \in H$.

Proof (continued). Suppose, conversely, that $(H, \circ)$ is a subgroup of $(G, \circ)$. Then (ii) holds, because $\circ$ (properly restricted) is a binary operation on H. It remains to prove that (i) and (iii) hold.

Theorem 2.2.9

Let $(G, \circ)$ be a group with identity element e, and with the inverse of an element $a \in G$ denoted by a^{-1}. Then for all $H \subseteq G$, we have that $(H, \circ)$ is a subgroup of $(G, \circ)$ iff all the following hold:

(i) $e \in H$;

(ii) H is closed under $\circ$, that is, $\forall a, b \in H$: $a \circ b \in H$;

(iii) H is closed under inverses, that is, $\forall a \in H$: $a^{-1} \in H$.

Proof (continued). Suppose, conversely, that $(H, \circ)$ is a subgroup of $(G, \circ)$. Then (ii) holds, because $\circ$ (properly restricted) is a binary operation on H. It remains to prove that (i) and (iii) hold.

Since H is a group, it must have an identity element e_H, and each element of H must have inverse in $(H, \circ)$.

Theorem 2.2.9

Let $(G, \circ)$ be a group with identity element e, and with the inverse of an element $a \in G$ denoted by a^{-1}. Then for all $H \subseteq G$, we have that $(H, \circ)$ is a subgroup of $(G, \circ)$ iff all the following hold:

(i) $e \in H$;

(ii) H is closed under $\circ$, that is, $\forall a, b \in H$: $a \circ b \in H$;

(iii) H is closed under inverses, that is, $\forall a \in H$: $a^{-1} \in H$.

Proof (continued). Suppose, conversely, that $(H, \circ)$ is a subgroup of $(G, \circ)$. Then (ii) holds, because $\circ$ (properly restricted) is a binary operation on H. It remains to prove that (i) and (iii) hold.

Since H is a group, it must have an identity element e_H, and each element of H must have inverse in $(H, \circ)$. The question is whether the identity element of $(H, \circ)$ is the same as in $(G, \circ)$, and similar for inverses.

Theorem 2.2.9

Let $(G, \circ)$ be a group with identity element e, and with the inverse of an element $a \in G$ denoted by a^{-1}. Then for all $H \subseteq G$, we have that $(H, \circ)$ is a subgroup of $(G, \circ)$ iff all the following hold:

(i) $e \in H$;

(ii) H is closed under $\circ$, that is, $\forall a, b \in H$: $a \circ b \in H$;

(iii) H is closed under inverses, that is, $\forall a \in H$: $a^{-1} \in H$.

Proof (continued). We first deal with the identity element.

Theorem 2.2.9

Let $(G, \circ)$ be a group with identity element e, and with the inverse of an element $a \in G$ denoted by a^{-1}. Then for all $H \subseteq G$, we have that $(H, \circ)$ is a subgroup of $(G, \circ)$ iff all the following hold:

(i) $e \in H$;

(ii) H is closed under $\circ$, that is, $\forall a, b \in H\colon\ a \circ b \in H$;

(iii) H is closed under inverses, that is, $\forall a \in H\colon\ a^{-1} \in H$.

Proof (continued). We first deal with the identity element. If we compute in $(H, \circ)$, we have that $e_H \circ e_H = e_H$ (because e_H is the identity element of $(H, \circ)$),

Theorem 2.2.9

Let $(G, \circ)$ be a group with identity element e, and with the inverse of an element $a \in G$ denoted by a^{-1}. Then for all $H \subseteq G$, we have that $(H, \circ)$ is a subgroup of $(G, \circ)$ iff all the following hold:

1. $e \in H$;
2. H is closed under $\circ$, that is, $\forall a, b \in H$: $a \circ b \in H$;
3. H is closed under inverses, that is, $\forall a \in H$: $a^{-1} \in H$.

Proof (continued). We first deal with the identity element. If we compute in $(H, \circ)$, we have that $e_H \circ e_H = e_H$ (because e_H is the identity element of $(H, \circ)$), and if we compute in $(G, \circ)$, then we have that $e_H \circ e = e_H$ (because e is the identity element of $(G, \circ)$).

Theorem 2.2.9

Let $(G, \circ)$ be a group with identity element e, and with the inverse of an element $a \in G$ denoted by a^{-1}. Then for all $H \subseteq G$, we have that $(H, \circ)$ is a subgroup of $(G, \circ)$ iff all the following hold:

(i) $e \in H$;

(ii) H is closed under $\circ$, that is, $\forall a, b \in H\colon\ a \circ b \in H$;

(iii) H is closed under inverses, that is, $\forall a \in H\colon\ a^{-1} \in H$.

Proof (continued). We first deal with the identity element. If we compute in $(H, \circ)$, we have that $e_H \circ e_H = e_H$ (because e_H is the identity element of $(H, \circ)$), and if we compute in $(G, \circ)$, then we have that $e_H \circ e = e_H$ (because e is the identity element of $(G, \circ)$). But now $e_H \circ e_H = e_H \circ e$,

Theorem 2.2.9

Let $(G, \circ)$ be a group with identity element e, and with the inverse of an element $a \in G$ denoted by a^{-1}. Then for all $H \subseteq G$, we have that $(H, \circ)$ is a subgroup of $(G, \circ)$ iff all the following hold:

(i) $e \in H$;

(ii) H is closed under $\circ$, that is, $\forall a, b \in H$: $a \circ b \in H$;

(iii) H is closed under inverses, that is, $\forall a \in H$: $a^{-1} \in H$.

Proof (continued). We first deal with the identity element. If we compute in $(H, \circ)$, we have that $e_H \circ e_H = e_H$ (because e_H is the identity element of $(H, \circ)$), and if we compute in $(G, \circ)$, then we have that $e_H \circ e = e_H$ (because e is the identity element of $(G, \circ)$). But now $e_H \circ e_H = e_H \circ e$, and so by Proposition 2.2.4(a) applied to $(G, \circ)$, we have that $e_H = e$.

Theorem 2.2.9

Let $(G, \circ)$ be a group with identity element e, and with the inverse of an element $a \in G$ denoted by a^{-1}. Then for all $H \subseteq G$, we have that $(H, \circ)$ is a subgroup of $(G, \circ)$ iff all the following hold:

(i) $e \in H$;

(ii) H is closed under $\circ$, that is, $\forall a, b \in H$: $a \circ b \in H$;

(iii) H is closed under inverses, that is, $\forall a \in H$: $a^{-1} \in H$.

Proof (continued). We first deal with the identity element. If we compute in $(H, \circ)$, we have that $e_H \circ e_H = e_H$ (because e_H is the identity element of $(H, \circ)$), and if we compute in $(G, \circ)$, then we have that $e_H \circ e = e_H$ (because e is the identity element of $(G, \circ)$). But now $e_H \circ e_H = e_H \circ e$, and so by Proposition 2.2.4(a) applied to $(G, \circ)$, we have that $e_H = e$. So, $e \in H$, and it follows that (i) holds.

Theorem 2.2.9

Let $(G, \circ)$ be a group with identity element e, and with the inverse of an element $a \in G$ denoted by a^{-1}. Then for all $H \subseteq G$, we have that $(H, \circ)$ is a subgroup of $(G, \circ)$ iff all the following hold:

1. $e \in H$;
2. H is closed under $\circ$, that is, $\forall a, b \in H$: $a \circ b \in H$;
3. H is closed under inverses, that is, $\forall a \in H$: $a^{-1} \in H$.

Proof (continued). Finally, fix $a \in H$.

Theorem 2.2.9

Let $(G, \circ)$ be a group with identity element e, and with the inverse of an element $a \in G$ denoted by a^{-1}. Then for all $H \subseteq G$, we have that $(H, \circ)$ is a subgroup of $(G, \circ)$ iff all the following hold:

(i) $e \in H$;

(ii) H is closed under $\circ$, that is, $\forall a, b \in H$: $a \circ b \in H$;

(iii) H is closed under inverses, that is, $\forall a \in H$: $a^{-1} \in H$.

Proof (continued). Finally, fix $a \in H$. Since $(H, \circ)$ is a group, a has an inverse a' in $(H, \circ)$, so that $a \circ a' = e_H = e$.

Theorem 2.2.9

Let $(G, \circ)$ be a group with identity element e, and with the inverse of an element $a \in G$ denoted by a^{-1}. Then for all $H \subseteq G$, we have that $(H, \circ)$ is a subgroup of $(G, \circ)$ iff all the following hold:

1. (i) $e \in H$;
2. (ii) H is closed under $\circ$, that is, $\forall a, b \in H$: $a \circ b \in H$;
3. (iii) H is closed under inverses, that is, $\forall a \in H$: $a^{-1} \in H$.

Proof (continued). Finally, fix $a \in H$. Since $(H, \circ)$ is a group, a has an inverse a' in $(H, \circ)$, so that $a \circ a' = e_H = e$. On the other hand, if we compute in $(G, \circ)$, we get that $a \circ a^{-1} = e$.

Theorem 2.2.9

Let $(G, \circ)$ be a group with identity element e, and with the inverse of an element $a \in G$ denoted by a^{-1}. Then for all $H \subseteq G$, we have that $(H, \circ)$ is a subgroup of $(G, \circ)$ iff all the following hold:

(i) $e \in H$;

(ii) H is closed under $\circ$, that is, $\forall a, b \in H$: $a \circ b \in H$;

(iii) H is closed under inverses, that is, $\forall a \in H$: $a^{-1} \in H$.

Proof (continued). Finally, fix $a \in H$. Since $(H, \circ)$ is a group, a has an inverse a' in $(H, \circ)$, so that $a \circ a' = e_H = e$. On the other hand, if we compute in $(G, \circ)$, we get that $a \circ a^{-1} = e$. It follows that $a \circ a' = a \circ a^{-1}$,

Theorem 2.2.9

Let $(G, \circ)$ be a group with identity element e, and with the inverse of an element $a \in G$ denoted by a^{-1}. Then for all $H \subseteq G$, we have that $(H, \circ)$ is a subgroup of $(G, \circ)$ iff all the following hold:

1. (i) $e \in H$;
2. (ii) H is closed under $\circ$, that is, $\forall a, b \in H$: $a \circ b \in H$;
3. (iii) H is closed under inverses, that is, $\forall a \in H$: $a^{-1} \in H$.

Proof (continued). Finally, fix $a \in H$. Since $(H, \circ)$ is a group, a has an inverse a' in $(H, \circ)$, so that $a \circ a' = e_H = e$. On the other hand, if we compute in $(G, \circ)$, we get that $a \circ a^{-1} = e$. It follows that $a \circ a' = a \circ a^{-1}$, and so by Proposition 2.2.4(a) applied to $(G, \circ)$, we have that $a' = a^{-1}$, and consequently, $a^{-1} \in H$. This proves (ii). $\square$